2021 CYBER THREATS TO PUBLIC SAFETY

SUPPLY CHAIN FOCUS

Insights from the Motorola Solutions Threat Intelligence Team - Third in a Series

MOTOROLA SOLUTIONS

Motorola Solutions continues to grow as a global public safety solution leader. Our commitment to deliver the best-in-class products and services for emergency services, with a focus on cybersecurity, gives us direct insight into the cyber threats that uniquely challenge the first responders around the world. To improve the security posture and awareness of public safety organizations, the Motorola Solutions threat intelligence team has compiled their findings, research and analysis throughout 2021 as part of our Cyber Threats to Public Safety series. Our first two reports covered the unique threats to public safety technologies, and insights on the criminals seeking to compromise them. In this report, we share our insights on the growing supply chain threat to public safety operations. We seek to inform and educate the public safety leaders and practitioners on how threat actors conduct supply chain attacks, especially third party providers, and what defenders can do to mitigate the threats. The threat intelligence team used proprietary data, publicly reported and closed source cyber intelligence from Jan. 01 — Dec. 31, 2021 in this paper.

TABLE OF CONTENTS

SUPPLY CHAIN AND THIRD-PARTY PROVIDER THREATS

Emergency service organizations are becoming less self-contained, increasingly relying on third-party vendors to provide equipment and software that enable their day-to-day and emergency operations. This reliance requires organizations to use equipment supplied by third-parties while granting them trusted access to sensitive internal information through platforms they produce. This has created a web of interdependent supply chain companies that may not be aware that they are connected. While this has made organizations more efficient, it has also massively expanded the cyberattack surface. Threat actors are compromising legitimate hardware and software at the source to exploit downstream target organizations. This has a multiplier effect: in a multi-tier supply chain, one intrusion can create a platform from which threat actors can compromise the systems of hundreds — or thousands — of end users.

Supply chain attacks (SCA) are malicious actions taken to create and exploit a vulnerability during the production, development, or distribution cycle of hardware or software in order to detrimentally impact consumers or users of the finished product. Threat actors insert, replace, or modify a component of an otherwise secure, legitimate entity and persist until the altered component is part of an operational system. This can include modifying code or physical components prior to the product's delivery to end users.

Supply chain attacks are not a new phenomenon. Both hardware and software SCAs have been identified as early as 1984. However, beginning in early 2020, modern software SCAs have become increasingly sophisticated, taking advantage of the rapid rise in software-as-a-service (SaaS) offerings and cloud infrastructure. The success of security protections has also influenced the rise in SCA attacks. It is assessed that since organizations have begun incorporating more robust security protections, attackers have been forced to find new vectors to compromise their desired end targets.

Due to the required trust and access granted to suppliers, targeting them is a logical step for attackers. Organizations can be vulnerable to a SCA even when their own defenses are robust. Smaller third-party vendors within larger supply chains are likely to be seen as a weak link through which threat actors can target high-value, security-conscious organizations.

TYPES OF SUPPLY CHAIN ATTACKS

There are two overall categories of supply chain attacks: hardware and software. Hardware attacks refers to an adversary physically planting malicious code or components inside a piece of hardware or equipment and firmware. This type of attack typically occurs in the manufacturing and distribution stages of the supply chain. Threat actors often seek to create a backdoor connection between the device and an attacker-controlled system that, upon delivery to end users, can be leveraged to gain further access or exfiltrate data.

The contested 2018 Super Micro compromise reported by Bloomberg is a representative, if unconfirmed, example of a hardware SCA.[1] In the alleged attack, Chinese state-backed operatives implanted microchips into motherboards made in China and sold by the U.S.-based Super Micro, which enabled the operating system to be altered and beacon to computers to download additional information. This allegedly gave the Chinese operatives access to servers belonging to numerous U.S. companies, including Apple, Amazon, and various government entities. These allegations, however, were disputed by China and all companies listed in the report.

Software SCAs refer to threat actors inserting malicious code into a legitimate software or app by gaining access to source codes, build processes, or update mechanisms. This type of attack typically occurs in the manufacturing and maintenance stages of the supply chain. Threat actors target unsecure network protocols, unprotected system infrastructure, and coding malpractices.

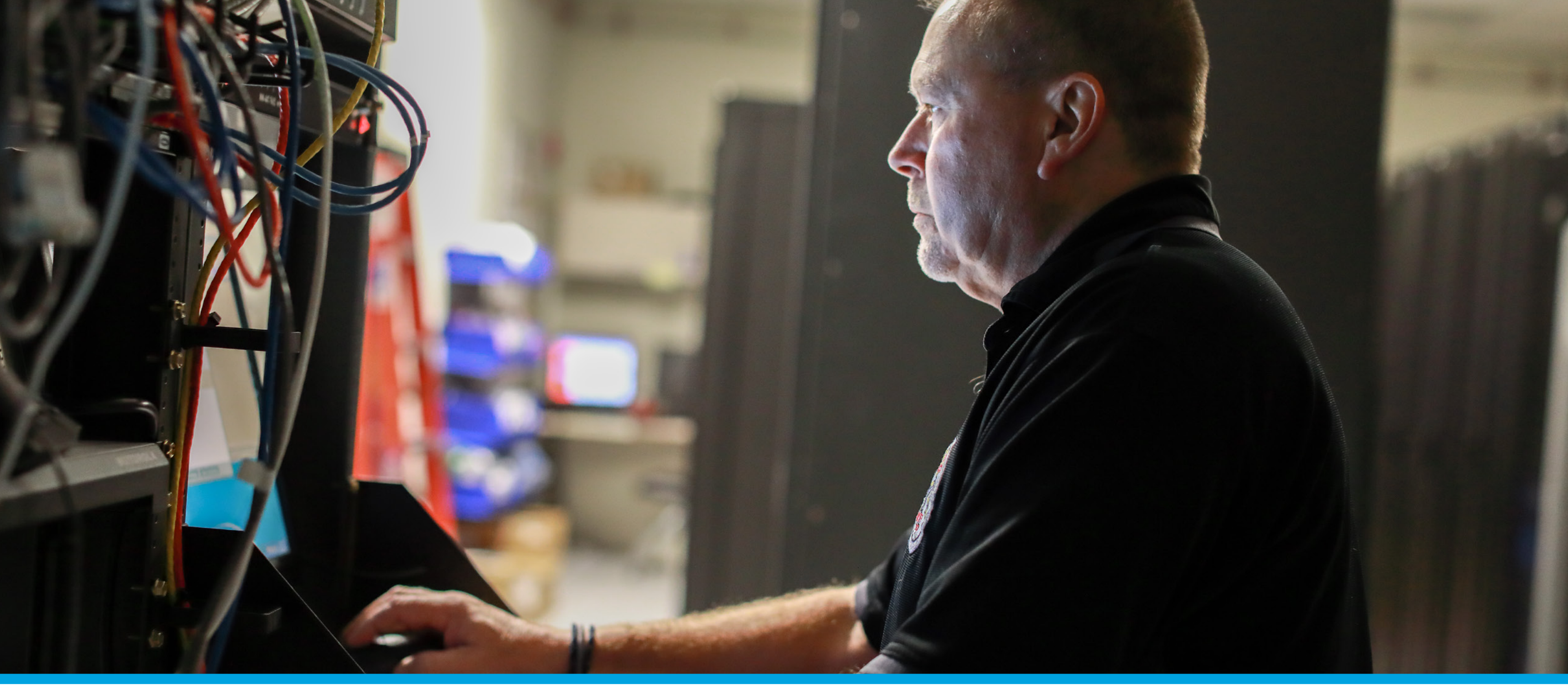
Vendors are most likely unaware that their software has been infected with malicious code when it is released to end users. Software issued by these vendors is given trusted access to customers' systems, enabling malicious code to run with the same permissions as the rest of the software. This enables threat actors to distribute malware to multiple end users. Three software-based SCAs methodologies have emerged as favorites by threat actors:

- **Compromise of third-party code libraries:** Software developers often leverage containers, software development kits (SDKs), and frameworks to package software during production. These can rely on third-party code, including multiple open-source libraries that rely on contributions from numerous developers and other open-source projects. By targeting third-party libraries, threat actors can inject malicious code into software prior to its release downstream. Reporting indicates that attacks targeting open-source software projects increased 430 percent between 2019 and 2020.[2]
- **Compromise of software and development infrastructure:** Threat actors target software developers and engineers with traditional initial access techniques such as phishing or Remote Desktop Protocol (RDP) compromise. Threat actors can obtain sign-in credentials and move laterally or escalate privileges until they have access to the desired build environment or servers. From there, they can manipulate or implant malicious code and steal code signing certificates[3] to approve tampered software prior to release to customers. Once software is signed with a digital signature, it can evade security detection or built-in product anti-tampering mechanisms.
- **Compromise of software update servers:** Rather than compromising the product itself, threat actors compromise servers that are used to distribute an organization's software updates. This enables threat actors to replace legitimate files with various types of malware that, if automatically distributed to customers, can create a worm effect across downstream end users.

Software SCA attacks are more common than those targeting hardware. As software-focused SCAs have spread beyond nation-state operatives, such as those attributed to the Dec. 2020 SolarWinds attack, they have become widespread and frequently reported. In the SolarWinds instance, Russian agents obtained access to the networks, systems, and data of thousands of platform users — including multinationals and U.S. government departments — by planting malicious code in the SolarWinds IT management tool Orion.[4] Top tier eCrime groups have observed the success of SCAs, too. In July 2021, the REvil extortion group was able to leverage a zero-day vulnerability to gain access to Kaseya's Virtual System/ Server Administrator software and inject ransomware across 800 — 1,500 downstream customers.[5]

Public Safety was the primary target of a SCA in a rare instance. On August 16, 2019, 23 Texas government entities were impacted by a ransomware attack that leveraged a shared undisclosed managed service provider to deploy the Sodinokibi ransomware.[6] The attack was able to disrupt medium to small town and city networks for a few days to a few weeks, degrading emergency and municipal services.

[1] https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies
[2] https://www.sonatype.com/hubfs/Corporate/Software%20Supply%20Chain/2020/SON_SSSC-Report-2020_final_aug11.pdf
[3] https://attack.mitre.org/techniques/T1588/003/
[4] https://whatis.techtarget.com/feature/SolarWinds-hack-explained-Everything-you-need-to-know
[5] https://helpdesk.kaseya.com/hc/en-gb/articles/4403584098961-Incident-Overview-Technical-Details
[6] https://www.zdnet.com/article/at-least-20-texas-local-governments-hit-in-coordinated-ransomware-attack/



WHO ARE THE THREAT ACTORS?

Nation-state or state-backed entities are likely the largest category of threat actors conducting SCAs. This is partially due to the fact that the complexity of conducting such attacks is beyond the capabilities and resources of most cyber threat actors. SCAs are particularly useful for conducting espionage or destructive campaigns, both of which are within the modus operandi of some state-linked entities. Of the 24 SCAs reported between Jan. 2020 and July 2021, half have been attributed to well-known advanced persistent threat (APT) groups.[7] However, the report also states that 42 percent of SCAs in this period have not yet been attributed to a specific group, indicating the proportion of attacks likely conducted by APT groups could be significantly higher.

The Russian military conducted one of the most destructive and widespread SCAs in 2017 with the NotPetya malware. They were able to inject NotPetya into a legitimate software update for the M.E.Doc accounting software solution, which then leveraged wormlike techniques to spread across networked systems. NotPetya encrypted whole systems, rendering entire hard drives unusable. In encrypting the data, the malware damaged files beyond repair, meaning that even if victims paid, their data could never be recovered. The total cost to NotPetya victims may exceed $10 billion USD, with at least nine organizations suffering losses in excess of $100 million USD. It is considered the costliest cyberattack in history.[8]

More recently, financially motivated threat actors, such as REvil, are looking to conduct SCAs as a means to deploy ransomware. The trickle-down effect, together with the potential to infect hundreds or even thousands of end users and obtain files that can be sold or used as leverage in extortion attempts, likely represents an attractive return on investment for financially motivated threat actors. It is possible that high-profile SCAs and the rise in ransomware-as-a-service (RaaS) operations could encourage a broader range of threat actors to conduct these types of attacks. Another possible threat actor conducting SCAs are those seeking to steal intellectual property or other corporate information that could help a competitor obtain an advantage.

[7] ENISA Threat Landscape For Supply Chain Attacks, European Union Agency for CyberSecurity, July 2021

[8] https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and

MANAGING SUPPLY CHAIN RISK

It is projected that the frequency of SCAs are likely to increase in the short term, rather than the scale. This assessment is underpinned by widespread reporting of SCAs outlining the potential impact they can have, as well as providing proof-of-concept for threat actors that may have previously deemed such attacks beyond their capability.

Smaller third-party vendors within larger supply chains are likely to be seen as a weak link through which threat actors can target high-value organizations with mature cybersecurity programs. There is likely to be an increase in non-nation state and non-state-linked threat actors seeking to conduct SCAs. The use of SCAs as a means to distribute ransomware is likely to increase, driven in part by RaaS offerings lowering the barriers to entry for threat actors seeking to conduct ransomware attacks. This would place highly effective malware in the hands of more operators.

To manage supply chain cybersecurity risk, organizations should[9]:

- Identify and document types of suppliers and service providers
- Define risk criteria for different types of suppliers and services (e.g., important supplier and customer dependencies, critical software dependencies, single points of failure)
- Assess supply chain risks according to their own business continuity impact assessments and requirements through cybersecurity audits
- Define measures for risk treatment based on good practices
- Monitor supply chain risks and threats, based on internal and external sources of information and findings from suppliers' performance monitoring and reviews
- Make their personnel aware of the risk.

This knowledge is a core building block of every product and service Motorola Solutions offers. Our customers face increasingly sophisticated and dangerous cyber threats. However, they are not facing this threat alone. Armed with insights such as those found in the Motorola Solutions 2021 Cyber Threats to Public Safety reports, they can confront today's cyber challenges with confidence.

For more information, visit motorolasolutions.com/cybersecurity or download the previous two reports.

[9] Derived by cybersecurity controls in standards ISO/IEC 27002, ISO 9001 and ISO 31000

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, Il 60661 U.S.A. **motorolasolutions.com**