SolarWinds Supply Chain Attack

Introduction

As our reliance on technology keeps increasing in this digital age, new threats and dangers are added into the equation. Because we have not found a way to protect systems and information with 100% efficiency, the likelihood of attacks will always be high. Whether the goal is disruption, theft, or destruction, there will always be people with malicious intentions who want to get into our systems and information. Opposing countries now conduct frequent cyber-attacks against each other to try and steal information and get an edge over each other. This new form of warfare called “Cyber Warfare” had a direct tie to the cyberattacks on SolarWinds back in 2020.

Background

SolarWinds is an American company that develops software for managing IT services such as networks, applications, databases, and security. They have over 300 thousand customers that use their products for IT purposes in their organizations. According to the US Government Accountability Office, SolarWinds is widely used by the federal government to monitor network activity on federal systems. This large-scale use of their products, including use by the US government means that the attackers in the SolarWinds cyberattacks were able to gain access to many different types of systems from many organizations. One specific product of theirs is the SolarWinds Orion software. According to the advertisement on their website “The SolarWinds Orion Platform is a powerful, scalable infrastructure monitoring and management platform designed to simplify IT administration for on-premises, hybrid, and software as a service (SaaS) environments in a single pane of glass.” This specific product it what lead to the cyber-attacks being sucessful

The Attacks

The SolarWinds product that was affected was their IT performance and management system called Orion. This software turned out to be a perfect target for cyber-attacks because in order to strengthen its network management, it had access to the user company's private logs and data. This means that if the attackers got into the Orion software, they could get valuable information from any company that used it. The attacks on SolarWinds initially started in late 2019. An unknown group at the time was conducting test attacks on SolarWinds and the Orion software. By 2020, the hackers were able to create a backdoor into a SolarWinds update server and insert their malicious code into the regularly scheduled Orion updates that consumers would then install. Specifically, the malicious code was interted into a normal library file that is used in Orion software updates. Usually, these files would have to be digitally signed to prove they havent been tampered with, but the attackers managed to compromise a SolarWinds certificate and used it to digitally sign the library file. The CISA believes that the initial access or break in was done by password spraying and said, “Incident response investigations have identified that initial access in some cases was obtained by password guessing, password spraying, and inappropriately secured administrative credentials accessible via external remote access services.”

Password spraying is where common passwords are tried on multiple accounts to see if there is an unsecure account. Multiple sources report that the attackers got in using a very easy to guess company password, being “solarwinds123 “. This type of attack is called a supply chain attack. A less secure 3rd party is targeted and used to get into other systems. The trojan that was uploaded to the update servers was nicknamed SUNBURST. Once they had gotten into a system, they started gathering any useful information such as passwords, account keys and tokens, remote access, and any sensitive information they could get their hands on. Because they got this information and posed as the users, they stole the information from, it took a very long time for anyone to figure out that there were intruders in their systems.

The Aftermath

The SolarWinds attack was reported to have affected more than 18,000 of their customers. Not only did this affect smaller organizations that used this software, but also corporations such as Microsoft and government agencies. The federal government widely used their network monitoring software, and it is still unknown exactly how much information the attackers were able to get. The US has identified the Russian Foreign Intelligence Service to be responsible for these attacks. They were likely conducted to try and steal important information from the US government agencies that used the Orion software. The US government and CISA have since been attempting to give guidance to companies to avoid software supple chain attacks and attack mitigation in general. This also led to the Biden Administration to create an executive order that mandated the US government only use software from vendors that provide Software Bill of Materials. These show consumers the exact contents of what is in a product, in this case, they allow consumers to decide for themselves if the product they want to use will be a danger to them and their organization. Part of the executive order stated that, “"Those who operate software can use SBOMs to quickly and easily determine whether they are at potential risk of a newly discovered vulnerability.”

The Ongoing Fight

The entire SolarWinds intrusion ended up being possible because of a very simple and easy to counter cyber-attack technique. Having secure passwords and authentication such as two factor authentication is very important. There should never have been an account in the organization that had such a guessable password such as “solarwinds123”. A simple mistake like this not only can lead to one organization being breached but as shown in the SolarWinds attack, can affect such many people. Organizations should require their employees to use secure passwords set by standards that the organization deems appropriate. Setting up two factor organization can greatly help secure accounts even if a password is compromised. Cyber-attacks are and will be a constant threat as we move farther into a digital age. Almost everything we do today has to do with technology and the internet. Because of this, we need ever evolving security standards and practices to combat these attacks

https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic

https://www.solarwinds.com/

https://www.securityweek.com/solarwinds-likely-hacked-least-one-year-breach-discovery

https://www.trentonsystems.com/blog/solarwinds-hack-overview-prevention

https://spycloud.com/solarwinds-attack-breakdown/