On SolarWinds Orion Platform Security Breach

Lindsay Sterle and Suman Bhunia
Department of Computer Science and Software Engineering, Miami University, Oxford, Ohio
sterlel5@miamioh.edu, bhunias@miamioh.edu

***Abstract*—Persistent Threat agents from across the world are ever evolving their technological techniques to gain access to these systems and the information within. The potential for harm that can be exploited through cybersecurity attacks has no bounds. We must analyze and learn from our experiences to further our exploration in solutions preventing, detecting and remediating these attacks. This article is designed to analyze the security incident regarding SolarWinds' Orion Platform, the details of its occurrence, the influence on the individuals involved, the industry as a whole, the financial sector, and elements of SolarWinds' incident response as well as potential contingency plans. This paper serves as a tool in the exploration of cybersecurity solutions by providing a case study on an unprecedented security incident.**

***Index Terms*—Sunburst, Security. Hotfixes, Supply Chain Attack, Build Process, Software Driver, Orion Platform.**

I. Introduction

The SolarWinds Orion (SUNBURST) cybersecurity breach may be the paramount of all information security incidents the United States has ever encountered. The scope and sophistication of the attack are unprecedented, infiltrating an abundance of corporate and administrative bodies, while remaining undetected for so many months [1]. December 2020 marks the initial breach disclosure, occurring five days after FireEye, a cybersecurity incident response company, announced an intrusion in their network, resulting in the theft of proprietary software tools [2]. This concerning event led to the discovery that hackers were trojanizing SolarWinds' Orion Platform software updates to distribute malware [3]. SolarWinds' Orion Platform is a tool used by IT professionals and government organizations such as Microsoft, Intel, Nvidia, and government departments of Homeland Security, State, Commerce and Treasury [4]. The March 2020 update released to the Orion Platform resulted in malicious code pushed to approximately 18,000 customer networks, potentially victimizing these clients to cybercrime [2]. Speculation regarding those responsible for the attack points to a country sponsored espionage activity [4]. Although responsibility was denied by the government, this "state sponsored" attack is seen as an incursion against the state government.

Threat actors gained access to the SolarWinds Orion Platform by first performing reconnaissance and gaining information on SolarWinds and their clients, eventually stealing authorized credentials. Posing as an authorized entity using the stolen credentials, threat agents gained access to the SolarWinds network. Once inside the network, agents elevated their access privileges and found their way into the software development and delivery pipeline for the Orion Platform and inserted malicious code that would be executed during the build process of the most recent update. Installation of the update on client networks led to compromised devices, allowing threat agents to communicate through these client devices using their command-and-control servers. Threat agents used their servers to access client networks, steal information, push additional malware and execute remote commands on client networks.

An attack that has infiltrated so many administrative bodies is sure to have effects on the nation's individuals. The information stolen can be used in further criminal activity such as identity theft, credit card fraud, etc. harming the reputation of individuals. Access to the programs controlling physical machinery can lead to physical harm to individuals as well. It is important to analyze the impact of a breach on the company it stems from as well. The overall finances and reputation of a company face serious consequences in light of a breach, which can potentially threaten its entire existence. About 45% of SolarWinds' total revenue, $343 million, stems from the Orion Platform [2]. This major incident regarding the company's greatest revenue earner, is surely going to hurt SolarWinds' financial standings moving forward. Clients no longer have the same level of trust in SolarWinds' software, especially the Orion Platform. This major hit to SolarWinds' reputation will surely factor into any future business endeavors of current and potential clients moving forward. How SolarWinds responds to the breach moving forward will ultimately determine their existence as an organization.

The wide-range of institutions affected by the breach has changed the course of the cybersecurity industry. A 'reaction' approach is no longer an acceptable method of defense regarding cybersecurity, a new methodology of 'prevention' has become the main focus [5]. A reorganization of cybersecurity in businesses and the United States government is required to align with this new method of defense [6]. Responses to the incident were made in collaboration with SolarWinds and the United States government. To remedy the situation, SolarWinds issued public disclosure reports with federal authorities, sharing discoveries of the breach. The company removed the malicious code from the update and prevented the malware from operating further. An action plan was published by SolarWinds to advise additional client responsibilities to secure their respective systems. The company began working to improve the Orion Platform and deployed hotfixes that could be installed to remove vulnerabilities exploited by the breach. Solutions regarding future outcomes of the breach are discussed including a prevent rather than react ideology for cybersecurity, as well as potential government actions that should be considered as we move forward.

To the best of our knowledge, this is the first paper that provides an overview of the details of the security breach, its impact and its countermeasures. The extensive explanation of the breach compiles into an important tool to be used in the battle that is cybersecurity. Raising awareness on the importance and effects of security breaches must be shared in order to create a nation focused on breach prevention. Technical details must be analyzed and understood to create effective controls used to prevent future cybersecurity attacks, for more than 90% of all attacks are based on previously used techniques [7] [8] [**?**]. To compile the information presented within this paper, we reviewed news sources, SolarWinds documentation and other online resources as well as speculated on the information gathered.

The document is structured as follows; we begin with Section II, which provides technical details regarding the security incident, including an introduction to the Orion Platform, and a walkthrough of the methods used and access gained by responsible parties. Next, in Section III we analyze potential impacts, SolarWinds' financial standings, and the cybersecurity industry in its entirety. We continue with Section IV which notes and explores the remediation actions taken by SolarWinds and government authorities in response to the incident, updates released by SolarWinds to secure the Orion Platform, and future solutions as affected parties weather through the breach's implications. Lastly, we move onto Section V which provides a holistic view on the importance of the breach and what its outcomes provide for future cybersecurity solutions.

II. SOLARWINDS BREACH

This section discusses the technical details of the SolarWinds Orion Platform security breach. We begin with an introduction to the solutions offered by SolarWinds, specifically the Orion Platform and why it was targeted. Next, we introduce the probable threat agents, and the Supply Chain Attack and Backdoor methodologies used to infiltrate the Orion Platform. Once the attack methodologies have been explained, we will explore what information our threat agents had access to, discussing specific examples disclosed from the breach. Lastly, we will learn what devices were compromised throughout the breach.

A. SolarWinds Software

SolarWinds offers software solutions for the main challenges in IT Management, more specifically, network management, systems management, IT security, database management, IT service management, application management and managed service providers. Although SolarWinds offers a variety of products and services, the Orion Platform sits firm as the company's greatest revenue earner. The platform contains management and monitoring products geared towards networks, IT operations and security. Orion delivers central visibility and control throughout the most complex of IT environments [9], which typically would be ideal, but not in the case of a cybersecurity attack. By its very nature, the platform has visibility and control over an entire network, which is why it was a target for threat agents.

What made the Orion platform a perfect target was not only visibility and control over networks, but which specific networks threat actors would have visibility and control over. The platform is used by major corporate entities such as Microsoft, Intel, Cisco, etc. as well as major governmental agencies such as the *Infrastructure Security Agency*, *Department of Homeland Security*, *Department of the Treasury, Department of Justice, Pentagon*, etc. [7]. Organizations such as these have control over and contain the most sensitive information in the nation. The most concerning aspect is that the access threat agents had to view and steal this information can just as easily be used to alter or destroy it, leading to serious implications for these corporate and governmental institutions.

B. Threat Agents

There is not sufficient evidence to prove exactly who the threat agents, or threat actors, responsible for the security breach are. However, the evidence that has been obtained indicate patterns consistent with a foreign government's espionage behaviors and hacking techniques [6]. The accused government has denied any involvement and all responsibility involving the incident, however with suspicions growing, the state administration intends to respond to the attack, threatening actions against the accused foreign country [6].

C. Supply Chain Attack and Backdoor Methodology

Threat agents began their reconnaissance mission by implementing a very simple version of a Supply Chain Attack, a process accomplished by targeting a third-party client with access to SolarWinds' resources, rather than trying to hack SolarWinds' network directly [4]. Posing as authorized users allowed the hackers to blend into network activity without detection, even by security and antivirus software [4], rendering the company clueless of the intrusion. This small-scale attack began with a small code fragment, used as a proof of concept to see if it was possible to manipulate SolarWinds' signed-and-sealed software code and get it published into a working update, and threat agents realized they could [7]. Now threat agents knew they had the ability to take the attack further and implement a large-scale Supply Chain Attack without being detected by the intrusion detection systems. The main challenge with the larger scale attack is that the threat agents knew software companies typically audit their source code before they can begin compiling an update. If any of the source code has been tampered with, it will be found. In order to bypass this security control, threat agents waited until the last second to insert their malicious code into the build process which was when SolarWinds' update began compiling [7]. To remain inconspicuous during the build process, threat agents reverse-engineered the protocols used to communicate between the Orion Platform and company servers [7]. Hackers built their own program to mimic the specific syntax and format used in traffic packets.

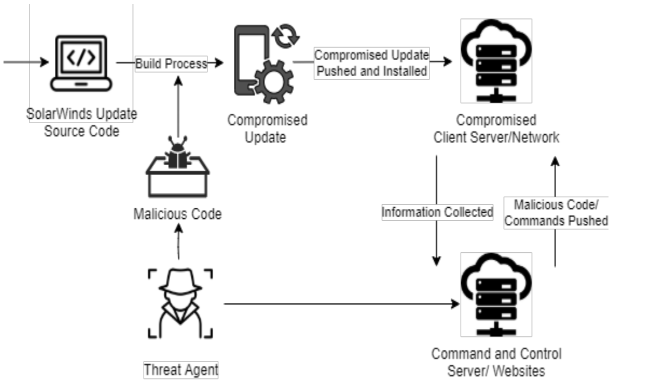

Fig. 1: Fig. Supply Chain Attack. (Illustration of how threat agents compromised the SolarWinds Orion Platform update and client networks.)

Once threat agents had successfully inserted their malware into the software update, it was published and installed to client servers. Once the update was present and active on client servers, the threat actors' external domains, one of which was *avsvmcloud[...]com*, sprang into action [4]. The command-and-control server was used by the hackers to communicate with systems that had installed the Orion product updates which gave them backdoor access to these systems [4]. The external domain provided threat agents the means to enter and alter these networks on multiple occasions, collecting user information as well as pushing additional malicious payloads. The use of the external domain, as well as an analysis of the malicious code itself implies that the code requires manual intervention, which means threat agents had specific client targets in mind [12].

Fig. 1. illustrates the implemented Supply Chain Attack. With access to the software development and delivery pipeline, threat agents were able to insert malicious code during the build process of the update. The compromised update was then delivered to client networks, containing a backdoor to the threat agents' command-and-control servers. Through the control servers, the hackers collected information from client networks and had the ability to push additional malware into these networks.

D. Threat Agent Access

With an established measure to enter the SolarWinds' network as an authorized identity, the threat agents had access to all the resources as the identity they falsely claimed to be. Actions went undetected, as the threat actors were viewed as a legitimate source in the SolarWinds network. Once inside the network, hackers were able to exploit privilege vulnerabilities and escalate their access to write permissions in the SolarWinds' software development and delivery pipeline, where the legitimate update code was developed, tested and stored [10]. Access to the pipeline allowed threat agents to insert their malicious code into a platform driver named SolarWinds.Orion.BusinessLayer.dll [10]. The specific driver chosen had been digitally signed by SolarWinds, thus deeming the code within to be legitimate and from a trusted source [10]. The driver resides in the OrionImprovementBusinessLayer class which is executed in parallel with the driver itself by creating a thread to avoid interrupting the regular flow of the driver. Exploiting this specific driver was genius for its execution was inconspicuous.

The installation of this software driver included the installation of the threat agents' malicious code which created a backdoor into client systems which was used to push even more malware to spy on and disrupt organizational operations [6]. The addition of the malware to customer IT systems allowed the threat actors to gain personal and professional information on SolarWinds' clients. One instance in particular proved threat agents had gained access into dozens of email accounts and networks in the Departmental Offices of the United States Treasury [3], leading to a breach of confidentiality in the United States government.

The threat actors' strategy sought to balance the value of compromising each client with the relative likelihood of detection [4]. By maintaining this balance, the threat actors' presence remained unknown within client networks, including those of "Department of State, Department of Homeland Security, National Institutes of Health, Department of Energy, Department of the Treasury, Pentagon, Department of Commerce, Centers for Disease Control and Prevention, and even some state and local governments" [15]. The most alarming access point was into the Department of Homeland Security, whose job is to defend federal computer networks from cyberattacks [14].

E. Compromised Devices

As the investigation into the breach progressed, SolarWinds informed its customers that they were the victims of a cyberattack that inserted malicious code known as SUNBURST within Orion Platform software update builds. Specifically affected were versions 2019.4 Hotfix 5, 2020.2 unpatched, and 2020.2 Hotfix 1 [11]. The statements warned customers that if the update was present and active on their systems, the server in which they were installed had been compromised [11]. The compromised server, which communicates with all other devices in the network, could be used to compromise the entire network, thus giving the threat actors access to all devices in each client network.

III. Global Impact

This section discusses the various parties affected by the security incident. We begin with an analysis on the impact of individuals, regardless of their association to SolarWinds, and the technical or physical harm that could be caused. Next, we will discuss the financial implications of the incident on SolarWinds and what the outcomes mean for the existence of the company. Lastly, we will explore and theorize on what this breach contributes to the future of the cybersecurity industry.

A. Individuals

Since the breach was fairly recent, the exact impact on the safety of individuals is unknown, however the potential may be detrimental. With footholds in organizations, such as medical or governmental institutions, threat actors reach nearly all those residing in the United States. With access to these institutions, hackers can view, steal, falsify or destroy data, leading to serious consequences.

In viewing or stealing information, threat agents breach confidentiality but what threat agents do with the information can lead to far worse. Viewing personal or sensitive information may seem passive, but what if military secrets were told to Foreign Intelligence? We can only imagine the possibilities. When information is stolen, it now 'belongs' to the threat actors who can do whatever they choose with it. Threat agents could hold data for ransom, publish it to the web, destroy it, etc. Personal information of individuals including names, social security numbers, credit card numbers, etc. can be used in identity theft, credit fraud, etc. With access to important medical and governmental information, threat agents could cause catastrophic events.

The seriousness of the hacker's ability to falsify or destroy data can be showcased in a "cyber intrusion that removed an indication of an allergy to a certain medication" [12], ultimately threatening the livelihood of the individual. With access to the networks of medical institutions and an exploitation of privileges, hackers can cause serious harm to the livelihoods of many individuals.

Most alarming is the fact that nearly all physical machinery and their controls are tied to a network, controlled by a network device. The range and full extent of cyber-capabilities is unknown and consequently so are their vulnerabilities [12]. With access to medical networks, hackers have the ability to access all medical devices connected to the network, including those used in surgeries, or even those implanted within patients. Additionally, with access to governmental networks, threat actors have the potential to tamper with controls regarding military machinery, such as nuclear weaponry, which could be potentially devastating to entire populations of people. These worst-case scenarios may seem unlikely, but with unauthorized access to systems and a desire to cause harm, it is an all too real possibility. It is too soon to say exactly how far of a reach the threat agents currently have, or how it will impact each individual. What we can say is the potential for harm is alarming and possibly disastrous.

B. Financial

There are always financial matters following a security incident, and they are apparent in the SolarWinds breach as individuals began to lose confidence and trust in the company. On December 14th SolarWinds filed an SEC Form 8-K report, informing the discovery of the cyberattack to the public [3]. Following the report on December 14th, SolarWinds' stock (SWI) fell approximately 19 percent in pre-market trading [13]. The demand for SolarWinds' stock continued to fall as news of the breach surfaced. Individual's skepticism rose, perceived risk of the stock rose, and stock prices fell. Within just a few days the value of SolarWinds' stock had fallen 25 percent [2]. The total revenue from Orion products was approximately $343 million, or roughly 45 percent of the firm's total revenue [2], an even further loss potential. As of now, the company has not reported significant financial losses due to the breach, however, the fact that the biggest revenue earner has been compromised, and a downward trend in stock price could push SolarWinds into the throes of a financial crisis.

To add to the series of misfortunes, additional financial losses were on the horizon as investors in SolarWinds began filing lawsuits against the company. The lawsuits question the financial reports that SolarWinds filed while threat actors had access to the network. The lawsuits accuse company executives of failed cybersecurity practices and misleading statements [14]. More lawsuits are sure to follow as more information on the breach is disclosed and more clients are affected. Unfortunately, the breach at SolarWinds may become an existential event for the company, depending on how SolarWinds is able to weather the lawsuits and legal responsibilities that ensue [2].

C. The Cybersecurity Industry

The significant impacts of the breach affect the entire industry of Cybersecurity. Awareness and importance of securing networks has dramatically increased in light of the breach. The demand for security services is on the rise, in hopes to reduce the impact of the breach on client networks. Instead of following a 'reaction' approach, organizations are adopting a new method that assumes there are already breaches within their networks, rather than merely reacting to breaches after their discovery [6]. Government institutions are realizing that defense is no longer enough. Institutions are working to disrupt and deter adversaries from undertaking cyberattacks in the first place [5]. Discussions have geared towards a reorganization of United States cybersecurity efforts, including a recommendation to make the Cyber Command independent from the National Security Agency [6]. The increase of awareness in risks and desire to better security efforts as well as the importance in securing a network trends towards an increased demand for security methods. Methods in demand include those that prevent breaches before they even occur, detect attacks as soon as possible and remediate threats immediately, ultimately exploding the demand and potential profits within the Cybersecurity industry.

IV. DEFENCE MEASURES

This section explores current and potential solutions to the Orion Platform breach. First, we will note the remediation actions taken and suggested by SolarWinds. We continue by listing the patch updates created by SolarWinds to remove vulnerabilities discovered in the Orion Platform and conclude this section by theorizing future solutions for those affected by the breach and for cybersecurity as a whole.

A. Remediation Actions

In response to the initial discovery by FireEye, the U.S. Cybersecurity, and Cybersecurity and Infrastructure Security

Agency (CISA) issued an emergency directive [15] regarding the SolarWinds' breach. SolarWinds assured clients that they had removed the software builds that contained and were affected by SUNBURST from their download sites with a kill switch [11]. The kill switch contained code to disconnect the specific command and control servers used by threat agents from the SolarWinds network. The implementation of the kill switch essentially "kills" the connection needed to operate the malware, which prevents further damages, but does not remediate damage already done.

To advise remediations of damage, SolarWinds published an action plan pertaining to the security incident explaining how they will and how clients should deal with implications of the breach. The company posted a list of affected clients and urged them to determine what systems and networks have been impacted. For affected clients, this meant a deep dive into their overarching network, virtual private networks, company routers, staff home routers, device management tools, etc. [15]. An investigation into and the determination of compromised devices within each client network also included the vendors, customers and third parties' networks that communicate with the client network. The effects of the breach were so far reaching that SolarWinds advised client organizations to initiate their own cybersecurity response plans, testing and monitoring, to reduce the effects of the attack. As an additional resource, SolarWinds advised client to contact Compliance Alliance with additional questions on threat remediation.

The far-reaching effects of the breach lead to actions beyond SolarWinds itself. The White House National Security Council (NSC) established the Unified Coordination Group (UCG) to implement a coordinated federal agency response, which provided federal support for the incident [15]. Additionally, the administration began discussions on potential actions against foreign government, including economic and diplomatic sanctions [12].

B. Patches

In addition to their initial remediation actions, SolarWinds has released a series of hotfixes designed to eliminate security vulnerabilities in the Orion Platform, versions 2019.4 through 2020.2.1, that had been exploited in the security breach. Table I lists these patches.

C. Continual/Future Solutions

The still-unfolding breach coupled with the continual discoveries involving the breach indicate the need for continuous remediation efforts [2]. The best defense against cybersecurity attacks in the United States is to learn from past attacks and adapt strategies accordingly. As more breaches occur, we learn how to defend against them, thus ever evolving our methods of defense. It may be in the best interest of the United States government and corporate organizations alike to consider a federal disclosure law that requires all organizations to report the existence and full extent of any breach [16]. Implementing this law would help us to learn more on the techniques used in cyberattacks and further our exploration into possible solutions in prevention methods.

TABLE I: SolarWind Orin Hotfixes (Series of hotfixes designed for Orion Platform versions 2019.4 through 2020.2.1

Date	Name	Description
Feb. 2021	2019.2 Hotfix 4	Installation files are signed with a new digital code-signing certificate. Prevents Improper Access Control Privilege Escalation and MSMQ Remote Code Execution.
Feb. 2021	2019.4 Hotfix 2	Protects against XSS vulnerabilities and privilege escalations. Improvements made to the SQL Always on Listener, session timeout on new installs, License issues that caused syslogs, Named Pipeline Privilege Escalation Vulnerability, etc.
Jan. 2021	2020.2 Hotfix 4	Orion Platform products are signed with a new digital code-signing certificate. Prevents Improper Access Control Privilege Escalation, MSMQ Remote Code Execution and Unprivileged Users gaining DBO owner Access.
Dec. 2020	2019.2 Security Patch	Improvements made to securing corruption caused by the licensing plugin on the main polling engine, XSS vulnerabilities, the Cortex REST API vulnerability, etc.
Dec. 2020	2018.4 Security Patch	Upgrades to Authenticate users with the SAML protocol, performance analysis and Orion Deployment Health.
Dec. 2020	2018.2 Security Patch	Updates to XSS vulnerabilities, configuration wizard, credentials cache, credentials manager, etc. Discontinued use of SHA1 certificates.

It is important for clients to continually monitor their network for suspicious activity, even years after an initial breach. Employing software-as-a-tool to detect, prevent and remediate breaches, should be considered [4]. Other security services should also be considered to grow defenses against breaches from occurring in the first place.

In the specific case of the SolarWinds' breach, the only way to ensure the threat no longer exists is to rebuild networks. However, rebuilding a system from scratch leads to the loss of significant amounts of work plus the risks of restoring compromised data from backups [12]. The amount of time spent to actually recreate these networks would take away from normal business operations and lead to an overall loss of productivity in client networks. It is up to the client organizations to determine whether their risk appetite is great enough for possible effects of the breach or if they can afford a loss of productivity to rebuild their networks.

More drastic measures may even be taken as the state administration considered imposing diplomatic and economic sanctions on the accused Government [5] to protect national security interests. As those responsible are seemingly a state sponsored group, who aimed at large groups of corporations, medical and governmental institutions, the attack is viewed as an attack on the United States itself, rather than these institutions independently. Due to the breach's unprecedented nature and those responsible for it, the United States administrative bodies see it as a responsibility to the nation to take action in the remediation of the breach. As we will not know the full extent of the breach for years to come, it is vital to explore future remediation and recovery efforts.

V. Conclusion

Understanding the details of the breach, its global impact, and remediation efforts are vital in preventing, detecting and resolving future breaches. The details of the breach discussed including those responsible, the attack methods used, what the intruders had access to and what client devices were compromised, should serve as investigative evidence used to create future defenses. The effects of the breach on individuals, the financial sector of SolarWinds and the cybersecurity industry as a whole should be viewed as cautionary tales to be heeded throughout the creation and implementation of defenses.

The SolarWinds security breach serves as evidence in cybersecurity solutions exploration, and its details should be analyzed, discussed, theorized, tested and incorporated into future defense mechanisms. The breach, although unfortunate, may be the best tool we have to defend ourselves against future attacks, for upwards of 90 to 95 percent of all security breaches are based upon known techniques [7]. The Orion Platform intrusion has shown us how threat actors are manipulating aspects of multiple known techniques to produce stealthy and effective new ways to infiltrate systems. SolarWinds may have had internal controls to prevent the attack methods individually, but did they have the means to prevent a combination? That is why this breach is vital, it serves as a warning that it's time to up our security efforts.

The remarkable sophistication and stealth of the attack, coupled with the far-reaching effects only proves the battle of cybersecurity has no end in sight. This breach sparked action and discussion within the states government and corporate institutions and encouraged new philosophies and strategies. With a new ideology, a focus on defending against cybersecurity attacks, we have begun a new era within the Information Age. An era defined in the protection of technology.

References

[1] M. Witter, "Unpacking an unprecedented cyberattack: What is the solarwinds breach and how did it happen." https://jost.syr.edu/unpacking-an-unprecedented-cyberattack-what-is-the-solarwinds-breach-and-how-did-it-happen/#_ftnref12.

[2] B. Krebs, "Solarwinds hack could affect 18k customers -krebs on security." https://krebsonsecurity.com/2020/12/solarwinds-hack-could-affect-18k-customers.

[3] P. Baker, "The solarwinds hack timeline: Who knew what, and when?." https://www.csoonline.com/article/3613571/the-solarwinds-hack-timeline-who-knew-what-and-when.html.

[4] S. Oladimeji, "Solarwinds hack explained: Everything you need to know." https://whatis.techtarget.com/feature/SolarWinds-hack-explained-Everything-you-need-to-know.

[5] J. Murdock, "Who has been affected by the huge solarwinds cyberattack so far." https://www.newsweek.com/solarwinds-orion-software-cyberattack-hack-victims-targets-list-1555840.

[6] I. Jibilian and K. Canales, "Here's a simple explanation of how the massive solarwinds hack happened and why it's such a big deal." https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12.

[7] D. Temple-Raston, "A 'worst nightmare' cyberattack: The untold story of the solarwinds hack." https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.

[8] S. Sriram, R. Vinayakumar, M. Alazab, and K. Soman, "Network flow based iot botnet attack detection using deep learning," in *IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 189–194, IEEE, 2020.

[9] Solarwinds and Com, "Orion platform -scalable it monitoring solarwinds." https://www.solarwinds.com/solutions/orion.

[10] P. Mishra, "Technical deep dive into solarwinds breach | qualys security blog." https://blog.qualys.com/vulnerabilities-research/2021/01/04/technical-deep-dive-into-solarwinds-breach.

[11] SolarWinds, "Solarwinds security advisory." https://www.solarwinds.com/sa-overview/securityadvisory#anchor1.

[12] H. Lin, "Reflections on the solarwinds breach." https://www.lawfareblog.com/reflections-solarwinds-breach.

[13] J. Panettieri, "Hackers weaponize solarwinds orion for worldwide cyberattacks; solarwinds, fireeye release counter measures - mssp alert." https://www.msspalert.com/cybersecurity-news/solarwinds-orion-vulnerability-investigation.

[14] D. Todd, "Solarwinds sued by investors following data breach." https://www.secureworldexpo.com/industry-news/solarwinds-sued-following-data-breach.

[15] Solarwinds, "Solarwinds data breach action plan." https://www.pabankers.com/UploadedFiles/pdfFiles/SolarWinds_Data_Breach_Action_Plan_122320.pdf.

[16] J. Cianci, "The solarwinds software hack: A threat to global cybersecurity." https://jolt.law.harvard.edu/digest/the-solarwinds-software-hack-a-threat-to-global-cybersecurity.