CRITICALSTART

Cyber Threat Intelligence Summary

November 22, 2021

In the spotlight: Supply Chain Attacks – A Continuing Trend

Supply chain attacks have been at the forefront of security practitioners concern for a number of years due to the potential ripple effect created by a single attack. Although the supply chain has always been a high-value target for cyber criminals, the industry has been facing a greater number of highly sophisticated and organized attacks since early 2020. A cyber incident at any organization participating in the global supply chain could further disrupt an already vulnerable supply chain at an already vulnerable time of year.

Most Active Source Countries	Russia, China, Iran
Tactics, Techniques, & Procedures	Hijacking Updates, Undermining Code Signing

The Breakdown

The security concerns for the organizations that make up the global supply chain have been high priority for a number of years, but in the last 12 to 24 months, the threats against this complex and fragile system have intensified. This industry has been targeted by a higher level of organization from Advances Persistent Threat Groups or APT. Cyber risks to the supply chain include vendor sourcing and management, logistical continuity and quality mechanisms, as well as transportation security and many other facets across the vertical. A supply chain attack is a combination of at least two attacks. The first attack is on a supplier that is then used to attack the target to gain access to its assets. The target can be the final customer or another supplier. Therefore, for an attack to be classified as a supply chain one, both the supplier and the customer have to be targets.

As a whole, more robust security protections have been implemented at the organizational level, likely shifting the focus to industry suppliers, but the sophistication of the attacks impact system downtime, monetary losses and reputational damage. Targeting of supply chains is attributed to the fact that there is a large downstream ripple effect from the affected supplier impacting hundreds to thousands of customers in its wake. This cascade from a single attack is widely propagated thus the target becomes more valuable.

Supply chain refers to the ecosystem of processes, people, organizations, and distributors involved in the creation and delivery of a final solution or product. In cybersecurity, the supply chain involves a wide range of resources (hardware and software), storage (cloud or local), distribution mechanisms (web applications, online stores), and management software. Supply chain attacks have both increased in number and sophistication in the year 2020 and this trend is continuing in 2021, posing an increasing risk for organizations.[1] Current estimates are around four-fold for the increase in supply chain attacks in 2022 than in 2021. With half of the attacks being attributed to Advanced Persistence Threat (APT) actors, their complexity and resources greatly exceed the more common nontargeted attacks, and, therefore, there is an increasing need for new protective methods that incorporate suppliers in order to guarantee that organizations remain secure.

[1] https://www.cyberpion.com/resource-center/blogs/types-of-supply-chain-attacks/

So what?

Composed of an attack on one or more suppliers with a later attack on the final target, namely the customer, supply chain attacks may take months to succeed. Similarly, Advanced Persistence Threat (APT) attacks, supply chain attacks are usually targeted, quite complex and costly with attackers probably planning them well in advance. All such aspects reveal the degree of sophistication of the adversaries and the persistence in seeking to succeed and with the almost limitless potential of the impact of supply chain attacks on numerous customers, these types of attacks are becoming increasingly common.

In order to compromise the targeted customers, attackers focused on the suppliers' code in about 66% of the reported incidents. This highlights the importance of validating third-party code and software before using them to ensure they were not tampered with or manipulated. For about 58% of the supply chain incidents in 2020, the customer assets targeted were predominantly customer data, including Personally Identifiable Information (PII) data and intellectual property and a further 66% of the supply chain attacks in that period, suppliers did not know, or failed to report on how they were compromised.

The impact of attacks on suppliers may have far reaching consequences because of the increased interdependencies and complexities of the techniques used. Beyond the damages on affected organizations and third parties, there is a deeper cause for concern when classified information is exfiltrated and national security is at stake or when consequences of a geopolitical nature could emerge as a result.

The seriousness of a supply chain attack was demonstrated in December of 2020, when Russian state actors hacked the software firm SolarWinds and placed malicious code in Orion, its IT management tool—allowing access to an estimated 18,000 networks that used the application worldwide.[2] The Russian foreign intelligence service (SVR) used that access to dig deep into the networks of at least nine US federal agencies. These agencies include the State Department, the US Treasury, the Department of Defense, Homeland Security, and NASA.[3]

What's next?

In this complex environment for supply chains, establishing good practices and getting involved in coordinated actions at the industry and federal level are both important to support all organizations in developing security capabilities – to reach a common level of security.[4][5]

The answer to both software and hardware supply chain attacks may be more organizational and less technical. Governments and companies need to know who supplies software and hardware, vet them, and hold them to a specific set of standards. The list below details a few recommendations for both customers and suppliers:

[2] https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack
[3] https://www.fedscoop.com/solarwinds-recap-federal-agencies-caught-orion-breach/
[4] https://www.wired.com/story/hacker-lexicon-what-is-a-supply-chain-attack/
[5] https://www.cnbc.com/2018/10/04/chinese-spy-chips-are-said-to-be-found-in-hardware-used-by-apple-amazon-apple-denies-the-bloomberg-businessweek-report.html

Recommendations for customers include:

- Identify and document all suppliers and service providers and ensure role based access control is implemented universally.
- Define risk criteria for different types of suppliers and services such as supplier & customer dependencies, critical software dependencies, single points of failure.
- Monitor supply chain risks and threats.
- Manage suppliers over the whole lifecycle of a product or service, including procedures to handle end-of-life products or components.
- Classify critical and non-critical assets and information shared with or accessible to suppliers, and defining relevant procedures for accessing and handling them.

There are also several recommended actions to ensure that the development of products and services complies with security practices. Suppliers are advised to implement good practices for vulnerability and patch management for instance. [6]

Recommendations for suppliers include:

- Ensure the infrastructure used to design, develop, manufacture, and deliver products, components and services follows cybersecurity practices.
- Implement a product development, maintenance and support process that is consistent with commonly accepted product development processes.
- Monitor security vulnerabilities reported by internal and external sources that includes used third-party components, specifically those related to CISA and other federal agency guidelines.
- Maintain an inventory of assets that includes patch-relevant information.

Services at scale rely on supply chain applications to provide the necessary services to businesses. However, that trust may reduce the complexity of operations, but it will increase the overall risk. Companies can mitigate the impact of supply chain attacks by controlling third-party connections. There are tactics and tools designed to detect malicious code and deny access to threat actors. By ensuring that infrastructure that does not need a connection to the internet is disconnected, you can provide a significant barrier to successful attacks.

Sources	The information in this article is derived from threatpost.com, checkpoint.com, cloudflare.com, information-age.com, zdnet.com, cisa.gov and securitymagazine.com.
Source reliability	**B (Usually reliable)** Minor doubts; history of mostly valid information
Information reliability	**2 (Probably true)** Logical, consistent with other relevant information; not confirmed

[6] https://www.automotivelogistics.media/supply-chain-management/toyota-doesnt-let-a-good-crisis-go-to-waste/41525.article

Weekly highlights in brief

Emotet Stages a Comeback

Researchers from a number of cybersecurity companies have warned that Emotet has returned. Another malware botnet, TrickBot is being used to install Emotet on infected Windows systems. Currently, Emotet isn't attempting to redistribute itself, instead relying on TrickBot to spread new infections. However, this does indicate that those behind Emotet are trying to get the botnet up and running again.

Zoom Patches High-Risk Flaws in Meeting Connector, Keybase Client

The Keybase Client for Windows before version 5.7.0 contains a path traversal vulnerability when checking the name of a file uploaded to a team folder. A malicious user could upload a file to a shared folder with a specially crafted file name which could allow a user to execute an application which was not intended on their host machine. If a malicious user leveraged this issue with the public folder sharing feature of the Keybase client, this could lead to remote code execution.

Keybase addressed this issue in the 5.7.0 Keybase Client for Windows release. Users can help keep themselves secure by applying current updates or downloading the latest Keybase software with all current security updates from https://keybase.io/download.[7]

Chrome 96 Plugs High-Risk Browser Flaws

Of the externally reported security flaws, seven are rated "high severity." Google described the high-risk bugs as use-after-free issues in components such as media, storage foundation, and loader. A total of ten medium severity bugs were patched in Chrome this week, including a Type Confusion in V8, a heap buffer overflow in fingerprint recognition, an out of bounds write in Swiftshader, inappropriate implementations in input, navigation, and referrer, and insufficient policy enforcements in background fetch, iframe sandbox, CORS, and contacts picker. Google also patched an inappropriate implementation in WebAuthentication, which is considered low severity.[8]

[7] https://explore.zoom.us/en/trust/security/security-bulletin/

[8] https://chromereleases.googleblog.com/2021/11/stable-channel-update-for-desktop.html

CRITICALSTART

Cyber Threat Intelligence Summary

November 22, 2021

Language of Uncertainty

Throughout this intelligence summary and all Critical Start Cyber Threat Intelligence publications, Critical Start assesses probability using qualitative statements from a defined matrix, known as "Expressions of Likelihood," where terms of likelihood are aligned with terms of probability and percentages of chance. To give the reader perspective, each of these statements is associated with a probability range listed in the table below.

Terms of Likelihood	Terms of Probability	Associated Percentages of Chance
Almost No/Near Zero Chance	Remote or Highly Unlikely	<1-5%
Improbable or Very Unlikely	Highly Improbable or Very Unlikely	5–20%
Unlikely	Improbable/Improbably	20-45%
Roughly Even Chance	Realistic Possibility/Even Odds	45–55%
Probable or Likely	Probable/Probably	55–80%
Highly/Very probable/likely	Highly/Very Probable/Likely	80–95%
Almost certain(ly)	Almost/Nearly Certain	>95-99%

Source evaluation

Critical Start evaluates sources by scoring both the reliability of sources and the accuracy and validity of the information gathered from them.

	Source	Description
A	Reliable	Limited doubt about the source's authenticity, trustworthiness, or competency; history of reliability
B	Typically reliable	Minor doubts; history of mostly valid information
C	Fairly reliable	Doubts; provided valid information in the past
D	Not usually reliable	Significant doubts; provided valid information in the past
E	Unreliable	Lacks authenticity, trustworthiness, and competency; history of invalid information
F	Cannot be judged	Insufficient information to evaluate reliability; may or may not be reliable

	Information	Description
1	Confirmed	Logical, consistent with other relevant information, corroborated by independent sources
2	Probably true	Logical, consistent with other relevant information, not confirmed
3	Possibly true	Reasonably logical, agrees with some relevant information, not confirmed
4	Doubtfully true	Not logical but possible, no other information on the subject, not confirmed
5	Improbable	Not logical, contradicted by other relevant information
6	Cannot be judged	The validity of the information cannot be determined

Analytic techniques

To provide objective, robust and quality intelligence, The Critical Start Cyber Threat Intelligence Team uses a variety of analytical techniques in our production, primarily, Analysis of Competing Hypotheses (ACH), A & B Teaming, and Key Assumption Checks. Our team is highly educated in how to guard against biases, such as groupthink, confirmation bias and mirror imaging, and our work is subjected to rigorous peer review. To learn more about our Analytical Techniques, see our cyber threat intelligence blogs at: https://criticalstart[.]com/blog/cyberthreatintelligence/intelligence-gathering-and-production