International Journal of Safety and Security Engineering
Vol. 11, No. 5, October, 2021, pp. 537-545
Journal homepage: http://iieta.org/journals/ijsse

Software Supply Chain Attacks, a Threat to Global Cybersecurity: SolarWinds' Case Study

Jeferson Martínez*, Javier M. Durán

Department of Information System, Faculty of Engineering, Metropolitan Technological Institute (ITM), Cl. 54a ##30-01, Medellín, Antioquia 050012, Colombia

Corresponding Author Email: jefersonmartinez@itm.edu.co

https://doi.org/10.18280/ijsse.110505

Received: 1 September 2021
Accepted: 12 October 2021

Keywords:
software supply chain attack, solarwinds, cyber attack, C-SCRM, NIST SP 800-161, Zero trust, SBOM, malware, multi-factor authentication mechanisms (MFA)

ABSTRACT

Exploitation of a vulnerability that compromised the source code of the Solar Winds' Orion system, a software that is used widely by different government and industry actors in the world for the administration and monitoring of networks; brought to the fore a type of stealth attack that has been gaining momentum: supply chain attacks. The main problem in the violation of the software supply chain is that, from 85% to 97% of the code currently used in the software development industry comes from the reuse of open source code frameworks, repositories of third-party software and APIs, creating potential vulnerabilities in the development cycle of a software product. This research analyzes the SolarWinds case study from an exploratory review of academic literature, government information, but also from the articles and reports that are published by different cybersecurity consulting firms and software providers. Then, a set of good practices is proposed such as: Zero trust, Multi-Factor authentication mechanisms (MFA), strategies such as SBOM and the recommendations of the CISA guide to defend against this type of attack. Finally, the research discusses about how to improve response times and prevention against this type of attacks, also future research related to the subject is suggested, such as the application of Machine Learning and Blockchain technologies. Additionally for risk reduction, in addition to the management and articulation of IT teams that participate in all the actors that are part of the software life cycle under a DevSecOps approach.

1. INTRODUCTION

A software supply chain attack occurs when hackers manipulate the code in third-party software components to compromise the 'downstream' applications that use them [1]; This means that the attackers manage to compromise the integrity of the source code of a software widely used in the industry, to insert back doors or malicious code "malware" that allow them to reach the corporations and users that acquire those technologies through the mentioned supplier. Hence, these attacks are called supply chain: they do not go directly against the last compromised organization but they are reached through software vendors as attack vectors.

Attacks on the software supply chain have become increasingly recurrent in recent years, and that's why they are seen as the rebirth of large-scale attacks. That's why this article looks at the SolarWinds case, a supply chain attack that wreaked havoc on a multitude of industries and governments and led to massive data leaks.

The statistics are alarming. Attacks on the software supply chain increased 78% in 2018, according to Symantec's "Internet Security Threat Report 2019" [2]. For its part, ECC IT Solutions, Inc [3] defined a "software supply chain" attack as a breach carried out by hackers who compromised third-party software. Where a malicious actor manages to gain access to the system of an organization through malware installed in software from a trusted third-party vendor or partner. This malware is distributed to all associated entities (clients, partners, suppliers, etc. - to the affected organization). The procedure begins when malicious actors infiltrate a legitimate application, then change the source code and hide the malware in the compilation and update processes with the intention of automatically distributing that malware to a wider audience [4].

This article takes exploitation of SolarWinds company as a case study and reference as the software supply chain attack, where the attackers spoofed the identity and authentication mechanisms of access accounts and managed to insert functions in the source code of a particular dynamic library file (.dll) in the network monitoring and management platform software known as Orion. Subsequently, SolarWinds signed and distributed the .dll as part of its update processes, infecting more than 18,000 customers and 40 public entities from different sectors with malware, including government entities, technology companies, insurance companies, financial companies, retail companies and different organizations located on all continents as shown in Figure 1.

1.1 Research problem statement

According to the research [5], from 85% to 97% of the code in applications or tools from software providers is not originally written by them but comes from the reuse of open source code frameworks, software repositories and APIs. third parties. The foregoing makes it complex to examine the libraries, the code and everything related to the application compilation processes, resulting in software solutions for which there is neither full knowledge nor the control of the code and this opens up to introduce malicious code known as malware.

The purpose of this article is to help answer the question: How could organizations react in a timely, proactive manner and implement actions that help improve response times, and defend against attacks on software supply chain?

This article is organized as follows: First, it is carried out the literature review about the most common types of threats on the software supply chain, then some cases of hacking to the software supply chain are presented, afterwards the methodology is presented from the SolarWinds' case study, the results and discussion are commented and finally, the conclusions and possible future research work are explained.

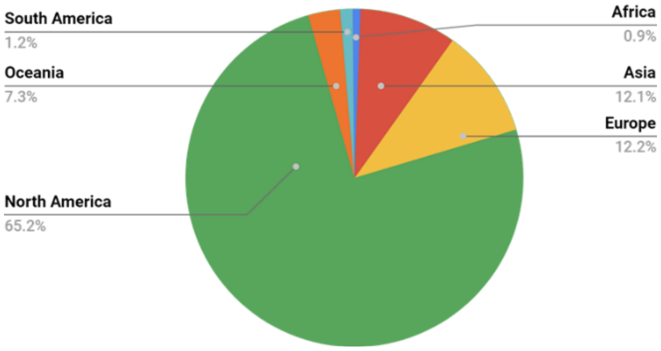


Figure 1. The impact of the attack is worldwide. Source [6]

2. LITERATURE REVIEW

This study presents a "concept-focused" approach [7] to conduct a systematic literature review (SRS) by adapting key elements from Tranfield et al. [8], Rousseau et al. [9] and Denyer and Tranfield [10]. The stages of the process are shown in Figure 2.

Articles published in 4 electronic databases were selected: Scopus, Sciencedirect, IEEE and Taylor & Francis between 2018 and 2021. Afterwards, mind maps were built, and combinations of important search strings that included keywords such as "Solarwinds", "Software Supply Chain", "Cyberattack" and "NIST" were gathered as shown in Figure 3.

The search found: 7 documents in the SCOPUS database, from those 5 are directly related to the case study; 0 results were found in arXiv, 22 publications related to the subject of study were found in Sciencedirect; Two articles related to the purpose of the article were found in the Taylor & Francis database; 2 articles were found in the IEEE database; 8 articles of interest were found on websites associated with cybersecurity for the purpose of this article. Table 1 presents a summary of the search results.

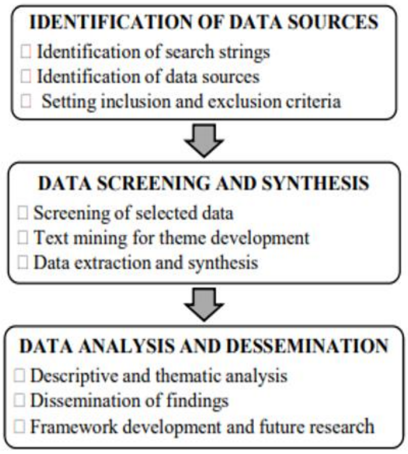

IDENTIFICATION OF DATA SOURCES
□ Identification of search strings
□ Identification of data sources
□ Setting inclusion and exclusion criteria
DATA SCREENING AND SYNTHESIS
□ Screening of selected data
□ Text mining for theme development
□ Data extraction and synthesis
DATA ANALYSIS AND DESSEMINATION
□ Descriptive and thematic analysis
□ Dissemination of findings
□ Framework development and future research

Figure 2. Systematic literature review process, adapted from [11-13]

2.1 Hacking timeline SolarWinds

Figure 4 shows the SolarWinds supply chain attack timeline from the day the suspicious activity occurred; It is observed that an access to the SolarWinds' network by the malicious agent occurs, then it manages to materialize a code injection; induces these changes to be compiled and deployed in software updates to customers, and finally there is a consequent reaction from SolarWinds that released "hot-fix" patches and that also led to alerts and subsequent investigations by authorities such as the US -CERT that published the CVEs worldwide.

2.2 Techniques and threats to the software supply chain

According to the Cybersecurity and Infrastructure Security Agency report (2021), The lifecycle of the ICT supply chain has six phases. In each phase of the lifecycle, software runs the risk of malicious or inadvertent vulnerabilities being introduced as shown in the examples in Table 2.

Let's see, in the design phase, hidden functions are incorporated in the source code to perform actions in the background without the user's consent; In the development and production phase persistent infiltrations can occur to achieve intrusions to the software's update services; In the distribution phase, pre-installed malware is infiltrated into devices before they are sent to the customer; in the acquisition and deployment phase, "spyware" tools can be introduced into the software of certain vendors; in the maintenance phase backdoors are introduced through the upgrade services; and in the final disposal phase, data can be recovered from discarded devices that have not had a correct data cleaning and eradication process.

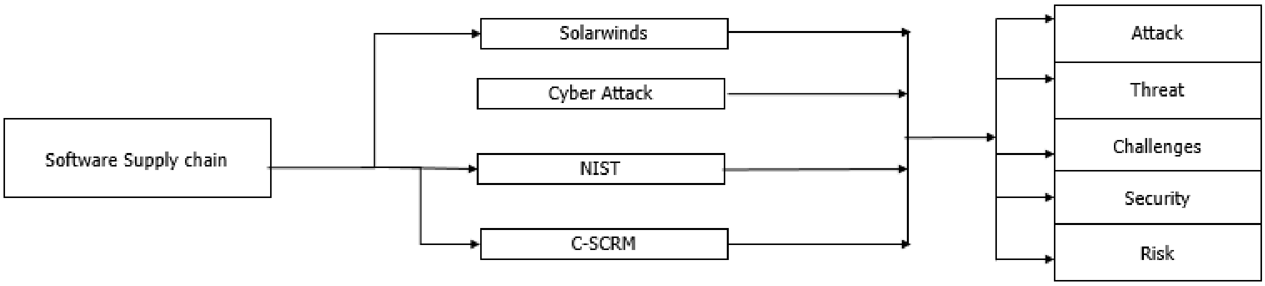


Figure 3. Keyword chain

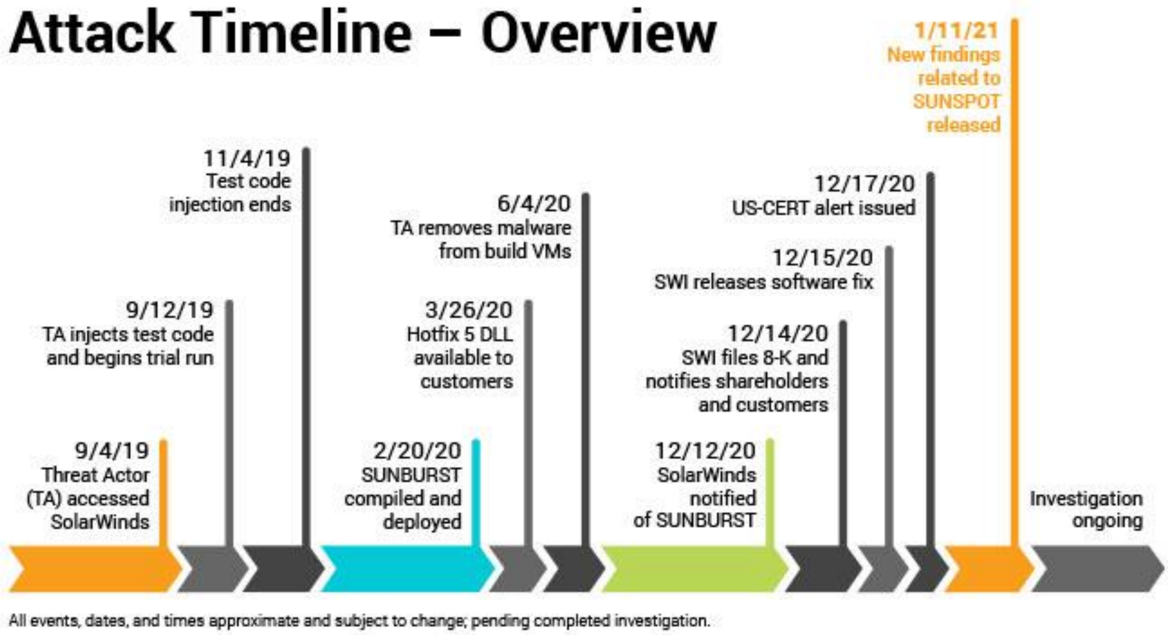

Attack Timeline – Overview
9/4/19 Threat Actor (TA) accessed SolarWinds
9/12/19 TA injects test code and begins trial run
11/4/19 Test code injection ends
2/20/20 SUNBURST compiled and deployed
3/26/20 Hotfix 5 DLL available to customers
6/4/20 TA removes malware from build VMs
12/12/20 SolarWinds notified of SUNBURST
12/14/20 SWI files 8-K and notifies shareholders and customers
12/15/20 SWI releases software fix
12/17/20 US-CERT alert issued
1/11/21 New findings related to SUNSPOT released
Investigation ongoing
All events, dates, and times approximate and subject to change; pending completed investigation.

Figure 4. SolarWinds timeline, Source [14]

Table 1. Article keyword string search

Author	Publication medium	Publication type	Extracts
[15]	Sciencedirect	Article review	A breach of SolarWinds’ Orion system and network monitoring platform has led to backdoors being implanted ...
[16]	Sciencedirect	Article review	Hot on the heels of the SolarWinds debacle, another software supply chain attack has been discovered ...
[17]	Sciencedirect	Article review	The distinction between unknown and known threats might seem simple. But in practical terms there is a huge difference between the way we deal with them: for many, this is a huge problem.
[18]	Sciencedirect	Article review	We study the decision-making problem in cybersecurity risk planning concerning resource allocation strategies by government and firms.
[19]	Sciencedirect	Article review	Modern software systems employ large IT infrastructures hosted in on-premise clouds or using “rented” cloud resources from specific vendors. The unifying force across any cloud strategy is incremental product and application improvement against conservation of those resources. This is where monitoring of cloud applications becomes a key asset
[20]	Sciencedirect	Article review	For decades, firewalls have protected networks from attack by restricting and inspecting traffic at the network perimeter. With cloud computing and increase demands for remote access to corporate networks, the network boundaries have widened.
[21]	Taylor & Francis	Article review	Russia’s SolarWinds hack appears to constitute reconnaissance and espionage of the sort that the US itself excels at, not an act of war.
[22]	IEEE	Article	SolarWinds hack is an eyeopener to the current practices of the software industry. In the “Perspectives” department in this issue, some of IEEE Security & Privacy’s editorial board members discussed.

2.3 Security operations center (SOC)

The function of a security operations team and, frequently, of a security operations center (SOC), is to monitor, detect, investigate, and respond to cyber threats around the clock. Security operations teams are charged with monitoring and protecting many assets, such as intellectual property, personnel data, business systems, and brand integrity [23].

2.4 Security Information and Event Management (SIEM)

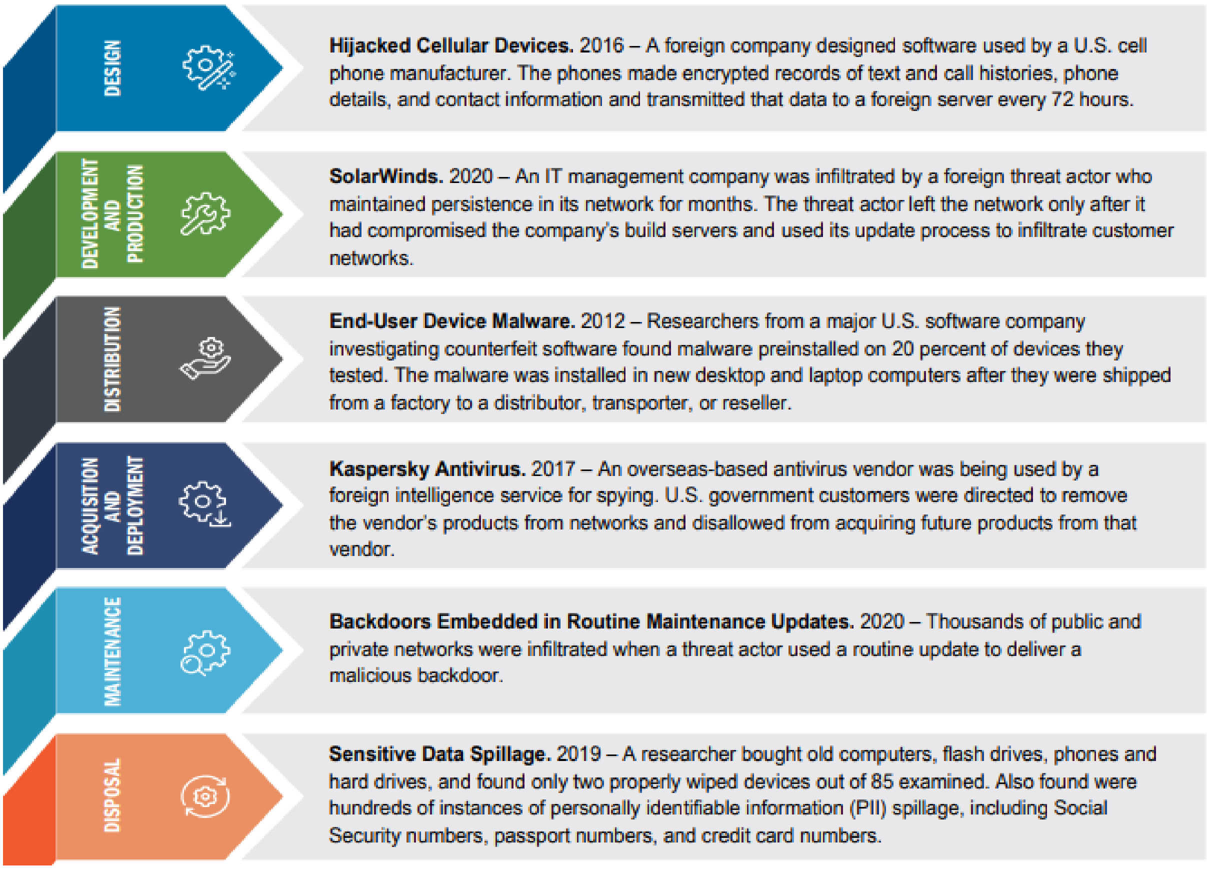
SIEM is a security solution that helps organizations recognize potential security threats and vulnerabilities before they have a chance to disrupt business operations. It surfaces user behavior anomalies and uses artificial intelligence to automate many of the manual processes associated with threat detection and incident response and has become a staple in modern-day security operation centers (SOCs) for security and compliance management use cases.

Today, SIEM offers advanced user and entity behavior analytics (UEBA) thanks to the power of AI and machine learning. It is a highly efficient data orchestration system for managing ever-evolving threats as well as regulatory compliance and reporting [24].

2.5 SOAR (security orchestration, automation and response)

SOAR (security orchestration, automation and response) is a stack of compatible software programs that enables an organization to collect data about security threats and respond to security events without human assistance. The goal of using a SOAR platform is to improve the efficiency of physical and digital security operations. SOAR platforms have three main components: security orchestration, security automation and security response [25].

Table 2. ICT supply chain lifecycle and examples of threats, Source [26]



DESIGN	**Hijacked Cellular Devices.** 2016 – A foreign company designed software used by a U.S. cell phone manufacturer. The phones made encrypted records of text and call histories, phone details, and contact information and transmitted that data to a foreign server every 72 hours.
DEVELOPMENT AND PRODUCTION	**SolarWinds.** 2020 – An IT management company was infiltrated by a foreign threat actor who maintained persistence in its network for months. The threat actor left the network only after it had compromised the company's build servers and used its update process to infiltrate customer networks.
DISTRIBUTION	**End-User Device Malware.** 2012 – Researchers from a major U.S. software company investigating counterfeit software found malware preinstalled on 20 percent of devices they tested. The malware was installed in new desktop and laptop computers after they were shipped from a factory to a distributor, transporter, or reseller.
ACQUISITION AND DEPLOYMENT	**Kaspersky Antivirus.** 2017 – An overseas-based antivirus vendor was being used by a foreign intelligence service for spying. U.S. government customers were directed to remove the vendor's products from networks and disallowed from acquiring future products from that vendor.
MAINTENANCE	**Backdoors Embedded in Routine Maintenance Updates.** 2020 – Thousands of public and private networks were infiltrated when a threat actor used a routine update to deliver a malicious backdoor.
DISPOSAL	**Sensitive Data Spillage.** 2019 – A researcher bought old computers, flash drives, phones and hard drives, and found only two properly wiped devices out of 85 examined. Also found were hundreds of instances of personally identifiable information (PII) spillage, including Social Security numbers, passport numbers, and credit card numbers.

The three most common attack techniques used by cybercriminals in breaching the software supply chain are described below: Hijacking updates, Undermining code signing, and Compromising open-source code.

2.5.1 Hijacking updates

Software vendors typically distribute updates from centralized servers to customers as a routine part of product maintenance. Attackers can hijack an update by infiltrating the provider's network and insert malware into the outgoing update or alter the update to obtain the control over the software's functionality [26].

2.5.2 Undermining code signing

The attacker manages to gain access to build servers or developer workstations without any obstacle from code signing systems, allowing them to successfully hijack software updates, as they act as a trusted provider, in the end they succeed insert malicious code into a theoretically benign update and spread its distribution without any detection [27].

2.5.3 Compromising open-source code

It occurs when attackers insert malicious code into publicly accessible code libraries, which is then used by unsuspecting developers looking for free code blocks to perform specific functions, finally that reuse of code results in adding attackers' code [28].

2.6 Recent supply chain breach attacks

We now describe some recent cases of software supply chain breaches that illustrate the exponential impact of these types of attacks on information security:

2.6.1 Colonial pipeline cyber attack

Colonial Pipeline suffered a ransomware attack due to attackers gaining access to computer networks using a compromised password, forcing the US power company to shut down its entire fuel distribution pipeline and thus threatening distribution of gasoline and jet fuel on the east coast of the United States [29].

2.6.2 JBS cyber attack

JBS, the world's largest meat company by sales, revealed that it was the victim of an "organized cybersecurity attack" targeting its IT network, temporarily shutting down its operations in Australia, Canada and the US. The intrusion was attributed to REvil (also known as Sodinokibi), a prolific Russian-linked cybercrime group that has become one of the top-earning ransomware cartels for attacks of this type [30].

2.6.3 Kaseya cyber attack

A supply chain attack on the VSA product, a tool that combines endpoint management and network monitoring. VSA can automate tasks such as backup and patch management and provides tools for access control and remote management. The product was infected with REvil ransomware and was distributed to more than 40 of its customers worldwide, and the company believes that between 800 and 1,500 companies worldwide have been affected [31].

2.6.4 Realtek flaw cyber attack

A vulnerability in the software development kit (SDK) of famous Taiwanese semiconductor firm Realtek put dozens of companies using their technology for IoT devices at risk through a variant of malware called Mirai, which induces vulnerabilities that allow an attacker to gain control of the

Wifi's module of the IoT devices and even gain root access to the operating system. This in effect represents a risk of attack on the supply chain for companies that implement this type of Realtek's devices.

3. RESEARCH METHODS

This Research article provides a description and analysis of the case study of the attack on the Solarwinds supply chain based on 6 of the 7 Essential Steps of the Cybersecurity Kill-Chain Process Cyber Kill Chain see Figure 5.

Stage 1: Reconnaissance

The attackers collected information from the database of the emails of all the employees of the victim company using techniques such as social engineering and exploiting an authentication vulnerability in the mail server and created a profile of the developers they should target in order to launch the attack.

Stage 2: Weaponization

Then, they created a DLL backdoor is known as Sunburst (as per FireEye) or Solorigate (as per Microsoft) and is executed by the "SolarWinds.BusinessLayerHost.exe" program.

Stage 3: Delivery

The attackers use the Spear Phishing technique, taking advantage of the developer profile to disguise the malware in an updated version of the Orion company's network management software that would later be distributed throughout the supply chain. (see Figures 6, 7).

Stage 4: Exploitation

The attackers just had to wait for the victims to run the Orion network management software update and the malware (SolarWinds.Orion.Core.BusinessLayer.dll with a file hash of [b91ce2fa41029f6955bff20079468448] and 2. C: \ WINDOWS \ SysWOW64 \ netsetupsvc.dll - A file that is not normally found on a Windows system.

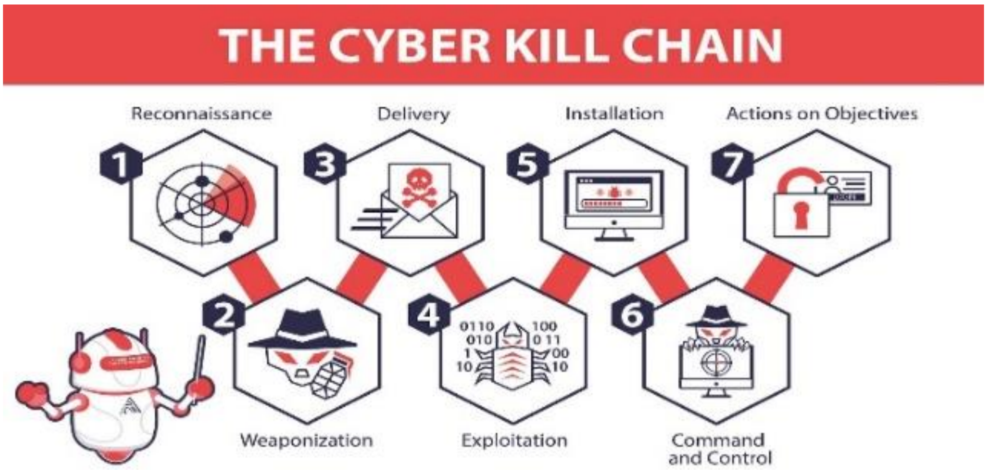


Figure 5. Steps of SolarWinds, Source [29]

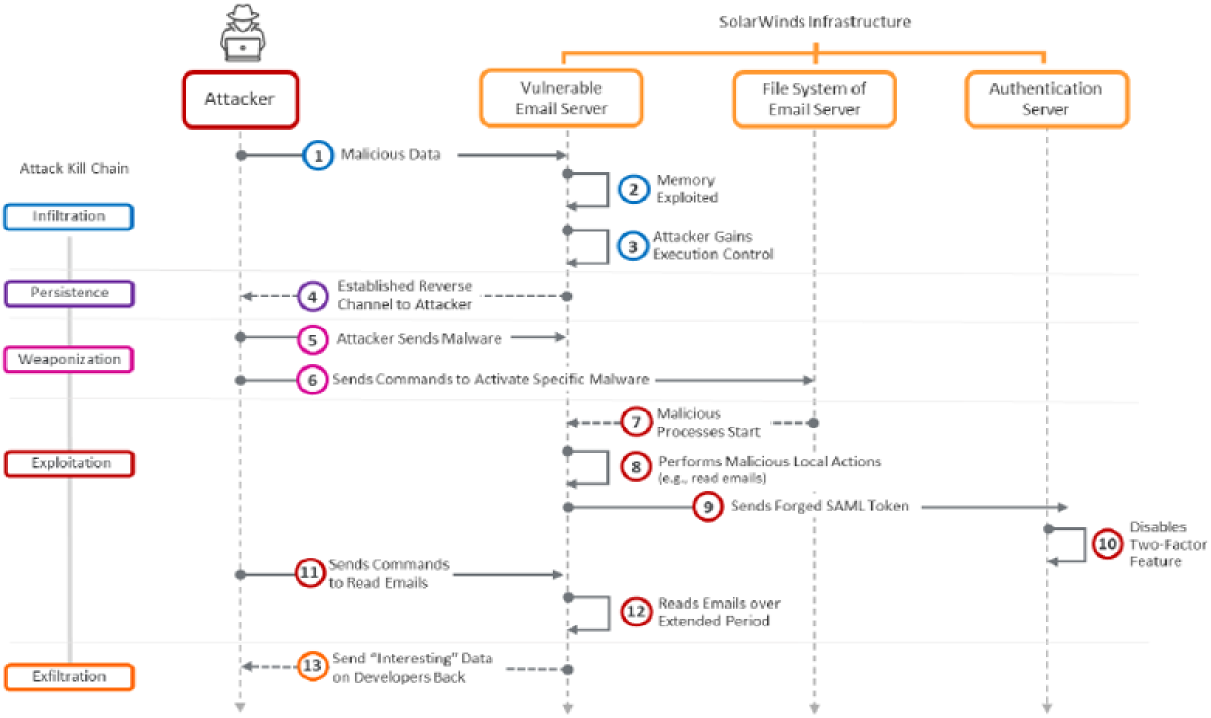

SolarWinds Infrastructure
Attacker
Vulnerable Email Server
File System of Email Server
Authentication Server
Attack Kill Chain
Infiltration
Persistence
Weaponization
Exploitation
Exfiltration
1 Malicious Data
2 Memory Exploited
3 Attacker Gains Execution Control
4 Established Reverse Channel to Attacker
5 Attacker Sends Malware
6 Sends Commands to Activate Specific Malware
7 Malicious Processes Start
8 Performs Malicious Local Actions (e.g., read emails)
9 Sends Forged SAML Token
10 Disables Two-Factor Feature
11 Sends Commands to Read Emails
12 Reads Emails over Extended Period
13 Send "Interesting" Data on Developers Back

Figure 6. Stage 1 Attack on a vulnerable server in SolarWinds infrastructure, Source [30], p. 4

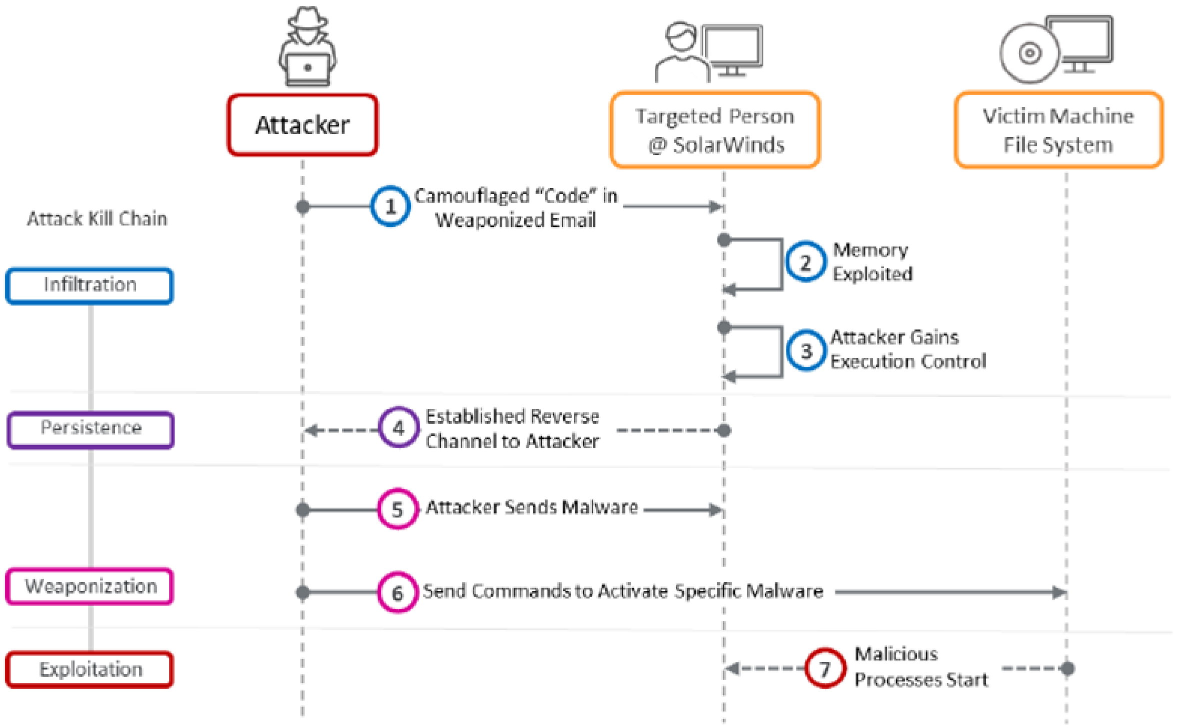

Attacker
Targeted Person @ SolarWinds
Victim Machine File System
Attack Kill Chain
Infiltration
Persistence
Weaponization
Exploitation
1 Camouflaged "Code" in Weaponized Email
2 Memory Exploited
3 Attacker Gains Execution Control
4 Established Reverse Channel to Attacker
5 Attacker Sends Malware
6 Send Commands to Activate Specific Malware
7 Malicious Processes Start

Figure 7. Stage 3 Attack on gullible human
Source [30], p. 5

Stage 5: Installation

The attackers expected that the victim would install the network management software update executable and the malware would automatically install itself by opening a backdoor on the victim's server for the attackers to access the services.

Stage 6: Command & Control (C2)

For a typical infection, Sunburst will first send to the C&C server the first 14 characters of the Windows domain name. This will continue for each 14 character chunk, until the entire Windows Domain name is sent.

Next, the attackers will instruct Sunburst to send the current security product statuses and then send information enabling Sunburst to launch a more robust secondary HTTP-based C&C shown in Figure 8.

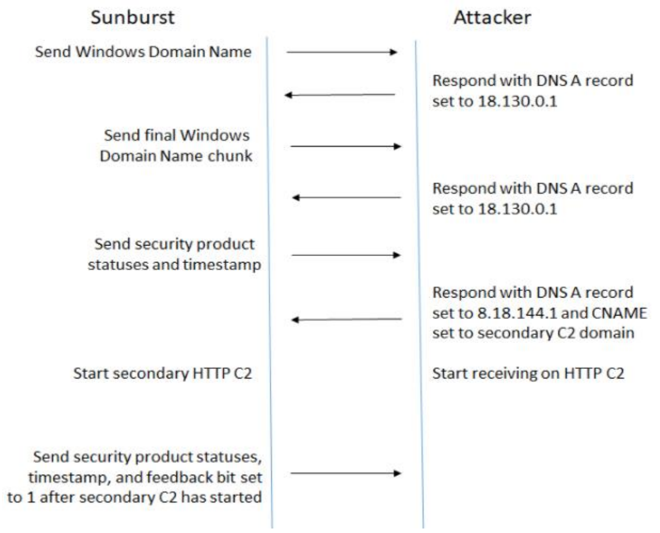

Sunburst
Attacker
Send Windows Domain Name
Respond with DNS A record set to 18.130.0.1
Send final Windows Domain Name chunk
Respond with DNS A record set to 18.130.0.1
Send security product statuses and timestamp
Respond with DNS A record set to 8.18.144.1 and CNAME set to secondary C2 domain
Start secondary HTTP C2
Start receiving on HTTP C2
Send security product statuses, timestamp, and feedback bit set to 1 after secondary C2 has started

Figure 8. Example of C&C control flow, Source [31]

4. RESULTS AND DISCUSSION

4.1 Results achieved with the Solarwinds attack

The attackers were able to remotely execute code with administrator privileges and insert the SUNSPOT malware into the Orion platform development environment, allowing them to sow a backdoor in the code of this important network monitoring and management tool. By controlling the source code of the software, the attackers inserted the SUNBURST backdoor before it was compiled, creating a "Dropper" version that would be distributed as a software update to all clients. SolarWinds signed the updates and distributed them, and customers had no reason to suspect that the update was infected and that it was going to compromise their application and service infrastructure.

"The impact is huge when you think that SolarWinds' customers include 425 of the Fortune 500 companies, 10 of the top US telecommunications companies.

US, Top Five US Accounting Firms, Hundreds of Universities and Colleges, and Several Federal Defense Agencies." [32].

Q1 How can organizations react in a timely, proactive manner and implement actions that help improve response times, and defend against attacks on software supply chain breaches?

Detecting and preventing attacks on the software supply chain is a major challenge, but from a geopolitical field, strategies can be led to help mitigate such attacks. The term "Software Bill of Materials" or "SBOM" means a formal record containing the details and supply chain relationships of various components used in building software. Software developers and vendors often create products by assembling existing open source and commercial software components. The SBOM enumerates these components in a product. It is analogous to a list of ingredients on food packaging. An

SBOM is useful to those who develop or manufacture software, those who select or purchase software, and those who operate software. Developers often use available open source and third-party software components to create a product; an SBOM allows the builder to make sure those components are up to date and to respond quickly to new vulnerabilities [33].

Based on the above, from a geopolitical perspective, governments should undertake initiatives and joint executive orders against the specifications of the requirements to share information from the Software Bill of Materials (SBOM) to defend against supply chain attacks. of software, since the software providers and the supply chain involve all the states and governments that do acquire the product.

The Attacks on the supply chain can be considered Zero Day, "Zero-day" is a broad term that describes recently discovered security vulnerabilities that hackers can use to attack systems. The term "zero-day" refers to the fact that the vendor or developer has only just learned of the flaw – which means they have “zero days” to fix it. A zero-day attack takes place when hackers exploit the flaw before developers have a chance to address it [34].

Also is recommended to explore security models based on early detection techniques through algorithms that use Machine learning, for example: alongside configuration management, an organization should identify its critical data and baseline how that data flows between processes or systems. Defenders can deploy analytics, including those based on machine learning/artificial intelligence, to identify subsequent anomalies in data flows, which may be early indicators of a threat actor’s exploitation of a vulnerability.

Another important element is that technology companies that incorporate software should have interdisciplinary teams that are part of the entire software supply chain management lifecycle and they should apply best practices based on agility such as DevSecOps (https://www.plutora.com/blog/devsecops-guide).

In addition, it is necessary to have governance around Cybersecurity in organizations. For this, the implementation of a SOC (Security Operation Center) or a SIEM (security information and event management tool) or a SOAR (security orchestration, automation and response tool) is recommended.

4.2 Access and authentication mechanisms

Strengthening access mechanisms to services should be one of the priorities of cybersecurity teams, implementing security schemes with Zero Trust techniques that reduce the risks of attacks on the software supply chain.

One of the strategies is to implement is the access credentials through Multi-Factor Authentication (MFA) and the encryption of data in transit through VPN. MFA is very important because users are required to provide two or more separate logon credentials before accessing a file or System. Some mechanisms to validate the authentication access are: sending notification through SMS messages, answering some questions, a smart card. a software certificate, or a fingerprint and iris pattern [35].

4.2.1 What is Multi-Factor Authentication (MFA)?

Multi-factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN. MFA is a core component of a strong identity and access management (IAM) policy. Rather than just asking for a username and password, MFA requires one or more additional verification factors, which decreases the likelihood of a successful cyber-attack.

Multi-Factor Authentication (MFA), as part of an identity and access management (IAM) solution, can help prevent some of the most common and successful types of cyberattacks, including: Phishing, Spear phishing, Key loggers, Credential stuffing, Brute force and reverse brute force attacks, Man-in-the-middle (MITM) attacks shown in Figure 9.

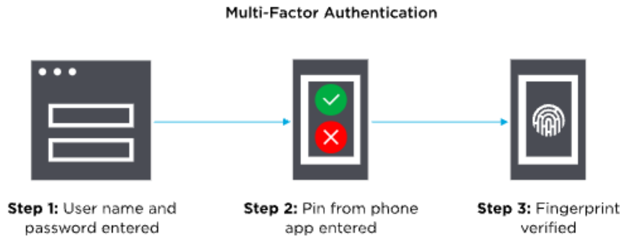

Multi-Factor Authentication
Step 1: User name and password entered
Step 2: Pin from phone app entered
Step 3: Fingerprint verified

Figure 9. Multi-factor autentication, Source [36]

5. CONCLUSIONS

It is also important to perform ethical hacking and pen testing; this permanently throughout the entire product lifecycle to find any vulnerabilities that could compromise the infrastructure or code of the organization's software products. While avoiding these types of attacks is challenging because modern software is built largely from the reuse of pre-built code and third-party software, governments and all actors in the supply chain must work together. in a series of standardized requirements for the development and management of applications from initiatives such as controlling software ingredients such as SBOM (Software Bill of Materials), and also being aligned to good practices with a layered defense approach such as Zero trust to protect their assets.

Companies should also continually apply good practices such as NIST SP 800-161 (Supply Chain -Risk Management Practices for Federal Information Systems and Organizations).

Another recommendation is to strengthen good identity and access practices to guarantee user authentication. One strategy is to implement single sign-on (SSO) with Multi-factor authentication where it is safe to manage access and maintain control over who can access the applications, as well as what devices and locations can be used. Another strategy would be to strengthen the authentication mechanisms through rules and policies based on AWS IAM and / or Azure AD or those offered by the cloud operator that the organization has contracted.

Based on this study, the authors suggest future research related to the present object of study: 1) Management strategies and articulation of hybrid work teams that integrate the entire lifecycle of the product from practices such as DevSecOps, 2) Creation of DataSet associated with the attack vector to be able to better analyze and predict the behavior and scope, through the use of techniques and models supported in Machine Learning, 3) Risk mitigation models for avoiding compromise to the supply chain through technologies as Blockchain 4) Define appropriation and articulation scenarios that help deliver a better experience to the end user in the identification and mitigation of this attack vector in software services derived from third parties.

REFERENCES

[1] Software supply chain attacks – everything you need to know | The Daily Swig. https://portswigger.net/daily-swig/software-supply-chain-attacks-everything-you-need-to-know, accessed on Nov. 04, 2021.

[2] Symantec Security Center. https://www.broadcom.com/support/security-center, accessed on Nov. 04, 2021.

[3] Software Supply Chain Attacks Are on the Rise - ECC IT Solutions. https://eccitsolutions.com/2019/05/06/software-supply-chain-attacks-are-on-the-rise/, accessed on Nov. 04, 2021.

[4] Software Supply Chain Attacks - WhiteSource. https://www.whitesourcesoftware.com/resources/blog/software-supply-chain-attacks/, accessed on Nov. 04, 2021.

[5] SolarWinds SUNBURST Backdoor DGA And Infected Domain Analysis. https://cybersecurityventures.com/solarwinds-sunburst-backdoor-dga-and-infected-domain-analysis/, accessed on Nov. 04, 2021.

[6] Why Software Supply Chain Attacks Are Inevitable and What You Must Do to Protect Your Applications - Security Boulevard. https://securityboulevard.com/2021/05/why-software-supply-chain-attacks-are-inevitable-and-what-you-must-do-to-protect-your-applications/, accessed on Nov. 04, 2021.

[7] Webster, J., Watson, R.T. (2002). Analyzing the past to prepare for the future: Writing a literature review. MIS Quarterly, 26(2): Xiii-Xxiii. https://www.jstor.org/stable/4132319

[8] Tranfield, D., Denyer, D., Smart, P. (2003). Towards a methodology for developing evidence-informed management knowledge by means of systematic review. British Journal of Management, 14(3): 207-222. https://doi.org/10.1111/1467-8551.00375

[9] Rousseau, D.M., Manning, J., Denyer, D. (2008). 11 Evidence in management and organizational science: Assembling the field's full weight of scientific knowledge through syntheses. Academy of Management Annals, 2(1): 475-515. https://doi.org/10.5465/19416520802211651

[10] Denyer, Y.D., Tranfield. (2009). Producing a systematic review. The Sage Handbook of Organizational Research Methods, 671-689.

[11] SolarWinds Orion Security Breach: Cyberattack Timeline and Hacking Incident Details - Page 3 of 4 - ChannelE2E. https://www.channele2e.com/technology/security/solarwinds-orion-breach-hacking-incident-timeline-and-updated-details/3/, accessed on Nov. 04, 2021.

[12] (2021). SolarWinds supply chain breach threatens government agencies and enterprises worldwide. Network Security, 2021(1): 1-3. https://doi.org/10.1016/S1353-4858(21)00001-5

[13] (2021). Supply chain attack puts thousands of firms at risk, Network Security, 2021(5): 1-2. https://doi.org/10.1016/S1353-4858(21)00044-1

[14] Campfield, M. (2021). The practical difference between known and unknown threats. Computer Fraud & Security, 2021(5): 6-9. https://doi.org/10.1016/S1361-3723(21)00051-8

[15] Paul, J.A., Zhang, M. (2021). Decision support model for cybersecurity risk planning: A two-stage stochastic programming framework featuring firms, government, and attacker. European Journal of Operational Research, 291(1): 349-364. https://doi.org/10.1016/j.ejor.2020.09.013

[16] Tamburri, D.A., Miglierina, M., Di Nitto, E. (2020). Cloud applications monitoring: An industrial study. Information and Software Technology, 127: 106376. https://doi.org/10.1016/j.infsof.2020.106376

[17] Haddon, D.A.E. (2020). Zero Trust networks, the concepts, the strategies, and the reality. Strategy, Leadership, and AI in the Cyber Ecosystem: The Role of Digital Societies in Information Governance and Decision Making, 195-216. https://doi.org/10.1016/B978-0-12-821442-8.00001-X

[18] Willett, M. (2021). Lessons of the SolarWinds Hack. Survival, 63(2): 7-26. https://doi.org/10.1080/00396338.2021.1906001

[19] Massacci, F., Jaeger, T., Peisert, S. (2021). Solarwinds and the challenges of patching: Can we ever stop dancing with the devil? IEEE Security & Privacy, 19(2): 14-19. https://doi.org/10.1109/MSEC.2021.3050433

[20] Mcafee. What Is a Security Operations Center (SOC)? https://www.mcafee.com/enterprise/en-us/security-awareness/operations/what-is-soc.html, accessed on Oct 16, 2021.

[21] IBM. What is SIEM? https://www.ibm.com/topics/siem, accessed on Oct 16, 2021.

[22] Techtarget, "What is SOAR (Security Orchestration, Automation and Response)? A definition from WhatIs.com." https://searchsecurity.techtarget.com/definition/SOAR, accessed Nov. 04, 2021.

[23] I. Security Agency, "Defending Against Software Supply Chain Attacks," Available: http://www.cisa.gov/tlp/, accessed on Nov. 04, 2021.

[24] Keyfactor, "What is Code Signing? The Definitive Roadmap to Secure Code Signing," *https://www.keyfactor.com/resources/what-is-code-signing/#why_security_matters*. https://www.keyfactor.com/resources/what-is-code-signing/#why_security_matters, accessed on Nov. 04, 2021.

[25] Curtis, F. "How Hackers Infiltrate Open Source Projects," Jun. 27, 2019. https://www.darkreading.com/application-security/how-hackers-infiltrate-open-source-projects, accessed on Nov. 04, 2021.

[26] Turton, W., Mehrotra, K. "Colonial Pipeline Cyber Attack: Hackers Used Compromised Password - Bloomberg," *Hackers Breached Colonial Pipeline Using Compromised Password*, Jun. 04, 2021. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password, accessed on Nov. 04, 2021.

[27] Lakshmanan, R. "Beef Supplier JBS Paid Hackers $11 Million Ransom After Cyberattack," Jun. 09, 2021. https://thehackernews.com/2021/06/beef-supplier-jbs-paid-hackers-11.html, accessed on Nov. 04, 2021.

[28] Cyber Security News, "Kaseya's Software Supply-Chain Attack Hits 40 Customers Worldwide," Jul. 05, 2021.

https://cybersecuritynews.com/kaseya-supply-chain/?amp, accessed on Nov. 04, 2021.

[29] CyCraft Technology Corp, "CyCraft Classroom: MITRE ATT&CK vs. Cyber Kill Chain vs. Diamond Model," *In cybersecurity, there have been several approaches used to track and analyze the various characteristics of cyber intrusions by advanced threat actors.*, Jun. 30, 2020. https://medium.com/cycraft/cycraft-classroom-mitre-att-ck-vs-cyber-kill-chain-vs-diamond-model-1cc8fa49a20f, accessed on Nov. 04, 2021.

[30] Gupta, S. (2020). Taxonomy of The Attack on SolarWinds and Its Supply Chain. https://www.virsec.com/whitepaper/taxonomy-of-the-attack-on-solarwinds-and-its-supply-chain.

[31] Threat Hunter Team and Symantec, "SolarWinds: Insights into Attacker Command and Control Process | Symantec Blogs," Jan. 15, 2021. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/solarwinds-sunburst-command-control, accessed on Nov. 04, 2021.

[32] Daasel, "¿Qué podemos aprender del ciberataque a Solarwinds? https://daasel.com/que-podemos-aprender-del-ciberataque-a-solarwinds/, accessed on Nov. 04, 2021.

[33] Wadhvani, V. "SBOM: the 1st Step Towards Defending Against SW Supply Chain Attacks," Jun. 13, 2021. https://www.deepfactor.io/blog/sbom-plus-appsec-observability-can-defend-against-software-supply-chain-attacks, accessed on Nov. 04, 2021.

[34] Kaspersky, "Zero-Day Exploits & Zero-Day Attacks," *What is a Zero-day Attack? - Definition and Explanation*, 2021. https://www.kaspersky.com/resource-center/definitions/zero-day-exploit, accessed on Nov. 04, 2021.

[35] Johnson, K. "How to Implement Multi-Factor Authentication — and Why It Matters," *SupplyChainBrain*, Jul. 30, 2020. https://www.supplychainbrain.com/blogs/1-think-tank/post/31733-how-to-implement-multi-factor-authentication-and-why-it-matters, accessed on Nov. 04, 2021.

[36] "What is Multi-Factor Authentication (MFA)?" *OneLogin*. https://www.onelogin.com/learn/what-is-mfa, accessed on Nov. 04, 2021.