TLP: WHITE

May 2024

The Domino Effect: Understanding Supply Chain Attacks in Healthcare

"Cyber resilience is much more than a matter of technology. Agility, balance and high-level view are indispensable"
- Stéphane Nippo - Global CISO of the Year, 2018

A Product of the Health-ISAC UCF Internship Program
Spearheaded By: Taylor Porter, Gabriel Saavedra

Health-ISAC™
Collaborating for Resilience in Healthcare
SHARING SINCE 2010

TABLE OF CONTENTS

Key Judgements

- The inherent complexity of organizational supply chains creates vulnerabilities threat actors can exploit.
- The critical nature of the health and public health sector makes it a valuable target for threat actors.
- Asking the right questions is crucial for identifying knowledge gaps and mitigating third-party supply chain vulnerabilities.

Executive Summary

The June 2023 cyberattack on Progress MOVEit demonstrated how threat actors can target an organization's supply chain through third-party and partner connections to cause disruptions across multiple sectors. Other recent major cyberattacks include SolarWinds, Kaseya, NMP IconBurst, and Cyber Av3ngers Unitronics. These attacks demonstrate how threat actors with varying intents and capabilities can exploit vulnerabilities within a supply chain. By attacking a third-party entity to target an organization (or set of organizations), threat actors can circumvent a strong security infrastructure by exploiting the supply chain itself as a springboard by exploiting previously unknown vulnerabilities, or zero-days.

Examining these attacks can allow us to glean insights into the current state of supply chain risk management and its future. These insights can provide CISOs with questions to inform how their cybersecurity teams can best identify and mitigate risks in their environments. These questions can expose the range of possible attack vectors like security misconfigurations, such as leaving default passwords unchanged, or the use of open-source code in products, which can be sabotaged by threat actors. Answering these questions can also assist in maximizing an organization's security infrastructure and understanding the security posture of a third party that may be operating a critical business function.

Supply chains attacks will continue to be prevalent in critical infrastructure sectors moving forward as threat actors seek to prey on the reliance of their services. However, this can be mitigated by developing a strong security infrastructure, forward-thinking CISOs asking their teams the right questions, and promoting a culture of cyber resilience by engaging in information sharing and developing relationships with peers, partners and public sector agencies.

Introduction

Over the last decade, attacks on third-party entities such as Progress MOVEit Managed File Transfer (MFT) solution have resulted in a cascading of impacts on the healthcare sector. These attacks exploit the trust between vendors and customers, abusing preexisting permissions. Therefore, third-party risk should be at the forefront of an organization's security concerns. To build resilience in the healthcare sector, this document will discuss the nature of third-party risk, case studies of major third-party attacks, recommendations for how CISOs can help mitigate risk, and forecast possible trends to understand what the future of third-party risk may look like.

Third-Party Risk

A supply chain represents the components that make up an organization's product and the processes that go into creating a final product. Typically, it describes the entire process by which final products are created, including suppliers, logistics, manufacturers and any other entity involved in the creation process of a given product. In the security context, the supply chain refers to the network of tools and entities involved in cybersecurity day-to-day operations.

Supply chains are most often largely made up of third parties; vendors or other external entities that are hired to assist in the security or operations of a given organization. Unaddressed third-party risk in security supply chains can lead to some of the most devastating attacks in terms of damage to an organization's security and reputation. Due to the inherent length and complexity of a security supply chain of an operating environment that meets all the needs of a healthcare organization, the operating environment often includes multiple vendors. Each vendor included also brings their respective supply chains and third-party risk.

The relationship between healthcare entities and third-party services contain some inherent trust because vendor tools could be used to work with patient or proprietary data. While inclusion of these third parties facilitate the streamline of daily operations, it also introduces new security concerns as the vendor's vulnerabilities become the organization's vulnerabilities as well through the use of vendor-created software. Threat actors are taking advantage of this relationship by engaging in what is called a supply-chain attack.

A supply chain attack is when a threat actor attacks a third-party entity to indirectly gain access to an organization[1]. This attack can be perpetuated in a variety of third-party compromise methods, including island-hopping and zero-day exploitation.

Third-party compromise is when a third-party entity is breached by a threat actor to gain access to a target company's network[2]. This can be seen when threat actors compromise a software vendor to send out phony updates to organizations that result in malware infection, or social engineering attacks that target specific organizations using their own sensitive data in email lures.

Similarly, an island-hopping attack is when a threat actor works its way up their target's supply chain by targeting smaller affiliates and using them as a springboard to attack larger third parties until access to the target organization is gained[3]. Attacks such as these are often done when a victim's security infrastructure is too difficult to penetrate directly, leading threat actors to investigate less secure links in their supply chain as an alternative method of access.

Once access is gained, threat actors can convert frequently used company websites into a metaphorical watering hole, infecting them with malware to compromise company devices used to access it. Also, threat actors could compromise a third party's email server to send malware packages to their victims from an organization that the victim already trusts.

An especially damaging type of supply chain attack is what is known as a zero-day, a vulnerability in a product's security that is unknown to its owners, developers, or anyone else that could remediate it. In the hands of threat actors, zero-days can be used to gain access to their target's systems to deploy ransomware, a type of malware that steals and encrypts a victim's data, denying them access unless they receive a decryption key.

Supply chain attacks are becoming more prevalent each passing year, with attacks increasing by 72% between 2022 and 2023[4].

[1] CISA (2021). Defending Against Software Supply Chain Attacks. Cybersecurity & Infrastructure Security Agency https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf

[2] Pope, T. (2018). Supply Chain Threats to Industrial Control: Third-Party Compromise. Dragos. https://www.dragos.com/blog/industry-news/supply-chain-threats-to-industrial-control-third-party-compromise/

[3] Scammell, R. (2019) 'Island hopping' cyberattacks are threatening supply chains. Verdict. https://www.verdict.co.uk/island-hopping-cyberattacks-supply-chains/?cf-view

[4] Mello, J. (2024). Zero-day, supply-chain attacks drove data breach high for 2023. CSO Online. https://www.csoonline.com/article/1298730/zero-day-supply-chain-attacks-drove-data-breach-high-for-2023.html#:~:text=The%20report%20noted%20that%20the,was%20fueled%20by%20old%20adversaries

The ever-evolving nature of the cybersecurity landscape means that there will always be new challenges for organizations to contend with. One such challenge is rapid technological advancements in the cybercriminal sphere. These advancements allow threat actors to carry out stealthier attacks that avoid detection and capitalize off the integration of artificial intelligence in the cybercriminal workflow.

Additionally, the healthcare threat environment is evolving as cybercriminals, nation-state actors, and hacktivists all try to exploit less secure elements in supply-chains using various methods to accomplish different objectives. Cybercriminals are financially motivated threat actors who target organizations through a wide range of means, such as ransomware attacks, to make a profit. Nation-state actors are threat actors directly sponsored by a specific country, driven by direct commands from the governing body for which they work, often aligning with geopolitical motivations, such as committing intellectual property theft to bolster the domestic economy. Hacktivists are threat actors operating for political reasons. An example of this would be disrupting a government office’s IT systems to protest a new law.

Incorporating an external vendor into a security environment brings a lot of enhanced capability, but also the challenges of how to incorporate an external system with its own vulnerabilities. A compromise on a vendor system can mean a compromise for the customer as well if security teams do not maintain third-party products or audit their permissions. Other challenges include regulatory and compliance pressures that influence the balance between security and business obligations. Despite its importance in protecting customers and data, many organizations have difficulties allocating proper resources to their security teams to ensure the proper deployment of third-party software as security is often considered necessary but does not bring in additional revenue. This has led many governments to put out new guidelines mandating sector-specific minimum-security baselines for organizations handling sensitive data. There are multiple real-world examples that exemplify why threat actors perform supply chain attacks and the way they have impacted entire sectors and countries. Through retroactive analysis, there is significant overlap between major third-party compromise incidents that help guide CISO efforts to protect their organizations.

Case Studies

SolarWinds:

The attack on the remote monitoring company, SolarWinds, unfolded mid-December 2020. The attack targeted the SolarWinds Orion platform which is a network management software used to manage IT architectures. Orion clientele included many high value customers such as U.S. government agencies. In October 2019, the initial code injection was tested and between December 2019 to February 2020 the command-and-control (C2) infrastructure was set up to create a malicious update. The code was known as Sunburst. By March 2020, a remote access tool malware was planted into the Orion updates. Once rolled out in the form of an update, approximately 18,000 Orion customers became infected with malware. As of October 2023, the US Securities Exchange Commission (SEC) is suing SolarWinds for concealing vulnerabilities before the attack.[5] The vulnerability associated with the attack is CVE-2020-10148.[6] This attack was carried out by Nobelium, a Russian nation-state actor. It was suspected that the focus of this attack was the three letter agencies that used SolarWinds services.

[5] Oladimeji, S. & Kerner S. (2023). SolarWinds hack explained: Everything you need to know. TechTarget. https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know

[6] CIS (2021). The SolarWinds Cyber-Attack: What You Need to Know. CISECURITY. https://www.cisecurity.org/solarwinds

Various key lessons could be drawn from the SolarWinds attack to mitigate the risk of similar attacks, such as understanding what vendor systems are connected to an organization. Conducting vendor risk assessments can provide some insight into the potential vulnerabilities within a vendor system and what information a vendor may have access to. Ensuring that high-value members of an organization are not readily listed for the public to view can reduce the risk of a threat actor directly targeting that organization based on who their members are.

Kaseya:

The attack on the software company Kaseya occurred on July 2, 2021, when ransomware gang, REvil, exploited a zero-day vulnerability in the Kaseya software, CVE-2021-30116.[7] This allowed them to gain initial access to Kaseya's on-site virtual system administrator (VSA) servers through a public-facing application. Once on the server, REvil distributed their payload to Kaseya's managed service provider (MSP) customers through a malicious software update. This attack targeted the users of their remote monitoring and management platform (RMMP), a product that allows users to remotely manage endpoint devices. The malicious software update allowed REvil to exploit an older version of windows defender to bypass anti-virus programs on a victim's local workstation.

Once victims downloaded the phony update, REvil escalated their administrative privileges on the Kaseya RMMP while revoking the victims' access allowing them to gain access to all Kaseya-managed endpoint devices. This allowed them to disable Microsoft Defender's real-time monitoring and execute their ransomware program.

The Kaseya ransomware attack is an example of how a cybercriminal supply chain attack can be used for profit. The attack took advantage of the cascading nature of the impacts following a successful supply chain attack by targeting companies that are hired to perform remote IT functions and therefore possess third-party access to a plethora of organizations. Kaseya software is popular among MSPs as Virtual System/ Server Administrator, allowing them to remotely monitor and access client endpoints for IT management. Because MSPs handle IT operations at multiple organizations, REvil was able to extend the scope of the attack to the clients of the MSPs that used Kaseya software as well. Of the approximately 50 MSPs initially breached, over 1,500 organizations were ultimately attacked.[8]

NPM IconBurst:

NPM IconBurst is the name of a campaign that was carried out by cybercriminals targeting software developers. Threat actors created malicious npm packages that had names very similar to popular libraries containing icons that software developers would incorporate into their applications. These malicious packages utilized typosquatting, a tactic which uses common misspellings on popular names to lure unsuspecting web users to download malware-laden packages instead of the legitimate ones.

Once integrated into applications or websites, the malicious packages would steal data from victim machines. At the time of writing, one of the malicious packages has over 17,000 downloads.[9] Without proper validation of open-source code, members can inadvertently implement code into their software that contains malware.

Log4j is another widely used piece of open-source software. It was found to contain a remote code execution (RCE) flaw that began to be exploited by threat actors in 2022. Many organizations were susceptible to this vulnerability due to poor visibility into their software supply chains. This phenomenon is precisely why the attack was so successful. Threat actors were able to attack numerous organizations that did not know they had this software in their environment. Log4j highlighted the need to be aware of the risk associated with open-source code and ensure visibility into the software supply chain of applications used in sensitive environments, whereas npm IconBurst shows the need for validation of all open-source packages used in applications to avoid the implementation malicious packages.[10]

[7] Cimpanu, C. (2021) Kaseya zero-day involved in ransomware attack, patches coming. The Record. https://therecord.media/kaseya-zero-day-involved-in-ransomware-attack-patches-coming

[8] Allen, J. (2021) Kaseya VSA Ransomware Attack Explained. Purplesec. https://purplesec.us/kaseya-ransomware-attack-explained/#respond

[9] Gatlan, S. (2022). NPM supply-chain attack impacts hundreds of websites and apps. BleepingComputer. https://www.bleepingcomputer.com/news/security/npm-supply-chain-attack-impacts-hundreds-of-websites-and-apps/

[10] Jones, D. (2023). 2 years on, Log4j still haunts the security community. Cybersecurity Dive. https://www.cybersecuritydive.com/news/log4j-haunts-security-community/702011/

Cyber Av3ngers Unitronics

An example of a hacktivist targeting the supply chain of an organization for political gain is when the pro-Palestinian hacktivist group Cyber Av3ngers targeted the US water sector in protest of US support to Israel. The Iranian-based threat actor targeted products made by the Israeli company, Unitronics, as a form of protest. One of their notable attacks was detected on November 25, 2023, targeting the Municipal Water Authority of Aliquippa in Pennsylvania.[11]

The group exploited CVE-2023-6448 to access internet facing programmable logic controllers (PLCs) that had not changed their default passwords.[12] PLCs are computers designed to automate and monitor industrial processes that if compromised can disrupt an entire facility's operation. The attack on Aliquippa displayed a defacement message on the human-machine interface that rendered the PLC inoperable.

The attack ultimately only resulted in defacement but could have impacted critical infrastructure across the United States as the PLCs used in water treatment facilities ensure filtered water is potable. Jeopardization of this function could have led to the contamination or disruption of large swathes of people's water supply.

MOVEit Attack

The attack on MOVEit is one of the most recent examples of a major cybersecurity incident involving third-party compromise and the cascading impacts it can have. MOVEit, a managed file transfer (MFT) service from Progress Software, was designed to allow users to move large quantities of data through the internet in a secure manner, making it popular across multiple industry sectors. The proximity to sensitive business data, and its widespread use at thousands of organizations made MOVEit a valuable target for threat actors.

The attack occurred on June 6, 2023, when the Ransomware as a Service (RaaS) gang Cl0p, exploited a zero-day vulnerability in MOVEit , later tracked as CVE-2023-34362, to gain initial network access through the frontend of the application.[13] The vulnerability allowed Cl0p to acquire administrator level access which allowed the threat actor to establish a backdoor in the program and obtain a list of all the files, users, and folders within the program. Instead of deploying ransomware, the Cl0p actors decided to use the MFT to simply exfiltrate data without encryption and extort the victims.[14]

The attack resulted in hundreds of organizations having valuable data stolen and 16 million individuals having their personally identifiable information (PII) being leaked, including Health and Public Health (HPH) entities. For the healthcare sector, file transfers can contain not only PII, but also protected health information (PHI) that threat actors could use to extort healthcare organizations and patients alike. Health-ISAC sent out approximately 61 targeted alerts to member organizations that had vulnerable MOVEit instances in their environment.

The MOVEit attack leveraged a zero-day vulnerability within a product with access to multiple organizations' sensitive internal infrastructure to amplify the scope of the cyberattack. MOVEit, along with previous major third-party compromises demonstrate how supply chains can be exploited by threat actors. However, to truly keep an environment not only secure, but resilient, it is important to look toward the developing trends in the healthcare cyber threat landscape and predict what supply chain attacks will look like in the future.

[11] Stanish, E. (2023) Municipal Water Authority of Aliquippa hacked by Iranian-backed cyber group. CBS News. https://www.cbsnews.com/pittsburgh/news/municipal-water-authority-of-aliquippa-hacked-iranian-backed-cyber-group/

[12] CISA (2023). IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities. Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a

[13] Hammond, J. (2023). MOVEit Transfer Critical Vulnerability CVE-2023-34362 Rapid Response. https://www.huntress.com/blog/moveit-transfer-critical-vulnerability-rapid-response

[14] Outpost24 (2023). The MOVEit hack and what it taught us about application security. BleepingComputer. https://www.bleepingcomputer.com/news/security/the-moveit-hack-and-what-it-taught-us-about-application-security/

Analysis: Supply Chain Attacks Moving Forward

A study[15] done by Juniper Research found software supply-chain attacks are expected to continue in the coming years, reaching over $81 billion in damages by 2026. This has created a growing concern about cybercriminals, hacktivists and nation-state actors targeting critical infrastructure organizations to cause cascading impacts. Attacks such as these often lead to a community-wide impact due to the interdependence present in critical infrastructure systems. Additionally, attacks on third-party entities that disrupt other sectors of industry can also heavily affect the healthcare sector through collateral damage and disruption of external operational dependencies.

The single points of failure in supply chains will continue to be exploited by threat actors, especially in the large and complex systems that support critical infrastructure organizations. The longer the supply chain, the harder it is for security teams to investigate vulnerabilities as third-party products include multiple supply chains within themselves. Due to the presence of third and fourth parties, it can be very difficult to evaluate the full scope of a given supply chain. An organization can have so many products and auxiliaries that component details are hidden through obfuscation. Such complexity could attract threat actors to research the prospect of attacking an overlooked component that is critical to business operations in the pursuit of larger payouts.

Software providers with large clienteles will likely continue to be targeted by threat actors Because of their trusted access to many organizations and the proprietary data they hold. If compromised, these widely adopted products could represent a catalyst to increase the scope of a cyber-attack from one large software organization to also encompass its entire professional clientele.

Questions For CISOs

It’s important for CISOs to ask questions of their cybersecurity teams to ensure that information security programs are effective in reducing risk and maximizing resilience, while living within budget and personnel allocations. Here are a few important questions CISOs can ask their teams to gauge organizational third-party security posture, enumerate knowledge gaps and create thought provoking action to improving overall supply chain security:

- How often do you have vendor risk assessments? Are applications being regularly checked for vulnerabilities? Continue to review and monitor Common Vulnerabilities & Exposures (CVEs) along with their criticality to ensure appropriate priorities are applied to software patch management of internal systems and satellite products of centralized administrative software.
- Is patch management following a mature, repeatable process? Patch Management processes should call for priority testing of critical patches and implementation where warranted, plus a continuous review of current common vulnerabilities and exposures to infrastructure to reduce organizational attack surface.
- Are staff properly trained in organizational cyber policies?
- Are administrative privileges kept to an absolute minimum? Privileged Access Management (PAM) principles should be followed to help prevent unauthorized privileged access to critical resources.
- What are the current and future values of your data?

[15] SKapko, M. (2023). Costs of software supply chain attacks could exceed $46B this year. Cybersecurity Drive. https://www.cybersecuritydive.com/news/software-supply-chain-attacks/650148/

- If an adversary were to obtain access to the network, is there an opportunity for lateral movement? How long until they are detected? And how long until they are stopped?
- Are you incorporating Zero-Trust architecture and multifactor authentication?
- Are you monitoring reliable and timely cyber threat intelligence? Threat intelligence reports should be analyzed and potentially acted upon in a timely matter to protect the organization from new and emerging threats.
- Are you monitoring network traffic to determine what is normal baseline activity and able to detect anomalous activity?
- Are open-source software libraries evaluated thoroughly for security risks?

Additional Risk Management Considerations

- Identify mission critical third-party software, solutions and services utilized by the organization.
- Risk categorize and risk rank based upon scope of access to networks, volume and sensitivity of data.
- Risk rank based upon criticality to operations, revenue capture and most importantly, impact to patient care and safety.
- Utilize a vendor risk management program which incorporates cybersecurity, legal, compliance, clinical, finance and operations teams to assess risk in these types of mission critical third party, enterprise level applications.
- Ensure cybersecurity teams are involved in the scoping, purchase and acquisition of new technologies and have conducted appropriate cybersecurity due diligence on the product or service and the business associate organization.
- Develop business associate agreements which include and scale cybersecurity requirements proportionally with the risk ranking of the business associate organization and service being provided.
- Require business associates to notify within 72 hours of the discovery of any vulnerability, breach or compromise or which has the potential to impact the confidentiality, integrity and availability of your data, and or their services.
- Include cybersecurity insurance requirements in business associate agreements which scale proportionally with the identified risk ranking of the business associate.

Recommendations

Identifying Potential Risks Inside the Environment

Risks presented within healthcare environments include third-party transfer of patient information, large clienteles, misconfigured privileges and the use of open-source software – factors that could contribute to a huge payout for threat actors in a successful attack. The transfer of sensitive information across third-party managed file transfer products is often necessary due to the large volume of data being processed and its sensitive nature. For threat actors, this presents an opportunity to exploit third-party products to gain access to sensitive patient data via a supply chain attack, such as the attack on the MFT solution, MOVEit where threat actors were able to exploit a flaw in the product and steal sensitive patient data.

Familiarizing oneself with the makeup of organizational clientele and the size of the customer base is important for identifying risk. Threat actors are likely to target organizations with large clienteles to amplify the scope of their attack, allowing them to impact multiple victims. A cyberattack on an organization with a large clientele made up of influential companies can result in massive security impacts for customers, and potentially damage their reputation, leading to a mass migration of clients to other vendors and loss of revenue. For example, the fact that military and government agencies were customers of SolarWinds may have been a contributing factor as to why a nation state devoted resources into compromising the Orion software.

Identifying opportunities for a threat actor to abuse elevated privileges within the network is essential for shoring up your overall security. The SolarWinds attack utilized lateral movement to spread across a victim's network to escalate privileges to accomplish additional actions on objectives. A potential solution to this problem is the implementation of the principle of least privilege, a security architecture that limits the access a user has in a system to only what is necessary to perform their role, and reducing excessive privileges that could be exploited by an adversary.

Misconfigurations in third-party software can increase an organization's attack surface. In this context, misconfigurations are typically weaknesses in a software or application implementation due to oversights. Common misconfigurations include using default passwords, excessive permissions, and not installing available patches. Misconfigurations can lead to applications having vulnerabilities that threat actors would otherwise not be able to exploit if the application was properly maintained. One such misconfiguration was exploited in the Cyber Av3ngers Unitronics attack, where threat actors used the default passwords to attack the victim's PLC systems. Misconfigurations also lead to software staying at the version it was when it was installed, leaving it open to legacy vulnerabilities and new vulnerabilities alike. Organizations should ensure that all third-party software that acts on patient data is consistently patched to avoid legacy vulnerability exploitation. The use of open-source software brings the risks of threat actors integrating malicious packages in the software. Open-source software is open to the public, meaning it is accessible by anyone. The NPM IconBust campaign focused on sabotaging open-source code integration efforts through typo squatting. There are several reasons why an organization might use open-source software. It is cost-saving, easy to customize and has a quick response time for errors. However, if the software goes unchecked, then potential vulnerabilities can be exploited by threat actors without detection. To mitigate this, organizations can consume software bill of materials (SBOMs) to increase visibility into the open-source components in the software used in daily operations. SBOMs are lists of all components within a given product. By consuming SBOMs, it can help identify components within an application or system that contain known vulnerabilities.

Furthermore, regular vendor risk assessments can be completed to better understand the security controls a vendor has in place and how resilient they are to an attack (Ramos, 2020). By identifying the potential risks a vendor may have, an organization can determine whether they can tolerate the risk presented by onboarding an additional third party. Vendors are an external entity with their own respective supply chains, so it is often difficult to truly know what systems and supply chains are connected to an organization. In the event a fourth party gets compromised, it is important to have transparency agreements in place so that healthcare organizations can apply the relevant mitigations and disconnect impacted systems if possible.

Conclusion

Threat actors will continue to target the supply chain of large organizations, so it is important to identify the risks and the mitigation strategies pertaining to third-party compromise to minimize the potential impact of a security event. Information sharing and collaboration among cybersecurity professionals are vital in ensuring that an attack is not prolonged, and damages are minimized.

The healthcare sector is especially susceptible to supply chain attacks, just as any critical infrastructure sector is due to the importance of the services they provide. An attack on the healthcare sector or any of its third parties could have detrimental impacts to patient care, revenue and organizational reputation. After reviewing nearly, a decade's worth of supply chain attacks, their impacts, and the motivations behind them, it appears that the supply chain attacks will continue and grow in intensity and variety. Organizational supply chains will continue to be a major target for threat actors looking for large payouts and to maximize impacts. Mitigations for this issue include a strong cybersecurity program and vigilant CISOs asking their teams the right questions. Finally, participating in information sharing communities and creating strong relationships with public- and private-sector partners can help build resilience in the face of new and emerging cyber threats.