Abstract

The SolarWinds supply chain attack, which occurred in late 2020 and early 2021, was a sophisticated and targeted cyber-attack that used SolarWinds' software (i.e., Orion network monitoring software) update process to gain access to the networks of numerous organizations. The attack highlighted the importance of supply chain security and the need for organizations to carefully vet the companies with which they do business and to update their software and security measures on a regular basis.

This research paper examines various security technologies that could have potentially assisted in detecting, preventing, or even mitigating the impact of the SolarWinds attack. These technologies include firewall, intrusion detection system (IDS), intrusion prevention system (IPS), and security information and event management (SIEM). The paper discusses how each of these technologies works and how they could have potentially helped in the SolarWinds attack. The paper also includes a case analysis and case findings section, which discusses the details of the SolarWinds attack and the implications of the attack.

The paper also discusses the importance of implementing a combination of security measures and regularly updating and patching software in order to reduce the risk of a successful cyber-attack. It concludes that while it is not possible to completely eliminate the risk of a cyber-attack, implementing security technologies and following best practices for cybersecurity can help reduce the risk of a successful attack.

Table of Abbreviation

CSI	Crime Scene Investigation
EDR	End-point Detection and Response
HIDS	Host-based Intrusion Detection System
HIPS	Host-based Intrusion Prevention System
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
NGFW	Next Generation Firewall
NIDS	Network-based Intrusion Detection System
NIPS	Network-based Intrusion Prevention System
NMS	Network Management System
SIEM	Security Information and Event Management
SIM	Security Information Management
SOAR	Security Orchestration and Automation Response
XDR	Extended Detection and Response

Table of Contents

Table of Figures

1. Introduction

The internet has evolved significantly since its invention, and with this evolution has come an increased risk of cyber threats. As more people and organizations rely on the internet for communication, commerce, and access to information, the potential for cyber-attacks has grown. These attacks can range from simple phishing scams to sophisticated nation-state sponsored attacks and can have serious consequences, including financial losses, reputational damage, and even physical harm.

To mitigate these risks, organizations and individuals have turned to various security technologies, such as firewalls, intrusion prevention systems, and security information and event management systems, to help protect against cyber threats. In this research paper, we will examine the evolution of the internet and the various cyber threats that have emerged, as well as the security technologies that have been developed to mitigate these threats.

These days, security technologies are crucial for every business for various reasons because it helps the businesses to:

- Protect information and systems from both internal and external threats.
- Ensure stable business operations to achieve goals.
- Maintain brand value and reputation in the market.
- Minimize losses in the event of an incident.

This report introduces various security technologies, including firewall, intrusion detection system (IDS), intrusion prevention system (IPS), and security information and event management (SIEM). It also gives a brief overview of the histories of these technologies and offers in-depth coverage of each. The report also analyses the latest cyber-attack that occurred on SolarWinds in early 2021, identifying the primary flaw and offering suggestions for mitigating the attack using the mentioned security technologies.

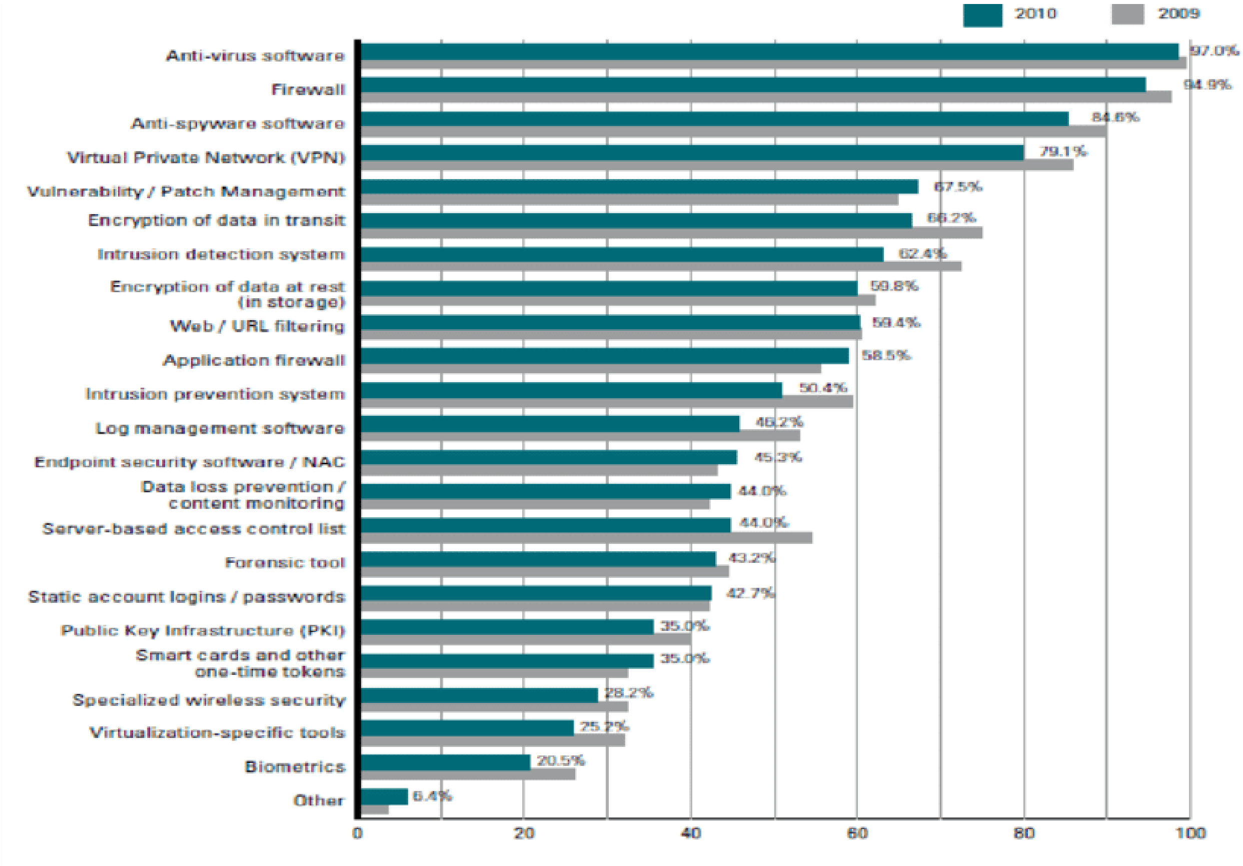


Figure 1 Types of security technologies used by percentage of respondents in CSI survey (Anshu Tripathi, 2012).

2. Aim and Objectives

This report aims to learn about current security technologies used by businesses and examine a recent cyber incident/attack. The objective of this report is to:

- Conduct thorough research on various security technologies.
- Perform in-depth analysis of a recent cyber-attack incident.
- Analyze the incident based on findings.
- Offer constructive feedback and suggestions on the incident and recommend a security technology for implementation.

3. Background

3.1. History

Security technologies such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and security information and event management (SIEM) have evolved significantly over the years as the internet has grown and cyber threats have become more sophisticated.

Firewalls were some of the first security technologies to be developed, with the first firewall software being released in the early 1990s. These early firewalls were designed to block unauthorized access to a network by examining incoming traffic and allowing or denying access based on predetermined security rules. As the internet has evolved, so have firewalls, with newer versions offering more advanced features such as stateful inspection and application-level filtering (Cisco Systems, Inc., 2002).

Intrusion detection systems (IDS) were developed in the late 1980s and early 1990s as a way to detect potential security threats by monitoring network traffic and system logs for unusual activity. Early IDS systems were based on simple rule-based systems, but more advanced systems now use machine learning algorithms to detect anomalies and identify potential threats (Bruneau, 2021).

Intrusion prevention systems (IPS) were developed in the late 1990s as a way to not only detect potential security threats but also prevent them by taking automated action to block or mitigate the threat. Like IDS systems, IPS systems have evolved over the years and now use machine learning algorithms to detect anomalies and identify potential threats (Fuchsberger, 2005).

Security information and event management (SIEM) systems were developed in the early 2000s to provide real-time visibility into the security posture of an organization and help coordinate the response to a security incident. They have evolved over the years and now use machine learning algorithms to detect anomalies and identify potential threats (Wilkie, 2012).

3.2. Security Technologies

3.2.1. Firewall

A firewall is a network security system that monitors, and controls incoming and outgoing network traffic based on predetermined security rules. A firewall can be hardware-based, software-based, or a combination of both. There are several types of firewalls, including packet filtering firewalls, stateful inspection firewalls, and application-level firewalls (Cisco Systems, Inc., 2002).

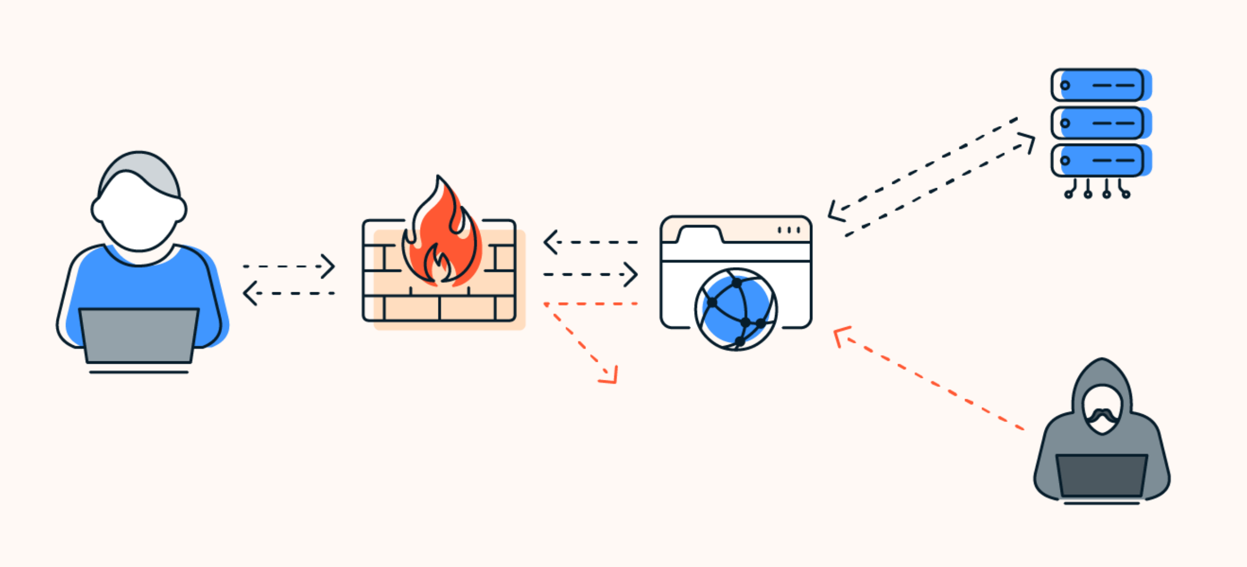


Figure 2 Diagram of a network protected by firewall (Freda, 2022).

Firewalls are used to protect a network from unauthorized access and to prevent attacks from spreading within the network. For example, a firewall can be configured to block incoming traffic from known malicious IP addresses or to allow only certain types of traffic, such as HTTP or HTTPS, to pass through (Bianco, 2020).

3.2.2. Intrusion Detection System (IDS)

An intrusion detection system (IDS) is a type of cybersecurity technology that is designed to detect and alert administrators to potential security threats on a network. IDS systems monitor network traffic for signs of unusual or suspicious activity, such as attempts to access unauthorized resources or the injection of malicious code. When an IDS detects such activity, it generates an alert, which can be used to take appropriate action to prevent or mitigate the threat (Michael E. Whitman, 2016).

There are two main types of IDS: network-based IDS (NIDS) and host-based IDS (HIDS). NIDS monitors traffic on a network and is typically deployed at strategic points on the network, such as at the boundary between the organization's network and the Internet. HIDS monitors activity on a single host, such as a server or a desktop computer, and is typically installed on the host itself (Michael E. Whitman, 2016).

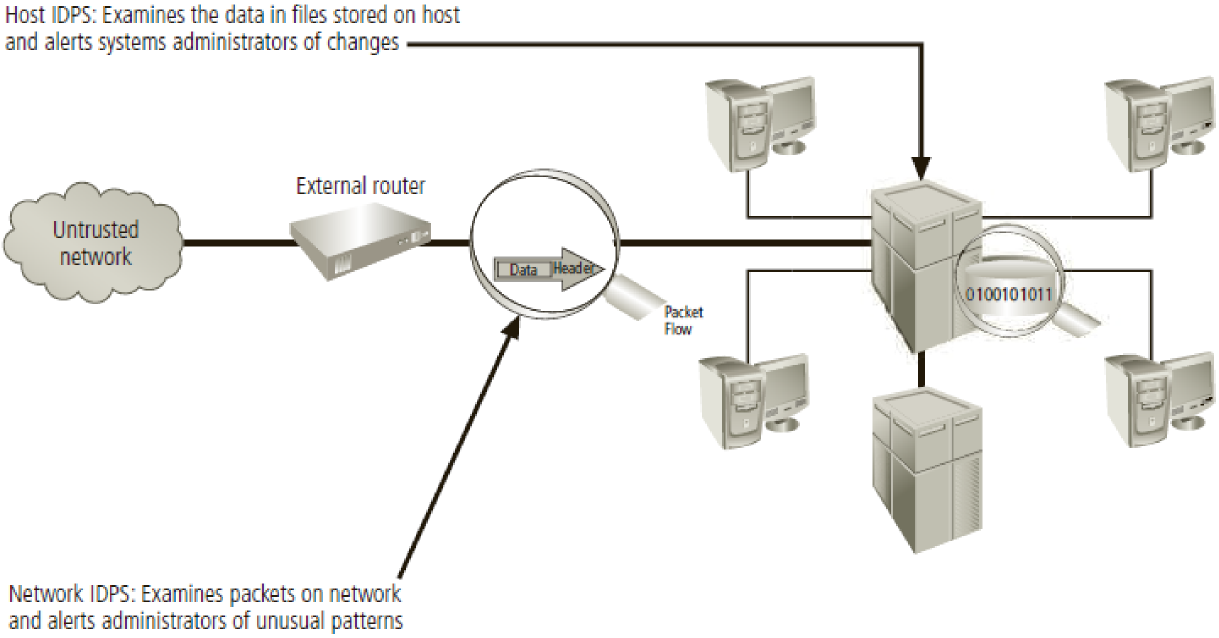

Host IDPS: Examines the data in files stored on host
and alerts systems administrators of changes
External router
Untrusted network
Data
Header
Packet Flow
0100101011
Network IDPS: Examines packets on network
and alerts administrators of unusual patterns

Figure 3 Intrusion Detection and Prevention Systems (Michael E. Whitman, 2016).

Some of the main advantages of IDS systems include the ability to detect and alert administrators to potential security threats in real-time, the ability to identify and alert administrators to unusual or suspicious activity that may indicate a security breach, and the ability to provide historical data that can be used to investigate security incidents. IDS systems are an important part of a multi-layered cybersecurity strategy and can help organizations to identify and respond to potential threats before they can do significant damage (Fuchsberger, 2005).

3.2.3. Intrusion Prevention System (IPS)

An intrusion prevention system (IPS) is a type of cybersecurity technology that is designed to detect and prevent potential security threats on a network. Like an intrusion detection system (IDS), an IPS monitors network traffic for signs of unusual or suspicious activity, such as attempts to access unauthorized resources or the injection of malicious code. However, an IPS goes a step further than an IDS by automatically taking action to prevent the threat from being successful (Michael E. Whitman, 2016).

There are two main types of IPS: network-based IPS (NIPS) and host-based IPS (HIPS). NIPS monitors traffic on a network and is typically deployed at strategic points on the network, such as at the boundary between the organization's network and the Internet. HIPS monitors activity on a single host, such as a server or a desktop computer, and is typically installed on the host itself (Michael E. Whitman, 2016).

Some of the main advantages of IPS systems include the ability to detect and prevent potential security threats in real-time, the ability to identify and prevent unusual or suspicious activity that may indicate a security breach, and the ability to provide historical data that can be used to investigate security incidents. IPS systems are an important part of a multi-layered cybersecurity strategy and can help organizations to identify and respond to potential threats before they can do significant damage (Michael E. Whitman, 2016).

3.2.4. Security Information and Event Management (SIEM)

Security Information and Event Management (SIEM) is a type of cybersecurity technology that combines security information management (SIM) and security event management (SEM). It is designed to provide a centralized view of an organization's cybersecurity posture by collecting, storing, and analysing security-related data from a variety of sources, such as firewalls, intrusion detection and prevention systems (IDS/IPS), and network logs.

SIEM systems are used to monitor network activity for signs of unusual or suspicious behaviour, alerting administrators to potential threats in real-time. They can also be used to detect and respond to security breaches, as well as to provide regulatory compliance reporting.

Figure 4 The Top 10 SIEM Solutions (Jones, 2022).

Some of the main advantages of SIEM systems include the ability to monitor and analyse security data from a variety of sources, the ability to detect and respond to security threats in real-time, and the ability to provide compliance reporting. They are an important part of a multi-layered cybersecurity strategy and can help organizations to identify and respond to potential threats before they can do significant damage.

4. Literature Review

4.1. Case Study

For the case study, I have used the SolarWinds supply chain attack in order to gain a deeper understanding of the tactics and techniques used by the attackers and the ways in which businesses can protect themselves from similar attacks in the future.

4.1.1. Finding

The SolarWinds supply chain attack occurred in late 2020 and was discovered in December of that year. The attack was particularly sophisticated and targeted SolarWinds, which provides IT management software to a wide range of organizations. The attackers inserted malicious code into a legitimate software update for Orion, which was then distributed to SolarWinds' customers. The malware allowed the attackers to gain access to the networks of organizations that installed the update. The attack was discovered in December 2020 and is believed to have affected a large number of organizations, including government agencies and private companies.

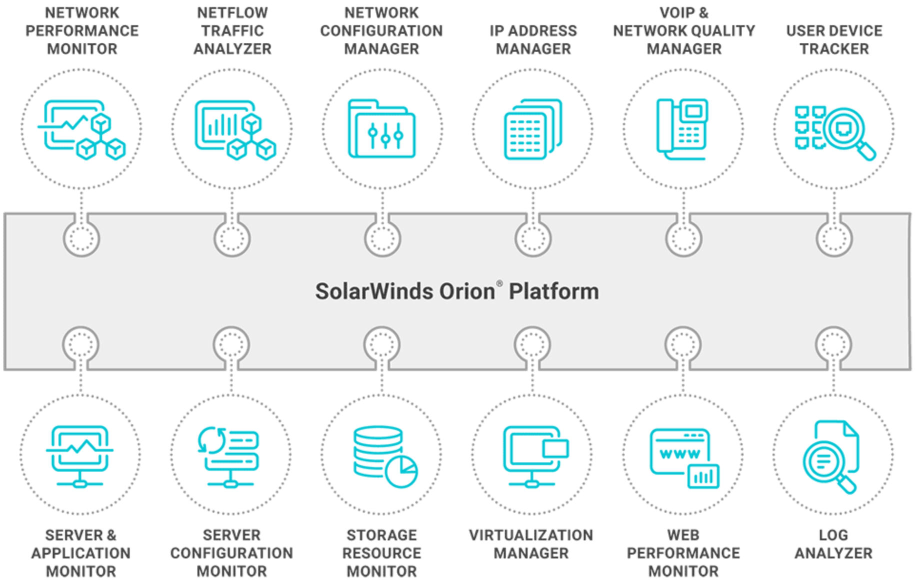

NETWORK PERFORMANCE MONITOR
NETFLOW TRAFFIC ANALYZER
NETWORK CONFIGURATION MANAGER
IP ADDRESS MANAGER
VOIP & NETWORK QUALITY MANAGER
USER DEVICE TRACKER
SolarWinds Orion® Platform
SERVER & APPLICATION MONITOR
SERVER CONFIGURATION MONITOR
STORAGE RESOURCE MONITOR
VIRTUALIZATION MANAGER
WEB PERFORMANCE MONITOR
LOG ANALYZER

Figure 5 SolarWinds' Orion Platform (SolarWinds, 2019).

The impact of the attack was significant, as many organizations that had installed the compromised software updates discovered that they had been compromised months after the initial attack. The attackers were able to gain access to a wide range of sensitive data, including emails and other confidential information. This had serious consequences for the affected organizations, as the attackers were able to steal sensitive data and disrupt their operations.

In addition to the impact on SolarWinds' customers, the attack also had serious consequences for the company itself. SolarWinds' reputation was severely damaged by the incident, as the company was seen as being responsible for the compromise of its customers' networks. This led to a significant decline in the company's stock price and a loss of trust in its products and services.

The problem behind the attack was the lack of security measures in place to protect the software update process. The attackers were able to exploit this vulnerability to insert their malicious code into the updates, which were then distributed to SolarWinds' customers. This highlights the importance of ensuring that all stages of the software development process are secure in order to prevent similar attacks in the future.

4.1.2. Analysis

In my view, the SolarWinds attack was particularly concerning because it demonstrated the ability of attackers to compromise the supply chain of a well-respected and widely used software company. This highlights the importance of carefully vetting the companies that businesses do business within order to ensure that their security practices are robust. It also demonstrates the need for businesses to regularly update and patch their software in order to prevent similar attacks.

To protect against such attacks, the company could have implemented a range of security technologies such as firewalls, intrusion detection and prevention systems (IDS/IPS), and security information and event management (SIEM) systems, and many other technologies which has been explained at the appendix section and in the previous pages as well. These technologies can help to identify and respond to potential threats in real-time, as well as provide historical data for investigating security incidents. In addition to these technologies, businesses can also implement other measures such as network segmentation, secure software development, and regular security testing and assessments to reduce their risk of being impacted by cyber-attacks.

5. Conclusion

In conclusion, the SolarWinds supply-chain attack was a major and complex cyber-attack that had significant consequences for the affected organizations. Through my research, I learned about the importance of supply-chain security and the need to carefully vet the companies that a business works with to ensure that their security practices are strong. I also learned about the value of regularly updating and patching software to prevent similar attacks.

I also learned about the role of security technologies, such as firewalls, intrusion detection and prevention systems (IDS/IPS), and security information and event management (SIEM) systems, in protecting businesses from cyber threats. These technologies can help organizations to identify and respond to potential threats in real-time, as well as provide historical data for investigating security incidents.

In addition, I learned about other practices that can help businesses to reduce their risk of being impacted by cyber-attacks, such as network segmentation, secure software development, and regular security testing and assessments.

Going forward, I plan to share my knowledge and insights with other businesses to help them better understand the threats that they face and the steps that they can take to protect themselves. By raising awareness about these issues, I hope to help other businesses reduce their risk of being impacted by cyber-attacks and create a safer and more secure online environment.

6. References

Anshu Tripathi, U. K. (2012). *Aggregate Analysis of Security Surveys in Quest of Current Information Security Landscape.* International Journal of Computer Applications.

Bianco, D. J. (2020). *Mastering Security Operations Center (SOC) Management.* Birmingham: Packt Publishing.

Bruneau, G. (2021). *The History and Evolution of Intrusion Detection.* SANS Institure. Retrieved from https://sansorg.egnyte.com/dl/TmT2wf11v7

Cisco Systems, Inc. (2002, September 28). *Evolution of the Firewall.* Retrieved from docstore.mik.ua: https://docstore.mik.ua/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ch3.pdf

Freda, A. (2022, November 25). *What Is a Firewall and Why Do You Need One?* Retrieved from Avast: https://www.avast.com/c-what-is-a-firewall

Fuchsberger, A. (2005). *Intrusion Detection Systems and Intrusion.* Royal Holloway: Information Security Group.

Jones, C. (2022, November 24). *The Top 10 SIEM Solutions* | *Expert Insights*. Retrieved from Expert Insights: https://expertinsights.com/insights/the-top-10-siem-solutions/

Michael E. Whitman, H. J. (2016). *Principles of Information Security* (Sixth ed.). Cengage Learning.

SolarWinds. (2019, November 14). *Installing the Orion Platform Agent*. Retrieved from SolarWinds: https://www.solarwinds.com/resources/video/installing-the-orion-platform-agent

SolarWinds. (2022). *Orion Platform* | *SolarWinds*. Retrieved from SolarWinds: https://www.solarwinds.com/orion-platform

Wilkie, T. (2012). *SIEM: A Brief History and Overview.* Datamation.

Williams, J. (2020, December 15). *What You Need to Know About the SolarWinds Supply-Chain Attack*. Retrieved from SANS: https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/

7. Bibliography

Evan D. Wolff, K. M. (2021). *Navigating the SolarWinds Supply Chain Attack.* The Procurement Lawyer.

Isabella Jibilian, K. C. (2021, April 15). *What Is the SolarWinds Hack and Why Is It a Big Deal?* Retrieved from Business Insider: https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12

Jeferson Martínez, J. M. (2021). *Software Supply Chain Attacks, a Threat to Global Cybersecurity: SolarWinds' Case Study.* International Journal of Safety and Security Engineering.

Josh Huddleston, P. J. (2021). *How VMware Exploits Contributed to SolarWinds Supply-chain Attack.* International Conference on Computational Science and Computational Intelligence (CSCI).

Lindsay Sterle, S. B. (2021). *On SolarWinds Orion Platform Security Breach.* : 2021 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Internet of People and Smart City Innovation .

Michael E. Whitman, H. J. (2013). *Management of Information Security.* Cengage Learning.

Newman, L. H. (2021, December 8). *A Year After the SolarWinds Hack, Supply Chain Threats Still Loom*. Retrieved from Wired: https://www.wired.com/story/solarwinds-hack-supply-chain-threats-improvements/

8. Appendix

What is SolarWinds?

SolarWinds is a software company that provides systems management tools for IT professionals, with its most widely used product being Orion, a Network Management System (NMS). NMSs are attractive targets for attackers because they must be able to communicate with all managed devices and often have the ability to make changes on behalf of their configurations. The Orion NMS has a range of capabilities for monitoring and managing systems, including servers, workstations, and network devices. The recent security event involving SolarWinds highlights the need for IT and IT security teams to assess the risks associated with NMSs (Williams, 2020).

Who uses SolarWinds?

The better question would be, who doesn't use SolarWinds? They are one of, if not the, Network Management System. SolarWinds is to NMS as Kleenex™ is to tissues. SolarWinds has over 300,000 customers and many of them heavy hitters, much of the US Federal government including the Department of Defense, 425 of the US Fortune 500, and lots of customers worldwide (Williams, 2020).

What is Orion NMS?

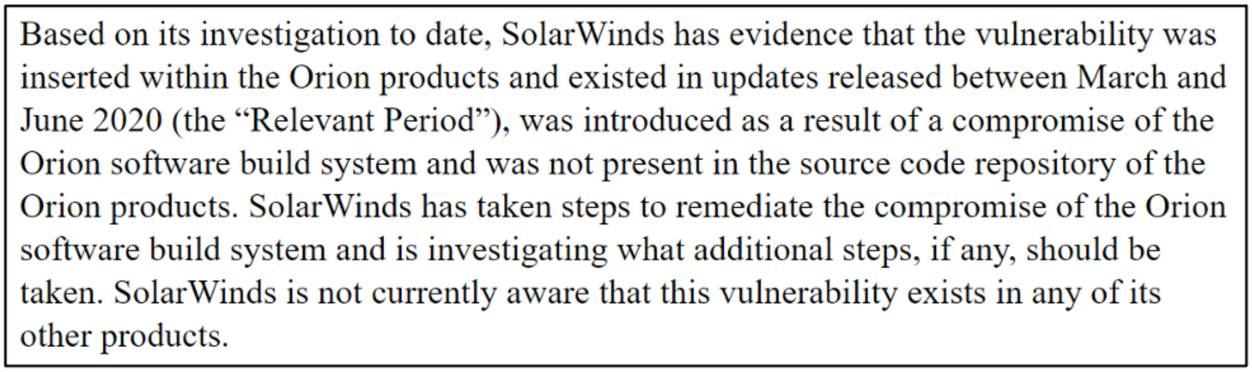
Orion is a Network Management System (NMS) developed by SolarWinds, a software company that provides systems management tools for IT professionals. It has a range of capabilities for monitoring and managing systems, including servers, workstations, and network devices (SolarWinds, 2022).

How was the SolarWinds Malware Deployed?

The malware was delivered through a software update in Orion NMS and was authenticated with a valid digital certificate issued by Symantec. This suggests that the attack was carried out through the supply chain and the certificate had a serial number of 0fe973752022a606adf2a36e345dc0ed (Williams, 2020).

According to CISA's alert, "Incident response investigations had 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.”

SolarWinds’ Response



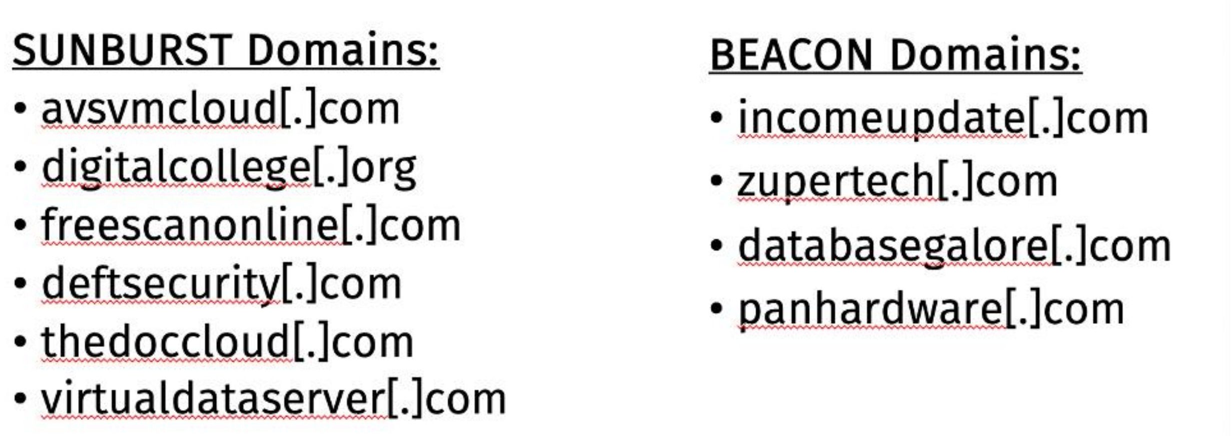
Based on its investigation to date, SolarWinds has evidence that the vulnerability was inserted within the Orion products and existed in updates released between March and June 2020 (the “Relevant Period”), was introduced as a result of a compromise of the Orion software build system and was not present in the source code repository of the Orion products. SolarWinds has taken steps to remediate the compromise of the Orion software build system and is investigating what additional steps, if any, should be taken. SolarWinds is not currently aware that this vulnerability exists in any of its other products.

Figure 6 SolarWinds' Response to the incident (Williams, 2020).

SolarWinds had published limited information in which they state they believe the build environment was compromised. They have identified that these updates were released between March and June 2020, and they believe only 18,000 of its 300,000 Orion customers are impacted by the update. But this all leaves a lot of questions that will hopefully be answered as SolarWinds publishes more data from their internal investigation (Williams, 2020).

Network IOCs

FireEye had released domains useful for hunting (Discovery COA) if you have DNS logs or full PCAP:



SUNBURST Domains:

- avsvmcloud[.]com
- digitalcollege[.]org
- freescanonline[.]com
- deftsecurity[.]com
- thedoccloud[.]com
- virtualdataserver[.]com

BEACON Domains:

- incomeupdate[.]com
- zupertech[.]com
- databasegalore[.]com
- panhardware[.]com

Figure 7 Network IOCs (Williams, 2020).

Recommendations

To protect against supply chain attacks like the SolarWinds attack in 2021, organizations can implement the following measures:

1. Strong authentication and access controls
2. Regular software updates
3. Implementing various security technologies as a barrier
4. Network segmentation
5. Monitoring for unusual activity
6. Regular security assessments
7. Verified sources for software updates
8. Incident response plans

More security technologies that can be used to protect against various cyber risks and incidents

EDR: Endpoint Detection and Response (EDR) is a security solution that monitors and detects malicious activity on a computer or network and provides tools for responding to and mitigating threats.

XDR: Extended Detection and Response (XDR) is a security solution that combines multiple data sources and technologies to detect and respond to threats across an organization's entire infrastructure, including on-premises, cloud, and endpoint environments.

NGFW: A Next-Generation Firewall (NGFW) is a network security system that combines traditional firewall capabilities with advanced features such as intrusion prevention, application control, and network traffic analysis to provide more comprehensive protection against cyber threats.

SOAR: Security orchestration, automation, and response (SOAR) is a security solution that uses automation and integration to streamline and enhance the process of detecting, responding to, and mitigating security threats. SOAR aims to improve the efficiency and effectiveness of security operations by automating repetitive tasks and enabling analysts to focus on more complex and high-impact activities.