SolarWinds breach, one of the worst cyberattacks in history

Nicholas Robertson

CYSE 300

Dr. Joseph Kovacic

January 19, 2023

SolarWinds is a software company that specializes in software that helps businesses manage their network, systems, and information technology. They provide their services to companies all over the world including to multiple government agencies like the department of Homeland Security, State, Commerce and Treasury. Out of all the other network management service providers, SolarWinds were at the top of the food chain. But on December 13, 2020, an alert would be made out to the public signifying that the U.S. government had been attacked through a cybersecurity breach, most likely by nation state actors and it all revolved around a system called SolarWinds. So, what were the vulnerabilities, how did the threat exploit it, what were the repercussions, and how could it have been mitigated? To answer these questions, we must understand how this attack even happened in the first place.

In November of 2020 a professional cybersecurity service firm known as FireEye was the first organization to find and report that there was an intrusion within the SolarWinds monitoring system known as Orion. The attack was deemed a supply chain attack, meaning that the malware within was granted access though a distributer (SolarWinds) and disguised itself as a legitimate piece of software. The hackers use the SolarWinds, Orion system as a backdoor access point to pull this off this attack. This method of attack was perfect for the hackers, as it allowed them to gain access to the multitude of different companies, without the need to directly hack a certain network. The backdoor method is an obvious vulnerability that exist in a lot of companies, but it wasn't the only one that was used within this attack. The supply chain attack took some time to implement, going off the timeline provided by the site TechTarget.com it seems, that the hackers infiltrated and gained access to the SolarWinds network on September 2019. From October 2019 – February 20th, 2020, the injected test code that the hackers injected into Orion, sat on its system where it finally received the name Sunburst and became what we

know of it today. Finally on March 26th, 2020, the code was unknowingly sent out an update for Orion. Interesting enough, Sunburst was never detected during the time it was hibernating within the supply chain. On the site Mandiant.com there is a threat research post made by the firm FireEye going over the attack in more detail. They claimed that "SUNBURST performed numerous checks to ensure no analysis tools are present. It checks names, file write timestamps, and Active Directory (AD) domains before proceeding." (Stephen Eckels, Jay Smith, William Ballenthin, 2020). They believe this was how Sunburst was able to avoid the numerous anti-virus checks and forensic investigators for the better part of a year.

The repercussions of the incident were felt though many companies and government organizations in the US. With over 18,000 customers effected by the attack including government agencies. The interesting thing about this attack seems to be the suspicion that many of the other companies seem to have been collateral, with the main target being the government agencies. It has been reported in Reuters that, "The hackers stole digital certificates used to convince computers that software is authorized to run on them and source code from Microsoft (MSFT.O) and other tech companies." (Joseph Menn and Christopher Bing, 2021). We can assume that more has been stolen, but it's unknown how much has been stolen and not released to the public conscious. The more concerning aspect to this whole incident however is the long-term effect of this attack is still unknown. Currently agents are still investigating and trying to find out who was behind this attack, but the only thing they can go off on now is that it was possibly nation state actors from Russia behind it.

Mitigating an attack like this requires a lot of foresight, but it also requires a lot of regular maintenance to your system. Looking at the site DarkReading.com, they give use a list of four important actions that should have been taken to prevent this attack from happening in the first

place. The first one being, audit active directories and changes and this one should be common placed in every organization. Accentually it requires that there be a note or change log implemented, whenever someone makes changes or request to change something within the system. This gives a clear track of names and time on who tampered with the systems code. The second solution would be to implement SIEM and Log Management, which is the same as the previous solution, except that it makes flags of suspicious activities, by making multiple logs within the system to alert the company that something might be going on. The third option is to fine-tune your DLP (data loss prevention), which can be managed to audit trusted software to see how many files are being added with the new updates and exactly what type of information is being created. Finally conducting regular penetration testing, which is the process of hacking into your own system to find vulnerabilities and fix them when needed. On DarkReading.com they claim that "if penetration testing had identified that environment as vulnerable. The attack could've been prevented at the login stage." (Joseph Cortese, 2021). I point this out because out of every other solution, this one seems like the most effective in preventing the attack. As mentioned before this malware did everything it could to avoid detection and intentionally stayed dormant to further its objectives. I feel as though the only way to really know if there was something in the system before it got out would be to take more of a hands-on approach and go through the system yourselves.

In the end the SolarWinds attack was a sophisticated and unpredictable attack that infiltrated hundreds of companies and government organizations around the country. I believe that this is the worst cyberattack by far. Mainly because while no catastrophic outcomes came of this so far, the fact that the government organizations could be compromised and have information stolen off their systems that easily is terrifying to think about. The good news is that

this event has brought some attention to the current state of cybersecurity. And hopefully it can be a reworking of the cybersecurity system from the ground up.

Works cited:

Stephen Eckels, Jay Smith, William Ballenthin (2020) SUNBURST additional technical details https://www.mandiant.com/resources/blog/sunburst-additional-technical-details

Joseph Menn and Christopher Bing (2021) Hackers of SolarWinds stole data on U.S. sanctions policy, intelligence probes https://www.reuters.com/world/us/hackers-solarwinds-breach-stole-data-us-sanctions-policy-intelligence-probes-2021-10-07/

Joseph Cortese (2021) How to avoid falling victim to a SolarWinds-style attack https://www.darkreading.com/risk/how-to-avoid-falling-victim-to-a-solarwinds-style-attack

Saheed Oladimeji, Sean Michael Kerner (2022) SolarWinds hack explained: Everything you need to know, *SolarWinds breach news center* https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know