CASE STUDY

CYBERSECURITY

2.4.2 - Ransomware

FBI Response to REvil Ransomware

Article:

Ransomware victims panicked while FBI secretly held REvil decryption key

SEP 21, 2021

Retrieved from: https://arstechnica.com/information-technology/2021/09/ransomware-victims-panicked-while-fbi-secretly-held-revil-decryption-key/

Source: Ars Technica
Author: Tim De Chant

Up to 1,500 companies were ensnared in the July attacks.

For three weeks during the REvil ransomware attack this summer, the FBI secretly withheld the key that would have decrypted data and computers on up to 1,500 networks, including those run by hospitals, schools, and businesses.

The FBI had penetrated the REvil gang's servers to obtain the key, but after discussing it with other agencies, the bureau decided to wait before sending it to victims for fear of tipping off the criminals, The Washington Post reports. The FBI hadn't wanted to tip-off the REvil gang and had hoped to take down their operations, sources told the Post.

Kaseya gets master decryptor to help customers still suffering from REvil attack

Instead, REvil went dark on July 13 before the FBI could step in. For reasons that haven't been explained, the FBI didn't cough up the key until July 21.

"We make the decisions as a group, not unilaterally," FBI Director Christopher Wray told Congress on Tuesday. "These are complex… decisions, designed to create maximum impact, and that takes time in going against adversaries where we have to marshal resources not just around the country but all over the world."

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

Years of disruption

REvil has a long history of using high-pressure tactics to extort victims. The Russia-based gang first appeared in 2019, and it was on a tear earlier this year. In March, the group hacked a celebrity law firm that represented U2, Madonna, and Lady Gaga, demanding $21 million. When the law firm balked, REvil doubled the demand and released some of Lady Gaga's files. In April, the gang stole data from contract manufacturer Quanta Computer, publishing details of two Apple products. Then in May, it shut down Colonial Pipeline's operations from New Jersey to Texas, leading to fuel shortages.

FURTHER READING

Attack on meat supplier came from REvil, ransomware's most cutthroat gang

The group resurfaced this summer when it disrupted operations at Brazil-based meat processor JBS and caused several plants in the US, Canada, and Australia to shut down. It struck again when it exploited a zero-day in remote management tools made by Kaseya, a Florida-based IT firm. The hole in the company's VSA product gave REvil access to 54 service providers who manage networks for up to 1,500 businesses and other organizations.

Grocery stores in Sweden, town halls in Maryland, schools in New Zealand, and a hospital in Romania were all affected by the attack. Coop, the Swedish grocery store chain, closed around 700 stores and took some six days to reopen. Other victims spent weeks restoring their systems.

They're back

Last Thursday, cybersecurity firm Bitdefender published a universal decryptor tool for networks and computers encrypted before REvil's hibernation began on July 13. About 250 victims have used the tool so far, a Bitdefender executive said. The key that made the tool possible reportedly came from a law enforcement agency—but not the FBI.

Despite the FBI's efforts to take it down, REvil is back this month with a new string of attacks, ensnaring at least eight new victims, the Post reported. The Bitdefender tool, however, won't work for the new victims, a sign that REvil has retooled its operations after a brief downtime.

Summary

The REvil ransomware group, based out of Russia, affected over 1,500 different networks in the summer of 2021 asking for ransoms. The FBI had uncovered the key to decrypt all the networks and give the data back to the victims, which included schools and hospitals, but instead decided to not release the key so REvil wouldn't know they had it. A few weeks later, Bitdefender was able to create a decryptor tool that was able to decrypt the ransomware for the victims.

Questions

- Should the FBI have withheld the keys to decrypt the ransomware from other organizations?
- The FBI's mission states, "Protect the American people", do you feel that they lived up to their mission in this case?
- The FBI didn't want to tip off REvil that they had discovered the key to their ransomware, do you feel this is ok if it helps stop more ransomware attacks in the future?
- Should the FBI be held liable for any ransoms that were paid out while they were withholding the decryption key?

Further Study

[1] Wikipedia's article on the REvil ransomware group: https://en.wikipedia.org/wiki/REvil

[2] Reuters article on multiple countries helping to take REvil down: https://www.reuters.com/technology/exclusive-governments-turn-tables-ransomware-gang-revil-by-pushing-it-offline-2021-10-21/

[3] Bitdefenders announcement with the universal decryptor: https://www.bitdefender.com/blog/labs/bitdefender-offers-free-universal-decryptor-for-revil-sodinokibi-ransomware/