ENPM686-0201

Samridha Murali

02/14/2022

Current Event 3

Kaseya is a Florida based company that provides IT infrastructure management solutions for Managed Service Providers(MSP), internal IT organisations. Russian hacker organization Revil launched a ransomware attack, demanding payment of $70 million holding more than 1000 companies (kaseya's clients) for ransom. In the hands of the hackers the software turned into a malware distributor, rendering files unreadable, business email unusable, and machine inoperable. Revil gained access to a zero day vulnerability in Kaseya's virtual system administrator (VSA), a popular remote management tool used by more than 35,000 Kaseya clients. Revil organisation compromised the company's update server and released a malicious patch containing a payload named "sadinokibi", which encrypts server and shared folders. The attack was developed in such a way that marware avoids systems using Russian or related languages.

Kasaeya has more than 35,000 clients using VSA software, among them 60 were fully penetrated by this attack. The most affected among them is Swedish supermarket chain Coop, which had to close more than 800 outlets on weekends. It's checkout became unavailable. Swedish media, pharmacy chain Apotek Hjartat and Finnish energy had major problems with payments. 1,500 companies worldwide were affected. It has been revealed that the cyber criminals send two different ransom demands directly to businesses, asking for $50,000 from small businesses and $5 million from large businesses.

MSPs should make sure that the service providers they work with have a robust vulnerability management program in place. Since Kaseya was a trusted software, there might have been no monitoring in place on the ports used by Kaseya's VSA or might have given unrestricted access to ports. So even trusted third party software should not be granted unrestricted access to vulnerable ports, instead follow the principle of least privilege.

References :

1. Anthony Etien, (July 23, 2021) https://www.globalsign.com/en/blog/kaseya-attack-2021-are-ransomware-attacks-inevitable
2. Jeff Stout, (October 04, 2021) https://www.datacenterdynamics.com/en/opinions/lessons-from-the-kaseya-ransomware-attack/
3. Techstalking, (July 3, 2021) https://technostalking.com/tech-facts/ransomware-attack-affects-coop-sj-and-apotek-hjartat/