Sang Hwa Lee

INST 346

December 11, 2022

Homework - 03: Exploring the Security Ecosystem of a Cyber Incident

Causes and Progression of Incident

The Kaseya cyber incident occurred in July of 2021. The attack was on Kaseya, which is an American software company that manages information systems and infrastructure. The ransomware attack targeted the vulnerability of Kaseya's Virtual System Administrator (VSA) software, bypassed authentication, and attacked managed service providers (MSPs) and their customers.

Technical Aspects of Networked Systems

The attack took advantage of Kaseya's network and system. First, the attacker, the ransomware gang called REvil, gained access to Kaseya's VSA and SaaS platforms. The attacker then used weaknesses on the systems to make encryptions. This impacted the MSPs and the MSP customers. This incident made possible the transport layer of the OSI model. The transport layer ensures complete and reliable delivery of data packets. Therefore, Kaseya's program with malicious code is indiscriminately sent to many customers through this transmission layer.

Aspects of Human Behavior

A few months before the incident, Dutch Institute for Vulnerability Disclosure researchers identified seven vulnerabilities of the VSA. Kaseya was able to patch four of them, but three remained towards the end of the 90-day disclosure deadline, and the attackers exploited one of these, spreading malware to many customers around the world.

The human behavior that can be seen here is how the researchers warned the company of the vulnerabilities and how the people of Kaseya attempted to solve the problems as best as possible in the time available. However, the human limitations can also be seen here when they did not have enough manpower to solve all of the vulnerabilities quickly enough.

Also, after the attack, the employees shut down its cloud and SaaS (Software as a Service) servers and issued a security advisory. However, another human limitation can be seen because it was up to the customers to check and follow the security advisory. Kaseya had no control over how and when they would do so, which made this cyber incident grow as much as it did.

Interventions Taken to Address Problem

To address the problem, the company went through with several short-term actions to reduce the impact of the attack, as well as some long-term fixes. First, the company shut down its cloud. Then, it issued a security advisory notification to clients to shut down the VSA server, and the company additionally shut down the SaaS servers. The company also advised clients to not click any links. Lastly, it started to restore its SaaS infrastructure through distributing hacking detecting tools and patches.

As for long timer, more permanent fixes, the company released a statement to its MSP clients and customers. It recommended the clients to back up and separate from the company's network to be able to easily search for and save information. It stated that it would switch to a system processor that would manage manual patches and include MFA (multi-factor authentication) in order to strengthen security. Finally, it provided further patches to solve additional functional problems and bugs.

Attack's Outcome

Kaseya first claimed that SaaS customers were never at risk, and that they estimated fewer than 40 clients were affected around the world. However, although a small number of Kaseya's clients may have been directly impacted, these MSPs have other customers further down the chain that would have been affected. This means that thousands of companies may have been impacted. For example, the incident affected a Norwegian financial software developer called Visma, which managed parts of a Swedish supermarket chain called Coop. Because of the attack, Coop had to close about 800 stores because the cash registers were unavailable for use. They had to rebuild their systems after waiting for an update from Kaseya.

The attacker of this cyber incident was the REvil Russia-based ransomware gang, who claimed to have encrypted many systems through this incident. They originally demanded $70 million for a decryption key. Kaseya notified the US law enforcement and cybersecurity organizations, including the FBI and CISA. Additionally, Biden warned Putin about acting on this issue before the USA will have to take action. After this, the attacker's websites were taken down. However, no decryption key has been provided and is now working on recovery plans.

Changes Needed for the Future

There are several ways that changes can be made to prevent or minimize the impact of a similar attack in the future. In technical aspects, the end point security should be strengthened. When malicious code is invaded, EDR checks whether it is malicious through judgment like a regular vaccine, and further checks whether it is malicious by identifying the structural characteristics of the file through AI. If malicious code that cannot be blocked is executed, it is blocked or defended by determining whether it is malicious through an AI engine that determines malicious code abnormal behavior.

This detected malware can isolate files within the endpoint PC and, if necessary, isolate the PC on the network to prevent further infection from other terminals. Security data can be checked in real time by using an EDR solution for the end point. Also, data about incoming threats can be collected automatically by this mechanism to protect the system from ransomware attacks.

In human behavior, the clients would need to install the most updated patches. Additionally, they could use systems that monitor network traffic regarding security. Clients should not open suspicious files. They could even block pop-ups from untrusted websites. Using security solutions could detect and eliminate ransomware threats. Clients could also keep back up files, preferably offline rather than online ones that could still be subject to hackers' threats. Finally, the human behavior on the company's side should have been quicker and more efficient to find solutions to problems that others warned them about.

Works Cited

CISA. "Kaseya Ransomware Attack: Guidance for Affected Msps and Their Customers." *CISA*, 2021, https://www.cisa.gov/uscert/kaseya-ransomware-attack.

Kaseya. "Incident Overview & Technical Details – Kaseya." *Kaseya*, 2021, https://helpdesk.kaseya.com/hc/en-gb/articles/4403584098961-Incident-Overview-Technical-Details.

Newman, Lily Hay. "The Unfixed Flaw at the Heart of Revil's Ransomware Spree." *Wired*, Conde Nast, 8 July 2021, https://www.wired.com/story/revil-ransomware-kaseya-flaw-fix-disclosure-april/.

Osborne, Charlie. "Updated Kaseya Ransomware Attack FAQ: What We Know Now." *ZDNET*, 2021, https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/.

Wikipedia. "Kaseya VSA Ransomware Attack." *Wikipedia*, Wikimedia Foundation, 17 Nov. 2022, https://en.wikipedia.org/wiki/Kaseya_VSA_ransomware_attack.

Won , Byeong-cheol. "What Were the 'Cyber Security Incidents/Accidents' That Plagued 2021?" *Security News*, 2021, https://www.boannews.com/media/view.asp?idx=103733.