The SolarWinds Hack

Project for ITE 420

Fundamentals of Information Security

By Christine Byrd

**Details of the Problem**

It started simply. On December 8th 2020, FireEye’s CEO Kevin Mandia posted on the official FireEye blog(1) brief details of a breach on their own systems by what they called an “attack by a nation with top-tier offensive capabilities.” The unknown attackers had somehow accessed their systems and had stolen their own internal “Red Team” hacking tools. Though those tools included no zero-day exploits or unknown techniques(2), FireEye publicly released countermeasures against their own tools in order to mitigate the damage the hackers can do with them. Fireeye also spoke of the attacker’s attempts to access information relating to government customers- a sign of state-sponsored cyber-espionage. FireEye declared that it was working with the FBI, Microsoft, and others in their investigation.

This was the first reported clue in what would later be called the SolarWinds Hack.

In March 2020, The SolarWinds Orion Platform, “A powerful, scalable infrastructure monitoring and management platform designed to simplify IT administration” (3) pushed out an update that included malicious code opening a backdoor, codenamed SUNBURST(5), to the networks it is installed on. All updates from February 20th to June 2020 (4) had this backdoor. SUNBURST was then used to deploy different malicious code, codenamed SUPERNOVA (5), as well as other specialized software such as TEARDROP(9) on the attack-target’s networks that were running the vulnerable Orion code. The backdoor itself was inserted into the source code of Orion Platform during compiler runtime from the machines of the Orion development team using malicious code codenamed SUNSPOT.(6)

This amazing chain of completely unique and specialty (and therefore unknown to antiviruses) malware was used in conjunction with the SolarWinds Orion platform because the platform is a third-party-product used in businesses and organizations across the globe, including in many U.S. Government Departments and Agencies (7)(8). This is known as a Supply Chain Attack, because it is an attack that focuses on a third party that supplies resources, in this case SolarWinds’s IT Management Software Orion, instead of the main target itself.

Only some of this was known by the time of the first major report, released December 13, 2020, only five days after FireEye’s first report on their own internal detection of the hack. But by this time, it was definitely known that the backdoor was from SolarWind’s Orion. The next week news articles abounded talking about the SolarWinds hack and its implications, everything from new victims verified to be targets to speculation on the possible implications of a state actor such as Russia having secret information, as shown in the news article “US Treasury Hack Info May Have Helped Russia Tycoons Dodge Sanctions” by Newsweek(10). Not much more information has come to light since then, as businesses are leery about exposing their failures and governments even more so.

On February 23, 2021 the Senate had a hearing on the SolarWinds Hacking. Testifying before the committee were various major players in the hack, including FireEye, Microsoft, Solarwinds. The need for prevention of these types of attacks, and how this attack was undiscovered for so long, and what could be done about other cybersecurity issues were some of the things discussed. The talk is available in it’s entirety at https://www.c-span.org/video/?509234-1/senate-intelligence-hearing-solarwinds-hacking

What is known is that from March 2020 to December 2020, malicious state-sponsored actors have been conducting a campaign of cyber-espionage. These actors, who have tentatively been identified as being Russia’s Foriegn Intelligence Service (SVR), have had access to an unknown depth of US government agencies and services, major companies like Microsoft, Cisco, Intel, and other companies based across the globe for months.(11) The possible damage in stolen information and technology can only be speculated upon. If not for FireEye detecting and announcing the threat, this espionage could still be on-going with both the public and security officials across the globe unknowing. This whole event highlights how important security is on all levels.

**The Technicalities** CVE-2020-10148

Listed as CVE-2020-10148 and/or UNC2452, the Solarwinds hack was massive. Solarwinds, who’s Orion customers number around 33,000, believes fewer than 18,000 installed the compromised version of their product with the SUNBURST trojan.(12)

Now, a detailed look at the different parts of this attack:

SUNBURST

This is a backdoor inserted into the main *Solarwinds.Orion.Core.BusinessLayer.dll*. As a compiled part of the main program it utilizes the same digital security signature that the rest of the un-altered program does.(9) It has a dormancy period of 288 to 336 hours(13) (around two weeks) before it communicates to a third party server (avsvmcloud[.]com) via HTTP.(9)(14) This is the Command and Control Server.(14) Each server uses an encoded version of the victim network name as part of the sub-domain.(8) A list decoded domain names available at (8). The traffic the the individualized domains is designed to mimic normal SolarWinds API communications.(9)

SUNBURST then executes a variety of malicious commands including “file transfer, executing files, disabling system services, and gathering system info.”(14)(9) More importantly, it analyzes the forensic and anti-virus tools on a system using multiple obfuscated blocklists. (9)It’s network traffic uses the Orion Improvement Program protocol.(9) It stores data in legitimate plugin configuration files. (9) For more information see (9).

SUPERNOVA

This is one of the malware that was deployed from the C2 using SUNBURST. It keeps the naming convention because it looks like it is part of the SolarWinds product. It does NOT use the signed certificate that SUNBURST does. It does require Orion to run, as it is a dll file. It is named “app\_web\_logoimagehandler.ashx.b6031896.dll.”(16)

TEARDROP

Also deployed from SUNBURST, this is a new unseen memory-only dropper used for BEACON - “Cobalt Strike’s Payload to model advanced attackers[,] used to egress a network over HTTP/S or DNS”(15)) it reads a file called “Gracious\_Truth.jpg” then “Next it checks that HKU\SOFTWARE\Microsoft\CTF exists, decodes an embedded payload using a custom rolling XOR algorithm and manually loads into memory an embedded payload using a custom PE-like file format.” (9)

SUNSPOT

SUNSPOT is the codename for the malware used to inject the backdoor SUNBURST into SolarWind’s Orion. According to the Crowdstrike Analysis of SUNSPOT post-discovery, the malware ran on the machines of developers who developed SolarWind’s Orion platform.(6) SUNSPOT is single threaded with a mutex lock to make sure that it only runs one instance of itself. It watches for Visual Studio running on it’s host machine (MsBuild.exe), then looks to see if VisualStudio is being used to compile Orion.(6) It checks every second.(6) This allows SUNSPOT to insert it’s trojan code into the source files before the compiler runs, then takes the trojan source files back out after the compiler is complete.(6) It has many checks to make sure that it targets the right build, that it doesn't stop mid-process, and that the file it replaces is compatible and will not cause build errors, because build errors could lead to discovery.(6) It even uses compiler statements ( #Pragma statements) to disable warnings on the trojan code.(6) This prevents it from appearing in build logs. For more detailed information see the Crowdstrike Analysis at (6).

**Mitigation**

There is value in a product that you keep entirely in-house. Third party products and contractor made products have inherent risk that is far less able to be controlled. It is also something that a company can point to and say “This is not my fault,” disclaiming liability. Third party products are also created by experts in their field, so that first party companies don’t have to hire those experts. Almost no company will decide to make their own operating system from scratch, for example. Therefore there will always be the risk of a Supply chain attack like this happening again. How do we mitigate it?

One of the contributors to the hack may be that SolarWinds outsourced its development to Eastern Europe, as discovered by the New York Times(17). Certainly it would be easier for foreign interests to affect US interests when the very thing you are creating is being created on foreign soil. According toTheCoversation.com, “Russian operatives have been known to use companies in former Soviet satellite countries to insert malware into software supply chains. Russia used this technique in the 2017 NotPetya attack that cost global companies more than US$10 billion.”(18) While the internet means that everyone lives right next door to each other, this hack demonstrates you are still much more vulnerable when you are physically right next door also.

According to TheCoversation.com, “SolarWinds also failed to practice basic cybersecurity hygiene, according to a cybersecurity researcher. Vinoth Kumar reported that the password for the software company’s development server was allegedly “solarwinds123,” an egregious violation of fundamental standards of cybersecurity.”(18)

FireEye has released detection rules in multiple languages such as Snort, Yara, IOC and ClamAV on their github free to the community: github.com/fireeye/sunburst\_countermeasures

Crowdstrike has a list of potential signs of virus such as SUNSPOT listed at (6), such as “Persistence using scheduled tasks, triggered at boot time”, “Access to the remote process arguments made via the remote process’s PEB structure” , and “Detection of the targeted Visual Studio solution build by reading the virtual memory of MsBuild.exe processes, looking for the targeted solution filename”.

The best mitigation is the same mitigation strategies that work for all viruses and malware: know your system, know your network, keep things separate, use least privilege, keep things secure, always watch. FireEye’s detection of their internal tools being copied when they were not supposed to was the only reported time, over a period of months, where this hack was detected and we should learn from that.

As said in the Senate hearing on the SolarWinds Hacking, the best mitigation for such widespread cyber-espionage is a better, larger cybersecurity workforce and the modernization of the cyber infrastructure. Only more people, with better awareness, can see these new novel attacks happening and do something about them. Prevention can only get you so far- it is statistically inevitable that something will happen. Detection is key to mitigation.

**Citations**

(1)<https://www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html>

(2)<https://www.fireeye.com/blog/threat-research/2020/12/unauthorized-access-of-fireeye-red-team-tools.html>

(3)<https://www.solarwinds.com/orion-platform>

(4) <https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst>

(5)<https://www.solarwinds.com/sa-overview/securityadvisory>

(6)<https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/>

(7)<https://www.businessinsider.com/list-of-the-agencies-companies-hacked-in-solarwinds-russian-cyberattack-2020-12>

(8)<https://securityaffairs.co/wordpress/112555/hacking/solarwinds-victims-lists.html>

(9)<https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html>

(10)<https://www.newsweek.com/hack-us-yield-sanctions-info-ex-officials-1555287>

(11)<https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12>

(12)<https://apnews.com/article/solarwinds-fireeye-hack-explained-07e55dfd7fb9e6de96b55a7788eaa93e>

(13)<https://twitter.com/KyleHanslovan/status/1338865692116885504>

(14)<https://securityaffairs.co/wordpress/112376/apt/solarwinds-backdoor-kill-switch.html>

(15)<https://www.cobaltstrike.com/help-beacon>

(16)<https://www.solarwinds.com/sa-overview/securityadvisory#anchor2>

(17)<https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html>

(18)<https://theconversation.com/the-solarwinds-hack-was-all-but-inevitable-why-national-cyber-defense-is-a-wicked-problem-and-what-can-be-done-about-it-153084>