JOURNAL OF APPLIED SECURITY RESEARCH
https://doi.org/10.1080/19361610.2022.2086785

Security Enhancement of Third Parties Is Needed in Global Supply Chain Management

Yoshiyasu Takefuji

Faculty of Data Science, Musashino University, Tokyo, Japan

ABSTRACT
Incident reports show the high risk of losing trust in global supply chain management. Under the covid-19 pandemic, cloud-based global supply chains have been vulnerable to malicious attacks. The goal of this paper is to show the high risk caused by third-party access in the current global supply chains and how to mitigate it. Based on the incident reports, global supply chain leaders are unaware of the risks of third-party access. The current global supply chains must be transformed into robust and resilient systems against malicious attacks. This paper shows methods on how to mitigate the high-security risk.

HIGHLIGHTS

- Incident reports show the high risk of losing trust in global supply chain management against malicious attacks.
- The high risk caused by third-party access in the current global supply chains will be illustrated.
- Global supply chain leaders are unaware of the risks of third-party access. The global supply chains must be transformed into robust systems.
- This paper shows methods on how to mitigate the high-security risk in third-party logistics.
- The lower the risk, the lower the chance of losing trust. The more a leader is aware of the high risks, the less likely he or she is to lose trust.

KEYWORDS
Global supply chain; security vulnerabilities; third-party access

Introduction

The COVID-19 pandemic and Russia's invasion of Ukraine have brought cybersecurity issues into the spotlight worldwide. This paper examines the current important issue in global supply chain management. This paper identifies cybersecurity challenges that leaders need to solve. Traditional academic papers have not disclosed the real critical security issues in the global supply chain, and this paper clarifies them and will also elaborate on cybersecurity terminology.

CONTACT Yoshiyasu Takefuji takefuji@keio.jp Faculty of Data Science, Musashino University, 3-3-3 Ariake Koto-ku, Tokyo 135-8181, Japan.

Steven Carter reported that hackers have been putting the global supply chain at risk (Carter, 2020). In light of breaches connected to the vulnerable third-party suppliers of Walmart, Equifax, Apple, Target, CVS, CNN, and others, for business reasons, organizations are increasingly providing third parties with access to their IT infrastructure (Carter, 2020). IT and security leaders really need to help their business leaders understand the risks of third-party access and take steps to help manage these risks to an acceptable level (Carter, 2020).

Resilience 360 also reported that nearly 300 cybersecurity incidents were impacting supply-chain entities in 2019 (Fielding, 2020). With the average business sharing data with more than 500 third parties, it's no wonder that the Ponemon Institute reports that roughly 61% of U.S. companies have experienced a data breach within their supply chains (Fielding, 2020). As of June 2020, an incredible 42% of American workers were conducting business remotely from home and migrating offices. With a highly mobile workforce and supplier ecosystems that are becoming increasingly complex and globally dispersed, the threat to intellectual property and classified or sensitive information intensifies (Fielding, 2020).

Risk Ledger found that over 60% of data breaches happening at present can be attributed to a third party (Mühlberg, 2020). The details are as follows the impact of covid-19 on supply chain security has been profound (Mühlberg, 2020).

In December 2020, FireEye announced that it was attacked by what they believe is a sophisticated threat actor, one whose discipline, operational security, and techniques indicate a state-sponsored adversary (Geenens, 2020). While the attacker was able to access some internal systems, at the time of the announcement, there was no evidence of the attackers having exfiltrated confidential or sensitive data (Geenens, 2020). FireEye did confirm that the attacker accessed and stole their red team assessment tools (Geenens, 2020). Malicious attackers can create unidentifiable backdoors using the stolen assessment tools.

This paper depicts how supply chains have been attacked and how to defend them against malicious attacks. Supply chain attacks are detailed and classified for novices to understand for preventing security problems including Phishing, Smishing, and Vishing, respectively. The top malicious threat, Emotet is explained. This paper also shows why Emotet problems cannot be resolved easily. Educating all employees including third parties plays a key role in protecting supply chains against malicious attacks since there is no effective method for mitigating Emotet and Emotet variants problems which are called immune escape in medicine.

Supply chain attacks

This paper addresses what are supply chain attacks and how to defend our supply chain systems against malicious attacks.

According to Microsoft (Simpson & Davis, 2022), supply chain attacks are an emerging type of threat that targets software developers and suppliers. The goal of supply chain attacks is to gain access to source code, build processes, or update mechanisms by infecting legitimate apps and distributing malware.

The New York Times reported that the intrusion into supply chains is far more widespread than first thought (Sanger et al., 2021). Initial estimates were that Russia sent probes to only a few dozen of the 18,000 government and private networks it accessed by inserting code into network management software made by SolarWinds in Texas. But as companies that provide cloud services like Amazon and Microsoft dug deeper for evidence, it appears that Russia gained access to as many as 250 networks using multiple layers of the supply chain (Sanger et al., 2021).

Today's supply chain is an extended, connected web that spreads in every direction. It can be a digital supply chain where risks, such as compromised code present a third-party risk as follows (IronNet, 2020).

Peter Firstbrook summarized that the recent supply chain attacks that affected nearly 18,000 SolarWinds customers left many organizations scrambling to respond to the threat and ensure continued network operations (Firstbrook, 2021). Supply chain attacks can be classified into five types: (1) attacks embedding a backdoor in suppliers, (2) remote access attacks between suppliers and customers, (3) attacks impersonating customers to suppliers, (4) attacks on supplier's email system, and (5) authentication attacks on the supplier's identity management.

While 48% of hospital IT executives reported system outages caused by ransomware in the past six months, <11% of the same executives in the August 2021 health tech survey mentioned cybersecurity was a high-priority investment.

According to a February 23, 2022 IBM report, manufacturing was cyber-attacked in 2021, disrupting the supply chain not only by shutting down ransomware groups but also by new Linux ransomware code in the cloud and a shift to Docker-focused targeting. Before invading Ukraine, Russia launched a massive cyber-attack on the government's infrastructure and supply chain, paralyzing the country. In other words, protecting the supply chain plays a significant role in protecting the country.

Cyberterrorism vs. hacking

We must define and clarify what is cyberterrorism and hacking. It is important to distinguish hacking from cyberterrorism. According to

Matusitz (2014), hacking is delving into computer systems or networks but not destroying them. A computer expert who seeks glory and who harms an entire computer system is not a cyberterrorist if the act of hacking is not premeditated and if the intention is not to cause fear or terror. Consequently, the term "hacking" does not necessarily imply that it is "cyberterrorism." According to the U.S. Federal Bureau of Investigation (FBI), cyberterrorism is defined as any "premeditated, politically motivated attack against information, computer systems, computer programs and data, which results in violence against non-combatant targets by subnational groups or clandestine agents."

What are phishing, smishing, and vishing?

According to WebTitan's advice (WebTitan, 2021), phishing is not only performed via email. Rather than using email to deliver the hook, many threat groups use SMS or instant messaging platforms and increasing numbers of phishing campaigns are now being conducted by telephone and these types of phishing attacks are harder to block.

Phishing using SMS messages is known as smishing (WebTitan, 2021). Instead of an email, an SMS message is sent that contains a link that the user is instructed to click on. Instant messaging platforms, such as WhatsApp are also used. A variety of lures are used, but it is common to send security alerts that warn of unauthorized transactions or other security threats and require the recipient to log into their account.

In December 2019, the U.S. Federal Bureau of Investigation (FBI) identified a campaign by cybercriminals to conduct phishing by phone, known as vishing. Cases of vishing attacks are on the rise (WebTitan, 2021).

To avoid malicious attacks, educating employees including third parties on phishing, smishing, and vishing via email, SMS, Apps, and other messaging applications plays a key role.

Emotet attacks

The number of critical vulnerabilities is 164409 as of November 15, 2021, so it is inevitable to avoid malicious attackers entering global supply chains by exploiting critical vulnerabilities (CVE, 2020).

Emotet is a trojan malware that is primarily spread through spam emails (malspam) of remote workers. The more remote workers, the more vulnerable global supply chains are exploited. Emotet is constantly evolving and remains one of the most current threats out there (Kupreev, 2020). Save for the explosive growth in distribution after five months of inactivity, we have yet to see anything previously unobserved (Sanger et al., 2021).

On top of that, we are currently observing the evolution of third-party malware that propagates using Emotet (Kupreev, 2020). Emotet botnet has returned with updated payloads and a campaign that is hitting 100,000 targets per day (Tara Seals, 2020). Emotet has more than 33,000 variants as of 2019 which had already been recorded in the databases (Gierow, 2019).

Based on the latest information from Emotet, there are 470,000 variants as of December 2020 (The New York Times, 2020). This means that the conventional profiling based on malware detection is not effective for mitigating the latest malware including Emotet. Check point clearly stated that Emotet continues to reign as the top malware threat despite takedown as of February 12, 2021 (Check Point, 2021). In other words, there is no effective method for mitigating Emotet and Emotet variants problems. The current supply chain is compromised with no effective security tools other than training employees.

The recent progress of hypervisor technology for detecting and nullifying unknown malicious code execution with buffer overflows enables us to inactivate Emotet and all variants of Emotet (Takefuji, 2005). However, the protection mechanism against Emotet and variants is not disclosed yet.

During a pandemic, telework must be specially taken care of because of the following vulnerabilities:

- Vulnerabilities in telework software
  The exploitation of vulnerabilities in the environment deployed for telework, such as VPNs and web conferencing services.
- Vulnerability of private PCs and home networks
  Vulnerability of using private PCs with disparate security measures. Vulnerability of using home networks with disparate security measures, even if the PCs are provided by the organization.
- Inadequate management system
  Inadequate management systems, such as rule maintenance and security measures due to the sudden shift to teleworking caused by the COVID-19 pandemic.

Discussion

The worst malicious attack is called Emotet. There are as many as 470k variants of Emotet as of December 2020. The current malicious detection and prevention mechanisms using profiling schemes cannot resolve the Emotet problems at all. Malicious code behavior detection and protection methods are only used for experiments and research studies. Therefore, current security methods cannot solve this Emotet problem and we have to rely on employee training for avoiding Emotet attacks as far as we know.

Attacks on remote workers

(Belzunegui-Eraso and Erro-Garcés (2020) argued that most companies and governments are adopting telework globally to ensure worker safety and to ensure continuity and sustainability of economic activities after the COVID-19 pandemic. Abukari and Bankas (2020) introduced the guidelines provided by the National Institute of Standards and Technology (NIST, 2020) and argued "Most organizations and government agencies do not have a comprehensive telework security policy that protects teleworkers, BYOD (Bring Your Own Device), and remote access." Thus, teleworking, which is expanding after the COVID-19 pandemic, is at risk from criminals and poses an increased information security risk.

Suggestions for future research

Attackers share critical security information and cracking techniques and tools intensively, while defenders do not share useful security information, such as blacklisted IPs. Broadband routers must stop communication from IPs on the blacklist. However, current dumb broadband routers do not have such a blacklist feature or capability. We must be able to distinguish blacklisted IPs to mitigate "Distributed Denial-of-Service" (DDoS) attacks. All existing broadband routers over the Internet must share the blacklist feature in the world for supporting defenders.

EMOTET is a new malware that cannot be easily detected by conventional signature-based malware detection methods. Because EMOTET can generate a large number of variants with distributed execution codes over the Internet, it is impossible to discover EMOTET variants by the conventional signature-based malware detection method. In other words, EMOTET's executable code will be constructed by assembling and integrating multiple execution pieces distributed across the Internet.

However, while behavior-based malware detection methods are useful, current ones are very slow. Therefore, we must develop a fast behavior-based malware detection method on the hypervisor which is indeed needed for real-time EMOTET and variants detection.

GIS-based location acquisition methods or tools are needed to obtain the physical location of Internet communications devices to mitigate malware codes and shutdown malicious hackers and cyberterrorists. However, the privacy issues must be resolved with the GIS-based location acquisition methods. In other words, it is not so easy to construct a location acquisition method that solves the privacy issue.

Conclusion

There are more than 164409 known critical vulnerabilities in our software as of November 15 in 2021. Malicious attackers using Emotet variants are expected to break into global cloud supply chains where third-party remote workers can be easily exploited by clicking on emailed or SMS documents. To turn today's global supply chain into a robust and resilient system, third parties in individual global supply chains must provide special security care against malicious attacks. Training all supply chain employees including third parties plays a key role in protecting them against malicious attacks since there is no effective method for mitigating Emotet and Emotet variants problems.

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

Yoshiyasu Takefuji http://orcid.org/0000-0002-1826-742X

References

Abukari, A. M., & Bankas, E. K. (2020). Some cybersecurity hygienic protocols for teleworkers in Covid-19 pandemic period and beyond. *International Journal of Scientific and Engineering Research*, *11*(4), 1401–1407.

Belzunegui-Eraso, A., & Erro-Garcés, A. (2020). Teleworking in the context of the Covid-19 crisis. *Sustainability*, *12*(9), 3662. https://doi.org/10.3390/su12093662

Carter, S. D. (2020). Hackers putting global supply chain at risk. https://www.nationaldefensemagazine.org/articles/2020/7/2/hackers-putting-global-supply-chain-at-risk

Check Point. (2021). January 2021's most wanted malware: Emotet continues reign as top malware threat despite takedown. https://www.globenewswire.com/news-release/2021/02/11/2173870/0/en/January-2021-s-Most-Wanted-Malware-Emotet-Continues-Reign-as-Top-Malware-Threat-Despite-Takedown.html

CVE. (2020). Distribution of all vulnerabilities by CVSS Scores. https://www.cvedetails.com/cvss-score-distribution.php

Fielding, J. (2020). Protecting the global supply chain with borderless data. https://www.supplychainbrain.com/blogs/1-think-tank/post/32201-protecting-the-global-supply-chain-with-borderless-data

Firstbrook, P. (2021). Gartner: Steps to respond to a supply chain attack. https://www.cybersecuritydive.com/news/supply-chain-attack-response/594271/

Geenens, P. (2020). FireEye hack turns into a global supply chain attack. https://securityboulevard.com/2020/12/fireeye-hack-turns-into-a-global-supply-chain-attack/

Gierow, H. (2019). New record in 2019: Emotet now has over 30.000 variants and counting. https://www.gdatasoftware.com/blog/2019/07/35071-emotet-now-has-over-30000-variants-and-counting

IronNet. (2020). A sobering reminder for more vigilant supply chain security. https://securityboulevard.com/2020/12/a-sobering-reminder-for-more-vigilant-supply-chain-security/

Kupreev, O. (2020). The chronicles of Emotet. https://securelist.com/the-chronicles-of-emotet/99660/

Matusitz, J. (2014). The role of intercultural communication in cyberterrorism. *Journal of Human Behavior in the Social Environment*, *24*(7), 775–790. https://doi.org/10.1080/10911359.2013.876375

Mühlberg, B. (2020). Supply chain security on thin ice in the age of COVID-19. https://www.cpomagazine.com/cyber-security/supply-chain-security-on-thin-ice-in-the-age-of-covid-19/

National Institute of Standards and Technology. (2020). Telework cybersecurity resources: New ITL bulletin and blog posts. https://csrc.nist.gov/News/2020/teleworkcybersecurity-itl-bulletin-blog-posts

Sanger, D. E., Perlorth, N., & Barnes, J. E. (2021). As understanding of Russian hacking grows, so does alarm. https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html

Simpson, D., & Davis, C. (2022). Supply chain attacks. https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/supply-chain-malware

Takefuji, Y. (2005). Nullification of unknown malicious code execution with buffer overflows. Driverware IMMUNE. https://apps.dtic.mil/docs/citations/ADA451745

Tara Seals. (2020). Emotet returns to hit 100K mailboxes per day. https://threatpost.com/emotet-returns-100k-mailboxes/162584/

The New York Times. (2020). FireEye, a top cybersecurity firm, says it was hacked by a nation-state. https://www.nytimes.com/2020/12/08/technology/fireeye-hacked-russians.html

WebTitan. (2021). Cybersecurity advice. https://www.webtitan.com/blog/category/cybersecurity-advice/