Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

The cyber threat from supply chains

Canada

About this document

Audience

This Cyber Threat Bulletin is intended for the cyber security community.

Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see https://www.first.org/tlp/.

Contact

For follow up questions or issues please contact Canadian Centre for Cyber Security at contact@cyber.gc.ca.

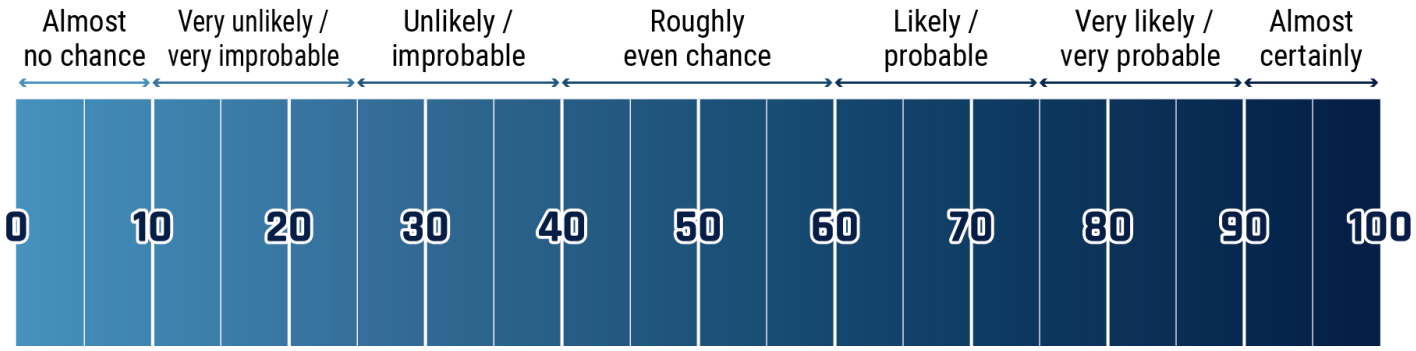
Assessment base and methodology

The key judgements in this assessment rely on reporting from multiples sources, both classified and unclassified. The judgements are based on the knowledge and expertise in cyber security of the Canadian Centre for Cyber Security (the Cyber Centre). Defending the Government of Canada's information systems provides the Cyber Centre with a unique perspective to observe trends in the cyber threat environment, which also informs our assessments. CSE's foreign intelligence mandate provides us with valuable insight into adversary behavior in cyberspace. While we must always protect classified sources and methods, we provide the reader with as much justification as possible for our judgements.

Our judgements are based on an analytical process that includes evaluating the quality of available information, exploring alternative explanations, mitigating biases and using probabilistic language. We use terms such as "we assess" or "we judge" to convey an analytic assessment. We use qualifiers such as "possibly", "likely", and "very likely" to convey probability.

The assessments and analysis are based on information available as of August 31st, 2022.

The cart below matches estimative language with approximate percentages. These percentages are not derived via statistical analysis, but are based on logic, available information, prior judgements, and methods that increase the accuracy of estimates.



Key judgements

- We assess that threat actors will almost certainly continue to develop their capability to compromise organizations through supply chains as an alternative to direct action against a target's network defences.

- We assess that state-sponsored threat actors will almost certainly continue to use supply chains to compromise targets of strategic interest, and that they will almost certainly continue to develop persistence within supply chains to facilitate the ongoing theft of valuable information.

- We assess it very likely that adversary states can influence their domestic vendors to compromise products to advance their national interest, counter to Canadian clients' interests, and the interests of Canada.

- We assess criminal threat actors, especially ransomware operators, are very likely to continue targeting supply chains to maximize the number of potential victims and profits per compromise.

- We assess it very likely that software will continue to be the primary vector for cyber threat movement in supply chains and assess it very unlikely that hardware trojans and hardware supply chain compromises will become a significant threat vector within supply chains in the near term.

- We assess it likely that zero-day exploits will continue to be used in supply chain compromises by sophisticated threat actors, allowing them to bypass security controls, avoid detection and make the most efficient use of the valuable exploit.

CONTENTS

The cyber threat from supply chains

Introduction

Supply chain compromises are an evolving threat to Canadian businesses, critical infrastructure, and governments. Supply chains are trusted ecosystems of suppliers and service providers that enable organizations to develop and deliver products and services. They increasingly feature the bidirectional movement of digital information in addition to the movement of products, services, and currency. Cyber threats propagate through digital information transfer, meaning supply chains provide an extended attack surface against Canadian organizations and an alternative for cyber threat actors to direct action against an organization's networks. Supply chain compromises are not a new technique for threat actors, but several recent notable compromises have brought supply chain security front-of-mind for organizations in Canada and around the world. We assess that supply chains will almost certainly continue to be targeted by threat actors in the near term.

The extended attack surface from supply chains can be difficult to secure. Supply chains, especially for information and communications technology, can be complex, globally distributed, and consist of multiple tiers of outsourcing.[1] The compromise of a single supplier upstream in the supply chain may result in the introduction of vulnerabilities to many downstream organizations and consumers. Over the past several years, threat actors have demonstrated an increased capacity to navigate through supply chains to compromise their ultimate targets. We assess that threat actors will almost certainly continue to develop their capability to compromise organizations through supply chains as an alternative to direct action against a target's network defences. We judge that Canadian organizations will almost certainly continue to experience cyberespionage and cybercrime originating from supply chains over the near term.

Why target supply chains?

Supply chain compromises provide an alternate and indirect means for threat actors to compromise their ultimate targets. A vulnerability may be introduced at any point in the supply chain or the life cycle of a good or service. This provides a much-expanded attack surface for threat actors to exploit rather than just targeting the external perimeter of a victim network. After the vulnerability has been deployed within the victim network, a threat actor's objectives are the same as with conventional cyber compromises. These objectives include cyber espionage or attack. In the context of supply chain compromises, this often means the theft of valuable information or intelligence, or the deployment of malware such as ransomware.

Supply chain compromises have several characteristics that distinguish them from conventional cyber compromise. One characteristic is that **supply chain compromises are indirect**. By first compromising a supplier and subsequently exploiting their trusted relationships with downstream organizations, threat actors can entirely circumvent those organizations' cyber network perimeter, thus avoiding the need for direct action against a target network's defences. These compromises can be difficult to detect and attribute because they often originate from a legitimate product or service from a trusted supplier. Because of this, a supply chain's cyber security is only as strong as the weakest link.

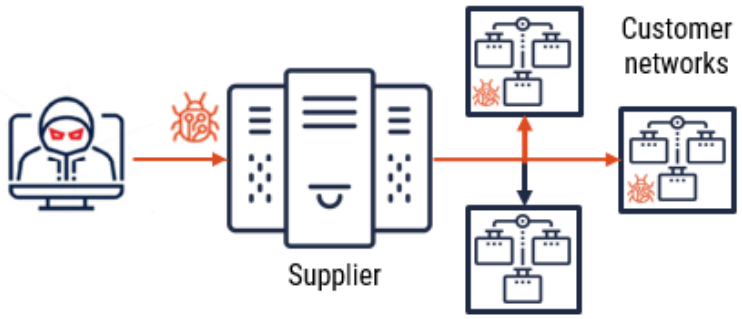


Figure 1: Threat movement through the supply chain

By compromising a supplier, threat actors can use their trusted relationships to facilitate further compromises against downstream organizations. These further compromises can be targeted or indiscriminate.

Alternatively, threat actors may be able to achieve their objectives without ever pivoting to a downstream network. Depending on the industry, suppliers may possess information of value to threat actors. This is particularly true for industrial organizations such as utilities in the critical infrastructure sector, explained further in the below text box. In early 2021, Quanta Computer, a Taiwanese technology manufacturer and Apple partner, was compromised by the REvil ransomware group. Quanta's systems were encrypted and sensitive data including "…large quantities of confidential drawings and gigabytes of personal data with several major brands" was exfiltrated. In addition to demanding ransom to decrypt the affected systems, REvil also attempted to extort Apple for ransom to prevent the stolen schematics and data from being leaked.[2]

Valuable information within CI supply chains

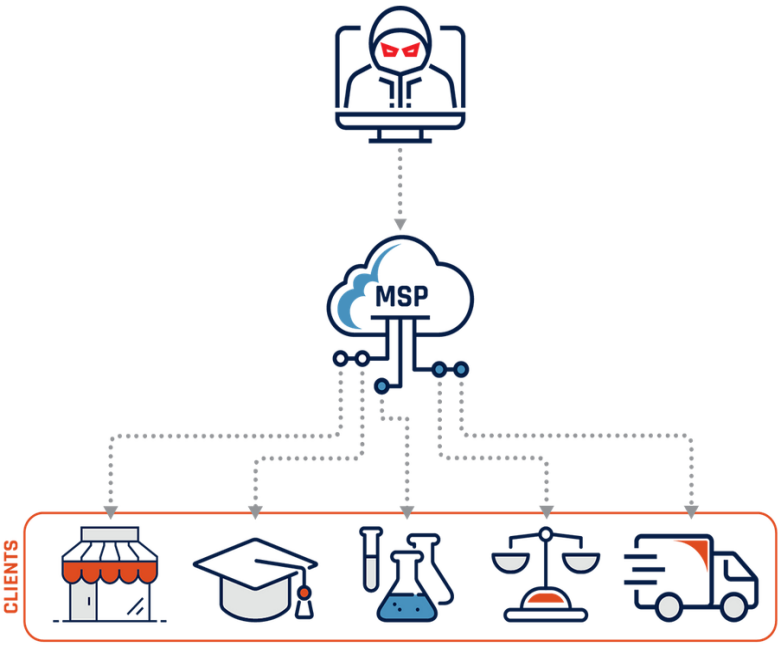
Industrial organizations, such as utilities in the critical infrastructure sector are highly dependent on industry support organizations for their daily functioning. Industry support organizations include private sector professional engineering and consulting services contracted by critical service providers in the development and management of infrastructure assets, as well as vendors that provide technologies, services, and supplies.[3] A compromise against critical infrastructure supply chains may result in disruption or degradation of services or the exfiltration of design documents or schematics that will provide an advantage for further attempts to compromise the critical infrastructure provider's networks and systems.

Another characteristic of supply chain compromises for threat actors is scalability. Suppliers often serve many organizations with products or services. Some organizations, such as **managed service providers (MSPs), have enhanced access to the networks of many different clients**, allowing threat actors to affect multiple targets through a single compromise with the network privileges afforded to the MSP, as illustrated in Figure 2.

Supply chains provide an opportunity for threat actors to maximize their value from exploiting zero-day vulnerabilities. A zero-day vulnerability is one that was unknown to the developer before it was detected as a means of compromise. With no patch available to address the vulnerability, zero-day attacks have a high likelihood of success and developers then have "zero days" to implement a patch. Once a zero-day has been detected and a fix implemented, it can no longer be used against patched systems.

Instead of potentially "burning" that asset to compromise a single network, it may be used against a supplier higher in the supply chain to facilitate access to many downstream networks. The 2021 Kaseya VSA compromise by REvil used several zero-day vulnerabilities, including CVE-2021-30116[4] and CVE-2021-30120,[5] which allowed them to bypass authentication requirements to access VSA servers en route to deploying ransomware in up to 1500 downstream client networks. [6]

Figure 2: Exploitation of managed service providers



By targeting MSPs, threat actors can gain access to the MSP's clients (including businesses, universities, and other institutions) without having to compromise each client directly.

We assess it likely that zero-day vulnerabilities will continue to be used in supply chain compromises by sophisticated threat actors, allowing them to bypass security controls, avoid detection, and make the most efficient use of the valuable exploits. However, the use of zero-day exploits in supply chain compromises will be restricted by their rarity and the high cost of developing or acquiring them.

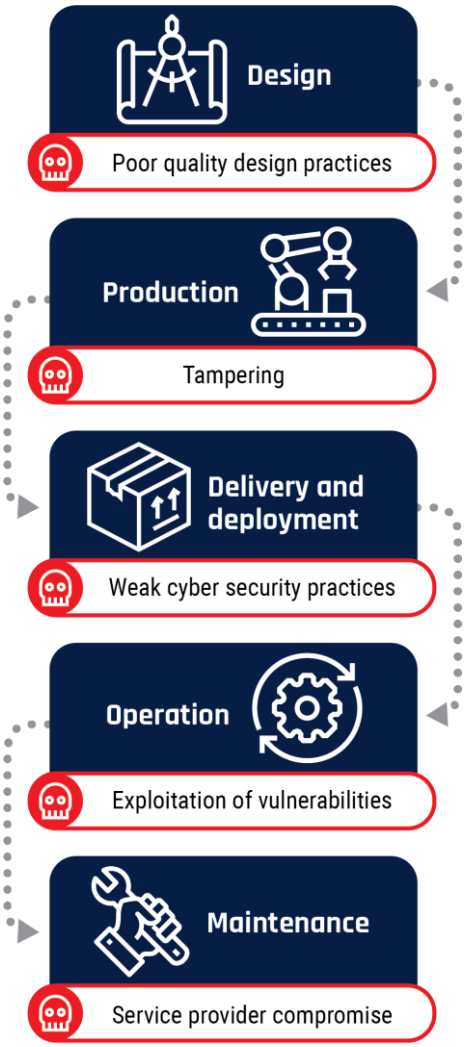
Types of supply chain compromises

We assess it very likely that software will continue to be the primary vector for cyber threat movement in supply chains and assess it very unlikely that hardware trojans and hardware supply chain compromises will become a significant threat vector within supply chains in the near term. Software supply chain compromises alter a supplier's software or otherwise leverage a supplier's trusted relationships to introduce a vulnerability or deploy malware on their ultimate target, the purchaser or user of the software.[7]

As illustrated in Figure 3, threat actors may impact the supply chain at any stage in a product or service's lifecycle. The most observed methods of software supply chain compromises include open-source components, hijacked code signing, and compromised updates. This is a non-exhaustive list of vulnerabilities and methods – the techniques for threat actors to propagate through supply chains are only limited by their ability to exploit the trusted relationship between organizations and their vendors or suppliers.

Note that the exploitation of common software vulnerabilities discovered organically during the life cycle of the software, such as the Microsoft Exchange[8] or Log4Shell[9] vulnerabilities, do not constitute supply chain compromises as they do not stem from a threat actor's activity higher in the supply chain.

Figure 3: Supply chain vulnerabilities



Open-source software components

Software development increasingly includes the use of open-source software components to decrease development times and support innovation.[10] Open-source software components are publicly available packages of code or software maintained by collaborative communities of developers in support of a larger marketplace of ideas.[11] Common methods of compromise include typo squatting, malicious code injection, and dependency confusion, described in more detail in Table 1 below.

On March 9, 2020, GitHub—a website that hosts and facilitates code sharing—was notified that malware was being served by several repositories hosted on their platform. When a user downloaded a project from one of those repositories, they would also download malware that would scan their system for the Java-based development environment NetBeans and, if discovered, would install a malware dropper that downloaded a remote access trojan.[12] The repository owners were unaware of this activity, and it appears that the repositories had been infected as early as 2018. In total, GitHub found 26 repositories that had been infected with this malware, dubbed Octopus Scanner.[13]

Table 1: Common open-source software compromises

Typosquatting:	The hosting (for example, on GitHub) of a malicious component named similarly to a legitimate project, often with one letter mistyped or other typing mistakes a developer could easily make in trying to load the component into their development project.
Malicious Code Injection:	The implanting of malicious code into a legitimate open-source component by any means that will run when the component is called.
Dependency Confusion:	A targeted attack by which threat actors identify proprietary software dependencies and upload malicious components by the same name to a public repository. When expecting to call the proprietary dependency, the software may unintentionally load the publicly available malicious component.

Undermining code signing

Code signing is a method of validating the authenticity and integrity of executables and scripts (i.e., code). If a threat actor alters code while maintaining the integrity of the signature, the recipient will unknowingly incorporate the malicious additions to their code. This can be done by compromising a certificate authority (i.e., the source of the trusted certificate), or acquiring the private keys of a legitimate developer. Private keys may be stolen or unintentionally disclosed by the author. Alternatively, if the code is signed with weak cryptography, a threat actor may be able to break the encryption and forge the signature.

In January of 2019, a cyber security company discovered that the ASUS Live Update Utility had been used to install malware on an estimated 500,000 computers.[14] The compromise, dubbed Operation ShadowHammer, had been in progress since at least mid-2018. Part of the reason the compromises persisted for so long was that the malicious files still had a valid digital signature. Typically, any changing of the files would break the signature and flag that alterations had been made. However, the threat actors were able to compromise the digital signature itself and reapply it to the files after making the malicious alterations. Although the compromised files were downloaded widely, the malware was designed to identify and only conduct follow-on activities for specific targets.[15]

Hijacked updates

A distinguishing feature of the software supply chain is that software is supported after its release by updates from the developer to address bugs and security issues or add functionality. Updates from software vendors are trusted and often installed by users without any view to the underlying code or its relative integrity. Hijacked updates include malicious code inserted by threat actors to be distributed through official, trusted update channels. Updates are afforded the same level of privilege as the software it is applied to, which can be considerable especially if it is a security related application, allowing malicious code to avoid some security measures and to possibly gain permission to modify key system files.

Operation ShadowHammer is also an example of a compromise involving hijacked updates, as the compromised update was distributed directly through the real ASUS Live Update Utility to users. Another example of a compromise through hijacked updates came from the popular utility software, CCleaner. CCleaner is software that allows users to remove unwanted files and programs from their systems. Threat actors leveraged access to a Piriform developer account to update the CCCleaner installer to include malware. Users who updated or downloaded CCleaner through the official website during August and September of 2017 received maliciously altered versions of the software. Avast was notified by security researchers of the issue on September 13, 2017, and with the assistance of the FBI, the threat actor's command-and-control systems were disabled. By that time, the malicious version of CCleaner had been downloaded by 2.27 million users.[16] Despite the high number of infected downloads, only approximately 40 machines were targeted by the second stage malware; just 11 of those machines were subject to further targeted exploitation by the threat actor.[17]

Threat from hardware and physical products

We assess that hardware trojans and hardware supply chain compromises are very unlikely to become a significant threat vector within supply chains in the near term. Hardware supply chain compromises refer to the malicious addition or alteration of components with the intention of creating a backdoor or nascent vulnerability to be exploited when the hardware has been deployed by the purchaser. That vulnerability may later be used to install a rootkit or remote system access, exfiltrate data, or degrade or destroy the equipment on remote command.

While physical products have been observed as an infection vector through supply chains, they are typically used as vehicles for software-based threats. For example, Schneider Electric issued a security notification in 2018 regarding removable USB media devices that had been shipped packaged with other products. Schneider became aware that the removable media devices had been contaminated with malware during manufacturing by one of their suppliers, and while the malware should have been detected and neutralized by most anti-malware programs, they recommended that they be discarded.[18] Although the vulnerability was transported by hardware, it was software in nature. Hardware trojans could hypothetically provide sophisticated threat actors a means to systemically introduce hard-to-detect vulnerabilities into products or components, but this has yet to be observed.

Threat actors

The threat from state-sponsored actors

We assess that state-sponsored threat actors will almost certainly continue to use supply chains to compromise targets of strategic interest, and that they will almost certainly continue to develop persistence within supply chains to facilitate the ongoing theft of valuable information.

State-sponsored threat actors have additional tools available to them to achieve their objectives through supply chains. Instead of clandestinely compromising a supplier, they may have the ability to legally compel the co-operation of vendors operating under their jurisdiction with military or intelligence activities. This could include compelling the production of customer data, or of application source code which would allow them to exploit applications more effectively in target environments in future operations. One such program is Russia's lawful access program, the System of Operative Investigative Activities (SORM). SORM is directly administered by the Federal Security Service (FSB) and lacks effective assurances against arbitrariness and abuse.[19] SORM and Russia's data localization laws provide the FSB and other law enforcement and intelligence agencies abundant opportunity to compel sensitive information from organizations operating in Russia.[20] We assess it very likely that adversary states can influence their domestic vendors to compromise products to advance their national interest, counter to Canadian clients' interests, and the interests of Canada.

In addition to leveraging supply chain compromise technique such as compromised-updates,[21] state-sponsored threat actors have demonstrated their ability to compromise service providers such as MSPs as a method of infiltrating the supply chain of organizations of strategic interest, establishing persistence, and securing access to downstream targets. Establishing persistence within a service provider's networks allows for opportunistic yet selective development of strategic targets. The SolarWinds Orion compromise is an example of such a campaign, with evidence that the early stages began almost a year prior to its discovery in December of 2020, and malware having been deployed for months before it was detected.[22]

Case study: SolarWinds Orion

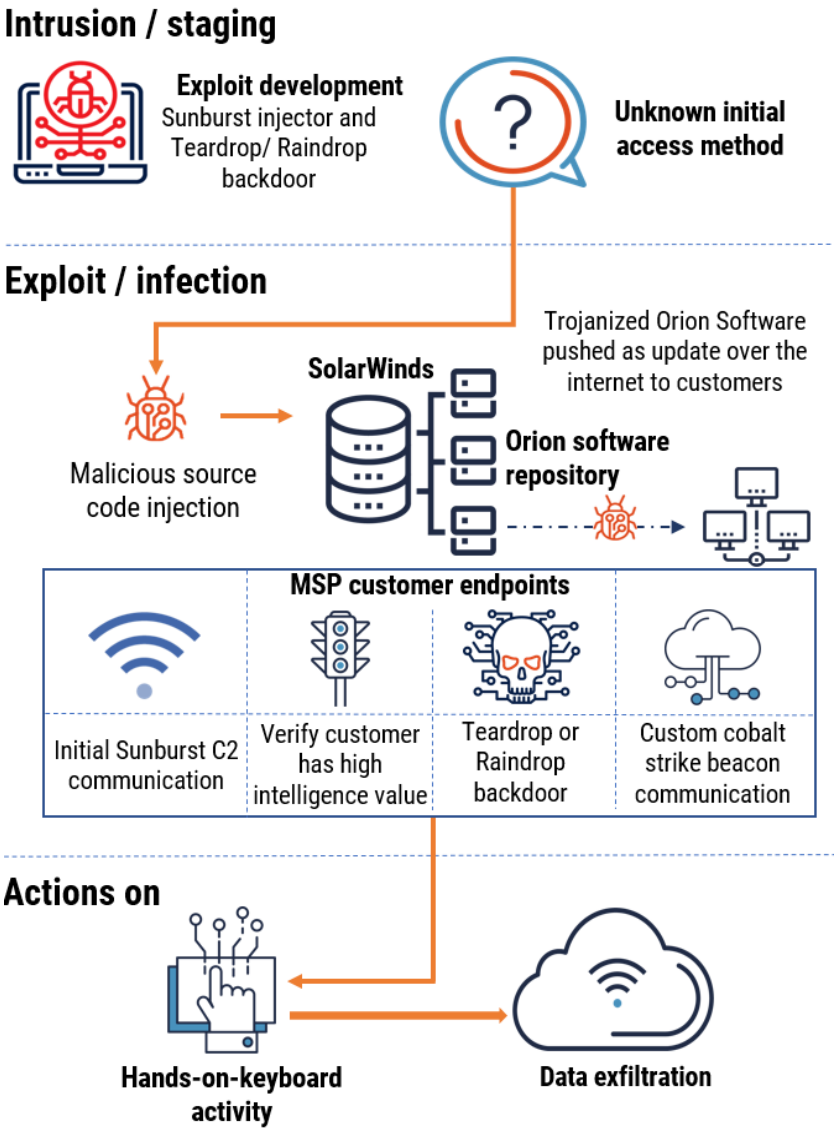
SolarWinds is a software company and MSP that came to public attention in late 2020 when cyber security firm FireEye discovered that a threat actor had obtained access to their systems via a compromised update from SolarWinds Orion – a software-as-a-service (SaaS) environment that businesses use to centralize the monitoring and control of their networks, and which was used heavily by industry and government organizations in North America, Europe, Asia, and the Middle East.[23]

Canada and its partners later formally named the Russian Foreign Intelligence Service (SVR), otherwise known as APT 29 or Cozy Bear, as the actor responsible for the compromise.[24]

Orion is a platform that runs on the customer's own networks rather than being hosted on SolarWinds servers. This means that customers must regularly download software updates from SolarWinds to apply the most recent bug and security patches. Such updates are signed by the publisher to certify that the contents are genuine and allows the recipient to verify that the contents are unmodified.[25]

Figure 4 illustrates the "Kill Chain",[26] or sequence of actions taken by the threat actor over the course of the compromise. The threat actor inserted malicious software into Solarwinds' development environment, infecting Orion's source code with the SUNBURST malware. The compromised build was pushed to customers as an update to their existing Orion installations, deploying SUNBURST into customer environments. SUNBURST then communicated with the threat actors, who would verify that the accessed environment had information of value worth exfiltrating. If further actions were taken, TEARDROP or RAINDROP backdoors would be deployed, which would install a customized Cobalt Strike beacon in the environment, enumerating the domain and allowing for the collection and exfiltration of information of value using hands-on-keyboard techniques.

Figure 4: SolarWinds Orion kill chain analysis



The compromise made upwards of 18,000 of the approximately 300,000 SolarWinds customers vulnerable, with at least 200 identified organizations that had been subject to targeted follow-on activities.[27] Impacted organizations included industry leaders such as Microsoft, where hackers were able to view some of its source code,[28] as well as United States government departments including the Justice Department, the State Department, and the National Nuclear Security Administration.[29]

While it appears that some Canadian organizations may have downloaded the compromised versions of SolarWinds Orion, it does not appear that any Canadian organizations were subject to follow-on exploitation activity by the threat actor. The consequences of the compromise are still being determined, though estimates place the cost to organizations around the world in the hundreds of billions – not including the cost of any intellectual property theft.[30] Microsoft has also attributed ongoing compromises by this same state actor, almost certainly the Russian Foreign Intelligence Service (SVR), against cloud service providers, MSPs, and other parts of the technology supply chain to the group, claiming that they have targeted up to 609 organizations with a total of 22,868 attacks.[31]

The threat from criminal actors

We assess criminal actors, especially ransomware operators, are likely to continue targeting supply chains to maximize the number of potential victims and profits per compromise.[32] Criminal threat actors are financially motivated with very few exceptions, either seeking to exfiltrate commercially valuable information for sale, extorting victims through the deployment of ransomware, or deploying cryptojackers, malware that "mines" cryptocurrency using the resources of an infected device.[33]

Criminal supply chain compromises are particularly concerning given the lack of discrimination in their targeting. Supply chain compromises have the potential to expose a wide cross-section of organizations to business disruptions, including elements of critical infrastructure including schools, hospitals, utilities, and other typical "Big Game Hunting" targets as described in the textbox below. While some criminal threat actors have indicated they would not target certain sectors, other criminal groups have fewer scruples, specifically attacking targets such as hospitals that cannot tolerate sustained service disruptions and have the financial resources to pay large ransom demands.[34]

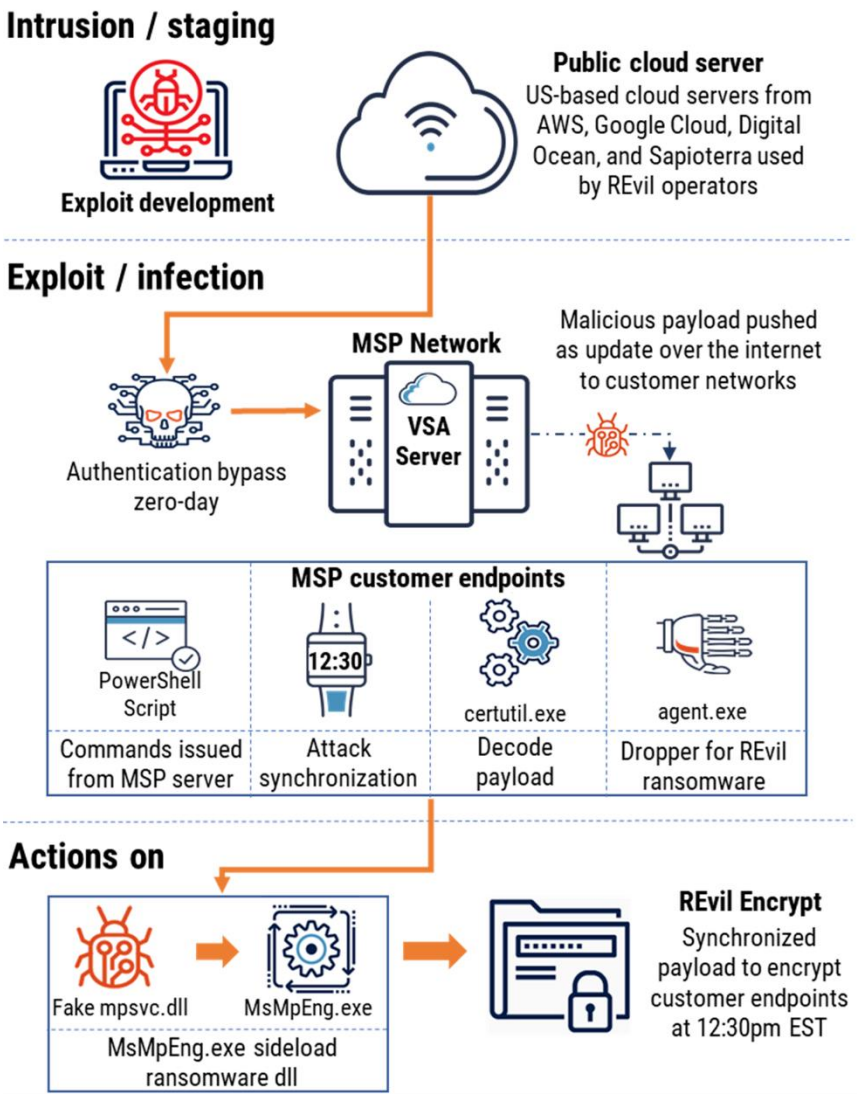
Open-source software component compromises have been a common tool for criminal threat actors as well, providing a low-barrier-to-entry method of widely propagating a vulnerability or malicious addition to software. In May of 2021, cyber security vendor Palo Alto published the results of their investigation into malicious software hosted on the popular developer community site, Docker Hub. Palo Alto identified 30 malicious files that were typosquatting popular downloads. The malicious files contained cryptojackers[35] and had been downloaded over 20 million times, generating an estimated $200,000 USD in revenue before they were removed.[36]

Case study: Kaseya VSA

On July 2, 2021, the Friday leading up to the US Independence Day long weekend, Kaseya issued a warning indicating that their incident response team was investigating a possible compromise involving their Virtual System Administrator (VSA) service.[37] Kaseya VSA had been compromised by REvil, otherwise known as Sodinokibi, a Russian Ransomware-as-a-Service group. A VSA is a system through which MSPs administer their client's networks. As an administrative tool, the VSA requires administrative privileges within a customer's networks to function. REvil compromised vulnerable MSP-hosted VSA servers by leveraging several zero-day exploits.

Figure 5 illustrates the Kaseya VSA compromise's kill chain. The threat actor either developed or purchased custom exploits to take advantage of zero-day vulnerabilities discovered in the Kaseya VSA software. They gained initial access to MSPs'

Figure 5: Kaseya VSA kill chain analysis



environments through an authentication zero-day exploit, followed by exploitation of inclusion zero-days to upload malware and run malicious code. The payload was then distributed to the MSPs' clients through a compromised update posing as a hotfix. After waiting until a specified time, the ransomware payload was deployed across customer environments all at once, encrypting data and locking systems.

The Kaseya VSA compromise affected not just the MSPs who use the Kaseya software, but each MSPs' clients as well. The compromise infected approximately 60 MSPs, and in turn up to 1500 downstream clients from across North America, Europe, Australia, and New Zealand. Affected downstream organizations range from New Zealand public schools to Swedish retail pharmacies.[38]

REvil placed a $70 million USD price tag on a universal decryptor through their unlisted website, the "Happy Blog", where they post ransom demands and publish or auction victim data.[39] The use of the zero-days, the sophistication of the attack, and the large number of affected organizations sets the Kaseya compromise apart from previous ransomware attacks by cybercriminals.

Conclusion

With supply chains becoming more digital and globally distributed, there is increased opportunity for threat actors to identify weaknesses and exploit trust between organizations. The potential for threat activity from supply chains must be managed throughout the product or service's lifecycle from design and production through to deployment and decommissioning. Organizations should maintain a robust supply chain integrity program and ensure that their suppliers are adhering to supply chain integrity and security best practices. In this assessment, we identified why supply chains are appealing targets for threat actors and described the most commonly observed techniques for supply chain compromise. We also identified the motivations and relative capacity for state-sponsored and criminal threat actors for compromising supply chains.

Many cyber threats can be mitigated through awareness and best practices in cyber security and business continuity. Cyber threats continue to succeed today because they exploit deeply rooted human behaviours and social patterns, and not merely technological vulnerabilities. Defending Canada against cyber threats and related influence operations requires addressing both the technical and social elements of cyber threat activity. Cyber security investments will allow Canadians to benefit from new technologies while ensuring that we do not unduly risk our safety, privacy, economic prosperity, and national security.

The Cyber Centre is dedicated to advancing cyber security and increasing the confidence of Canadians in the systems they rely on daily, offering support to CI and other systems of importance to Canada. We approach security through collaboration, combining expertise from government, industry, and academia. Working together, we can increase Canada's resilience against cyber threats.

Please refer to the following on-line resources for more information and for useful advice and guidance:

Threat detection and mitigation:

- Cyber supply chain: An approach to assessing risk – ITSAP.10.070
- IT security risk management: A lifecycle approach (ITSG-33)
- Baseline cyber security controls for small and medium organizations
- Protecting your organization from software supply chain threats – ITSM.10.071
- Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. National Institute for Standards and Technology. 2022
- Risk management framework for information systems and organizations: A system life cycle approach for security and privacy (SP 800-37 Rev, 2). National Institute for Standards and Technology. 2018
- Best practices in cyber supply chain risk management. National Institute for Standards and Technology. 2021

- Security and resilience – Security management systems (ISO 28000:2022). International Standards Organization. 2022
- Cyber security – Supplier relationships (ISO 27036:2021). International Standards Organization. 2021

Threat assessment:

- National cyber threat assessment 2023-2024
- Cyber threat bulletin: The cyber threat to operational technology
- Cyber threat bulletin: The ransomware threat in 2021

Planning:

- Fundamentals of Cyber Security for Canada's CI Community. Public Safety Canada
- Ransomware playbook (ITSM.00.099)

ENDNOTES

[1] Joe Boyens, Angela Smith, Nadya Bartol, Kris Winkler, Alex Holbrook, and Matthew Fallon. "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (NIST SP 800-161r1)." National Institute of Standards and Technology. May 2022.

[2] Sergio Gatlan. "REvil gang tries to extort Apple, threatens to sell stolen blueprints." Bleeping Computer. April 20, 2021.

[3] Canadian Centre for Cyber Security. "Cyber Threat Bulletin: The Cyber Threat to Operational Technology." June 29, 2021. p. 9.

[4] NIST. "CVE-2021-30116 Detail." March 25, 2022.

[5] NIST. "CVE-2021-30120 Detail." March 1, 2022.

[6] Alexander Andersson. "How the Kaseya VSA Zero-Day Exploit Worked." TrueSec. July 6, 2021; Doug Olenick. "List of Victims of Kaseya Ransomware Attack Grows." Bank Info Security. July 8, 2021.

[7] Charles Clancy, Joe Ferraro, Robert A. Martin, Adam G. Pennington, Cristopher L. Sledjeski, and Craig J. Wiener. "Deliver Uncompromised, Securing Critical Software Supply Chains." The MITRE Corporation. January 2021. p. 1; ODNI. "Software Supply Chain Attack Graphic." 2017.

[8] Canadian Centre for Cyber Security. "Alerts - Active Exploitation of Microsoft Exchange Vulnerabilities." March 2, 2021.

[9] Canadian Centre for Cyber Security. "Alerts – Active Exploitation of Apache Log4j Vulnerability." December 10, 2021.

[10] Trey Herr, William Loomis, Stewart Scott, June Lee. "Breaking Trust: Shades of Crisis Across an Insecure Software Supply Chain." Atlantic Council. July 2020. p. 20.

[11] Michael Ayukawa, Mohammed Al-Sanabani, and Adefemi Debo-Omidokun. "How Firms Relate to Open Source Communities." Technology Innovation Management Review. January 2011; J.V. Joshua, D.O. Alao, S.O. Okolie, and O. Awodele. "Software Ecosystem: Features, Benefits and Challenges." International Journal of Advanced Computer Science and Applications (4:8). 2013. p. 242-247.

[12] Tara Seals. "Octopus Scanner Sinks Tentacles into GitHub Repositories." ThreatPost. June 2, 2020.

[13] Alvaro Munoz. "The Octopus Scanner Malware: Attacking the open source supply chain." GitHub Security Lab. May 28, 2020.

[14] Kim Zetter. "Hackers Hijacked ASUS Software Updates to Install Backdoors on Thousands of Computers." Vice. March 25, 2019.

[15] SecureList. "Operation ShadowHammer: a high-profile supply chain attack." April 23, 2019.

[16] Swati Khandelwal. "CCleaner Attack Timeline – Here's How Hackers Infected 2.3 Million PCs." The Hacker News. April 18, 2018.

[17] Lily Hay Newman. "Inside the Unnerving Supply Chain Attack that Corrupted CCleaner." Wired. April 17, 2018.

[18] Schneider Electric. "Security Notification – USB Removable Media Provided with Conext Combox and Conext Battery Monitor." August 24, 2018.

[19] *Roman Zakharov v Russia [GC]*. European Court of Human Rights Judgement 4.12.2015 [GC]. December 25, 2015.

[20] Justin Sherman. "Reassessing RuNet: Russian internet isolation and implications for Russian cyber behaviour." Atlantic Council. July 12, 2021.

[21] John Speed Meyers. "A Recent Chinese Hack Is a Wake-up Call for the Security of the World's Software Supply Chain". The Diplomat. September 7, 2022.

[22] Robert Chesney. "Cybersecurity Law, Policy, and Institutions (Public Law Research Paper No. 716)." University of Texas. August 23, 2021. p. 6.

[23] Kevin Mandia. "Global Intrusion Campaign Leverages Software Supply Chain Compromise." FireEye Stories Blog. December 13, 2020.

[24] White House Briefing Room. "FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government." April 15, 2021; GAC. "Statement on SolarWinds Cyber Compromise." April 15, 2021.

[25] Robert Chesney. "Cybersecurity Law, Policy, and Institutions (Public Law Research Paper No. 716)." University of Texas. August 23, 2021. p. 4-6.

[26] Lockheed Martin. "Gaining the Advantage: Apply Cyber Kill Chain Methodology to Network Defences." 2015.

[27] William Turton. "List of Hacked Organizations Tops 200 in SolarWinds Case." Government Technology. December 21, 2020.

[28] Nicole Perlroth. "Microsoft Says Russian Hackers Viewed Some of its Source Code." The New York Times. December 31, 2020.

[29] Isabella Jibilian and Katie Canales. "The US is readying sanctions against Russia over the SolarWinds cyber attack. Here's a simple explanation of how the massive hack happened and why it's such a big deal." Business Insider. April 15, 2021.

[30] Ryan Gallagher. "SolarWinds Adviser Warned of Lax Security Years Before Hack." Bloomberg. December 21, 2020; Gopal Ratnam. "Cleaning up SolarWinds hack may cost as much as $100 billion." Roll Call. January 11, 2021.

[31] Ravie Lakshmanan. "Microsoft Warns of Continued Supply-Chain Attacks by the Nobelium Hacker Group." The Hacker News. October 25, 2021.

[32] Canadian Centre for Cyber Security. "Cyber threat bulletin: the ransomware threat in 2021." December 9, 2021.

[33] Jay Chen. "Graboid: First-Ever Cryptojacking Worm Found in Images on Docker Hub." PaloAlto. October 16, 2019.

[34] Ellen Nakashima and Jay Greene. "Hospitals being hit in coordinated, targeted ransomware attack from Russian-speaking criminals." The Washington Post. October 29, 2020.

[35] Canadian Centre for Cyber Security. "National Cyber Threat Assessment 2020." 2020. p. 17.; Interpol. "Cryptojacking." September 2020.

[36] Aviv Sasson. "20 million miners: finding malicious cryptojacking images in docker hub." PaloAlto. March 26, 2021.

[37] Kaseya. "Important Notice." August 4, 2021.

[38] Malwarebytes Labs. "Kaseya hijacked, thousands attacked by REvil, fix delayed again." July 7, 2021.

[39] Ionut Ilascu. "REvil ransomware asks $70 million to decrypt all Kaseya attack victims." Bleeping Computer. July 5, 2021; Scott Ikeda. "Revil Ransomware Group Missing from Dark Web; Temporary Vacation, or Permanently Out of Business?." CPO Magazine. July 16, 2021.

CAT. D96-93/2022E-PDF
ISBN 978-0-660-46246-2