AARMS Vol. 19, No. 3 (2020) 85–98.

10.32565/aarms.2020.3.6

The Remarkable 10th Anniversary of Stuxnet[1]

Analytical Summary of the SolarStorm Cyber Espionage Campaign

Gábor SELJÁN[2]

It has been ten years since Stuxnet, a highly sophisticated malware that was originally aimed at Iran's nuclear facilities, was uncovered in 2010. Stuxnet is considered to be the first cyber weapon, used by a nation state threat actor in a politically motivated cyberattack. It has significantly changed the cybersecurity landscape, since it was the first publicly known malware that could cause physical damage to real processes or equipment. Its complexity and level of sophistication, due to the exploitation of four different zero-day vulnerabilities in Windows and the usage of two stolen certificates, has triggered a paradigm shift in the cybersecurity industry. The recently uncovered cyber espionage campaign known as SolarStorm is a worthy anniversary celebration for Stuxnet. Especially because now the tables have turned. This campaign targeted the United States Government and its interests with a highly sophisticated supply chain attack through the exploitation of the SolarWinds Orion Platform used by thousands of public and private sector customers for infrastructure monitoring and management. In this article, I attempt to summarise the key points about the malware deployed in the SolarStorm campaign that can be drawn from reports available at the time of the writing.

Keywords: *backdoor, cybersecurity, cyber warfare, malware, supply chain attack*

Introduction

2020 has brought many challenges and changes to the cybersecurity landscape. The coronavirus pandemic has forced many companies to embrace work-from-home solutions without any preparations at all. This significant transition has led to increased risks of security breaches and data thefts. However, the increasing dangers of working from home were not the only notable events regarding cybersecurity.

[1] This paper was supported by the BCE EFOP-3.6.3-VEKOP-16-2017-00007 project.

[2] PhD student, Corvinus University of Budapest; e-mail: gabor.seljan@stud.uni-corvinus.hu

On December 8, FireEye, one of the largest cybersecurity firms, published a blog post to notify the public of a security breach by a highly sophisticated attacker that had unauthorised access to the company's various custom-made security testing tools (for example scripts, scanners, techniques and so on) used in red-team engagements.[3] This is how the investigation into the most significant cyberattack in recent memory has started. After a few days' analysis, the FireEye breach turned out to be just the tip of the iceberg. Incident responders uncovered highly sophisticated malware hiding in a worldwide used management software developed by a company called SolarWinds.

Thousands of customers turned out to be affected by a widespread software supply chain attack that compromised SolarWinds' software build process and leveraged the update mechanism of its Orion Platform to deliver a backdoor Trojan tracked as SUNBURST. Microsoft and Palo Alto refers to this still ongoing campaign of attacks connected to a suspected nation state threat actor as *Solorigate* or *SolarStorm*, respectively. Though these aliases already suggest the attack's impact on the information security industry, the purpose of this paper is to help interpret this campaign by providing both holistic and analytical summary of the sources available at the time of the writing, while focusing on key aspects of the malware, due to the scale and complexity of the campaign.

The sum of all fears

> *"You may take the most gallant sailor, the most intrepid airman, or the most audacious soldier, put them at a table together — what do you get? The sum of their fears."*
> Winston Churchill

Trusting trust

Back in 1984, in his Turing Award Lecture, Ken Thompson brought forth one of the most significant security challenges that the information technology industry faces: *trust*. Thompson described how easily an attacker could change a compiler binary to produce malicious versions of some programs, including the said compiler itself. This chicken or egg problem demonstrates that there is no truly trustworthy solution to verify the originality and the integrity of software.

> You can't trust code that you did not totally create yourself.... No amount of source-level verification or scrutiny will protect you from using untrusted code.... As the level of program gets lower, these bugs will be harder and harder to detect. A well-installed microcode bug will be almost impossible to detect.[4]

[3] FireEye, 'Unauthorized Access of FireEye Red Team Tools', 08 December 2020.
[4] Ken Thompson, 'Reflections on Trusting Trust', *Communications of the ACM* 27, no 8 (1984), 761–763.

This problem affects the setup and update mechanisms of our information systems being used today, because most application installations and system updates are performed with very high privileges. We simply cannot implement such complex systems by ourselves, hence we completely trust the vendor of the operating system running on our machine, because vendors have practically unlimited power over the device the operating system runs on. In most cases, Windows Updates are automatically installed in the background in the context of the SYSTEM user, while on Linux systems packages are usually manually applied with root privileges, though some distributions install security patches automatically. Security tools and appliances also typically run with high privileges and have access to sensitive assets. This trust relationship between customers and vendors makes the supply chain an extremely valuable target for threat actors.

Software supply chain attacks seek to damage government agencies and economic operators by targeting elements at any levels in their supply chain, including sub-contractors, integrators and so on. The attack could occur at any location in the supply chain, including development tools or business processes. For example, by inserting malicious software components during early phases of the software development lifecycle, adversaries could gain control of the systems using the malicious software for later remote exploitation. In his technical report submitted to MITRE in 2013, John F Miller gathered a wide range of supply chain attack information and provided a comprehensive view of supply chain attacks of malicious insertion across the full acquisition lifecycle.[5]

While these types of attacks have been around now for decades, they have started to become a hot topic in the security world, as the number of attacks, their sophistication and impact increased in the past few years. In his talk, in 2018 at the *BlueHat* conference, Elia Florio described 2017 as the year when the growing trend of such attacks became concerning.[6] Palo Alto Networks also laid out notable software supply-chain attacks in their professional blog, highlighting incidents involving Apple's *Xcode* software and *Transmission,* a popular open source BitTorrent client, and predicting an increased focus on attacking trusted developers.[7]

Among the several reported breaches, for example, *Cisco* revealed that the *CCleaner* installer distributed over a month's period contained a malicious payload.[8] Even today, it is still a very popular application used by many administrators to perform routine system maintenance. Reports at that time suggested that the malicious version of the application had been installed 2.27 million times until *Cisco* discovered the rouge app, hence the potential impact of this incident was severe.[9]

It is also among the most notable incidents of recent time, when Mossad, the Israeli secret service alerted the United States of America (USA) in 2015, after discovering attackers searching computers worldwide for documents with information regarding American

---

5 John F Miller, 'Supply Chain Attack Framework and Attack Patterns', *MITRE,* December 2013.

6 Elia Florio, 'Software Supply Chain Attacks in 2018', *Microsoft,* 30 November 2018.

7 Ryan Olson, 'The Era of Software Supply-Chain Attacks Has Begun', *Palo Alto Networks,* 18 December 2017.

8 Edmund Brumaghin, Ross Gibb, Warren Mercer, Matthew Molyett and Craig Williams, 'CCleanup: A Vast Number of Machines at Risk', *Cisco Talos Intelligence Group,* 18 September 2017.

9 Andy Greenberg, 'Software Has a Serious Supply-Chain Security Problem', *Wired,* 18 September 2017.

intelligence programs. This incident became infamous, because authorities confirmed that Russian attackers were able to steal confidential documents from the National Security Agency (NSA), through an employee who had improperly stored them on his personal computer running Kaspersky Lab's anti-virus software, which the attackers used as their very own search engine to conduct cyber espionage.[10]

There was another supply chain related security breach, with the probable involvement of the NSA, which have made the headlines in 2015. The National Institute of Standards and Technology (NIST) published an encryption algorithm in 2006 as a government standard at the NSA's request, despite the concerns of independent cryptography experts, suggesting that the proposed algorithm likely contained a backdoor that could be used to decrypt data. In 2008, the algorithm was secretly added to several Juniper products at the request of a customer, whom Juniper refused to identify.

In 2015, the company publicly revealed that its systems have been hacked in 2012, likely by a foreign government, and the intruder made a small code change of the said algorithm, that could be exploited to decrypt sensitive data.[11] Several United States government officials still seek answers to many questions regarding Juniper's internal investigation into the origin of the suspected NSA backdoor mechanism. In their open letter sent to Juniper, they have asked the vendor to publish the results of their investigation: 'Juniper's experiences can provide a valuable case study about the dangers of backdoors, as well as the apparent ease with which government backdoors can be covertly subverted by a sophisticated actor.'[12]

Basic cyber hygiene

History also shows that SolarWinds had struggles to get basic security hygiene implemented. As Bloomberg reported, a former security adviser of SolarWinds had warned the company's management of security risks in 2017. A former software engineer of the company also shared the view that a major breach is inevitable at SolarWinds, if they do not commit to security.[13] Their opinion seems to be justified by the fact that the company was also alerted in 2017, by an independent security researcher, because their update server was accessible with an easily guessable default password *solarwinds123*.

Further reinforces the negative image that the malicious binaries were still available for download days after the incident have been publicly disclosed and security updates have been published.[14] The firm also advised customers in a support page to exclude files, directories and ports from antivirus protection to run SolarWinds products more

---

10 Nicole Perlroth and Scott Shane, 'How Israel Caught Russian Hackers Scouring the World for U.S. Secrets', *The New York Times,* 10 October 2017.

11 Kim Zetter, 'Researchers Solve Juniper Backdoor Mystery; Signs Point to NSA', *Wired,* 22 December 2015.

12 Catalin Cimpanu, 'Congress asks Juniper for the results of its 2015 NSA backdoor investigation', *ZDNet,* 10 June 2020.

13 Ryan Gallagher, 'SolarWinds Adviser Warned of Lax Security Years Before Hack', *Bloomberg,* 21 December 2020.

14 Raphael Satter, Christopher Bing, Joseph Menn, 'Hackers used SolarWinds' dominance against it in sprawling spy campaign', *Reuters,* 16 December 2020.

efficiently. This is a quite common practice by vendors to avoid conflicts with endpoint protection software and often implemented using broad exclusion rules.[15]

Zero Day Initiative (ZDI) published details of some recently patched vulnerabilities in the Orion Platform, including a remote code execution vulnerability known as CVE-2020-14005 and a privilege escalation vulnerability through an SQL injection bug identified as CVE-2020-27869. These are low complexity, easily identifiable security flaws that might not seem to be severe by themselves, as they are only exploitable after user authentication. However, combining these vulnerabilities with the previously mentioned authentication bypass vulnerability tracked as CVE-2020-10148, could allow an unauthenticated remote attacker to take full control of the affected system.[16]

Weapons of mass espionage

SUNBURST

Initial reports suggested, but during the writing of this paper the vendor also confirmed, that the actors behind the SUNBURST malware have tested their methodology as early as September 2019, without performing any other malicious actions, to ensure that their modifications to the SolarWinds Orion code base would arrive to customers undetected. As a highly organised and disciplined attacker, the threat actor left a very narrow window of time between the compilation and the deployment of the compromised code base and later also removed the malware from the build environment. In their filing with the Securities and Exchange Commission (SEC) on December 21, 2020, SolarWinds confirmed that the malicious code appears to have been inserted during the build process and was not found in the source code of the Orion Platform products.[17]

According to Charles Carmakal, chief technology officer at Mandiant, FireEye's incident response arm, their security team received an alert, after a new unknown device has been registered with the company's multi-factor authentication system. This event prompted FireEye to investigate the situation. As FireEye was working to determine how the intruders have obtained the employee's credentials to register their device, they uncovered the SolarWinds breach into their network. The attackers presumably obtained the employee's credentials once they were already inside FireEye's network.[18]

Researchers recovered multiple malware samples that deliver different payloads, including novel memory-only droppers known as TEARDROP and RAINDROP. In one analysed case, the threat actor used TEARDROP to deploy BEACON, a payload included with Cobalt Strike, which is a well-known penetration testing tool based on the Metasploit Framework. The malware runs in-memory, but it registers a Windows service that calls the

---

15 Tara Seals, 'The SolarWinds Perfect Storm: Default Password, Access Sales and More', *Threatpost*, 16 December 2020.

16 Sivathmican Sivakumaran, 'Three Bugs in Orion's Belt: Chaining Multiple bugs for Unauthenticated RCE in the SolarWinds Orion Platform', *Zero Day Initiative*, 21 January 2021.

17 Kevin B Thompson, 'FORM 8-K', *SolarWinds Corporation*, 17 December 2020.

18 Kim Zetter, 'Hackers last year conducted a dry run of SolarWinds breach', *Yahoo News*, 18 December 2020.

exported Tk_CreateImageType function and writes a JPEG image in the current directory. This random named image file is then decrypted, resulting in a file with a PE header that turned out to be BEACON. The attacker's choice to use a common payload seems to be odd.[19]

RAINDROP, uncovered by Symantec, though is a very similar loader, appears to be used for lateral movement within the victim's network. Currently available evidence suggests that it might have been delivered by other means, unlike TEARDROP, which was delivered directly by SUNBURST. It is compiled as a DLL module, which is built from a modified version of *7-Zip* source code in order to hide malicious activity.[20]

The in-depth analysis of the malware paints a troublesome picture for the information security community and the industry. The backdoor was deployed as an update, including the digitally signed SolarWinds.Orion.Core.BusinessLayer.dll module, which is loaded by the legitimate SolarWinds.BusinessLayerHost.exe of the Orion Platform software. The trojanised update contains the backdoor that communicates to various third-party servers via HTTP protocol.

In his blog post, Tomislav Peričin, Chief Software Architect at ReversingLabs, also emphasised the level of stealth the attackers used to remain undetected as long as possible. There is a clear pattern of naming classes, members and variables appropriately to blend in with the code base, mimic the developers' coding style and naming standards. Strings are obfuscated using DEFLATE compression with Base64 encoding and 64-bit FNV-1a, a non-cryptographic hash function to hinder reverse engineering.

The malicious OrionImprovementBusinessLayer class and many of its methods can be found in other Orion software libraries. The attackers added a small block of code to the InventoryManager class to create a new thread that runs the backdoor during the legitimate background inventory checks. All these imply that the attackers were highly familiar with the code base.[21]

Several key points can be identified in the following excerpt of the code responsible for the initialisation of the backdoor. The initial analysis of this code already suggests a very specific targeting profile. Lack of evidence of second-stage payloads on the networks of many customers also suggest that instead of taking advantage of all compromised systems, the threat actor focused on some high-profile targets.

---

19 Check Point Research, 'SUNBURST, TEARDROP and the NetSec New Normal', *Check Point*, 22 December 2020.

20 Symantec Threat Hunter Team, 'RAINDROP: New Malware Discovered in SolarWinds Investigation', *Symantec*, 18 January 2021.

21 Tomislav Peričin, 'SunBurst: the next level of stealth', *ReversingLabs*, 16 December 2020.

```
public static void Initialize() {
  if (GetHash(Process.GetCurrentProcess().ProcessName.ToLower()) ==
  17291806236368054941UL) { ❶
  DateTime lastWriteTime = File.GetLastWriteTime(Assembly.
  GetExecutingAssembly().Location);
    int num = new Random().Next(288, 336);
    if (DateTime.Now.CompareTo(lastWriteTime.AddHours((double)num)) >= 0) { ❷
    instance = new NamedPipeServerStream(appId);
    ConfigManager.ReadReportStatus(out status);
    if (status!= ReportStatus.Truncate) {
      DelayMin(0, 0);
      domain4 = IPGlobalProperties.GetIPGlobalProperties().DomainName;
      if (!string.IsNullOrEmpty(domain4) &&!IsNullOrInvalidName(domain4)) { ❸
        DelayMin(0, 0);
        if (GetOrCreateUserID(out userId)) { ❹
        DelayMin(0, 0);
          ConfigManager.ReadServiceStatus(false);
          Update(); ❺
          instance.Close();
}}}}}}
```

On execution of the Initialize() method, the malware performs several checks to verify that the infected system is among the target machines. ❶ It verifies the name of the process using a hash, ❷ the write time of the assembly and ❸ checks that the machine is domain joined. The malware then ❹ generates a unique identifier for the victim machine and ❺ invokes the method Update() which is the core event loop for periodic beaconing to the command and control (C&C) server. The patience and operational security demonstrated by this threat actor allowed the malware to stay hidden and operate for a long period of time.

After an initial dormant period of 12–14 days (depending on a random offset), it attempts to resolve a subdomain of avsvmcloud[.]com to get in contact with its designated C&C server, from which it retrieves and executes various built-in commands that, among other things, allow internal reconnaissance, persistence and data exfiltration. In order to evade detection, the malware masquerades its communication as legitimate network traffic, stores information within original configuration files to blend in with usual application activity and uses extensive blocklists to avoid forensic and anti-virus tools.

Subdomains are constructed by a Domain Generation Algorithm (DGA) to vary DNS requests and to control the behaviour of the malware on specific targets based on their unique identifier.[22] On December 15, 2020, Microsoft intervened in cooperation with industry partners, and seized the domain name avsvmcloud[.]com used for the campaign. By sinkholing the C&C communication with the compromised systems, they effectively

[22] FireEye, 'Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor', 13 December 2020.

rendered this malware inoperable.[23] Anyway, the shutdown of one specific malware did not stop the campaign.

SUPERNOVA

As their investigation unfolded, FireEye have identified another malware named SUPERNOVA, that consists of a small persistent backdoor. Based on the technical analysis of the second malware, Wes Riley of GuidePoint Security described the operation of this backdoor in-depth in his blog post.[24] PaloAlto and Microsoft have also conducted their own research into SUPERNOVA and noted that – unlike in case of SUNBURST – the affected DLL module was not digitally signed, hence it was determined to be likely unrelated to the *SolarStorm* campaign and possibly used by another threat actor.[25]

This backdoor was implemented in the form of a .NET C# web shell, as a modification to the app_web_logoimagehandler.ashx.b6031896.dll module that is otherwise responsible to return the user-defined logo image of the Orion web application. Traditional web shells provide a means of remote access and allow the execution of arbitrary commands on the server, by communicating with the underlying operating system via the interpreter of the scripting language being used. These tools are especially useful to exploit file inclusion vulnerabilities that allow an attacker to trick the affected application into executing malicious code.

The SUPERNOVA web shell is somewhat unconventional. The threat actor added a new DynamicRun() method to the LogoImageHandler class and appended a few new lines of argument-handling code to the beginning of the ProcessRequest() function to call this new method with arbitrary parameters. The new method allowed the on-the-fly compilation and in-memory execution of arbitrary.NET code supplied by the attacker via HTTP requests, leaving behind minimal forensic artifacts, as no files will be written to disk, except the temporary files used by the.NET utilities invoked during compilation of the payload. The in-memory execution of shellcode is a well-known technique used to disguise execution and bypass antivirus software. Similar web shells have been used by attackers for decades, against applications developed in common interpreted languages such as PHP or JSP. Using this technique against a system that was built in a compiled language is a novel approach.

A possible suspected entry point of the threat actor that have planted the second malware is a recently discovered authentication bypass vulnerability in the Orion Platform. This vulnerability is now known as CVE-2020-10148 and it could allow an unauthenticated remote attacker with access to the network to execute Orion API commands on the target system. As stated in the vulnerability note published by US-CERT, ❶ by appending

---

[23] Catalin Cimpanu, 'Microsoft and industry partners seize key domain used in SolarWinds hack', *ZDNet*, 15 December 2020.

[24] Wes Riley, 'Supernova SolarWinds.NET Webshell Analysis', *Guide Point Security,* 17 December 2020.

[25] Matt Tennis, 'SUPERNOVA: A novel.NET Webshell', *Palo Alto Networks,* 17 December 2020; MSTIC, 'Analyzing Solorigate, the compromised DLL file that started a sophisticated cyberattack', *Microsoft,* 18 December 2020.

specific strings like Skipi18n to the path of an HTTP request, the attacker could trick the Orion server to ❷ set the SkipAuthorization property, which may allow an API request to be processed without requiring authentication.[26] This property is intended for use by authentication modules that need to redirect to resources that allow anonymous connections, for example stylesheets or scripts and localisation resources.[27] The below is the relevant excerpt from the source code the OnRequest() method of the i18nRedirector class.

```
HttpContext context = ((HttpApplication)sender).Context;
string path = context.Request.Path;
if (path.IndexOf("Skipi18n", StringComparison.OrdinalIgnoreCase) >= 0) { ❶
  context.SkipAuthorization = true; ❷
  context.User = new NullUser();
};
```

SUNSPOT

The SUNSPOT malware is quite another piece fitting well with such sophisticated campaign like *SolarStorm*. The CrowdStrike team provided a technical analysis of this malicious tool that was deployed into SolarWinds' build environment to inject the SUNBURST backdoor into the Orion Platform without arousing any suspicion.[28]

The malware monitored running processes on the infected machines for those involved in compilation of the Orion product and replaced one of the source files to smuggle the backdoor into the release binaries. The design suggests that the threat actor invested a lot of effort to ensure their code was properly inserted and remained undetected. According to the build timestamp found during the technical analysis of a binary sample, the malware was likely built on February 20, 2020.

The following is an excerpt of the source code of the malware that shows the method implemented for tracking build processes:

```
private static class ProcessTracker {
  private static bool SearchConfigurations() { ❶
    ManagementObjectSearcher s =
      new ManagementObjectSearcher(
        ZipHelper.Unzip(
          "C07NSU0uUdBScCvKz1UIz8wzNooPriwuSc11KcosSy0CAA==")); ❷ // Select *
          From Win32_SystemDriver
    foreach (ManagementObject i in s.Get()) {
```

[26] Oliver Madison and Will Dormann, 'SolarWinds Orion API authentication bypass allows remote command execution', *CERT/CC*, 26 December 2020.
[27] Microsoft, 'HttpContext.SkipAuthorization Property', 31 December 2020.
[28] CrowdStrike Intelligence Team, 'SUNSPOT: An Implant in the Build Process', 11 January 2021.

```
      ulong hash = GetHash(
        Path.GetFileName(
           i.Properties[ZipHelper.Unzip(
             "C0gsyfBLzE0FAA==")].Value.ToString()).ToLower()); ❷ // PathName
      if (Array.IndexOf(configTimeStamps, hash)!= -1) {
        return true;
      }
    }
    return false;
}
```

The malware carries out some common steps expected from malicious code, like creating a mutex to ensure only one instance is running, creating an encrypted log file or granting itself debugging privileges to read other processes' memory. After initialisation, the malware is constantly looking for a build process using the ProcessTracker class and ❶ modifies the target source code, if the SearchConfigurations() method determines that the software being built is the Orion application.

As a fail-safe mechanism, it also checks another mutex the existence of which would instruct the malware to discretely stop and seize operation. SUNSPOT extracts the command line arguments of the build process and looks for the directory path of the Orion software, which is hard-coded in the binary in an encrypted form. ❷ String obfuscation techniques, similar to those used in SUNBURST, can be observed in the source code, leveraging DEFLATE compression and Base64 encoding. The stored malicious source code for SUNBURST is encrypted with the AES128-CBC algorithm.

To avoid errors that might raise suspicion, the threat actor also added a MD5 hash verification check to ensure compatibility with the original source. The malware replaces the source file only if both the decryption and the hash verification is successful. After the successful build of the backdoored Orion solution, the original source code is restored.

Conclusion

Ten years after Stuxnet, the cybersecurity industry have reached a new milestone. Brad Smith, president of Microsoft, wrote in his blog post that 'this attack provides a moment of reckoning' and drew attention to the need of a strong and global cybersecurity response.[29] Such complex and highly sophisticated attack against the United States of America by a nation state actor really represents a turning point in cybersecurity. The fact that the *SolarStorm* espionage campaign managed to infiltrate the systems of the United States government give light towards the necessity of a next paradigm shift in cybersecurity.

The Cyberspace Solarium Commission (CS) – an intergovernmental body established to develop a strategic approach to defend against significant cyberattacks – made the first

[29] Brad Smith, 'A moment of reckoning: the need for a strong and global cybersecurity response', *Microsoft*, 17 December 2020.

step by acknowledging that 'the reality is that we are dangerously insecure in cyber'. The final report of the CSC offers legal and policy recommendations that signal a fundamental shift in cybersecurity policy, including a new law establishing that software vendors and hardware manufacturers are liable for damages from incidents that exploit known and unpatched vulnerabilities.[30]

Then-president-elect Biden said in a statement, that his administration will make cybersecurity a top priority. Now the new Biden–Harris Administration has a huge amount of work to do in response to the *SolarStorm* campaign. The Trump Administration removed experienced cybersecurity professionals from their positions and eliminated several important posts altogether. Nevertheless, President Trump also made an important step to address the situation by issuing an executive order to ensure that service providers verify the identity of persons using United States Infrastructure as a Service (IaaS) and maintain records of those transactions.[31]

Attacker attribution is hard, but it is not impossible. A joint statement released by the Cyber Unified Coordination Group (UCG) on January 5, 2021, officially attributed most or all of the recently discovered cyber compromises to Russia. Kaspersky's security researchers have also found several similarities between SUNBURST and KAZUAR, which is believed to have been used by the Russian Advanced Persistent Threat (APT) group TURLA, a sophisticated team suspected of operating out of Moscow's FSB intelligence agency.[32] The United State's relationship with Russia was already challenging due to, among others, Moscow's interference in the presidential election, its annexation of Crimea, its support for Syria's Bashar al-Assad in the civil war or a second assassination attempt on Kremlin critic Alexei Navalny. This recent incident could further increase tensions with Russia.

The *SolarStorm* campaign has demonstrated that significant weaknesses in today's cyber space – the fourth operational domain acknowledged by the NATO in 2016 – could allow determined adversaries to carry out successful targeted attacks even when lacking the economic, military and political power, by engaging in asymmetric warfare. The investigation is still ongoing and will certainly take months to conclude due to the scale of the campaign. However, seeing only the tip of the iceberg could be convincing enough to break the vicious circle of cat and mouse by changing the perspective from which we view cybersecurity today. Only by addressing the root cause can a problem be fixed.

References

Brewster, Thomas, 'Hackers Abuse Another Adobe Zero-Day To Attack Thousands Of Web Users'. *Forbes*, 02 February 2015. Online: www.forbes.com/sites/thomasbrewster/2015/02/02/yet-another-adobe-flash-zero-day/

30 Angus King and Mike Gallagher, 'Cyberspace Solarium Commission Report', *CSC*, 11 March 2020.

31 Donald J Trump, 'Executive Order on Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities', *The White House*, 19 January 2021.

32 Georgy Kucherin and Igor Kuznetsov, 'Sunburst backdoor – code overlaps with Kazuar', *Securelist*, 11 January 2021.

Brumaghin, Edmund, Ross Gibb, Warren Mercer, Matthew Molyett and Craig Williams, 'CCleanup: A Vast Number of Machines at Risk'. *Cisco Talos Intelligence Group*, 18 September 2017. Online: https://blog.talosintelligence.com/2017/09/avast-distributes-malware.html

Check Point Research, 'SUNBURST, TEARDROP and the NetSec New Normal'. *Check Point*, 22 December 2020. Online: https://research.checkpoint.com/2020/sunburst-teardrop-and-the-netsec-new-normal/

Cimpanu, Catalin, 'Congress asks Juniper for the results of its 2015 NSA backdoor investigation'. *ZDNet*, 10 June 2020. Online: www.zdnet.com/article/congress-asks-juniper-for-the-results-of-its-2015-nsa-backdoor-investigation/

Cimpanu, Catalin, 'Microsoft and industry partners seize key domain used in SolarWinds hack'. *ZDNet*, 15 December 2020. Online: www.zdnet.com/article/microsoft-and-industry-partners-seize-key-domain-used-in-solarwinds-hack/

CISA, 'Alert (AA20-352A)'. *Cybersecurity and Infrastructure Security Agency*, 17 December 2020. Online: https://us-cert.cisa.gov/ncas/alerts/aa20-352a

CrowdStrike Intelligence Team, 'SUNSPOT: An Implant in the Build Process', 11 January 2021. Online: www.crowdstrike.com/blog/sunspot-malware-technical-analysis/

DHS, 'Emergency Directive 21-01'. *Department of Homeland Security*, 13 December 2020. Online: https://cyber.dhs.gov/ed/21-01/

FireEye, 'Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor', 13 December 2020. Online: www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

FireEye, 'Unauthorized Access of FireEye Red Team Tools', 08 December 2020. Online: www.fireeye.com/blog/threat-research/2020/12/unauthorized-access-of-fireeye-red-team-tools.html

Florio, Elia, 'Software Supply Chain Attacks in 2018'. *Microsoft*, 30 November 2018. Online: www.youtube.com/watch?v=sMwKqSsML5E

Gallagher, Ryan, 'SolarWinds Adviser Warned of Lax Security Years Before Hack'. *Bloomberg*, 21 December 2020. Online: www.bloomberg.com/news/articles/2020-12-21/solarwinds-adviser-warned-of-lax-security-years-before-hack

Greenberg, Andy, 'Software Has a Serious Supply-Chain Security Problem'. *Wired*, 18 September 2017. Online: www.wired.com/story/ccleaner-malware-supply-chain-software-security/

King, Angus and Mike Gallagher, 'Cyberspace Solarium Commission Report'. *CSC*, 11 March 2020. Online: https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view

Lambert, John, 'Important steps for customers to protect themselves from recent nation-state cyberattacks'. *Microsoft*, 13 December 2020. Online: https://blogs.microsoft.com/on-the-issues/2020/12/13/customers-protect-nation-state-cyberattacks/

Microsoft, 'HttpContext.SkipAuthorization Property', 31 December 2020. Online: https://docs.microsoft.com/en-us/dotnet/api/system.web.httpcontext.skipauthorization

Madison, Oliver and Will Dormann, 'SolarWinds Orion API authentication bypass allows remote command execution'. *CERT/CC*, 26 December 2020. Online: https://kb.cert.org/vuls/id/843464

Miller, John F, 'Supply Chain Attack Framework and Attack Patterns'. *MITRE*, December 2013. Online: www.mitre.org/sites/default/files/publications/supply-chain-attack-framework-14-0228.pdf

MSRC, 'Customer Guidance on Recent Nation-State Cyber Attacks'. *Microsoft*, 13 December 2020. Online: https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/

MSTIC, 'Analyzing Solorigate, the compromised DLL file that started a sophisticated cyberattack'. *Microsoft*, 18 December 2020. Online: www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/

Newman, Lily H, 'Inside the Unnerving Supply Chain Attack That Corrupted CCleaner'. *Wired*, 17 April 2018. Online: www.wired.com/story/inside-the-unnerving-supply-chain-attack-that-corrupted-ccleaner/

Olson, Ryan, 'The Era of Software Supply-Chain Attacks Has Begun'. *Palo Alto Networks*, 18 December 2017. Online: https://blog.paloaltonetworks.com/2017/12/2018-predictions-recommendations-era-software-supply-chain-attacks-begun/

Peričin, Tomislav, 'SunBurst: the next level of stealth'. *ReversingLabs*, 16 December 2020. Online: https://blog.reversinglabs.com/blog/sunburst-the-next-level-of-stealth

Perlroth, Nicole and Scott Shane, 'How Israel Caught Russian Hackers Scouring the World for U.S. Secrets'. *The New York Times*, 10 October 2017. Online: www.nytimes.com/2017/10/10/technology/kaspersky-lab-israel-russia-hacking.html

Riley, Wes, 'Supernova SolarWinds.NET Webshell Analysis'. *Guide Point Security*, 17 December 2020. Online: www.guidepointsecurity.com/supernova-solarwinds-net-webshell-analysis/

Satter, Raphael, Christopher Bing and Joseph Menn, 'Hackers used SolarWinds' dominance against it in sprawling spy campaign'. *Reuters*, 16 December 2020. Online: www.reuters.com/article/global-cyber-solarwinds/hackers-at-center-of-sprawling-spy-campaign-turned-solarwinds-dominance-against-it-idUSKBN28P2N8

Seals, Tara, 'The SolarWinds Perfect Storm: Default Password, Access Sales and More'. *Threatpost*, 16 December 2020. Online: https://threatpost.com/solarwinds-default-password-access-sales/162327/

Sivakumaran, Sivathmican, 'Three Bugs in Orion's Belt: Chaining Multiple bugs for Unauthenticated RCE in the SolarWinds Orion Platform'. *Zero Day Initiative*, 21 January 2021. Online: www.zerodayinitiative.com/blog/2021/1/20/three-bugs-in-orions-belt-chaining-multiple-bugs-for-unauthenticated-rce-in-the-solarwinds-orion-platform

SolarWinds, 'SolarWinds Security Advisory', 18 December 2020. Online: www.solarwinds.com/securityadvisory

Smith, Brad, 'A moment of reckoning: the need for a strong and global cybersecurity response'. *Microsoft*, 17 December 2020. Online: https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/

Symantec Threat Hunter Team, 'RAINDROP: New Malware Discovered in SolarWinds Investigation'. *Symantec*, 18 January 2021. Online: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-raindrop-malware

Tennis, Matt, 'SUPERNOVA: A novel.NET Webshell'. *Palo Alto Networks*, 17 December 2020. Online: https://unit42.paloaltonetworks.com/solarstorm-supernova/

Thompson, Ken, 'Reflections on Trusting Trust'. *Communications of the ACM* 27, no 8 (1984), 761–763.

Thompson, Kevin B, 'FORM 8-K'. *SolarWinds*, 17 December 2020. Online: https://d18rn0p25nwr6d.cloudfront.net/CIK-0001739942/6dd04fe2-7d10-4632-89f1-eb8f932f6e94.pdf

Trump, Donald J, 'Executive Order on Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities'. *The White House*, 19 January 2021. Online: https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-taking-additional-steps-address-national-emergency-respect-significant-malicious-cyber-enabled-activities/

Zetter, Kim, 'Researchers Solve Juniper Backdoor Mystery; Signs Point to NSA'. *Wired*, 22 December 2015. Online: www.wired.com/2015/12/researchers-solve-the-juniper-mystery-and-they-say-its-partially-the-nsas-fault/

Zetter, Kim, 'Hackers last year conducted a dry run of SolarWinds breach'. *Yahoo News*, 18 December 2020. Online: https://news.yahoo.com/hackers-last-year-conducted-a-dry-run-of-solar-winds-breach-215232815.html