Check Point
SOFTWARE TECHNOLOGIES LTD

SECURE YOUR EVERYTHING™

HOW SAFE IS YOUR
TECHNOLOGY SUPPLY CHAIN?

Introduction

Although a digital divide exists in many areas of the world, it's likely your organization relies heavily on an internet-based technology infrastructure. Serving as an economic backbone, it's effectiveness to deliver depends on an extensive supply chain with interconnected software and hardware. These tech chains have long relied on each embedded application offering high standards of baked-in security. One recent study, however, found "only 54 percent of CISOs believe the applications developed by their organization would withstand an advanced targeted attack and front-line security teams even less at 44 percent." [1]

It should therefore come as no surprise that technology organizations, too, can fall victim to cyberattacks. When it does occur, it can impact virtually all industries that use products and services from tech companies.
If recent cyberattacks are an indication of what's next, then such technology supply chains offer attackers the ability to breach any weak link in an interconnected chain of partners.

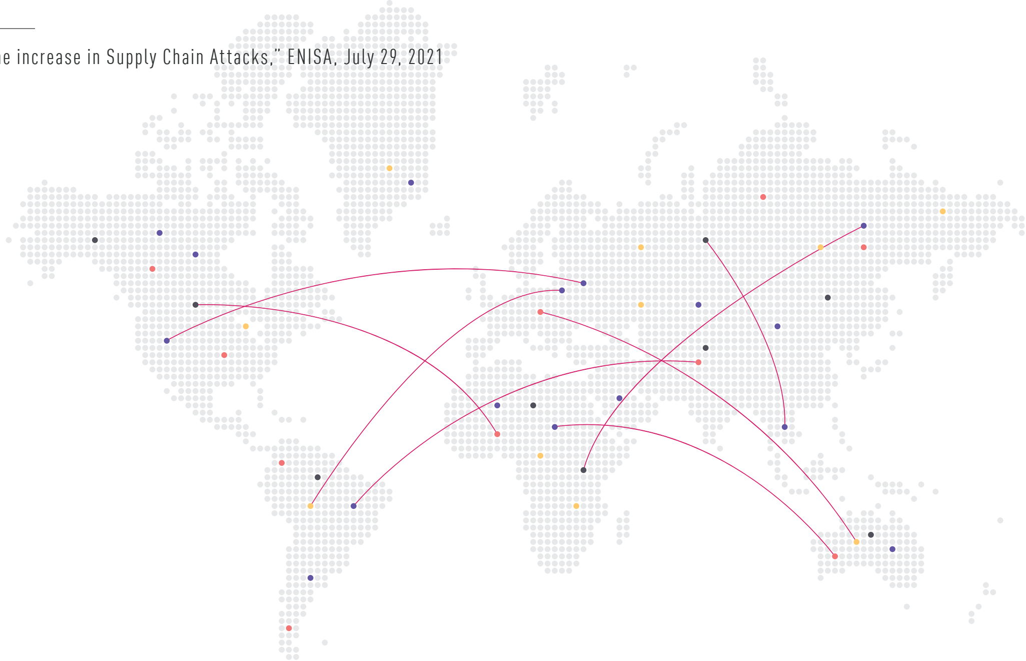
Let's look at how recent attacks on technology firms have played out.

[1] "Imperfect People, Vulnerable Applications," Osterman Research, May 2021

> " Supply chain attacks are now expected to multiply by 4 in 2021 compared to last year. Such new trend stresses the need for policymakers and the cybersecurity community to act now. This is why novel protective measures to prevent and respond to potential supply chain attacks in the future while mitigating their impact need to be introduced urgently." [2]

Tech Companies as Attack Vectors

The explosion of ransomware attacks in 2021 point to a cyber pandemic. Cybercriminals have used vulnerabilities in the tech supply chain to extort more ransom from more victims. Attacking a single company network has been supplanted by more nefarious schemes. A trusted mechanism for software installation and updates could be breached to lockdown systems all along the supply chain of providers, partners, and customers. The compromise of a tech company's website or it's email infrastructure to spread malware can impact customers around the globe.



[2] "Understanding the increase in Supply Chain Attacks," ENISA, July 29, 2021

Tech companies delivering apps have been compromised with malware added during production phase. Pre-installed malware has been a particular problem for smartphones.[3] These 5th generation multi-vector attacks on technology companies are generating more revenue with less effort than previous threats. Here are some recent examples:

- On July 2nd, 2021 attackers compromised IT tools provided by U.S. technology firm Kaseya to launch a ransomware attack, paralyzing between 800 and 1,500 business customers on five continents. The attackers demanded $70 million to restore all the affected businesses' data.[4] It isn't clear how Kaseya responded to the attack, but they received a universal key to decrypt the businesses and public organizations crippled in the global incident.[5]
- In June 2021, threat actors compromised a secure remote access platform to gain unauthorized access to networks at Verizon and several businesses and government agencies.
- The Russian cybercrime group REvil hit Brazilian-based JBS, the world's largest meat processing company, with ransomware on May 2021. The attack shut down meat processing facilities in the US, Canada and Australia.
- On May 4th and 5th 2021, attackers hit Volue, a Norwegian energy technology company with ransomware shutting down water and water treatment facilities in 200 cities, impacting 85% of Norway's population.
- In January of 2021, Hezbollah breached telecom companies, ISPs, and hosting providers in the US, UK, Egypt, Israel, Lebanon, Jordan, Saudi Arabia, the UAE, and the Palestinian Authority for the purposes of espionage and data theft.
- Russian hackers compromised the software provider SolarWinds in December 2020. The attack let the hackers monitor internal operations and steal data at over 200 organizations around the world including US government agencies.
- November 2020: Ransomware hit a Mexican facility owned by Foxconn. The hackers claimed their ransomware encrypted 1,200 servers with 20-30 TB of backups being deleted. They also claimed they stole 100 GB of encrypted files.
- Software supply-chain attacks in November 2020 by a North Korean hacking group compromised a South Korean security software company with the intent to attack South Korean Internet users.
- In August of 2020 it was revealed that suspected Chinese state hackers targeted the source code, software development kits, and chip designs of 7 semiconductor vendors in Taiwan.[6]

[3] Charlie Osborne, More pre-installed malware has been found in budget US smartphones, ZDNet, July 9, 2020.
https://www.zdnet.com/article/more-pre-installed-malware-has-been-found-in-budget-us-smartphones/

[4] Raphael Satter, Up to 1,500 businesses affected by ransomware attack, U.S. firm's CEO says, Reuters, July 6, 2021.
https://www.reuters.com/technology/hackers-demand-70-million-liberate-data-held-by-companies-hit-mass-cyberattack-2021-07-05/

[5] Frank Bajak, Kaseya gets master decryption key after July 4 global attack, AP News, July 26, 2021.
https://apnews.com/article/lifestyle-technology-joe-biden-europe-business-bb7298b31b7157640fbd5f90fc19c224

[6] Anon, Significant Cyber Incidents, Center for Strategic and International Studies, aws viewed on 07/27/2021.
https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

> "Due to the cascading effect of supply chain attacks, threat actors can cause widespread damage affecting businesses and their customers all at once. With good practices and coordinated actions at EU level, Member States will be able to reach a similar level of capabilities raising the common level of cybersecurity in the EU."[7]

Reducing supply chain attacks requires teamwork

If ransomware continues to morph with greater threat potency, then all organizations must enter a new phase of honest cyber security assessment and strong prevention. This recent article offers five keys to proactively reduce the risks with supply chain attacks:[8]

1. **Inform Developers About Cyberattacks**—Update developers on a frequent, on-going basis about new cyberattacks and best practices
2. **Monitor Open-Source Projects**—It's reported that cyberattacks on open-source code increased 430 percent between 2019 and 2020. Simulated attacks can get first-hand information on how software holds up during an attack.
3. **Zero Trust**—Assume that any device, user, or data isn't safe until proven otherwise to reduce and remove supply chain threats.
4. **Built-in Data Protection**—Ensure that all data privacy and protection laws are followed in code building. Latest encryption built into applications is a must.
5. **Focus on Third-Party Risks**—Each connection in the supply chain offers more high-risk vectors. All integrations must be doubled checked as well as working with vendors and partners to ensure cyber security best practices are followed.

[7] "Understanding the increase in Supply Chain Security Attacks," by Luhan Lepassaar, ENISA, July 29, 2021

[8] "5 Ways to Defend Against Supply Chain Cyberattacks," by Jennifer Gregory, Security Intelligence, August 16, 2021

The Biden Administration announced that the National Institute of Standards and Technology (NIST) will collaborate with industry and other partners to develop a new framework to improve the security and integrity of the technology supply chain.[9]

Zero Trust: It's one piece of a complicated puzzle

Given the severity of damage to tech companies financially and to their reputations when attacked, it's imperative for tech companies to establish a state of zero trust across their complete information environments. The multivector nature of today's attack means security controls must cover datacenters, cloud deployments, SaaS, smartphones, remote workers, IoT devices, endpoints, web applications, email servers and more. Software, devices, people and networks must all be considered suspect. Every element in each of these categories must be micro-segmented with advanced threat prevention, be covered by effective user-access policies, provide clear oversight of security events, and be straightforward enough to operate with limited IT/security staffs.

Consolidated security architecture makes zero trust doable

In the past, as security professionals at tech companies discovered new threats, their strategy was to find the "best-in-class" security solution for each threat. The result was a patchwork of point solutions that could take 60 or more different security engines to fully secure IT environments at today's tech companies. Given this, using point solutions to establish real zero trust is complex end-to-end from sourcing, to deployment of incompatible technologies, to managing and administering solutions separately through a bewildering maze of user interfaces.

[9] "Fact Sheet: Biden Administration and Private Sector Leaders Announce Ambitious to Bolster Nation's Cybersecurity," U.S. White House, August 25, 2021

A consolidated security architecture is the realistic way to establish zero trust. In sourcing, it provides —on-demand—all of the security controls needed to microsegment each element and establish user access policies from a single source. All security engines are purpose-built to be mutually compatible, which simplifies deployment.

Likewise, security staff monitors, manages, and administers all security engines through a single interface, which reduces staff workloads while increasing accuracy. The interface's common environment makes staff training highly repeatable across locations. In addition, using a consolidated security architecture provides seamless security that shares threat information among security controls across data centers, cloud, SaaS, remote workers, mobile devices, endpoints, networks and other infrastructure.

Conclusion

The avalanche of cyber threats to tech companies are more sophisticated than ever. Now is the time to fully assess your organization's ability to withstand elevated attack variants that can evade organizations lacking in real prevention capabilities.

To learn more about best practices to protect against supply chain attacks, go to this webpage.

For information on zero trust security through a consolidated infrastructure approach, visit this page.

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