CLCT
ARTIFICIAL INTELLIGENCE

Ransomware & Supply Chain Attacks

Ransomware Utilizing Supply Chain Attacks

The use of ransomware by threat actors is on the rise globally. Ransomware is a type of malicious code that encrypts a victim's files in order to demand a ransom payment to restore access. Supply chain attacks are a type of cyber attack when threat actors infiltrate a software or IT service supply chain to spread malicious code to connected users (typically other customers) or infiltrate other connected systems.

In December 2020, SolarWinds was targeted by threat actors believed to be connected to the SVR, the Russian intelligence service. The attack was effectuated by threat actors surreptitiously embedding malware to a SolarWinds update package and victims later installing the infected update software to their SolarWinds systems. Once the infected update package was installed, customers' networks were compromised, and threat actors could remotely monitor and deploy additional malicious payloads for further cyber intrusion operations without detection.

More recently, in July 2021, Kaseya VSA experienced a sophisticated supply chain attack that encrypted the files of thousands of customers. On July 2, 2021, at around 11 AM EST, several Kaseya VSA servers were used by threat actors to deploy ransomware. Threat actors exploited an arbitrary file upload (allowing threat actors to upload malicious code to a system) and code injection vulnerability (allowing threat actors to inject malicious code into a program that executes the malicious code) in Kaseya VSA software to upload and execute malicious code while bypassing security protocols. The malicious exploits enabled threat actors to take control of the compromised Kaseya VSA servers. They were also able to take direct control of thousands of business customers' IT systems. Threat actors installed ransomware on all accessible systems, which disrupted business operations among managed service provider customers.

Helpful Resources

Ransomware: Everything You Need to Know, CROWDSTRIKE, https://www.crowdstrike.com/cybersecurity-101/ransomware/.

Ransomware as a Service (RAAS) Explained, CROWDSTRIKE, https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/.

Dina Temple-Raston, *A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack*, NPR (Apr. 16, 2021), https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.

Chris Mellor, *Kaseya VSA Vulnerability Opens a Thousand-plus Business Doors to Ransomware*, BLOCKS & FILES (July 4, 2021), https://blocksandfiles.com/2021/07/04/kaseya-vsa-vulnerability-opens-1000-plus-business-doors-to-let-in-ransomware/.

Cryptocurrency

Threat actors mostly demand ransom payment by cryptocurrency because, unlike traditional payment modes, these transactions cannot be canceled or reversed. Additionally, cryptocurrency transactions allow threat actors to maintain their anonymity without fear of their identity being revealed. The Federal Bureau of Investigation recommends not making ransom payments. However, whether or not to pay a ransom is a complex decision involving many factors, including whether the costs of paying the ransom may be significantly less than attempting to restore the files through other means. The possibility always exists that, even with ransom payment, threat actors do not restore access to one’s files.

Helpful Resources

PRE-DRAFT Call for Comments: Supply Chain Risk Management Practices for Federal Information Systems and Organizations, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (Feb. 4, 2020), https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/archive/2020-02-04.

Cyber Supply Chain Risk Management Practices for Systems and Organizations, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (Apr. 2021), https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/draft.

Supply Chain Risk Management, THE NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER, https://www.dni.gov/index.php/ncsc-what-we-do/ncsc-supply-chain-threats.

Mitigation Practices

Preparation of an incident response plan for a ransomware attack is an important tool in minimizing the damage of a ransomware attack. Anticipate experiencing a ransomware attack and needing to purge and completely restore entire systems. The incident response plan should be printed out, as well as maintained outside of a company’s network where files may be encrypted. It is important to maintain an up-to-date, disconnected backup of the full system where threat actors cannot access file shares. For individuals, this backup should include the full system, not just work files.

Helpful Resources

defense-in-depth, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, https://csrc.nist.gov/glossary/term/defense_in_depth.

Yev, *The 3-2-1 Backup Strategy*, BACKBLAZE (Apr. 7, 2015), https://www.backblaze.com/blog/the-3-2-1-backup-strategy/.

Federal Cyber Resources

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, https://www.cisa.gov/.

What We Investigate: The Cyber Threat, Federal Bureau of Investigation, https://www.fbi.gov/investigate/cyber.

Cyber Hygiene Services, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, https://www.cisa.gov/cyber-hygiene-services.

Scams and Safety: Ransomware, FEDERAL BUREAU OF INVESTIGATION, https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware.

Stop Ransomware, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, https://www.cisa.gov/stopransomware.