Current event: FBI withheld keys to REvil Kaseya ransomware attack

Jonathan Lam

09/22/21

Two months ago, while working at an internship at my makeshift work-from-home office, my mom (also WFH in the next room over) sighed in frustration. When asked, she said that her work systems were down due to a ransomware attack. Since it was work-from-home, all the remote work services were shut down and operations at her office stopped for a few days. Luckily, the company was able to restore their systems from a backup, and all of the employees had to bring in their personal devices to be scanned for malware.

It turns out that this was part of a large-scale ransomware attack on a IT firm called Kaseya, which affected a number of their small- to medium-sized clients [3]. The attack was carried out by a Russian "Ransomware-as-a-Service" group called REvil, which also carried out the ransomware attack on JBS, the world's largest meat supplier, in June. Kaseya creates VSA software, "a unified remote-monitoring and management tool for handling networks and endpoints." This software is high-value for an attacker because all the devices that are managed by this software trust the commands sent out by the device (the Kaseya installation folders must be excluded from antimalware/firewalls for the program to work). As a result, after performing a zero-day attack on the server, malicious commands that were sent to managed devices were not checked by malware and were able to perform the attack. Sophos published a detailed description of the attack [1].

This was a fairly high-level attack (Sophos notes that zero-day supply-chain attacks are rare and sophisticated) so it is not the fault of poor security practices (such as bad password practices). Sophos notes that the antimalware evasion that was performed by the attack (which targets Microsoft Defender) would have been detected by its own antimalware software, as would the certificate that was injected as part of the attack. They also note that this is the

In a high-level technical attack like this, most of the methods to mitigate the fallout is due to roundabout measures. The saving grace for a number of companies (such as my mom's company) was the use of backups – this cannot protect against zero-day exploits or prevent ransomware attacks that exfiltrate data (which this attack does not), but it allows a company to restore operations. Shutting down servers as soon as an attack is discovered can mitigate ransomware spread. Installing more advanced antimalware software, such as Sophos's antimalware or Intercept X's cryptoransomware protection software, would have detected these attacks (as Sophos notes).

Politics is clearly at play here as well. REvil is not the first RaaS group, and they operate with apparent impunity in Russia. They have attacked multiple international corporations, including several large scale attacks involving U.S. corporations. The Washington Post article notes that "The White House has made fighting ransomware a priority, and President Biden has urged Russian President Vladimir Putin to rein in ransomware criminals operating out of Russia." Threat of punitive action by the government would likely be a deterring factor.

A highly related issue of ethics arose three weeks (19 days) later when the FBI released a global decryption key for Kaseya [2]. It turns out that they had obtained from the REvil servers much earlier, but had hoped to "was planning to carry out an operation to disrupt the hackers, a group known as REvil, and the bureau did not want to tip them off" [2]. However, they did not get a chance to because REvil went offline in mid-July, after which they revealed their knowledge of the key to Kaseya. The ethical issue is the tradeoff between helping victim businesses (by releasing the key immediately) or potentially dealing much damage to the attackers (by holding the key and performing a counterattack). The FBI had to constantly weigh the damage dealt by both options.

References

[1] Mark et al. Loman. *Independence Day: REvil uses supply chain exploit to attack hundreds of businesses.* July 2021. URL: `https://news.sophos.com/en-us/2021/07/04/independence-day-revil-uses-supply-chain-exploit-to-attack-hundreds-of-businesses/` (visited on 09/22/2021).

[2] Ellen Nakashima and Rachel Lerman. *FBI held back ransomware decryption key from businesses to run operation targeting hackers.* Sept. 2021. URL: `https://www.washingtonpost.com/national-security/`

ransomware-fbi-revil-decryption-key/2021/09/21/4a9417d0-f15f-11eb-a452-4da5fe48582d_story.html (visited on 09/22/2021).

[3] Charlie Osborne. *Updated Kaseya ransomware attack FAQ: What we know now.* July 2021. URL: https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/ (visited on 09/22/2021).