10.17625/NKE.2012.008

ZRÍNYI MIKLÓS NEMZETVÉDELMI EGYETEM
HADTUDOMÁNYI KAR
KATONAI MŰSZAKI DOKTORI ISKOLA

GYÁNYI SÁNDOR

Túlterheléses informatikai támadási módszerek és a velük szemben alkalmazható védelem

Doktori (PhD) értekezés

Témavezető: Prof. Dr. Kovács László mk. alezredes

2011. BUDAPEST

Tartalomjegyzék

BEVEZETÉS

Az informatika alig néhány évtized leforgása alatt része lett mindennapjainknak, egyre bonyolultabb rendszerek vesznek bennünket körbe, befolyásolják életünket. Ezzel párhuzamosan a modern társadalom informatikai függősége is növekszik, ami komoly veszélyekkel jár a közigazgatás, a védelmi szféra, de közvetlenül az állampolgárok számára is. Korábban ismeretlen fenyegetések jelennek meg, amelyek egyre nagyobb károkat képesek okozni. Túlzás nélkül elmondható, hogy az utóbbi pár év az informatikai biztonság területén soha nem látott eseményeket hozott. A megerősödött polgári engedetlenségi mozgalom fegyverként kezdte alkalmazni a számítógépes hálózatokon működő tagjait, különböző aktivista csoportok heteken, hónapokon át tartó internetes akciókkal támadták a nekik nem tetsző szervezeteket, személyes adatokat tulajdonítottak el és hoztak nyilvánosságra. Egyre több bizonyíték utal arra, hogy a virtuális teret az államok is saját, nem feltétlenül békés céljaikra kívánják használni. A hadviselésben is sok helyen paradigmaváltás következett be, több állam is deklarálta, hogy lehetséges veszélynek tartja a kiberháborút, és a számítógépes hálózatokat is harctérnek tekinti. Emellett nagyszabású adatlopási ügyekre is fényt derült, amelyek esetében az állami közreműködés sem zárható ki.

A számítógépes kártevők új generációja jelent meg, immár komoly veszélyként kell tekinteni az informatikai eszközökkel végrehajtott szabotázsakciókra, amelyek nem csak információs, de kritikus infrastruktúrákat is veszélyeztethetnek. Megjelentek, és hatalmas tempóban kezdtek terjedni az olyan mobilkommunikációs eszközök, amelyek gyakorlatilag teljes értékű számítógépként képesek működni az egyre gyorsabb mobil adatátviteli hálózatokon keresztül. Az informatika a hétköznapok egyéb területein is megjelent, a szórakoztató elektronikai berendezések egyre komplexebbek lesznek, itt is felmerül az adatátviteli hálózathoz csatlakozás igénye. Ezek a folyamatok egyrészt új, soha nem látott szolgáltatásokat nyújtanak, azonban emellett a sérülékenységek új lehetőségét is megteremtik.

A számítógépes rendszerek védelmével kapcsolatban legnagyobb figyelmet a különböző, szofisztikált eljárások segítségével végrehajtott cselekmények kapják, amelyekkel a célpont felett a támadó képes a teljes ellenőrzést megszerezni, holott sok esetben egyszerűbben, nyers erővel is lehet kárt okozni. A célpont erőforrásait túlterhelve is megbéníthatóvá válik anélkül, hogy a rendszerbe bárki is sikeres betörést hajtana végre. A túlterhelés érkezhet a világ bármelyik pontjáról, és a szokásos védelmi

intézkedések – megfelelő üzemeltetési szabályok, hitelesítési, fizikai és hozzáférési biztonsági megoldások – nem garantálják a célpont megfelelő védelmét. Míg a szokásos informatikai támadásokra kialakult kockázatbecslési, megelőzési és elhárítási eljárások állnak rendelkezésre, addig a túlterheléses támadások hatásossága az egymás ellen ütköztetett erőforrások nagyságától függ, ezért mind a felkészülés, mind a védekezés nehezen kivitelezhető. Az erőteljes védelmi mechanizmusokkal ellátott információs infrastruktúrák közvetlen megtámadása helyett egyszerűbb a sokkal kevésbé védett eszközöket célba venni, majd az ezek feletti ellenőrzés megszerzése után, támadó eszközként használni az erőforrásaikat. Az egyre elterjedtebb számítógépes kártevők felhasználásával bárki – a szükséges ismeretek birtokában – képes lehet megfertőzni nem megfelelően védett informatikai eszközöket, majd azokból olyan támadó kapacitást létrehozni, amely komoly veszélyt jelent a nagyobb erőforrásokkal rendelkező informatikai rendszerek számára is. Az így kialakított hálózatokba bevont számítógépek darabszáma elérheti a több tízezret is, amely jelentősen nehezíti mind a támadás elleni védekezést, mind pedig a támadó hálózat felszámolását is.

Az elmúlt években rendszeressé váltak a kisebb-nagyobb károkat okozó túlterheléses, úgynevezett DoS[1] és DDoS[2] támadások, és a tapasztalatok azt mutatják, hogy ezek elhúzódó, sokáig fenntartható akciók sorozatából állnak, amelyek segítségével akár állami információs infrastruktúrákat is lehetséges megbénítani. Hatásossága és viszonylagos egyszerűsége miatt a hadseregek és különböző politikai szervezetek figyelmét is felkeltette a módszer.

A tudományos probléma megfogalmazása:

A nyilvános adatátviteli hálózatra kapcsolódó kiszolgáló számítógépek üzemeltetése során sokszor tapasztalhatók olyan, elsőre megmagyarázhatatlannak tűnő jelenségek, rendellenességek, amelyek a gépek működésének lelassulását, időnként pedig működésképtelenségét okozzák. A hibajelenségek vizsgálata során az eszközök meghibásodására visszavezethető problémák mellett egyre többször nyer bizonyítást, hogy ezek szándékos támadások, amelyek a rendszer túlterhelését célozzák. Ilyen esetekben a védekezés első lépése mindig a támadási módszer felismerése, mivel ez alapján lehetséges a védelmi eljárás kiválasztása. A védelmi eljárások egy DoS vagy

[1] DoS: Denial of Service. A szolgáltatás működésképtelenségét okozó támadás.
[2] DDoS: Distributed Denial of Service. A DoS támadás olyan változata, amikor a támadásban egy időben nagyszámú végpont vesz részt.

DDoS támadás esetén többnyire a működőképesség minimális színvonalon történő fenntartására irányulnak egészen addig, amíg az akcióban részt vevő végpontok semlegesítése megtörténik, vagy pedig az esemény előidézője magától befejezi tevékenységét. A minimális működési szint fenntartása is gondokat okozhat, mivel a legtöbb információs rendszer nem rendelkezik akkora erőforrás tartalékkal, ami a normál működési igénybevétel többszörösét is kibírná. Fontos kérdés, hogy a védekezés helyett milyen lehetőségek vannak a megelőzésre, különös tekintettel az informatikai hálózatokban működő rosszindulatú komponensek azonosítására. A felderítés során a felhasználók által forgalmazott adatok vizsgálatára lehet szükség, ezért nem elhanyagolható kérdés az adatvédelem, illetve a számítógépes végpontok tulajdonosainak egyéb jogai sem. A cél nem szentesítheti az eszközt, tehát olyan eljárásokra van szükség, amelyek összhangba hozzák a közérdek (csökkenteni a kibertér veszélyeztetettségét) és a magánérdek (ne sérüljenek személyiség- vagy adatvédelmi jogok) igényeit.

Napjaink eseményei egyre inkább előtérbe helyezik a kiberteret,[3] az információs társadalom egyik alappilléréről lévén szó. Ezért a veszélyek felmérése, megismerése során fontos a terrorizmus és a bűnözés kapcsolatának vizsgálata is.

Kutatásaim során az információs infrastruktúrák elleni támadási módszereket vizsgáltam, és azt tapasztaltam, hogy azok egyre komplexebbé váltak. A korábban jól elkülöníthető veszélyforrások összemosódtak, ezek szintéziséből új fenyegetések jöttek létre, amelyeket előszeretettel használnak számítógépes bűnözők és különböző politikai célú szervezetek is. A lehallgatásra vagy a célpont feletti uralom átvételére irányuló tevékenységek mellett előtérbe kerültek azok a módszerek, amelyek a célpont működésének ellehetetlenítését okozzák. Ezekre a módszerekre nincsenek általános érvényű védelmi szabályok, az újabb DDoS akciókban pedig annyira sok számítógépes végpont jelenik meg támadóként, hogy ellenük nem alkalmazható a korábban bevált számítógépes hálózati adatszűrés. Egy másik, általánosan használt eljárásban a célpont igyekszik annyi erőforrást mozgósítani, amivel képes felülmúlni a támadó rendelkezésére álló kapacitást, és így „túlélni” az akciót, ennek kivitelezhetősége és főként gazdaságossága azonban kételyeket ébresztett bennem.

[3] A számítógépes hálózatok és az általuk összekötött számítógépek és egyéb berendezések egy virtuális teret alkotnak, amelynek angol elnevezése a „cyberspace”, magyarul pedig „kibertér”. A kifejezést William Gibson használta először „Izzó króm” című könyvében.

A legkézenfekvőbbnek tűnő megoldás az, ha a DDoS támadások elindítóját azonosítják, és vele állíttatják le az akciót. Ez könnyű feladat lenne, ha a saját eszközeit használná fel, azonban a számítógépes hálózatok természetét kihasználva ezt – érthető okból – próbálják elkerülni. A vírusok és más kártékony programok fejlesztői olyan megoldásokat szolgáltatnak, amikkel megnehezítik a tényleges elkövető személyének felderítését. A korszerű számítógépes kártevők már rendelkeznek olyan funkciókkal is, amelyek segítségével a fertőzött számítógép – vagy egyéb eszköz, amely célszámítógépet tartalmaz, és számítógépes hálózatra kapcsolódik – képes feladatokat fogadni egy központi irányító személytől. Ezek a berendezések hálózatba szerveződnek, és az így kialakult, úgynevezett botnetek kiválóan alkalmasak a túlterheléses támadások kivitelezésére. Egy botnet nagyon sok elemből állhat, ezért a semlegesítése nem könnyű feladat, főként, ha egy ilyen támadás már folyamatban is van. Nagyon fontos feladatnak tekintem ezek felderítését a tényleges támadás megkezdése előtt, amikor az időtényező még nem annyira kritikus.

Kutatási hipotézisek:

Munkám során abból a feltételezésből indultam ki, hogy a túlterheléses DoS és DDoS támadások növekvő veszélyt jelentenek az információs infrastruktúrára, ezért indokolt részletes és alapos vizsgálatuk. Feltételeztem továbbá, hogy lehetséges olyan védelmi eljárásokat alkalmazni, amelyek segítségével elfogadható erőforrás felhasználás mellett is lehetséges egy informatikai rendszer működését fenntartani egy DDoS incidens közben. Hipotézisem szerint a DDoS támadásokért felelős kártékony hálózatok felhasználási célja nem csak a túlterheléses támadások kivitelezése, ezért az egyéb tevékenységük során is keletkezhetnek összegyűjthető nyomok, amelyek segítségével lehetséges a botnetek tagjait felderíteni, és semlegesíteni még azelőtt, hogy a tényleges DDoS akció elindulna.

Kutatási célkitűzéseim:

Célul tűztem ki a különböző túlterheléses támadások elleni védelmi módszerek, illetve az ilyen akciók kivitelezésére alkalmas eszközök elleni ellentevékenységek kutatását.
Ennek elérése érdekében az alábbi részfeladatokat tűztem ki magam elé:

1. Megvizsgálni a különböző típusú informatikai támadási módszereket, azok veszélyeit és az általuk okozható károkat, az informatikai támadások és a hadviselés, terrorizmus kapcsolatát.
2. Felmérni a túlterheléses támadások hatásait, a velük szemben alkalmazható védelmi módszereket, a szolgáltatások fenntartását biztosító eljárásokat és ezek hatékonyságát a védelmi intézkedések megvalósíthatósága és az igénybe vett erőforrások nagysága alapján. A minél gyorsabb felismerés és azonosítás érdekében felkutatni és kategorizálni az interneten működő informatikai infrastruktúrák ellen kivitelezhető DoS és DDoS támadási módszereket, és működési elvüket.
3. Megvizsgálni a botnetek egyéb funkcióit abból a szempontból, hogy a működésük során milyen nyomok keletkezhetnek, amelyek az ilyen hálózatokat alkotó, fertőzött végpontokhoz vezetnek.
4. Olyan, a túlterheléses támadásra alkalmas számítógép-hálózati végpontok felderítésére alkalmas eljárást keresni, amely során biztosítható, hogy a végpontok tulajdonosainak személyiségi és adatvédelmi jogai ne csorbuljanak.
5. Meghatározni egy olyan rendszer alapvető funkcióit, amely segítségével a DDoS támadásokért felelős végpontok még a tényleges támadás megkezdése előtt semlegesíthetők. Megvizsgálni annak lehetőségét, hogy ez a rendszer milyen szervezeti keretek között működhetne.

A kutatásaim során alkalmazott módszerek:

Széleskörű irodalomkutatást folytattam az elérhető hazai- és nemzetközi irodalomban. A kutatás – témám természete és a technológia gyors változásai miatt – nagyobb részben az elektronikus, kisebb részben a nyomtatott szakirodalmat érintette. A forrásanyagok rendszerezésével és feldolgozásával bővítettem a kutatási céljaim eléréséhez szükséges szaktudásomat. Minden olyan esetben, amely során erre lehetőség volt, saját gyakorlati teszteket és számítógép-hálózati kísérleteket végeztem, amelyek eredményeivel igazoltam felállított elméleteimet.

Rendszeresen részt vettem – mind hallgatóként, mind előadóként – szakmai konferenciákon, kutatásaim eredményét rendszeresen publikáltam szakmai folyóiratokban. Munkahelyemen több olyan kutatás-fejlesztési projektben működtem közre, amely segítette szakmai fejlődésemet.

Értekezésemet az alábbi szerkezetben készítettem el:

1. fejezet: bemutatom az informatikai infrastruktúrák elleni támadások módszereit, kategóriáit, különös tekintettel a kritikus infrastruktúrák sebezhetőségeire. Elemzem az ilyen akciók katonai vonatkozásait, a hazai és nemzetközi incidenskezelés folyamatait. Egy elképzelt komplex támadás példáján keresztül bemutatom egy hazánk elleni akció lehetséges lefolyását, következményeit.

2. fejezet: bemutatom az informatikai támadások, elsősorban az úgynevezett DDoS támadások károkozó képességét, illetve az ilyen akciók elleni védekezés lehetőségeit. Kategorizálom a túlterheléses támadásokat az alkalmazott módszer és a megtámadott egység szempontjából. A szakirodalomban fellelhető gyakoribb módszereket besorolom a definiált kategóriákba, így megkönnyítve az alkalmazható védekezési lehetőségek kiválasztását.

3. fejezet: elemzem a botnetek működésével, terjedésükkel kapcsolatos információkat. Ismertetem a fejlődéstörténetüket, valós és lehetséges felhasználási területeiket a számítógépes bűnözők, terroristák és katonai szervezetek szempontjából.

4. fejezet: rámutatok arra, hogy egy bekövetkezett DDoS támadás során elkerülhetetlen működéskiesések lépnek fel, így fontos a megelőző tevékenység folytatása. Bemutatom egy saját kísérletem eredményét, amely segítségével a botnetek fertőzött tagjai egyszerűen, pusztán a már meglévő adatok feldolgozásával lokalizálhatók, így könnyen semlegesíthetők.

1. FEJEZET
INFORMATIKAI TÁMADÁSOK

A számítógépes hálózatok által összekötött információs rendszerek olyan színteret hoztak létre, amely korábban ismeretlen akciók kivitelezését teszi lehetővé. Az így kialakult virtuális tér, vagy kibertér felkeltette a szervezett bűnözés, a terrorizmus és a hadseregek figyelmét is. A virtuális térben kivitelezett támadások veszélyeztethetik nem csak az információs, de a társadalom számára kiemelt jelentőségű, létfontosságú infrastruktúrákat is.
Mivel az informatika mindennapi életünkkel szorosan összefonódott tudományág, szakkifejezéseinek értelme, jelentése a gyakori és széleskörű használat miatt sok esetben nem egyértelmű, nem pontos, használatuk félrevezető lehet. Ezért fontosnak tartom néhány, a dolgozatomban fellelhető informatikai szakkifejezés egyértelműsítő magyarázatát.

Az információs rendszerek „*szűkebb értelemben funkcionálisan összetartozó, egységes szabályozás hatálya alá tartozó, szervezett információs tevékenységek, folyamatok. Tágabb értelemben az egyes információs rendszerek részét képezik az általuk kezelt információk, az információs tevékenységeket végrehajtó szereplők és a végrehajtás során felhasznált erőforrások is.*” [1]

Informatikai rendszer alatt az információs rendszer egy részhalmazát értem, a [2] forrásnak megfelelően:

„Az informatikai rendszer (általában) eszközök, programok, adatok, valamint a működtető személyzet információs funkciók, tevékenységek megvalósítására létrehozott rendszere.”

Számítógépes hálózatoknak olyan kommunikációs hálózatokat tekintettem, amelyek számítógépeket – nem csak általános felhasználású, hanem célszámítógépeket is – kötnek össze egymással. Ezzel szemben az „*informatikai hálózat elemei nem kizárólag számítógépek, hanem bármilyen információs tevékenységet támogató rendeltetésű (tágabb értelemben vett informatikai), vagy egyszerűen csak más rendeltetésű, de*

információs képességekkel rendelkező (informatizált) technikai eszközök is lehetnek." [3]

Információs infrastruktúrák a [4] forrás definíciója szerint:

„Az információs infrastruktúrák olyan állandó helyű vagy mobil létesítmények, eszközök, rendszerek, hálózatok, illetve az általuk nyújtott szolgáltatások összessége, amelyek az információs társadalom működéséhez szükséges információk megszerzését, előállítását, tárolását, elosztását, szállítását és felhasználását teszik lehetővé."

A hadtudományok területén az elmúlt évtizedekben megjelent az „információalapú hadviselés" kifejezés. Ennek megfelelően a hadszínterek közé is bevonult az információs hadszíntér, ahol a katonai terminológia által információs műveleteknek nevezett tevékenységek folytathatók. Az információs műveletek körébe a következők tartoznak: [5]

- az információs infrastruktúrák, vezetési objektumok fizikai pusztítása (Physical Destruction – PD);
- katonai megtévesztés (Military Deception – MILDEC);
- műveleti biztonság (Operation Security – OPSEC);
- elektronikai hadviselés (Electronic Warfare – EW);
- pszichológiai műveletek (Psychological Operations – PSYOPS);
- számítógép-hálózati hadviselés (Computer Network Operations – CNO).

Értekezésemben alapvetően csak a számítógépes és számítógép-hálózati támadásokkal foglalkozom, ezért ezekre a tevékenységekre – amelyek az információs műveletek legfiatalabb tagjai – összefoglaló névként az „informatikai hadviselés" kifejezést használom.

A fejezet további részében az informatikai támadások lehetséges módszereinek kutatási eredményeit, illetve a bekövetkezett támadások tapasztalatait adtam meg. Bemutatom a támadások rendszertani besorolására alkalmas osztályozások közül néhány, munkám szempontjából relevánsnak tekinthetőt, illetve a különböző típusú támadások által okozott károk statisztikájának eredményeit. Végül felvázolok egy elképzelt komplex informatikai támadási forgatókönyvet.

1.1 Informatikai hadviselés

Az informatikai berendezések és az őket egymással összekötő informatikai hálózatok egyre nagyobb szerepet kapnak a mindennapok során. A polgári alkalmazások mellett a katonai műveletekben is elengedhetetlenné válik az informatikai támogatás, az információs fölény kivívása.

A virtuális térben lényegesen egyszerűbb bármilyen támadást elindítani, mint a valódi helyszíneken. Nem szükséges haditechnika felvonultatása, ennek megfelelően a szükséges erőforrások mennyisége is jóval kisebb, mivel a harcolókat itt a számítógépes hálózatok végpontjai illetve önállóan működő számítógépes programok helyettesítik. A mai nyilvános informatikai hálózatok (és itt leginkább az internetre[4] kell gondolni) alacsony költségek mellett jelentős mennyiségű adat mozgatását teszik lehetővé fizikailag egymástól nagy távolságokra levő végpontok között. Az internetre bárki csatlakozhat, a mai technikai fejlettség mellett a szegényebb, katonailag jelentéktelenebb államok, militáns csoportok, terroristák vagy akár magánszemélyek is komoly eszközparkot képesek felvonultatni. Az informatikai támadásokkal szemben a fejlettebb infrastruktúrával rendelkező államok sokkal sebezhetőbbek, mint egy fejletlenebb hátterű ország, így az ilyen akciók kiválóan megfelelnek az aszimmetrikus hadviselés igényeinek. Nem utolsó szempont az sem, hogy az elkövetőket azonosítani is rendkívül problémás, a semlegesítésükről nem is beszélve.

A támadásokban – akár áldozatként, akár támadóként – szereplőket három nagy csoportba sorolhatjuk:

- önállóan tevékenykedő magánszemélyek;
- csoportok, szervezetek;
- államok, állami szervezetek.

A „magánszemély támad államot” kategória által okozott probléma nemzetbiztonsági jelentőségű is lehet, ha a célpont fontossága azt indokolja, ilyenkor egy magányos „merénylő” ellen kell fellépnie az állami apparátusnak. Elszigetelten működő támadó általában nehezen képes eredményeket elérni, így az állami célpontnak – és csak annak - komoly károkat okozó informatikai támadás nehezen kivitelezhető. Az állami informatikai rendszerek folyamatosan ki vannak téve támadásoknak, azonban ezekről

[4] Maga az „internet” szó több, egymással összekötött helyi hálózatra utal, így internetből rengeteg van a világon. Létezik egy mindenki által használható, nyilvános internet is, ezért véleményem szerint ebben az esetben indokolt lenne tulajdonnévként használni. A magyar helyesírás szabályai szerint azonban ennek a hálózatnak a neve is kisbetűvel írandó, ezért a későbbiekben is így hivatkozom rá.

nehezen megállapítható az elkövető magányos volta. Az első világméretű pusztítást okozó, magát az interneten terjesztő számítógépes malware[5] a 2000. május 4-én elszabadult „I love you” nevű féreg volt, amely az agresszív terjedésével több komoly – így állami tulajdonú - levelező rendszert is időszakosan működésképtelenné tett. Szerzőjeként aztán egy Onel de Guzman nevű Fülöp-szigeteki diákot azonosítottak, akit azonban a helyi törvények szerint nem lehetett elítélni, mivel a Fülöp-szigeteken a számítógépes víruskészítés a cselekmény időpontjában nem számított bűncselekménynek [6]. Az eset kiválóan rávilágít arra a tényre, hogy a támadások a világ bármelyik pontjáról indulhatnak, így a támadó elleni állami fellépést nehezítheti a támadó tartózkodási helyén érvényes jogszabályi háttér is.

A „szervezet támad államot” a legvalószínűbb, előbb-utóbb biztosan bekövetkező esemény. A különböző szélsőséges csoportok, terrorszervezetek előszeretettel használják az internetet egymás közti titkos kapcsolattartásra, propagandaanyagok terjesztésére, toborzásra. Az utóbbi időben elsősorban az iszlám terrorizmus okozza a nyugati világ számára a legtöbb problémát, az ilyen csoportok tevékenysége különösen erős Nagy-Britanniában és a szintén jelentős iszlám közösséggel rendelkező Németországban. [7] A kapcsolattartást és a propagandaterjesztést nehéz korlátozni: a kapcsolattartásban a terroristák is képesek alkalmazni a titkosítás eszközeit, míg a propaganda terjesztését a nyugati demokráciákban komolyan vett szólásszabadság teszi lehetővé. Iszlám ideológiákat követő hackerek komoly mennyiségű weboldalt támadtak meg és törtek fel sikeresen, helyeztek el rajta propaganda jellegű üzeneteket. Ezek az akciók azonban általában kevésbé gondosan védett informatikai rendszereket értek, és az ilyen típusú támadások ellen hatékony óvintézkedések tehetők.

Előbb-utóbb azonban fegyverként is felhasználják majd az informatikai hálózatokat, nem csak célpontként tekintenek rá. A háttérben zajlanak a „fegyverkezési verseny” folyamatai, szinte elképzelhetetlen mennyiségű számítógépet vonnak uralmuk alá különböző szervezetek, amelyeket aztán hálózatba szerveznek, divatos elnevezéssel „zombie” hálózatokat, vagy más néven botneteket alakítanak ki. Ezeket a botneteket valószínűleg bűnözői csoportok hozzák létre, megfelelő ellenszolgáltatásért cserébe az ilyen kapacitások bérelhetők is tőlük. Ez azt jelenti, hogy akár egy terrorcsoport is képes viszonylag olcsón hozzájutni és támadásokat indítani velük. Fontosságuk miatt a botnetekkel az értekezés későbbi részében külön foglalkozom.

[5] Malware: a „malicious software” szavak összevonásából született kifejezés.

A legérdekesebb esetek azok, amelyekben az állam, vagy valamelyik szervezete kerül a támadó szerepkörébe, ugyanis egy nyilvánvaló bűncselekmény elkövetése mindig is kényes terület. Az „állam támad magánszemélyt” esete nem túl valószínű forgatókönyv, bár sokan támadásnak tekintik az állam túlzott érdeklődését az állampolgárok magánügyei iránt is. A végrehajtó hatalom természetesen a pozitív szándékait emeli ki: a minél több információ begyűjtésével könnyebben deríthetők fel a különböző bűnözői vagy egyéb csoportok szándékai, tervei. Ezzel szemben az állampolgárok igyekeznek saját titkaikat biztonságban tudni még akkor is, ha semmi félnivalójuk az államtól. Emlékezetes Philip Zimmermann és a PGP (Pretty Good Privacy) elektronikus levéltitkosító program esete. A PGP 1991-es megjelenése után az USA kormányzata jogi hadjáratot indított ellene, amelyet csak 1996-ban szüntettek be. [8] Az ok nyilvánvalóan az volt, hogy a PGP-vel titkosított üzeneteket az akkori technológiai szinten még a kormányzati erőforrások birtokában sem lehetett kellő gyorsasággal megfejteni.

Ha egy állam egy szervezet ellen követ el informatikai támadást, akkor a logika szabályai szerint annak megelőző jellegűnek kell lennie, csak valamilyen veszélyhelyzet kialakulásának elkerülését szolgálhatja. A támadónak – tehát az államnak, vagy egy szervezetének - kellő indokkal, bizonyítékkal kell rendelkeznie, a támadásnak a fenyegetettséggel arányosnak kell lennie, amennyiben a fegyveres konfliktusokra érvényes szabályokat próbáljuk rájuk alkalmazni. A megelőző támadás indokoltsága és különösen a módszere sok vitás pontot tartalmaz, amelyekkel érdemes behatóbban foglalkozni.

Az „állam támad másik államot” kategória túllép a civil szféra határain, hiszen ez két szuverén hatalom közti olyan katonai konfliktusnak is tekinthető, amelyet nem hagyományos fegyverekkel vívnak. A legelső ilyen esetként sokan a 2007. májusi észtországi kormányzati szerverek ellen elkövetett DDoS támadást tekintik, jóllehet az orosz állam szerepe nem kellően bizonyított az akcióban. Az észt szakemberek sok olyan végpontot azonosítottak, amelyek orosz állami hivatalokban működtek, azonban ezek a végpontok lehettek fertőzött gépek is, amelyek egy botnet tagjaként vették ki részüket a támadásból. Érdemes kitérni az üzemeltetői felelősség kérdésére, hiszen ilyen esetekben a nem kellő gondossággal üzemeltetett számítógépek által végzett tevékenység kiválthat egy ellencsapást, vagy hosszas jogi eljárást.

Az államok közti kibertámadások rengeteg jogi problémát is felvetnek, amivel mindeddig keveset foglalkoztak a döntéshozók. Kína már az 1990-es évek elején

kialakította saját, kiberhadviselésre szolgáló katonai infrastruktúráját. A Kínai Néphadsereg két ezredesének 1999-ben tett nyilatkozata szerint egy Tajvan miatti USA-Kína incidens esetén kínai hackerek képesek lennének lerombolni az USA polgári informatikai infrastruktúráját. A kínaiak mellett természetesen más országok (Franciaország, Oroszország, Nagy-Britannia, Izrael) is rendelkeznek kifejezetten katonai jellegű informatikai támadások végrehajtására kiképzett állománnyal. [9]

1.2 Informatikai támadások és a terrorizmus

Az "információs terrorizmus" kifejezés a valódi terrorizmus fogalmának átültetése az információs rendszerek világába. Ahhoz, hogy eldöntsük, létezik-e egyáltalán ilyen, célszerű elsőként megvizsgálni, mi is az a terrorizmus?

Definíciószerűen a terrorizmus [10]:

1. megfélemlítés, zsarolás, bosszúállás céljából elkövetett rémtettek sorozata;
2. politikai okokból végrehajtott merényletek (emberrablás, robbantás, gyilkosság stb…) sorozata.

Vagy egy másik definíció szerint [11]:

„Terror, *megkülönböztetés nélküli támadás*: minden olyan erőszakos cselekmény, vagy azzal való fenyegetés, amelynek elsődleges célja, hogy rettegést keltsen a polgári lakosság körében."

Az információs terrorizmus tehát különböző merényletek végrehajtása információs rendszerek ellen, azonban fontos megjegyezni, hogy egy ilyen akció elkövetése önmagában nem jelent feltétlenül terrorista tevékenységet. A különböző számítógépes bűnözők által elkövetett cselekményeket általában anyagi haszonszerzés, a learatott dicsőség motiválja, míg a terroristák politikai, vallási vagy ideológiai meggyőződésből követik el tetteiket. Egy információs rendszer megtámadása, működésének lehetetlenné tétele nagy sajtóvisszhangot vált ki, a terrorizmus egyik legfontosabb motiváló tényezője pedig a minél nagyobb nyilvánosság, amely fontos része a stratégiának.

A „cyber-terrorism" angol kifejezés egy Barry C. Collin nevű szakértőhöz kötődik, aki 1997-ben először vont párhuzamot a valódi és a virtuális világban elkövetett terrorcselekmények között. A fogalomnak többféle definíciója ismert. Egy tág értelmezés Kevin Coleman nevéhez kötődik [12]:

"The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological,

religious, political or similar objectives. Or to intimidate any person in furtherance of such objectives."

A fenti idézet magyarul a következő:

„Előre megfontolt szándékkal elkövetett pusztító tevékenység, vagy ezzel való fenyegetés alkalmazása számítógépek és/vagy számítógépes hálózatok ellen, a károkozás vagy egyéb társadalmi, ideológiai, vallási, politikai illetve hasonló célok elérése érdekében. Ide tartozik még valamely személy megfélemlítése is az előbbi okokból."

A definíció alapján bárki vagy bármely szervezet besorolható a kategóriába, aki a felsorolt célok érdekében követ el informatikai elemeket érintő cselekményt. Ha azonban ugyanazokat a paramétereket támasztjuk az információs terrorizmussal szemben is, mint a valódi terroristákkal szemben, akkor az ilyen, ismertté vált akciók története meglehetősen szegényes lesz. Az első és mindmáig egyetlen, bizonyítottan terrorszervezet által elkövetett akciónak legtöbben a Tamil Tigrisek[6] internetes akciókra szakosodott szervezete (Internet Black Tigers) által 1997 augusztusában elkövetett email támadását tekintik. [13] A csoport napi 800 elektronikus levél elküldésével túlterhelte Sri Lanka külföldi nagykövetségeinek levelezőrendszerét, közel két hétre működésképtelenné téve azt. Természetesen ezen kívül is voltak gyanús esetek, azonban hivatalosan egyetlen terrorista szervezet sem vállalta a felelősséget.
Mivel a „hagyományos" terrorista akciók esetében sem szükségszerű, hogy egy ismert szervezet hajtson végre akciót, ezért véleményem szerint az információs terrorizmust az akciók célja illetve hatásai alapján lehet és kell megítélni. Így már elég jelentős történelemmel „büszkélkedhet" ez a bűnelkövetői magatartás. Néhány példa, a teljesség igénye nélkül:

- 1997-ben egy számítógépes bűnöző az USA Worcester (MA) város repülőterének kommunikációs hátterét biztosító telefontársaság számítógépes rendszerébe tört be, és leállította az egyik, a reptér telefon- és adatforgalmát vezérlő számítógépet. Emiatt a reptér légi irányítása hat órán keresztül működésképtelenné vált. [14]

[6] Liberation Tigers of Tamil Eelam (LTTE).

- 2003-ban, az iraki háborúra válaszul a Unix Security Guards (USG) nevű iszlám csoport közel 400 weboldalt tört fel és helyezett el rajta[7] ellenállásra buzdító üzeneteket. [15]
- Ugyancsak 2003-ban az USA antarktiszi Amundsen-Scott kutatóállomásának két email szervere közül az egyiket és egy csillagászati adatokat tároló számítógépet törték fel román kalózok, és próbáltak az ott talált információkból zsarolás segítségével pénzt csinálni. John Ashcroft államügyész a másfél évvel korábbi USA PATRIOT Act alapján terrorcselekménynek minősítette az ügyet, állítása szerint a betörés során a román elkövetők átvették a hatalmat az energiaellátást irányító gép felett, így az állomáson tartózkodó 58 tudós életét fenyegették. Ezt az állítást a későbbi vizsgálatok – és az ott tartózkodók is – határozottan cáfolták. [16]
- 2010 őszén és telén a hamar hírhedtté vált Anonymous csoport DDoS támadásokat intézett számos weboldal ellen. Az áldozatok közt volt a Motion Picture Association of America (MPAA), a Recording Industry Association (RIAA), a Hustler magazin, a fájlcserét élesen támadó Gene Simmons zenész. Az akciók alapja a Pirate Bay ellen folyó per volt, később a WikiLeaks ellehetetlenítésében szerepet játszó weboldalak is sorra kerültek. Ilyenek voltak a különböző, a WikiLeaks alapítója számára pénzgyűjtést biztosító, majd befagyasztó oldalak (Mastercard, VISA, Paypal, Amazon). [17] Az Anonymous később odáig ment, hogy az egyiptomi zavargások idején az egyiptomi kormányt is megfenyegette. [18]

Annak ellenére, hogy eddig nem ez volt a fő tevékenységi területük, feltételezhetjük, hogy a terroristák figyelmét nem kerüli el a virtuális tér, és a terveikben komoly szerepet fog játszani. Fouad Hussein, egy jordán újságíró 2005 végén megjelent könyvében (al-Zarqawi - al-Qaeda's Second Generation) az Al-Kaida belső köreiből[8] származó információkat oszt meg az olvasóival. Eszerint az Al-Kaida 2020-ig fogja megvalósítani a Nyugat ellenes terveit, a következő fázisokon keresztül [19]:

1. fázis, az „ébredés"

Ez a fázis 2000-től 2003-ig tartott. A tényleges cselekmények 2001. szeptember 11-től, az USA-t ért terrortámadásoktól kezdődtek és 2003-ig, Bagdad elestéig tartottak. A

[7] Egy feltört weboldal megváltoztatását valamilyen figyelem felkeltési célból deface-nek nevezik.
[8] Fouad Hussein együtt ült börtönben az ismert terroristával, al-Zarqawival, és később is kapcsolatban állt az al-kaida vezetőségéhez tartozó személyekkel.

2001-es támadások célja az volt, hogy az USA és szövetségesei hirdessenek harcot az iszlám ellen, ami a muszlimokat ráébreszti a harc fontosságára. Ez a fázis az Al-Kaida stratégái szerint sikeres volt, a harctér megnyílt, az amerikaiak és szövetségeseik közelebbi és könnyebb célpontokká váltak.

2. fázis, a „szemek felnyitása"

Ezt a fázist a 2003-2006 közötti időszakban tervezték végrehajtani (a könyv 2005-ben íródott), célja a nyugati összeesküvés-elmélet propagálása az iszlám közösségben. Új tagokat szerveztek be, és csoportokat hoztak létre az arab országokban. Az egyik első, de mindenképpen a legnagyobb hatású ilyen aktivista a magát Irhabi007[9]-ként nevező Younis Tsouli volt. A 2003-as iraki háború kitörése után az Al-Kaida is megkereste, és segítségével radikális iszlámista weblapokat hoztak létre. Tsouli emellett az amerikai katonák által készített videókat keresve, majd azokat elemezve segítséget nyújtott az amerikai katonai bázisok elleni támadások koordinálásában. Tevékenységéhez internetes csalásokkal szerzett pénzt, 2005. októberi letartóztatása után 16 év börtönbüntetést kapott. [20]

3. fázis, a „felemelkedés és talpra állás"

A tervek szerint ez 2007-2010 között volt esedékes és Szíriára fókuszált. Erre az időszakra terrortámadásokat terveztek Törökország és Izrael ellen. A szervezet irányítói szerint az Izrael elleni támadások segítségével növelhetik ismertségüket. A könyv megjelenése óta bekövetkezett események igazolták a szerző információit: 2006 nyarán a Libanonban komoly erőnek számító, Szíria és a shiita Irán támogatását élvező Hezbollah egy rajtaütés során foglyul ejtett két izraeli katonát. Erre válaszul Izrael légicsapásokat mért a Hezbollah vélt állásaira, majd szárazföldi akciót indított a határhoz közeli területek megtisztítása érdekében. [21]

Törökországban is történtek az al-kaidához köthető terroresemények, például az USA konzulátusa ellen. [22]

4. fázis

A 2010 és 2013 közötti időszakot öleli fel, az elsődleges célja pedig a gyűlölt – nyugatbarát - arab rezsimek megbuktatása, ami a reményeik szerint a helyi Al-Kaida csoportok megerősödéséhez vezet. Ezzel párhuzamosan az olajüzletben érdekelt cégek elleni támadások és az USA gazdasága elleni akciók fognak történni az információs terrorizmus eszközeivel.

---

[9] A szó jelentése terrorista, a 007 pedig utalás James Bondra.

A történelem ismét igazolta a szerzőt, 2010 végén Tunéziában [23] kezdődött események több arab kormány és a hatalomban állócsillagnak tűnő vezető bukásához vezettek.

A közeli jövőben várható, hogy az információs infrastruktúrák elleni akciók komoly problémákat okozhatnak. Bár az ilyen akciók legelterjedtebb típusa, a hacktivism - amelynek során különböző weboldalak feletti uralom megszerzésével és az ott található tartalom megváltoztatásával próbálják a képviselt ügyre felhívni a figyelmet – csak propaganda célokból veszélyes, de már léteznek ennél ártalmasabb formák is. A később ismertetett támadások és módszerek alkalmazásával már a kritikus infrastruktúra is veszélybe kerülhet, illetve nem elhanyagolható tényező az önkéntesek interneten történő toborzása sem. Oszama bin Laden likvidálása után sokan az Al-Kaida meggyengülését, sőt összeomlását jósolták, azonban dzsihádista weboldalakon megindultak a bosszúra felszólító kampányok. Az Al-Kaida 2011. augusztus 20-i közleményében 100 terrorakciót helyezett kilátásba Irak egész területén a ramadán alatt. Az ezt megelőző augusztus 15-i terrorhullámban 70-en haltak meg különféle merényletekben, így a további akciók valószínűsége nem elhanyagolható. [24]

1. ábra Deface áldozatául esett weboldal (forrás: The Hacker News – www.thehackernews.com)

5. fázis

Ebben az időszakban fogják kikiáltani az iszlám államot vagy kalifátust. A tervezők szerint a 2013-2016 közti időszakban Izrael meggyengülésével párhuzamosan az iszlám világra már olyan kevés hatása lesz a Nyugatnak, hogy ellenállástól nem kell tartani. Az terrorszervezet reményei szerint ez lesz egy új világrend kialakulásának kezdete.

6. fázis, a „teljes konfrontáció"

Hussein szerint 2016-tól az iszlám kalifátus harcot fog kezdeményezni a hívők és a hitetlenek közt, ahogy azt Oszama bin Laden is sokszor hangoztatta.

7. fázis, a „végső győzelem"

Ebben a végső szakaszban a terroristák szerint a világ többi részét legyőzi a másfél milliárd muszlim, és a kalifátus vitathatatlan győzelmet arat. Ez a fázis 2020-ra befejeződik, a háború pedig nem tart tovább két évnél.

A könyv állításai meghökkentőek, a megjelenés óta bekövetkezett események pedig a legtöbb állítását igazolják, véleményem szerint nagyon komolyan kell venni az információs terrorizmus szerepét, és küzdeni a virtuális tér biztonságáért.

1.3 Informatikai támadások taxonómiája

Az informatikai biztonság a Közigazgatási Informatikai Bizottság 25. számú ajánlásában [25] szereplő definíció szerint:

„Az informatikai biztonság az informatikai rendszer olyan – az érintett számára kielégítő mértékű – állapota, amelynek védelme az informatikai rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint a rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos."

Az informatikai támadás a célpont informatikai biztonságára veszélyes fenyegetés,[10] így a rendszerben tárolt információt, vagy a rendszer elemeit célozza meg. A védelmi intézkedések tervezésének egyik első lépése a fenyegetések, ezen belül pedig a szóba jöhető támadások felmérése. A támadások csoportosítására, rendszerbe foglalására sokféle szempontrendszer, osztályozási metódus található a szakirodalomban, ezért nagyon nehéz általános érvényű, minden esetre alkalmazható támadási taxonómiát

10 A fenyegetések Munk Sándor definíciója szerint: a biztonság alanyát veszélyeztető, a védendő tulajdonságokat károsan, a meg nem engedett/elfogadható mértéknél jobban befolyásoló potenciálisan káros [kölcsön]hatások. [126]

meghatározni. Attól, hogy egy akció során nem sérül a három fontos tényező (bizalmasság, sértetlenség és rendelkezésre állás), még nem biztos, hogy nem támadásról van szó. Edgar G. Amoroso „Fundamentals of Computer Security” [26] című könyvében rávilágít arra, hogy a támadások besorolása időnként nehézkes lehet. Elképzelhető olyan eset, amely során a támadó átveszi a célpont felett az ellenőrzés lehetőségét, de nem sérti meg az ott tárolt adatok bizalmasságát, nem módosítja vagy törli az adatokat, és nem veszélyezteti a rendelkezésre állást. Ez nem tekinthető biztonságos állapotnak, még akkor sem, ha a rendszer szempontjából tényleges káresemény nem történt.

Egy taxonómia számára szükséges feltételeket támasztani. Matt Bishop javaslata [27] szerint ezek:

- Egymáshoz hasonló sérülékenységek ugyanabba a kategóriába kerüljenek.
- A kategóriákba sorolás egyszerű legyen, lehetőleg egy „igen” vagy „nem” válasz segítségével.
- A kategóriák elnevezései legyenek egyértelműek.
- A besorolás alapja kizárólag technikai paraméterekre korlátozódjon.
- A sérülékenységek besorolhatók legyenek több osztályba is.

Más publikációk ennél több, vagy eltérő feltételeket tartanak szükségesnek, de véleményem szerint ezek a tulajdonságok egyértelművé teszik a besorolási osztályokat anélkül, hogy esetleg túlzottan szigorú követelményeket szabnának meg. A témában Daniel Lowry Lough [28] végzett egy nagyon alapos kutatást, a legfontosabb taxonómiák összevetésével. Kutatási céljaimmal összhangban ezek közül azokat a rendszerezési eljárásokat vizsgáltam meg, amelyek a számítógépes hálózatokon keresztül, távolról végrehajtható módszerekre is vonatkoznak.

Neumann és Parker a támadási eljárásokra 9 osztályt határozott meg:

- Külső adatgyűjtés: vizuális megfigyelés, felhasználók megtévesztése.
- Hardveres visszaélések: adathordozók megszerzése, kommunikáció lehallgatása, megzavarása, fizikai támadás az eszközök ellen.
- Megtévesztés: hamis személyazonosság használata, végpontok valós helyének meghamisítása,
- Rosszindulatú programok használata: vírusfertőzés, trójai programok, logikai bombák.
- Hitelesítés kijátszása: meglevő sérülékenységek kihasználása, jelszó feltörés.

- Aktív visszaélés: hamis adatok készítése, rendszerbe juttatása, meglévő adatok módosítása, működésképtelenné tétel.
- Passzív visszaélés: adatgyűjtés, adatbázisok megszerzése, forgalomanalízis, bizalmas kommunikáció lehallgatása.

Jayaram és Morse kifejezetten a számítógépes hálózatokra definiált kategóriákat:

- Fizikai: a rendszer elemeinek eltulajdonítása.
- Gyenge pontok: a rendszer gyenge pontjainak kihasználása engedély nélküli hozzáférés céljára.
- Rosszindulatú programok: speciális programkódok rendszerbe juttatása az ott tárolt adatok megsemmisítésének szándékával.
- Hozzáférési jogok: felhasználók hitelesítési adatainak megszerzése és így a rendszer erőforrásainak jogosulatlan felhasználása.
- Kommunikáció-alapú: a hálózati hozzáférésen keresztül végrehajtott támadások (hamisítás, lehallgatás).

A tapasztalatok azt mutatják, hogy az informatikai támadások egyre összetettebb módszereket használnak, így az említett osztályok közül több is alkalmas a befogadásukra. Az elkövetési módszerek mellett természetesen lehetséges egyéb szempontok szerint is kategorizálni az informatikai támadásokat. Egy – véleményem szerint egyszerű, és emellett mégis univerzális – taxonómia a támadás eredménye alapján osztályozza a fenyegetéseket. Frederick B. Cohen szerint mindössze három eredménye lehet egy sikeres informatikai támadásnak [29]:

- Sérülés (corruption), vagyis az informatikai rendszerben található adatokat a támadónak sikerül megváltoztatnia, vagy törölnie.
- Szivárgás (leakage), amikor a támadónak olyan adatokat sikerül megszereznie, amihez nem szabadna hozzáférnie.
- Megtagadás (denial), a megtámadott rendszer működése lehetetlenné válik.

A besorolás nem foglalkozik azzal, hogy a támadónak milyen módszerrel sikerült elérnie, csak a céllal magával.

Az ilyen, különböző alapelvekre épülő osztályozási módszereket párhuzamosan is lehet használni. A következőkben néhány, a közelmúltban történt incidenst mutatok be többféle osztályozási módszert felhasználva:

Sony Playstation Network

2011 áprilisában a Sony Playstation Network (PSN) esett adatlopás áldozatául. A támadók több millió felhasználó személyes adatait (hitelkártya szám, vásárlási előzmények, számlázási cím, biztonsági kérdés a jelszócseréhez) szerezték meg. [30] A betörést egy teljesen triviális SQL Injection[11] nevű eljárás használatával valósították meg. A PSN több hétig elérhetetlen volt az eset után, ennyi időbe telt, amíg a cég kijavította a biztonsági problémákat. Az esetet súlyosbította, hogy a Sony több weboldala is hasonló sérülékenységeket tartalmazott, ezért több kisebb oldalt is feltörtek a javítások megtörténte előtt.

Az incidens végkimenetele adatszivárgáshoz vezetett, és a hitelesítés kijátszásának módszerét használta, ugyanis egy meglévő sérülékenységet használt fel az adatbázishoz férés céljára.

RSA SecureID adatlopás

2011 márciusában az informatikai biztonság terén kiemelkedő hírnévvel rendelkező RSA nevű céget ért adatlopásra irányuló támadás. Az elkövetők a jól ismert phishing[12] eljárást alkalmazták a cég dolgozóival szemben: egy „2011 Recruitment Plan" tárgyú levélben küldtek nekik elektronikus levelet, amihez egy fertőzött Excel állományt csatoltak. Ebben az állományban egy addig ismeretlen (0 day exploit) Adobe Flash hibát kihasználó programkód volt megtalálható, ami a fertőzött fájl megnyitása után egy hátsó ajtót (backdoor) nyitott a támadók számára az alkalmazott gépén. Ezután a támadók felderítették az alkalmazott jogosultságait egyéb rendszereken, majd ezeket kihasználva fontos SecureID[13] kulcsokat szereztek meg, amit egy külső szerverre továbbítottak. [31] A megszerzett adatok azért voltak fontosak, mert segítségükkel más rendszerek is támadhatóvá váltak.

Az incidens több szempontból is figyelemre méltó: egyrészt az egyik leghíresebb információ biztonsággal foglalkozó céget ért sikeresen végrehajtott támadás, másrészt

[11] SQL Injection: a weboldalak a megjelenítendő információkat általában adatbázisban tárolják. Az adatbázisban tárolt adatok lekéréséhez az elterjedt SQL nyelvet használják. Beléptetéskor a felhasználótól kapott információkat (például felhasználói név és jelszó) beépítik egy ilyen lekérdezésbe, mielőtt elküldik az SQL szervernek. Ha nem megfelelően szűrik a felhasználótól megkapott adatokat, akkor a lekérdezés olyanná alakítható, ami meghamisítja az eredményeket, így kijátszva a beléptetési folyamatot.

[12] Phishing: adathalászat, az áldozatot egy megtévesztő üzenettel bírják rá arra, hogy a támadó számára kedvező tevékenységet hajtson végre (például egy hamisított oldalra irányítják, ahol megszerzik tőle a fontos információkat.

[13] A SecureID egy hardver eszköz, amivel az informatikai rendszerek felhasználóinak hitelesítése megbízhatóbbá tehető. Az eszköz egyedi hitelesítő adatot generál minden belépéshez, így az esetleg megszerzett adat később már nem használható fel.

az elkövetők több, egymásra épülő akciót hajtottak végre. A végső eredmény adatszivárgás lett, de ehhez szükség volt a célpont rendszerében sérülést is előidézni. A felhasznált módszerek pedig sok osztályba is besorolhatók: megtévesztés (phishing technika), rosszindulatú programok használata, hitelesítés kijátszása. Jayaram és Morse osztályozási rendszerében gyakorlatilag csak a fizikai módszer használata hiányzik.

Lockheed Martin adatlopás

2011 májusában az amerikai Lockheed Martin cég esett betörők áldozatául, az elérhető információk szerint az RSA betörés során megszerzett SecureID kulcsok miatt. A támadók a cég alkalmazottai által használt VPN[14] hozzáférésekkel jutottak be a belső hálózatba. A cég állítása szerint a vadászrepülőgépek terveihez és fontos kormányzati dokumentumokhoz nem fértek hozzá a betörők. [32]

Ebben az esetben a támadók egy korábbi esetben megszerzett adatokat használtak fel a kivitelezésre. Adatszivárgás történt, amihez hamis azonosságot és megtévesztést alkalmaztak.

Citibank ügyféladatok eltulajdonítása

2011. június elején az amerikai Citibank 200 000 ügyfelének bankszámlaszámát, nevét és email címét szerezték meg a támadók – a bank szerint igazán fontos adatok nem kerültek ki. [33] Az adatlopás egészen elképesztően primitív módszerrel történt, a weblapot azonosító URL[15] címben szerepelt az ügyfél azonosító kódja, amelynek megváltoztatásával probléma nélkül egy másik ügyfél adataihoz lehetett hozzáférni. A támadónak csak egy automata programra volt szüksége, ami véletlenszerűen generált azonosítókkal lekérte a szükséges adatokat.

Ismét adatszivárgásról van szó, amelyet a passzív visszaélés módszerével követtek el. A nem megfelelő biztonsági tervezés miatt lett sikeres a visszaélés.

Stuxnet

A számítógépes vírusok által okozott károk sokáig nem lépték túl a számítógép határait, így sokan csak múló kényelmetlenségnek tekintették az ilyen problémákat. A

[14] VPN: Virtual Private Network, virtuális magánhálózat.

[15] URL: Unified Resource Locator, a weben tárolt dokumentum elérését lehetővé tevő cím, amely globálisan egyedi.

számítógépes kártevő programokkal elkövetett szabotázsok és valószínűleg a kiberháború történelmében új korszak kezdődött, amikor 2010. június 16-án a fehérorosz VirusBlokAda nevű kis minszki számítógépes biztonsági cég egy elektronikus levelet kapott egy teheráni ügyfelétől. [34] Az ügyfél által felügyelt számítógépek egyfolytában újraindultak, ezért felmerült a vírusfertőzés lehetősége. A komolyabb vizsgálatok aztán kimutatták, hogy tényleg egy vírusról van szó, amely azonban kifejezetten bizonyos típusú ipari eszközök – urándúsító centrifugák – elleni szabotázsakcióra lett kifejlesztve. A Stuxnet sokféle összeesküvés elmélet elindítója lett, sokan az Egyesült Államok és Izrael érintettségét valószínűsítik.

Ez az incidens annyira összetett volt, hogy osztályba sorolása bonyolult, szinte mindegyik támadási kategóriát lefedi. Összefoglalva a vírus készítéséhez szükséges erőforrásokat:

- Szükséges volt 4 db Windows „0 day exploit” felderítése vagy megvásárlása;
- El kellett lopni két megbízható tanúsítványhoz tartozó titkos kulcsot;
- Magas szinten ismerni kellett a Siemens Step7 fejlesztőrendszerét, sérülékenységeket kellett találni benne;
- Ismerni kellett a PLC-k[16] programozását olyan szinten, hogy a szabotázst végző kód megfelelően működjön, illetve a működést el tudja rejteni az operátorok elől;
- Ismerni kellett a két érintett típusú motorvezérlő egység működését. Egyikük, a Fararo Paya iráni cég annyira titkosan működött, hogy sokáig az Atomenergia Hivatal sem tudott róla [35];
- Ismerni kellett az IR-1 urándúsító centrifuga mechanikai paramétereit, és működésének határait;
- Rendelkezni kellett megfelelő tesztkörnyezettel, illetve olyan centrifugákkal, amelyeken kikísérletezhető volt a szabotázs;
- Az első fertőzést okozó pendrive-ot oda kellett juttatni az iráni atomlétesítmény egyik számítógépére.

Látható, hogy ezek az erőforrások nem egyszerűen elérhetők, így valószínűsíthető az állami közreműködés. Izrael érintettségét bizonyíthatja az a videó, amelyen Gabi Ashkenazi altábornagy, az izraeli haderő leköszönő parancsnoka egyik sikereként említi

[16] PLC: Programmable Logic Controller, általában ipari környezetben használt programozható vezérlőegység.

a Stuxnetet. [36] A károkozó mechanizmus teszteléséhez szükséges centrifugák a líbiai atomprogram feladásakor az Egyesült Államokhoz került berendezések lehettek, de ez is csak feltételezés. Tény, hogy ezekkel az eszközökkel az Egyesült Államok nem tud, vagy inkább nem akar elszámolni. [37] A szabotázsakciót általában sikeresnek tartják, holott pontos eredményeket nem ismerünk.

1.4 Informatikai támadások által okozott károk

Egy informatikai támadás által okozott kár meghatározása nem egyszerű dolog, hiszen rengeteg tényezőből áll össze a teljes veszteség. Alapvetően egy ilyen támadás hatása ugyanolyan lehet, mint egy katasztrófa által okozott kár, így az üzletmenet folytonossági- és katasztrófa elhárítási tervek készítésekor alkalmazott módszerek elviekben használhatók. A károk négy nagy csoportra oszthatók: [38]

- bevétel kiesés;
- megnövekedett költségek;
- forgótőke problémák;
- hitelességi és tőkevonzó képességre gyakorolt hatás (anyagi vonzattal járó erkölcsi kár).

Bevétel kiesés

A legérzékenyebb és leginkább meghatározható veszteséget a bevétel lecsökkenése, vagy akár teljes kiesése okozza. Ez előállhat a megrendelések elapadása (a megrendelők nem képesek rendeléseiket eljuttatni), de akár a megrendelések teljesítésének ellehetetlenülése miatt is. Bevétel kiesést okozhat még ezen kívül az is, ha a támadást elszenvedő nem képes az általa lebonyolított üzleti tranzakciók pénzügyi mozgásait (számlázás, teljesülés vizsgálata) nyomon követni.

Megnövekedett költségek

Egy sikeres támadás előre csak nehezen kalkulálható idejű kiesést okoz, azonban az áldozat (sértett) elemi érdeke, hogy ezt az időt a lehető legrövidebbre csökkentse. Ehhez természetesen költségek társulnak, hiszen:

- az ügyfelekkel kötött szolgáltatásminőségi (SLA[17]) szerződések a kiesett időtartamra kártérítési kötelezettséget róhatnak a cégre;
- a támadás elhárításához szükséges lehet külső szakértők bevonása;

[17] SLA: Service Level Agreement.

- a védekezés koordinálásához külső és belső erőforrásokat kell felhasználni;
- szükséges lehet újabb eszközök vagy szolgáltatások (tartalék informatikai eszközök, magasabb számítógépes hálózati sávszélesség) biztosítása.

Forgótőke problémák

Az előző két kárcsoport egymást erősítő hatású, vagyis a megnövekedett költségekkel alacsonyabb bevétel áll szemben. Emiatt előfordulhat olyan eset, amikor az áldozat számára nem áll rendelkezésre kellő mennyiségű forgótőke, amiből fedezze a kiadásokat. Ekkor vagy külső finanszírozást kell bevonni (aminek járulékos költségei vannak), vagy pedig az egyéb célokra használható tőkéhez kell nyúlni – ami például az alapanyag beszerzést nehezíti meg.

Hitelességi és tőkevonzó képességre gyakorolt hatás

Véleményem szerint ez a terület a legnehezebben számszerűsíthető, nem közvetlen vagyoni jellegű veszteség. Egy nem megfelelően kezelt vagy kommunikált kiesés elbizonytalaníthatja a befektetőket, ami a cég tőzsdei árfolyamára gyakorolhat negatív hatást. Nem lebecsülendő hatások közé tartozik a cég dolgozói morálját ért csapás, a cég belső és külső megítélésének kedvezőtlen változása sem. Bár informatikai támadás miatt eddig még hitelt érdemlően bizonyított emberi veszteség nem volt, de a jövőben ezzel is számolni kell.[18]

A Ponemon Institute 2010-ben 45 cég bevonásával készített egy felmérést a kiberbűnözés által okozott károkról. A felmérés fő megállapításai a következők voltak:

- A kiberbűnözés komoly károkat okozott, a 45 cég átlagos elszenvedett vesztesége ilyen okokból 3,8 millió USA dollár volt, a legmagasabb veszteség pedig 52 millió!
- Az informatikai támadások gyakoriak, a felmérés ideje alatt a cégek átlagosan 50 támadást szenvedtek el, amelyből legalább egy sikeres is volt.
- A legnagyobb kárt az információlopás okozta (42%), a DDoS támadásokkal összefüggő események a teljes kár 22%-át képezték.
- Az áldozatok között minden ipari szegmens megtalálható.
- A felmérésben részt vevő cégek 29%-a szenvedett el botnetekkel (és így a DDoS támadásokkal) kapcsolatos támadásokat.

[18] A Stuxnet vírus által okozott károkhoz az iráni illetékesek szerint emberi veszteség is társult, azonban ezt fenntartásokkal kell kezelni.

- A botnetekkel kapcsolatos támadások egyenlő arányban érintették a kis-, közepes- és nagyvállalatokat. [39]

A fentiekből kitűnik, hogy bár a DDoS nem a leggyakoribb támadási forma, azonban az általuk okozott kár az összes kár több mint egyötödét képezi. Fontos megjegyezni, hogy a botnetekkel kapcsolatos problémák az összes eset 29%-át fedték le!
Magyarországi veszteségekről nincsenek nyilvánosan elérhető adatok, mivel a nyilvánosságra került DDoS támadások száma is elenyésző. Ez természetesen nem azt jelenti, hogy a hazai szervezetek nem szenvednek el ilyen akciókat, inkább a nyilvánosságra hozatallal bánnak óvatosan. Sok szervezetnek elemi érdeke a titkolózás, hiszen egy sikeres támadás beismerésével ügyfelei bizalmát veszíthetné el. Az Egyesült Államokban nyilvánosan hozzáférhető statisztikák vannak, például a Computer Security Institute 2008-as, vállalatvezetők megkérdezésére épülő felmérése szerint a botnetekkel kapcsolatos káresemény átlagos értéke közel 350000 USD volt. [40]

1.5 Kibertámadások kezelése

A társadalom informatikai függőségének növekedésével párhuzamosan a kockázatok is növekednek. Egy jól kivitelezett támadás a társadalom kritikus informatikai infrastruktúráinak időszakos leállását vagy meghibásodását is okozhatja, amivel az állampolgárok mindennapi életét nehezíthetik meg, alááshatják a pénzügyi, államigazgatási rendszerekbe vetett hitüket, vagy egyéb módon veszélyeztethetik őket. Az egyre újabb támadási módszerek megnyitották a szabotázsakciók elkövetésének lehetőségeit is, az ipari infrastruktúra is támadhatóvá vált, ami már emberi életeket is veszélyeztethet. Az államoknak kötelességük polgáraikat megvédeni, ami a virtuális térben kivitelezett támadások esetére is vonatkozik.
A legnagyobb problémát az idegen államokból érkezett támadásokra adott reakciók jelentik, ugyanis a diplomáciai és nemzetközi jogi szabályok akadályozhatják az alkalmazható módszereket. Már a tényleges támadó kilétének felderítése is komoly gondot okoz, de a támadás irányításáért felelős személyek lokalizálása még ennél is nehezebb. Ha mégis sikerülne egy informatikai támadás elkövetőjét és az irányító személy vagy személyek tartózkodási helyét azonosítani, akkor három különböző lehetőség jöhet szóba [41]:

- a kiinduló ország illetékeseivel fel kell venni a kapcsolatot, és közösen leállítani a támadást;

- a kiinduló ország illetékeseinek tudta nélkül fel kell deríteni a támadót és meg kell próbálni letiltani hozzáférését (a hozzáférést biztosító szolgáltató segítségével);
- a kiinduló ország illetékeseinek tudta nélkül semlegesíteni kell a támadót.

Természetesen a fenti három lehetőség egyike sem áll fenn, ha a támadás szervezését valóban egy idegen állam szervezi, ekkor nyílt konfliktusról van szó, ami eddig még példa nélküli. Az egyre inkább elszaporodó, informatikai biztonságot veszélyeztető konfliktusok hatására keményebb hangot ütnek meg a kormányzati illetékesek, elsősorban a leginkább célpontnak számító Egyesült Államokban. A Pentagon első hivatalos, a virtuális térre vonatkozó stratégiája 2011 júniusában készült el, ebben a kibertámadásokat háborús cselekménynek (act of war) nyilvánítják, és az ellencsapások közül nem zárják ki a hagyományos katonai eszközök használatát sem, emellett a virtuális teret a hadviselés ötödik tartományának nyilvánítják (a szárazföld, a tenger, a levegő és a világűr mellett). [42]

A leggyakoribb – nem állami szervezet által elkövetett – támadásokkal szembeni fellépés során a fő problémát az együttműködés hivatalos folyamatának hosszadalmas volta jelenti. Míg egy támadás elindításához néhány másodperc is elegendő, a hivatalos szervekkel történő kapcsolatfelvételhez ennél lényegesen több idő szükséges. Figyelembe véve a szervereken képződő naplók mennyiségét és a szükséges rendszernaplók számát (egy támadó általában több feltört rendszer közbeiktatásával csatlakozik a tényleges akciót végző végpontokhoz, így valós hálózati címének felderítéséhez több végpontot is meg kell vizsgálni), a hivatalos csatornák közbeiktatásával kevés esély mutatkozik a valódi elkövető azonosítására.

Ha egy támadót a kiinduló ország illetékeseinek tudta nélkül próbálnak azonosítani, akkor diplomáciai gondot okozhat az, hogy egy másik ország ügynöke által elkövetett adatszerzést a legtöbb ország jogrendszere szankcionálja. Hírszerzési munka nélkül viszont esélytelen lokalizálni a támadásért felelős személyt vagy szervezetet.

A kiinduló ország illetékeseinek tudta nélkül semlegesíteni a támadót – még ha csak virtuálisan, a használt eszközök leállításával is - a legveszélyesebb lehetőség a három, szóba jöhető megoldás közül. Egy idegen államban elkövetett, nem bejelentett akció akár háborús helyzethez is vezethet, amennyiben a kiinduló ország illetékesei ezt kibertámadásnak tekintik. Márpedig - a módszerét tekintve - egy ilyen kísérlet ténylegesen támadásnak számít, még ha a célja különbözik is. Mindhárom esetben még

kényesebbé válhat a helyzet, ha a támadás kiindulási pontjáról kiderül, hogy az ottani végpont csak egy korábban uralom alá vont (tehát szintén áldozat) végpont, amit az elkövető „ugródeszkaként” használt céljaihoz. Ha a tettes egy harmadik államból – vagy extrém esetben a célpont országból - kezdte akcióját, akkor az ellentevékenység komoly presztízsveszteséget okozhat mindegyik félnek.

Ha előfordulna olyan, alacsony valószínűségű eset, amikor a támadóról minden kétséget kizáróan bebizonyítható, hogy állami megbízásból tevékenykedett, akkor az incidens akár komolyabb következményekkel is járhat. Az eddig napvilágra került esetek egyikében sem sikerült minden kétséget kizáróan igazolni a közvetlen állami érintettséget, jóllehet sejtések mindig napvilágra kerülnek.

A sort 1999-ben, a Pentagon hálózata ellen elkövetett adatlopási akció nyitotta. Az események felderítésére indított "Moonlight Maze" kódnevű FBI akció felderítette, hogy a támadók sikeresen bejutottak a Pentagon routereibe - hálózati útválasztóiba - és az adatforgalmat nyolc másik olyan végponton vezették keresztül, amelyet könnyen lehallgathattak. A támadás szisztematikus volt, nem véletlenszerű adatokra vadásztak, a támadást elkövető végpontok közül pedig sikerült azonosítani egy Moszkvától 30 kilométerre található internetes szervert. Az orosz érintettséget a szakértők azzal is igyekeztek bizonyítani, hogy az akciók mindig moszkvai idő szerint 8:00 és 17:00 között, tehát munkaidőben történtek. Természetesen az orosz hatóságok tagadták érintettségüket az ügyben. [43]

A következő, nagy port kavaró esetet a nyomozók által Titan Rain névre keresztelt kínai hackercsoport követte el, több fontos amerikai katonai beszállító ellen. A nyomozás során kínai végpontokig sikerült a nyomokat visszakövetni, de természetesen a kínai szervek nem vállalták a felelősséget. A kínai kormányzatot is folyamatosan gyanúsítják különböző, az Egyesült Államokban működő cégek elleni akciókkal. A Google által nyújtott ingyenes email szolgáltatás (Gmail) kínai aktivisták által használt postafiókjai rendszeresen adathalászok áldozataivá válnak. [44] [45]

A legújabb, 2011-es Gmail ellenes támadások elkövetői a Google szerint Jinanból – Kína keleti, Shandong tartományának fővárosa – indították akcióikat, amelyben nem csak kínai aktivisták, de ázsiai (főként dél-koreai) hivatalnokok és az amerikai kormányzatban dolgozók jelszavainak megszerzése volt a cél. A Google állítását kínai állami illetékesek hevesen cáfolták, holott a cég nem vádolta meg a kínai kormányt az elkövetéssel. A dolog érdekessége az, hogy Jinanban található a Kínai Néphadsereg hat technikai megfigyelőközpontjának egyike. [46]

2011-ben hozta nyilvánosságra megfigyeléseit az amerikai McAfee információbiztonsági cég, amely egy állami támogatottságú, közel 5 éven át folyó adatgyűjtési akciót leplez le. Az Operation Shady RAT[19] névre keresztelt akcióban 71 szervezetet érintett adatlopás, nagy részük USA, de akadt köztük kanadai, európai és ázsiai illetőségű is. A McAfee szerint az állami érintettségre utal az, hogy a 2008-as olimpia után hosszú ideig gyűjtöttek adatot két ázsiai ország olimpiai bizottságától is. [47] Véleményem szerint a kínai érintettségre ebben az esetben utalhat az is, hogy az áldozatok között egyetlen kínai célpont sincs (egy Hong Kongban működő amerikai hírügynökséget leszámítva).

Érdemes megvizsgálni azt az esetet, mi történne akkor, ha egy állam bizonyítottan megtámadná egy másik állam kritikus infrastruktúráját. A megtámadott fél ellentevékenységéhez jelenleg nem állnak rendelkezésre kiforrott eljárások, ráadásul a nemzetközi jog sem foglalkozik külön ezekkel a kérdésekkel. A nem kibertámadások esetére az ENSZ alapokmányának [48] VII. fejezete ad útmutatást. A 41. cikkely rendelkezik a nem fegyveres erők felhasználásával foganatosítható rendszabályokról:

"A Biztonsági Tanács határozza meg, hogy milyen fegyveres erők felhasználásával nem járó rendszabályokat kíván foganatosítani abból a célból, hogy határozatainak érvényt szerezzen és felhívhatja az Egyesült Nemzetek tagjait arra, hogy ilyen rendszabályokat alkalmazzanak. Ilyeneknek tekintendők a gazdasági kapcsolatok, a vasúti, tengeri, légi, postai, távírói, rádió és egyéb forgalom teljes vagy részleges felfüggesztése, valamint a diplomáciai kapcsolatok megszakítása."

Az angol nyelvű változatban az "egyéb forgalom" eredetileg "other means of communication" kifejezésként szerepel, ami "a kommunikáció egyéb formája" értelmű. Vagyis, ha a Biztonsági Tanács a nem katonai jellegű beavatkozás mellett dönt, akkor a támadó fél valamennyi kommunikációs lehetőségét (beleértve az internethez hozzáférést is) korlátozhatják. Ez egy elképzelt konfliktus esetén nem feltétlenül hozna megoldást, ugyanis a támadásokhoz használt eszközök földrajzilag elszórtan helyezkednek el, és általában képesek autonóm, felügyelet nélküli üzemmódra is, így a megindított támadást folytatni tudnák az irányító kiesése esetén is. Ezért, ha a kommunikációs lehetőségek korlátozása nem hoz eredményt, akkor a 42. cikkely szerint:

[19] A RAT szó jelen esetben a Remote Access Tool rövidítése, ami a távoli hozzáférést biztosító eszközökre utal.

"Ha a Biztonsági Tanács úgy találja, hogy a 41. cikkben említett rendszabályok elégtelenek, vagy elégteleneknek bizonyulnak, úgy légi, tengeri és szárazföldi fegyveres erők felhasználásával olyan műveleteket foganatosíthat, amelyeket a nemzetközi béke és biztonság fenntartásához, vagy helyreállításához szükségesnek ítél. Ezek a műveletek az Egyesült Nemzetek tagjainak légi, tengeri és szárazföldi hadereje által foganatosított tüntető felvonulásból, zárlatból (blokád) vagy egyéb műveletekből is állhatnak."

Ennek értelmében az ENSZ felügyelete alatt akár fegyveres akcióvá is eszkalálódhat egy virtuális konfliktus, aminek – bár elméleti lehetőség van rá – valószínűsége napjainkban csekély. A Biztonsági Tanács tevékenységére eddigi fennállása során, még a komoly fegyveres konfliktusok esetén sem volt jellemző a gyorsaság és az egyetértés. Talán emiatt, de az 51. cikkely biztosítja az államok számára az önvédelem jogát:

"A jelen Alapokmány egyetlen rendelkezése sem érinti az Egyesült Nemzetek valamelyik tagja ellen irányuló fegyveres támadás esetében az egyéni vagy kollektív önvédelem természetes jogát mindaddig, amíg a Biztonsági Tanács a nemzetközi béke és a biztonság fenntartására szükséges rendszabályokat meg nem tette. A tagok az önvédelem e jogának gyakorlása során foganatosított rendszabályaikat azonnal a Biztonsági Tanács tudomására tartoznak hozni és ezek a rendszabályok semmiképpen sem érintik a Biztonsági Tanácsnak a jelen Alapokmány értelmében fennálló hatáskörét és kötelességét abban a tekintetben, hogy a nemzetközi béke és biztonság fenntartása vagy helyreállítása végett az általa szükségesnek tartott intézkedéseket bármikor megtegye."

A fegyveres támadás kifejezés kiterjesztése a kibertámadásokra egy újabb érdekes problémát vet fel: mi számít fegyvernek egy támadás során? Ha olyan eszközre gondolunk, amely segítségével képes a fegyver használója emberéletben kárt okozni, akkor érdemes elgondolkodni egy olyan számítógépes támadáson, amely segítségével egy atomerőmű vezérlését teszi tönkre a behatoló, ezzel az erőmű leállását vagy túlterhelését okozva. Az ilyen cselekmények immár nem a fantázia szülöttei, a Stuxnet vírus után teljesen másként kell gondolni a szabotázsakciók lehetőségére.

Kibertámadások kezelése a NATO-ban

Mivel hazánk a NATO tagja, ezért egy esetleges katonai támadás esetén a Washingtoni szerződés 5. cikkelye alkalmazandó, amely a szövetség tagjait közbelépésre kötelezi, ha

valamelyik tagállamot támadás érné. Ez a rendelkezés is az ENSZ Alapokmány 51. cikkelyére hivatkozik:

„5. cikk. A Felek megegyeznek abban, hogy egyikük vagy többjük ellen, Európában vagy Észak-Amerikában intézett fegyveres támadást valamennyiük ellen irányuló támadásnak tekintenek; és ennélfogva megegyeznek abban, hogy ha ilyen támadás bekövetkezik, mindegyikük az Egyesült Nemzetek Alapokmányának 51. cikke által elismert jogos egyéni vagy kollektív védelem jogát gyakorolva, támogatni fogja az ekként megtámadott Felet vagy Feleket azzal, hogy egyénileg és a többi Féllel egyetértésben, azonnal megteszi azokat az intézkedéseket - ideértve a fegyveres erő alkalmazását is , amelyeket a békének és biztonságnak az észak-atlanti térségben való helyreállítása és fenntartása érdekében szükségesnek tart. Minden ilyen fegyveres támadást és az ennek következtében foganatosított minden intézkedést azonnal a Biztonsági Tanács tudomására kell hozni. Ezek az intézkedések véget érnek, ha a Biztonsági Tanács meghozta a nemzetközi béke és biztonság helyreállítására és fenntartására szükséges rendszabályokat.” [49]

Az idézett cikkely kibertámadásokra vonatkoztatott első alkalmazásának lehetősége 2007-ben, az Észtország információs infrastruktúráját ért súlyos DDoS támadás idején vetődött fel. Jaak Aaviksoo, az észt védelmi miniszter szerint egy kibertámadás napjainkban ugyanolyan hatással bír, mint kétszáz évvel ezelőtt egy tengeri blokád: elvágja az országot a világ többi részétől. [50] A feltételezett támadó Oroszország volt, ezért az 5. cikkely alkalmazása előre nem látható bonyodalmakat okozott volna. Az eset rávilágított arra a tényre, hogy a kibertámadásokat egyre komolyabban kell venni. A 2010-es lisszaboni tanácskozás során meg is született a NATO egységes stratégiája, amelyben immár szerepelnek a virtuális teret érintő biztonsági problémák is:

„tovább fejlesztjük a képességet a kibertámadások megelőzése, felismerése, az ellenük való védelem és a helyreállítás terén, beleértve a NATO tervezési folyamatának használatát a nemzeti kibervédelmi képességek növelésében és koordinálásában. Centralizált kibervédelem alá vonunk minden NATO szervezetet, és e téren jobban összehangoljuk a NATO tájékoztatási, előrejelzési és válaszadási képességét a tagországokkal;” [51]

A stratégiára építve a szövetség 2011 júniusára kidolgozta a védelmi tevékenység szervezeti hátterét. Operatív szinten a NATO Cyber Defence Management Board (CDMB) feladata a NATO központja, a parancsnokságok és ügynökségek közti együttműködés koordinálása. Az operatív tevékenységek – incidensek kezelése, ezekkel kapcsolatos információk szolgáltatása a biztonsági felelősök és felhasználók fel - végrehajtása a NATO Computer Incident Response Capability (NCIRC) szervezet technikai központjainak a feladata. A szövetséges tagállamok számára is támogatást nyújtanak a nemzeti kommunikációs infrastruktúra biztonságosabbá tételéhez.

A kibertámadások kezelése Magyarországon

Egy támadás célpontja természetesen szeretné rendszerét működőképes, elérhető állapotban tudni, ehhez pedig igyekszik a megfelelő védelmi intézkedéseket megtenni. Ha ezek az incidens bekövetkeztét nem tudják megakadályozni, akkor a támadás mielőbbi leállítása szükséges, ami a támadó végpontok vagy pedig a rosszindulatú adatfolyam semlegesítésével lehetséges. Egy kibertámadásban részt vevő végpontok földrajzilag bárhol elhelyezkedhetnek, így a kikapcsolásukhoz harmadik fél – általában a hálózati hozzáférést nyújtó szolgáltató – felkérése szükséges, aki ráadásul nem is biztos, hogy ugyanabban az országban működik, mint az áldozat. Ez a művelet az átlagos cégek számára nehezen kivitelezhető, ezért a számítógépes incidensek kezelésére létrejött a CERT[20] nevű szervezet. Napjainkra már az egész világot behálózza, általában egyetemek, kutatóintézetek vagy nagyobb informatikai cégek működtetik. Magyarországon két CERT üzemel, az MTA SZTAKI által működtetett HUN-CERT illetve a 223/2009 (X. 14.)-es Kormányrendelet által Nemzeti Hálózatbiztonsági Központnak is kijelölt, a Puskás Tivadar Közalapítványon belül működő PTA CERT Hungary. A kormányrendelet 9. §-a részletezi a Központ szolgáltatásait. Ezek közül kiemelem a következő pontokat:

„9. § (1) A Központ szolgáltatásai:

a) A Központ a magyar és nemzetközi hálózatbiztonsági és kritikus információs infrastruktúra védelmi szervezetek felé magyar Nemzeti Kapcsolati Pontként (a továbbiakban: NKP), kormányzati számítástechnikai sürgősségi reagáló egységként (kormányzati CERT) működik, folyamatos rendelkezésre állással;

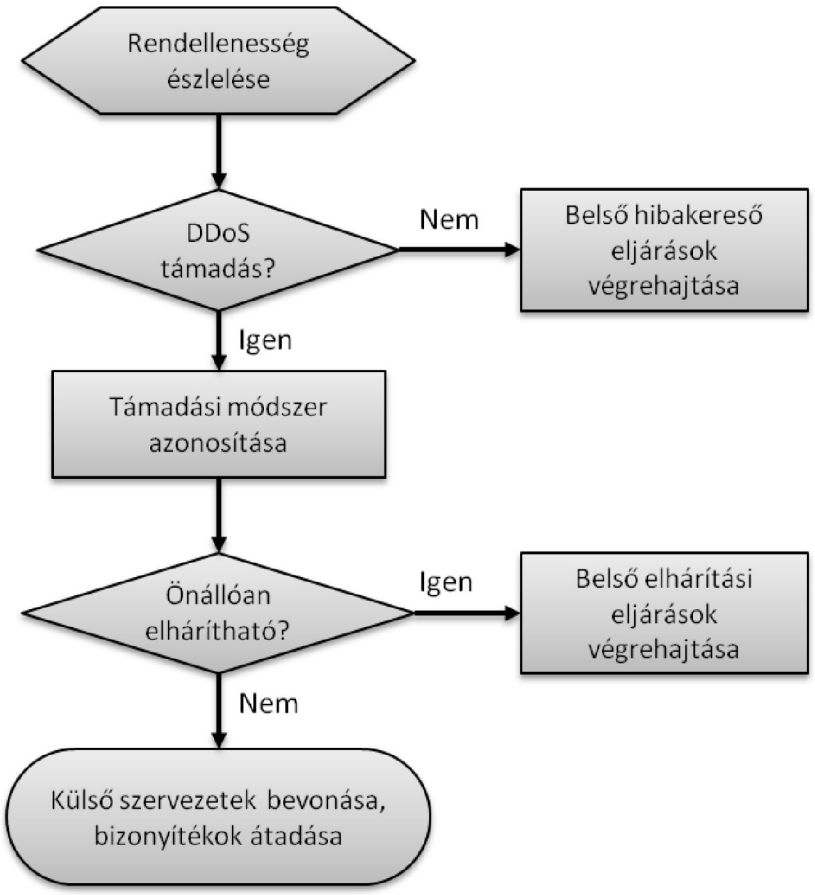
[20] CERT: Computer Emergency Response Team.

DOI azonosító: 10.17625/NKE.2012.008

b) A Központ, mint NKP ellátja a magyar és nemzetközi hálózatbiztonsági és kritikus információs infrastruktúra védelmi szervezetek felé az internetet támadási csatornaként felhasználó beavatkozások kezelését és elhárításának koordinálását;"

Az a) pont a Nemzeti Kapcsolati Pont üzemeltetésére, míg a b) pont az internetes támadások kezelésére és a védekezés koordinálására ad felhatalmazást. Ennek megfelelően a Központ alapszolgáltatásai[21] közé tartozik az incidenskezelés, amelyhez kapcsolódóan folyamatosan elérhető ügyelet működik. Az ügyeleten jelenthetők be az informatikai támadások, amelyek kezeléséhez, a védekezés koordinációjához, az érintett hazai és nemzetközi szervezetek együttműködéséhez nyújtanak segítséget. A külföldön található támadó végpontok semlegesítése az együttműködő külföldi CERT szervezeteken keresztül lehetséges.

Egy kibertámadás kezelésének jelenlegi folyamata a következő, saját kutatásaim eredményére és gyakorlati tapasztalataimra támaszkodva, általam készített ábrán látható:



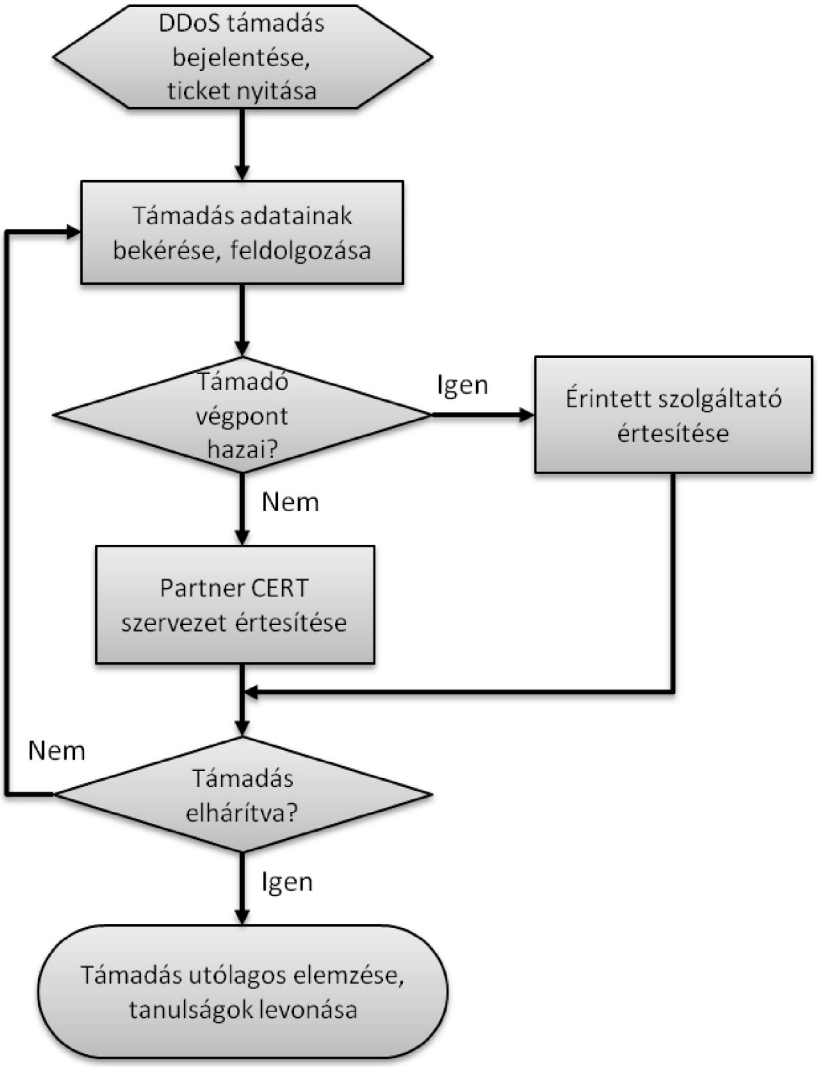
2. ábra DDoS támadás kezelésének folyamata (szerkesztette a szerző)

[21] http://www.cert-hungary.hu/node/13

DOI azonosító: 10.17625/NKE.2012.008

Ha a megtámadott bevonja a hazai CERT szervezetet, akkor a bejelentést a CERT ügyeletén tudja megtenni, ahol egy ticketing rendszerbe kerül az incidens. A bejelentéshez célszerű mellékelni a támadást igazoló adatokat is (általában naplóbejegyzések, amelyek tartalmazzák a támadó végpont címét, az észlelés idejét). Ezekből az adatokból később meghatározható a rosszindulatúan viselkedő végpontokat tartalmazó hálózat üzemeltetője, akinek segítségével ezek kikapcsolhatók. Egy ilyen akció természetesen iteratív jellegű, tehát a rendelkezésre álló összes adatot feldolgozva, majd a később beérkező adatokat újra feldolgozva lehet eredményt elérni.

A PTA CERT munkatársaival folytatott interjú alapján elkészítettem egy ilyen akció folyamatábráját:



3. ábra CERT incidenskezelés egyszerűsített folyamata (szerkesztette a szerző)

1.6 Egy elképzelt komplex támadás menete

Sokáig csak a regényírók fantáziájában létezett a valós életre is komoly kihatással bíró informatikai támadás forgatókönyve. Az informatikai függőség és a terrorizmus veszélyének növekedése azonban magával hozta az aggodalmakat is. A 2001-es USA terrortámadások aztán újra felvetették a kritikus infrastruktúrák informatikai veszélyeztetettségének kérdését. 2002 júliusában a Gartner és a U.S. Naval War College tartott egy három napos szemináriumjellegű rendezvényt, ahol a kritikus infrastruktúrák informatikai és üzleti vezetői segítségével próbálták egy összehangolt, az élet több területét érintő kibertámadás forgatókönyvét kidolgozni. A „Digital Pearl Harbor" nevű eseményt több kritika is érte amiatt, hogy egyrészt szükségtelenül hívják fel a figyelmet a témára (kinyitják Pandora szelencéjét), másrészt pedig semmi újat nem lehet megtudni a találgatások segítségével. [52]

Természetesen sok igazság van abban, hogy spekulációkkal nehéz bármit is bizonyítani, azonban úgy gondolom, szükség van az ismert, illetve bizonyos mértékig az elképzelt, addig ismeretlen veszélyforrások figyelembe vételével megpróbálni egy lehetséges folyamatot tervezni, mivel így a védekezés menete is kidolgozhatóvá válik. Az élet minden területét érintő, kizárólag informatikai eszközöket alkalmazó támadás nehezen megvalósítható, a terroristák vagy egy reguláris haderő által alkalmazható eszközök használata azonban már előre nem látható mértékű pusztítást okozhat. Készült már ilyen hibrid támadásra elképzelt magyar forgatókönyv is, stílszerűen „Digitális Mohács" címmel [53], én azonban az azóta bekövetkezett események – és itt elsősorban a SCADA[22] biztonságát érintő problémákra gondolok – fényében megpróbálom felvázolni egy fizikai pusztítás nélküli összehangolt támadás általam elképzelt menetét.

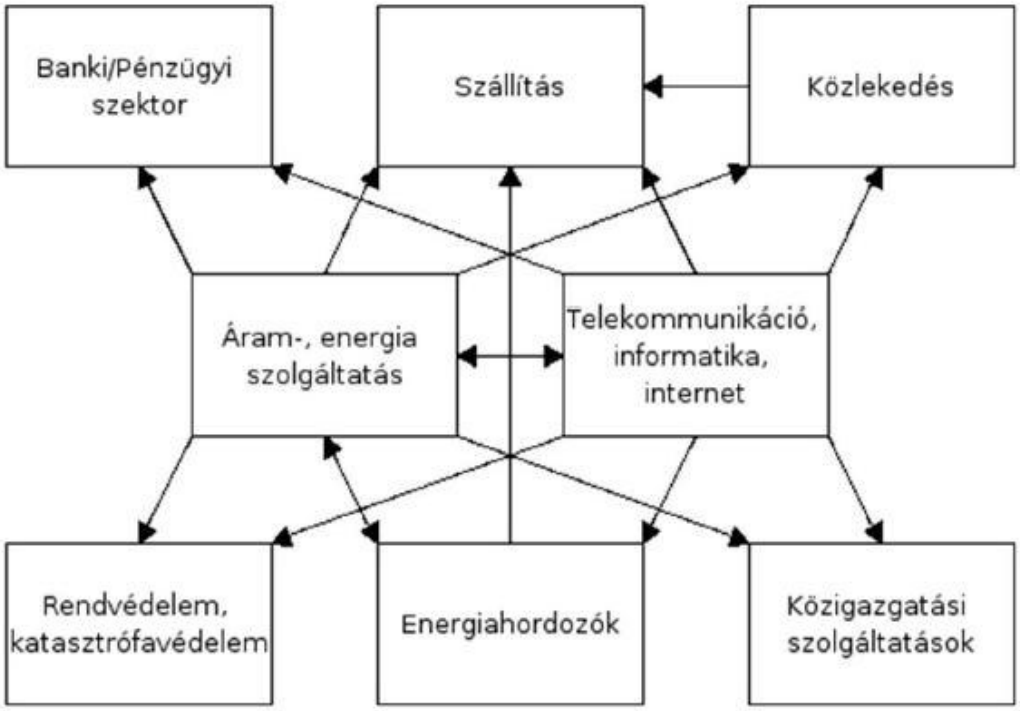
Az infrastruktúra célba vett területei:

- villamosenergia-szolgáltatás;
- telekommunikáció.

Ettől a két területtől függ az összes többi infrastruktúra, ezért ezeket kritikus infrastruktúráknak tekintjük. [54] Bár minden infrastruktúrának létezik működés szempontjából kritikus, támadható információs infrastruktúrája, de a nagyfokú függés miatt én ezt a két területet tekintem kiemelt célpontnak. Egy sikeres támadás ezen

[22] SCADA: Supervisory Control and Data Acquisition.

információs infrastruktúrák ellen az élet több területére is kihat, így kisebb energiával nagyobb pusztítás végezhető.



4. ábra Kritikus infrastruktúrák interdependenciája (forrás: Muha Lajos)

A támadás végrehajtása komoly erőforrások meglétét feltételezi a támadótól, fontos paramétere a támadásnak az összehangoltság és az egyes lépések megfelelő időzítése.

Első lépés: az előkészületek

Ebben a szakaszban kerül sor a támadáshoz szükséges eszközök beszerzésére, az új eszközök megtervezésére és kifejlesztésére. A célpontok kiválasztása és a támadó eszközök ezekhez való kialakítása hosszú folyamat, és komoly szakembergárdát – ilyen módon komoly anyagi áldozatot - igényel. Charlie Miller amerikai informatikai biztonsági szakértő a DefCon[23] 18 konferencián tartott előadása [55] tartalmaz egy érdekes kalkulációt arról, hogy milyen szakemberekkel és mennyibe kerülne egy ütőképes kiberháborús egység létrehozása és fenntartása. Miller szerint a szükséges pozíciók, és a feladatkörök:

- Sérülékenységi elemzők: a célpont által használt informatikai rendszerek vizsgálata, kihasználható programhibák, sérülékenységek keresése.

[23] A DefCon az egyik legnagyobb hacker konferencia, amelyet 1993 óta rendszeresen megtartanak az Egyesült Államokban. Nevét egyrészről a telefon középső sorának billentyűiről, másrészt a katonai szlengben használt „Defence Condition” rövidítéséből kapta.

- Exploit fejlesztők: a felderített programhibákra épülő támadó kódok készítése, 0-day exploitok előállítása.
- Botnet építők: új, támadásra alkalmazható botnetek telepítése, vagy mások irányítása alatt álló botnetek eltérítése.
- Botnet karbantartók: a meglevő botnetek felügyelete, frissítések elvégzése, a botnet kliensek földrajzi elhelyezkedésének nyilvántartása.
- Operátorok: a tényleges támadások végrehajtása, a „kemény célpontok", vagyis a jól védett, komoly hálózatok felderítése, behatolás megkísérlése.
- Kihelyezett személyek: a célpontokhoz telepített ügynökök, akik igyekeznek beépülni és a nyilvános hálózatoktól elzárt belső hálózatokhoz hozzáférést biztosítani.
- Fejlesztők: a támadásokhoz szükséges eszközök (botnet kliensprogramok, víruskódok) kifejlesztése.
- Tesztelők: a támadó eszközök kipróbálása különböző hálózati környezetekben, biztonsági programok használata mellett.
- Technikai konzultánsok: olyan, speciális szaktudással rendelkező szakemberek, akik egy adott részterületen - nagyrészt a célpont által használt környezettől függően - tudnak információkat szolgáltatni (mint például a SCADA, esetleg közlekedési irányító rendszerek).
- Rendszeradminisztrátorok: az egység infrastruktúráját működtetik.

A szerző számításai szerint egy ilyen egység kevesebb, mint 600 emberrel működőképes, és évi 50 millió USD költségvetéssel üzemelhet. Látható, hogy ez nem kevés, de egy terrorszervezet vagy egy kisebb állam számára azért elérhető összeg.

A hazánk energetikai szektora elleni támadás előkészülete tartalmazná az alkalmazott SCADA rendszerek vizsgálatát, a működésüket megbénítani tudó rosszindulatú kód kifejlesztését és telepítését néhány kulcsfontosságú helyen. A hazai energiaellátás jelentős részét a Paksi Atomerőmű[24] adja, így ennek megtámadása tűnik a „legkifizetődőbbnek". Mivel ez egy logikus célpont a támadók számára, ezért a védelme is a legerősebb, így sokkal célravezetőbbnek tűnik olyan kisebb erőművek megtámadása, amelyek azonos SCADA felügyeleti rendszereket használnak. Az erőművek kiválasztását meg kell előznie egy sérülékenységi felmérésnek, amely

[24] Magyarországon jelenleg 19 nagy- és 270 kiserőmű működik, a paksi atomerőmű 2000MW teljesítményével a hazai megtermelt energia mintegy 40%-át biztosítja. Forrás: http://www.atomeromu.hu/download/5526/Gyakran%20ismételt%20kérdések.pdf

segítségével a teljes villamos hálózatra gyakorolt hatás maximalizálható. Célszerű a hálózatok túlterhelését előidézni, ezért a villamos energia elosztó rendszereinek vizsgálatával ki kell választani azokat a nagyfogyasztókat, akiknek fogyasztása egyéb módszerekkel az erőmű leállásokkal egy időben megnövelhető, így a védőmechanizmusok kikapcsolására lehet törekedni.

Fontos a kellő kapacitású DDoS támadásokat biztosító botnetek létrehozása, a botnet kliensek földrajzi elhelyezkedésének meghatározása. Jelentős számú magyarországi kliensre van szükség, hogy a nemzetközi számítógépes hálózati kapcsolatok lekapcsolásával ne lehessen a támadásokat megszüntetni. Minden olyan országban is kell üzemeltetni támadó kapacitást, ahova a magyarországi szolgáltatóknak jelentős kapacitású kommunikációs vonala csatlakozik. Ezekhez a feladatokhoz fontos felderíteni a magyar internetes hálózat topológiáját és kapacitását. Szintén fontos a támadást erősíteni tudó eszközök (DNS[25] szerverek, nagykapacitású védtelen hálózatok) felderítése, és azok támadásba integrálása. Adatlopási és csalási (phishing) módszerekkel minél több állampolgár adatait meg kell szerezni, aminek segítségével dezinformációs kampány végezhető.

Az előkészületek akkor érnek véget, amikor sikerül az energiaszektorban a szükséges számú erőmű és vezérlőközpont működésképtelenné tételéhez elegendő fertőzést előidézni, illetve a túlterheléses informatikai támadásokhoz megfelelő kapacitást létrehozni, ami több hónap, de akár több év is lehet. A villamos energia előállítás és továbbítás rendszere nem várt sérülékenységet is tartalmazhat, amit már több példa is igazolt. 2003-ban az USA északkeleti államaiban 50 millió ember maradt áram nélkül, amikor túlnőtt fák zárlatot okoztak egy nagyfeszültségű távvezetékben, és egy programhiba miatt az operátorok nem tudtak időben reagálni a hibára. A zárlat miatt a többi vezeték terhelése megnőtt, így további három vezeték is működésképtelenné vált, a rendszerben működő erőművek pedig leálltak. A kiesés 11 emberéletet követelt, és 6 milliárd USD kárt okozott. [56] Hasonló eset hazánkban szerencsére nem következett be, azonban volt már példa arra, hogy hirtelen kiesett termelőkapacitások és az irányítás problémái miatt szolgáltatáskorlátozással kellett megvédeni a hálózatot. 2007 május 19-én az oroszlányi, május 20-án a Mátrai erőműben történt meghibásodás, ami a rendelkezésre álló kapacitást mintegy 150MW-al csökkentette. Ez még nem okozott problémát, azonban a következő nap a mátrai erőműben meghibásodás miatt leállt az V-

[25] DNS: Domain Name System. A tartománynevek IP címre fordítását végző szolgáltatás.

ös blokk, majd két megszakító miatt kiesett a Tiszai erőmű két blokkja is. A kiesett kapacitást a tartalékok indítása nem tudta fedezni, ráadásul importkapacitás sem állt rendelkezésre. Az üzemzavar elhárításához szükséges időt végül fogyasztói korlátozással sikerült áthidalni. [57]

Második lépés: támadás megindítása

A támadást több területen, megfelelő időzítéssel kell elindítani. Az első lépés a telekommunikáció megzavarása. Ehhez a megfelelő számú botnet szükséges, amelyek első feladata a nagyobb olvasószámmal rendelkező hírszolgáltatók működésképtelenné tétele DDoS támadások segítségével. A botnetek támadási metódusa összetett kell, hogy legyen, többféle támadási módszer alkalmazását kombinálva és váltogatva. Célravezető a korábban feltérképezett hálózati elemeket támadni, lehetőleg reflektív módszerekkel, ezáltal a botnet kliensek felderítése nehezíthető, a támadás ideje pedig elnyújtható. A botnetek működése a támadás megindításától kezdve autonóm lesz, vagyis a C2 csatornából semmilyen információ nem halad a kliensek felé. Az előre berögzített támadási menetrend alapján a botnetek különböző időpontokban kezdik meg a működést, ezzel nehezítve a felderítést és a semlegesítést. Ilyen módon gátolhatók a hagyományos, DDoS ellenes akciók, és a támadás hosszú időre is fenntartható.

A mértékadó internetes hírforrások elnémítása mellett a hagyományos hírforrások kommunikációját is nehezíteni kell, a szerkesztőségek internetes kommunikációjának zavarásával. Értekezésem írásának idejében az állami tulajdonú média – és a versenytársak kiszorulása miatt a magántulajdonú média egy részének is – híreit központosított módon, az MTI[26] szolgáltatja, így ez a csatorna is hatásosan támadható, megtévesztéssel megfelelő hírek, közlemények juttathatók célba. Röviddel ezután az előkészületi fázisban adatlopással megszerzett személyiségek nevében a lakosság megzavarására alkalmas, dezinformáló üzeneteket kell elhelyezni a támadásból szándékosan kihagyott internetes fórumokon, illetve főként a közösségi oldalakon. Célszerűen ebben az infrastruktúrák elleni hisztériakeltésre alkalmas szövegeket kell alkalmazni, mint például:

- Bankok csődbejutásával kapcsolatos információk, amivel a lakossági betétek kivételére lehet kényszeríteni az állampolgárokat;

[26] Magyar Távirati Iroda.

- Várható katasztrófahelyzettel kapcsolatos üzenetek, amivel a közösségi közlekedés bénítható meg;
- Vízhiányra figyelmeztető üzenetek, amivel a lakossági tartalékolás miatt a vízellátás akadozni kezd, így a jóslat önbeteljesítővé válik;
- Áramkimaradásra figyelmeztető üzenetek, a sikeres támadás miatt később ez is igazolódhat, tovább növelve a pánikot, illetve a későbbi – hisztériakeltésre alkalmas – üzenetek hitelességét.

Az üzenetküldésben komoly szerepe lehet a napjainkban egyre népszerűbb okostelefonoknak, az ezeken futó operációs rendszerek ugyanis engedélyezik a rajtuk futó alkalmazásoknak, hogy hozzáférjenek akár a telefon, akár a szöveges üzenetküldő funkciókhoz. Ennek köszönhetően lehetséges olyan kártevőt készíteni, amely a tulajdonos ismerőseinek SMS[27] üzenetben továbbítja a fenti szövegeket. A DDoS támadások kiterjednek ezekre az eszközökre is, így mind az adatkapcsolati (internetes), mind a szöveges üzenetek csatornáit is túlterhelhetik, de akár hanghívásokat is kezdeményezhetnek előre meghatározott célpontok felé. Kiemelt célpontok lehetnek például a segélyhívó számokat kezelő diszpécserközpontok (112, 104, 106, 107), amelyek elérését a mobiltelefon szolgáltatóknak kiemelt prioritással kell kezelniük. A mobilhálózatok túlterhelésekor kiemelt szerepe van az emberi tényezőnek, hiszen megfelelően célzott pánikkeltő üzenetekre adott reagálásukkal az előfizetők maguk lesznek azok, akik használhatatlanná teszik a hálózatot a forgalmi torlódás miatt.

A botnetek alkalmazhatók elektronikus levelek küldésére is, így minden internetes és mobilkommunikációs csatornában lehetséges az akció végrehajtása. A dezinformációs kampánynak alkalmaznia kell a pszichológiai hadviselés eszközeit, célja a lakosság körében a minél nagyobb bizonytalanság előidézése. Fontos megemlíteni a közösségi média szerepét, a Facebook és az iWiW nevű közösségi oldalak a magyar lakosság millióihoz jutnak el, a webnaplókon (blogokon) keresztül pedig véleményvezérek nevében lehet hamis információt eljuttatni a tömegekhez. Ebben a szakaszban indíthatók azok a DDoS támadások is, amelyek feladata az ország külföldi kommunikációs csatornáinak elzárása, amivel a külföldi tulajdonú szervezeteket lehet elszigetelni a tulajdonosaiktól, tovább fokozva a pánikhangulatot. Fontos célpontok lehetnek a bankok internetes szolgáltatásai is, ugyanis ezeket megbénítva sokan éreznék veszélyben megtakarításukat, és így a bankfiókokban vagy a bankjegykiadó

[27] Short Message Service.

automatáknál próbálnának meg készpénzhez jutni. Ez természetesen tumultuózus jeleneteket eredményezne, ami csak tovább erősítené a bizonytalanságot.

A megtévesztéses támadás után indítható a villamosenergia-ellátás elleni akció, amivel szabotálni lehet a hagyományos médiát is, elvágva a lakosságot a hiteles információktól. A cél az, hogy csak szóbeszéd, vagyis gondosan megválogatott és meghamisított adatok alapján jusson csak hozzá információhoz. A korábban fertőzött SCADA rendszerek segítségével előidézhetők katasztrofális események: például erőműleállások vagy a vezérlő rendszerek hibás működése miatti üzemszünet. A 90-es évek óta működik az RKV[28] rendszer, amely különböző energetikai berendezések távvezérlését teszi lehetővé a hosszúhullámú frekvencián. 2004 óta a Budapest melletti lakihegyi adó segítségével a rendszer lefedi egész Közép-Európát, mintegy 800 000 készüléket vezérelve. [58] Jelenleg ugyan nincs ismert informatikai biztonsági problémája, azonban elméleti síkon elképzelhető az, hogy nagyteljesítményű rádió adóberendezés segítségével megzavarják a rendszer működését. A nagyfogyasztókat és a közvilágítást megfelelő ütemben fel- és lekapcsolva előidézhetők olyan terhelési viszonyok, amelyek tovább növelhetik a rendszer működési zavarait, vagy akár időszakosan le is béníthatják azt.

Az áramellátásban előidézett nehézségek bizonyítékot szolgáltatnak a lakossági pánikhoz, ami a későbbiekben tovább kumulálódhat, akár az alkotmányos rendet is veszélyeztetve.

Harmadik lépés: az előidézett állapot fenntartása

Ha a második lépés sikeres, akkor a támadó érdeke a bizonytalan állapot fenntartása minél hosszabb időre. Ehhez alkalmas technika lehet az „alvó sejtek” használata, vagyis olyan eszközök megléte, amelyek az első két lépésben nem vesznek részt, aktivizálásuk az első két fázistól független csatornákon keresztül történik. Célszerűen ezek olyan elemek, amelyek önállóan, valamely környezeti paraméter megváltozása után lépnek akcióba (például hosszabb idejű üzemszünet után vagy a kezdeti támadás után egy előre meghatározott idő elteltével).

[28] Rádiófrekvenciás Központi Vezérlés.

1.7 Következtetések

A jelenleg is zajló folyamatok azt mutatják, hogy – elsősorban költségtakarékossági okokból – katonai használatra a polgári életben széleskörűen használt informatikai technológiákat igyekeznek rendszeresíteni, természetesen a különleges követelmények figyelembe vételével. Bár a megfelelőnek tűnő titkosítás és a harctéri körülményeket is elviselő berendezések alkalmazása megfelel a katonai elvárásoknak, azonban ezek a rendszerelemek széles körben használt technológiákat tartalmaznak, amiket jól ismernek a polgári élet szakemberei is. Emiatt a potenciális támadók („harcosok") köre is jelentősen kibővült.

Valószínűleg a jövőbeni katonai konfliktusok nem kizárólag informatikai hálózatokban, azaz virtuális térben fognak zajlani, azonban az ebben a fejezetben ismertetett esetek elemzése alapján bátran kijelenthető, hogy az ilyen fajta katonai tevékenységek növekvő szerepével és volumenével a jövőben komolyan kell számolni.

A terroristák és a katonai szervezetek internetes tevékenységének fent ismertetett eseteinek leírásával és azok elemzésével alátámasztottam, hogy a virtuális térben már jelenleg is zajlanak komoly károkat és zavarokat okozó katonai és terrorista műveletek.

A Stuxnet elnevezésű komplex vírus-féreg által okozott károk egyértelműen bizonyítják, hogy a jövőben egyre nagyobb károkat lehet okozni az ilyen eszközök kritikus infrastruktúrák elleni bevetésével. Az ENSZ Alapokmányának vonatkozó szakaszait, illetve a Pentagon legfrissebb katonai doktrínáját elemezve arra a következtetésre jutottam, hogy egy számítógépes hálózati eszközökkel vívott konfliktus valódi, fegyveres konfliktussá erősödése elképzelhető, valós veszélyforrás.

Informatikai támadások elemzésével megállapítottam, hogy a DDoS támadások előfordulási valószínűsége és az általuk okozott kár nagysága jelentős, így kiemelt figyelmet igényelnek.

Megállapítottam, hogy a kibertámadások kezelésére jól működő nemzetközi együttműködés létezik, ez azonban mindig reaktív jellegű, vagyis a bekövetkezett támadás esetére nyújt megoldást. Ismert támadási módszereket és az szakirodalomban elérhető hasonló elemzéseket alapul véve elkészítettem egy hazánk elleni komplex információs támadás forgatókönyvét. Ezen keresztül bemutattam, hogy a jelenleg is rendelkezésre álló módszerek alkalmazásával összeállítható olyan komplex eljárás, amely képes a valós terrortámadások által okozott tömegpánik és gazdasági károk nagyságát megközelíteni. A felkészülés során alapvető fontosságúnak tartom, hogy a

leírtakhoz hasonló forgatókönyvek készítésével megvalósuljon a fenyegetések felmérése, majd az infrastruktúrák egyéni védelmi terveinek összehangolása, esetleg tesztelése. Mivel az infrastruktúrák információs rendszerei közti függőség egyre nagyobb, ezért egy összehangolt, a függőségeket ismerő és ezekre optimalizált támadás hatása túlmutatna az egyes rendszerek leállásából származó problémákon. Jóllehet emberi életet közvetlenül nem, azonban indirekt módon, másodlagos hatásokkal fenyegetne egy ilyen akció.

2. FEJEZET
TÚLTERHELÉSES INFORMATIKAI TÁMADÁSOK

Az informatikai támadások által okozható károk felmérése alapján arra a következtetésre jutottam, hogy a DoS támadások napjaink információs infrastruktúrájára komoly veszélyt jelentenek, ezért kutatásaimat erre a támadástípusra szűkítettem.

Egy informatikai rendszer feletti uralom megszerzése nem mindig lehetséges, vagy ha mégis, akkor nem éri meg a belefektetett munkát. Időnként az is elegendő, hogy ha a célpont rendszere hosszabb-rövidebb ideig működésképtelenné válik. Az informatikai rendszerek véges erőforrásokkal rendelkeznek, a szükséges kapacitás méretezése során a várható terhelést és a kiszolgálásukhoz szükséges eszközök költségeit egyaránt figyelembe kell venni. Az eszközparkot úgy alakítják ki, hogy képes legyen a csúcsterhelést kiszolgálni, esetleg még tartalékkapacitással is rendelkezzen. Ha a rendszert ennél a tervezett maximális forgalomnál nagyobb terhelés éri, akkor a rendszer lelassul, szélsőséges esetben pedig akár működésképtelenné is válik. A teljes működésképtelenség nem is minden esetben szükséges, legtöbbször elegendő az is, ha annyira lelassul a működés, hogy a felhasználók tűréshatárát meghaladja a válaszidő. Jakob Nielsen „Usability Engineering” [59] című könyvében (R. B. Miller 1968-as kutatásaira támaszkodva) megvizsgálta az elfogadható válaszidőket számítógépes alkalmazások esetén. Eszerint:

- 0,1s vagy rövidebb válaszidő esetén a felhasználó a választ azonnalinak érzékeli, így a rendszernek az eredmény megjelenítésén kívül semmilyen egyéb visszajelzést nem kell produkálnia.
- 1s alatti válaszidők esetén a felhasználó még nem érzi úgy, hogy a munkáját indokolatlanul megzavarnák, de már érzékeli a rendszer lassulását. A rendszernek még nem szükséges a lassulásról visszajelzést adnia.
- 10s az a határ, amit meghaladva a felhasználó már elkezd egyéb feladatokkal is foglalkozni, vagyis elveszti érdeklődését a rendszerrel szemben. 1-10s közötti válaszidőnél már fontos kijelezni a válasz várható időpontját, és így fenntartani az érdeklődést.

A fenti adatokból látható, hogy ha egy megtámadott rendszer esetében sikerül elérni azt, hogy a válaszidő mindenféle figyelmeztetés megjelenítése nélkül meghaladja a 10

másodpercet, akkor a felhasználók nem fogják megvárni a késve érkező választ. Ekkor előáll az a helyzet, hogy bár a rendszer működik – csak lassan – de a használói számára funkcionálisan működésképtelenné válik, nem képes szolgáltatást nyújtani.

A DoS (Denial of Service) támadások - melyeket szokás "szolgáltatás megtagadásos" támadásoknak is nevezni – éppen erre a hatásra építenek. Noha a szolgáltatás nyújtását számos egyéb módszerrel is el lehet érni (fizikai megsemmisítéstől kezdve a tápáramellátás megszüntetéséig), azonban a szakirodalom DoS támadásnak kifejezetten azokat a módozatokat nevezi, amelyek a célpont túlterhelésével érik el a működésképtelenséget. Ezért véleményem szerint az eljárás lényegét jobban fedi a "túlterheléses támadás" kifejezés.
A DoS támadások sikeres kivitelezéséhez a támadónak:

- a célpontnál nagyobb erőforrásokkal kell rendelkeznie, vagy
- a célpont valamely hibáját kell kihasználnia.

A támadás irányulhat a célpont hálózati forgalmának, vagy pedig a célpont rendszerében működő valamely – szolgáltatást nyújtó – alkalmazásának túlterhelésére. A hagyományos DoS támadások során az elkövetők a célpontot egyetlen pontból támadják, általában egy „feltört”, megfelelő adottságokkal rendelkező hálózati végpontot (hálózatra kötött számítógépet) használva fegyverül. A „klasszikus” DoS helyett napjainkban sokkal elterjedtebb az egy időben, nagyszámú végpontból kiinduló támadási módszer, amelyet a „Distributed” (elosztott) szóval kiegészítve DDoS-nek nevezünk. Ekkor a túlterhelésre irányuló próbálkozást feltört számítógépekből álló hálózat, úgynevezett botnet segítségével végzik.
A fejezetben bemutatom a túlterheléses támadások történetét, valamint a védekezés lehetséges módszereit. A létező rendszertechnikai besorolások mellett felvázolok egy lehetséges osztályozási módszert, amellyel a túlterheléses támadások azonosíthatók.

2.1 Túlterheléses támadások története

Az első, jól dokumentált túlterheléses támadás 1999 augusztusában történt, amikor a Trinoo nevű program segítségével legalább 227 számítógép árasztott el rosszindulatú adatfolyammal egy University of Minnesota számítógépet. Az első, nagy nyilvánosságot szerző akció 2000. február 7-én következett be, amikor a Yahoo!, majd a következő napon az Amazon, a Buy.com, a CNN és az eBay esett áldozatul. A Yahoo!

500 000, az Amazon 600 000 dollár kárról számolt be. A támadások nem álltak le, február 9-én a ZDNet és az E*Trade is elérhetetlenné vált. [60]

A következő években folyamatosan történtek kisebb-nagyobb támadások, majd 2007-ben következett egy olyan esemény, amelyet sokan a kiberháború főpróbájának, vagy első csatájának tartanak. 2007. április 27-én a helyi orosz kisebbség tiltakozása ellenére az észt főváros, Tallin második világháborús szovjet emlékművét lebontották és áthelyezték. Hamarosan utcai zavargások törtek ki, és Oroszország is tiltakozott az eset miatt. Hamarosan az észt állami internetes infrastruktúra ellen túlterheléses támadások indultak. [61]

Az akciók közel két hétig folytatódtak kisebb-nagyobb intenzitással, a támadások közt voltak rövidebbek (kevesebb, mint 1 percig tartó), de nagyon hosszú idejűek is. A 128 elkülöníthető támadásból 7 olyan volt, ami 10 óránál is hosszabb ideig tartott! [62] Az akcióért az észt szakemberek Oroszországot tették felelőssé, ezt azonban a Kreml folyamatosan tagadta. Számos orosz fórumon jelentek meg a támadás kivitelezéséhez szükséges útmutatók. A támadások egy része automatizált DDoS volt, másik részük azonban az aktivisták által, kézi úton végrehajtott sorozatos weboldalletöltések. Közel két év múlva ismerte el a „Nasi" nevű orosz ifjúsági szervezet vezetője, hogy ők indították a támadást. Konsztantyin Gloszkokov szerint az akció inkább védekezés volt, ráadásul semmi törvénytelent nem csináltak, csak észt szerverekről töltöttek le adatokat, amit azok nem bírtak kiszolgálni. [63]

A DDoS támadások vizsgálata során kitűnik, hogy egy-egy új technológiára épülő támadási módszer mindig alapot szolgáltat a következők kivitelezésére, ennek megfelelően az egymást követő újabb és újabb támadások az előzőek hatásait legalábbis megismétlik, de inkább felülmúlják. Ennek megfelelően – és természetesen a technológia fejlődésével párhuzamosan – a friss DDoS támadások egyre nagyobb sávszélességgel, egyre nagyobb károkat okoznak.

Az alábbi táblázatban összefoglaltam az általam fontosnak tartott – általában valamilyen új mechanizmust vagy speciális célpontot tartalmazó – DDoS támadásokat a 2000-es évek elejétől. Ehhez a [64] [65] forrásokat használtam fel:

1. táblázat Emlékezetes DDoS támadások (szerkesztette a szerző)

Dátum	Célpont	Leírás
2000. február	Yahoo!, Amazon, Buy.com, eBay, CNN, ZDNet, E*Trade	Az első, kereskedelmi cégek ellen végrehajtott akció, amely tetemes károkat okozott.
2002. október	ROOT DNS szerverek	Az internet alapszolgáltatásának számító ROOT DNS szerverek kiesése esetén gyakorlatilag a teljes internet működése megbénulna.
2003	Online fogadóirodák szerverei	Egy orosz csoport online fogadóirodákat támadott, pénzt követelve. Aki nem fizetett, annak szervereit DDoS támadással működésképtelenné tették. Az első pénzszerzési célú támadás.
2007. február	ROOT DNS szerverek	A második nagy támadási hullám, amely a 13 ROOT szerverből kettőt működésképtelenné is tett.
2007. április	Észt kormányzati szerverek	Az első, államok közti konfliktus.
2008. július	Grúz kormányzati szerverek	A dél-oszét fegyveres konfliktushoz kapcsolódó kibertámadás.
2010. december	Paypal, Mastercard, Visa	Az Anonymous nevű szervezet „Operation Payback” akciója keretében a WikiLeaks számláinak befagyasztása miatt indított DDoS akciók nagy nyilvánosságot kaptak, de kevés kárt okoztak. A hacktivism előretörése.

2.2 Túlterheléses támadások besorolása

A gyakorlatban nagyon szerteágazó a túlterheléses támadások során alkalmazott eljárások köre, ezért célszerű az informatikai támadásokhoz hasonlóan ezeket is rendszerezni. Stephen M. Specht és Ruby B. Lee [66] az adatátviteli hálózatokat célzó támadásokra koncentrált, és két fő támadási osztályt definiált:

- Sávszélesség túlterhelés;
- Erőforrás túlterhelés.

A sávszélesség túlterhelés az elárasztásos illetve az erősítéses technikákat tartalmazza, míg az erőforrás túlterhelésbe főként a szándékosan a protokollok gyengeségére építő eljárások kerültek. Ez a besorolási metódus véleményem szerint túlságosan leegyszerűsíti a támadási módszerek kategóriáit, így a két osztályba túl sok elem kerül, ami megnehezíti a tájékozódást.

Jelena Mirkovic és Peter Reiher [67] ennél lényegesen több osztályt definiált:

- Automatizálás foka: kézi, félautomata vagy teljesen automata.
- Kihasznált sérülékenység: egy speciálisan a célpont rendszerében létező sérülékenység kihasználása vagy pedig a nyers erő módszere.
- Forráscím létezősége: a támadás adatfolyama hamisított címekről érkezik-e.
- Támadás adatfolyamának dinamikája szerint.
- A támadás adatfolyamának tipizálása szerint: felismerhetők-e a támadás típusára jellemző, egyedi sajátosságok.
- A támadó ágensek állandósága: a támadó végpontok ugyanazok-e vagy pedig cserélődnek.
- Áldozatok típusa: a végponton futó alkalmazás, maga a végpont, hálózat vagy pedig infrastruktúra.
- A támadás hatása az áldozatra: végleges, átmeneti működésképtelenség vagy szolgáltatási szintet csökkentő.

Ez a taxonómia részletes, megítélésem szerint túlságosan is, vannak benne kevésbé fontos elemek is. Példának okáért a támadás adatfolyamának dinamikája teljesen esetleges, ugyanaz a támadási módszer ennek az osztálynak több alkategóriájába is sorolható, pusztán a támadó szándékától függően. Problémát látok abban is, hogy a támadás hatása az áldozatra nem ítélhető meg objektíven: egy szolgáltatási szintet csökkentő támadás külső körülmények fennállása esetén okozhat átmeneti működésképtelenséget is.

A fentieken kívül még sok más olyan osztályozási módszer érhető el, amelyek a túlterheléses támadásokkal foglalkoznak, ezek azonban többnyire a [67] forrás részhalmazait képezik. Emiatt elkészítettem saját módszeremet a különböző, túlterhelést okozó támadási módszerek kategorizálásához. Célom az volt, hogy lehetőleg kevés számú osztály és ezeken belül kategóriák segítségével egyértelmű besorolási mechanizmust alkossak.

2.3 DoS támadások fő típusai

A DoS támadás valójában nem egy konkrét eljárás, hanem csak egy gyűjtőfogalom, az elérni kívánt cél – a szolgáltatás nyújtásának meghiúsítása - meghatározása. A konkrét kivitelezés nagyon sok mindentől függ, változhat a támadni kívánt célpont és a támadási módszer is. A szakirodalom rengeteg féle támadási módszert ismer, amelyek a célpont rendszerének különféle elemeit veszik célba, ezért tartottam szükségesnek a támadási módszerek rendszerezését, kategorizálását. A lehetséges támadási felületek, veszélyforrások ismeretében a védekezés is sokkal könnyebben szervezhető meg.
A DoS támadásokat három fő kategóriába soroltam:

- „Hagyományos" DoS támadás, amely során a támadó egy kellő erőforrásokkal rendelkező végpontot felhasználva igyekszik a célpont erőforrásait túlterhelni. Természetesen a támadó erőforrásainak meg kell haladnia a célpont erőforrásait.
- Elosztott DoS támadás (DDoS), amely során a támadó egy időben, nagyszámú végpontot használ a célpont erőforrásainak túlterhelésére. Ezzel a módszerrel bármilyen célpont túlterhelhető, mivel a támadó végpontok erőforrásai összeadódnak, így pusztán az elegendő számú támadó végpontról kell gondoskodni.
- Reflektív vagy erősített DDoS[29] támadás. Ekkor a támadó nagyszámú olyan hálózati végpontot használ, amelyek felett nem szerezte meg az ellenőrzést. Ezek az úgynevezett reflektorok – amelyek többnyire valós szolgáltatást nyújtó kiszolgáló számítógépek - sokszorozzák meg és irányítják át a támadó forgalmat a célpont irányába.

A DoS támadások során a számítógépes hálózatokat használják a célpont megbénítására, ezért a célhálózaton vagy célszámítógépen belüli erőforrások túlterhelésére csak a hálózati kommunikáció eszközeivel van lehetőség. Az így megcélzott rendszerelemek számossága jelentős lehet, azonban nem láttam értelmét konkrét részegységekre bontani a kategorizálást (felesleges lenne például a különféle hálózati kártyákat különböző célpontnak tekinteni, hiszen a hálózati hozzáférési technológiák sűrűn változnak, és így rendkívül sok lenne a lehetséges célpontok száma). Az informatikai rendszerek összekapcsolására régóta és elterjedten használják a

[29] A módszert „Reflective" vagy „Amplified" elnevezéssel említi a szakirodalom. Viszonylag újkeletű, néhány évre visszatekintő támadási módszer, azonban a legnagyobb hatású akciókat ezzel lehet elérni.

különböző rétegmodelleket, ezért a támadható elemek kategorizálása során ezeket a modelleket használtam fel.

2.4 Rétegmodell szerinti besorolás alapjai

Számítógépes hálózati eszközöket világszerte sokan gyártanak. Ezeknek az eszközöknek együtt kell működniük egymással és a meglevő infrastruktúrával, így elég korán felmerült a szabványosítás igénye. Ez az igény – bár alapvető jelentőségű – nehezen elégíthető ki, mivel a technológiai változások sokkal gyorsabbak, mint a szabványosítás folyamata. A jelenlegi, legnagyobb méretű informatikai hálózatot – az internetet – alkotó eszközök működését az alapelvek kidolgozói egymással együttműködő, de jól elválasztható funkciókat ellátó rétegekbe szervezték. Ezt a rétegmodellt – amelyet szokás DoD rétegmodellnek is nevezni a kutatásokat finanszírozó USA Védelmi Minisztériuma (Department of Defense) után – vette át, fejlesztette tovább, majd foglalta szabványba az ISO (International Standard Organization) nevű szervezet. A szabvány az OSI (Open System Inteconnection) nevet kapta és ISO 7498-1 azonosítóval 1984 óta létezik. Az OSI modell célja a kommunikációs eszközök funkcionális rétegeinek definiálása anélkül, hogy technológiai kérdésekben túlzottan megkötné a tervezők kezét. Az OSI referenciamodell szerint a hálózat elemeit logikai egységekre, rétegekre bontják, minden réteg egy jól definiált feladatkörrel rendelkezik, kommunikálni csak a szomszédos rétegekkel képes. A rétegek között csatolófelületek (úgynevezett interfészek) találhatók, a kommunikáció ezeken keresztül folyik. Minden réteg az előzőre épül, szolgáltatásokat nyújt a fölötte vagy alatta levő rétegnek, illetve igénybe veszi a szomszédos rétegek által nyújtott szolgáltatásokat. Egymással összekötött rendszerek esetén minden végpont egy adott rétege a vele kapcsolatban álló másik végpont azonos rétegével kommunikál. Az OSI rétegmodell 7 réteget definiál, ami sokak szerint túl sok, megnehezítve a teljes implementációt. Sok rendszerben összevonnak több réteget, illetve arra is van példa, hogy egy réteget több alrétegre bontanak (például az Ethernet esetében az adatkapcsolati réteget egy LLC[30] és egy MAC[31] alrétegre).

[30] Logical Link Control.
[31] Media Access Control.

A „magasabb” rétegek felé haladva a felhasználóhoz, a másik irányban pedig a kommunikációs közeghez kerülünk egyre „közelebb”. Az OSI 7 rétegének fontosabb funkciói az alacsonyabb rétegek felől kezdve:

Fizikai réteg

Az átvinni kívánt információt (bitekre bontott digitális adathalmaz) átvitelre alkalmas formátumú jelsorozattá (szimbólumokká) alakítja. A vételi oldalon ennek ellenkezője történik, a fogadott fizikai mennyiségek (általában elektromágneses hullám) által hordozott szimbólumok kinyerése, majd bitsorozattá konvertálása.

Adatkapcsolati réteg

A felette található – hálózati – réteg által küldött adatokat a fizikai réteg által továbbítható darabokra bontja (ezeket az adatelemeket szokás kereteknek is nevezni), majd továbbítja a fizikai réteg számára. Megjegyzendő, hogy a fizikai és az adatkapcsolati rétegek között elég szoros kapcsolat van, emiatt a DoD modell ezt a két funkciót egy rétegként definiálta.

Hálózati réteg

A hálózati réteg feladata a kommunikációs adatelemek (tipikusan adatcsomagok) célba juttatása a hálózatok között. Ehhez szükséges egy logikai címzés használata (amely segítségével meghatározható a célállomás helye a hálózati topológián belül), illetve a csomagok megfelelő irányba történő továbbítása, vagyis az útválasztás (routing). Napjainkban a legnagyobb elterjedtségnek örvendő hálózati rétegbeli protokoll az Internet Protocol (IP).

Szállítási réteg

A felek közti adatfolyamot szabályozza, szükség esetén hibaellenőrzést végez és gondoskodik a csomagok sikeres átviteléről. Ehhez nyugtázásokat és adatújraküldést használ, a felsőbb rétegek számára transzparens módon.

Viszony réteg

Két, egymással kommunikáló rendszer alkalmazásai számára biztosít egy virtuális kapcsolatot. Feladata lehet még az azonosítás és a jogosultságok ellenőrzése.

Megjelenítési réteg

A kimenő üzeneteket absztrakt formátumúvá alakítja, itt valósítható meg a titkosítási és tömörítési funkció is.

Alkalmazási réteg

Lehetővé teszi az alkalmazások számára a hálózati szolgáltatásokhoz való hozzáférést.

A DoS és DDoS támadások kategorizáláshoz nem használtam az összes réteget. A legfelső 3 réteg funkciója nehezen elkülöníthető, ezért ezeket az alkalmazási rétegbe összevonva fogom a besorolásokat elvégezni. A szállítási és hálózati réteg erősen kapcsolódik egymáshoz (a TCP/IP[32], UDP/IP[33] protokollpárosok szorosan együttműködnek egymással), ezért ezeket is összevonva, együttesen a hálózati rétegbe sorolom őket. Az összevonás azért is indokolt, mert a szállítási réteg protokoll gyengeségét kihasználó támadási módszerek segítségével is lehetséges a hálózati forgalmat túlterhelni, így mindkét réteget érinti az eredmény. A legalsó, fizikai rétegben elkövetett túlterheléses támadások speciálisak és elsősorban a rádiós hálózatokhoz kapcsolódnak. Noha ezek inkább zavarásnak tekinthetők, a DoS támadások között ismertetem őket, mivel nem általános jellegű rádiózavarásról van szó, hanem a konkrét technológia ismeretén alapuló, kifejezetten az adatkapcsolat tönkretételére szolgáló támadási módszerről. Ilyen módon a következő rétegeket tekintettem a besorolás alapjának:

- Fizikai réteg;
- Adatkapcsolati réteg;
- Hálózati réteg;
- Alkalmazási réteg.

Bár elméletileg minden támadástípusban lehetséges az összes rétegbe tartozó módszer használata, a gyakorlatban nem használják az összes lehetséges kombinációt.

2.5 DoS támadások

A DoS támadások napjainkban már kevésbé gyakoriak, mivel az elosztott és reflektív támadási formák sokkal hatékonyabbak, ráadásul a szükséges támadó eszközök is könnyebben megszerezhetők. A klasszikus DoS támadás esetében a támadó rendelkezik az akció kivitelezéséhez elegendő erőforrással rendelkező hálózati végponttal – általában átveszi az uralmat felette. A támadási módszer valamennyi rétegben kivitelezhető.

[32] TCP: Transmission Control Protocol.
[33] UDP: User Datagram Protocol.

DoS támadások (zavarás) a fizikai rétegben

A fizikai rétegben kivitelezett támadásokhoz az átviteli közeghez közvetlen hozzáférésre van szüksége a támadónak. A különböző vezetékes (galvanikus vagy optikai csatolású) hálózatok esetében ez általában a célpont épületén belüli jelenlétet igényel a támadótól, ami a lebukás veszélyét hordozza magában, ennek köszönhetően ilyen támadási módszereket nem használnak. A rádiós hálózatok esetében egy kicsit más a helyzet, a rádióhullámok ugyanis áthatolnak a falakon, így az adó szóráskörzetében – mondjuk a célpont épülete előtti utcán – lehetőség van a támadást megvalósító eszközök elhelyezésére. Jelenleg a legelterjedtebb rádiós számítógépes hálózati funkciókat biztosító megoldás az IEEE[34] 802.11 szabványcsaládba tartozó Wireless LAN[35] (a továbbiakban WLAN). Ez egy nagysebességű hálózati kapcsolatot biztosító, fejlett modulációs módszereket (szórt spektrum) használó rendszer, amelynek megzavarása viszonylag egyszerűen megoldható. Az ISM[36] sávba tartozó 2,4 GHz környéki frekvenciasávokat használja, amelyek használata ingyenes, így a zavartatása már alaphelyzetben is nagyobb, mint az engedélyköteles frekvenciáké. A hagyományos, szélessávú vagy csúszó zavarás mellett lehetséges a 802.11 által alkalmazott protokollokra speciális zavarást is végezni, ezáltal a kisugárzott teljesítményt célirányosan, csak a szükséges időre – de nagyobb amplitúdóval – bekapcsolni és így a teljesítményfelvételt drasztikusan csökkenteni. Mivel az adatátvitel keretekben történik, ezért ilyen esetben a cél nem a teljes keret átvitelének a zavarása, hanem csak egy kis részének megváltoztatása. A keret sértetlenségét mindössze egy 32 bites CRC[37] segítségével ellenőrzik, ezért hibajavításra nincs lehetőség, a keret sérülése esetén a küldő félnek a teljes keretet meg kell ismételnie. A WLAN által használt keretek formátuma szándékosan olyan, hogy azokat a fejléc lecserélésével probléma nélkül lehessen továbbítani egy vezetékes, IEEE802.3 vagy Ethernet-II szabványnak megfelelő

[34] Institute of Electrical and Electronics Engineers. Az elektromosság és elektronika – és egyre inkább a számítógépek – területén foglalkozik új technológiák szabványosítási munkáival.

[35] A 802.11 WLAN szabványcsalád definiálja az infravörös fényt is, mint információ átviteli közeget, azonban ennek használata nem terjedt el. A 802.11 egy gyűjtőszabvány, a betűkkel jelölt alpontok különböző megoldásokat jelentenek.

[36] Industrial, Scientific and Medical: ipari, tudományos és orvosi célokra fenntartott, bizonyos feltételek betartása mellett szabadon felhasználható frekvenciatartomány.

[37] Cyclic Redundancy Check: a küldő és a címzett által egyaránt ismert algoritmussal képzett speciális hibafelfedő kód. A küldő a képzett CRC értéket mellékeli az adatátvitel során. A címzett a fogadott adatokból előállítja ugyanezt az eredményt, majd összeveti a kapott értékkel. Ha a kettő nem egyezik, akkor az átvitel során sérültek az adatok, ha egyezik, akkor – a CRC hatékonyságától függően – egy adott valószínűség mellett az átvitel hibamentes volt. A 802.11 szabványcsalád újabb tagjai (802.11e és 802.11n) már hibajavító kódolást (FEC) használnak, amely bizonyos mértékű hibát nagy valószínűséggel javítani is képes.

hálózatba. Ennek hozadékaként a keretek maximális hossza körülbelül 1500 byte lehet, tehát 12000 bit zavarásához elegendő akár 1 bit tartalmát az ellenkezőjére változtatni, ekkor a CRC értéke hibás lesz, így a keretet a küldőnek meg kell ismételnie. A 802.11b hálózatok által használt modulációk (adatátviteli sebességek) szerint a zavarás hatékonysága a következőképpen alakul [68]:

2. táblázat 802.11b zavarási hatékonyság értékek. Forrás: sigmobile.org

Kódolás	Maximális csomaghossz	Bit/szimbólum	Hatékonyság
BPSK[38]	12000 bit (1500byte)	1	1:12000
QPSK[39]	12000 bit (1500byte)	2	1:6000
CCK[40] (5.5Mbps)	12000 bit (1500byte)	4	1:3000
CCK (11Mbps)	12000 bit (1500byte)	8	1:1500

Látható, hogy ha a zavaróegység figyeli az adatátvitel keretszerkezetét, és csak a megfelelő időben, egy szimbólumnyi időre kapcsolja be a zavaró adót, akkor jelentős effektív teljesítménycsökkenést lehet elérni. A legjobb hatékonyság a kis átviteli sebességű hálózatoknál érhető el, mivel ebben az esetben a keret átviteléhez szükséges idő nagy, így az 1 bit megváltoztatásához elegendő ritkán bekapcsolni az adót. A nagyobb átviteli sebességnél sűrűbben kell zavarni, a szimbólumidő ráadásul nem is tér el jelentősen (a nagyobb átviteli sebesség a fejlettebb moduláció és kódolás által biztosított nagyobb bit/szimbólum érték miatt van), így a bekapcsolási periódus sem lehet kisebb.

Az ilyen zavarókészülék megvalósítható intelligens kivitelben (a keretek figyelésével csak a tényleg szükséges időközökben kapcsolja be az adót) vagy egyszerűbb esetben egy átlagos keretidőnkénti automatikus bekapcsolással. Ekkor a készülék egyszerűbb lehet, hiszen a keretfigyelő elektronika helyett elegendő egy időzítő is.

[38] BPSK: Binary Phase Shift Keying.
[39] QPSK: Quadrature Phase Shift Keying.
[40] Complementary Code Keying.

A másik egyszerűsítési lehetőség a zavart sávok számának csökkentése. Bár a 2400-2500 MHz sávban 14 csatornát jelöltek ki, a WLAN által használt szórt spektrumú adás 22 MHz sávszélessége miatt több csatornát is átfog a sugárzás. Így elegendő a 14 csatorna helyett kevesebbet – ám azt nagyobb adási jelszinttel – zavarni a lefedéshez.
A kereskedelmi forgalomban kapható WLAN zavaró eszközök a gyártók marketing anyagai szerint nem a hálózatok megzavarására készültek, a fő cél az adatlopás, lehallgatás megakadályozása. Ezt a célt igyekeznek elérni azzal, hogy a készülék körzetében minden olyan rádiós kommunikációt meggátolnak, ami a működési frekvenciatartományban folyna. Magyarországon a 2400-2500 MHz közti tartomány használata a vonatkozó szabályok betartása mellett nem engedélyköteles, így egy ezeknek megfelelő zavarókészülék használata nem illegális. Ellenben a maximális adóteljesítmény és spektrumhasználat szabályozott, ezért az ezeket be nem tartó zavaró berendezések használata jogszabályokba ütközik.

DoS támadások az adatkapcsolati rétegben

Az ilyen támadási módszerek nem tekinthetők túlságosan elterjedtnek, mivel ez ellen lehet a legkönnyebben védekezni, a támadót lokalizálni és semlegesíteni. A támadó lehetőségei azonban tágabbak, mivel helyi hálózaton lehetséges akár a többi végpont hálózati forgalmának figyelése, és az így nyert adatok segítségével precízebben meghatározott zavaró információk küldése a célpont vagy célpontok irányába. Itt már szét kell választani a rádiós és a vezetékes hálózatok támadási módszereit, mivel az adatkapcsolati réteg MAC alrétege különbözőképpen működik a WLAN és a leggyakrabban használt LAN megoldás, az Ethernet esetében.
A WLAN hálózatok második, adatkapcsolati rétegét használva a támadáshoz, az eszköznek megfelelő fedélzeti logikával kell rendelkeznie, amely segítségével képes lehet megfelelő adatokat a többi eszköz számára érthető keretekbe szervezni, és így magának a hálózatnak a működését befolyásolni. A WLAN hálózatok alapvetően két üzemmódban működnek: (i) egy központi eszköz (Access Point - AP) köré szerveződött kliensekből álló hálózatban, vagy (ii) „egyenrangú” kliensekből felépült, úgynevezett „Ad hoc” hálózatban. Mivel a legelterjedtebb az AP köré szerveződött WLAN hálózat, ezért a legtöbb adatkapcsolati rétegben működő DoS támadás is ezt a mechanizmust érinti. Zavaró eszközként bármilyen WLAN adapter vagy speciálisan átalakított AP alkalmas, így a konkrét megoldások száma a létező szoftvereszközöktől függően több százra tehető. Egy eszközt emelnék ki a sok közül, amelyet kifejezetten WLAN zavarási

célokra alakítottak át. A „Fon Bomb” egy hordozható WLAN zavaróeszköz, amely a Fonera nevű cég Access Point készülékén alapszik. A Fonera a hozzá csatlakozott tagok számára végez WLAN szolgáltatást olyan módon, hogy a tagok WLAN hálózatait osztja meg a fizetős ügyfelekkel, a bevételből pedig a hálózatba lépett tagok is részesednek. A megosztáshoz egy speciális AP[41] szükséges, ami elkülöníti a tulajdonos saját hálózati forgalmát a fizetős ügyfelek forgalmától. A „Fon Bomb” lényegében egy letölthető firmware, ami egy Fonera AP-re tölthető. A lehetőségei sokrétűek:

- képes a Beacon Flood támadási módszer segítségével hamis AP-kat generálni;
- képes Authentication Flood támadásra, amivel a környező AP-k működése válhat lehetetlenné;
- a Deauthentication/Deassociation Attack segítségével az összes kliens eltávolítható a környező WLAN hálózatokról;
- emellett még néhány tervezési hibára épülő támadást is képes kivitelezni, valamint a behatolás érzékelő (IDS[42]) rendszerek elleni tevékenység is az eszköztárában szerepel.

A firmware Linux alapokon nyugszik, nyílt forráskódú, így fejlesztése várhatóan folyamatos lesz.

Támadási módszerek a WLAN hálózatok adatkapcsolat rétegében:

Association Flood

Az AP-k nyilvántartják a hozzájuk kapcsolódott klienseket egy úgynevezett Association Táblázatban. A támadó hamisított csatlakozási üzenetekkel feltölti ezt a táblázatot, így az AP nem képes újabb klienseket fogadni. [69]

EAPOL-Start Attack

Az EAP (Extensible Authentication Protocol) egy hitelesítési protokoll, amely segítségével a kliensek képesek magukat azonosítani. A támadás során a kliens egy EAPOL-Start üzenettel kezdi meg a folyamatot. Erre az AP egy válaszüzenetet generál (kihívás), amely során természetesen erőforrásokat különít el a hitelesítési folyamat számára. A kliens nem válaszol a kihívásra, így ezek a lefoglalt erőforrások csak egy időkorlát túllépése után szabadulnak fel. Kellő számú hamisított MAC című EAPOL-Start üzenet elküldésével a támadó lefoglalhatja az AP összes erőforrását. [70]

[41] Access Point.
[42] Intrusion Detection System.

RTS Flood

Rádiós hálózatok esetén felléphet az úgynevezett „rejtett terminál”[43] problémája. Ez ellen a 802.11 szabvány speciális adási időszeletet igénylő (RTS – Request to Send) illetve azt engedélyező (CTS – Clear to Send) üzenetekkel védekezik, a terminál csak akkor kezdheti meg saját adatcsomagjának küldését, ha arra a CTS keretet megkapta. A támadási módszer használata során a támadó speciális RTS keretekkel árasztja el a WLAN hálózatot, így lefoglalva magának az adási időréseket. [71] Ugyanez megvalósítható az RTS üzenetre válaszul adott CTS üzenetek hamisításával is.

Authentication-Failure Attack

A WLAN hálózatok kliensei egy hitelesítési folyamat végén kerülhetnek csatlakoztatott állapotba. A támadási módszer ennek a csatlakoztatott állapotnak a megszüntetésére irányul, és kétféleképpen is kivitelezhető. A támadó az AP nevében „Authentication Failed” üzeneteket küld a hálózat tagjai számára, emiatt a kliensek nem képesek csatlakozni az AP-hoz. A másik módszer fordított, ekkor a támadó a kliensek nevében hamis hitelesítési üzenetet küld az AP számára, amely erre válaszul kijelentkezteti a klienst. [72]

Disassociation Flood

A támadó első lépésben azonosítja az AP-hez csatlakozott klienseket, majd az AP nevében a kapcsolat bontására szolgáló üzeneteket kezd küldeni. A kliensek az üzenetet fogadva bontják a kapcsolatot, így a hálózat működése lehetetlenné válik. [72]

Beacon Flood

A támadó hamis Beacon üzeneteket küld, amikben hamis, nem létező AP-kat hirdet. Emiatt a még nem csatlakozott kliens nem tudja kiválasztani a számára fontos AP-t, így csatlakozni sem tud. [73]

A WLAN hálózatok mellett a vezetékes hálózatok is túlterhelhetők az adatkapcsolati rétegben. Az ilyen támadási módszerek nem tekinthetők túlságosan elterjedtnek, mivel ez ellen lehetséges a legkönnyebben védekezni, a támadót lokalizálni és semlegesíteni. Időnként azonban a támadónak megéri a kockázatot vállalni, mivel helyi hálózaton lehetséges akár a többi végpont hálózati forgalmának figyelése is, és ez alapján hatékony akció indítása is. Lehetséges olyan forgatókönyv is, amely során a

[43] Rejtett terminál (hidden terminal): egy központi egységhez kapcsolódó két terminál egymás vételkörzetén kívül helyezkedik el, így egymás adását nem tudják figyelni. Ha az egyik adása közben a másik terminál is adni kezd, az a központi egységnél ütközést okoz.

célhálózatba kívülről bejuttatnak egy kártevő programot, amely aztán a kívánt időpontban megbénítja az egész rendszer működését, többek között egy adatkapcsolati DoS támadással. Emiatt érdemes áttekinteni a – legtöbbször Ethernet technológiával működő – helyi hálózatok támadási felületeit, az alkalmazható módszereket.

MAC flooding

Az Ethernet switch[44] eszközök minden csatolójukon figyelik és nyilvántartják az ott található végpontok MAC[45] címeit, és a keretek irányítása során felhasználják ezeket az adatokat. Mivel a switch egyik csatolójára egy másik switch is kapcsolódhat, ezért az eszközöket fel kellett készíteni arra az állapotra is, amikor egy csatolón több MAC cím is előfordulhat. Speciális alkalmazásokkal lehetséges olyan kereteket generálni, amelyekben a feladó MAC címe véletlenszerűen változik, kellően sok ilyen MAC címet generálva előbb-utóbb betelik az adatok tárolására szolgáló memória,[46] és ettől a pillanattól kezdve a switch már nem tudja tovább folytatni a normál működést, átkapcsol „fail-safe" módba. Ez azzal jár, hogy valamennyi bemenetére érkező keretet továbbítja az összes kimenetére, lényegében egy hub[47] funkcionalitását biztosítva. Ez egyrészt lelassítja a hálózat működését, másrészt pedig lehetővé teszi a támadó számára a teljes hálózati forgalom lehallgatását. [74]

DoS támadások a hálózati rétegben

A hálózati réteg a helyi hálózatok egymáshoz kapcsolásáért felelős, az itt használt címzési módok már nem a hálózat fizikai, hanem inkább a logikai felépítéséhez alkalmazkodnak. A hálózati rétegben kivitelezett támadások már érkezhetnek távoli hálózatokból, így népszerűségük jóval nagyobb, mint a helyi hálózatokban alkalmazott módszereké. A támadó egyetlen végpontból olyan hálózati forgalmat generál, amelynek feldolgozását a célpont nem képes végrehajtani, így működésképtelenné válik. A támadó végpont általában egy jól megválasztott, jelentős erőforrással rendelkező

[44] Hálózati kapcsolóeszköz.

[45] Az Ethernet típusú hálózatok az üzenetszórásos elvet követik, vagyis az üzenetet küldő végpont a küldött adathalmazt ellátja a címzett azonosítójával és elküldi a hálózat minden eleme számára. A címzett azonosítójának vizsgálatával minden végpont eldönti, hogy az üzenet neki szól-e. Ha nem, akkor egyszerűen figyelmen kívül hagyja. Ezt a 48 bit méretű azonosító számot nevezik MAC címnek. A mai, modern Ethernet hálózatok már kapcsolókat (switch) használnak a hálózati forgalom vezérlésére, amely képes a MAC címek alapján közvetlenül a címzettnek küldeni az adatokat.

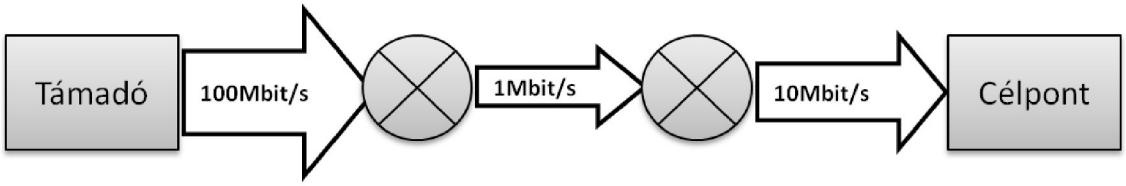
[46] A MAC címek tárolására szolgáló memória neve: Content-addressable Memory (CAM).

[47] HUB: hálózati elem, a kábeleken keresztül, látszólag csillag topológiában hozzá kapcsolódó végpontokat köti egy közös használatú sínre, más néven buszra.

DOI azonosító: 10.17625/NKE.2012.008

rendszer. Napjainkban az IP[48] szinte egyeduralkodónak tekinthető a hálózati rétegben működő kommunikációs protokollok között, ezért a későbbiekben csak az ilyen módszerek olvashatók.

A támadó által generált forgalom általában olyan csomagok sokasága, amelyek forráscíme – a feladó hálózaton belüli azonosítója - könnyen hamisítható. Az ilyen DoS támadások hatásossága nem túl jó, mivel a támadás könnyen felfedhető, és a támadó által generált forgalom letiltható, ezért az új támadások már az elosztott módszereket (DDoS) használják. Az erőforrások fontossága miatt a támadó végpont kiválasztása körültekintést igényel, mivel a támadó és a célpont között húzódó teljes kommunikációs csatornának bírnia kell a túlterheléshez szükséges forgalmat. Az ábra ezt a csatornát mutatja:



5. ábra Sávszélesség szűkülésének problémája (szerkesztette a szerző)

Érvényesül a „leggyengébb láncszem" elve, ha a láncban van a támadóénál kisebb áteresztőképességgel rendelkező szakasz, akkor a támadás eleve sikertelen lesz.

ICMP flooding

Az ICMP (Internet Control Message Protocol) [75] az IP fontos segédprotokollja. Segítségével tudatják az útválasztók egymással a csomagok továbbítása során bekövetkező hibákat, eseményeket, emellett diagnosztikai célokat is szolgál. Egy hálózati végpont a leggyorsabban úgy győződhet meg egy másik végpont működőképességéről (vagy az odáig vezető hálózati út működőképességéről), hogy küld számára egy „Echo Request" ICMP üzenetet. A másik végpont, ha megkapta a kérést, egy „Echo Reply" üzenettel válaszol. Ez az üzenetváltás játszódik le a legtöbb operációs rendszer alatt elérhető „ping" parancs hatására. Ezek a csomagok rövidek (tipikusan 74 byte méretűek), így normál alkalmazás mellett nem terhelik jelentősen sem a hálózatot, sem pedig a végpontok számítási kapacitását. Lehetséges azonban az „Echo Request" üzeneteket nagyobb méretben is küldeni, Windows XP használatakor a –l, Linux alatt pedig a –s kapcsolók használatával. A támadás kivitelezése során a

[48] Internet Protocol, az interneten használt csomagkapcsolt hálózati adatátviteli protokoll.

támadó - ilyen módon megnövelt méretű - „Echo Request” csomagokat küld a célpont számára, esetleg erősített, vagy reflektív módszerrel nagyszámú végpontról megsokszorozva. A támadó végpontok számától és a rendelkezésükre álló sávszélességtől függően a célpont sávszélessége túlterhelhető, így az általa nyújtott szolgáltatások annyira lelassulnak, hogy a normál, üzemszerű működés lehetetlenné válik. [76]

Ping of Death Attack

Egy régi támadási módszer, amelynek nyilvánosságra kerülése után minden operációs rendszerben hamar megszüntették a sérülékenységet, azonban a programhiba sajátossága miatt érdemes a problémával foglalkozni. A Ping of Death szintén az ICMP Echo Request üzenetet használja, és szintén a csomagméret növelésével éri el az eredményt. A programhiba minden, BSD TCP/IP protokoll és ping parancs megvalósítást használó operációs rendszert érintett, gyakorlatilag az összes akkori elterjedt rendszert. A támadás során az „Echo request” csomag mérete meghaladja a 65535 byte-ot, ami elméletileg lehetetlen, hiszen a csomagok mérete erre az értékre korlátozott. Azonban az IP csomagok mérete nagyobb lehet az adatátviteli hálózatok második rétegében használt protokollelemek maximális MTU[49] méreténél. Ekkor üzenetet szállító IP csomagokat a továbbításban részt vevő útválasztók széttördelik kisebb részekre (fragment), majd a címzett állítja össze őket újból. Minden egyes ilyen fragment rendelkezik egy címmel (Fragment Offset), amely azt adja meg, hogy az adott rész a teljes csomagon belül hol helyezkedik el. A küldő végpontnak – bár a szabvány ezt nem engedélyezi – lehetősége van olyan üzenetet küldeni, amely már eleve tördelt, így a Fragment Offset mezőket tetszés szerint állíthatja be. Ilyen módon lehetősége nyílik arra, hogy olyan csomagot készítsen, amely a 65535 byte méretű puffer végénél kezdődik, viszont a fragment vége már túlnyúlik a lefoglalt memóriaterület végén. A hibás TCP/IP stack „Echo request” üzeneteit kezelő programrésze erre nincs felkészítve, így puffer túlcsordulás következik be, ami a cél összeomlását eredményezi. [77]

A puffer túlcsordulás a modern számítógépes rendszerekben is állandó problémát jelent, nagyon sok támadási módszer alapját képezi.

[49] MTU: Maximum Transmission Unit, a legnagyobb, egy darabban átvihető adategység, Ethernet hálózatok esetén például 1500 byte.

Teardrop Attack

Ha egy router olyan IPv4 csomaggal találkozik, amelynek mérete meghaladja a célhálózaton engedélyezett maximális keretméretet, akkor a csomagot fel kell darabolnia (fragmentálás). Az IP csomag fejléce ugyanaz marad minden részcsomag esetében, kivéve a Fragment Offset, Identification és a Fragment bitek állapotát. A Fragment Offset adja meg a részcsomag helyét a teljes csomagon belül (8 byte-os egységekben). Normál esetben az egymás utáni részcsomagok a teljes csomagon belül egymás utánra kerülnek, átfedés nélkül. Mivel a routerek nem állítják össze a feldarabolt csomagokat (ez a feladat a címzettre vár), ezért lehetséges a feladó oldalán olyan csomagokat generálni, amik már a küldéskor feldarabolt állapotban vannak, és a soron következő darab kezdete átfedésbe kerül az előző csomagban utazó darabbal. Ügyesen megválasztott csomagokkal egy előző csomagban utazó magasabb rétegbeli protokoll fejléce is felülírható, így kijátszhatók a csomagszűrő tűzfalak, vagy erre érzékeny operációs rendszer esetében akár végtelen ciklusba is vihető az áldozat. [78]

Land Attack

A támadás nyitott TCP portok ellen irányul, vagyis olyan végpontok érintettek, ahol van működő TCP szolgáltatás. A módszer lényege az, hogy az elkövető olyan speciális csomagot küld (TCP SYN)[50] az áldozatnak, amely hamisított forráscímmel és forrás port címmel rendelkezik. A LAND alkalmazása során mind a forrás, mind a cél cím ugyanaz, az áldozat IP címe, a forrás és célport címek pedig megegyeznek a nyitott szolgáltatás címével, így a célpont által küldött válaszüzenet visszakerül a küldő szolgáltatáshoz. Az erre érzékeny rendszerekben ez jelentős lassulást vagy akár működésképtelenséget okoz. [79]

Bonk Attack

Az eljárás hasonló a Teardrop Attackhoz, de itt a Fragment Offset értéke nem átfedéseket tartalmaz, hanem a teljes csomag határain túlra mutat. A fogadó fél (az áldozat) az IP csomag első darabjának fogadásakor lefoglal akkora méretű tárterületet, ami elegendő a teljes csomag tárolásához. Az egyes darabok beérkezésekor ezen a területen történik meg a csomag helyreállítása. Ha egy beérkező darab csomagon belüli kezdete ezen terület határain kívül esik, akkor az operációs rendszer olyan memóriaterületeket is felülírhat, ahol más, fontos adatokat tárol (például a veremtár). Ennek a puffer túlcsordulásnak (buffer overflow) az eredménye részleges, de akár teljes

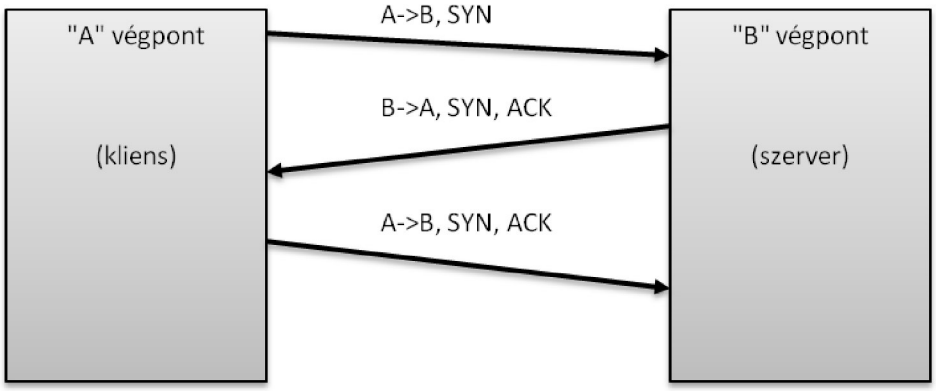
[50] A TCP kapcsolat felvételének első lépéseként a kezdeményező egy SYN csomaggal jelzi csatlakozási szándékát.

DOI azonosító: 10.17625/NKE.2012.008

rendszerleállás is lehet. Természetesen ehhez az is szükséges, hogy az operációs rendszer – programozói hiba miatt – ne ellenőrizze a beérkező darabok megfelelőségét. A módszer az UDP 53-as portot használta (DNS szolgáltatás), később megjelent egy fejlettebb változata is (Boink Attack), amely több portot célzott meg. [80]

TCP SYN Flood Attack

Az IP hálózatok – beleértve természetesen az internetet is – legnépszerűbb, leggyakrabban használt szolgáltatásai TCP [81] kapcsolatot használnak. Az IP egy összeköttetés-mentes[51] csomagkapcsolt hálózati protokoll, amely azt jelenti, hogy a két fél között az adatok kisebb, tipikusan néhány 100 byte méretű csomagokban közlekednek; minden csomag továbbítása a hálózatban működő útválasztók segítségével, a csomag fejlécében elhelyezett forrás- és célcímek alapján történik. Két, egymást követő csomag nem feltétlenül ugyanazon az útvonalon halad, a hálózatban el is tűnhetnek csomagok vagy a beérkezés sorrendje nem ugyanúgy alakul, mint a küldésé. Mindezek ellenére a TCP segítségével virtuális összeköttetés alakítható ki a két fél között, a TCP-t használó alkalmazások úgy képesek kommunikálni egymással, hogy nem kell foglalkozniuk a továbbítás során bekövetkező hibák kezelésével. Ezt a virtuális kapcsolatot egy összeköttetés-felépítési fázis, úgynevezett „háromutas" kézfogás[52] hozza létre, ami során a két fél megállapodik a kapcsolat paramétereitől. Normál esetben ez a következő módon történik:



6. ábra TCP kapcsolat létrehozása, háromutas kézfogás (RFC 793 alapján szerkesztette a szerző)

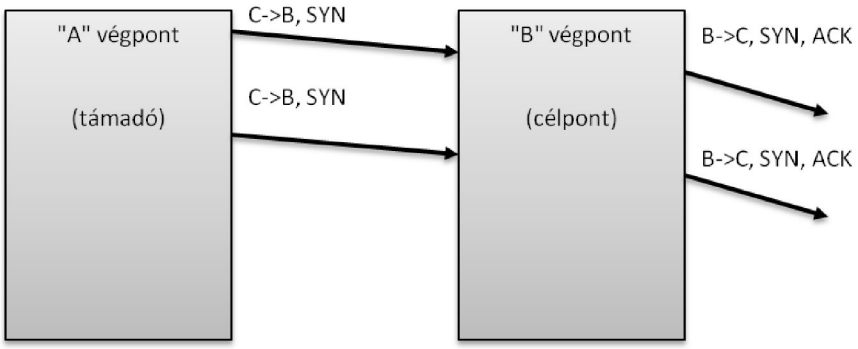
[51] Az összeköttetés-mentes módszer során a két fél között nincsen fix, a kommunikáció teljes idejére lefoglalt összeköttetés. Az átvinni kívánt információ elemeit önállóan továbbítják a végpontok közt, az aktuális terhelés, ennek köszönhetően pedig eltérő késleltetési és egyéb minőségi paraméterek függvényében.

[52] Háromutas kézfogás: eredetileg „Three-way handshaking". Fontos szerepe van a TCP kapcsolatok eltérítésének megakadályozásában.

DOI azonosító: 10.17625/NKE.2012.008

- A kliens SYN csomagot küld, egyidejűleg generál egy kezdeti sorozatszámot (Sequence Number), amelynek feladata az egyes adatelemek adatfolyamban elfoglalt helyének jelölése.
- A szerver SYN + ACK csomaggal nyugtáz, egyidejűleg saját maga is előállítja saját sorozatszámát. A másik féltől kapott Sequence Number értéket megnöveli eggyel, és ezt az értéket elhelyezi a fejléc Acknowledgement Number mezőjében.
- A kliens SYN + ACK csomaggal nyugtáz. Az Acknowledgement Number mezőben visszaküldi a szervertől kapott kezdeti sorozatszám megnövelt értékét. A kapcsolat ettől a ponttól működőképes, a csatorna kiépült.

A támadás menete:



7. ábra TCP SYN flood attack (szerkesztette a szerző)

A támadó a célpont számára egy hamisított forráscímmel SYN csomagot küld. A célpont ennek hatására előkészíti a létrehozandó kapcsolatot, meghatározza az általa használni kívánt kezdősorszámot, és tárolja a paramétereket. Ezután SYN + ACK nyugtázó csomagot küld a feladónak a hamisított forráscímre. A célpont erre az üzenetére természetesen nem kap választ, ezért néhányszor (általában még háromszor) újraküldi azt, minden alkalommal kivárva az előírás szerinti időt. Ha az utolsó próbálkozásra sem kap választ, akkor felszabadítja a kapcsolat tárolására szolgáló memóriát.

A „félkész” kapcsolatok paramétereinek tárolására szolgáló memória mérete véges, ezért ha a támadó nagy mennyiségű SYN csomaggal árasztja el a célpontot, akkor hamarosan megtelik ez a tárterület, így nem lesz képes új TCP kapcsolatot létrehozni, ami a felhasználók szempontjából a szolgáltatás működésképtelenségét jelenti.

A védekezés módszerei már rendelkezésre állnak, a „félkész” kapcsolatok tárolására szolgáló memória (Syn Cache) megnövelése illetve a Syn Cookie nevű eljárás képében. A memóriaméret növelése természetesen csak fokozza a védekezőképességet, igazi megoldást a Syn Cookie[53] használata biztosít. [82] Bár a támadási módszer és a védekezés is régóta ismert, a 2007. májusi észtországi DDoS támadások során is sikerrel alkalmazták az elkövetők.

UDP Flood Attack (Pepsi attack)

A működés hasonló a TCP SYN flood attackhoz, de ebben az esetben UDP csomagokat használnak a bénításra. Az UDP protokoll nem használ a kapcsolat felépítésére handshake mechanizmust, ezért hamisított forrás IP címekkel könnyen támadható (a TCP esetében a kapcsolat felépítéséhez szükséges a kétirányú üzenetváltás, ami hamisított címmel nem megoldható). A csomag beérkezése után a megfelelő szolgáltatás elindul a szerveren (ezáltal CPU időt, memóriát és átviteli sávszélességet foglalva), majd a válasz előállítása után a hamisított IP címre történik a csomagküldés. Tipikus módszer egyes szerverdiagnosztikai szolgáltatások vagy a DNS támadása. [83]

DoS támadások az alkalmazási rétegben

A támadás során a támadó gondosan megválasztott üzeneteket küld a célpontnak. A támadási módszer a kliens-szerver rendszerekben tapasztalható aszimmetria jelenségét használja ki. Egy kérés elküldése sokkal kevesebb erőforrást igényel, mint a választ előállítani. Ha a valódi világban működő telefonos tudakozóra gondolunk, belátható, hogy a kérdezőnek egyszerűbb feltennie a kérdést, mint a tudakozónak megkeresni a kérdésre adandó választ. A népszerű World Wide Web kiszolgálók a visszaküldött tartalmakat napjainkban már legtöbbször dinamikusan, a kérés feldolgozása során állítják elő valamilyen adatbázisból nyerve a szükséges adatokat. Ha elég sok adatbázis műveletre kényszerül a kiszolgáló, akkor kifogyhatnak az erőforrások. De a célnak bármilyen kliens-szerver elven működő alkalmazás megfelel, a lényeg az, hogy a kliens kérésének előállítása és elküldése sokkal kisebb erőforrást emésszen fel, mint a válaszüzenet generálása.

[53] A Syn Cookie eljárás során a „félkész” kapcsolatok állapotát nem tárolja a szerver, hanem a paramétereket a válaszüzenetbe kódolja, így amikor a kliens visszaküldi ezt a végső nyugtázás során, akkor a szerver ebből elő tudja állítani a szükséges paramétereket. Az adatok tárolására és hitelességének ellenőrzésére kriptográfiai módszereket használnak.

Néhány egyszerű példa ilyen típusú támadásokra:

Email flooding

A támadó a célpont SMTP[54] szervere számára nagy mennyiségű – esetleg speciálisan a célpont hiányosságaihoz méretezett - elektronikus levelet küld. Ha a célpont a beérkező elektronikus levelek számára kisméretű tárolókapacitással rendelkezik, akkor lehetséges a célpont háttértárának megtöltése, amely a további levelek fogadását, szélsőséges esetben akár a teljes operációs rendszer működését is lehetetlenné teszi. Mivel napjainkban egyre több kéretlen levél érkezik, ezért a levelezőszervereken gyakran működnek spam-,[55] illetve vírusszűrő alkalmazások. Egy ilyen szűrő is megtámadható, kifejezetten a szolgáltatás gyengéire optimalizált levelekkel. Egy időben elterjedt módszer volt a levélbombák, vagy extrém nagyméretű tömörített állományokat tartalmazó levelek (Zip-bomb) használata. Egy tömörített állomány vírusellenőrzése csak úgy hajtható végre, ha a szerver visszaállítja a tömörítetlen változatot, majd ezen futtatja végig a tesztet. Ha a tömörítetlen állomány mérete nagyobb, mint a rendelkezésre álló szabad memória, akkor a szervernek a háttértáron kell biztosítania a szükséges helyet, ezen viszont több nagyságrenddel lassabb az adatok elérése. Kellő mennyiségű levéllel fenntartható ez a memóriaszegény állapot, vagyis a szerver erőforrásai lefoglalhatók. [84]

Webszerver támadása

Egy webkiszolgáló általában maximalizálja az egy időben működő példányainak (processz vagy szál) számát, pont a túlzott igénybevétel megakadályozására. Ha a támadó egyidejűleg sok példányt hozat létre a webszerverrel (egy időben sok letöltést indít el kis sebességű hálózaton), akkor igénybe veszi az összes rendelkezésre álló processzt, így a többi felhasználó nem képes a kiszolgálóhoz csatlakozni. Ekkor a szerver erőforrásai nincsenek túlzottan leterhelve, a sávszélesség kihasználatlan, a látogatóknak mégis várakozniuk kell.

Egy ilyen támadást kivitelezni normál DoS (1 támadó végpont-1 célpont) módszerrel csak helytelenül konfigurált kiszolgáló ellen lehetséges.

---

[54] SMTP: Simple Mail Transfer Protocol. Az elektronikus levelet küldő kliens, és a levél célba juttatását végző szerver közti kommunikációt meghatározó eljárás. Leírása az RFC 821-ben található.

[55] Spam: a kéretlen – elsősorban reklám – levelekre alkalmazott kifejezés, eredetileg egy húskészítmény neve. Az elnevezést a Monty Python társulat egyik tévés jelenetére vezetik vissza, amelyben az eladó leginkább csak spam-et kívánt a vendégekre tukmálni. http://www.youtube.com/watch?v=BIWk5bGno58

2.6 DDoS támadások

A DDoS támadások valójában egyetlen dologban különböznek a DoS támadásoktól: a támadó nem egyetlen végpontból indítja akcióját, hanem központilag koordinálva, egyszerre sok – lehetőleg minél több – helyről. A DDoS (Distributed Denial of Service) kifejezésben a „Distributed" szó az elosztott rendszerekre utal, amelyeknek sok definíciója létezik. Andrew S. Tanenbaum és Maarten van Steen szerint: [85]

„Az elosztott rendszer az önálló számítógépek olyan összessége, amely kezelői számára egyetlen koherens rendszernek tűnik."

Ez a definíció két követelményt támaszt: önálló számítógépekből álljon, illetve a felhasználója számára egyetlen rendszerként funkcionáljon, azaz összehangolt működésre legyen képes. Ehhez természetesen az szükséges, hogy a rendelkezésre álljon egy ilyen rendszer. A később bemutatott botnetek kiválóan megfelelnek a fenti követelményeknek, így nem véletlen, hogy a nevük szinte összefonódott a DDoS támadásokkal. A módszerek gyakorlatilag DoS módszerek, így a besorolás is megegyezik az ott végzett besorolással, a támadás igazi erejét azonban a nagyszámú támadó végpont jelenti.

DDoS támadások a hálózati rétegben

A támadási módszerek lényegében megegyeznek a DoS támadások esetén használt módszerekkel, azonban itt egy időben sok végpont kezdi meg a műveletet. A védekezés nehéz, mert a támadó végpontok a hálózaton szétszórva találhatók. Csomagszűréssel a hálózati forgalomból kiszűrhetők túlterhelést okozó üzenetek, de ez sok kényelmetlenséggel is jár. Egyrészt a szűrés jelentős számítási teljesítményt vesz igénybe a hálózati eszközökben, másrészt a kiszűrt csomagok közé óhatatlanul bekerülnek a normál forgalom adatai is.

DDoS támadások az alkalmazási rétegben

A szolgáltatást nyújtó alkalmazást egy időben nagyszámú végpont veszi „tűz" alá. Nagy mennyiségű végponttal lehetséges akár egy levelező szerver háttértárolóját is teletölteni használhatatlan levelekkel. Ha a célponton kéretlen levelek elleni szűrés is működik, akkor a hatalmas levéltömeg átvizsgálása a processzort fogja túlterhelni, így a kiszolgáló feldolgozási ideje olyan drámaian megnő, ami gyakorlatilag egyenértékű a leállással.

Alkalmazási rétegben kivitelezett HTTP támadás

A HTTP (Hypertext Transfer Protocol) a weboldalak eléréshez használt internetes protokoll, talán a legszélesebb körben használt internetes technológia. A működése kliens-szerver modellt követ, tranzakció alapú. A kliens a lekérni kívánt weboldal – vagy egyéb elérhető objektum – azonosítóját (URL: Unified Resource Locator) elküldi a szervernek, a szerver pedig a válaszüzenetében továbbítja a kért objektumot. A kérés általában sokkal rövidebb, mint a válasz, vagyis a legtöbb webes szolgáltatás aszimmetrikus működésű. Manapság egyre több webes szolgáltatás dinamikusan, a kérés kiszolgálása során valamilyen adatbázist felhasználva állítja elő a kért oldalt, ezáltal extra szolgáltatásokat biztosítva a felhasználók számára. Ilyen extra szolgáltatás lehet a tartalomban végzett szabadszöveges keresés, amelynek kiszolgálása során sok, nehezen optimalizálható lekérdezést kell végrehajtani az adatbázisban tárolt adatokon. Ha a támadó képes ilyen, sok erőforrást igénylő kérést előállítani és azt nagyszámú végpontról egy időben elküldeni a kiszolgáló számára, akkor jelentős terhelést okoz a kiszolgáló adatbázis kezelőjének. Szélsőséges esetben ez akár a kiszolgáló leállásához is vezethet. A helyzetet súlyosbítja, hogy egy HTTP kérés mérete néhány 100 byte, így nagyon rövid idő alatt sok is elküldhető belőle, míg a válasz összeállítása nagy teljesítményű számítógépek használata mellett is több időt vesz igénybe.

A szolgáltatások általában aszimmetrikus működésűek (a kérést elküldeni egyszerűbb, mint a választ előállítani), így könnyű lefoglalni az erőforrásokat (hálózati sávszélesség, számítási kapacitás).

A támadás akár egy egyszerű HTML[56] oldal betöltésével is kezdeményezhető, amelyet egy időben nagyszámú végponton elindítva komoly terhelést lehet okozni. Ilyen támadásra alkalmas lehet az alábbi kód:

```
<html>
<head>
<title>DOS</title>
<script type="text/javascript">
function Tolt()
{
      sSearch = "";
      for (i=0; i<7; i++)
```

[56] Hypertext Markup Language.

```
      sSearch+=String.fromCharCode(65+Math.floor(Math.random()*27));
      sSearch="http://www.aldozat.valahol/kereso?keresd="+sSearch;
      document.getElementById("dframe").src=sSearch;
      var tt = setTimeout("Tolt()",1000);
}
</script>
</head>
<body onload="Tolt()">
<iframe id="dframe" src="about:blank" width="600"
height="600"></iframe>
</body>
```

Egy ehhez hasonló (természetesen jóval kifinomultabb módszert használó) támadás ellen csaknem lehetetlen védekezni, roppant nehéz a rosszindulatú forgalmat megkülönböztetni a normál, üzemszerű forgalomtól. Ha sikerült a támadás módszerét azonosítani, az adott támadás ellen már lehetséges egyedileg védekezni. Drága megoldást jelent az elosztott architektúra (cache szerverek,[57] fürtözés[58]), ezek használatával a hálózatban elosztott támadó végpontok nem képesek egy célpontra összpontosítani a támadást. A nagyméretű botnetek terjedésével azonban a támadók is egy elosztott rendszert képeznek, így minden célpontot a hozzá közeli botnet kliensek támadhatnak.

2.7 Reflektív (erősített) DDoS támadások

A DDoS támadási módszerek továbbfejlesztését jelentik azok a támadások, melyek során más, „ártatlan” végpontokat – úgynevezett reflektorokat - használnak fel támadóként (vagy inkább fegyverként). Ezeket a végpontokat nem szükséges uralni, elegendő az Internet sajátosságait megfelelő módon kihasználni. A reflektív támadás során a támadó gondosan megválasztott adatforgalom segítségével készteti arra a támadásban részt vevő ártatlan végpontokat, hogy a célpont számára kárt okozó adatforgalmat generáljanak, ezért a tényleges támadó kiszűrése szinte lehetetlen.

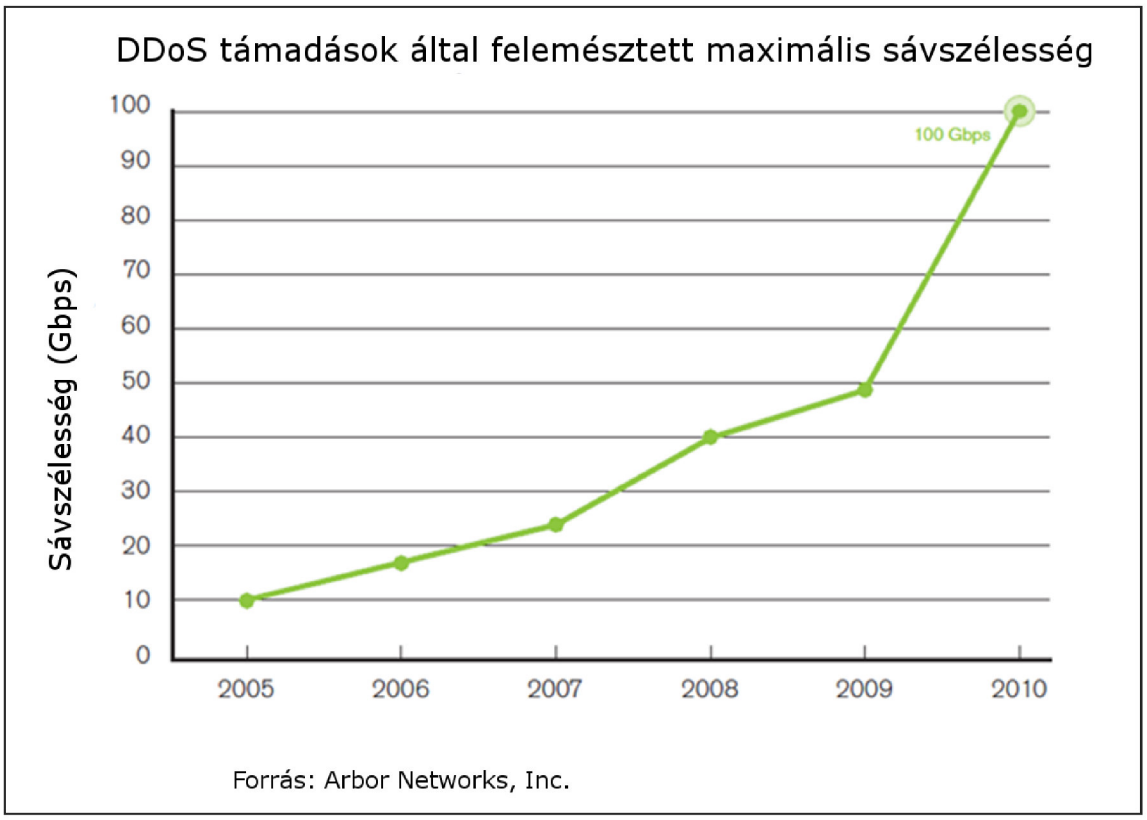
---

[57] A cache szerverek egy webhely tartalmát osztják el a hálózat különböző pontjain megtalálható háttérszerverekre. A címfeloldás és a hálózati forgalom megfelelő vezérlésével így megoldható, hogy a kliensek kérését mindig a hozzájuk legközelebbi szerver szolgálja ki, csökkentve a felesleges hálózati terhelést, a szűk keresztmetszetek kialakulását.

[58] Fürtök, klaszterek: olyan rendszerek, amelyekben a szerver valójában több számítógép összekapcsolásával alakul ki, a felhasználók számára viszont egy egységként látszik. Lényegében egy elosztott rendszer.

DOI azonosító: 10.17625/NKE.2012.008

A DDoS támadásokhoz hasonlóan, a hálózati és az alkalmazási rétegben egyaránt kivitelezhető. A reflektív támadások egyre nagyobb veszélyt jelentenek, az segítségükkel kivitelezett támadások volumene évről-évre jelentősen nő. Az Arbor Networks hálózatbiztonsági cég mérései szerint 2009 és 2010 között a legnagyobb (egy reflektív DNS módszerrel elkövetett) DDoS támadás által lefoglalt sávszélesség megduplázódott, és elérte a 100Gbit/s-ot!



8. ábra A DDoS támadások sávszélessége éves bontásban (forrás: Arbor Networks)

Hálózati rétegben kivitelezett reflektív DDoS támadások

Az ilyen támadások során az elkövető olyan hálózati végpontokat keres, amelyeket valamilyen módszerrel rábír arra, hogy a célpont felé küldjenek – többnyire – IP csomagokat. Ezek az adategységek válaszüzenetek, így a módszer elemi feltétele az, hogy az adatforgalmat kiváltó üzenetek forráscíme hamisított legyen.[59] Az ilyen csomagok előállítása nem bonyolult feladat, hiszen csak 32 bit beállítását kell megoldani az elküldött csomagban, amire kész segédprogramok nyújtanak lehetőséget. A kivitelezést csak a támadó végpont hálózati szolgáltatója nehezítheti, amennyiben a más hálózatok irányába tartó adatforgalomból kiszűri a nem saját hálózati

[59] A hamisított forráscímet használó módszereket IP Spoofing néven ismerik.

címtartományba tartozó IP forráscímet tartalmazó csomagokat. Azonban, ha egy szolgáltató be is tartja a vonatkozó szabvány [86] előírásait, akkor sem tudja kiszűrni a saját hálózatból saját hálózatba irányuló IP címhamisítást, így a védekezés elméletileg sem lehet teljesen megoldott. Ráadásul az RFC[60] implementálása nem kötelező érvényű, csak a szolgáltató hozzáállásán múlik, hogy alkalmazza-e vagy sem.

„Smurf" attack

Minden IP hálózatnak létezik egy broadcast (szórási) címe, amelyre üzenetet küldve a hálózat összes végpontja megszólítható. Ha a hálózat rendszergazdája az útválasztót úgy állítja be, hogy ez a cím külső hálózatok irányából is elérhető, akkor egy kívülről érkező, a hálózat broadcast címére szóló csomagra a hálózat minden tagja válaszol. A „Smurf attack" során a támadó hibásan konfigurált, nagy sávszélességű, sok végpontot tartalmazó hálózatokat keres. A célpont címét hamisítva feladóként, a hálózat broadcast címére elkezd Echo request üzeneteket küldeni, amire a hálózat összes végpontja válaszol, Echo reply üzeneteket küldve a célpont címére. [87]

A támadási módszernek – amely nevét az első implementációt tartalmazó forráskód neve alapján kapta - ma már inkább történelmi jelentősége van, az újonnan forgalomba kerülő hálózati útválasztók már gyárilag úgy konfiguráltak, hogy ne tegyék lehetővé az ilyen jellegű módszereket.

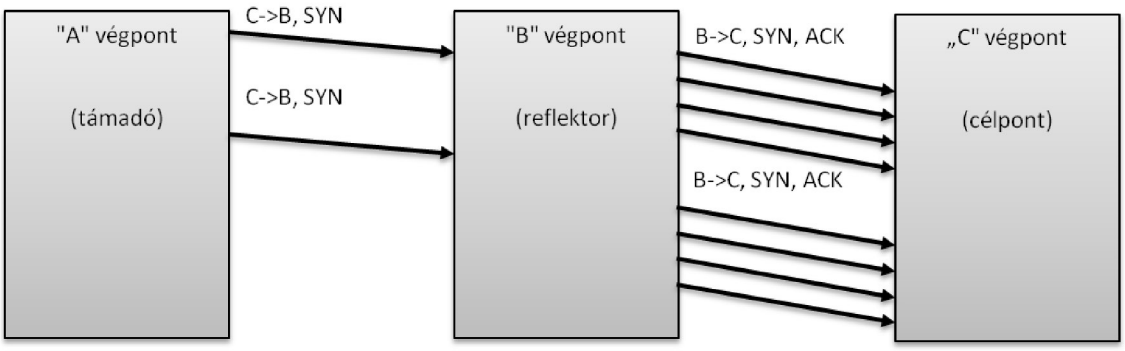
TCP Syn+ACK Attack

A támadás nagyon hasonló a TCP SYN Flood támadáshoz, azonban ebben az esetben nem a célpont számára küldik a kapcsolat felvételi kérést, hanem egy ártatlan végpontnak. Természetesen a csomag forrás IP címe hamisított, és a célpont IP címét tartalmazza. A SYN csomagra válaszul keletkezik legalább négy SYN+ACK csomag, amelyet a célpont kap meg. A módszernek két nagy előnye van:

- a célpont számára érkező csomag egy semleges helyről érkezik, így a csomagszűrők nagy valószínűséggel átengedik;
- az ártatlan végpont nem csak egy SYN+ACK csomagot küld. Mivel a célponttól nem érkezik meg a háromutas kézfogás utolsó csomagja (ACK), ezért még legalább háromszor újraküldi azt, tehát a támadó egyetlen csomagjának hatására a célpont négy csomagot kap, az erősítés mértéke így négyszeres lesz. [61]

[60] RFC: Request for Comment. Az internet alapvető megoldásainak de facto szabványai.
[61] Egy valós, ilyen módszert használó támadás leírása a következő címen olvasható: http://www.grc.com/dos/drdos.htm

DOI azonosító: 10.17625/NKE.2012.008



9. ábra Reflektív TCP SYN+ACk támadás (szerkesztette a szerző)

Hatásosan védekezni ilyen támadások ellen csak az internet-szolgáltatók bevonásával lehet, mivel a káros csomagokat még a célpont hálózatának határain kívül kell elfogni. A legtöbb hálózati rétegben végrehajtott DoS támadás alkalmazza a forrás IP címek hamisítását, ezért az internet-szolgáltatók feladata a saját hálózatuk határain működő útválasztók helyes konfigurálása, amely meggátolja a saját hálózatukból más hálózatok felé tartó olyan csomagok továbbítását, amelyek forrás IP címe nem a saját hálózati címtartományába tartozik, amint azt az RFC 2827[62] részletezi. Ez a módszer azonban – sajnos - nem véd a szabálynak megfelelő, de mégis hamisított forráscímű csomagok ellen.

„Fraggle" attack

A Smurf attack módosított változata, azonban ez UDP[63] portokra küld hamisított csomagokat. Ha a port létezik, akkor válaszüzenet megy a célpontnak, míg ha nincs ilyen port, akkor egy ICMP „Port Unreachable" üzenet, tehát mindkét esetben lehetséges reagálásra bírná a reflektor végpontokat. A használt portok tipikusan az „echo" (7) és a „chargen" (19) szolgáltatások.

Reflektív DNS támadás

Napjaink legveszélyesebb támadási módszere. A DNS szolgáltatás UDP csomagokat használ, mivel egy ilyen kérés általában néhány byte hosszúságú. A kéréshez képest a válasz már jelentősen nagyobb méretű lehet, így ez a két tulajdonság ideális eszközzé

---

[62] Az IP cím két részből tevődik össze: a hálózat azonosítójából és a hálózaton belül kiosztott végpont címből. Az IP címek hamisításakor a feladó saját azonosítója helyett egy tetszőlegesen választott másik címet illeszt a csomagba, így a későbbiekben nemhogy a feladó, de még a feladó hálózata sem azonosítható. Mivel a feladó mindenképpen a saját hálózatából küldi a hamis csomagokat, a hálózat útválasztóján (routeren) keresztülhalad. Az RFC 2827 előírja, hogy az ilyen útválasztók külső hálózatba csak a saját hálózatuk címtartományába tartozó feladójú csomagokat továbbíthatják. Ezáltal a támadó csak saját hálózatán belüli végpontcímet képes hamisítani.

[63] User Datagram Protocol: szállítási rétegben működő, összeköttetés-mentes protokoll, lényegében az IP kiegészítése a TCP által használt portcímekkel és integritásvédelmi megoldással (checksum).

teszi a reflektív DDoS támadásokhoz. Az UDP esetében viszonylag könnyen hamisítható egy csomag feladójának IP címe. Az áldozat IP címét elhelyezve a feladó IP cím mezőbe a válasz nem a csomagot ténylegesen elküldő támadóhoz, hanem az áldozathoz fog eljutni. A válasz általában jóval hosszabb a kérésnél, így a támadónak jóval kisebb sávszélességre van szüksége a küldéshez, mint az áldozatnak a fogadáshoz. Egy DNS „A” rekord lekéréséhez a következő 77 byte méretű kérésre van szükség:

```
0000  00 0c 6e a8 fd 4e 00 11  09 ac 14 ae 08 00 45 00   ..n..N.. ......E.
0010  00 3f 7f 14 00 00 80 11  38 46 c0 a8 01 02 c0 a8   .?..... 8F......
0020  01 01 1c 30 00 35 00 2b  ac e3 03 18 01 00 00 01   ...0.5.+ ........
0030  00 00 00 00 00 00 03 77  77 77 09 6d 69 63 72 6f   .......w ww.micro
0040  73 6f 66 74 03 63 6f 6d  00 00 01 00 01            soft.com .....
```

10. ábra DNS kérés (Wireshark programmal készítette a szerző)

A 77 byte kérésre válaszul a következő csomag érkezik:

```
0000  00 11 09 ac 14 ae 00 0c  6e a8 fd 4e 08 00 45 00   ........ n..N..E.
0010  01 a5 00 00 40 00 40 11  b5 f4 c0 a8 01 01 c0 a8   ....@.@. ........
0020  01 02 00 35 1c 30 01 91  e1 c7 03 18 81 80 00 01   ...5.0.. ........
0030  00 05 00 09 00 05 03 77  77 77 09 6d 69 63 72 6f   .......w ww.micro
0040  73 6f 66 74 03 63 6f 6d  00 00 01 00 01 c0 0c 00   soft.com ........
0050  05 00 01 00 00 0e 10 00  1a 06 74 6f 67 67 6c 65   ........ ..toggle
0060  03 77 77 77 02 6d 73 06  61 6b 61 64 6e 73 03 6e   .www.ms. akadns.n
0070  65 74 00 c0 2f 00 05 00  01 00 00 01 2c 00 04 01   et../... ....,...
0080  67 c0 36 c0 55 00 05 00  01 00 00 01 2c 00 06 03   g.6.U... ....,...
0090  6c 62 31 c0 36 c0 65 00  01 00 01 00 00 00 55 00   lb1.6.e. ......U.
00a0  04 cf 2e 13 fe c0 65 00  01 00 01 00 00 00 55 00   ......e. ......U.
00b0  04 cf 2e 13 be c0 3d 00  02 00 01 00 00 15 1b 00   ......=. ........
00c0  0f 02 7a 64 06 61 6b 61  64 6e 73 03 6f 72 67 00   ..zd.aka dns.org.
00d0  c0 3d 00 02 00 01 00 00  15 1b 00 07 04 65 75 72   .=...... .....eur
00e0  31 c0 3d c0 3d 00 02 00  01 00 00 15 1b 00 07 04   1.=.=... ........
00f0  75 73 65 33 c0 3d c0 3d  00 02 00 01 00 00 15 1b   use3.=.= ........
0100  00 07 04 75 73 65 34 c0  3d c0 3d 00 02 00 01 00   ...use4. =.=.....
0110  00 15 1b 00 07 04 75 73  77 32 c0 3d c0 3d 00 02   ......us w2.=.=..
0120  00 01 00 00 15 1b 00 08  05 61 73 69 61 39 c0 3d   ........ .asia9.=
0130  c0 3d 00 02 00 01 00 00  15 1b 00 05 02 7a 61 c0   .=...... .....za.
0140  9a c0 3d 00 02 00 01 00  00 15 1b 00 05 02 7a 62   ..=..... ......zb
0150  c0 9a c0 3d 00 02 00 01  00 00 15 1b 00 05 02 7a   ...=.... .......z
0160  63 c0 9a c1 12 00 01 00  01 00 00 3f 24 00 04 d5   c....... ...?$...
0170  fe cc c5 c1 23 00 01 00  01 00 00 3f 24 00 04 0c   ....#... ...?$...
0180  b7 7d 05 c1 34 00 01 00  01 00 00 3f 24 00 04 7c   .}..4... ...?$..|
0190  28 34 85 c0 97 00 01 00  01 00 00 3f 24 00 04 cc   (4...... ...?$...
01a0  02 b2 85 c0 fe 00 01 00  01 00 02 94 3a 00 04 dc   ........ ....:...
01b0  49 dc 04                                          I..
```

11. ábra DNS válasz (Wireshark programmal készítette a szerző)

A válasz mérete 435 byte lett, pedig ez nem is egy speciálisan felkészített DNS bejegyzésre vonatkozik. A példában a kérés és a válasz közti arány 1:5,65, vagyis majdnem hatszoros adatforgalom generálható. Külön problémát jelent, hogy a DNS szerverek csomagjai nem szűrhetők, mivel ez a hálózat működését veszélyeztetné. A fenti példában egy nyilvános DNS szerver által generált, hétköznapi válaszról van szó. Azonban lehetséges olyan DNS bejegyzéseket is készíteni, amelyekben a jelentős funkcióval nem rendelkező TXT rekord több ezer byte hosszú. Ezzel egy DNS válasz

mérete 10 kB-ra is növelhető, ami 1:200 arányú erősítést jelent, vagyis például egy 192 kbit/s feltöltési iránnyal rendelkező támadó (ami jelenleg egy teljesen átlagosnak tekinthető sebesség) 14 Mbit/s adatforgalmat képes generálni az áldozat irányába. Ebben segítségére a nem kellő körültekintéssel konfigurált rekurzív DNS szerverek vannak, amelyek elfogadnak és végrehajtanak lekérdezéseket más végpontok számára is. Az ilyen „open resolver” néven ismert szerverek száma több százezerre tehető.

Alkalmazási rétegben kivitelezett reflektív DDoS támadások

Az alkalmazási rétegben működő programokat is lehetséges reflektív módon túlterhelni, mindössze az „ártatlan” végpontokat kell rávenni, hogy a célponton futó alkalmazásnak küldjenek olyan mennyiségű kérést, aminek kiszolgálására a célpont erőforrásai elégtelenek. Nyilvános hálózatról elérhető egyik legnépszerűbb – és így a legtöbb helyen működő – szolgáltatás az elektronikus levelezés, így ennek támadása a legkifizetődőbb.

Email támadás

Az elektronikus leveleket továbbító SMTP (Simple Mail Transfer Protocol) egy egyszerű, párbeszédes módszert alkalmaz a levelek kézbesítésére, melyet az alábbi üzenetváltás mutat be:

```
HELO tamado
250 Hello 3e44bd93.adsl.enternet.hu [62.68.189.147], pleased to meet
you
MAIL FROM: bill.gates@microsoft.com
250 2.1.0 bill.gates@microsoft.com... Sender ok
RCPT TO: george.w.bush@whitehouse.gov
550 5.7.1 george.w.bush@whitehouse.gov... Relaying denied
RCPT TO: bill.clinton@kewl.hu
550 5.1.1 bill.clinton@kewl.hu... User unknown
```

A vastagított sorokban olvasható üzeneteket a kliens küldi, a levél címzettjét az „RCPT TO:” után adja meg a küldő. A címzett megadása után a levelezőszerver döntési helyzetbe kerül:

- azonnal ellenőrizze, hogy a címzett létezik-e, vagy
- átvegye a levelet, elhelyezze egy feldolgozási sorba, majd később ellenőrizze, hogy a levél kézbesíthető-e.

Az első lehetőség meglehetősen erőforrás igényes, hiszen a beérkező levél esetén, a szerver aktuális terheltségétől függetlenül azonnal el kell végezni az ellenőrzést. A második lehetőség a levél beérkezésekor kevesebb erőforrást igényel, viszont később, a várakozó sor feldolgozásakor a szabványnak megfelelően értesíteni kell a feladót arról, hogy levele kézbesíthetetlen.

A hagyományos email DDoS támadások ellen már léteznek hatásos technikák (Reverse DNS figyelés, feketelisták), azonban a reflexió elvét kihasználva megtámadható egy jól védett szerver is. Az ilyen támadás az olyan levelezőszervereket használja a célpont megtámadására, amelyek átveszik a levelet, majd egy későbbi fázisban ellenőrzik a címzett meglétét. A támadó hamisított feladói email címmel (a célpont címével) küld leveleket a szerveren nem létező email címre. A szerver ezeket átveszi, majd az értesítést a célpont számára küldi el, jelentős terhelést okozva.

Ha egy ilyen támadásra botneteket és nagyszámú reflexiós szervert használnak, a védekezés meglehetősen nehézzé válik. A levelező szerverek helyes és gondos konfigurálása mindenképpen csökkenti az ilyen akciók bekövetkezésének esélyeit, azonban az elektronikus levelezés gyengeségeit jól mutatja a rengeteg kéretlen levél is, amivel mindenki naponta szembesül.

2.8 DDoS támadások elleni védekezés módszerei

A DDoS támadások elleni védekezés első lépése a támadás észlelése. Tapasztalataim szerint ez nem mindig egyértelmű, mivel a megtámadott csak annyit tapasztal, hogy valami nincs rendben a rendszer működésével. A működési problémák, lelassulások az esetek döntő többségében nem külső támadásnak köszönhető: az informatikai rendszer valamely eleme elromlik, a kommunikációs csatornát biztosító szolgáltató hálózata lelassul, a belső vagy a külső hálózati elemek helytelen konfigurálása miatt romlik a teljesítmény. Az is előfordulhat, hogy a normálistól eltérő, de nem rosszindulatú érdeklődés okozza a problémát. 2006. november másodikán és 2007. október 30-án a Netrisk DDoS támadásról számolt be, éppen akkor, amikor elérhetővé tette kötelező biztosítás kalkulátorát. [88] Az akkori szabályozás szerint november 1. és 30. között volt lehetséges biztosítót váltani a gépjármű kötelező biztosítás kötéséhez, így – bár a cég hivatalosan nem ismerte be – valószínűleg csak a felfokozott érdeklődéshez képest alulméretezett kapacitású volt a biztosítási alkusz cég informatikai rendszere.

A támadás tényének felismerése tehát az első lépés, ettől a ponttól kezdve már el lehet kezdeni az ilyen esetekben szokásos eljárásokat. A védekezés kezdeteként meg kell

határozni a támadás módszerét, ugyanis csak ennek birtokában lehet a lehetséges válaszlépéseket megtenni. Ezzel bővebben az értekezés következő fejezetében foglalkozom, ahol összegyűjtöttem és kategorizáltam a leggyakoribb eljárásokat.
A már megindult DDoS támadások elleni védekezés két alapvető módszerrel lehetséges: preventív vagy reaktív módon. [67]
A **preventív módszer** arra épül, hogy a célpont igyekszik megelőzni vagy a támadás bekövetkeztét, vagy pedig próbálja fenntartani a szolgáltatás kiesését a támadás ideje alatt. A támadás bekövetkeztét természetesen sosem lehet meggátolni, csak a potenciális gyenge pontokat lehet megerősíteni, vagy ismert sérülékenységeket megszüntetni. Ez a lehetőség főként a DoS támadások ellen lehet hatékony, mivel ezek közül nagyon sok épül valamilyen rendszerhiba kihasználására. A DDoS akciók ezzel szemben legtöbbször a „nyers erőszak" módszerét követik, és akkora terhelést jelentenek a célpontnak, ami nem igényli rendszerhiba kihasználását. Ekkor a védelem erőforrás kiosztási vagy erőforrás sokszorozó mechanizmus segítségével valósítható meg. Az erőforrás kiosztási mechanizmus a meglevő erőforrásokat próbálja a tényleges felhasználók számára allokálni, a támadók elöl pedig elzárni. Ebben az esetben a nagy problémát a jogosult felhasználók azonosítása jelenti, ami ugyan megvalósítható az alkalmazások szintjén, azonban a számítógépes hálózati forgalomban már komoly akadályai vannak. Míg az alkalmazások esetében a bonyolult személyiség lopások (identity theft) segítségével képesek a támadók kijátszani a védelmet, addig a hálózati eszközök szintjén sokkal egyszerűbb dolguk van. Napjaink internet hálózata egyszerű csomagszerkezetet használ, aminek minden eleme hamisítható. Azok a DDoS támadások, amelyek a hálózati erőforrások teljes mértékű lefoglalására törekednek, nem védhetők ki az erőforrás kiosztási módszerekkel. Az okozott kár csökkenthető, ha a megfelelő óvintézkedések megtétele megtörténik. A [89] forrás által javasolt módszerek a következők:

- hamisított feladói címmel rendelkező csomagok szűrése (ingress és egress filtering);
- minden olyan hálózati szolgáltatás letiltása, amelyek használata külső hálózatok irányából nem szükségszerű;
- redundás informatikai eszközök beszerzése.

Ezek a módszerek azonban csak bizonyos – az idő múlásával egyre túlhaladottabb – karakterisztikájú támadások ellen hatásosak.

A másik módszer - az erőforrás sokszorozó mechanizmus - a támadások idejére többlet erőforrásokat foglal, amellyel optimális esetben képes fenntartani az üzletmenetet. Ez sem minden esetben nyújt megbízható védelmet, ugyanis a többlet erőforrások beszerzése anyagilag komoly terhet róhat a potenciális célpontra, ráadásul a támadó is képes bevonni újabb eszközöket a támadásba.

A **reaktív módszer** alkalmazásakor a célpont azonosítja a támadás elemeit, majd megfelelő módon reagálva képes azt megállítani. Ehhez pontosan kell ismerni a támadás módszerét, a támadásban részt vevő végpontokat, illetve szükséges olyan eszközökkel rendelkeznie, amelyekkel ezek a végpontok semlegesíthetők.

A két módszer együttesen is alkalmazható, sőt ez biztosíthatja a legerősebb védelmet. Kiváló példa erre a 2003-ban bekövetkezett, a BetCris nevű online bukméker iroda elleni DDoS támadás esete. 2003 októberében ismeretlenek elektronikus levélben pénzt követeltek a Costa Ricában működő cégtől, nem fizetés esetére pedig a szerverek használhatatlanná tételét helyezték kilátásba. Mint később kiderült, a BetCris nem volt egyedül, sok más fogadóirodát is megcéloztak, másik nagy áldozatuk a Canbet Sports Bookmakers nevű fogadóiroda volt. Akadtak olyanok, akik fizettek, mások – mint a BetCris és a CanBet is – megtagadták a néhány ezer dolláros „védelmi pénz” kifizetését. Erre válaszul a támadók túlterhelték a cégek szervereit DDoS módszerek használatával. A CanBet vesztesége ez idő alatt körülbelül 200 000$ volt, a BetCris pedig napi 100 000$ bevételkiesést szenvedett el. A két hasonló eset közül a BetCris az érdekesebb, ők ugyanis felvették a harcot, és bár összességében 1 millió dollárjukba került, de végül sikerült legyőzniük a támadókat. A zsaroló levél beérkezését követően úgy gondolták, hogy saját erőből is képesek túlélni a támadást, azonban a DDoS akció olyan erős volt, hogy nem csak a szervereik, hanem a szerverek elhelyezését biztosító szolgáltató hálózata is működésképtelenné vált. Ekkor egy külső szakértő segítségével kiépítettek egy proxy rendszert az USA-beli Phoenix városában, amely a feltételezéseik szerint elég erőforrással rendelkezett ahhoz, hogy túlélje a támadás által generált hálózati forgalmat. Mint kiderült, csúnyán alulbecsülték a támadó botnet méretét, az események során a rekord adatátviteli sebesség elérte a 3Gbit/s-t is. A forgalom szűréséhez szükséges rendszer kapacitását folyamatosan bővítve, végül két hét csatározás után a támadások megszűntek, azonban a veszély nem csillapodott, hiszen bármikor felbukkanhatott egy újabb próbálkozó, egy még hatalmasabb zombi hálózattal. Ezért saját erőből nekiálltak a támadók után nyomozni, és hónapokon át tartó próbálkozás után sikerült is azonosítaniuk egy orosz fiatalembert. [90]

A CanBet feljelentést tett, a BetCris pedig átadta nyomozásának eredményeit a brit NHTCU-nak,[64] amely az orosz hatóságokkal együttműködve felgöngyölített egy 10 tagú lettországi bandát, illetve három orosz fiatalembert, akik a technikai hátteret biztosították a zsarolásokhoz. [91] A bűntett bizonyítási eljárása után 2006 októberében mindhárman fejenként 8 év börtönbüntetést kaptak. [92]

A fenti eset jól mutatja, hogy mekkora veszélyt jelenthet egy kisebb cég számára a túlterheléses támadás, szélsőséges esetben akár a cég csődjét is okozhatja. Nagyméretű botnetekkel akár több hétig is folyamatosan működésképtelenné tehető egy cég teljes internetes szolgáltatási képessége, így sokan inkább engednek a zsarolásnak. Fontosnak tartom kiemelni azt is, hogy a DDoS támadások ellen csak a fenyegetés megszüntetése az egyedüli megbízható módszer, ugyanis az erőforrás sokszorozó vagy kiosztó módszerek bármikor hatástalaníthatók, ha a támadó megfelelő erőforrásokkal rendelkezik. Ennek illusztrálására vizsgáljuk meg a következő példát: a támadó a célpont adatátviteli kapcsolatának túlterhelésére törekszik. Céljai eléréséhez olyan botnetet használ, amelynek tagjai szélessávú internet hozzáféréssel rendelkeznek, 128 kbit/s átlagos feltöltési sávszélességgel. Ez az érték jelenleg egy nagyon óvatos becslés, a technológia fejlődési ütemével illetve az újabb – például optikai – hozzáférési hálózatok kialakulásával és térnyerésével számolva a közeli jövőben akár nagyságrendi ugrás is elképzelhető. A sávszélesség túlterheléséhez szükséges kliensszámokat táblázatban ábrázoltam különböző célpontok esetén, az alkalmazott támadási módszerek függvényében. :

3. táblázat Adathálózati DDoS támadások sikeres kivitelezéséhez szükséges kliensszámok

Támadási módszer / Célpont	TCP SYN FLOOD (1:1 erősítés)	Reflektív TCP SYN FLOOD (4:1 erősítés)	Reflektív DNS (6:1 erősítés)
Bérelt vonal (2 Mbit/s)	16	4	3
Bérelt vonal (8 Mbit/s)	64	16	11
Átlagos internetes szerver (100 Mbit/s)	781	195	131
Gyors internetes szerver (1 GB/s)	7812	1953	1303

[64] National High-Tech Crime Unit.

Látható, hogy a megadott – nem túl szigorú – feltételeknek megfelelve, a jelenleg kifejezetten gyorsnak tekinthető 1 GB/s sávszélesség és erősítetlen DDoS támadási módszer mellett is kevesebb, mint 8000 tagból álló botnet szükséges a sikeres támadás végrehajtásához. A célpont lehetőségei a preventív módszerek alkalmazásával ekkor a rosszindulatú adatfolyam szűrésére vagy pedig saját sávszélességének növelésére korlátozódnak. Az adatfolyam szűrése nem minden esetben valósítható meg – a reflektív DNS támadás esetén ez saját működésének megnehezítését vagy lehetetlenné tételét jelenti. Az erőforrások megnövelése egyrészt időigényes, másrészt költségvonzatai is vannak. A támadónak ezzel szemben több lehetősége is van a túlterhelés fenntartására:

- Megnöveli a támadásban részt vevő kliensek számát. A botnetek átlagos mérete pontosan nem ismert, de derítettek már fel több százezer tagból állókat is, így a botnet tulajdonosa szabadon dönthet a támadásban részt vevő elemek számáról.
- Olyan klienseket válogat be az akcióba, amelyek erőforrásai az átlag felettiek.
- Másik, hatékonyabb DDoS technikát választ. A táblázatban szereplő reflektív DNS támadás erősítési értéke átlagos DNS rekordméretre vonatkozik, de elképzelhetők olyan speciális DNS rekordok is, amelyek ennél jóval hatékonyabbak (például extrém hosszú TXT bejegyzésekkel).

A reaktív módszer időnként nehézkesebb, de mindenképpen célravezetőbb. A BetCris elleni támadás során alkalmazott erőforrás sokszorozó mechanizmus ugyan csökkentette a veszteségeket, de a tetemes bevételkiesés azt bizonyítja, hogy minden ilyen típusú védelem megtörhető, ha a támadó rendelkezik a kellő méretű támadó botnettel. A támadások csak a támadó felkutatása és semlegesítése után szűntek meg.

2.9 Következtetések

Célkitűzéseimnek megfelelően megvizsgáltam a DoS és DDoS támadásokban alkalmazott támadási módszereket, és az irodalomban fellelhető rendszertani besorolásokat. Mivel úgy ítéltem meg, hogy az irodalomban fellelhető ilyen taxonómiák nem fedik le teljesen az általam elvárt követelményeket, ezért saját osztályozási módszert dolgoztam ki. A túlterheléses támadásokat három osztályba soroltam, majd az ISO/OSI szabvány által ajánlott hálózati rétegek alapján kategorizáltam őket. A támadást kivitelező adatfolyam keletkezési illetve továbbítási módszere szerint a következő háromféle osztályba sorolást javasoltam:

- DoS (kevés számú támadó végpontból kezdeményezett adatfolyam);
- DDoS (egyidejűleg nagyszámú végpontból kezdeményezett támadó adatfolyam);
- Reflektív DDoS (erősítőként használt „ártatlan” végpontok felhasználásával végrehajtott támadás).

Mindegyik osztályon belül háromféle megcélzott réteget különítettem el:

- Adatkapcsolati;
- Hálózati;
- Alkalmazási.

Az így kialakított kilenc alosztályról megállapítottam, hogy a támadások gyakoriságának alakulása arra mutat, hogy a leginkább valószínűsíthető támadási módszerek a DDoS és a reflektív DDoS, amelyek a hálózati réteget célozzák, így a védekezést erre célszerű optimalizálni.
Rámutattam, hogy a hálózati rétegben kivitelezett reflektív DDoS támadás jelenti a legnagyobb veszélyforrást, mivel a támadók ebben az esetben mindenki által használt, és emiatt nehezen szűrhető végpontok segítségével képesek támadást végrehajtani. Gyakorlati példán keresztül bemutattam, hogy az így előállított rosszindulatú adatfolyam sokszorosa lehet az egyszerű DDoS támadásoknak, emiatt kisebb méretű botnetek ellen is sokkal nehezebb a védekezés.

3. FEJEZET
BOTNETEK

Kutatásaim során megállapítottam, hogy az informatikai infrastruktúrák működésében komoly gondokat, és így jelentős anyagi kárt is képesek okozni a túlterheléses támadások. Bizonyítottam, hogy az ilyen támadások ellen hatékonyan csak reaktív módon, a fenyegetés megszüntetésével lehet fellépni. A támadó végpont az esetek túlnyomó többségében egy fertőzött számítógép, ezért az információs infrastruktúrák védelmének erősítéséhez szükségesnek tartottam az ilyen számítógépek működésének megismerését. A nagyszámú fertőzött végpont akkor válik igazán veszélyessé, ha egy központi irányítás alá kerül, az ilyen hálózatokat a szakirodalom „botnet" néven ismeri. Jelenleg a legtöbb túlterheléses DDoS támadást ilyen botnetek hajtanak végre, ezért fontosnak tartottam ezek megismerését. Feltételeztem, hogy a botnetek életciklusa jól meghatározható, a küzdelem ellenük ezért mindig az adott állapotnak megfelelő módszerrel lehetséges.

Ebben a fejezetben bemutatom a botnetek működésének jellemzőt, kialakulásuk történetét, felhasználási területeket. Ez utóbbit azért tartom fontosnak, mivel ezek a tevékenységek biztosíthatnak lehetőséget a botnetet alkotó fertőzött számítógépek felkutatására. Szintén a felkutatás lehetősége miatt fontos az architektúra, a fertőzött gépek közötti hierarchia megismerése is, mivel az irányítás lehetőségének megvonása a támadótól hatásos megoldás lehet. A technológia fejlődésével párhuzamosan új eszközöket alkalmazó megoldások is létrejöhetnek, ezért megvizsgáltam más intelligens eszközök veszélyeztetettségét is.

3.1 Párhuzamos, elosztott rendszerek

A számítástechnikában régről ismert fogalom az „elosztott rendszer" (distributed system), amelyben a feladatot nem egyetlen számítógép végzi el, hanem a rendszert alkotó – egymástól akár nagy távolságban lévő - számítógépek párhuzamosan, egy időben dolgoznak, a feladatot felosztva egymás között. Az ilyen rendszerek sokkal nagyobb teljesítményre lehetnek képesek, mint egyetlen – bármekkora számítási kapacitású – számítógép, hiszen az alkotóelemek számát elméletileg nem korlátozza a befoglaló épület mérete, a tápáramellátás nehézségei, a hűtés és egyéb paraméterek. Van azonban egy nagy hátrányuk: nem minden feladat osztható szét egymástól független

részfeladatokra, így az alkalmazási területük erősen korlátozott. Emellett a végrehajtás ütemezése is bonyolultabb, mivel a rendszer elemeinek működését egymáshoz kell szinkronizálni, a végpontok által elvégzett feladat eredményét be kell gyűjteni, az újabb részfeladatokat ki kell osztani.

Az internet terjedésével egyre több számítógép kapcsolódik össze egymással, az egyes számítógépek teljesítményének és a kapcsolódó kommunikációs hálózatok sávszélességének növekedésével hatalmas számítási kapacitás keletkezett, amely felhasználása sokak figyelmét felkeltette. Vannak pozitív céllal indult kezdeményezések is, de természetesen az árnyékos oldal képviselői is komoly potenciált sejtenek a számítógépek összekapcsolásával létrejövő hálózatokban.

Az olyan – a felhasználó tudta nélkül megfertőzött - számítógépeket, amelyek távolról észrevétlenül irányíthatók, a számítógépes szleng „zombi" néven emlegeti. Másik elnevezésük a robot szóból származtatott „bot", a több bot összekapcsolásával keletkezett hálózatot pedig botnetnek nevezik. A kialakított botneteket előszeretettel használják túlterheléses támadások indítására és egyéb célokra is, ezek összefoglalója ebben a fejezetben található. Napjainkra a botnetek tekinthetők az információs bűnözés legfontosabb eszközeinek, aminek oka a segítségükkel elérhető hatalmas mennyiségű számítástechnikai erőforrás (számítási kapacitás, adatátviteli sebesség, felhasználói adatok sokasága). [93]

3.2 A botnetek működése, életciklusa

Egy botnet általában négy nagy egységet tartalmaz:

- A botnet tulajdonosa, aki az irányítást végzi, kiosztja a feladatot a fertőzött számítógépeknek. Az irányító személy vagy személyek „botherder"[65] vagy „botmaster" néven ismertek.
- A botnet tagjai, vagyis a fertőzött számítógépek.
- A botmaster és a botnet közti kapcsolatot biztosító, az utasításokat a botnethez eljuttató kommunikációs útvonal, amelyet szokás Command&Control (C2) csatornának is nevezni.
- Drop server, a botnet által gyűjtött adatok tárolására szolgáló tároló hely, amelyhez a botnet tagjai és a botmaster is hozzáfér.

[65] A „herder", magyarul „pásztor" egy szellemes hasonlat, ami arra utal, hogy a botnetet is kell terelgetnie valakinek.

A botmaster kétféleképpen juthat egy működő botnethez: saját maga kezd el felépíteni egyet, vagy elrabol egy már létrejöttet. A botnetek életciklusa rövid, néhány hónapnál tovább általában nem működőképesek. Egy botnet életciklusa az alábbi fázisokból áll: [94]

Terjedési fázis

A botnet szervezője igyekszik minél több számítógépre telepíteni a rosszindulatú programot, vagy malware-t. Ehhez változatos technikákat használ fel, kéretlen levél csatolásaként küldi, a böngészőprogramok biztonsági réseit kihasználva fertőző kódokat juttat be weboldalakra vagy akár az operációs rendszerek hibáit kihasználva, automatikusan telepíti fel. Általában ez a fázis csak egy letöltőprogramot (downloader) telepít, amely egy előre meghatározott helyről képes letölteni a tényleges, teljes funkcionalitású kliensprogramot.[66]

Fertőzési fázis

Ebben a fázisban történik meg a tényleges botnet kliens telepítése és a felhasználó – meg természetesen a vírusirtó programok – előli elrejtése. Ehhez ugyanazokat a módszereket használja, mint a vírusok. A két legnépszerűbb eljárás a polimorfizmus (a programkód bizonyos részeinek a detektáló mechanizmusok előli elrejtése titkosítással), vagy a rootkitting (rendszeradminisztrációs jogokkal rendelkező program indítása már a rendszer betöltésének korai szakaszában). A fertőzést úgy kell végrehajtani, hogy a kliensprogram működése később is rejtve maradjon, ezzel is meghosszabbítva a bot működési idejét.

Vezérlő (C2) csatorna kiépítése, csatlakozás

A fertőzött számítógépek a C2 csatorna használatával csatlakoznak a botnethez. A központi vezérlés segítségével a botmaster egyszerre képes a csatlakozott számítógépeket vezérelni, részükre feladatot adni. A C2 csatorna kialakításánál fontos szempont az, hogy a kommunikáció nehezen legyen felderíthető, ez ismét a botnet túlélési idejét hosszabbítja meg.

Támadó fázis

Ez a végső fázis, a botnet aktív működésének ideje. A támadás lehet tényleges támadás (DoS vagy DDoS), de akár csak valamilyen „békeidős” tevékenység is. Ez az a fázis, ahol a legkönnyebben észlelhetők a botnetek, és az észlelés után a C2 csatorna tiltásával működésük beszüntethető.

---

[66] Az ilyen, utólag letöltött programot „szállítmánynak” (payload) nevezik.

3.3 Botnetek története

Tudományos céllal indult a SETI@Home project, amely idegen, értelmes lények nyomainak felkutatására indult. A SETI egy betűszó, a „Search for Extra Terrestrial Intelligence” szavak kezdőbetűjéből keletkezett, és a Berkeley Egyetem felügyeli a kutatást. A több száz rádiótávcső naponta körülbelül 40 GB adatmennyiséget szolgáltat, amely elemzéséhez szuperszámítógép teljesítmény szükséges. Ezt az adathalmazt a rendszerbe interneten kapcsolódó körülbelül 3 millió számítógép dolgozza fel, amikor a tulajdonos éppen nem használja másra. Megvalósítása egy képernyővédőként történt, néhány perc felhasználói inaktivitás után bekapcsol, és a SETI@Home project számára végez munkát. A tervek szerint a svájci CERN kutatóintézet által üzemeltetett részecskegyorsító és ütköztető berendezés által szolgáltatott rengeteg adat feldolgozását is ilyen hatalmas méretű elosztott számítógépes rendszer fogja végezni.
Ezek a projektek természetesen a felhasználók tudtával és beleegyezésével használják a kihasználatlan erőforrásokat, azonban van egy másik, kevésbé legális módszer is. Az elosztott rendszerek kliensprogramjai telepíthetők a felhasználók tudta és beleegyezése nélkül is, az alapokat a 90-es évek végének vírusai már lefektették.
Ha osztályozni szeretnénk a rosszindulatú alkalmazásokat, akkor az osztályozás két fő paraméter alapján történhet: fertőzési módszer vagy a szállított kód célja szerint.
A fertőzési módszer szerint egy rosszindulatú kód lehet:

- Passzív, valamilyen hordozó, „vírusgazda” által végzett fertőzés. Az ilyen kódokra előszeretettel használják a „vírus” nevet, mivel egy fertőzött számítógép további számítógépeket képes megfertőzni. A terjedést végrehajtó kódot eleinte állományokba, később elektronikus levelekbe rejtve juttatják az áldozathoz, annak „immunitását” pedig valamilyen trükkel igyekeznek kikerülni, magukat hasznos tartalomnak álcázva.
- Aktív, amely esetben a károkozó kód saját maga képes az áldozatot megfertőzni. Ehhez általában a célpont rendszerében található programozási hibát használja ki, amely segítségével a távoli számítógép rávehető a támadó által küldött programkód végrehajtására. Az ilyen típusú programok neve a „féreg”, ami utal arra is, hogy ezek jóval fejlettebb mechanizmusok, mint a vírusok.

Kezdetben a rosszindulatú kódok célja csupán a károkozás volt, a fertőzéssel szállított tartalom - „payload” – általában állományok törlését, megváltoztatását végezte el a megfelelő, előre programozott feltételek teljesülése esetén. Később megjelentek a

kifinomultabb eljárások, amely segítségével az áldozat számítógépének vezérlése a támadó számára elérhetővé vált, így teljes ellenőrzése alá tudta azt vonni. Mivel ez egy hátsó ajtót nyitott a számítógépen, ráadásul magát ártalmatlan alkalmazásnak álcázta, trójai falónak is kezdték nevezni, a görögök által Trója ostrománál használt trükkre emlékezve.

A kezdeti próbálkozások (Back Orifice 2000 és hack-a-tack) hamar megmutatták az ilyen alkalmazások erejét, azonban komoly célokra még nem voltak használhatók, mivel a fertőzött gépeket egyenként kellett irányítani. A hatékony felhasználás érdekében ki kellett alakítani egy olyan csatornát, amellyel a nagy mennyiségű fertőzött számítógép menedzselhető, számukra feladat kioszthatói, illetve a keletkezett eredmények begyűjthetők.

Az ilyen, fejlettebb backdoor programokat a „robot" szó egyszerűsítésével létrehozott „bot" kifejezéssel szokták emlegetni, a belőlük szervezett elosztott rendszernek pedig „botnet" az elfogadott megnevezése.

A bot alkalmazások fejlődése során a centralizált architektúra volt a kiindulási alap, a sokak által az első, ilyen típusú alkalmazásnak tekintett, 1993-as EggDrop Bot nevű program az Internet népszerű csevegő protokollját, az IRC-t[67] használta, amely lényegét tekintve egy központi szerverre kapcsolódó kliensekből áll. A bot funkcionalitása is elsősorban az IRC-ben elvégezhető műveleteket segítette, nem kifejezetten nevezhető rosszindulatúnak. [95]

A kezdeti trójai faló programok egy háttérben futó önálló programszálat (process) indítottak el a gazdagépen, amely egy TCP portot figyelve várta a rá kapcsolódó távoli kéréseket. A támadónak emiatt nem volt egyszerű dolog a fertőzött gépet megtalálnia, lényegében vakon kellett a teljes Interneten vizsgálódnia, és keresnie áldozatait. Ezeket a keresési próbálkozásokat az akkoriban divatba jött személyes tűzfalak nagy hatékonysággal voltak képesek megakadályozni.

A következő mérföldkő az 1999-ben megjelent a SubSeven trójai faló program 2.1-es változata volt, amely egy IRC szerverre jelentkezett be, és így a fertőzést okozó elkövető könnyen megtalálhatta. Innen datálható a fejlett C2 csatorna és a botnetek létrejötte is.

Az egy évvel később terjedő GT Bot már a botnet egyesített erőforrásait képes volt támadási célokra is felhasználni, segítségével DDoS támadásokat lehetett indítani. A

[67] IRC: Internet Relay Chat.

későbbi, nagyméretű botneteket létrehozni képes programok is előszeretettel használták az IRC protokollt C2 csatornaként, amelynek oka a széles elterjedtségben és egyszerű megvalósíthatóságban keresendő.

2002-ben egy „sd" fedőnevű, orosz programozó nyilvánosságra hozta egy bot kliens program forráskódját, aminek segítségével mindenki számára lehetővé vált a saját igényeinek megfelelő programkód kialakítása. Az SDBot más programozókat is arra késztetett, hogy hasonló módon készítsék el munkáikat, sőt a nem sokkal később megjelenő AgoBot már a modularitást is biztosította. A kód egyes részei nem egyetlen, monolitikus kódként érkeztek, hanem egymást aktiváló modulokként, amelyeket a készítő testre is szabhatott. Az első modul csak az IRC C2 csatornát figyelő mechanizmust és a távoli hozzáférést biztosító funkcionalitást tartalmazta, majd letöltötte és aktiválta a következő modult, amelynek feladata a számítógépen futó antivírus folyamatok leállítása volt. Ez a második fokozat töltötte le és aktivizálta a harmadik modult, amely a tényleges feladatot végrehajtó kódrészlet volt (és emellett korlátozta az áldozat lehetőségeit a fertőzés eltávolítására, például az antivírus cégek honlapjainak letiltásával). A saját, testre szabott botkliens készítéséhez elegendő volt a kettes és hármas modulokat módosítani, így nem kellett különösebb programozói készség a használatához. Bár az AgoBot még IRC C2 csatornát használt (centralizált architektúrájú volt), de mindemellett nyitott egy hátsó ajtót a fertőzött gépen és terjedéséhez már felhasználta az egyenrangú, P2P[68] hálózatok lehetőségeit, a korai fájlcserélő rendszerek (például Kazaa, Grokster) segítségével.

2004-ben jelent meg PolyBot, az első polimorfikus, saját kódját változtatni képes bot kliens, amely minden fertőzéskor átalakította a belső, fertőzést okozó programrészeket, így csökkentve a vírusirtó programok hatékonyságát.

Az egyre fejlettebb bot alkalmazások megjelenése után eljött az újgenerációs botnet ideje. 2007 elején kezdtek olyan elektronikus levelek terjedni, amelyek európai viharok halálos áldozatairól szóló híreket tartalmaztak, a csatolt állomány viszont egy rosszindulatú kódot telepített a számítógépre. A hordozó levelek tárgyáról „Storm" névre keresztelt bot kliens minden korábbinál veszélyesebb volt: a szerveződő botnet tagjai az eDonkey nevű P2P fájlcserélő protokollját használták a C2 kommunikációra, ráadásul SSL[69] titkosítással. A kliensek képesek voltak frissíteni saját kódjukat, a botnet pedig ezeket az állományokat aktív védelemmel is ellátta. Ha valaki a frissítéseket nem

[68] P2P: Peer to Peer.
[69] SSL: Secure Socket Layer.

megfelelő viselkedési módot használva töltötte le, akkor a botnet egy összehangolt DDoS támadást intézett a letöltő ellen. A Storm botnet méretéről nagyon ellentmondó adatok vannak, egyes források néhány ezer, mások néhány millió áldozatról tudnak. A pontos szám a titkosított kommunikáció miatt nem határozható meg pontosan.

A botnetek terjedése komoly fenyegetést jelent a modern társadalom számára. A hétköznapi élet egyre több funkciója bonyolítható le az interneten, ami nagyobb kényelmet, de egyben nagyobb függőséget is jelent. Mióta a szervezett alvilág is felfigyelt az ingyen megszerezhető számítógépes kapacitásokban rejlő lehetőségekre, azóta minden felhasználó szenved a különböző témájú kéretlen levelek áradatától. Egyre inkább előtérbe kerülnek a katonai és nemzetbiztonsági kérdések is, a kellő kapacitású botnet segítségével összehangolt támadások indíthatók az olyan infrastruktúra ellen, amely rendelkezik internetes elérhetőséggel. Az elmúlt néhány év tapasztalatai arra utalnak, hogy a fegyveres összecsapások kísérői lettek az interneten végrehajtott DDoS támadások is.

3.4 A botnetek alkalmazási területei

Ha egyszer a botnet irányítójának sikerült létrehoznia egy nagymennyiségű végpontból álló botnetet, akkor természetesen azt használni is szándékozik valamire. A hackerek[70] egymás ellen vívott virtuális harcán felül néhány éve bűnözői körök is megjelentek a botnetek körül, komoly üzletet szimatolva az ilyen hálózatok által képviselt potenciálban. Az információs infrastruktúra fejlődésével a militáns szervezetek is újfajta fegyvert láttak a számítógépes hálózatokban, amely nem igényel különösebben nagy anyagi ráfordítást, mégis komoly károkat képes okozni a szemben álló félnek.

Néhány alkalmazási terület:

- Adatlopás;
- Elosztott túlterheléses támadás (DDoS);
- Kéretlen levélküldés;
- Reklám manipulációk;
- Gépesített jelszófeltörés.

[70] A hacker elnevezést előszeretettel aggatják a rosszindulatú számítógépes támadásokat elkövetőire. Az érintettek szerint a hacker lét nem egyenlő a betörésekkel, kizárólag a technológiai fejlődést szolgálja. Sok hacker száll csatába a rosszindulatú programokat fejlesztőkkel szemben is. A betöréseket végrehajtókra talán szerencsésebb elnevezés a cracker szó.

Adatlopás

Régi közhely, de igaz: az információ érték. A megfertőzött és uralom alá vont számítógépeken rengeteg olyan személyes adat található, amit a tolvajok könnyen készpénzre is tudnak váltani. Ha eltekintünk a triviális lehetőségektől (hitelkártya adatainak megszerzése, internetes banki hozzáférés adatainak megszerzése), akkor is rengeteg módon profitálhat a támadó az adatokból. Az áldozat gépére telepített keylogger alkalmazás (ami a leütött billentyűket tárolja, majd a támadó számára elküldi) rengeteg hozzáférési adatot képes begyűjteni. Ezek a hozzáférési jogosultságok aztán akár direkt, akár indirekt módon készpénzzé tehetők.

2006-ban komoly csalássorozatot követtek el az online árveréseket bonyolító eBay.com weboldalon. Az eBay regisztrált felhasználói aukcióra bocsáthatnak különböző tárgyakat, amire más felhasználók licitálnak, majd a győztes megvásárolja a kikiáltott tárgyat. Természetesen a vásárlónak óvatosan kell eljárnia, mivel az interneten, felhasználói nevek mögé bújva zajlanak a tranzakciók. A megbízhatóság ellenőrzésére az eBay a „feedback score" nevű mérőszámot rendeli minden felhasználójához. Ez az érték a vásárlók és az eladók visszajelzései alapján generálódik egy algoritmus alapján, és két részből áll: a felhasználó tranzakcióinak számából és a visszajelzések pozitív vagy negatív voltából képzett százalékos értékből. Minél több tranzakcióval rendelkezik egy eladó, és minél nagyobb a vevőelégedettségi mutatója, annál valószínűbb, hogy a megvásárolt termék a hirdetett minőségben el is jut a vásárlóhoz.

Ezzel éltek vissza a támadók: bot segítségével regisztráltak fiktív felhasználókat, majd 1 centes aukciókat hirdettek meg a nevükben, amiket szintén botok segítségével meg is vásároltak (lehetőség van azonnali áron elvinni a terméket), majd automatikusan pozitív visszajelzéseket adtak egymásról. A tapasztalt eBay felhasználók a 100 tranzakcióval rendelkező, 99% feletti pozitív visszajelzéssel rendelkező eladókat általában megbízhatónak tekintik. Amint a bot elérte ezt az értéket, aukcióra bocsátottak népszerű berendezéseket (általában MP3 lejátszókat) kedvező áron. A nyertes vásárló kifizette az ellenértéket, azonban sosem kapta meg a terméket. Az eBay természetesen letiltotta ezeket az eladókat, azonban a botnet segítségével néhány dollárból pillanatok alatt egy új azonosságot építhettek. Az eBay regisztrációhoz elektronikus levélcím is szükséges, azonban a begyűjtött bejelentkezési adatok segítségével tetszőleges számú postafiók állt a csalók rendelkezésére. [96]

Az adatlopások veszélye véleményem szerint túlmutat az adatbiztonság sérülésének illetve az eltulajdonított adatok értékesítéséből származó közvetlen károkon. A megszerzett adatok közvetett felhasználása jóval súlyosabb problémát jelenthet, ha azt egyéb támadási módszerek kiindulásaként alkalmazzák. Egy kiszivárgott tervezési dokumentáció sok év munkáját teheti semmissé, egy kulcspozícióban levő alkalmazott elleni kompromittáló adatok megszerzésével és zsarolásra használásával olyan információk is megszerezhetők, amelyek egyébként más módszerrel nem lennének hozzáférhetők.

DDoS támadások nem katonai alkalmazása

A DDoS támadás során a támadó egy időben nagyszámú internetes végpontot felhasználva olyan mennyiségű adatot küld az áldozat számára, amit az nem képes kezelni, így működésképtelenné válik. A működésképtelenség nem minden esetben jelent tényleges leállást, a funkcionális működésképtelenséghez elegendő a nagymértékű lassulás, a válaszidő elfogadhatatlan nagyságúra növekedése is. Mivel egy időben rengeteg végpont vesz részt a támadásban, hagyományos eszközökkel – csomagszűrés, támadó végpontok forgalmának letiltása - szinte lehetetlen a védekezés. Egy hatásos támadás lebonyolításához nem is szükséges hatalmas méretű botnet. A jelenlegi hálózati sávszélességek mellett néhány száz tagból álló botnet a teljes, gépenként rendelkezésre álló feltöltési sebességet kihasználva képes egy 100 Mbit/s sávszélességű hálózatot túlterhelni. A néhány száz tag jelentéktelennek tekinthető méretet jelent, figyelembe véve azt, hogy például a Storm botnet több millió tagból áll.
Napjainkban az ilyen jellegű támadások szinte kizárólag botnetek művei, veszélyességüket tekintve pedig talán az első számú veszélyforrás az internet számára. A legtöbb DDoS támadást nem a pénzszerzés motiválja, de az alvilág számára is jövedelmező üzletág lehet egy támadásokat végrehajtani képes hálózat. Felmerül persze a kérdés, hogy egy ilyen támadás milyen módon váltható át valódi pénzre, ki hajlandó fizetni érte? Néhány ismertebb módszer:

- Konkurencia működésének ellehetetlenítése;
- Zsarolás;
- Támadó kapacitás bérbeadása.

Konkurencia működésének ellehetetlenítése

Az elektronikus – és azon belül is az internetes - kereskedelem egyre nagyobb forgalmat bonyolít le. Az internetes tartalomszolgáltatás reklámokból képződő árbevételében már megközelítette, sőt el is hagyta a rádiós piacét. [97] Az internetes piac szereplői kiélezett versenyben próbálják részesedésüket megőrizni vagy mások kárára tovább növelni. Az ügyfelekért vívott harcban komoly, pénzben is mérhető hátrányt jelenthet egy hosszabb időre működésképtelenné váló weboldal. A hosszabb kiesést a konkurencia saját javára fordíthatja. Egy DDoS támadás mögött álló megrendelőt még az elkövetőnél is sokkal nehezebb azonosítani.

Zsarolás

Az előző pontban felsorolt veszélyek ellen nem könnyű védekezni, a komolyabb támadásokat is sikeresen kiálló informatikai háttér megteremtése nem kevés pénzbe kerül. Egy támadással megfenyegetett cég két dolgot tehet: vagy megpróbálja túlélni a támadást a megfelelő óvintézkedések megtétele mellett, vagy pedig kifizeti a támadó által kért váltságdíjat.

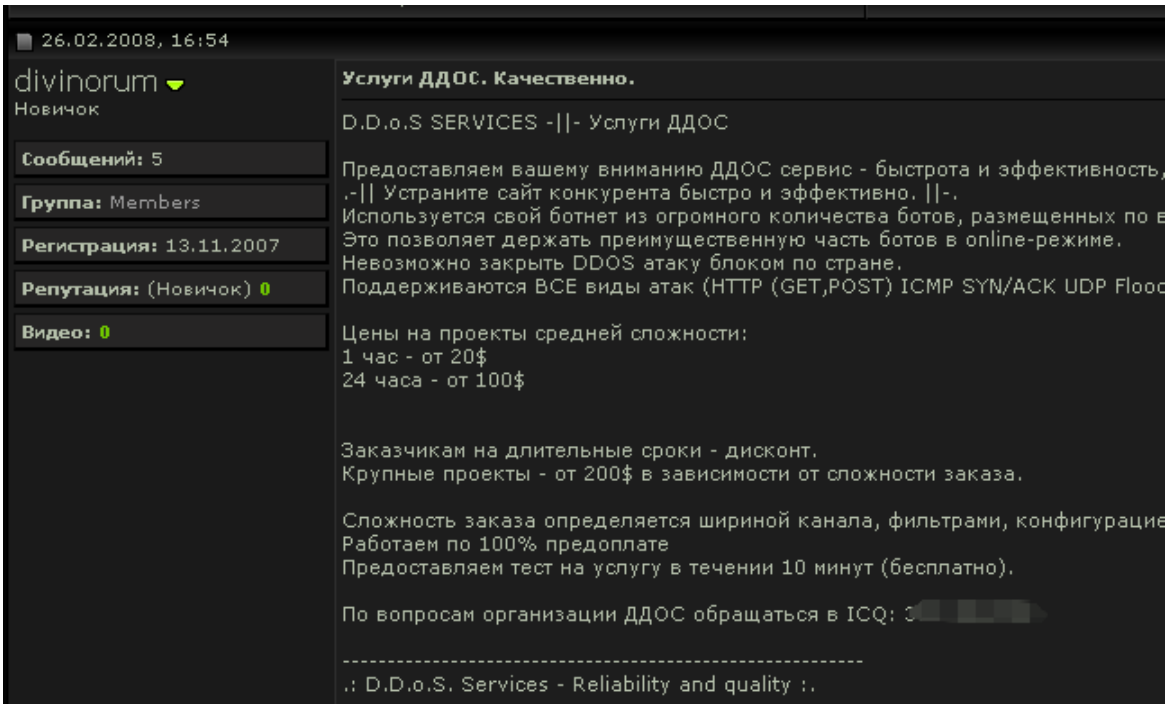
A korábban már ismertetett online bukmékerek elleni támadássorozat a tettesek lekapcsolásával megszűnt, azonban ez nem jelenti azt, hogy az ilyen bűnelkövetési forma azóta ismeretlen lenne: 2011 júniusában ítéltek el egy német számítógépes bűnözőt, mert 2010 nyarán megzsarolt néhány online fogadóirodát a labdarúgó világbajnokság idején. A megzsarolt oldalak egy része fizetett is, 5000 euro bevételhez juttatva az elkövetőt, aki lebukása után letöltendő börtönbüntetést is kapott. [98]

Támadó kapacitás bérbeadása

A zsarolások végrehajtása mindig jelentős kockázattal bír, az áldozat és a tettes között pénzügyi kapcsolatnak kell lennie, ami nyomozói eszközökkel felderíthető. Ennél sokkal kényelmesebb módszer az, amikor a botmaster csak a botnet képességeit árulja. Ekkor a tényleges támadást végrehajtó és az áldozat között nincs közvetlen kapcsolat, így a lebukás veszélye is csökken.

Léteznek olyan megrendelők is, akik nem kívánnak pénzt szerezni az áldozattól. Az ő esetükben teljesen más motivációt kell keresni: a terroristákat a nyilvánosság figyelmének felkeltése, egyes államok katonai erőit a szembenálló fél informatikai infrastruktúrájának meggyengítése, a hacktivistáknak nevezett szélsőségeseket pedig az ügyük számára a széles körű nyilvánosság biztosítása hajtja. Az ilyen akciók minimális kockázattal járnak a botnet üzemeltetői számára.

Egy DDoS támadás kivitelezésére alkalmas botnet bérleti díja nem túl magas, az Internetet böngészve könnyen és gyorsan ráakadhat az ember egy megfelelő hirdetésre:



12. ábra DDoS szolgáltatás hirdetése egy orosz weboldalon (forrás: forum.xaknet.ru)

A forum.xaknet.ru oldalon egy divinorum nevű felhasználó garanciával hirdeti DDoS szolgáltatását, óránként 20$ vagy napi 100$ költséggel. A vevőelégedettség garantálása érdekében egy 10 perces tesztperiódust is biztosít, így a megrendelő nem vesz zsákbamacskát.

A DDoS támadások kiemelt szerepet játszottak 2007. április és május hónapban, az észtországi zavargások nyomán egyes észt szervereket működésképtelenné tevő akciókban, illetve 2008. júliusi Grúzia elleni orosz katonai akció során. A grúziai katonai akció alatt botnetekről kiinduló DDoS támadások a grúz kormányzati szervereket szinte leradírozták az internetről. Az orosz internetes alvilág fórumain megjelentek a DDoS támadásokat végrehajtani képes önkéntes botmaster toborzások, az eredményeket látva kijelenthető, hogy sikerrel jártak. Az elkövetők személye minden valószínűség szerint örökre ismeretlen marad (az egy évvel korábbi észt incidens kapcsán egyetlen észt – orosz ajkú - egyetemistát ítéltek el, holott egyértelmű, hogy nem ő volt felelős az összes támadásért). A történések azt bizonyítják, hogy hamarosan az interneten elkövetett DDoS támadások bevonulnak az állami hadseregek fegyvertárába is. Charles W. Williamson, az Egyesült Államok Légierejének ezredese egy írásában [99] amellett száll síkra, hogy az USA hadseregének is szüksége van

botnetekre, amivel az interneten képes lehetne „szőnyegbombázást” végezni. Szerinte a hagyományos hadviseléshez hasonlóan a virtuális hadszíntéren is ideje lenne az erődbe zárkózott haderő szemléletmódja helyett korszerűbb alapokra helyezni a hadviselést.

Kéretlen levélküldés

Jelenlegi felmérések és becslések szerint az internet elektronikus levélforgalmának közel 80%-a tartozik a kéretlen levél (népszerűbb nevén SPAM) kategóriájába. [100]

13. ábra Kéretlen levelek száma 2010-2011 között. (forrás: Commtouch Software Online Lab)

Bár az átlag számítógépes felhasználót irritálja a kéretlen levél, mégis vannak olyanok, akik számára hasznosnak bizonyul a levél tartalma. A hírek szerint minden 10000 kiküldött kéretlen elektronikus levélre jut egy vásárlás, ami ugyan kevésbé hatékony, mint a fizetett webes hirdetések 0,1-2% értéke, de sokkal olcsóbb is. Bizonyos üzleti körök számára más reklámlehetőség nincs is, lévén a forgalmazott termék vagy szolgáltatás a legtöbb országban illegális. Ugyanez fordítva is igaz, a legtöbb cég számára a kéretlen levelekben reklámozni veszélyeket hordoz, így a közmondással élve, a zsák megtalálta a foltját. Illegális levelekben nagyrészt hamisított vagy tiltott termékeket (potencianövelő szerek, hamis luxuscikkek), illetve megkérdőjelezhető szolgáltatásokat (egyetemi diploma, PhD fokozat) hirdetnek. A kéretlen levelek számára jótékony hatással van egy-egy nagyobb botnet lekapcsolása: 2011 márciusában egy

Microsoft által vezetett akció keretében sikerült működésképtelenné tenni a Rustock botnetet, ami a teljes kéretlen levélforgalmat egyharmadával vetette vissza.

A kéretlen levelek nem csak termékeket reklámoznak, előszeretettel használják őket csalások elkövetésére is. Rendkívül elterjedtek az úgynevezett „Nigériai" levelek, amelyekben valamilyen jól hangzó ajánlattal veszik rá az áldozatot a pénzküldésre. A tevékenységet büntető jogszabály száma után 419 néven is ismert csalássorozat keretében kéretlen levelekkel árasztják el a potenciális áldozatokat. Ezekben egy kevéssé hihető történetet adtak elő bebörtönzött nigériai gazdag emberekről, akiket az áldozatnak kellene kiváltania egy kevés pénz küldésével. Szolgálatait a gazdag bebörtönzött személy szabadulása után természetesen busásan megjutalmaznák. A kezdeti bárgyú történeteket folyamatosan változtatják az aktuális világpolitikai események függvényében. A 2010. januári Haiti földrengés után pár nappal már megjelentek az eseményre hivatkozó 419 levelek, de az egyiptomi forradalom illetve líbiai események után is hamar eszméltek a csalók. [101] Egy időben annyira jelentős volt ez a tevékenység, hogy néhány kalandvágyó ember nekiállt átverni a csalókat. A 419eaters.com külön trófeaszobát is üzemeltet az átvert csalók fényképeinek tárolására. [102]

A 2000-es évek elején kezdték el a „pump-and-dump" vagy „hype and dump" [103] néven ismert csalásokat komolyabb méretekben alkalmazni. Az eljárás a tőzsdei árfolyamok manipulálásán alapszik. A csaló bevásárol egy tőzsdei cég papírjaiból (jellemzően kis, viszonylag ismeretlen cégekről van szó), majd SPAM áradatban bennfentes információkként feltüntetett hamis adatokat küld szét. A leveleknek köszönhetően sokan kezdik vásárolni a részvényeket, emiatt az árfolyam is felszökik, a csaló pedig jelentős haszonnal adhat túl a birtokában álló mennyiségen.

A kezdeti időkben egzotikus országokban üzemelő levelezőszerverek ontották a kéretlen leveleket, azonban a különböző feketelistákkal ezt a módszert le lehetett tiltani. A második generációban megindult a rosszul konfigurált – és így áldozattá váló – szerverek használata, azonban a botnetek jelentették a legmegbízhatóbb megoldást. Mivel a levelek küldését hatalmas mennyiségű számítógép végzi, ezért a DDoS támadásokhoz hasonlóan, ezek sem helyezhetők egyenként tiltólistára. Ha egy küldő végpont „elesik", tiltólistára kerül, rögtön aktivizálható helyette másik.

A kéretlen levelek köre kibővült egy nagyon fontos elemmel: az elektronikus levélben terjedő vírusokhoz hasonlóan a botnetek is igyekeznek újabb tagokat szerezni a

hálózatba. Az új tagok fertőzését is a levélhez mellékelt futtatható állománnyal, vagy speciálisan beállított weboldalakra mutató linkekkel végzik.

A kéretlen levelek egyrészt feleslegesen foglalják a számítógépes hálózatok erőforrásait, másrészt komoly kockázatot is jelenthetnek. A nigériai csalások – bár a legtöbb meglehetősen primitív módszerrel próbálkozik – is szedik áldozataikat, az adatlopásokhoz is kiváló kiinduló pontot jelent egy kéretlen levélkampány. Egy komplex informatikai támadás során a célpont dezinformálásában is komoly szerepet kaphat egy levélküldési akció.

Reklám manipulációk, click fraud

Az interneten fontos bevételi forrás az online reklámok megjelentetése, a weboldalak reklámbevételeik nagy részét ebből szerzik. Az offline médiában megjelenő reklámokkal szemben az online reklámok hatékonysága egzakt módszerrel mérhető. A reklámokat megjelenítő szerver képes mérni a reklám megjelenési számát, illetve az erre kattintók számát is, így a hatékonyság szinte azonnal mérhető. Kezdetben azok a weboldalak, amelyek alacsony átkattintási értéket produkáltak hátrányban voltak, mivel a hirdető szempontjából kevésbé voltak értékesek. Ez a tény az egy reklám megjelenésére fizetett összeget lecsökkentette. A médium érdeke tehát az volt, hogy ezt az átkattintási arányt minél magasabbra tornássza. A „kattintás vadászatot” a később megjelenő üzleti modellek – mint a Google AdSense – is tovább erősítették, hiszen ezek a rendszerek a médium számára nem a hirdetés megjelentetéséért fizettek, hanem a hirdetésre kattintók után adtak jutalékot. Természetesen az egy számítógépről többször kattintókat statisztikai módszerekkel kiszűrték.

Ezekre a modellekre is alkalmas a botnetek által nyújtott elosztott felépítés. Egy alkalmas program segítségével a botnet valamennyi tagja képes a hirdetést tartalmazó oldalak letöltésére, majd a hirdetésre „kattintani”, így a médium tulajdonosa számára bevételt generálni. A lebukás után sincs különösebb gond, a botnet segítségével egyszerűen újrakezdhető más néven az egész folyamat.

Bár a reklám manipulációk látszólag csak a hirdetőnek – illetve a hirdetést továbbító szolgáltatónak - okoznak kárt, de az ilyen csalások hatása jóval súlyosabb, mint azt elsőre gondolnánk. Az internetes tartalomszolgáltatóknak mindig is gondot okozott a bevétel biztosítása, hiszen a látogatók már megszokták, hogy az interneten a legtöbb információ szabadon hozzáférhető. Emiatt a tartalomért kevés látogató hajlandó fizetni, az ilyen előfizetéses rendszerű szolgáltatások nem értek el átütő sikereket (néhány szűk

területet leszámítva). Ennek köszönhetően a legtöbb tartalomszolgáltató hirdetésekből próbál a működéséhez szükséges bevételhez jutni, vagyis lényegében a hirdető fizeti ki a látogató helyett az információ előállításához, és továbbításához szükséges díjat. Természetes okokból a hirdető szeretné, ha befektetése megtérülne, amit elsősorban a bevételének emelkedése igazol hosszabb távon. Amikor a természetes érdeklődést mesterségesen eltorzítják a csalók, akkor a teljes internetes reklámpiac hatásosságába vetett bizalmat ássák alá a hirdetők szemében, így áttételesen a tartalomszolgáltatók létét veszélyeztetik.

Gépesített jelszófeltörés

Egy védett számítógépes rendszerbe bejelentkezni csak a megfelelő jogosultsággal lehet. Ez a legtöbb esetben egy felhasználói név és a hozzátartozó jelszó megadásával történik (noha rendelkezésre állnak fejlettebb hitelesítő eszközök is, használatuk nem általános). Egy támadónak tehát csak annyi dolga van, hogy valamilyen módszerrel meghatározza ezeket. Ehhez segítségül hívhat kész szótárakat (a leggyakrabban használt jelszavak gyűjteményei), megpróbálhatja a felhasználótól kicsalni a kívánt adatot (amennyiben képes kapcsolatba kerülne vele), vagy egyszerűen végig próbálhatja az összes lehetséges kombinációt (brute force). A botnetekkel sokkal egyszerűbbé válik az akció: a feltört gépekre telepített keyloggerrel[71] begyűjthetők a gazdagép tulajdonosának jelszavai. Ha olyan rendszerről van szó, aminek jelszavai nem találhatók meg a botnet által begyűjtött adatok között, akkor pedig a botnet tagjainak segítségével automatizált szótáras támadást (dictionary attack[72]) lehet indítani. A leggyakrabban használt jelszavak szótárai ingyenesen letölthetők a legkülönbözőbb nyelvekhez.

Az utóbbi időkben egy új, aggodalomra okot adó tendencia kezd kibontakozni, mely segítségével a titkosított jelszavak nagyságrendekkel gyorsabban feltörhetők. A korszerű operációs rendszerek a felhasználók jelszavait kódolva tárolják, legtöbbször valamilyen egyirányú hash algoritmus segítségével. A hash algoritmus (például MD5, SHA-1) a bemeneti adatokból – jelen esetben a jelszóból – egy fix hosszúságú bináris számot állít elő, amely ugyanazon jelszóból minden futás esetén mindig ugyanazt a hash értéket állítja elő, azonban csak a hash érték ismeretében a kiinduló érték nem állítható

[71] Keylogger: olyan speciális alkalmazás, amely az áldozat számítógépére települve észrevétlenül begyűjti a billentyűzeten bevitt adatokat, majd azokat a támadó által elérhető, külső tároló helyre tölti. Főként jelszavak és egyéb bizalmas adat lopására használható.

[72] Szótáras támadás, olyan, próbálgatáson alapuló támadási módszer, amely során a jelszavak próbája nem véletlenszerűen, hanem valamilyen gyakorisági statisztika alapján történik.

vissza. Az elnevezés a darált húsos ételre (hasé) utal, egy hash értékből ugyanúgy nem lehet visszaállítani a jelszót, mint a haséból az alapul szolgáló állatot. Egy támadó a rendszerbe egyszerű hozzáférést szerezve és különböző konfigurálási hibákat kihasználva hozzáférhet a többi felhasználó (köztük a rendszeradminisztrátor) jelszavainak hash értékeit tartalmazó állományokhoz. A hash értékek visszafejtésére sokáig csak a nyers erő (brute force) módszerét használták, vagyis az összes létező jelszóra lefuttatták a hash algoritmust, majd a kapott értékeket összevetették a listában található értékekkel. Ahol egyezést találtak, ott a hash képzés alapjául használt szöveg volt a jelszó. Ez a folyamat meglehetősen időt rabló, mivel rengeteg jelszót kell egyenként kipróbálni. A folyamat jelentősen felgyorsítható az úgynevezett Rainbow táblák segítségével, amelyek előre generált hash értékeket tartalmaznak nagy mennyiségben (értelemszerűen egy Rainbow táblázat csak egyféle hash algoritmushoz használható). Minél nagyobb egy Rainbow tábla, annál gyorsabban törhető fel a jelszó, viszont egy ilyen táblázat előállítása rengeteg időbe kerül, azonban ilyen táblázatok készen elérhetők az interneten. [104] Az előállításhoz szükséges idő a munkában részt vevő számítógépek számának növelésével csökkenthető, így egy botnet komoly segítséget jelent, ráadásul a használatáért sem kell fizetni.

3.5 Botnet architektúrák

Architektúrának a számítógépes hálózatok esetében általában az egyes végpontok egymáshoz kapcsolódásának milyenségét nevezik. Meghatározza a végpontok alá- és fölérendeltségi viszonyait. Két nagy architektúrát ismerünk:

- Centralizált, központi vezérlésű botnet;
- Decentralizált, egyenrangú (P2P) botnet.

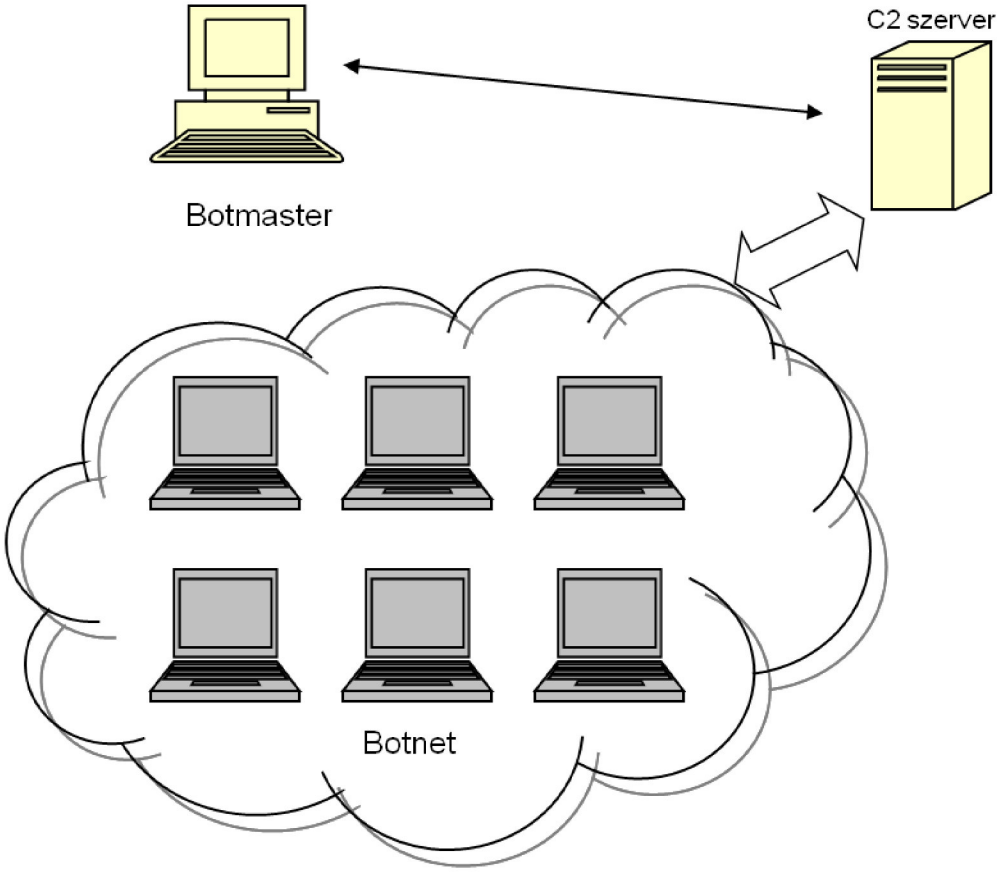
A központosított vezérlésű botnetek esetében az összes kliens egyetlen központi végponthoz kapcsolódik, és onnan várja az utasításokat, míg a decentralizált vezérlés esetén minden kliens egyenrangú, így bármelyik képes utasítást továbbítani a többiek számára.

Centralizált botnetek

Ez egyszerűsíti a programkódot, azonban egyben sérülékennyé is teszi a struktúrát, hiszen a vezérlő számítógép kiiktatásával a botnet gazdátlanná válik. A botnet irányítói is a lebukást kockáztatják, amikor bejelentkeznek a C2 gépre. Eleinte a legnépszerűbb – még napjainkban is gyakran használt – módszer az IRC volt. Elég könnyű IRC

DOI azonosító: 10.17625/NKE.2012.008

szervereket találni, ahol egy csevegő szobát (chat room) létrehozva máris készen áll egy pont-multipont összeköttetés. A chat alapja az, hogy az egyes kliensek által küldött üzeneteket a szerver minden, az adott szobában tartózkodó kliensnek továbbküldi. A botnet tagjai a bejelentkezést követően általában csak várakoznak, a botmaster pedig ugyanebbe a szobába belépve képes szöveges üzeneteket küldeni számukra. Előnye a gyors reagálás, mivel minden kliens majdnem egy időben kapja meg a vezérlő kódokat. A módszer hátránya, hogy a botnet összes tagjának egyszerre kell kapcsolódnia a szerverhez, ami a szerver számára jelentős terhelést okoz, így a kialakítható hálózat mérete általában néhány ezer tagra korlátozott.



14. ábra Centralizált vezérlésű botnet (szerkesztette a szerző)

Egyetlen C2 – IRC vagy webes – szervert használó botnet ellen viszonylag egyszerű a fellépés:

- A botnet kliensprogram egy példányának visszafejtésével meghatározható a kliens működése, a C2 szerver elérhetősége. A C2 szerver elérhetősége a hálózati forgalom figyelésével is meghatározható.

- A C2 szerver forgalmának figyelésével meghatározhatók a kliensgépek címei, hosszabb távú megfigyeléssel monitorozható a botmaster tevékenysége.
- A botmaster esetleges óvatlanságát kihasználva – például saját számítógépről jelentkezik be – elfogható a felelős.
- A C2 szerver lekapcsolásával a botnet semlegesíthető.
- Az ismert, fertőzött végpontok megtisztíthatók a fertőző kódtól.

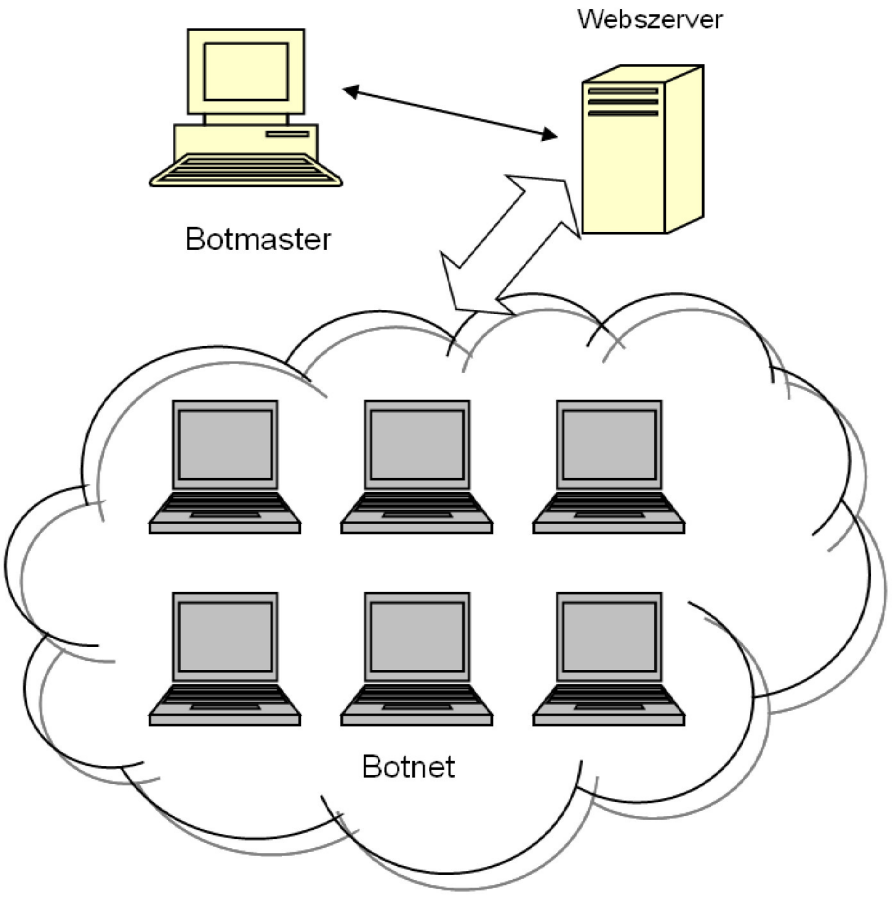
A kezdeti botnet kliensek általában a C2 szerver hálózati (IP) címén kezdeményezték a vezérlő csatorna kiépítését. Ez a módszer hamar korszerűtlenné vált, mivel elegendő volt az adott IP címen található végpontot lekapcsolni, és a teljes botnet irányíthatatlanná vált. A fix IP cím használata kiváltható a domain név használatával, ekkor egy logikai tartománynévhez rendelt IP cím könnyedén megváltoztatható, és a kezdeti C2 szerver lekapcsolását követően egy másik szerverre kapcsolható a teljes botnet irányítása. A domain nevek regisztrálása kockázatos dolog, ráadásul pénzbe is kerül, azonban megéri, mivel egy hálózati végpont általában gyorsabban lekapcsolható, mint amennyi időbe egy DNS rekord frissítése – az általában valamilyen egzotikus országban található felső szintű domain (Top Level Domain, TLD) tulajdonosával végzett egyezkedést is beleszámítva – kerül. Sok TLD regisztrátora nem kér semmilyen igazoló okiratot egy domain bejegyzéséhez, ezért ezek megfelelő partnerek a botmasterek számára.

A másik megoldás az ingyenes DYDNS szolgáltató, akinél online regisztrálható egy olyan domain, amelyhez gyorsan változó IP címeket lehet kapcsolni. A legfejlettebb domain manipulációs eljárás a fast flux, amely egyetlen domain névhez több száz, vagy több ezer IP címet regisztrál, a DNS szerver pedig a kiszolgálás során ezekből válogat. [105] A fast flux kiválóan alkalmazható centralizált, de P2P C2 csatornák túlélési idejének megnövelésére is.

Az IRC csatornát használó botnetek hátrányainak kiküszöbölésére kezdték használni a webes C2 csatornát, amelyben a kliensek a weboldalak lekérésére használt HTTP (Hypertext Transfer Protocol) protokoll segítségével kommunikálnak a C2 szerverrel. Előnye az, hogy sok klienst képes kiszolgálni, mivel a HTTP egy tranzakció alapú protokoll, a kliens és a szerver között csak a tranzakció lebonyolításának idejére létezik az adatkapcsolat. Egy tranzakció a botnet esetében viszonylag kevés adatmennyiséget igényel, így rövid idő alatt befejeződik. Hátránya, hogy nem valós idejű, hiszen csak a kliens tud kapcsolatfelvételt kezdeményezni, tehát a szervernek meg kell várnia a

DOI azonosító: 10.17625/NKE.2012.008

feladat kiosztásával a kliens kérését. A HTTP használatának járulékos előnye még népszerűsége, lévén ez a legnépszerűbb internetes protokoll, így kicsi a valószínűsége, hogy egy tűzfal ne eresztené keresztül az ilyen adatcsomagokat.



15. ábra Web alapú botnet (szerkesztette a szerző)

A módszer több előnnyel is jár:

- a botnet által generált http kérések elvegyülnek a normál webes forgalomban;
- a webszolgáltatást szinte minden hálózati tűzfal engedélyezi;
- megfelelő méretezés mellett egyetlen webes C2 szerver több százezer klienst is képes kiszolgálni.

A hátrány ebben az esetben is a C2 szerver üzemeltetése, a botok forgalmának figyelésével meghatározhatók a C2 szerverek elérhetőségei (hálózati címei), és így az üzemeltető botmaster is könnyen lebukhat.

A legújabb fejlesztésű botnet kliensek már kódolt vagy titkosított C2 csatornákat alkalmaznak a lebukás elleni védelemre. Ennek során igyekeznek a szteganográfia[73]

[73] Szteganográfia: adatrejtés, a továbbítandó adatot más adatok közé rejtik el.

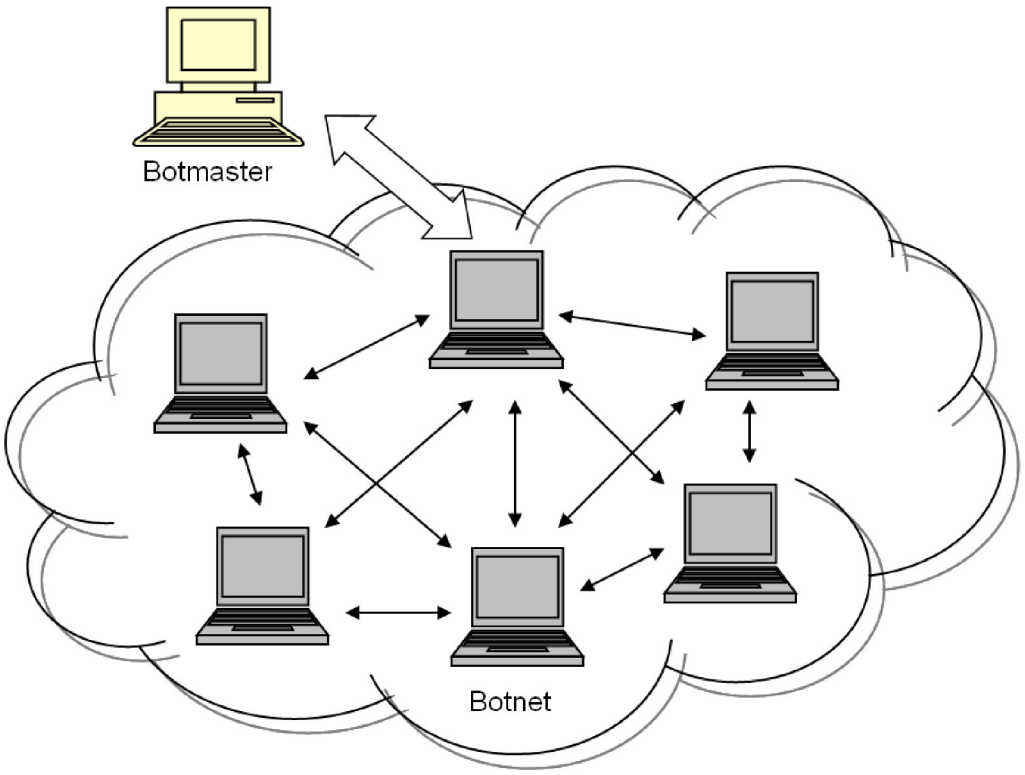
DOI azonosító: 10.17625/NKE.2012.008

módszereivel elrejteni más, a védelmi rendszerek figyelmét nem felkeltő adatforgalomba (például kép-, hang- vagy videoállományokba kódolva).

P2P alapú botnetek

A hagyományos, kliens-szerver architektúra jól használható olyan esetekben, amikor a kliensek kiszolgálásához szükséges információk a szerver rendelkezésére állnak. A modell előnye a központi menedzselhetőség, azonban a centralizáltság hátrányokkal is jár. Ha a központi eszköz kiesik, akkor a teljes rendszer működésképtelenné válik, ráadásul az erőforrások igénybevétele is erősen aszimmetrikus. Szűk keresztmetszetet okoz a szerver kapacitása, áteresztőképessége.

Az egyenrangú hálózatok segítségével a rendszer architektúrája decentralizálható, az erőforrások igénybevétele jobban eloszthető a tagok között, ráadásul a teljes rendszer megbízhatósága is növekszik az egyenrangú, egymást helyettesíteni képes elemek miatt. A P2P elven működő rendszerek néhány év óta rendkívüli népszerűségre tettek szert, elsősorban állományok megosztására, letöltésére használják őket, de említést érdemel még a Skype is, amely a P2P elvet telefonálásra, illetve a SayaTV, amely televíziós adások közvetítésére használja.



16. ábra P2P alapú, decentralizált vezérlésű botnet (szerkesztette a szerző)

A decentralizáltság és redundancia miatt rendelkezésre álló robosztusság felkeltette a botkliensek fejlesztésével foglalkozó programozók figyelmét is, emiatt hamarosan megjelentek a P2P elven működő C2 csatornát használó botnetek. Ebben a struktúrában a botmaster bármelyik tag számítógépre képes bejelentkezni, és onnan a teljes hálózat részére feladatokat kiosztani. Ez a tulajdonság természetesen a botmaster szemszögéből nézve nem csak kényelmes és biztonságos, de bizonyos veszélyeket is hordoz magában: kellő védelem nélkül bárki átveheti a botnet ellenőrzését, ezért az ilyen típusú C2 csatornát az illetéktelenek elől védeni kell, amelyre a legegyszerűbb módszer a kriptográfia.

Ha a decentralizált felépítéshez még hozzáadjuk a fast flux technikát, akkor egy nehezen felderíthető mechanizmust kapunk, ezért a P2P architektúrájú botnetek működéséről és méreteiről nincsenek teljesen pontos információk, csak becslések. Ráadásul az újabb generációs programkódok képesek azt is megállapítani, hogy a futtató környezet egy virtuális gép, ilyen esetben pedig nem a normál működésüket produkálják (a működés felderítéséhez általában egy virtuális gépet használnak a szakértők, mivel itt több lehetőség van a működés közbeni vizsgálatokra).

A gyakran emlegetett Storm botnet [106] működése során több, igen magas szintű megoldást is alkalmaz. Bár gyakran nevezik féregnek (worm), a működése mégsem olyan, mint azoké. Megtévesztő levélben érkezik, és trükkel veszi rá a felhasználót a telepítésre (például az amerikai NFL szezon csúcspontján „Football” tárgyú elektronikus levelekben terjedt), ezért inkább vírusnak tekinthető. A terjedéséhez nagyban hozzájárult a felhasználók tudatlansága, mivel a telepítéshez több figyelmeztető dialógusablakon is keresztül kellett navigálni (aláíratlan alkalmazás telepítésekor, stb…). A 2007. szeptember 11-i Microsoft rosszindulatú kódeltávolító programjának frissítése eltávolította a Storm kódját a felhasználó számítógépéről, a redmondi cég beszámolója szerint ez 250 000 gépet érintett. Ha ehhez a számhoz hozzáadjuk az illegális – és ezért nem frissített – operációs rendszerek használóit, akkor látható, hogy elég nagy a fenyegetés. A legnagyobb botnet címét a Conficker nyerte el, 2009 januárjában elérte a 10 milliós darabszámot. [107]

A decentralizált botnetek működésüket a népszerű fájlcserélő protokollok mögé próbálják rejteni, a biztonságról pedig a titkosított kommunikáció gondoskodik, amelyet a nyílt forráskódú OpenSSL biztosít. A titkosítás olyan kulcsmérettel történik, aminek visszafejtése a jelenlegi eszközök segítségével gyakorlatilag nem megoldható, így a felderítés is meglehetősen nehézkes. Szerencsére a detektáláshoz nem szükséges a

ténylegesen átvitt adatok ismerete, lehetséges olyan hálózatfigyelési szabályokat alkotni, amelyek képesek kiszűrni a tényleges P2P forgalomba rejtett botnet kommunikációt.

3.6 Speciális botnetek

A vírusfertőzéseket és ezen keresztül áttételesen a botneteket is sokáig csak a személyi számítógépek problémájaként ismertük. A legújabb események azonban ezeket a fenyegetéseket teljesen más területekre is kiterjesztik. Az internet terjedésével párhuzamosan egyre erősebb az igény a nem számítógépnek tekintett, „hagyományos" elektronikai eszközök hálózatra kapcsolására is. Az integráltsági fok növekedésének köszönhetően erre a lehetőség is megnyílt, azonban a komplexitás növekedésével a hibalehetőségek száma is megnő. 2007 óta robbanásszerű fejlődésen estek át a mobiltelefonok, az úgynevezett „okostelefonok" már sokkal inkább tekinthetők számítógépnek, mint telefonnak, ennek megfelelően itt is általános célú operációs rendszerek jelentek meg. Az IDC adatai szerint 2010 utolsó negyedévében közel 101 millió okostelefont adtak el, ami az előző évi adatokhoz képest 87,2% növekedést jelent. [108] A jelenlegi legnagyobb piaci részesedésű mobil operációs rendszer a Google által fejlesztett Android, amely 2011. második negyedévében már közel 50% részesedéssel rendelkezett. Sajnálatos módon az alkalmazásokat áruló Android Market nem teszteli biztonsági szempontból az alkalmazásokat, így jelenleg ez a rosszindulatú programokat készítők első számú célpontja. [109] A mobil eszközökre készített kártevő programok veszélye abban is rejlik, hogy nem csak a számítógépes hálózathoz képesek hozzáférni, de akár a mobiltelefon hálózatok rövid szöveges üzenetküldő vagy a hangátviteli szolgáltatásához is, így képesek akár ezeket is megtámadni.

A mobil eszközök mellett nem szabad elfelejtkezni a szórakoztató elektronikai készülékekről sem, a televíziók, blue-ray lejátszók alapszolgáltatásai közé is egyre többször kerül be az internetes kapcsolódási lehetőség. Sőt, a nagyon népszerű otthoni routerek is saját operációs rendszerrel rendelkeznek, amelyek akár ugyanúgy botnet klienssé válhatnak.

Érdekes problémát jelent a botnetek katonai alkalmazása is. Egy botnetet kiépíteni illegális tevékenység, amit egy reguláris hadsereg nem vállalhat fel. Rendkívüli körülmények között azonban felmerülhet a lefoglalás lehetősége, hasonlóan a polgári lakosság által birtokolt javakhoz. Erre a 2004. évi CV. törvény 197.§ (f) bekezdése adhat felhatalmazást:

„197. § Honvédelmi érdekből a 35. § (2) bekezdésében előírt szolgáltatásokon felül elrendelhető:

...

f) elektronikus hírközlő berendezés használatra való átengedése, illetve használatának mellőzése”

Természetesen ehhez szükséges az, hogy a honvédség rendelkezzen információkkal a lefoglalható botnetekről, amihez viszont komoly hírszerzési információkra van szükség. Szakértők szerint az interneten tapasztalt kínai aktivitás jelzi azt, hogy a kínai hadsereg komolyan veszi a botnetek használatának lehetőségét, akár úgy, hogy már rendelkezik saját kapacitásokkal, vagy a lefoglalható kapacitásokról szóló ismeretekkel. [110]

3.7 Következtetések

Irodalomkutatás segítségével felmértem a botnetek jelenleg használt architektúráinak sajátosságait illetve meghatároztam a felhasználási területeiket. Meghatároztam a felhasználási területek által kifejtett hatások veszélyeit, valamint megállapítottam, hogy a botnetek tevékenysége tartalmaz olyan jellemzőket, amelyek segítségével az ilyen hálózatok egyértelműen azonosíthatók. Megállapítottam, hogy a jelenlegi módszerek az irányítási (Command & Control, C2) csatorna működésének felderítését és megszüntetését tekintik első számú feladatnak, aminek segítségével a botnet tagjai elvághatók a központi irányítástól. A C2 mechanizmusok vizsgálatával arra a következtetésre jutottam, hogy ez a technika bizonyos esetekben – például a P2P alapú architektúrák esetében - nem megvalósítható, ezért célszerűbbnek tartom a botnetek felkutatását a tevékenységük miatt keletkezett egyéb nyomok vizsgálatával elvégezni.
Irodalomkutatás segítségével megállapítottam, hogy viszonylag egyszerűen hozzá lehet jutni támadó botnetekhez, illetve azt is, hogy léteznek olyan személyek, szervezetek, akik az ilyen eszközök telepítésével, kiépítésével és bérbeadásával foglalkoznak.

4. FEJEZET
BOTNETEK FELDERÍTÉSE, SEMLEGESÍTÉSE

A közelmúltban bekövetkezett nagyobb DDoS esetek tapasztalatai azt mutatják, hogy egy nagyméretű botnet képes aktív támadást folytatni hosszú időn keresztül is. A rengeteg támadó végpontot egyenként kell lokalizálni és kiiktatni, ami a védekezést végző szervezeteknek igen nagy munkát okoz. Ráadásul az ellenlépéseket egy éppen folyamatban levő támadás közben sokkal nehezebb megtenni, mivel közben a célpontok működőképességének megőrzése érdekében szükséges a hálózati forgalom korlátozása is.

További kutatásaim során annak bizonyítására koncentráltam, hogy lehetséges a támadásra használható botnetek tagjait már a támadás bekövetkezte előtt lokalizálni és semlegesíteni. Feltételezéseim a következők voltak:

- a botneteket nem csak DDoS támadások kivitelezésére használják, hanem egyéb, pénzszerzésre alkalmas cselekmények elkövetésére is;
- a botnetek tevékenysége szükségszerűen nyomokat hagy maga után;
- bár egy fertőzött számítógép birtoklása még nem, de a gép hálózaton végzett tevékenysége már alapot adhat a végpont ideiglenes vagy végleges lekapcsolására;
- lehetséges olyan proaktív rendszert készíteni, amely segítségével a botnet tagjai folyamatosan felderíthetők.

Feltevéseim bizonyítására egy számítógépes alkalmazás prototípusát készítettem el, amelyhez adatokat a saját tevékenységem során szereztem. Irodalomkutatás és a jogszabályok analizálásával végeztem el a működés szervezeti és jogszabályi működési feltételeinek vizsgálatát. Kutatásaim eredményét tartalmazza ez a fejezet.

4.1 Botnet kliensek lekapcsolásának háttere

A jelenlegi jogszabályok még nem nevesítik a botneteket veszélyforrásként, azonban ez valószínűleg változni fog. A rosszindulatú végpontok lekapcsolása nem minden esetben zökkenőmentes, mivel a végpontot tartalmazó hálózat tulajdonosát kell meggyőzni arról, hogy szüntesse meg a támadó – általában egy gyanútlan ügyfél – internet hozzáférését. Ez kényelmetlenséget, többletmunkát okoz a szolgáltatónak, ezért amíg nem egy támadást végző végpontról van szó, addig esetleges a fellépés határozottsága.

A szolgáltató feladata saját ügyfeleire ügyelni,[74] de a reakcióidejük illetve a válaszlépés milyensége természetesen eltérő lehet, ami tovább bonyolítja a támadások leállítását. Az internet szolgáltatók felügyeletére az Internet Szolgáltatók Tanácsa jogosult, amely nem hatóság, így eszközei korlátozottak. Szerencsére a szolgáltatók elemi érdeke is a hálózat üzemeltetésének biztonsága, ezért általában a felhasználóval kötött szerződésben (Általános Szerződési Feltételek – ÁSZF) szabályozzák a lekapcsolás alapját képező eseményeket. Átvizsgáltam a nagyobb magyar internet szolgáltatók szerződési feltételeit, és azt tapasztaltam, hogy mindnyájan foglalkoznak a hálózatukból kiinduló rosszindulatú akciók elkövetőinek korlátozásával, általában két megközelítési mód egyikét felhasználva. Az első megközelítési mód a T-Online ÁSZF-ben [111] található, és az ügyfél szolgáltatásának korlátozását helyezi kilátásba az alábbi esetekben (10.2 pont):

„a. Amennyiben az Előfizető akadályozza vagy veszélyezteti a Szolgáltató hálózatának rendeltetésszerű működését, így különösen, ha

a.1. Az Előfizető a számára nyújtott szolgáltatást felhasználva kéretlen illetve nagy mennyiségű levelet küld.

(...)

a.3. Az Előfizető a számára nyújtott szolgáltatást felhasználva jogosulatlan adatszerzésre, adatküldésre vagy más számítógépes rendszerekbe történő behatolásra tesz kísérletet illetve hajt végre, különösen:

i. az internethasználók személyi számítógépén vagy szerverén tárolt, illetve internetezés közben használt nem nyilvános vagy üzleti titkot képező adatok, állományok engedély nélküli megtekintése, megszerzése vagy az erre irányuló kísérlet,

ii. az internethasználók személyi számítógépén vagy szerverén tárolt adatok, állományok engedély nélküli megváltoztatása vagy az erre irányuló kísérlet,

[74] Az általános gyakorlat szerint a szolgáltatók az „abuse@” kezdetű email címen fogadják az ilyen jellegű bejelentéseket.

iii. az internethasználók személyi számítógépére vagy szerverére olyan adatok, állományok engedély nélküli feltöltése vagy ennek kísérlete, amely az előfizetőt kompromittálhatja, illetve a számítógép működését hátrányosan befolyásolhatja,

iv. mások tulajdonát képező számítógépek és azok erőforrásainak engedély nélküli felhasználása saját célra (pl. proxy, e-mail szerverek, nyomtatók, hálózati átjárók és egyéb kapcsolt hardvereszközök).”

Az a.1. pont egyértelműsíti a kéretlen levelek küldése esetén alkalmazható szankciókat, ez tehát már önmagában alapot képezhet egy felderített botnet kliens semlegesítésére. Amennyiben a fertőzött számítógép felderítése nem a kéretlen levél küldése alapján történt, akkor viszont az a.3. pont probléma nélkül alkalmazható, így az előfizető számítógépének hozzáférése a szükséges mértékben korlátozható.
Az UPC Magyarország ÁSZF [112] ezzel szemben – a másik megközelítési mód alapján – nem részletezi a szankcionálandó tevékenységeket, hanem az Internet Szolgáltatók Tanácsa által kiadott hálózathasználati irányelveket fogadja el. Fontos tényezőként bevonja a szankciók alá az előfizető tudta nélkül, de annak tulajdonát felhasználva elkövetett cselekményeket is, amelyek a botnet kliensek esetére is vonatkoztathatók:

„9.1.3.1. Az Előfizető köteles betartani az 4. számú függelékben csatolt, az Internet használata kapcsán kialakult és nemzetközileg elfogadott Hálózathasználati Elveket (AUP Acceptable Use Policy), amelyeket Magyarországon az Internet Szolgáltatók Tanácsa tesz közzé és vizsgál felül rendszeresen.

(...)

Amennyiben az előfizető bármely, a Hálózathasználati Elvekben tiltott cselekményt követ el, vagy magatartást tanúsít, - ***ideértve azt az esetet is, amikor ugyan nem az előfizető a közvetlen elkövető, de az előfizető gépének felhasználásával követik el a jelen pontba foglalt tiltott tevékenység valamelyikét*** *- a Szolgáltató azonnal korlátozhatja az Előfizető hozzáférését és felszólítja a fenti tevékenység 3 napon belüli megindoklására vagy a fenti tevékenységtől történő tartózkodásra a jogkövetkezmények feltüntetésével.*

Ha az Előfizető a Hálózathasználati Elvekben tiltott cselekmény elkövetésével, vagy magatartás tanúsításával nem hagy fel a felszólítást követő 3 napon belül, illetve arra magyarázatot nem ad, vagy az megismétlődik, úgy a Szolgáltató az előfizetői szerződést felmondhatja az ÁSZF. 10.3.2. pontja alapján."

A hálózathasználati irányelvekben részletesen szerepel minden tiltott tevékenység, beleértve az informatikai rendszerekbe történő behatolást és a túlterheléses (DoS) támadásokat is.

Tapasztalataim szerint a külföldi hálózatok ügyfeleivel szemben azonban kétséges a fellépés eredményessége, egy rendszergazda gyakorlatilag a külföldi hálózat üzemeltetőire van utalva az ellenséges tevékenységet folytató ügyfelekkel szemben vívott harcában. A nemzeti CERT-ek bevonása természetesen segítséget nyújthat ebben a kérdésben.

Az eddig bekövetkezett DDoS támadások elemzése alapján bizonyos, hogy a támadás leállítása bonyolult, erőforrás igényes folyamat. Fontos az időtényező is, hiszen a működésképtelenné tett végpontok kiesése mindenképpen veszteséget jelent az üzemeltető számára. A reaktív védelem helyett véleményem szerint hatékonyabb lehet a proaktív eljárás, vagyis a botnetek elleni megelőző jellegű küzdelem. Ekkor a botneteket még a kezdeti fázisok egyikében próbáljuk semlegesíteni. Ehhez természetesen alapvető fontosságú az ilyen végpontok elhelyezkedésének ismerete (ország, illetve a számítógépes hierarchiában elfoglalt helye alapján a tulajdonos szervezet szerint).

4.2 Megelőző csapás

Az aktív védelem két területre osztásával, a katonai fogalmakkal újabb párhuzam vonható: ezek az ellencsapás és a megelőző csapás fogalmai. Az ellencsapás virtuális megfelelője tisztán a technika eszközeivel is kivitelezhető, nem szükséges a szervezetközi kapcsolatrendszert felhasználni hozzá. A támadó által alkalmazott módszerek a célpont számára is elérhetők, amiket a támadó azonosítása után be is vethet. Azonban a célpontra is vonatkoznak a szabályok, a támadásra Letöltve sem alkalmazhat illegális módszereket. Egy klasszikus példa erre az 1998-ban az Electronic Disturbance Theater (EDT) nevű radikális politikai szervezet és a Pentagon között történt incidens. [113] A szervezet támogatói internetes böngészőjükben egy JavaScript

nyelven írt alkalmazást futtattak, ami nagy sebességgel elkezdett weboldalakat lekérni a Pentagon szerveréről. Kellően sok böngészővel és megfelelő hálózati sávszélességgel ez a módszer igen nagy terhelést okoz a kiszolgálónak, így a Pentagon rendszere egy időre elérhetetlenné vált. Az EDT által előidézett túlterheléses DoS támadásra válaszul a Pentagon szakemberei ellentámadást hajtottak végre. A támadó kliensekre töltöttek egy Java appletet (hostileapplet), amely a böngésző képernyőjén kávéscsészéket - a Java logója - és az "ACK" üzenetet jelenítette meg akkora mennyiségben, hogy a böngésző erőforrásai elfogytak, ami a támadó számítógép lefagyását idézte elő. Az EDT fontolóra vette a Pentagon perbe fogását a „Posse Comitatus”, egy 1878-as törvény alapján, amely tiltja a katonaság bevetését a belföldi törvények betartatása során.

A megelőző csapás fogalmát a virtuális térben értelmezve a „békeidőben” végzett felderítés és a felfedett potenciális veszélyforrások megszüntetése jelenti, amire érdemes több figyelmet szentelni. A botnetek működésük során észlelhető nyomokat hagynak maguk után. Minden kliens szükségszerűen egy külső ponthoz kell, hogy forduljon, ahonnan az utasításokat kapja, az ilyen Command&Control (C2) csatorna figyelésével azonosítható a vezérlést végző végpont és annak kikapcsolásával megszüntethetővé válik a botnet központi irányítása. Emellett egy internetes végpont reagálása bizonyos kiváltó eseményekre is jelezheti a fertőzöttséget. A gyakoribb botnet kliensek tesztelésére rendelkezésre is állnak ilyen alkalmazások, azonban a szélesebb körű, automatizált használattal szemben a következő érveket hozom fel:

- mivel ez az eljárás lényegében egy szűkített méretű portszkennelés, ezért – bár a cél nemes – az ilyen felderítést végző is az illegális tevékenység határait súrolja;
- az újgenerációs kliensek már szakítottak a hagyományos Command & Control struktúrával és egyenrangú, Peer-to-peer hálózatként funkcionálnak, emiatt az ilyen kliensek felderítése nem triviális;
- készíthetők olyan botnet kliensek, amelyek a felderítési szándékot érzékelve ellentámadást indítanak.

Az etikai aggályokat is szem előtt tartva, a legcélravezetőbb megoldás a botnet tagjainak felkutatására a passzív felderítés, vagyis olyan, árulkodó nyomok figyelése, amelyek csak a botnetekre jellemzőek.

4.3 Hálózati forgalom elemzése

Ha a botnet kliens vizsgálata nem megoldható (visszafejthető programkód nem áll rendelkezésre), akkor is vannak a C2 csatornát azonosítani tudó eljárások, mivel ez mindig valamilyen szabályszerűség szerint zajlik. Az IP csomagok átvizsgálása során felfedezhetők olyan sajátosságok, amelyek botnet tevékenységre utalnak. Például, az IRC alapú C2 csatornát használó bot kliens létrehoz egy TCP kapcsolatot az IRC szerver irányába (az IRC alapértelmezett TCP port száma a 6667), majd a bejelentkezést követően inaktív állapotban várja a beérkező üzeneteket, amelyek száma jóval kisebb, mint a szokásos mennyiség.

Természetesen az ilyen hálózati forgalomfigyelés adatvédelmi aggályokat vet fel, mivel a hatékony szűrés érdekében át kellene vizsgálni a teljes IRC adatforgalmat. A [114] forrás ismertet egy olyan eljárást, amely kizárólag az IP és TCP fejlécekből kinyerhető adatok – amelyek nem hordoznak személyes információkat – segítségével képes azonosítani a bot kliensek és a C2 szerverek közti adatforgalmat.

Az egyéb típusú C2 csatornák detektálása már nem ilyen egyszerű feladat, mivel ezekben a felhasználó által kezdeményezett „normális” hálózati forgalom közé vegyül a gyanús akció nyoma is. Az ilyen esetekben csak igen összetett szűrési módszerekkel lehetne pusztán fejléc információkból azonosítani a gyanús kommunikációt.

A [115] forrás az ilyen, passzív jellegű módszerek között megemlít még néhány lehetőséget:

- Adatfolyam analízis: az egyedi csomagok analizálása helyett adatfolyamokat figyel, így sokkal kevesebb erőforrás szükséges a felderítéshez. Egy adatfolyam jellemzői (forrás- és célcím, port címek, alkalmazott magasabb rétegbeli protokollok, az adatfolyam időtartama, mérete) árulkodhatnak a botnet tagjairól.
- DNS alapú megközelítések: egy botnet tagjai szükségszerűen kapcsolódnak a botnet központi irányítását végző végpontokhoz. Ezek a végpont címek lehetnek a kliensprogramba ágyazva, vagy pedig egy tartománynévhez (domain name) kötve. Ez utóbbi rugalmasabb megoldás, mivel így a névfeloldást végző szerver módosításával új C2 szerverre kapcsolhatók a kliensek. Ha egy ilyen tartománynevet sikerül azonosítani, akkor az ilyen DNS kérések is megkülönböztethetők a „normális” kérésektől.
- Csalik kihelyezése: olyan, szándékosan könnyű prédának látszó végpontok kihelyezése a hálózatokba, amelyek várhatóan felkeltik a fertőzést előidézni

kívánó más végpontok figyelmét. A fertőzési kísérleteket monitorozva összegyűjthetők a szükséges adatok.

Valamennyi, a botnet tevékenységének hálózati szintű megfigyelésére épülő módszernek van egy közös problémája: a teljes hálózati forgalmat figyelni és elemezni kell, ami hatalmas erőforrásigényt jelent.

4.4 Kéretlen levélforgalom elemzése

Mint azt az előző fejezetben bemutattam, a botnetek egyik alaptevékenysége a kéretlen levelek küldése. Egyrészt a botnet irányítójának ebből jövedelme származik, másrészt pedig a botnet tagjai saját maguk is megpróbálhatnak újabb tagokat „toborozni", amihez kiváló lehetőség egy megfelelően fertőzött elektronikus levél.

A kéretlen levelek küldése több fontos fejlődési szakaszon esett át. Kezdetben az ilyen levelek küldői saját üzemeltetésű, általában valamilyen egzotikus – és így nehezen lenyomozható – levelező szerverről indították kampányaikat. Ezek ellen hamarosan megjelentek a védekezési módszerek, egyszerűen a címzettek postafiókjait kezelő szerverek nem fogadtak el leveleket az ilyen, ismertté vált IP című szerverektől, amiket folyamatosan frissülő feketelistákon publikálják. A spammerek következő módszere az álcázás volt. Igyekeztek felkutatni olyan, tőlük teljesen függetlenül működő szervereket, amelyek rendszergazdája nem volt elég gondos és helytelenül konfigurálta fel rendszerét. A levelek továbbításában részt vevő, ún. SMTP szerverek ugyanis képesek lehetnek továbbítási (relay) funkciókra, vagyis átvehetnek olyan elektronikus leveleket, amelyek címzettje nem a saját postafiókjaik között található. Az átvétel után a feladó nevében továbbítják a tényleges címzettnek. Megjegyzendő, hogy az internet-szolgáltatók által az előfizetőiknek biztosított SMTP szolgáltatás is ilyen módon működik. A szolgáltatók saját előfizetőiket meg tudják különböztetni a többi internetezőtől (mivel saját hálózati címtartományukban működnek), így a levéltovábbítást csak ennek a zárt csoportnak engedélyezik. Az olyan levelezőszervereknek, amelyek bárkitől elfogadnak leveleket és azt bármely, nem saját kezelésű email címre továbbítják, „Open Relay" a neve. A védekezés ezek ellen már nehezebb, hiszen ilyen szerver sok van, ráadásul ezeket a tulajdonosaik nem csak kéretlen levél küldésére használják. Több, - Open Relay szerverek IP címeit tartalmazó - adatbázis jött létre, amelyeket a levelező szerverek figyelhetnek, és a tiltólistában szereplő szerverektől visszautasíthatják a levél elfogadását.

A következő fejlődési lépcső olyan hálózati végpontok keresése volt, amelyeket a kéretlen levél küldője saját céljaira fel tud használni. A botnetek minderre egyszerű, és hatalmas kapacitású megoldást kínálnak. Mivel a levelezőszerver is csak egy számítógép (amelyen SMTP alkalmazás fut), így egy egyszerű otthoni PC is alkalmas ilyen feladatokra. A botnet számos tagját felhasználva lehetővé válik egy időben, egyszerre sok végpontról indítani a levelek küldését. Az otthoni PC-k által használt IP címek nem szerepelnek a feketelistákban, ráadásul, ha némelyiket kitiltják, másik lép a helyére. Nem elhanyagolható problémát jelent a legtöbb, háztartásokban használt internet előfizetés dinamikus IP cím kiosztása sem. A szolgáltatók igyekeznek spórolni a nyilvános IP címek kiosztásával, mivel ezek számukra is pénzbe kerülnek. Mivel az összes ügyfelük egy időben valószínűleg úgysem csatlakozik a hálózatra, így felesleges mindegyiknek ilyen „drága", egyedi címet biztosítani. A gyakorlat az, hogy a hálózatra csatlakozás során a szolgáltató az éppen nem használt címekből ad egyet az ügyfélnek, folyamatos csatlakozás esetén pedig általában 24 óránként megújítja azt. Emiatt egy átlagos végpont IP címe legfeljebb 24 óráig marad ugyanaz, vagyis ha egy bot kliens IP címe tiltólistára is kerülne, akkor 24 órán belül egy újabb címmel szabadon folytathatná a levélküldést.

Napjainkban botnetek felelnek a káros levelek küldésének túlnyomó többségéért. 2011-ban ez az arány 80% feletti volt. [100]

A káros levelek szűrésének lehetőségei

Az SMTP a TCP protokollt használja az adatátvitelre. Szerencsére, a korábban ismertetett „3 utas kézfogás" mechanizmus meggátolja, hogy a kapcsolatot kezdeményező végpont hamisított címet használjon. Erre az úgynevezett Sequence Number szolgál, amely egy 32 bites bináris szám, és fő feladata az adatfolyamban átküldött elemek sorszámozása. A kapcsolat létrejötte előtti eljárás során mindkét félnek vissza kell igazolnia a másik által küldött Sequence Number értéket. Ez az érték minden kapcsolat elején kerül kiszámításra, egy folyamatosan, nagy sebességgel (minden 4 mikroszekundumban) növekvő számláló aktuális értékéből. [116] Emiatt, ha a kapcsolatot kezdeményező végpont nem kapja meg a visszaigazoló csomagot (márpedig hamis címet használva nem fogja megkapni), nem tudja a későbbiekben nyugtázni a másik féltől kapott adatokat, így a kommunikáció nem lesz lehetséges. Természetesen vannak ennek kikerülésére is módszerek (például a TCP Sequence Prediction Attack [117]), azonban egy helyesen működő TCP/IP implementáció nem érzékeny ezekre.

A kéretlen reklámlevelek és vírusos csatolást tartalmazó levelek elleni védekezés nem egyszerű. Egy elektronikus levél elküldése a következő lépésekben történik (abban az esetben, ha a küldő nem vesz igénybe továbbító szervert):

1. A levelet küldő (kliens) a címzett email címe alapján lekéri a domain névhez (az email cím „@” utáni része) tartozó DNS MX (Mail Exchanger) rekordot. Ez a rekord tartalmazza a domain névhez tartozó levelezőszerver elérhetőségét.
2. Az MX rekord alapján meghatározza a címzett levelezőszerver IP címét.
3. A kliens TCP kapcsolatot hoz létre a címzett szerver 25-ös portjára.
4. Az SMTP használatával megadja a feladó és a címzett email címét.
5. Elküldi a levelet.
6. Bontja a TCP kapcsolatot.

Mint látható, mindez nem igényel komolyabb erőforrásokat, a kommunikációt lebonyolító SMTP „motor” néhány tíz kilobyte méretben megvalósítható, így egy bot kliensbe is beépíthető. A fogadó szerver a 3. pont után hajthatja végre az első ellenőrzési folyamatot. Mivel a TCP kapcsolatban a feladó IP címe nem, vagy csak nagyon nehezen hamisítható, így a küldő kénytelen a tényleges IP címét használni. A fogadó szerver végrehajthat néhány biztonsági funkciót:

- Ellenőrizheti, hogy az IP cím szerepel-e a tiltólistában.
- Ellenőrizheti, hogy a küldő SMTP szerver IP címéhez tartozó fordított DNS (Reverse DNS) adat megegyezik-e azzal, amit a szerver magáról hirdet (az otthoni számítógépek által használt IP címekhez nem mindig állít be a szolgáltató Reverse értéket). Ha nem egyezik meg, akkor a küldőtől nem fogadja el a levelet.

A leghatékonyabb módszer a folyamatnak ebben a fázisában elutasítani a levél átvételét, hiszen ekkor történik a legkevesebb felesleges művelet elvégzése. A következő szűrési lehetőség a 4. pontban van, vagyis a feladó és a címzett email címének megadásakor. Ekkor a fogadó szerver:

- Visszautasíthatja a levéltovábbítást (ha a címzett email címe nem a saját postafiókok között található).
- Ellenőrizheti a feladó címét. Ha elindít egy levélküldést a feladó részére, és a címet kezelő szerver ismeretlennek jelzi vissza, akkor a feladó címe nem létezik, így a levél kéretlennek tekintendő. Ez egy erőforrás igényes folyamat, ráadásul a

mostani kéretlen leveleket többnyire létező (a tulajdonos tudta és engedélye nélkül használt) email címet megadva küldik, tehát a hatékonysága is alacsony.

- A feladó címét keresheti tiltólistán. Ha szerepel, akkor a levelet nem veszi át.

Az utolsó ellenőrzési fázis a levél átvétele után lehetséges, ekkor már a levél teljes terjedelemben rendelkezésre áll, vagyis annak tartalma megvizsgálható. A tartalomvizsgálatra több, szofisztikált módszer is létezik. Egyszerűbb esetben csak bizonyos kulcsszavak meglétét ellenőrzik, de lehetséges a valószínűségszámításra alapozott, öntanuló rendszereket is használni. A Bayes-tételt használó Bayes analizátor segítségével nem egyetlen szó előfordulását keresik, hanem a korábban érkezett levelekben található szavak együttes előfordulási valószínűségét vizsgálják. Ha bizonyos szavak kéretlen levelekben gyakrabban fordulnak elő együtt, és egy vizsgálandó levélben ugyanezek a szavak megtalálhatók, akkor a levél károsságának valószínűsége növekszik. Normál levelekben előforduló szavak egy vizsgált levélben a valószínűségi értéket csökkentik. Minél nagyobb a minta, minél több levelet vizsgált már át a szűrő, annál pontosabb lehet a becslés. Ehhez szükséges mind kéretlen levelekre (spam), mind normál levelekre (ham) lefuttatni az analizátort. Az eredmény egy valószínűségi érték lesz, az adminisztrátor feladata a káros/normális küszöbszint beállítása. Természetesen a spammerek is fejlődtek, a friss kéretlen levelek igyekeznek különféle módszerekkel kijátszani a spam szűrőket (például a levél szövegében normál tartalmat illesztenek, és egy grafikus csatolásban helyezik el a kéretlen reklámot). Kiemelem azt a tényt, hogy a spamszűrők napjainkban egyre inkább elterjednek a levelezőszervereken, így egyre több káros levél kiszűrése történik a normál levélforgalomból.

Potenciális veszélyforrások felderítése, lokalizálása email vizsgálat segítségével

A [115] forrás említi a spamrekordok elemzését is, mint lehetséges módszert a botnetek felderítésére. Az általam létrehozott kísérleti modell is ezt az utat járta be, a módszer kiválasztásának és megvalósításának alapjaként a következő tényeket fogadtam el:

- Egy DDoS támadás elleni védekezés nehéz és költséges dolog. A védekezést megkönnyíti, ha közelítő adatokkal rendelkezünk arról, merről várhatók támadások, az előzetes intézkedések korán megtehetők.
- A botnetek használatának egyik fontos célja a kéretlen levelek küldése.

- Napjainkban a kéretlen levelek túlnyomó többségéért a botnetek felelnek, vagyis egy kéretlen levél küldője 90% feletti valószínűséggel egy botnet tagja, így egy fertőzött számítógép.
- A kéretlen levelet küldő számítógép TCP/IP protokollpárost használ, ami garantálja, hogy a feladó IP címe nem hamisított.
- A kéretlen levél küldőjének IP címe valószínűleg egy botnet tagja.

Az elektronikus levélszűrő rendszerek valamennyi átvizsgált levélről tárolnak információkat, naplózzák a működésüket. Ebben a naplóban megtalálható a vizsgálat időpontja, a küldő végpont IP címe és a vizsgálat eredménye.

```
Aug 17 16:36:39 mail2 amavis[16478]: (16478-05) Blocked SPAM, [2.88.64.19]
Aug 17 16:37:21 mail2 amavis[16478]: (16478-06) Blocked SPAM, [200.161.95.148]
Aug 17 16:38:32 mail2 amavis[16478]: (16478-07) Blocked SPAM, [120.83.201.205]
Aug 17 16:40:39 mail2 amavis[16421]: (16421-10) Blocked SPAM, [200.37.62.146]
Aug 17 16:41:05 mail2 amavis[16478]: (16478-08) Blocked SPAM, [213.5.121.251]
Aug 17 16:41:55 mail2 amavis[16421]: (16421-12) Blocked SPAM, [31.162.90.149]
Aug 17 16:42:54 mail2 amavis[16478]: (16478-10) Blocked SPAM, [189.47.146.171]
Aug 17 16:43:16 mail2 amavis[16421]: (16421-13) Blocked SPAM, [121.214.203.54]
Aug 17 16:46:39 mail2 amavis[16478]: (16478-15) Blocked SPAM, [218.171.56.177]
Aug 17 16:48:15 mail2 amavis[16478]: (16478-16) Blocked SPAM, [59.33.38.91]
Aug 17 16:49:34 mail2 amavis[16478]: (16478-18) Blocked SPAM, [46.185.62.57]
Aug 17 16:51:07 mail2 amavis[16478]: (16478-20) Blocked SPAM, [46.19.230.136]
Aug 17 16:51:29 mail2 amavis[19315]: (19315-01) Blocked SPAM, [93.74.232.137]
Aug 17 16:51:36 mail2 amavis[19133]: (19133-04) Blocked SPAM, [202.133.61.130]
Aug 17 16:52:16 mail2 amavis[19315]: (19315-03) Blocked SPAM, [190.254.0.58]
Aug 17 16:54:02 mail2 amavis[19133]: (19133-06) Blocked SPAM, [125.228.227.109]
Aug 17 16:54:10 mail2 amavis[19315]: (19315-04) Blocked SPAM, [125.228.227.109]
Aug 17 16:54:11 mail2 amavis[19133]: (19133-07) Blocked SPAM, [125.228.227.109]
Aug 17 16:56:58 mail2 amavis[19133]: (19133-09) Blocked SPAM, [195.191.79.10]
Aug 17 17:00:10 mail2 amavis[19133]: (19133-10) Blocked SPAM, [182.64.127.239]
Aug 17 17:00:17 mail2 amavis[19315]: (19315-08) Blocked SPAM, [58.64.104.222]
Aug 17 17:00:50 mail2 amavis[19315]: (19315-09) Blocked SPAM, [120.59.65.173]
Aug 17 17:02:22 mail2 amavis[19315]: (19315-10) Blocked SPAM, [89.190.236.205]
Aug 17 17:04:09 mail2 amavis[19133]: (19133-15) Blocked SPAM, [89.76.99.156]
```

17. ábra Egy kéretlen levélszűrő naplójának részlete (készítette a szerző)

Az ebből nyerhető adatok feldolgozása viszonylag alacsony járulékos erőforrásigényű, hiszen csak a megfelelő adatokat kell egyszerű szűrőalgoritmus segítségével kinyerni, majd adatbázisba tölteni. A módszer előnye az, hogy nem kell csali rendszereket (honeypot) telepíteni, elegendő az amúgy is rendelkezésre álló adatokból dolgozni, a keletkezett adatok alapján aztán lokalizálni is lehet a fertőzött gépeket. Ha a naplóállomány valamiért nem áll rendelkezésre, akkor is lehetséges a fogadott, és kéretlennek talált levél fejlécéből kinyerni a szükséges információkat. A levél fejléce a címzett levelezőszerverére történő beérkezés után így néz ki:

```
Received: from 83.110.251.9 (dxb-b114995.alshamil.net.ae [83.110.251.9])  by mail.xy.hu  with ESMTP id m347L3XP014337;
                Fri, 4 Apr 2008 09:21:04 +0200
Message-ID: <000901c89624$051e9a4d$29abf7ab@fpfqfu>
From: "bourke kara" <*******@mail.ihs.gov>
To: <cimzett@xy.hu>
Subject:  Paris and Linsey lesbian video
Date: Fri, 04 Apr 2008 05:33:32 +0000
MIME-Version: 1.0
Content-Type: multipart/alternative;  boundary="----=_NextPart_000_0006_01C89624.051C0183"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2900.3138
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.3198
```

18. ábra Kéretlen elektronikus levél fejléce

Az első két sorban olvasható adatokat a levelet fogadó szerver illesztette a fejléchez, ezekben található a feladó számítógép IP címével kapcsolatos összes adat. Látható, hogy a példában szereplő IP cím egy „.ae" végű domain névhez tartozó hálózat – amelyet az Egyesült Arab Emirátusokban regisztráltak – tagja, míg a feladó email címe az Egyesült Államokban működő IHS (Indian Health Service) szervezet tulajdona.

A fenti kéretlen levél fejléc vizsgálatával látszólag könnyen azonosítható a feladó fizikai elhelyezkedése, hiszen a szerver képes volt meghatározni a domain nevet. A felismerés azonban hibás eredményt is adhat:

- ha a küldő IP címéhez nem tartozik Reverse DNS bejegyzés, akkor a domain név nem meghatározható. Ez esetben más módszert kell találni a hálózat tulajdonosának és fizikai elhelyezkedésének meghatározására.
- a küldő IP címéhez tartozó szervezet meghatározása még nem feltétlenül utal a tényleges elhelyezkedésre. Elképzelhetők olyan hálózatok, amelyeket – bár ugyanaz a tulajdonosa - kisebb részekre darabolnak, és ezek különböző helyeken (akár különböző országokban is) üzemelnek.
- A domain név nem feltétlenül utal a végpont földrajzi elhelyezkedésére (egy .hu végű domain a világ bármelyik részén lehet).

A Microsoft kutatói több botnet felderítési kísérletet is végeztek már a Hotmail levelezőrendszerben detektált kéretlen levelek alapján [118], [119]. Az általuk végzett vizsgálat főként a hálózati szintre korlátozódott, a rendelkezésükre álló hatalmas adatmennyiség segítségével pontos és többrétű elemzést tudtak lefolytatni.

Az ellenintézkedések - a kéretlen levelet küldő számítógép fertőzöttségének megszüntetése, vagy a hálózati forgalomból kiszűrése - végrehajtásához nagy segítséget nyújt, ha ismert a számítógép földrajzi, illetve hálózati szolgáltatón belüli elhelyezkedése. Idegen országban működő számítógép esetén lehetséges az adott ország megfelelő szervezeteit értesíteni, hazai hálózatok esetén pedig közvetlenül a hálózatot

birtokló szolgáltatót. Sajnos az IP hálózatok címeinek kiosztása semmilyen közvetlen kapcsolatban nincs az adott hálózat földrajzi elhelyezkedésével. Az IP címek kisebb, összefüggő területekből állnak, amely területeket bárki megvásárolhatja és használhatja. Ezek a területek különböző méretűek, ráadásul egy tulajdonos több, nem összefüggő területet is megvásárolhat. Szerencsére léteznek olyan adatbázisok, amelyek az IP címtartományokat és azok földrajzi elhelyezkedését tartalmazzák. Az esettanulmányban a MaxMind nevű cég GeoIP adatbázisának június elsejei kiadását használtam fel, annak is a GeoLite City változatát. Ez utóbbi ingyenes termék (a GeoIP előfizetéses) és 4 105 731 hálózat adatait tartalmazza. A hálózatokat az IP címtartomány kezdete és vége azonosítja. Mindegyik, ebben szereplő IP hálózatot egy földrajzi helyhez rendelték, míg a földrajzi helyekhez (245 831 darab) a következő adatok tartoznak:

- országkód;
- városkód;
- városnév;
- szélességi fok;
- hosszúsági fok.

Vagyis, az adatbázis segítségével lehetséges egy IP címet városhoz és térképen megjeleníthető ponthoz rendelni. Az adatbázist előállító cég szerint az ingyenes változat 99,5% pontosságú ország, míg 79% pontosságú város szinten, 25 mérföldes körben értelmezve. Ezek az adatok az USA hálózataira igazak, a világ többi részére nincs ilyen mérőszám. Természetesen léteznek más, hasonló célt szolgáló adatbázisok is [120], [121], sőt, véleményem szerint egy megfelelő állami apparátus segítségével a magyar szolgáltatókra érvényes változatot is lehetséges lenne összeállítani, és napra készen tartani.

Bár a térinformatikai rendszereket többnyire nem ilyen célra alkalmazzák, a jelenlegi, fejlett változatok egyszerű módszerekkel képesek többféle bemeneti formátumot használva együttműködni más rendszerekkel. A bemeneti formátumnak megfelelő állományok segítségével lehet pontokat kijelölni, amiket az alkalmazás aztán elhelyez a térképen. Az együttműködéshez az is szükséges, hogy a Föld gömbölyű voltából adódó ábrázolási problémákat azonos módon kezeljék. A GeoIP a WGS 84 (World Geodetic System) ábrázolásmódot használja, tehát a megfelelő együttműködéshez olyan térinformatikai alkalmazás szükséges, amely ismeri ezt a szabványt. A komoly tudással rendelkező fizetős alkalmazások fő problémáját a felhasználható térképek választéka

jelenti, de könnyen találhatunk ingyenes, egyszerű programozó felülettel rendelkező megoldást is. A teljes, részletes világtérképhez jutás problémáját egyszerűen kiküszöbölhetjük a weben elérhető térinformatikai megoldásokkal. A jelentősebb ilyen megoldások (a Microsoft Bing Maps [122], a Yahoo Map [123] és a Google Maps [124]) mindegyike rendelkezik programozói felülettel (API), amely segítségével bárki készíthet olyan térinformatikai alkalmazást, amely hozzáfér a teljes térképháttérhez, sőt, még műholdképekhez is. Hátrányuk, hogy csak online kapcsolat segítségével elérhetők, mivel a térképadatokat az üzemeltetők számítógépes rendszerei tárolják, a felhasználó csak a számára szükséges szeletekhez férhet hozzá.

Google Maps API

A kísérleti modell megvalósítása során választásom a Google Maps rendszerre esett, ennek oka főként a szélesebb támogatottság és emiatt a fellelhető példa alkalmazások nagyobb száma volt. Az API használata egyszerű: első lépésként egy kulcsot (egy szöveges azonosító, amely a felhasználási jogot adja meg a weboldal számára) kell igényelni, és máris használatba vehető a rendszer. Az alkalmazást JavaScript nyelven kell elkészíteni, a keretprogram a Google weboldaláról tölthető be, ez tartalmazza a térkép használatához szükséges osztályok (class) definícióit. A legfontosabb objektum a térkép objektum, amelyet a GMap2 osztályból lehet származtatni. Az objektumnak létrehozáskor meg kell adni azt a HTML szakasz azonosítót, amely a térképet fogja tartalmazni. A térképobjektumhoz tetszőleges számú vezérlőeszköz (nagyítás, kicsinyítés, térképtípus váltó gombok, stb…) adható, így a kezelőfelület is könnyen az igényekhez szabható.
A térkép definiálását és megjelenítését a következő függvény végzi:

```
function map_on() {
      if (GBrowserIsCompatible()) {
            map = new GMap2(document.getElementById("map"));
            map.setMapType(G_NORMAL_MAP);
            map.addControl(new GLargeMapControl());
            map.addControl(new GScaleControl());
            map.enableScrollWheelZoom();
            map.disableDoubleClickZoom();
      }
}
```

A térképen elhelyezkedő pontok megkereséséhez a legegyszerűbb módszer a szélességi és hosszúsági adatok megadása, ehhez a „GLatLng(szélesség, hosszúság)” osztály nyújt

segítséget. A szélességi és hosszúsági értékek fokokban, tizedes tört alakban (tehát nem szögmásodperc, hanem tized, század, ezred fok) adhatók meg.
Az így keletkező földrajzi pont objektum aztán elhelyezhető a térképen. Ha ezt a földrajzi pontot meg szeretnénk jelölni a térképen, akkor egy markert kell elhelyezni rajta, amihez rendelhetünk grafikát, a földrajzi koordinátáit, illetve egy eseménykezelőt, ami a különböző felhasználói aktivitást szolgálják ki (kattintás, dupla kattintás, vonszolás). A spamküldő bot kliensek koordinátáit ilyen markerek segítségével helyeztem el a térképen, a következő függvény segítségével:

```
function insertPoint(latitude, longitude, comment) {
      var coord = new GLatLng(latitude,longitude);
      map.setCenter(coord);
      var baseIcon = new GIcon();
      baseIcon.iconSize=new GSize(32,32);
      baseIcon.shadowSize=new GSize(56,32);
      baseIcon.iconAnchor=new GPoint(16,32);
      baseIcon.infoWindowAnchor=new GPoint(16,0);
      var icon = new GIcon(baseIcon, "marker.png", null,
"shadow.png");
      var botloc = new GMarker(coord,icon);
      GEvent.addListener(botloc, "click", function() {
            marker.openInfoWindowHtml(comment);});
      map.addOverlay(botloc);
}
```

A markerek segítségével jelöltem be a térképen a botnet kliensek helyét, természetesen nem egyenként, hanem csoportosítva. A csoportosítás háromféle volt:

- Világméretű: a küldő számítógépek IP címeit a GeoIP adatbázisa alapján országonként csoportosította az alkalmazás, majd az országokban előforduló egyik város koordinátáját felhasználva helyezte el a markert. Lehetett volna egyedi, országokra jellemző pontokat választani markerhelynek, de ez szükségtelenül sok plusz munkát jelentett volna (a világ összes országában be kellett volna jelölni a fővárost).
- Európai szintű: a küldő számítógépek IP címei közül az alkalmazás kigyűjtötte az európai országokat, majd országonként összesítette. A marker elhelyezése az adott ország fővárosának koordinátájára történt. Ehhez készítettem egy európai fővárosok adatait tartalmazó adatbázist.
- Magyarországi szintű: az alkalmazás csak a magyarországi hálózatokból érkezett kéretlen levelek IP címeit szűrte, majd városonként összegezte. A marker elhelyezése a városok koordinátája alapján történt.

Valamennyi mód esetében, áttekinthetőségi okokból csak a 100 legaktívabb küldő ábrázolása történt meg.

Esettanulmány

A kísérleti rendszer kipróbálásához szükség volt bemenő adatra is. Ehhez saját levelezőszerveremen több éve működő szűrőprogram adatait használtam fel, amelyet több milliónyi elektronikus levél szűrési naplójából állítottam elő. A feldolgozás első részében egy erre a célra írt egyszerű script segítségével a tárolt elektronikus levél fejlécek alapján egy adatbázis táblába gyűjtöttem a levelek feladóinak (akiket potenciálisan botnet tagnak tekintettem) IP címeit. Takarékossági okokból csak a 2007. január és 2009. május közti adatokat dolgoztam fel, a rekordok száma még így is 1184620 lett. A címek közül töröltem az ismertebb ingyenes levelezőrendszerekből érkezetteket. Ennek oka az, hogy 2008-ban spammerek sikeresen áttörték az automatikus, gépek által végzett regisztrációt megakadályozó CAPTCHA (a Completely Automated Public Turing Test To Tell Computers and Humans Apart kifejezés rövidítése) védelmi rendszert [125]. A GeoIP hálózati tartományokat tartalmazó adatbázisának segítségével lehetségessé vált az IP címekhez földrajzi elhelyezkedést rendelni. A hozzárendelés két lépcsős, a hálózatok adatbázisa csak egy földrajzi hely azonosítót tartalmaz, ez az azonosító aztán egy másik adatbázisban (location) a tényleges földrajzi adatokra mutat. Itt merült fel az első probléma, a rengeteg adat és a nehezen optimalizálható keresési metódus miatt a második lépés feldolgozási időigénye hatalmasra duzzadt, így valós idejű statisztikák készítésére csak elfogadhatatlanul nagy erőforrás felhasználás mellett lett volna lehetőség. Ezért ezt a lépést nem a statisztika készítésekor végzi az alkalmazás, hanem az IP címek feldolgozása során a rekordok egészülnek ki egy location ID mezővel, amelynek feltöltése is ekkor történik meg. Ez a probléma csak a kísérleti modell megalkotásához, általam használt eljárás nehézségéből adódott, lehetséges ennél sokkal jobban optimalizált változatot is készíteni.

Az így előálló adatbázis már könnyen és viszonylag gyorsan kezelhető, egy egyszerű PHP script képes a kívánt adatokat kigyűjteni, majd a megjelenítést végző JavaScript programnak átadni.

A próbarendszer felületét az alábbi ábra mutatja:

Terület: Magyarország Év: 2009 Hónap: Május Frissítés

Város	Szélesség	Hosszúság	Darab
Budapest	47.500000	19.083300	139
Oroszlány	47.483300	18.316700	15
Szeged	46.250000	20.166700	7
Ács	47.700000	18.016700	6
Rakamaz	48.133300	21.466700	5
Kazincbarcika	48.250000	20.633300	4
Jászberény	47.500000	19.916700	3
Dunakeszi	47.633300	19.133300	3
Budaörs	47.450000	18.966700	3
Vecsés	47.400000	19.283300	2
Székesfehérvár	47.200000	18.416700	2
Esztergom	47.800000	18.750000	2
Kiskunfélegyháza	46.713600	19.852200	2
Edelény	48.300000	20.733300	2

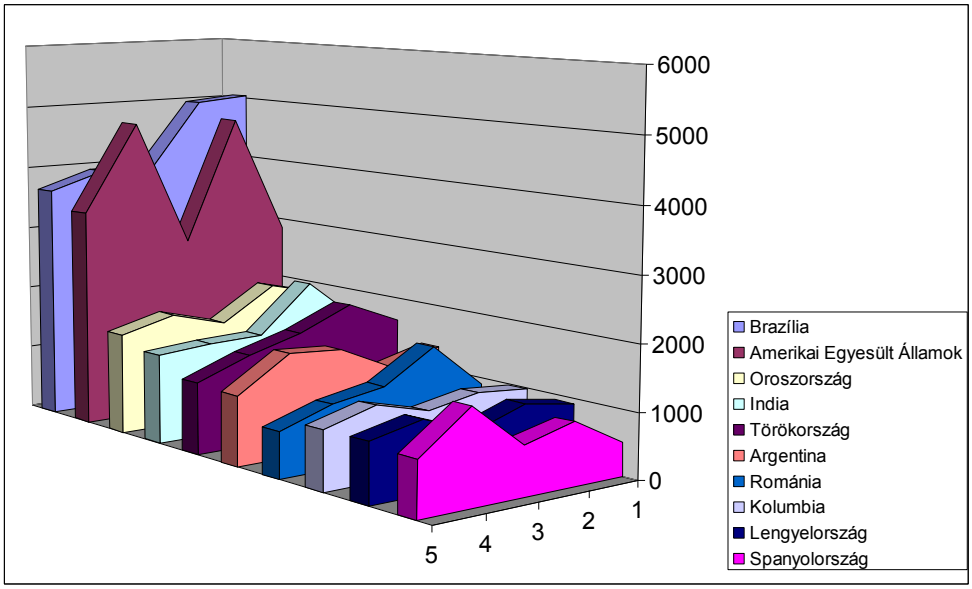
19. ábra Magyarország botnet fertőzöttsége 2009. májusban (készítette a szerző)

Fertőzöttségi térképek

Az elkészült alkalmazás segítségével gyorsan és egyszerűen lehet fertőzöttségi térképeket készíteni, amelyek a fertőzött végpontok földrajzi elhelyezkedését tartalmazzák.

20. ábra Európa botnet fertőzöttsége országokra lebontva 2009. májusban (készítette a szerző)

21. ábra A világ botnet fertőzöttsége országokra lebontva 2009. májusban (készítette a szerző)



22. ábra Országok botnet fertőzöttsége 2009 első 5 hónapjában (készítette a szerző)

Meglepő módon a statisztikát Brazília vezeti, az Egyesült Államok és Oroszország előtt. A fenti ábra a 2009. évből eltelt 5 hónap adatai, 158000 darab IP cím feldolgozása alapján készült, természetesen nem reprezentatív, hiszen csak az általam észlelt kéretlen levelek elemzését tartalmazza.

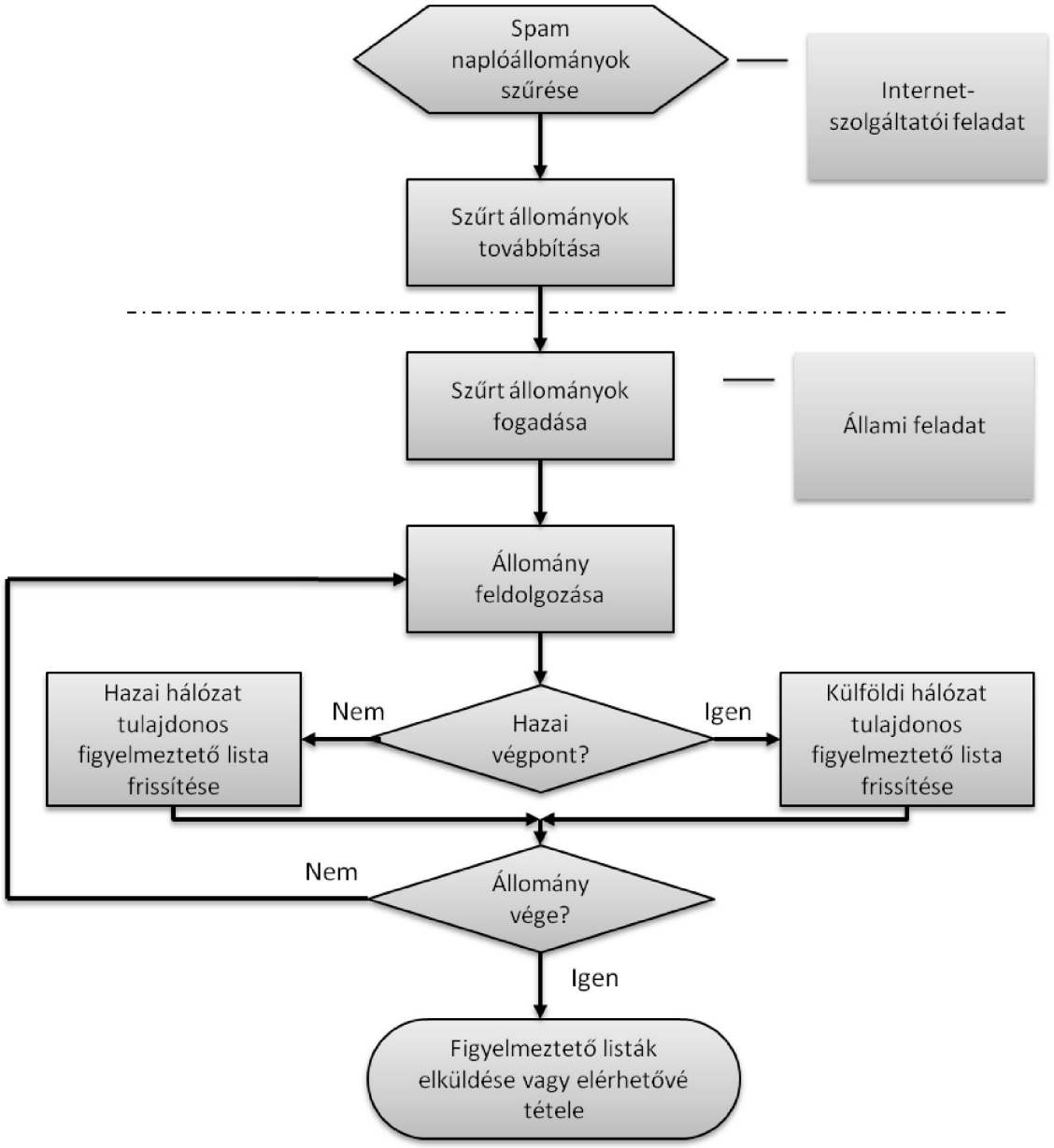
4.5 Proaktív botnet felderítő rendszer

Az általam javasolt rendszer szerint a módszert a hazai internet-szolgáltatók alkalmazhatnák működésük során, a saját – tehát nem speciálisan adatgyűjtési céllal üzemeltetett – levelezőrendszereikben meglévő, a kéretlen levelek küldőinek hálózati címét tartalmazó rekordokat adatbázisba szervezve. Ebben az adatbázisban a vizsgálati időszak alatt fogadott kéretlen levél küldőjének címe, és a küldés időpontja szerepelne. Az érintett IP cím csak egyszer, a legutolsó időponttal szerepel, így csökkentve a szükségtelen redundanciát. A keletkezett adatbázist egy állami felügyelet alatt álló szervezetnek juttatnák el naponta, vagy néhány napos időközönként. Ez a szervezet összegezné a listákat, majd a rendelkezésre álló hálózattérképek alapján szétválogatná hazai tulajdonú végpontokra, illetve külföldi végpontokra. A hazai végpontokat szolgáltatói szintre lebontva eljuttatná az érintett hálózatok tulajdonosainak, akik így képesek lennének azokat semlegesíteni. A külföldi végpontok listáját a nemzetközi kapcsolatokon keresztül a Nemzeti Hálózatbiztonsági Központ továbbíthatná az érintett országok hálózatbiztonsági központjainak.
Az ilyen tevékenységre egyébként a 223/2009. (X. 14.) Korm. rendelet 9§ 1. bekezdésének d) pontja meg is adja a felhatalmazást:

„d) A Központ - a központi rendszer üzemeltetőjétől a központi rendszer működtetője felhatalmazásával átvett információk és adatok alapján - folyamatosan megfigyeli és kiértékeli az internet forgalmat beavatkozásra utaló jeleket keresve, továbbá a folyamatos ügyeleti rendszerén keresztül szükség esetén értesíti a központi rendszer működtetőjét, valamint a hazai és nemzetközi hálózatbiztonsági és kritikus információs infrastruktúra védelmi szervezeteket a gyanús tevékenységekről.”

DOI azonosító: 10.17625/NKE.2012.008

Az ismertetett algoritmus folyamatábrája:



23. ábra A proaktív botnet felderítő rendszer folyamatábrája (készítette a szerző)

4.6 Következtetések

Kutatásaim segítségével bizonyítottam, hogy egy botnet tagjai jelentős, felderíthető tevékenységet folytatnak. Ehhez az általam üzemeltetett internetes levelezőszerver által generált adatokat vizsgáltam át és elemeztem. Irodalomkutatás segítségével igazoltam, hogy az elektronikus levelezés által alkalmazott adatátviteli módszer nagy bizonyossággal kizárja a feladó hálózati címének hamisítását, így a kéretlen levelek feladóiról eldönthető, hogy egy botnet tagjai.

Ezekre az alapelvekre építve felvetettem egy proaktív rendszer létrehozásának lehetőségét. Feltevésem működőképességének igazolására kísérleti modellt alkottam, amely valóságos adatok segítségével képes meghatározni botnet kliensek elhelyezkedését. A kísérleti modellben a térinformatika eszközeivel egy megoldást mutattam be a botnet kliensek földrajzi helyének megállapítására.
Egy lehetséges algoritmust alkottam, amellyel a jelenleg rendelkezésre álló technikai eszközök kismértékű fejlesztésével ütőképes felderítő mechanizmus készíthető. Megállapítottam, hogy ehhez a következő problémákat kell megoldani:

- A hazai internet-szolgáltatók által alkalmazott kéretlen levél-szűrő rendszerekre implementált adatfeldolgozó alkalmazások elkészítése.
- A hazai internet-szolgáltatókra vonatkozó jogszabályi környezet módosítása, az adatszolgáltatási kötelezettség előírása számukra.
- Az adatokat begyűjteni hivatott szervezet életre hívása, vagy egy meglevő szervezet hatáskörének megnövelése. Véleményem szerint a Nemzeti Hálózatbiztonsági Központ meglevő jogosultságai, képességei és erőforrásai alapján alkalmas erre a feladatra.
- Magyarország internetes hálózati térképének létrehozása és naprakészen tartása.

ÖSSZEGZETT KÖVETKEZTETÉSEK

Életünkben egyre nagyobb szerepet kapnak a számítógépes hálózatok, amelyek védelme alapvető fontosságú, nem csak a kritikus információs infrastruktúrák esetében, de minden egyéb területen is. A nyilvános hálózatok és az általuk összekötött hálózati végpontok együttesen egy olyan virtuális teret – kiberteret – alkotnak, amelyen már jelenleg is komoly veszélyeket jelentő tevékenység zajlik. A legelterjedtebb nyilvános számítógépes hálózatot – az internetet – bűnözők, terrorista szervezetek használják információcserére, adatok eltulajdonítására, információs infrastruktúrák működésképtelenné tételére. A katonai doktrínák változása azt jelzi, hogy a hadseregek is egyre nagyobb figyelmet szentelnek a kibertérnek, ez pedig egy információs infrastruktúrák elleni, tisztán számítógép-hálózati eszközökkel előidézett konfliktus veszélyességét is megnöveli. Egy kibertérben kezdődő konfliktus eszkalálódhat, és akár államok közti fegyveres akcióvá is alakulhat.

Megjelentek az olyan számítógépes kártevők, amelyek már nem csak informatikai eszközöket veszélyeztetnek, hanem más kritikus infrastruktúrában is képes anyagi károkat okozni, emellett létrejöttek olyan nagyméretű hálózatok, amelyek összehangolt akciókra is képesek. **Megvizsgáltam korábbi kibertámadások statisztikáit, és megállapítottam, hogy az ismertté vált akciók mintegy 22%-át egy speciális módszerrel, a túlterheléses DoS támadások képezték.** A DDoS, és különösen a reflektív DDoS támadási módszerek rendkívül hatásosak, több olyan nagyléptékű esemény is történt, amelyek során a támadások több héten keresztül tartottak, így a szolgáltatás kieséséből származó veszteség is jelentős volt. Megtörtént DDoS támadások elemzésével arra a következtetésre jutottam, hogy az ilyen típusú akciók elleni védekezés első lépéseként a megtámadottnak fel kell ismernie azt a tényt, hogy támadás alatt áll. Ehhez fontos a támadási módszerek és azok sajátosságainak ismerete, ezért **felállítottam egy átlátható keretrendszert, majd irodalomkutatás segítségével összegyűjtöttem a leggyakrabban használt eljárásokat**. Az eljárásokat három fő csoportba soroltam:

- DoS támadások.
- DDoS támadások.
- Reflektív DDoS támadások.

A legnagyobb támadó potenciállal a reflektív DDoS támadások rendelkeznek, amelyek közül a DNS kiszolgálókat felhasználó módszer ellen a legnehezebb védekezni.

A támadási módszerek kategorizálására javasoltam az ISO OSI referenciamodell egyes rétegeit, aszerint, hogy a támadó a célpont melyik rétegében működő folyamatok túlterhelésére törekszik.

A védelmi módszerek elemzése azt bizonyítja, hogy a DDoS támadás ideje alatt az áldozat rendszerének működőképességét fenntartani – vagyis megelőzni a szolgáltatás kiesését – ésszerű erőforrás-gazdálkodás segítségével nem lehetséges. Mivel egy ilyen incidens során a célpont erőforrásai (számítási kapacitás, hálózati sávszélesség) és a támadók erőforrásainak összessége ütközik egymással, ezért a védelemnek előre fel kellene készülnie az ismeretlen nagyságú kapacitást használó támadásra. A támadónak ezzel szemben a célpont meglévő kapacitásaira kell csak méreteznie az erőforrásokat, ráadásul az akciót kivitelező hálózati végpontok akár menet közben is bővíthetők újabb tagokkal, így egyszerűen növelhető a támadás intenzitása. Az informatikai rendszereket általában a normál üzemi működésre méretezik, ésszerű tartalékok biztosításával. Semmilyen szempontból nem tekinthető gazdaságosnak a normál működés sokszorosára méretezni a rendszer kapacitását, ráadásul az sem biztos, hogy ez elegendő a rendszer működésének fenntartására extrém nagy terhelés mellett.

Egy másik, elterjedt védelmi módszer a támadáshoz használt adatfolyamok tipizálása után, ezek kiszűrésén alapszik, vagyis igyekszik meggátolni a támadó által generált adatok célponthoz történő eljutását. **A DDoS és reflektív DDoS technikák vizsgálata alapján megállapítottam, hogy léteznek olyan technikák, amelyek ellen a hálózati forgalom szűrése nem kivitelezhető, mivel ez az informatikai rendszerek üzemszerű működését is gátolnák.**

Mindezek alapján bizonyítottnak látom, hogy a DDoS támadások elleni védekezés tisztán passzív eszközökkel – erőforrás növelés illetve adatfolyam szűrés – **nem vitelezhető ki ésszerű erőforrás felhasználás mellett**, ezért a támadó végpontok semlegesítését tekintem a leghatásosabb megoldásnak. A reaktív – tehát a támadást megszüntetni igyekvő – védelmi módszerek jelenleg is használatosak, és a hálózati szolgáltatók nemzetközi együttműködésén alapszanak. Bár a módszer hatásos, de ebben az esetben a problémát az időtényező okozza. Nagyszámú támadó végpont esetén sok időbe telik ezek azonosítása, majd a kiinduló hálózat tulajdonosának közreműködésével történő semlegesítése. Egy megindult támadás esetén ez az idő a célpont kiesésének

időtartamát, így a bekövetkező károkat is növeli. Emiatt olyan módszerek kutatására összpontosítottam, amely segítségével a DDoS akciók potenciális eszközeit még egy támadás megindulása előtt lehet felkutatni, és semlegesíteni.

A DDoS támadások veszélyességének illusztrálására elkészítettem egy képzeletbeli, kizárólag a kibertérben végrehajtott komplex informatikai támadás forgatókönyvét. Központi elemeként a kritikus információs infrastruktúrák, vagyis az energiaellátás és a telekommunikáció elleni akciókat jelöltem meg. Veszélyes folyamatként értékeltem a mobil kommunikációs eszközök, elsősorban a mobiltelefonok informatikai biztonságának hiányosságait.

A DDoS támadások vizsgálatával megállapítottam, hogy az ilyen jellegű támadásokért leginkább számítógépes kártevőkkel fertőzött gépekből kialakított, központi felügyelet alatt álló hálózatok, úgynevezett botnetek felelősek. A botnetek vezérlési (Command & Control) csatornáinak kommunikációs módszere szerint elkülöníthető architektúrák vizsgálatával arra következtetésre jutottam, hogy vannak létező eljárások a felderítésre. Azonban ezek sokszor a felhasználók adatforgalmának figyelésével és emiatt személyiségi jogaik sérülésével járhatnak, ráadásul a számítógépes hálózatokba telepített speciális eszközök használatát teszik szükségessé. Feltételeztem, hogy a botnetek tevékenysége nem csak a DDoS támadások kivitelezésére terjed ki, ezért megvizsgáltam az egyéb irányú felhasználásukat is. **Igazoltam, hogy ezek működése olyan nyomokat is hagy, amelynek vizsgálatával meghatározhatók a kliensek elérhetőségi paraméterei**, így megnyílik a lehetőség a semlegesítésükre. Kutatómunkám során arra a következtetésre jutottam, hogy az adatlopások, különböző személyiség eltulajdonítási módszerek mellett a leggyakoribb felhasználási területük a kéretlen reklámlevél (népszerű nevén SPAM) nagy mennyiségű küldése. A botnetek tulajdonosai ebből a tevékenységből tudnak a legbiztosabban bevételhez jutni, aminek eredményeképpen az internet forgalmának jelentős hányadát ezek teszik ki, ezért véleményem szerint a legegyszerűbben felhasználható módszer a kéretlen levelek küldésére specializálódott botnetek nyomainak vizsgálata.

Az elektronikus levelezés által használt TCP protokoll vizsgálata után megállapítottam, hogy a botnetek által egyébként előszeretettel használt címhamisítási eljárások itt nem működőképesek, ezért a levelező rendszerekből kinyert adatok felhasználhatók a kliensek hálózatban elfoglalt valós helyének azonosítására. A kéretlen levelek szűrését már nagyon sok szolgáltató végzi, aminek köszönhetően a kéretlennek bizonyult levelek feladóinak hálózati címe folyamatosan rendelkezésre áll, azok megszerzésére nem

szükséges külön hálózati vagy egyéb informatikai eszközöket telepíteni. A kéretlen levelek küldői között elsöprő többségben vannak a botnetek tagjai, tehát egy kéretlen levél küldőjének hálózati címe egyben egy botnet tagjának hálózati címét is jelenti. Egy, a kéretlen levelek forrásainak meghatározására használható rendszer kifejlesztéséhez **kísérleti modellt alkottam, amely a levelezőszerverekben egyébként is képződő adatok vizsgálatával képes botnetek klienseinek nyomára bukkanni**. **Működőképességének bizonyítására implementáltam a modell funkcióit**, majd a számítógépes program segítségével mintegy másfél millió, valós levélszűrés segítségével készített adatot vizsgáltam át. Az így nyert listák és a helymeghatározásra alkalmas adatbázis összevetésével bizonyítottam, hogy egy kellően pontos és naprakész adatbázis segítségével akár még földrajzi elhelyezkedés is megállapítható, de véleményem szerint a leghatékonyabb módszer a végpontok hálózati szolgáltatóját azonosító adatbázissal összevetés lehet.

A kísérleti modellel nyert tapasztalatokra alapozva felvetettem egy proaktív, tehát megelőző jellegű eljárás lehetőségét. Kutatásaim során arra a következtetésre jutottam, hogy erre egy államilag koordinált, a hazai internet-szolgáltatókat érintő rendszer a legmegfelelőbb. A rendszerhez csatlakozott internet-szolgáltatók saját elektronikus levélszűrési naplóállományukból gyűjtik ki a kéretlen levelek küldőinek hálózati címét, amelyet az alapvető szűrési feladatok – ismétlődések kiszűrése – után küldenek a koordinálást végző szervezethez. Itt történik meg a naplóállományban található hálózati címek feldolgozása, melynek során elkülönítik a hazai és a külföldi tulajdonú hálózatokhoz tartozókat. A hazai szolgáltatókhoz ezután közvetlenül jut el a veszélyesnek minősített címek listája, akik ez alapján megtehetik a semlegesítéshez szükséges lépéseket. A külföldi szolgáltatók számára a külföldi együttműködő szervezeteken keresztül jut el az információ. A módszer nagymértékben automatizálható és a rendelkezésre álló adatokra támaszkodik. Az internet-szolgáltató által küldött lista anonim, csak végpont hálózati címeket tartalmaz, így adatvédelmi szempontból sem látom aggályosnak.

ÚJ TUDOMÁNYOS EREDMÉNYEK

Értekezésem új tudományos eredményeinek az alábbiakat tekintem:

1. Valós esetekben használt támadási és védelmi módszerek elemzésével **megállapítottam, hogy egy megindult DDoS támadás során csak aránytalanul sok erőforrás bevonásával lehet fenntartani** a szolgáltatás folyamatosságát, így az ilyen védelmi eljárások önmagukban nem hatékonyak.

2. **A DDoS támadások módszereire osztályba sorolást** – külön kategóriára bontást - **dolgoztam ki**, amelyek segítségével az ilyen támadások elleni védelmi intézkedések megtétele nagymértékben hatékonyabbá tehető.

3. **A** túlterheléses támadásokért felelős **botnetek működésének elemzése után megalkottam ezek tagjainak passzív adatgyűjtési technika segítségével működő felderítési módszerét**.

4. **Kísérleti modellt alkottam** a botnet kliensek tevékenységének – kéretlen levelek küldésének nyomai – elemzésére, és helyük meghatározására, majd a megalkotott kísérleti modellel **bizonyítottam**, hogy **lehetséges proaktív módon felderíteni és semlegesíteni a DDoS támadásra használható végpontokat** (SPAM küldő végpontok) anélkül, hogy személyiségi és adatvédelmi jogokat sértenénk.

5. **Egy** olyan megvalósítható **rendszer alapjait dolgoztam ki, amely** az ismertetett eljárás segítségével **azonosítja a botnet klienseket**, majd az internet-szolgáltatók bevonásával **semlegesíti azokat**.

AJÁNLÁSOK

Munkám során igyekeztem kellő alapossággal körüljárni a kibertérben előforduló veszélyforrásokat, azon belül is a DDoS támadások és az ezeket megvalósítani képes botnetek problémáját. Értekezésem egészét javaslom felhasználni a felsőoktatásban, a számítógép-hálózati támadásokkal kapcsolatos tantárgyak keretében.

Az értekezésemben szereplő kategorizált DDoS támadási módszerek segítséget nyújthatnak az ilyen támadások felismerési idejének csökkentésére, a gyorsabb és a támadáshoz leginkább illeszkedő védelmi módszer kiválasztáshoz, ezért szakmai továbbképzések kiegészítő anyagaként is felhasználható.

Az általam javasolt proaktív védelmi módszer kiépítésekor felhasználható alap irodalomként.

Budapest, 2011. november 14.

Gyányi Sándor

TÉMAKÖRBŐL KÉSZÜLT PUBLIKÁCIÓIM

Lektorált folyóiratban megjelent cikkek

[GyS-1] DDoS támadások és az ellenük való védekezés
(Hadmérnök, 2008. február, különszám)
http://www.zmne.hu/hadmernok/kulonszamok/robothadviseles7/gyanyi_rw7.html
ISSN 1788-1919

[GyS-2] Cyber-támadások elleni védekezés és a válaszcsapások lehetőségei
(Hadmérnök III. évfolyam, 2. szám, 2008. június 114-128p)
ISSN 1788-1919

[GyS-3] Botnetek felkutatása a térinformatika segítségével
(Hadmérnök IV. évfolyam 3. szám, 2009. szeptember 248-257p)
ISSN 1788-1919

[GyS-4] Elektronikus hadviselés a civil világban 1.
(Biztonság, 2008/5 36-38p)
ISSN 0864-9189

[GyS-5] Elektronikus hadviselés a civil világban 2.
(Biztonság, 2008/6 36-40p)
ISSN 0864-9189

[GyS-6] Informatikai WLAN-hálózatok zavarása
(Bolyai Szemle, 2009. április, 119-132p)

Idegen nyelvű kiadványban megjelent cikkek

[GyS-7] Next Generation Viruses
28th International Conference June 3-4, 2010.
Sience in Practice kiadvány, Subotica, Serbia

Konferencia kiadványban megjelent előadás

[GyS-8] Az információs terrorizmus fegyverei és módszerei
(Biztonságtechnikai szimpózium kiadványa, ISBN 978-963-7154-68-3, 2007. november)

FELHASZNÁLT IRODALOM/IRODALOMJEGYZÉK

[1] **Munk Sándor:** INFORMÁCIÓBIZTONSÁG VS. INFORMATIKAI BIZTONSÁG. *Hadmérnök.* [Online] 2007. november 27. [Letöltve: 2011. november 11.] http://hadmernok.hu/kulonszamok/robothadviseles7/munk_rw7.html. ISSN 1788-1919.

[2] **Munk Sándor:** *KATONAI INFORMATIKA II.* Budapest : Egyetemi jegyzet, 2006. old.: 21.

[3] **Horvayné Fehér Judit, Munk Sándor:** A RENDŐRSÉGI INFORMATIKAI HÁLÓZAT FOGALMA,RENDELTETÉSE. *Hadmérnök.* [Online] 2011. június. [Letöltve: 2011. november 11.] http://www.hadmernok.hu/2011_2_horvayne_munk.pdf. ISSN 1788-1919.

[4] **Haig Zsolt, Várhegyi István:** *Hadviselés az információs hadszíntéren.* Budapest : Zrínyi Kiadó, 2005. old.: 73. ISBN 963-327-391-9.

[5] **Haig Zsolt, Várhegyi István:** *Hadviselés az információs hadszíntéren.* Budapest : Zrínyi Kiadó, 2005. old.: 186. ISBN 963-327-391-9.

[6] **Peter Hayes:** No 'sorry' from Love Bug author. *The Register.* [Online] május 11, 2005. [Letöltve: június 25, 2011.] http://www.theregister.co.uk/2005/05/11/love_bug_author/.

[7] **Neil Doyle:** *TERROR BASE UK.* 7 Albany Street, Edinburgh : Mainstream Publishing Company (Edinburgh) LTD., 2006. ISBN 1 84018 994 0.

[8] **Philip Zimmermann:** Phlip Zimmermann weboldala. [Online] [Letöltve: június 25, 2011.] http://www.philzimmermann.com/EN/background/index.html.

[9] **Erik Schechter:** Cyber catch-up. *C4 ISR Journal.* [Online] március 6, 2008. [Letöltve: augusztus 4, 2011.] http://www.c4isrjournal.com/story.php?F=3240557.

[10] **Bakos Ferenc:** *Idegen szavak és kifejezések.* Budapest : Akadémiai Kiadó, 2007. ISBN 9789630578752.

[11] **Ács Tibor, Amaczi Viktor:** *Hadtudományi Lexikon.* Budapest : Magyar Hadtudományi Társaság, 1995. ISBN 963-04-5226-X.

[12] **Kevin Coleman:** Cyber Terrorism. *Computer Crime Research Center.* [Online] [Letöltve: július 5, 2011.] http://www.crime-research.org/library/Cyberterrorism.html.

[13] **National Consortium for the Study of Terrorism and Responses to Terrorism:** Terrorist Organization Profile: Internet Black Tigers. [Online] University of Maryland. [Letöltve: július 13, 2011.] http://www.start.umd.edu/start/data_collections/tops/terrorist_organization_profile.asp?id=4062.

[14] **U.S. Department of Justice:** Juvenile Computer Hacker Cuts Off FAA Tower at Regional Airport. *www.cybercrime.gov.* [Online] [Letöltve: július 13, 2011.] http://www.cybercrime.gov/juvenilepld.htm.

[15] **Brian Krebs:** Web Sites Vandalized With Antiwar Messages. *SecurityFocus.* [Online] március 3, 2003. [Letöltve: július 13, 2011.] http://www.securityfocus.com/news/3288.

[16] **Kevin Poulsen:** South Pole 'cyberterrorist' hack wasn't the first. *The Register.* [Online] 2004. augusztus 19. [Letöltve: 2011. július 13.] http://www.theregister.co.uk/2004/08/19/south_pole_hack/.

[17] **Sandova, Greg:** FBI probes 4chan's 'Anonymous' DDoS attacks. *cNet News.* [Online] 2010. november 9. [Letöltve: 2011. július 13.] http://news.cnet.com/8301-31001_3-20022264-261.html.

[18] **Graham Cluley:** Egypt versus the internet - Anonymous hackers launch DDoS attack. *Naked Security.* [Online] Sophos, január 26, 2011. [Letöltve: július 13, 2011.] http://nakedsecurity.sophos.com/2011/01/26/egypt-versus-the-internet-anonymous-hackers-launch-ddos-attack/.

[19] **Yassin Musharbash:** What al-Qaida Really Wants. *SPIEGEL ONLINE.* [Online] december 8, 2005. [Letöltve: július 12, 2011.] http://www.spiegel.de/international/0,1518,369448,00.html.

[20] **Gordon Corera:** The world's most wanted cyber-jihadist. [Online] BBC News, január 16, 2008. [Letöltve: augusztus 4, 2011.] http://news.bbc.co.uk/2/hi/americas/7191248.stm.

[21] **Jeremy M. Sharp:** Lebanon: The Israel-Hamas-Hezbollah Conflict. *Congressional Research Service.* [Online] szeptember 15, 2006. [Letöltve: július 12, 2011.] http://www.fas.org/sgp/crs/mideast/RL33566.pdf.

[22] **FOX News:** Al Qaeda Blamed for Terror Attack Outside U.S. Consulate in Turkey. [Online] július 9, 2008. [Letöltve: július 12, 2011.] http://www.foxnews.com/story/0,2933,378346,00.html.

[23] **HVG:** Arab forradalmak: a fiú, aki feldöntötte az első dominót. *hvg.hu.* [Online] 2011. február 23. [Letöltve: 2011. július 12.] http://hvg.hu/vilag/20110222_arab_forradalmak_bouazizi.

[24] **QASSIM ABDUL-ZAHRA:** Al-Qaida in Iraq: 100 attacks to avenge bin Laden. *Yahoo! News.* [Online] augusztus 20, 2011. [Letöltve: augusztus 21, 2011.] http://news.yahoo.com/al-qaida-iraq-100-attacks-avenge-bin-laden-111715889.html.

[25] **Déri Zoltán, Lobogós Katalin, Muha Lajos, Sneé Péter, Váncsa Julianna:** *Informatikai Biztonsági Irányítási Követelmények.* Budapest : Közigazgatási Informatikai Bizottság, 2008.

[26] **Edgar G. Amoroso:** *Fundamentals of Computer Security Technology.* Prentice Hall, 1994. ISBN 9780131089297.

[27] **Matt Bishop:** *Vulnerabilities Analysis.* University of California at Davis, 1999.

[28] **Daniel Lowry Lough:** Virginia Polytechnic Institute. *A TAXONOMY OF COMPUTER ATTACKS WITH APPLICATIONS TO WIRELESS NETWORKS.* [Online] 2001. április. [Letöltve: 2011. 11 12.] http://scholar.lib.vt.edu/theses/available/etd-04252001-234145/unrestricted/lough.dissertation.pdf.

[29] **Frederick B. Cohen:** Information system attacks: A preliminary classification scheme. *Computers and Security.* 1997., 16. kötet, 1.

[30] **Dan Goodin:** User data stolen in Sony PlayStation Network hack attack. *The Register.* [Online] április 26, 2011. [Letöltve: június 26, 2011.] http://www.theregister.co.uk/2011/04/26/sony_playstation_network_security_breach/.

[31] **Uri Rivner:** Anatomy of an Attack. *RSA.* [Online] április 1, 2011. [Letöltve: június 26, 2011.] http://blogs.rsa.com/rivner/anatomy-of-an-attack/.

[32] **Jason Mick:** Reports: Hackers Use Stolen RSA Information to Hack Lockheed Martin. *DailyTech.* [Online] május 30, 2011. [Letöltve: június 26, 2011.] http://www.dailytech.com/Reports+Hackers+Use+Stolen+RSA+Information+to+Hack+Lockheed+Martin/article21757.htm.

[33] **Kelvin Chan, Pallavi Gogoi:** In latest attack, hackers steal Citibank card data. *Yahoo Finance.* [Online] június 9, 2011. [Letöltve: június 26, 2011.] http://finance.yahoo.com/news/In-latest-attack-hackers-apf-2621030252.html?x=0&.v=19.

[34] **Nick Hopkins:** Stuxnet attack forced Britain to rethink the cyber war. *Guardian.* [Online] május 30, 2011. [Letöltve: június 27, 2011.] http://www.guardian.co.uk/politics/2011/may/30/stuxnet-attack-cyber-war-iran.

[35] **Ed Barnes:** Mystery Surrounds Cyber Missile That Crippled Iran's Nuclear Weapons Ambitions. [Online] Fox News, movember 26, 2010. [Letöltve: augusztus 29, 2011.] http://www.foxnews.com/scitech/2010/11/26/secret-agent-crippled-irans-nuclear-ambitions/?test=latestnews.

[36] **Christopher Williams:** Israel video shows Stuxnet as one of its successes. *The Telegraph.* [Online] február 15, 2011. [Letöltve: június 27, 2011.] http://www.telegraph.co.uk/news/worldnews/middleeast/israel/8326387/Israel-video-shows-Stuxnet-as-one-of-its-successes.html.

[37] **Jeffrey Lewis:** On Spinning Libyan Centrifuges. *Arms Control Wonk.* [Online] február 15, 2011. [Letöltve: június 27, 2011.] http://lewis.armscontrolwonk.com/archive/3551/on-spinning-libyan-centrifuges.

[38] **Susan Snedaker:** *Business Continuity & Disaster Recovery for IT Professionals.* Burlington : Syngress Publishing, Inc., 2007. pp. 124-131. ISBN 978-1-59749-172-3.

[39] **Ponemon Institute:** First Annual Cost of Cyber Crime Study. [Online] ArcSight, július 2010. [Letöltve: augusztus 8, 2011.] http://www.arcsight.com/collateral/whitepapers/Ponemon_Cost_of_Cyber_Crime_study_2010.pdf.

[40] **Computer Security Institue:** 2008 CSI Computer Crime & Security Survey. [Online] 2009. [Letöltve: augusztus 8, 2011.] http://gocsi.com/sites/default/files/uploads/CSIsurvey2008.pdf.

[41] **Seymour E. Goodman, Stephen J. Lukasik, Gregory D. Grove:** *Cyber Attacks and International Laws***.** Survival, 2000, Vol. 42, pp. 89-103.

[42] **JULIAN E. BARNES, SIOBHAN GORMAN:** Wall Street Journal. [Online] május 31, 2011. [Letöltve: június 25, 2011.] http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html.

[43] **Bob Drogin:** Russians Seem To Be Hacking Into Pentagon. *SFGate.* [Online] október 7, 1999. [Letöltve: június 25, 2011.] http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/1999/10/07/MN58558.DTL.

[44] **NATHAN THORNBURGH:** The Invasion of the Chinese Cyberspies. *Time.com.* [Online] augusztus 29, 2005. [Letöltve: június 25, 2011.] http://www.time.com/time/magazine/article/0,9171,1098961,00.html.

[45] **Charles Arthur:** Google phishing: Chinese Gmail attack raises cyberwar tensions. *The Guardian.* [Online] június 1, 2011. [Letöltve: június 25, 2011.] http://www.guardian.co.uk/technology/2011/jun/01/google-hacking-chinese-attack-gmail.

[46] **Alexei Oreskovic, Sui-Lee Wee:** Google reveals Gmail hacking, says likely from China. *Reuters.com.* [Online] június 2, 2011. [Letöltve: augusztus 21, 2011.] http://www.reuters.com/article/2011/06/02/us-google-hacking-idUSTRE7506U320110602.

[47] **Dmitri Alperovitch:** Revealed**:** Operation Shady RAT. [Online] McAfee, 2011. [Letöltve: augusztus 20, 2011.] http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf.

[48] **Magyar ENSZ társaság:** Az Egyesült Nemzetek Alapokmánya. [Online] [Letöltve: 2011. június 25.] http://www.menszt.hu/layout/set/print/content/view/full/186.

[49] **NATO:** Washingtoni Szerződés. [Online] [Letöltve: 2011. augusztus 12.] http://www.mfa.gov.hu/kum/hu/bal/Kulpolitikank/Biztonsagpolitika/NATO_dokumentumok/.

[50] **SVERRE MYRLI:** 173 DSCFC 09 E bis - NATO and Cyber Defence. [Online] 2009. [Letöltve: augusztus 12, 2011.] http://www.nato-pa.int/default.asp?SHORTCUT=1782.

[51] **NATO - a Biztonságpolitikai Szakkollégium Egyesületének fordítása:** *Aktív Szerepvállalás, Modern Védelem - Az Észak-atlanti Szerződés Szervezetének Stratégiai Koncepciója Tagállamainak Védelméről és Biztonságáról.* Liszabon : ismeretlen szerző, 2010.

[52] **Richard Hunter, French Caldwell:** 'Digital Pearl Harbor': Defending Your Critical Infrastructure. [Online] Gartner, október 4, 2002. [Letöltve: augusztus 12, 2011.] http://www.gartner.com/pages/story.php.id.2727.s.8.jsp.

[53] **Krasznay Csaba, Dr. Kovács László:** Digitális Mohács. *Nemzet és Biztonság.* 2010.

[54] **Muha Lajos:** A Magyar Köztársaság kritikus információs infrastruktúráinak védelme. Budapest : ismeretlen szerző, 2008. Doktori (PhD) értekezés. kötet.

[55] **Charlie Mille:** *Kim Jong-il and me: How to build a cyber army to attack the U.S.* Charlie Miller, Las Vegas : s.n., 2010.

[56] **JR Minkel:** The 2003 Northeast Blackout--Five Years Later. *Scientific American.* [Online] augusztus 13, 2008. [Letöltve: augusztus 19, 2011.] http://www.scientificamerican.com/article.cfm?id=2003-blackout-five-years-later.

[57] **MAGYAR ENERGIA HIVATAL:** JELENTŐS ZAVAR VIZSGÁLATA. [Online] 2007. [Letöltve: 2011. augusztus 26.] http://www.eh.gov.hu/gcpdocs/200709/4362007mavir_lezr_02.pdf.

[58] **Sági József:** Rádiófrekvenciás Központi Vezérlés. [Online] EFR. [Letöltve: 2011. augusztus 19.] http://www.mee.hu/files/images/5/EFR_general_HU_25_Juni_09.pdf.

[59] **Jakob Nielsen:** *Usability Engineering.* San Francisco : Morgan Kaufman, 1993. ISBN 0-12-518406-9.

[60] **Gary C. Kessler:** Defenses Against Distributed Denial of Service Attacks. *garykessler.net.* [Online] npvember 2000. [Letöltve: augusztus 20, 2011.] http://www.garykessler.net/library/ddos.html.

[61] **Dr. Kovács László:** AZ INFORMÁCIÓS TERRORIZMUS ELLENI TEVÉKENYSÉG KORMÁNYZATI FELADATAI. *Hadmérnök.* III., 2008., 2.. kötet.

[62] **Nazario, Jose:** Estonian DDoS Attacks – A summary to date. [Online] Arbor Networks, 2007. május 17. [Letöltve: 2011. augusztus 20.] http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/.

[63] **Dan Goodin:** Kremlin-backed youths launched Estonian cyberwar, says Russian official. *The Register.* [Online] március 11, 2009. [Letöltve: augusztus 20, 2011.] http://www.theregister.co.uk/2009/03/11/russian_admits_estonian_ddos/.

[64] **Gigenet Cloud:** History of DDoS - Famous Attacks. [Online] [Letöltve: augusztus 20, 2011.] http://www.gigenetcloud.com/history_of_ddos.html.

[65] **Kim-Kwang, Raymond Choo:** Zombies and botnets. *TRENDS & ISSUES in crime and criminal justice.* [Online] Australian Institute of Criminology, március 2007. [Letöltve: augusztus 20, 2011.] http://www.aic.gov.au/documents/6/8/1/%7B68151067-B7C2-4DA4-84D2-3BA3B1DABFD3%7Dtandi333.pdf.

[66] **Stephen M. Specht, Ruby B. Lee:** *Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures.* Princeton, NJ, USA : Princeton University.

[67] **Janice Martin, Peter Reiher, Jelena Mirkovic:** *A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms.* Los Angeles : University of California, Los Angeles.

[68] **Guolong Lin, Guevara Noubir:** Low-Power DoS Attacks in Data Wireless LANs and Countermeasures. *Sigmobile.* [Online] június 1, 2003. [Letöltve: június 30, 2011.] http://www.sigmobile.org/mobihoc/2003/posters/p223-noubir.pdf.

[69] **CertPedia:** What is an association flood attack? [Online] április 8, 2011. [Letöltve: június 29, 2011.] http://www.certpedia.com/articles/what-is-association-flood-attack.html.

[70] **Wifimanager:** EAPOL Start Attack. [Online] [Letöltve: június 29, 2011.] http://www.wifimanager.nl/index.php?option=com_content&task=view&id=32&Itemid=.

[71] **Konstantin V. Gavrilenko, Andrew Vladimirov, Andrei A. Mikhailovsky:** Wireless Hacking: Breaking Through. *informIT.* [Online] december 17, 2004. [Letöltve: július 1, 2011.] http://www.informit.com/articles/article.aspx?p=353735&seqNum=9.

[72] **Cisco:** wIPS Policy Alarm Encyclopedia. [Online] [Letöltve: július 1, 2011.] http://www.cisco.com/en/US/docs/wireless/mse/3350/5.2/wIPS/configuration/guide/msecg_appA_wIPS.html.

[73] **Michael Roche:** Wireless Hacking Tools. *Washington University in St. Louis.* [Online] december 2, 2007. [Letöltve: július 1, 2011.] http://www1.cse.wustl.edu/~jain/cse571-07/ftp/wireless_hacking/index.html.

[74] **Cisco:** VLAN Security White Paper. [Online] [Letöltve: július 2, 2011.] http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a008013159f.shtml.

[75] **J. Postel:** Internet Control Message Protocol. *IETF.* [Online] szeptember 1981. [Letöltve: július 3, 2011.] http://www.ietf.org/rfc/rfc792.txt.

[76] **Juniper Networks:** Understanding ICMP Flood Attacks. [Online] [Letöltve: július 3, 2011.] http://www.juniper.net/techpubs/software/junos-es/junos-es92/junos-es-swconfig-security/understanding-icmp-flood-attacks.html.

[77] **Malachi Kenney:** Ping of Death. *Insecure.org.* [Online] január 22, 1997. [Letöltve: július 3, 2011.] http://insecure.org/sploits/ping-o-death.html.

[78] **CERT:** CERT Advisory CA-1997-28 IP Denial-of-Service Attacks. *Cert.org.* [Online] december 16, 1997. [Letöltve: július 3, 2011.] http://www.cert.org/advisories/CA-1997-28.html.

[79] **Insecure.org:** The LAND attack (IP DOS). [Online] november 20, 1997. [Letöltve: július 3, 2011.] http://insecure.org/sploits/land.ip.DOS.html.

[80] **Javvin Company:** Boink attack. [Online] [Letöltve: július 3, 2011.] http://www.javvin.com/networksecurity/Boinkattack.html.

[81] **Information Sciences Institute University of Southern California:** TRANSMISSION CONTROL PROTOCOL. [Online] IETF, szeptember 1981. [Letöltve: július 3, 2011.] http://tools.ietf.org/html/rfc793.

[82] **Wesley M. Eddy:** Defenses Against TCP SYN Flooding Attacks. *The Internet Protocol Journal - Volume 9, Number 4.* [Online] Cisco, december 2006. [Letöltve: július 3, 2011.] http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_9-4/syn_flooding_attacks.html.

[83] **Cisco:** Defining Strategies to Protect Against UDP Diagnostic Port Denial-of-Service Attacks. [Online] [Letöltve: július 3, 2011.] http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a008017690e.shtml.

[84] **John Leyden:** DoS risk from Zip of death attacks on AV software? *The Register.* [Online] július 23, 2001. [Letöltve: július 3, 2011.] http://www.theregister.co.uk/2001/07/23/dos_risk_from_zip/.

[85] **Maarten van Steen, Andrew S. Tanenbaum:** *Elosztott rendszerek.* Budapest : Panem Kft, 2004. p. 26. ISBN 963 545 387 6.

[86] **P. Ferguson, D. Senie:** Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing. [Online] IETF, 2000. május. [Letöltve: 2011. július 3.] http://www.ietf.org/rfc/rfc2827.txt.

[87] **CERT:** CERT® Advisory CA-1998-01 Smurf IP Denial-of-Service Attacks. [Online] január 5, 1998. [Letöltve: július 4, 2011.] http://www.cert.org/advisories/CA-1998-01.html.

[88] **Netrisk:** Rosszindulatú DDoS támadás a Netrisk.hu ellen. [Online] 2006. november 2. [Letöltve: 2011. augusztus 8.] https://www.netrisk.hu/publikaciok-biztositasi-hirek.html?hir_arhivumpage=7&hir_arhivum_kereses_szabaly=&hir_arhivum_kereses=#363.

[89] **Software Engineering Institute Carnegie Mellon:** Denial of Service Attacks. [Online] június 4, 2001. [Letöltve: augusztus 10, 2011.] http://www.cert.org/tech_tips/denial_of_service.html.

[90] **Scott Berinato:** How a Bookmaker and a Whiz Kid Took On a DDOS-based Online Extortion Attack. *CSO Online.* [Online] május 1, 2005. [Letöltve: augusztus 9, 2011.] http://www.csoonline.com/article/220336/how-a-bookmaker-and-a-whiz-kid-took-on-a-ddos-based-online-extortion-attack.

[91] **Paul Roberts:** Online Extortion Ring Broken Up. *PCWorld.* [Online] július 21, 2004. [Letöltve: július 4, 2011.] http://www.pcworld.com/article/116975/online_extortion_ring_broken_up.html.

[92] **Sophos:** Online Russian blackmail gang jailed for extorting $4m from gambling websites. [Online] október 6, 2006. [Letöltve: július 4, 2011.] http://www.sophos.com/en-us/press-office/press-releases/2006/10/extort-ddos-blackmail.aspx.

[93] **Microsoft:** Microsoft Security Intelligence Report volume 10. [Online] Microsoft Corporation, december 2010. [Letöltve: augusztus 28, 2011.] http://www.microsoft.com/security/sir/default.aspx.

[94] **Steve Orrin, Carl Livadas, Eve. M. Schooler, Jaideep Chandrashekar:** The Dark Cloud: Understanding and Defenfing Against Botnets and Stealthy Malware. *Intel Technology Journal.* 2, 2009, Vol. 13.

[95] **Jim Melnick, Ken Dunham:** *Malicious Bots.* Boca Raton FL : Auerbach Publications, 2008. ISBN 978 1 4200 6903 7.

[96] **Marius Oiaga:** eBay Bot Fraud. *Softpedia.* [Online] augusztus 2, 2006. [Letöltve: július 4, 2011.] http://news.softpedia.com/news/eBay-Bot-Fraud-31711.shtml.

[97] **Kreatív Online:** A rádiós piac bukta a legnagyobbat 2009-ben. [Online] március 30, 2010. [Letöltve: augusztus 29, 2011.] http://www.kreativ.hu/media/cikk/a_radios_piac_bukta_a_legnagyobbat_2009_ben.

[98] **CasinoListings:** Jail time and a hefty fine for DDoS attack blackmail. [Online] június 17, 2011. [Letöltve: július 4, 2011.] http://www.casinolistings.com/news/2011/06/jail-time-and-hefty-fine-for-ddos-attack-blackmail.

[99] **COL. CHARLES W. WILLIAMSON III:** Carpet bombing in cyberspace. *Armed Forces Journal.* [Online] május 2008. [Letöltve: július 4, 2011.] http://www.armedforcesjournal.com/2008/05/3375884.

[100] **SymantecCloud MessageLabs:** March 2011 Intelligence Report. [Online] március 2011. [Letöltve: július 4, 2011.] www.symanteccloud.com/mlireport/MLI_2011_03_March_Final-EN.pdf.

[101] **Paul Wood:** 419 Scammers Taking Advantage of Egypt's Revolution. [Online] Symantec, február 7, 2011. [Letöltve: július 4, 2011.] http://www.symantec.com/connect/blogs/419-scammers-taking-advantage-egypts-revolution.

[102] **419eater:** Trophy Room. [Online] [Letöltve: július 4, 2011.] http://forum.419eater.com/forum/album_cat.php?cat_id=1.

[103] **US Securities and Exchange Comission:** Pump and Dump Schemes. [Online] március 8, 2001. [Letöltve: július 5, 2011.] http://www.sec.gov/answers/pumpdump.htm.

[104] **Free Rainbow Tables:** [Online] [Letöltve: július 5, 2011.] http://www.freerainbowtables.com/.

[105] **Thorsten Holz, Jose Nazario:** As the Net Churns: Fast-Flux Botnet Observations. [Online] University of Mannheim, szeptember 5, 2008. [Letöltve: július 5, 2011.] https://pi1.informatik.uni-mannheim.de/filepool/publications/fastflux-malware08.pdf.

[106] **Joe Stewart:** Storm Worm DDoS Attack. *Secureworks.* [Online] DELL, február 8, 2007. [Letöltve: június 28, 2011.] http://www.secureworks.com/research/threats/storm-worm/.

[107] **John Leyden:** Conficker botnet growth slows at 10m infections. *The Register.* [Online] január 26, 2009. [Letöltve: július 14, 2011.] http://www.theregister.co.uk/2009/01/26/conficker_botnet/.

[108] **IDC:** IDC - Press Release. [Online] február 7, 2011. [Letöltve: augusztus 27, 2011.] http://www.idc.com/about/viewpressrelease.jsp?containerId=prUS22689111.

[109] **McAfee Labs:** McAfee Threats Report:Second Quarter 2011. [Online] 2011. [Letöltve: augusztus 27, 2011.] http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2011.pdf.

[110] **Strategy World:** The Mysterious Botnets of China. [Online] április 11, 2006. [Letöltve: augusztus 27, 2011.] http://www.strategypage.com/htmw/htiw/articles/20060411.aspx.

[111] **Magyar Telekom zRT:** Általános szerződési feltételek a T-Online internet szolgáltatásra. *T-Home.* [Online] Magyar Telekom zRT, március 25, 2011. [Letöltve: június 28, 2011.] http://www.telekom.hu/static/sw/download/Internet_aszf_110601.pdf.

[112] **UPC Magyarország:**HELYHEZ KÖTÖTT INTERNET HOZZÁFÉRÉSI (ELÉRÉSI) SZOLGÁLTATÁSRA VONATKOZÓ ÁLTALÁNOS SZERZŐDÉSI FELTÉTELEI. [Online] [Letöltve: július 25, 2011.] http://www.upc.hu/pdf/fn_dw_internet_aszf_0110606.pdf.

[113] Civil Disobedience in Cyberspace. [Online] [Letöltve: június 25, 2011.] http://home.clara.net/heureka/gaia/elec-act.htm.

[114] **Cliff Wang, David Dagon, Wenke Lee:** *Botnet Detection.* New York : Springer Science+Business Media, 2008. old.: 1-24. ISBN 978-0-387-68766-7.

[115] **Elmar Gerhards-Padilla, Felix Leder, Daniel Plohmann:** *Botnets: Detection, Measurement, Disinfection & Defence.* s.l. : European Network and Information Security Agency (ENISA), 2011.

[116] **Charles M. Kozierok:** TCP Connection Establishment Sequence Number Synchronization and Parameter Exchange. *The TCP/IP Guide.* [Online] 2005. [Letöltve: augusztus 17, 2011.] http://www.tcpipguide.com/free/t_TCPConnectionEstablishmentSequenceNumberSynchroniz.htm.

[117] **Spamlaws.com:** How TCP Sequence Prediction Attacks Work. [Online] [Letöltve: augusztus 17, 2011.] http://www.spamlaws.com/how-TCP-sequence-prediction-attacks-work.html.

[118] **Microsoft Research:** S-GPS: Spammer Global Positioning System. [Online] [Letöltve: július 5, 2011.] http://research.microsoft.com/en-us/projects/S-GPS/.

[119] **John Dunagan, Daniel R. Simon, Helen J. Wang, J. D. Tygar, Li Zhuang:** Characterizing Botnets from Email Spam Records. [Online] [Letöltve: július 5, 2011.] http://www.usenix.org/event/leet08/tech/full_papers/zhuang/zhuang.pdf.

[120] **Hostip.info:** My IP Address Lookup and GeoTargeting Community Geotarget IP Project – what country, city IP addresses map to. [Online] [Letöltve: július 5, 2011.] http://www.hostip.info/dl/index.html.

[121] **IPligence:** IP Geolocation Database Solutions. [Online] [Letöltve: július 5, 2011.] http://www.ipligence.com/.

[122] **Microsoft Corporation:** Bing Maps. [Online] [Letöltve: júlus 5, 2011.] http://msdn.microsoft.com/en-us/library/dd877180.aspx.

[123] **Yahoo! Developer Network:** Yahoo! Maps Web Services. [Online] [Letöltve: július 5, 2011.] http://developer.yahoo.com/maps/.

[124] **Google:** Google Maps API Family. [Online] [Letöltve: július 5, 2011.] http://code.google.com/intl/hu-HU/apis/maps/.

[125] **Websense:** Google's CAPTCHA busted in recent spammer tactics. [Online] február 22, 2008. [Letöltve: július 5, 2011.] http://securitylabs.websense.com/content/Blogs/2919.aspx.

[126] **Munk Sándor:** *A BIZTONSÁG KÉRDÉSEINEK DEKOMPOZÍCIÓJA.* [Online] **Hadmérnök,** 2010. június. [Letöltve: 2011. november 10.] http://hadmernok.hu/2010_2_munk.pdf. ISSN 1788-1919.

TÁBLÁZATOK JEGYZÉKE

ÁBRÁK JEGYZÉKE