How to Reduce The Risk of Cyber-Attacks on Global Supply Chains

Amy Nelson

Chair of TCG's PC Client Work Group | Trusted Computing Group (TCG)

The number of cyber-attacks attempting to compromise global industry supply chains are on the rise, and a new survey by BlueVoyant found that 97 percent of global firms have been impacted by a cybersecurity breach in their supply chain in the past 12 months. Not only that, but 95 percent of respondents said their organizations experienced a challenge in managing third-party risk. The high number of stages, organizations, and individuals involved makes it difficult to effectively secure supply chains as no single company has end-to-end control to enforce security measures. Current methods are mostly subjective and rely on human intervention, which are difficult to securely manage on a large scale.

This makes supply chains prime targets for attackers looking to infiltrate a large number of organizations via a single, targeted attack. Cyber-attacks are becoming more sophisticated and difficult to detect, so it is vital that stakeholders across supply chains have the knowledge and solutions to determine the security status of systems and devices at every stage of the process.

ATTACK OPPORTUNITIES

The many stakeholders, stages, and processes within a supply chain means that one weak link can make the entire chain vulnerable. While many organizations have stepped up their security measures in recent years, just one or two weak links in a global supply chain with an insufficient approach to security will open the door to the entire chain for cybercriminals.

Supply chain attacks are caused by hackers infiltrating a system, typically through tampering with the manufacturing process of a physical component or during distribution of a software component. By infecting or damaging legitimate applications, malware or malicious codes are then distributed throughout the rest of the chain with the same trust and permissions as the original application. Hackers are able to stay hidden for longer periods of time, and their malware can be distributed far and wide without detection to inflict significant damage.

Malicious and counterfeit software or hardware is extremely difficult to identify, with many end users not even considering that purchasing from a third-party vendor may come with risks. If a vendor is legitimate, many will assume that their reliability and trustworthiness extends to their products. In reality, the malpractice may have occurred much earlier in the lifecycle of the product. A recent report from the European Union Cybersecurity Agency (ENISA) found that around 62 percent of the analyzed attacks on customers took advantage of their trust in their supplier. This highlights that organizations must prioritize validating third-party code and software to ensure they have not been tampered with or manipulated.

> ***While many organizations have stepped up their security measures in recent years, just one or two weak links in a global supply chain with an insufficient approach to security will open the door to the entire chain for cybercriminals.***

For hackers, supply chain attacks have become an efficient way of harming a large number of organizations from one single entry point. Just one carefully planned attack to a specific stage in the supply chain can impact every organization that purchases hardware or software from that point onwards.

A NEW LEVEL OF CYBER-ATTACKS

The amount of data generated, analyzed, and stored is rising as Internet of Things (IoT) infrastructure is used across industries, from governments and militaries to healthcare and energy. For these industries, the data is significantly more sensitive and any breach could lead to devastating consequences. These industries have extremely large-scale businesses with complex supply chains, offering extra opportunities for hackers to take advantage of.

Dragonfly, a cyber espionage group, is an example of how attackers are conducting sophisticated supply chain attacks. The group has been known to target energy and pharmaceutical companies across Europe and North America in recent years by utilizing weaknesses in their supply chains. First, they gain access to legitimate industrial control system software and replace the files with their own compromised versions. By using legitimate files as Trojan Horses for their own malware, they are able to remain undetected through the supply chain. The same concept applies to hardware and IoT devices; attackers are able to identify the weakest link in the supply chain, and tamper with devices before they are distributed to the vendor. The malware that passes through these chains may contain remote access functionalities, giving the attackers some control over the system it has been installed on.

Earlier this year, researchers discovered that a UEFI (Unified Extensible Firmware Interface) bootkit had been used by attackers to backdoor windows systems as early as 2012, by modifying a legitimate Windows Boot Manager binary to achieve persistence. By doing this, the malware had circumvented Microsoft Windows Driver Signature Enforcement to load its own unsigned driver used for document theft, keylogging, and screen monitoring by periodically capturing screenshots. By infiltrating in the early stages of the system boot process, attackers' malware could bypass security measures and put its malicious driver into action at system start-up. This is another reminder of the importance of securing the entire supply chain and holding each level accountable.

As attacks rise in scale, sophistication, and cost, organizations must prioritize solutions that play a significant role in preventing supply chain attacks. As the volume of sensitive data stored within devices continues to rise, we can safely assume that attacks to access this data will continue.

VERIFYING THE RELIABILITY OF EQUIPMENT

Preventing supply chain attacks is no easy task, as there has previously been no definitive way to determine the security status of multiple endpoints within a network. However, the latest Firmware Integrity Measurement (FIM) specification, released this year by Trusted Computing Group, provides an official definitive guide. It provides the guidelines for products that can determine the integrity of a device at the manufacturing stage and offers a baseline measurement that allows for security result comparisons throughout its lifetime. This means that at any point in a products' life cycle, and at any stage of a supply chain, the user or manufacturer can determine the integrity of a device. This is especially significant for large production chains, where the vast number of stages and organizations involved can make it difficult to track the security status of a device.

The FIM specification verifies that an endpoint computer received by a customer matches what the customer ordered. For example, before a computer is shipped, the manufacturer takes a Reference Integrity Measurement (RIM) to take note of a baseline before any hackers have a chance to tamper with it in the supply chain. Once the customer receives the computer, it can measure the FIM and compare it to the RIM to detect if the computer's hardware and firmware configuration has been compromised. If each OEM in a supply chain follows this, each organization will be able to determine and be assured thatthe integrity of the device and what is running on the device have not been compromised.

One of the main difficulties with securing supply chains is that the malware installed by attacks is usually extremely difficult to detect as it travels through the supply chain. This specification puts a stop to this, as the integrity of devices and networks can be verified. Not only can end users gain another level of assurance in their devices, but by testing products throughout the chain, access points for attackers can be identified and strengthened. This allows for future attacks to be mitigated and protects data from falling into the wrong hands.

IMPROVING SUPPLY CHAIN SECURITY

According to ENISA, strong security protection is no longer enough for organizations when attackers have already shifted their attention to suppliers. Organizations within global supply chains must utilize the tools and technologies that can detect malware and determine the integrity of hardware on a device. This can be done at all stages, but the sooner the threat is identified, the less damage it can cause to the rest of the supply chain. Global supply chains are incredibly complex, but with so many attacks focusing on the suppliers' code in order to further compromise targeted customers, every organization and its users will benefit from a security-first approach. 🔒

ABOUT THE AUTHOR

Over the last 25 years, Amy Nelson has built up an extensive repertoire within the IT and cybersecurity space. Amy is a Security Architect and a Distinguished Member of the Technical Staff in the Modern Computing Solutions Group within Dell's Client Solutions Group. She represents Dell within the Trusted Computing Group, where Amy holds several positions, including Chair of the PC Client Work Group and TCG's Technical Committee.

TRUSTED®
COMPUTING
GROUP