A LOOK INTO THE SOLARWINDS CYBER ATTACKS

Dae'lyn Bellamy

Deparment of cybersecurity

CYSE 300

Proffessor: Dr. Joseph Kovacic

9/8/2024

INTRODUCTION

Today, In this paper I will be going over the SolarWinds cyber attack that happened on December 2020 and affected over a thousand organizations as well as the United States government. I will be going over what SolarWinds is as well as the vulnerabilities within Solarwinds that allowed this to happen, how the hacker exploited those vulnerabilities, the repercussions of this attack, as well as what could have been done to have prevented this from having occurred in the first place. Now that you know what we will be covering today, let us begin with our first section explaining what SolarWinds is.

WHAT IS SOLAR WINDS.

Solarwinds is a cybersecurity company that offers system management tools networks and infrastructure observations, as well as many other cybersecurity services to over a hundred thousand customers and organizations (Saheed Oladimeji, 2023). Now that you understand what SolarWinds is let's see what vulnerabilities they had that allowed this attack to occur.

CYBERSECURITY VULNERABILITIES and THEARTS THAT EXPLOITED IT

The SolarWinds company had also been operating and selling a monitoring software called Orien, which had high privileges within a system or network. When this software was breached it allowed the hacker to gain access to the networks, systems, and data of thousands of SolarWinds customers(Saheed Oladimeji, 2023). This was able to happen because the attackers used a method of attack called a supply chain attack. A supply chain attack is a type of malware that exploits a third-party software, hardware, or applications(CloudFlare). This meant that instead of hacking into the Orien system directly the hackers were able to instead get into a third-party's system which then allowed them access to Orien and any organization or user that was using it all awhile avoiding detection from antivirus software and all the hackers had to do in order to get the exploit into orien was to inject the malicious code into one of its Update patches(Saheed Oladimeji, 2023).

REPERCUSSION OF THE INCIDENT

The aftermath of the attack led to government departments including Homeland Security and even the Department of Treasury being breached by the attack as well as any company that was using the Orien software. The United States government later found that some of its departments were missing emails from their systems(Saheed Oladimeji, 2023). 18,000 government workers were also exposed to the malware making this attack much worse than first thought, with most if not all of the United States departments being breached as well as defense contractors, national labs involved in the creation of nuclear weapons, and most fortune 500 companies were also breached(SecureMac & Team, 2020). The amount of data that was potentially stolen was massive with many experts saying that the SolarWinds hack was one of the most effective cyber attacks against the U.S.A ever (SecureMac & Team, 2020).

WHAT COULD HAVE BEEN DONE TO PREVENT THIS

Here are a few things that SolarWinds could have done to have prevented this from happening and hopefully things that they are now implementing into their security systems so this never happens again. The first thing that could have been done to lower the risk of a breach was to implement a third-party risk assessment this would mean testing third parties and making sure their security systems and policies are following specific guidelines(CloudFlare). They could have also “configured their firewalls to block outbound connections from the servers running SolarWinds” - CISA which would have stopped the malware (Satter, 2021).

CONCLUSION

In summary, SolarWinds is a cyber security company responsible for selling different kinds of security solutions for its customers, and in 2019 the SolarWinds orien software hit by a supply chain attack that was able to bypass the SolarWinds security measures by going through a 3rd party and injecting malicious code into the Oriens software update, which allowed it to compromise hundreds of thousands of systems and networks including the united states government. This led to a massive incident which leads many companies, individuals and federal government departments to be breached, allowing for many highly critical systems within the United States and its companies to be exposed and exploited. As a result The SolarWinds attack has been lebaled by experts as one of the most effective cyberattacks against this country. This cyber attack could have been stopped however if the SolarWind company had taken better measures to protect themselves such as implementing a third party risk assessment to test third party software and to check see if venders are following specific security measures.

SOURCES:

Saheed Oladimeji, S. M. K. (2023, November 3). *Solarwinds Hack explained: Everything you need to know*. WhatIs. https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know

What is a supply chain attack? | cloudflare. (n.d.). https://www.cloudflare.com/learning/security/what-is-a-supply-chain-attack/

SecureMac, I., & Team, S. (2020, December 18). *Solarwinds hack impacts U.S. government and military, exposes most of Fortune 500*. SecureMac. https://www.securemac.com/news/solarwinds-hack-impacts-u-s-government-and-military-exposes-most-of-fortune-500

Satter, R. (n.d.). Solarwinds hackers could have been waylaid by simple countermeasure -US officials | Reuters. https://www.reuters.com/technology/solarwinds-hackers-could-have-been-waylaid-by-simple-countermeasure-us-officials-2021-06-21/