The SolarWinds Orion Breach:

A Cybersecurity Disaster

Levi Seibert

00086809

lseiber1@my.athens.edu

ITE 420 Project

On December 13, 2020, amidst all the chaos enveloping the United States, news of a major cybersecurity attack on SolarWinds Orion products flooded the news. What was first considered alarming by many, soon became terrifying as specific details were released. SolarWinds provides network management IT software for around 300,000 customers, 30,000 use the Orion software platform (Krebs). Of these 30,000 customers, up to 18,000 were exposed to the cyber-attack (Marshall and Smith). According to a webpage from their website that has been deleted (presumably because of the breach), SolarWinds provides service for over 80% of the US Fortune 500 companies, the top ten US telecommunications companies, all five branches of the US Military, hundreds of universities and colleges around the world, and several U.S. government agencies such as the Pentagon, NASA, the NSA, the State Department, the Department of Justice, and the Office of the President (SolarWinds Customers). Although it is unknown if all of these organizations were involved in the incident, it has been confirmed that several top U.S. government agencies were targeted and breached. Additionally, the attack infiltrated Microsoft's source code (Baker). Obviously, a data breach of this magnitude is (and should be) a major sense of alarm among its subjects. This attack goes to prove that no entity is truly safe from cyberattacks, and that a security mistake could cause major, disastrous consequences.

The discovery of the SolarWinds breach actually began December 8, 2020, a few days before the public announcement, when the cybersecurity firm FireEye announced it was victim to a cyber-attack, presumably from a nation-state (Baker). While investigating their own breach, FireEye "uncovered a widespread campaign" that trojanized SolarWinds Orion business software. This cyber event is still under investigation; however, it is believed that trojan came during some of Orion's updates (specially versions 2019.4 HF 5 through 2020.2.1). It seems that the attackers were able to manipulate an Orion plugin in those updates, specifically SolarWinds.Orion.Core. BusinessLayer.dll. The trojanized portion of the code was digitally signed and apparently did not yield any immediate concerns when it was released (Constantin). This weaponized plugin, dubbed SUNBURST, remained dormant on systems for up to two weeks, in order to prevent detection. After it “awoke”, the code began executing commands that allowed it to transfer files, execute program files, reboot the system, and disable services. All of this network traffic was hidden under the guise of the Orion Improvement Program protocol and hid data within legitimate configuration files. It also used blocklists to identify forensic and anti-virus tools that would cause alert (FireEye). Obviously, this attack was masterminded to spy on the innerworkings of SolarWinds customers and glean all sorts of private data.

The SUNBURST attack did make use of a malware dropper, named TEARDROP, however, the attack seemed to favor lateral movement, using methods such as credential stealing, as its means of progression (Constantin). FireEye detected SUNBURST activity around the world, thus making this a global attack of even greater concern (FireEye). FireEye has created a GitHub repository that includes a list of detections and signatures to help companies detect potential attack agents in their systems (FireEye).

According to their initial report on December 13, FireEye stated that the campaign “may have begun as early as Spring 2020” (FireEye). However, a more recent timeline places the exploitation as occurring as early as October 2019 (Baker). This would mean that attackers were hiding in the SolarWinds Orion software for over a year without being discovered. At a congressional hearing before the Senate Intelligence committee on February 23, 2021, the President of Microsoft, Brad Smith, testified that an estimated 1,000 attackers were involved in engineering the SUNBURST attack. Those testifying, representing both Microsoft and FireEye, agreed that Russia appeared to be the country behind the attack. This idea was accepted by many almost as soon as the breach became public; however, there some who question it (Baker).

On December 13, 2020, SolarWinds notified customers of the security event and urged them to immediately upgrade to Orion Platform 2020.2.1 HF1 to protect themselves from the threat. That same day, the Department of Homeland Security published "Emergency Directive 21-01" for federal agencies on dealing with the mitigation of the SolarWinds Orion code compromise. This directive claimed that the exploitation "poses an unacceptable risk…and requires emergency action." It also stated that, when it was written, the only known mitigation was disconnecting affected devices. However, it added that if the affected agency had IT expertise, they should forensically image the system memory and operating system of the affected devices and analyze their stored network traffic for signs of attack. (Department of Homeland Security). Unfortunately, because the attackers managed to live in the systems for so many months, it was unlikely that analyzing the network traffic produced many valuable results.

The Department of Homeland Security has published three supplemental guidance reports to their original emergency directive. The most recent of these was published on January 6, 2021, and it further specified which versions of the SolarWinds Orion software was affected by the attack as well as separated federal networks into three different categories, each with its own specific instructions on how to mitigate the breach. Regardless of the "category" an agency was placed under, the supplemental guidance ordered everyone to to upgrade to at least version 2020.2.1 HF2, which the NSA deemed to be free from the malicious code. The guidance further cautioned agencies that upgrading to 2020.2.1 HF2 did not guarantee security, considering the attackers' knowledge of SolarWinds' innerworkings and the fact that the previous attack remained unnoticed for so long. Agencies should still be aware of the risk that is involved with using any SolarWinds Orion products at this point (Department of Homeland Security).

SolarWinds has taken several measures to address concerns regarding SUNBURST, such as removing the vulnerable downloads from their websites and providing multiple software updates (with security improvements) in supported versions of the Orion server. One drastic step the company took just recently is the revocation of the code-signing certificate that was used to okay the vulnerable software updates (Security Advisory FAQ: SolarWinds).

On January 27, 2021, it was announced that SolarWinds was also subject to a malware attack, dubbed SUPERNOVA. Like SUNBURST, this malware targeted the Orion platform; however, it was not a supply chain attack. Rather, it was directly placed on a SolarWinds Orion-hosted system by an attacker (Malware Analysis Report (AR21-027A)). SUPERNOVA does not seem to be near the same magnitude as SUNBURST. This not to say that it is not an issue; it is a big deal. SolarWinds is a company that offers networking IT software, and a key element of IT is providing security. Alas, these events prove SolarWinds failed to provide security to their own software.   There are still a lot of unknowns about the attacks on SolarWinds; however, it goes to show that security should be a major concern and unfortunately, it is not being considered as seriously as it should be. As a result of the vulnerabilities in the Orion platform software, multiple U.S. government agencies suffered exposure to an unknown entity. This is never acceptable, but it is especially alarming when it is bureaus such as the National Nuclear Security Administration and the Department of Homeland Security, which defend our nation from attacks, even the exact type of attacks they were exposed to. One would think that, especially now with the recently formed Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, government systems would be safe from intrusion and security would be under control; however, this obviously is not the case. All companies, regardless of who they service, need to make security a high priority in order to prevent the next cyber disaster.

Works Cited

Baker, Pam. “The SolarWinds Hack Timeline: Who Knew What, and When?” CSO Online, CSO Online, 5 Apr. 2021, www.csoonline.com/article/3613571/the-solarwinds-hack-timeline-who-knew-what-and-when.html.

Constantin, Lucian. “SolarWinds Attack Explained: And Why It Was so Hard to Detect.” *CSO Online*, CSO, 15 Dec. 2020, www.csoonline.com/article/3601508/solarwinds-supply-chain-attack-explained-why-organizations-were-not-prepared.html.

Department of Homeland Security. “Emergency Directive 21-01.” *Cyber.dhs.gov*, Department of Homeland Security, 13 Dec. 2020, cyber.dhs.gov/ed/21-01/.

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

Krebs, Chris. “SolarWinds Hack Could Affect 18K Customers.” *Krebs on Security*, 15 Dec. 2020, krebsonsecurity.com/2020/12/solarwinds-hack-could-affect-18k-customers/.

Marshall, Joe, and Paul Smith. “The SolarWinds Orion Breach, and What You Should Know.” Cisco Blogs, Cisco, 8 Feb. 2021, blogs.cisco.com/security/the-solarwinds-orion-breach-and-what-you-should-know.

“Malware Analysis Report (AR21-027A).” *Cybersecurity and Infrastructure Security Agency CISA*, 26 Jan. 2021, us-cert.cisa.gov/ncas/analysis-reports/ar21-027a.

“Security Advisory FAQ: SolarWinds.” *IT Management Software & Remote Monitoring Tools*, 6 Apr. 2021, www.solarwinds.com/sa-overview/securityadvisory/faq#question3.

“SolarWinds Customers.” SolarWinds, 2020, web.archive.org/web/20201213234819/https:/www.solarwinds.com/company/customers.