Jack Sweeney
Michael McAlpin
CIS3360
9/15/2022

Cyberattack Case Study: 2020 SolarWinds Hack

(Trenton Systems, 2021)

Introduction

In 2020 hackers made their way into one company's system and injected malware into its software. The company unknowingly pushed this infected software to thousands of customers' systems. The company is SolarWinds, which develops software for businesses to manage their technology, systems, and IT infrastructure. This attack is equivalent to the attackers giving the primary victims malware, and the main victims do all the work. They continue to spread the malware to thousands of their customers.

Target Groups

The primary victim of this cyberattack was SolarWinds. Hackers modified SolarWinds “Orion" software on SolarWinds systems and then pushed it out in updates to even more victims.

According to Jibilian, the infected update was sent out to 18,000 clients (Jibilian, 2021). Many of the thousands the update it was sent out to were major companies and agencies. Some companies are Cisco, Intel, Nvidia, VMware, and many more. Among US state agencies, the following were victims, The Department of Commerce, the Department of Defense, the Department of Energy, and the Department of Homeland Security. This attack's main domain and target are government organizations and companies with extensive IT infrastructure. SolarWinds Orion software is for managing and monitoring IT infrastructure so anyone who had the software for that need could have been part of the group attacked. IT infrastructure is used everywhere now from schools to the military so the possibilities for those to have been attacked is large.

The Attackers

This attack's main perpetrator was Russia, specifically the Russian Foreign Intelligence Service. The first attack was in September 2019 to test the strategy, and starting in February 2020, Russia injected a trojan into the SolarWinds code (US GAO, 2022). Russia has a history of cyberattacking against the US and other nations, including Germany, Ukraine, Estonia, and Georgia. Russia has performed various attacks, including denial of service, taking over social media, and hacking into multiple systems. Russia has used attacks to gain influence over other nations' elections and to gain intelligence over others. Many of the previous attacks by Russia have been successful. This specific hack was done for the same reason for Russia to gain an edge or espionage over the United States, whether that be over the government and private companies in the United States.

The Attack

This attack by Russia, known as the SolarWinds SUNBURST attack or UNC2452, is a supply chain attack. Russia modified the source code on SolarWinds Orion software; the modified software included a backdoor. This code was eventually pushed in an update by SolarWinds-to-SolarWinds clients who used Orion software. SolarWinds was unaware of the modification and the code was still signed by SolarWinds, so the update would go out unknowingly and normally. Any clients who had installed the update now had a backdoor in their systems that Russia could use. The backdoor in the SolarWinds software recurrently sent a DNS query to the hacker's servers with identifying info of the organization that was running the

SolarWinds Orion software. The DNS query that was sent looked like the following "<DGA_value>.appsync-api.eu-west-1[.]avsvmcloud[.]com," according to *Truesec* (2020). "DGA_value" in the DNS query contained an encoded version of the Active Directory name, like a domain name which is the information that was used to identify the organization. Depending on the response of the DNS query, the backdoor would act with different further actions, which could be different based on who Russia further wanted to attack. When the DNS responded with a NetBios response, the backdoor would start a further stage of the attack. Other responses reset the backdoor (Ipx) or terminated it (Atm). The targets that received NetBios responses started an HTTP backdoor to gain further access and additional information to the hosts, and this allowed the possibility for different malware to be injected into the victim's networks.

Distinctiveness

Supply chain attacks like this SUNBURST attack have happened before but they are generally rare compared to other types of cyberattacks. As the name implies a supply chain attack requires access to the supply chain, which is much more complex than gaining access to an individual system via a vulnerability. The supply chain is usually watched over closer. An interesting aspect of this attack is how the backdoor is controlled. It uses DNS queries, and based on the response of the query, the backdoor will act differently. Usually, you would expect the backdoor to communicate over HTTP or other protocols, not DNS. This DNS use makes the backdoor communication harder to detect because DNS traffic isn’t usually expected to be malicious.

Information Exposed

The attack allowed Russia to access several private and government organization systems for several months. One of the organizations previously mentioned was the Department of Homeland Security. The attackers supposedly had access to email accounts of the Department of Homeland Security. The email accounts included the head of DHS and other officials. The full extent of the attack and exposed information is not fully known as there were so many victims, so it is sure to be more.

Active Descendants

After the attack was discovered, SolarWinds issued an urgent security update to remove the backdoor. On versions that have the backdoor, it was possible to kill the backdoor by modifying DNS queries of the domain that the backdoor used; the response from DNS would tell the backdoor to stop operation and no longer proceed. This was necessary before the update was available or for those who haven't updated the software. The problem is those who have updated and previously had the backdoor may still have attackers in their systems. The attackers may have already gained further access during the time when the back door was available. The other access by the attackers is likely not patched by the SolarWinds update, so attacks may still be going on to this day which all started from SUNBURST. It's similar to this analogy; once you have one door open and you open more, just because you close the original door doesn't mean all the rest close. Supply chain attacks are still possible as there are still some security concerns, and nothing is never 100% secure. Even after this attack, Codecov had a supply-chain attack like the SUNBURST attack.

Preventative Actions to Stop Similar Attacks

SolarWinds, the primary victim of this attack, says they are reviewing their security practices and investigating their connection with partners and the supply chain to prevent attacks like this from happening again. One thing SolarWinds has encouraged is open-source software. Opensource adds transparency and the ability for others to overview the company, allowing them to point out security concerns and problems.

Punishments on Russia

The United States and the Biden administration have enacted several sanctions against Russia for the SolarWinds SUNBURST attack. One of the sanctions was put on six Russian technology companies that provide support for intelligence works. Another embargo enacted prevents US banks from getting bonds from Russia's Central Bank. The final sanction goes after 32 people who tried to influence the 2020 election. The US said that the attacks were too hostile and nothing to the level of anything the US does.

Works Cited

Jibilian, I. (n.d.). *The US is readying sanctions against Russia over the SolarWinds cyber attack. here's a simple explanation of how the massive hack happened and why it's such a big deal*. Business Insider. Retrieved September 14, 2022, from https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12

The Solarwinds Orion Sunburst Supply-Chain Attack. Truesec. (2020, December 16). Retrieved September 15, 2022, from https://www.truesec.com/hub/blog/the-solarwinds-orion-sunburst-supply-chain-attack

Trenton Systems. (2021). *The SolarWinds Orion Hack Explained*. Trenton Systems. Retrieved September 16, 2022, from https://www.trentonsystems.com/blog/solarwinds-hack-overview-prevention.

U.S. Government Accountability. (2022, February 1). *Solarwinds cyberattack demands significant federal and private-sector response (infographic)*. U.S. GAO. Retrieved September 14, 2022, from https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic