SolarWinds:

A deeper dive into the details concerning the attack

Alex Garza

Supervisor: Anil Garimidi

Mentor: Jamie Crow

June 28, 2021

Abstract

SolarWinds is one of the most significant cybersecurity attacks to ever take place so far in history. This event is such a major event due to the effect it had. Usually these attacks affect a single company, but the advanced supply chain affected thousands of organizations, even the US government. Investigations are still under way, there is a great deal still unknown about the hack. There are new discoveries each day that help us piece together the entire event. This paper examines the details pertaining to the SolarWinds hack.

Background of the attack.

SolarWinds is a company that supports its clients by supplying software called Orion to monitor and manage IT networks. More than 30,000 public and private organizations use the Orion network management system to manage their IT resources. SolarWinds was the perfect target for this attack due to the wide variety of multinational companies and organizations that use their Orion software. Investigations into the breach show that the hackers infiltrated SolarWinds' Orion software as early as January 2019 for early recon purposes. This infiltration allowed the hackers to use a routine software security update to install malicious software in the company's clients' network. Microsoft stated, "at least 1,000 very skilled, very capable engineers" worked on the SolarWinds hack. Although not independently verified, the identity of the perpetrators is suspected to be a Russian intelligence agency. 18,000 of SolarWinds clients downloaded the infected software update. More than 1,000 clients received the second stage malicious code, which is operated by hackers to manage malicious code once it's inside a target network which is known as "command and control". Investigators have so far determined that at least 200 clients were further hacked.

The hackers reasoning.

Initial analysis indicates the goal of this hack was espionage. Meaning the intention is not meant to damage, disrupt or destroy networks, but rather to gain intelligence. The SolarWinds hack was also designed to gain an initial presence on a large number of networks. While the intent seems to have been to gather intelligence, the operations could be technically repurposed by the Russians at a time of their choosing to deliver a destructive effect. This may include attempts to figure out how U.S. federal agencies and American companies respond to a hack. Allowing for the hackers to use that knowledge to attack with more sophistication in the future. Their operations could also be hijacked by others with hostile intent, or could malfunction, causing an unintended accident.

What techniques they used to do it.

The hackers seem to have taken advantage of the inattentive security practices to infiltrate SolarWinds at first and, by hiding within that security update, evaded the clients' cyber-security defenses. A supply chain attack was the attack used in SolarWinds. Which is a technique that inserts malicious code or a malicious component into a trusted piece of software or hardware. With this inserted into a single supplier, hackers can turn any application, software, or hardware that they distribute into Trojan horses. With just one well-placed intrusion, it can quickly spread to the networks of a supplier's customers. The reason supply chain attacks are so hard to combat is because you are trusting every vendor whose code is on your machine, as well as trusting every vendor's vendor. Due to the software being trusted it is thought by the company that the code inserted is just trusted as well. In 1984, Ken Thompson one of the creators of Unix OS stated, "You can't trust code that you did not totally create yourself."

How to prevent more attacks like this in the future

The US needs to review and renew its approach to national cyber security, while at the same time working with allies and partners to redefine the boundaries of responsible cyber behavior. All organizations should plan for maximum resiliency, and perhaps new domestic regulations mandating the notification of breaches are necessary. To improve resiliency companies should make sure vendors are trusted. The notification of breaches early on could help other companies and it users that may use the software to uninstall it and prevent further intrusion. Companies are now assuming that there are already breaches, rather than merely reacting to attacks after they are found. This seems necessary due to the fact that the Solarwinds intrusion took place many months before it was initially discovered.

Impact on the company?

While the full extent of the SolarWinds breach is still under investigation, it is publicly known that at least nine U.S. federal agencies and about 100 private companies were hacked. The hackers gained access to sensitive data and emails of these companies. As stated previously, the intent was not to harm the company's but rather to spy on them and collect data. Due to the data breach hackers now have insights such as weaknesses, vulnerabilities, as well as defense strategies that each affected company used. Risks also associated with this hack that are not yet present would be employee and customer information being held for ransom as well as possibly leaking future product plans of an organization. BitSight is a cybersecurity ratings company that analyzes companies. Kovrr presents companies with data-driven insights into their cyber risk exposures. BitSight and Kovrr break down the different elements into cost components to produce the cost associated with the breach. This estimate is based on the specific organization location, industry, and size. Further analyzing the cost of forensics, incident response, regulatory

fines, and public relations services to communicate information about the attack. The estimate of insured losses from the SolarWinds hack amount to $90,000,000 for those companies with cyber insurance coverage.

Conclusion

This attack taught us that there are many things that we do not know about that is going on behind the scenes. The attack is still under investigation and new information is being discovered daily to help us fully grasp the extent of this attack. The timeline of events currently present in many other research papers are incorrect due to there being new information released/discovered about when SolarWinds was actually infiltrated. SolarWinds taught us many valuable lessons such as no matter how secure a network is hackers will always find a way in. SolarWinds is one of the most significant cybersecurity breaches of the 21st century.

Works Cited:

Adriano, Lyle. "SolarWinds Trojan Hack Estimated to Cost Cyber Insurers $90 Million." *Insurance Business*, Key Media, 15 Jan. 2021, www.insurancebusinessmag.com/us/news/cyber/solarwinds-trojan-hack-estimated-to-cost-cyber-insurers-90-million-243638.aspx.

Greenberg, Andy. "What Is a Supply Chain Attack?" *Wired*, Condé Nast, 31 May 2021, www.wired.com/story/hacker-lexicon-what-is-a-supply-chain-attack.

"Hackers Targeted SolarWinds Earlier than Previously Known." *SeekingAlpha*, Seeking Alpha, 19 May 2021, www.seekingalpha.com/pr/18325545-hackers-targeted-solarwinds-earlier-previously-known.

Oladimeji, Saheed Sean Michael Kerner. "SolarWinds Hack Explained: Everything You Need to Know." *WhatIs.Com*, TechTarget, 16 June 2021, www.whatis.techtarget.com/feature/SolarWinds-hack-explained-Everything-you-need-to-know.

Panettieri, Joe. "SolarWinds Orion Security Breach: Cyberattack Timeline and Hacking Incident Details." *ChannelE2E*, 29 June 2021, www.channele2e.com/technology/security/solarwinds-orion-breach-hacking-incident-timeline-and-updated-details.

Paul, Kari. "SolarWinds Hack Was Work of 'at Least 1,000 Engineers', Tech Executives Tell Senate." *The Guardian*, Guardian News & Media Limited, 24 Feb. 2021, www.theguardian.com/technology/2021/feb/23/solarwinds-hack-senate-hearing-microsoft.

Ramakrishna, Sudhakar. "New Findings From Our Investigation of SUNBURST." *Orange Matter*, SolarWinds Worldwide, 12 Jan. 2021,

www.orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst.

Shah, Samit. “The Financial Impact of SolarWinds Breach.” *BitSight*, BitSight Technologies, 12 Jan. 2021, www.bitsight.com/blog/the-financial-impact-of-solarwinds-a-cyber-catastrophe-but-insurance-disaster-avoided.

Turton, William. “List of Hacked Organizations Tops 200 in SolarWinds Case.” *GovTech*, e.Republic, 20 Apr. 2021, www.govtech.com/security/list-of-hacked-organizations-tops-200-in-solarwinds-case.html.

Willett, Marcus. “Lessons of the SolarWinds Hack.” *Taylor & Francis*, Informa UK Limited, 30 Mar. 2021, www.tandfonline.com/doi/full/10.1080/00396338.2021.1906001.