Supply Chain Attack
Case Study

SolarWinds

Design: **IBM**
Research by: **Murad Alnajjar**
Issue date: **01/03/2023**

According to ZDNET the SolarWinds hack could be classified as several different types of attacks, depending on how it is characterized. Some possible categories for the attack could include:

Attack Category

Supply chain attack

State-sponsored attack

Advanced persistent attack (APT)

Cyber espionage

- Supply chain attack: The SolarWinds hack was a supply chain attack, which is a type of cyber attack that targets an organization's supply chain to gain access to the organization's networks and systems.
- State-sponsored attack: The SolarWinds hack is believed to have been carried out by Russian state-sponsored hackers (group known as Cozy Bear). This means that the attack was likely sponsored or supported by the Russian government.
- Advanced persistent threat (APT): is a type of cyber attack that is characterized by its sophistication and the fact that it is carried out over an extended period. The SolarWinds hack is believed to have gone undetected for several months, which could classify it as an APT.
- Cyber espionage: The SolarWinds hack was a targeted attack that specifically sought to gain access to sensitive information, such as email and intellectual property. This could classify the attack as cyber espionage, which is the use of cyber means to gather sensitive information for political or strategic purposes.

Source: ZDNET

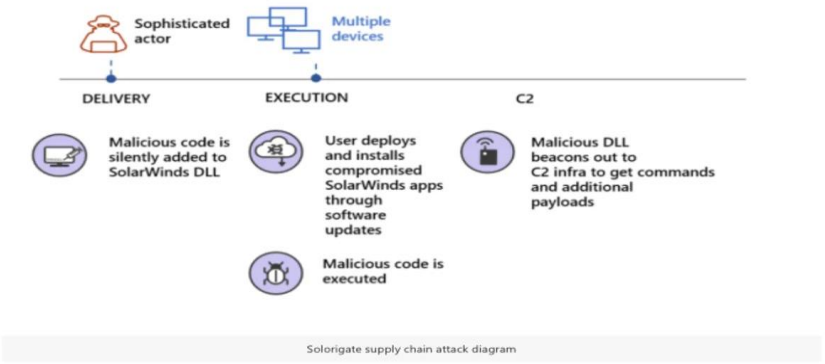
- The SolarWinds hack was a major cyber attack that occurred in December 2020. It was discovered that hackers had compromised the software supply chain of the IT infrastructure management company SolarWinds and inserted malicious code into the company's software updates.
- The updates were then installed by thousands of organizations around the world, allowing the hackers to gain access to the networks of these organizations. The attack was believed to have been carried out by Russian state-sponsored hackers.
- The SolarWinds hack was significant because it allowed the hackers to gain access to many networks, including those of government agencies and Fortune 500 companies.
- The attack was not discovered for several months, and the full extent of the damage is still not fully known. It is believed that the hackers were able to access a wide range of sensitive information, including email, intellectual property, and potentially even classified government data.
- The SolarWinds hack highlights the importance of supply chain security and the need for organizations to ensure that their software and systems are secure against potential threats. It is also a reminder of the importance of regularly updating software and monitoring networks for suspicious activity.

Source: ZDNET

Timeline

SolarWinds Attack

1. **The SolarWinds hack was not publicly discovered until December 2020, but it is believed that the attackers gained access to the company's systems as early as September 2019, meaning they may have had over a year of access to the network.**
2. The attack went undetected for more than a year, and when it was covered, analysis by FireEye showed that the attackers had taken several steps to cover their tracks.
3. The attackers used different credentials and moved laterally within the victim's network, bypassing multifactor authentication protocols and logging into other users' systems through the Server Message Block protocol and copying their Chrome browser data.
4. SUNBURST malware was deployed through an Orion update by the hackers. Orion is a software platform for centralized monitoring and management, often used to keep track of IT resources in large networks.
5. SolarWinds has admitted that Orion updates released between March and June 2020 were compromised with the malware. FireEye has referred to the malware as SUNBURST, and Microsoft has named it Solorigate.
6. SolarWinds plans to release a new update on December 15, 2020, to replace the compromised component and add additional security enhancements.



Solorigate supply chain attack diagram

Image: Microsoft

Source: ZDNET

Vulnerabilities

Overall Summary

The SolarWinds hack was made possible by a vulnerability in the software supply chain of the IT infrastructure management company SolarWinds. The hackers were able to compromise SolarWinds' software updates and insert malicious code into them. The updates were then installed by thousands of organizations around the world, allowing the hackers to gain access to the networks of these organizations.

Vulnerability #1

CVE-2021-25275 – a vulnerability in the interface between Orion and Microsoft Message Queue (MSMQ), which can allow attackers to access secured credentials and gain control over a Windows server running Orion.

Vulnerability #2

CVE-2021-25274 – The Collector Service could allow an unauthenticated user to inject malicious code and gain complete control to the Windows operating system on an Orion server.

Vulnerability #3

CVE-2021-25276 – vulnerability in the Serv-U FTP utility, allowing anyone who logs in either locally or via RDP to create an admin account and gain full access to the server and attached networks.

Vulnerability #4

It is also possible that the hackers used a combination of techniques, such as spear phishing (targeted email attacks) or social engineering (manipulating individuals into divulging sensitive information), to gain initial access to SolarWinds' systems.

Source: Bright & NIST

Costs

- In releasing preliminary first-quarter results, SolarWinds said it spent $18 million to $19 million to investigate and remediate the cyber incident.
- The attack affected thousands of organizations around the world, including government agencies and Fortune 500 companies.
- It is believed that the hackers were able to access a wide range of sensitive information, including email, intellectual property, and potentially even classified government data.
- Around 18,000 Orion customers installed the compromised update, many of whom are in the U.S. federal government.
- The attack has also disrupted operations and caused financial losses for some of the affected organizations, which until now not known.
- SolarWinds' shares rose 2.1% to $18.05 in trading as it also estimated it will lose between $16.62 million and $16.87 million in the first quarter.

Source: CFO

Prevention

- Implement strong password policies and use multifactor authentication: Ensuring that strong, unique passwords are used for all accounts and implementing multifactor authentication can help to prevent unauthorized access to systems.
- Regularly update software and systems: Keeping software and systems up to date with the latest patches and security updates is essential for closing known vulnerabilities.
- Monitor networks for suspicious activity: Regularly monitoring networks for unusual or suspicious activity can help to detect potential threats early on.
- Implement secure network architecture: Configuring network architecture in a way that minimizes the attack surface and reduces the potential for unauthorized access can help to prevent successful attacks.
- Conduct regular security assessments: Regularly evaluating and testing the security of systems and networks can help to identify vulnerabilities and weaknesses that need to be addressed.
- Educate employees: Ensuring that employees are aware of best practices for cybersecurity and are trained to recognize and report potential threats can also be an important prevention measure.
- Evaluate and monitor third-party vendors and suppliers: Carefully evaluating and monitoring the security practices of third-party vendors and suppliers can help to prevent supply chain attacks like the SolarWinds hack.

Source: Bright