2020

Anatomy of the SolarWinds Breach / SunBurst Hack

SHIVAJI SENGUPTA & MARLON JOHNSON

MAGNUS MANAGEMENT GROUP LLC | www.mmgllc.us

There are many entities throughout the world that use third-party software as part of their business. When they do this, the service they receive form part of the supply chain of the company. SolarWinds is a key vendor with 33,000+ of the world's companies and government entities use their software. The 22-year-old US-Based company, supply system management tools that are used by the IT professions within these organizations. The tools are responsible for a number of important services including software management, application monitoring, network configuration, etc. The Orion suite in particular, is SolarWinds most widely deployed network management system. It is used to manage and monitor the network infrastructure of the host company. To do its job effectively, the Orion suit needs absolute visibility of the company's diverse set of network technologies. For this reason, it is common practice for network administrators to configure SolarWinds Orion with extensive privileges consequently, making it the perfect target for threat actors. On December 13th, 2020, it was discovered that the Orion software suit was infected with the malicious software called Sunburst.

What happened?

According to the Cybersecurity & Infrastructure Security Agency's (CISA) incident response investigations team, an advanced persistent threat (APT) actor patiently leveraged a software supply chain compromise of SolarWinds Orion suits. In other words, instead of attacking the department of Treasury directly, the APT hacked their software provider (in this case SolarWinds). The attack successfully added a malicious file into the SolarWinds software lifecycle. The file itself is a core Data Link Library (DLL) that has a backdoor list that communicates via HTTP to third-party servers. This file is a part of the standard Windows installer patch file that includes suppressed resources associated with the update. Once the update is installed the malicious DLL is loaded into the system. It stays inactive for a while then it retrieves and executes commands that will transfer files, disable system services and reboot the system. This kind of access can be used to access sensitive information which will be sent back to the attackers.

When did this happen?

The world learnt that cyber intelligence company FireEye, was breached on December 8th, 2020. Five days after that, we learnt that more businesses were victims, including government agencies. It would appear that these intrusion events were anticlimactic since, according to the SolarWinds Sunburst timeline, the attackers were patiently conducting their advanced persistent threat since September 2019. The following bullet points abbreviates the moments leading up to the present investigations:

September 4, 2019: A threat actor accessed SolarWinds
September 12, 2019 - November 4, 2019: The threat actor injected test code and performed a trial run.
December 2019: The hackers accessed at least one of SolarWinds' Office 365 accounts. From there, they eventually gained access to the company's email environment.
February 20, 2020: SUNBURST attack was compiled and deployed
March 26 2020: Hotfix 5 DLL available to customers.
June 4, 2020: Threat actor removes malware from build VMs.
December 8, 2020: FireEye announced that they were breached by state-sponsored threat actors. They discovered that their Red Team Penetration Testing tool was stolen.
December 11, 2020: FireEye discovered that the threat stemmed from SolarWinds Orion updates. It was discovered that hackers did not only corrupt the system but weaponized it.
December 12, 2020: The National Security Council (NSC) discusses the companies and government agencies that were breached. This meeting was held at the White House.
December 13, 2020:
SolarWinds receives an order from CISA to power down their Orion suite because of the threat it posed.
SolarWinds' customers receive a security advisory.
December 14, 2020: SolarWinds discloses the breach and their stock plummets
December 15, 2020:
SolarWinds releases software fix.
Some of the attack victims were revealed. They include the U.S. Commerce and Treasury Departments; the Department of Homeland Security (DHS), the National Institutes of Health and the State Department.
December 16, 2020:
A key malicious domain name used in the attack has been commandeered by security experts and used as a "killswitch."
As part of their threat response responsibilities, the FBI has announced its efforts to investigate in order to find the APT responsible.
December 17, 2020:
40% of Microsoft customers were specifically targeted. Microsoft discovered that 44% of those targeted were IT service providers. Some of these companies were software providers.
Five IT solutions providers and consulting firms — Deloitte, Digital Sense, ITPS, Net Decisions and Stratus Networks — were discovered to be breached via the SolarWinds Orion vulnerability.
It was discovered that the National Nuclear Security Administration was breached. This government agency is responsible for the U.S. nuclear weapons stockpile.

The White House is meeting daily to discuss the SolarWinds Orion breach, attack victims, potential fallout, and a potential response.

December 21, 2020:

The unclassified systems of the US Treasury Department were impacted by the Hack.

Organizations such as Cisco Systems, Intel, Nvidia, Deloitte, VMware and Belkin had installed the infected SolarWinds Orion software, though it's unclear if the hackers actually took additional steps once the infected software found its way into those organizations.

December 22, 2020: High Ranking officials at the US Treasury department experienced email compromise.

December 23, 2020: Crowd Strike was targeted but the attacker's efforts were unsuccessful.

December 23, 2020: SolarWinds summarizes its latest patches.

December 30, 2020: CISA sends out new advisory on the SolarWinds Orion vulnerability

December 31, 2020: Microsoft says Russian hackers viewed some of the software company's source code, but the hackers were unable to modify the code or get into Microsoft's products and services.

January 5, 2021:

Several U.S. intelligence agencies attribute the sunburst attack to Russia.

Software company, Sentinel One launched a free open-source software to help affected companies identify the Sunburst malware in their environment.

January 11, 2021: SolarWinds CEO disclosed an updated attack timeline, indicating that hackers had first accessed SolarWinds on September 4, 2019.

What are the implications?

The implications for the Sunburst attack are far reaching and unimaginable. Consider firstly the nature of the solar winds tools as discussed earlier. The Orion suite is a network management tool. Which means it has privileges to freely access other parts of an entity's network. By having such access, attackers have essentially unlocked the keys to company's secrets, PII, PHI, government secrets, etc. The fact that SolarWinds are used by over 33,000 companies worldwide which includes Fortune 500 companies, Utilities, Military, healthcare facilities and all branches of government. We are potentially at the threat actor's mercy.

Looking back on the timeline, we have seen organizations along with the US Government making efforts to do damage control, like the call for federal agencies to shut down the SolarWinds system, the release of security patches and other charitable efforts by companies that provide free software to identify the Sunburst malware. But even if all the issues are solved perfectly, it might be too little too late, since the threat actor has been in the system from 2019. It is unthinkable how much

data has already been stolen. In fact, the attackers had more than enough time to escalate privileges and drill further into important systems. The fact of the matter is, we may not even know for sure the magnitude of the damage or how the stolen data will be used for some time to come.

What can we do?

In spite of the challenges associated with the Sunburst Attack, all mitigating factors must be considered. The first step towards mitigation is to identify the level of exposure. CISA ranks the level of exposure using a category system. Companies and government agencies at the category 1 level include those that have conducted a thorough forensic investigation and have identified no trace of the malicious Sunburst code on their network. Another qualifying factor include entities that have never employed the affected versions of the SolarWinds Orion product. On the other hand, organizations that fall within category 2 & 3 can confirm that they were exposed to the malware at varied levels.

Entities with a category 2 rating can confirm a mild exposure to the Sunburst malware. Based on forensic investigations it can be proven that no form of escalation had taken place. At this level, it is highly recommended that their platform is rebuilt, secured and hardened using the configuration guidelines outlined by SolarWinds. Before network services can commence, a thorough risk evaluation must be completed.

Companies with a category 3 rating have experienced severe exposure to the Sunburst attack which means the attackers may have attained administrative level access. The only remedy in this case is a complete overhaul of the network. This will require a complete rebuilding of the environment, to include the reconstruction of identity and trust services, as recommended by CISA.

.