Check Point®
SOFTWARE TECHNOLOGIES LTD

SECURE YOUR EVERYTHING™

SECURITY IMPLICATIONS OF WEAKENED SUPPLY CHAINS

Introduction: Predators instinctively hunt weakened prey

As in the wild, threat actors in the cyber world target vulnerable organizations. Such is the recent turmoil surrounding pandemic-induced supply chains that provide goods from raw materials, to finished materials and components, to finished goods. Incapacitated supply chains are currently scrutinized such as the attacks on the maritime industry's operational technology (OT) growing by 900% over the last three years.[1]

Logistics companies, critical to providing transportation, warehousing, maritime ports, and other services to global supply chains, are suffering. For example, 169 industries have been impacted by chip shortages[2] —and climate conditions that have harmed agricultural production are struggling at the supply end.[3] Labor shortages, especially in the trucking industry, are causing inventory deliveries to back up despite less inventory in the pipeline. With top management focused on these issues, the $100 billion shipping industry has become a prime target for ransomware attacks.[4]

What can be done to protect critical supply-chain infrastructure against costly ransomware and other types of threat-induced stoppages? The answer starts with understanding the problem.

[1] Anon, Maritime Security Incidents: Disruptive Cyber-attack Cripples Port Facility, Mission Secure, Mission Secure, as viewed on August, 26,2021. https://www.missionsecure.com/blog/disruptive-cyber-attack-cripples-port-facility

[2] Andrew Lisa , 4 Critical Industries Affected by the Chip Shortage, GoBanking Rates, Aug 26, 2021. https://www.gobankingrates.com/money/economy/4-critical-industries-affected-by-chip-shortage/

[3] Rob Quinn, Drought Is Hitting Corn, Wheat Production Hard, Newser, Aug 24, 2021, https://www.newser.com/story/310202/crop-inventories-fall-as-drought-grips-us.html

[4] Kevin Collier. The shipping supply chain is stressed from Covid. That makes it ripe for hackers., NBC News, Aug. 19, 2021. https://www.nbcnews.com/tech/security/ransomware-hackers-hit-us-supply-chain-experts-warn-rcna1718

Out of the almost 2,600 victims listed on ransomware data leak sites, 740 of them were named in Q2 2021, representing a 47% increase compared to Q1.[5]

Ransomware

Ransomware is not new. It uses malware to infect a victim's IT devices and networks. Once activated, ransomware encrypts the victim's files and drives that store mission-critical software and data. Such exploits lock the victim out of their systems and data until an extortion payment is paid and, if the transaction does go well, the attacker(s) give the victim a key to unlock the encrypted files and drives.

Although ransomware and other types of malware can enter an IT environment through many vectors, threat actors have traditionally gained first access through an endpoint device, then move laterally to traverse the network, infecting many other systems. Ransomware has now evolved into a triple extortion threat: locking up files needed to operate, exposing sensitive data, and inflicting collateral damage to the victim's customers and partners.[6] This last outcome is indicative of the outbreak of ransomware attacks in 2021.

[5] "740 ransomware victims named on data leak sites in Q2: report," By Jonathan Greig, ZDNet, July 22, 2021
[6] Charlie Osborne Black Hat: Enterprise players face 'one-two-punch' extortion in ransomware attacks, ZDNet, August 5, 2021

> “ If I had to use a paper manifest—if I had to walk over to a crane operator who wasn’t assisted by a computer in some way, if it wasn’t all being tracked by barcodes and scanners—it would take excruciatingly long to load those ships.” [7]

Logistics Vulnerabilities

Today’s supply-chain logistics relies heavily on the flow of information at every step to coordinate, track, and pay for the movement of goods both within an organization and among the many other organizations linked in the chain. In addition to the high integration among stakeholders, logistic organizations are highly automated as with fully robotic maritime ports, or in the process of becoming autonomous like long-haul trucking.

Supply-chain automation and automated operating technologies means the supply chain is built on a mass of vulnerable systems. The 3rd-party software systems that integrate the supply chain, when compromised by threat actors, can spread malware like ransomware through routine software updates and patches to large numbers of customers. This type of attack that compromises a software supply chain is called a “supply chain attack,” however all industries are susceptible.

Furthermore, operating technology (OT) that runs machinery is not created with cyber security in mind. Now that OT is integrated with IT, attackers can access OT software vulnerabilities via the Internet. Compromised OT systems can let attackers install ransomware, change cargo movements, disrupt operations, damage equipment and create safety risks.[8] Due to the great complexity of IT in the supply chain, the answer for cyber security professionals is realize a comprehensive consolidated security architecture.

[7] “The shipping supply chain is stressed from COVID. That makes it ripe for hackers,” by Kevin Collier, NBC News, August 19, 2021

[8] PORT FACILITY CYBERSECURITY RISKS INFOGRAPHIC, CISA, as viewed on August 25, 2021. https://www.cisa.gov/publication/port-facility-cybersecurity-risks

Consolidated security architecture provides a practical advantage

When you look at the systems used for automatic identification, EDI, warehousing, GPS, robotics, and other supply-chain integration as well as standard business infrastructure including data centers, cloud, SaaS, endpoints and mobile devices, experts estimate that 60 or more different cyber security engines are required to secure supply-chain organizations against today's sophisticated cyberattacks. At today's level of technology complexity, using a patchwork of standalone point solutions to provide security becomes impractical. From having to source technology from 60 companies, to managing and administering cyber security through the same number of user interfaces, and having multiple points of contact for support—for solutions that are not built to be compatible—having full security coverage based on point solutions is practically unworkable.

Instead, using a consolidated security architecture that delivers advanced threat prevention to the complete environment streamlines the practice of cyber security end-to-end: from single-source purchasing, to managing and administering all controls through one interface, to having a single point of tech support.

> "Ultimately, a consolidated solution will improve security by increasing visibility to threats and leveraging threat intelligence across all enforcement points. It's clear that we have to build things a little differently for the world today." [9]

[9] "Why consolidating your cybersecurity makes it stronger," by Cindy Baker, IT World Canada, June 17, 2021

When looking at unified cyber security, it is critical to ensure that it provides dedicated protection against today's greatest threat, which is ransomware. This should include advanced threat prevention to stop malware such as ransomware outside the environment. In addition, effective ransomware protection should include anti-bot, which stops ransomware from communicating with the attacker's communication and control (C&C) server. Ransomware protection should also include file backups as a third line of defense. Furthermore, a security architecture should incorporate artificial intelligence in both advanced threat prevention and as an aid to simplify management and administration.

As critical infrastructure, the world's supply chain must keep goods flowing to businesses and consumers. Consolidated security architecture enhanced with AI is the best path to making this happen.

To learn more about ransomware prevention, visit this page.

To realize the benefits of a consolidated security architecture, get started here.

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