Jimisha Cosby
CS 462
4 December 2022
Professor Susan Zehra

SolarWinds Attack

Introduction:

What Happened

The SolarWinds attack was a cybersecurity attack that targeted private and public organizations by way of advanced persistent threat. Multiple government agencies and major commercial instrudies around the world were affected. This also affected around 18,000 of the 300,000 customers of SolarWinds (Cisecurity). These customers were running and executing the vulnerable versions of the platform.

Who Was Involved

There were many different departments, organizations, and companies that were affected by this attack. Some that were attacked include: Homeland Security, Treasury, State, and Commerce – this was believed due to supposed missing emails from their systems. Companies including Intel, Microsoft, Cisco, Deloitte, and FireEye –the company that discovered the attack in the first place– were also affected. As for the attackers, they are believed to be Russian.

When The Attack Happened

Through forensics, it is believed that the SolarWinds attack occured in March of 2020, while files were being compiled from December of 2019. The attack was announced to the public on December 13, 2020.

The Purpose of the Attack:

FireEye, a cybersecurity company, found the APT supply chain attack on SolarWinds products. They found this in the midst of investigating their own network's vulnerabilities. This advanced persistent threat attack was done by inserting a backdoor and embedding themselves into a new SolarWinds update. When customers downloaded it, the attackers were now able to access SolarWinds products systems.

The attackers were very calculated in this attack, doing everything they could to stay undetected for as long as possible. The main purpose of the attack, however, still remains to be seen.

The Technology Used In The Attack:

In this attack, there were several systems of SolarWinds that were affected. The systems that were affected include: SolarWinds Orion Platform Version 2019.4 HF 5, SolarWinds Orion Platform Version 2020.2, and SolarWinds Orion Platform Version 2020.2 HF 1 (Cisecurity). As mentioned earlier, the attacker's way of getting into the system was through a backdoor. Security analysts discovered that on top of the SUNBURST backdoor, there were also 4 additional pieces of malware that were a part of the attack. The SUNBURST back door was believed to be delivered into SolarWinds systems from an initial implant called SUNSPOT. There is a “post exploitation, memory resident dropper” called TEARDROP. So far, it is believed to have dropped BEACON, a payload with Cobalt Strike, that is used by security professionals and malicious actors for things including moving laterally across protocols and other command and control functions. A recent discovery found something similar to TEARDROP moving laterally across those networks that were affected and compromised because of SUNBURST; it is called RAINDROP.

The Long Term Consequences:

With an attack of this magnitude, there is bound to be a major societal impact, as well as potential consequences. This attack spanned across the globe and affected major systems in the global market, from companies to government departments. This attack went undetected for a long period of time and that is the scary part– no one knows exactly what was taken or monitored during this attack as of now. This hack emphasizes a need for more cybersecurity aspects and jobs in the country. It has shown governments that they need to stay proactive when it comes to protecting their systems, and that they should always test their own systems' vulnerabilities in order to patch or monitor them, and protect them against inevitable future attacks. Since the attack, Solar winds has had patches for the vulnwrabilites and encourages customers to update their systems as well as update or change any passwords linked to accounts of the compromised servers.

References

https://www.cisecurity.org/solarwinds

https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know