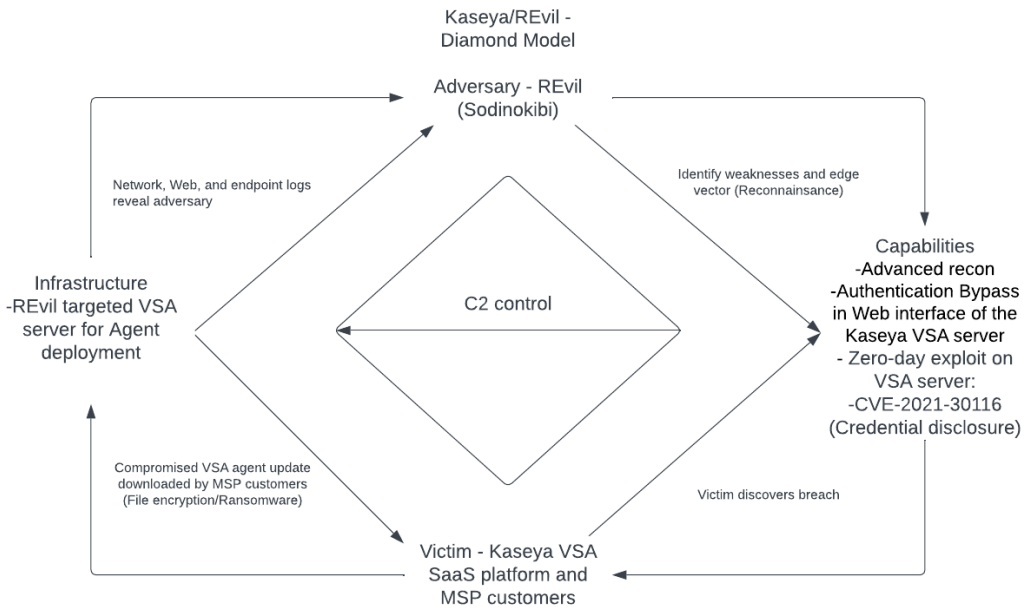
Diamond model and Policy assessment - Kaseya Ransomware

Andres Alvarez

Introduction

The Kaseya ransomware attack, which occurred in July 2021, was a significant cyber attack that had far-reaching consequences for businesses and organizations worldwide. The attack targeted the VSA software, a remote monitoring and management tool developed by Kaseya, a leading provider of IT management and remote monitoring services. The attack believed to be carried out by the REvil ransomware gang, resulted in widespread disruption and financial losses for businesses that relied on the VSA software for their IT operations. The incident shed light on the evolving and sophisticated tactics of ransomware attacks, the vulnerability of supply chains to cyber threats, and the challenges in dealing with ransomware-as-a-service operations.

In the following sections, we will delve into the details of the Kaseya ransomware attack using the Diamond Model for intrusion analysis. We will analyze the adversary, victim, infrastructure, and capability involved in the attack and discuss the social-political and technology meta-features of the attack. Finally, we will provide a policy assessment and recommendations for addressing this problem, considering the insights gained from applying the Diamond Model for intrusion analysis.



Adversary

REvil, also known as Sodinokibi, is the threat actor group behind Kaseya's ransomware attack. The REvil group is known for its ransomware-as-a-service (RaaS) model in exchange for a percentage of the ransom money collected in the attack. REvil is known for being linked with several other high-profile cases of ransomware.

REvil is known for using advanced techniques and tactics in its attacks, including encryption, data theft, and pressure tactics to extort ransom payments from victims. The group primarily targets large businesses and organizations seeking maximum financial gain from their attacks. They have been known to demand large ransom payments in Bitcoin, often reaching millions of dollars, and have a reputation for being ruthless in their attacks and negotiations with victims.

The REvil ransomware gang is known to exploit vulnerabilities in software and systems to gain unauthorized access and deploy ransomware. In the Kaseya attack, the group used a zero-day vulnerability in the VSA software, which had not been patched or addressed by Kaseya. This highlights the capabilities and technical expertise of the REvil ransomware gang and their ability to identify and exploit vulnerabilities in widely used software for their attacks.

The group is known for utilizing advanced infrastructure to execute the attacks, including command-and-control servers, crypto wallets, obfuscation, hijacking, and other tools and techniques to administer their campaigns. Communication channels with the victim involve online forums, dark web marketplaces, and gaming sites. They pressure their victims into paying the ransom by threatening to publish sensitive information and increasing it over time.

REvil operates in countries with no extradition treaty with the United States, making it challenging for law enforcement to identify and prosecute the individuals executing the campaigns under the REvil banner. The group has a significant online presence who are actively communicating with the media and victims through various channels and using cryptocurrency as their currency to increase layers of complexity to the attribution process of the investigation.

Victim

Kaseya VSA software is used to manage its IT systems and is used by businesses worldwide. The attacks impacted around 800 to 1,500 Kaseya customers dependent on the VSA software for all their IT infrastructure, including remote monitoring, patch management, and backup services.

All the impacted customers or victims faced challenges, including the loss of mission-critical systems and data, which directly impacted the ability of businesses to serve the needs of their customers resulting in availability and reputational damage. With the files encrypted, the

attackers demanded the ransom payment in exchange for a universal decryptor. Many affected businesses faced the difficult decision of whether to pay the ransom or not as they weighed the potential financial loss from downtime and data loss against the risks associated with engaging with cyber criminals.

The attack also had broader impacts beyond Kaseya's customers. Many businesses that relied on Kaseya's customers for services, such as managed IT services providers (MSPs), also faced disruptions in their operations. This cascading effect of the attack highlighted the interconnected nature of the global supply chain and the potential ripple effects of cyber attacks across multiple sectors and industries.

Infrastructure

The attackers identified a zero-day vulnerability (CVE-2021-30116) for compromising the VSA SaaS platform, which is responsible for the agent updates. They managed to inject their malicious payload into Kaseya’s MSP service or, in other words, the Kaseya Supply chain. Customers started downloading the malicious payload thinking it was a legitimate Agent update pushed by Kaseya.

Several infrastructure components were affected by the breach. Kaseya’s IR team identified Web, Endpoint, and network logs that indicated a potential compromise of the MSP supply chain.

IPs accessing VSA servers remotely(Network Logs):
-35.226.94[.]113
-161.35.239[.]148
-162.253.124[.]162

Files used as part of the encryptor deployment(Endpoint logs):

Filename	**MD5 Hash**	**Function**
cert.exe	N/A – Legitimate File with random string appended	Legit certutil.exe Utility
agent.crt	939aae3cc456de8964cb182c75a5f8cc	Encoded malicious content
agent.exe	561cffbaba71a6e8cc1cdceda990ead4	Decoded contents of agent.crt

mpsvc.dll	a47cf00aedf769d60d58bfe00c0b5421	Ransomware Payload

IIS access logs of compromised VSA server:

POST /dl.asp curl/7.69.1
GET /done.asp curl/7.69.1
POST /cgi-bin/KUpload.dll curl/7.69.1
GET /done.asp curl/7.69.1
POST /cgi-bin/KUpload.dll curl/7.69.1
POST /userFilterTableRpt.asp curl/7.69.1

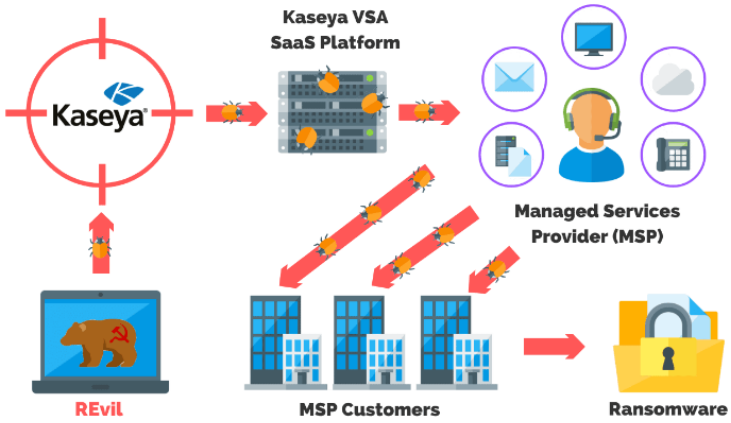
Capability

The attackers could exploit the zero-day vulnerability in the VSA software (CVE-2021-30116) and deploy ransomware on a large scale. They used advanced encryption and data theft techniques to pressure victims into paying for ransomware. They also had access to sophisticated infrastructure to carry out the attack, including command-and-control servers and Bitcoin wallets for ransom payments.

In more technical terms, REvil exploited (CVE-2021-30116) to compromise the Kaseya Software supply chain. Through the compromise of Kaseya's supply chain, REvil could wrap the malware in the platform as being signed by Kaseya, avoiding any type of signature detection and leveraging the trust between the clients and Kaseya to trick users into downloading it.

The failure of critical Business components opens up an opportunity for REvil to leverage that exact capability for monetary demands, usually in the form of cryptocurrency, since it allows for more anonymity and it's considered the standard in ransomware situations.

Image showing the attacks flow/sequence:



[6]

Social-Political meta-feature

The social-political features of the Kaseya ransomware attack refer to the socio-political factors that influenced the attack and its consequences. Several social-political features are worth noting in the case of the Kaseya attack.

First, the campaign concluded with significant economic and operational implications for the victims, including financial loss due to disrupted critical services and reputational damage. The depth to which an attack such as this can disrupt business operations highlights the vital need for robust cyber security measures and effective incident response plans to mitigate impacts in such scenarios.

Secondly, the Kaseya attack had broader geopolitical implications, affecting businesses and organizations globally. The connectivity of the digital world highlights the potential for these attacks to have geopolitical effects and the increased need for government participation in collaborating with the private sector in cyberspace.

The Kaseya attack is another situation that raises attention to the growing threat of ransomware attacks and the need for increased government participation in cyberspace. It sparked discussions on policy responses, regulations, and public-private partnerships to address the growing ransomware problem and protect critical infrastructure.

Technology meta-feature

REvil exploited a zero-day vulnerability in the VSA software to gain unauthorized access to the system to compromise the integrity of the Kaseya Software supply chain. This attack points out the urgent need for effective vulnerability management programs and practices to remediate and discover vulnerabilities that might present an entry vector for other attacks. Using a zero-day vulnerability also emphasizes the importance of placing constant and reliable monitoring control for network, web, and endpoint security.

Secondly, the attackers utilized a sophisticated ransomware-as-a-service (RaaS) model, obtaining the ransomware from a third-party group and deploying it to carry out the attack. This demonstrates the growing trend of ransomware attacks conducted by specialized criminal groups who lease or purchase ransomware from other actors, making attribution and investigation more complex. This also highlights the need for coordinated efforts to disrupt and dismantle ransomware-as-a-service operations.

Policy Assessment and Recommendations

The zero-day exploit in the attack allowed the attackers to deploy ransomware on a large scale. It reflected the need for increased awareness to secure software and implement effective vulnerability management programs, including identifying and patching vulnerabilities in software.

The best level of organization to address this problem is at the industry level (8.5) by adopting best practices for vulnerability management and the development of standards for software security. However, governments and policymakers can also promote more significant investments in cybersecurity and encourage companies to prioritize vulnerability management.

In conclusion, the incident reveals the growing need to proactively identify and remediate software vulnerabilities before being released in the software supply chain and the need for more coordinated cybersecurity collaboration between all stakeholders.

References:

Incident overview & technical details – kaseya. (n.d.). Retrieved April 18, 2023, from https://helpdesk.kaseya.com/hc/en-gb/articles/4403584098961-Incident-Overview-Technical-Details

Viaggiani, F. (n.d.). *All you need to know about kaseya supply chain attack*. Truesec. Retrieved April 18, 2023, from https://www.truesec.com/hub/blog/kaseya-supply-chain-attack-targeting-msps-to-deliver-revil-ransomware

Browning, K. (2021, July 6). *Up to 1,500 businesses could be affected by a cyberattack carried out by a Russian group.* The New York Times. Retrieved April 18, 2023, from https://www.nytimes.com/2021/07/06/technology/kaseya-cyberattack-ransomware-revil.html

Bajak, F. (2021, July 5). *Scale, details of massive Kaseya ransomware attack emerge*. AP NEWS. Retrieved April 18, 2023, from https://apnews.com/article/joe-biden-europe-government-and-politics-technology-business-fc0df4c42f8cd6148bf936ca24bb5cbe

Panettieri, J. (2022, March 11). *Alleged Kaseya Revil ransomware hacker extradited, arraigned*. MSSP Alert. Retrieved April 18, 2023, from https://www.msspalert.com/cybersecurity-breaches-and-attacks/kaseya-rmm-cyberattack-warning/

Allen, J. (2022). *How Did The Kaseya Ransomware Attack Happen?* Retrieved from https://purplesec.us/kaseya-ransomware-attack-explained/. [6]