SUPPLY CHAIN ATTACKS:
IS THIS A SIGN OF A CYBER PANDEMIC?

Introduction

After deploying a new system, you're likely to feel there's a honeymoon period before it comes under an attack. Likewise, when performing a software update, we can feel some relief believing the newest features and patches will protect our applications against exploits.

However, supply chain attacks are destroying this false sense of security by compromising trusted vendors to implant threats in new systems and software updates.

The SolarWinds malware campaign that has caused so much damage and uncertainty is just the latest example of the widespread devastation with a supply chain attack. Here is all you need to know about supply chain attacks and the actions you must take to secure your environment against them.

> Researchers have uncovered a software supply chain attack that is being used to install surveillance malware on the computers of online gamers. The unknown attackers are targeting select users of NoxPlayer, a software package that emulates the Android operating system on PCs and Macs.[1]

How supply chain attacks work

Supply chain attacks can compromise both trusted software and hardware vendors. Once attackers get past a vendors' defense systems and implant threats in their products, vendors will unknowingly distribute malware or embedded threats into other network environments.

[1] New supply chain attack uses poisoned updates to infect gamers' computers, by Dan Goodin, arsTechnica, February 1, 2021. https://arstechnica.com/information-technology/2021/02/new-supply-chain-attack-uses-poisoned-updates-to-infect-gamers-computers/

Software

When it comes to software vendors, supply chain attacks typically start by threat actors surveilling a vendor waiting to find insecure network protocols, unprotected servers, and unsafe coding practices. When threat actors find these, they change source code to embed malware in a software build and update processes and software update mechanisms. Because the software comes from a trusted vendor, the infected apps and updates are legitimately signed and certified.[2]

Hardware

In addition to software-based threats, IC and computer manufacturers are also susceptible to supply chain attacks. IC foundries face threats such as hardware Trojans and piracy breaches. Chip foundries use split secure fabrication and logic barriers that separate logical inputs from the outputs to prevent threats during chip fabrication. However, these are not foolproof.[3]

When moving up a level from chips to computing systems, there are two ways for threat actors to infiltrate computer equipment. One is through interdiction attacks that tamper with computing devices during transport from manufacturers to customers. The second method puts malicious chips on computers during the manufacturing of motherboards.[4]

> "Estimates indicate that around 60 percent of data breaches are linked to third parties, and we can expect that percentage to increase as more companies embrace digital platforms and new operating models that require sharing of data with partners and service providers."[5]

[2] Supply chain attacks, Microsoft, August 9, 2019
https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/supply-chain-malware

[3] Jake Hertz, The Most Significant Cyberattack in History Prompts Questions About Supply Chain Security, All about Circuits, December 29, 2020
https://www.allaboutcircuits.com/news/most-significant-cyberattack-in-history-prompts-questions-supply-chain-security/

[4] Jordan Robinson and Michael Riley, The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies, Bloomberg, October 4, 2018
https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

[5] Todd Carroll, CISOs: Make 2020 the year you focus on third-party cyber risk, Help Net Security, January 24, 2020
https://www.helpnetsecurity.com/2020/01/24/third-party-cyber-risk/#:%7E:text=Estimates%20indicate%20that%20around%2060,with%20partners%20and%20service%20providers

Why fear supply chain attacks?

Simply put, every element of your infrastructure is at risk. Supply chain attacks target software and hardware in your on-premises, cloud, mobile, and IoT environments, putting every element in your infrastructure at risk. Supply chain attacks not only target a victim's infrastructure, but they can also quickly spread among partners, customers, and other stakeholders, leading to an escalation attack. Successful escalation attacks could grant threat actors access to protected data and several IT environments. In addition to traditional hardware and software, security researchers have found supply chain attacks that preloaded malware in cloud infrastructure[6], smartphones[7], IoT[8], and endpoints[9].

How supply chain attacks escalate beyond hardware and software

Going back to the current attack, the U.S. Department of Justice reported that the SolarWinds supply chain attack added a Trojan to SolarWinds' Orion app to move across its network and access employees' Office 365 email accounts.[10] This attack demonstrates how SaaS applications are also at high risk. One can anticipate that the compromised email accounts not only leak sensitive information, but attackers can also use them to launch phishing attacks against third parties.

Thwart supply chain attacks with a zero-trust environment

With supply chain attacks putting every element in your environment at risk, the only solution is to create a zero-trust environment. Zero-trust means that no device, user, workload, or system is trusted by default.

The way zero-trust works is through micro-segmenting the security in your environment. Micro-segmentation creates junctions and inspection points that block malicious or unauthorized lateral movement in your networking environment. If a security breach should happen, micro-segmentation isolates the threat at the source and keeps it from spreading within your environment and to your third-party stakeholders. IT, public clouds, IoT, operating technologies (OT), applications, workloads, LANs, and WANs, need to be insulated with their own preventative cyber security controls that stop threats before lateral movement compromises the rest of the environment and exploits third parties.

[6] Kelly Jackson Higgins, 'Cloud Snooper' Attack Circumvents AWS Firewall Controls, Information Week, February 27, 2020
https://www.darkreading.com/cloud/cloud-snooper-attack-circumvents-aws-firewall-controls/d/d-id/1337171

[7] Brian Krebs, Tracing the Supply Chain Attack on Android, Krebs on Security, June 19, 2019
https://krebsonsecurity.com/2019/06/tracing-the-supply-chain-attack-on-android-2/

[8] Dan Cornell, Enterprise IoT Security Is a Supply Chain Problem, DarkReading, December 23, 2020
https://www.darkreading.com/iot/enterprise-iot-security-is-a-supply-chain-problem/a/d-id/1339758

[9] Gareth Corfield, Laptops given to British schools came preloaded with remote-access worm, The Register, January 21, 2021
https://www.theregister.com/2021/01/21/dept_education_school_laptops_malware/

[10] Catalin Cimpanu, SolarWinds fallout: DOJ says hackers accessed its Microsoft O365 email server, ZDNet
https://www.zdnet.com/article/solarwinds-fallout-doj-says-hackers-accessed-its-microsoft-o365-email-server/?ftag=TRE-03-10aaa6b&bhid=29524966930760714833143964508637&mid=13227645&cid=2326675408

In conclusion: Moving to a consolidated architecture for zero trust

Creating a zero-trust environment using standalone solutions for each element is highly impractical due to the complexity of monitoring, managing, and administering sixty or more security controls. The most practical way to institute zero-trust is by rolling out a consolidated cyber security architecture. This type of architecture provides all the essential security controls to implement micro-segmentation on-demand, streamlines deployment end-to-end from procurement to unified monitoring, management, administration, and service. Moreover, consolidated security architecture provides disc and document encryption, data loss prevention, forensics, anti-bot, and other controls to ensure comprehensive, preventative security.

Go here to learn more about a zero trust architecture. Check Point offers a comprehensive approach to consolidated security architecture.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com