Avaddon ransomware fixes flaw allowing free decryption

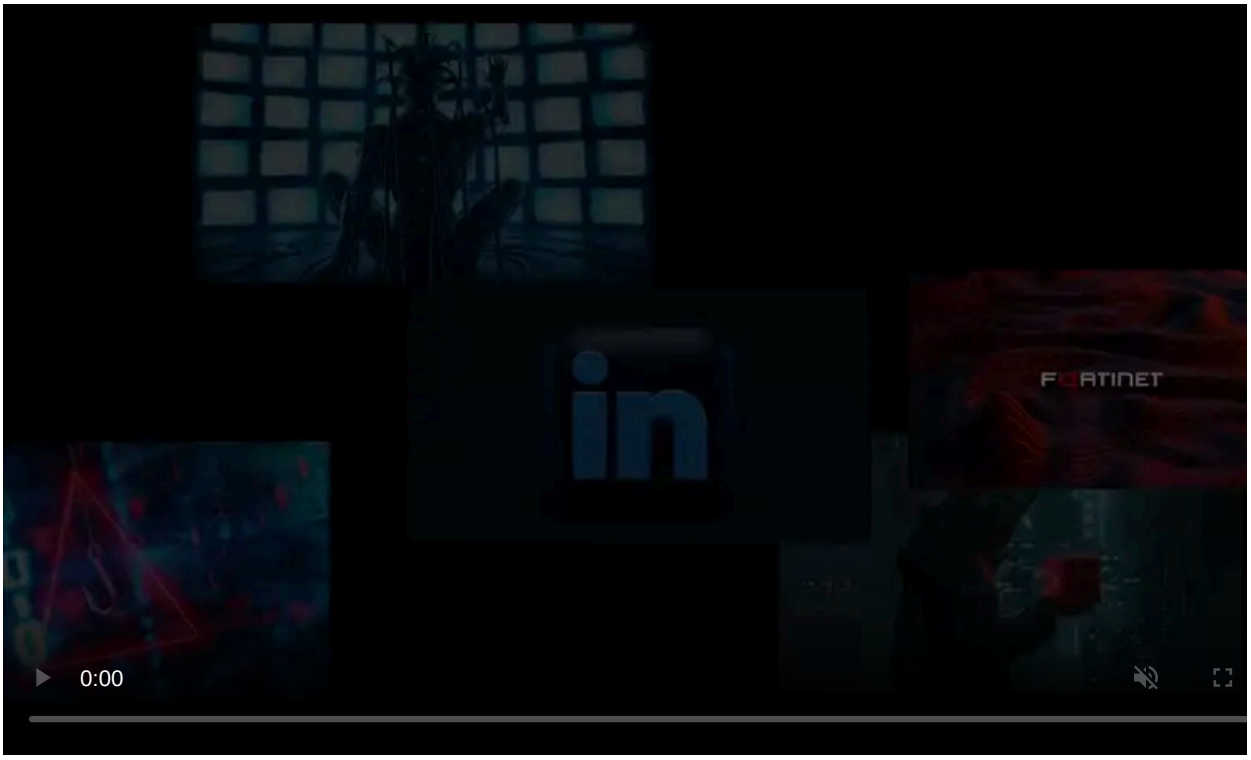
By Lawrence Abrams

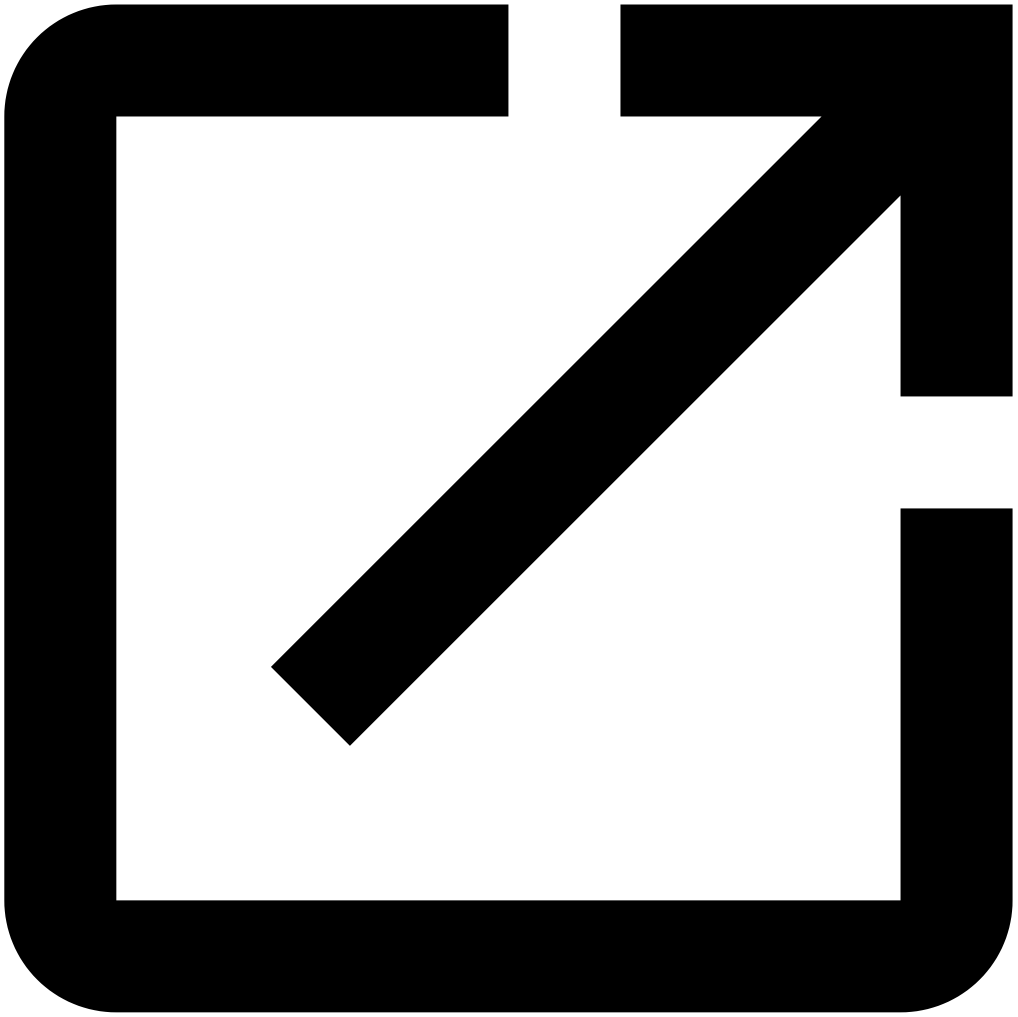
Published: 2021-02-11 · Archived: 2026-04-05 19:12:45 UTC

The Avaddon ransomware gang has fixed a bug that let victims recover their files without paying the ransom. The flaw came to light after a security researcher exploited it to create a decryptor.

On Tuesday, Javier Yuste, a Ph.D. student at Rey Juan Carlos University, published a decryptor for the Avaddon Ransomware on his GitHub page and released a report describing the flaw through ArXiv.

According to Yuste's research, when the Avaddon ransomware encrypts a device, it creates a unique AES256 encryption session key used to encrypt and decrypt the files.


0:00



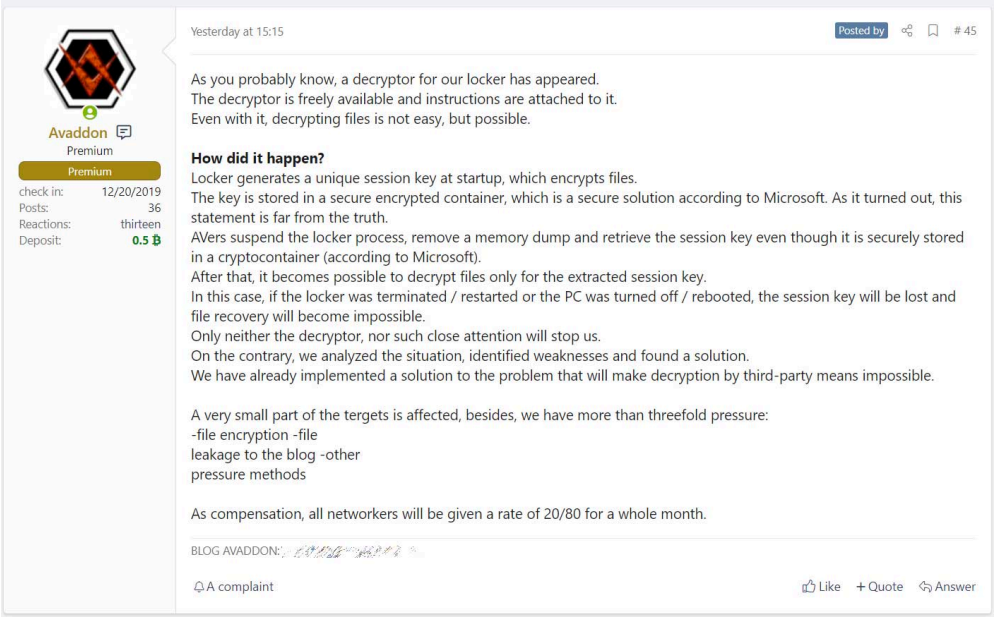
A flaw in how the ransomware clears this key, though, allowed Yuste to create a decryptor that retrieves the key from memory as long as the computer has not been shut down since being encrypted.

Ransomware dev fixes encryption flaw

As first reported by ZDnet, one day after the decryptor was released, the Avaddon ransomware developer posted to a hacker forum that they had fixed the flaw.

"Only neither the decryptor, nor such close atention will stop us. On the contrary, we analyzed the situation, identified weaknesses and found a solution."

"We have already implemented a solution to the problem that will make decryption by third-party means impossible," the Avaddon developer wrote in a forum post.



Post by the ransomware dev on a hacker forum

To compensate the operation's affiliates whose victims may have received free decryption, the ransomware developer increased affiliates' revenue share to 80%. The normal revenue share for Avaddon affiliates is 65-75%, depending on how many victims they generate.

Threat actors read the same security news as you

It is important to remember that ransomware and threat actors follow the same Twitter and news feeds that you do.

In the past, ransomware operations such as GandCrab and Maze routinely taunted antivirus companies, researchers, and even BleepingComputer after news or research was published.

One threat actor went as far as creating a ransomware called 'Fabiansomware' after the ransomware expert Fabian Wosar.

Fabiansomeware Ransomware

BleepingComputer has also been contacted numerous times by threat actors who wanted to clarify a point in an article or tell us further information.

Thus, it is always essential to assume that any ransomware flaws openly disclosed will also be seen by a threat actor.

We have seen this historically with CryptoDefense, DarkSide, and now Avaddon.

For this reason, most ransomware experts do not think security companies and researchers should publish encryption flaws or decryptors as it allows the threat actors to fix the bugs in their malware.

Instead, it is suggested that those who create a decryptor reach out to antivirus companies, incident response firms, law enforcement, and communities like BleepingComputer who commonly help ransomware victims.

These decryptors can then be used by these organizations to privately help victims, while at the same time not publicly revealing to the ransomware developers how to fix their flaws.

Source: https://www.bleepingcomputer.com/news/security/avaddon-ransomware-fixes-flaw-allowing-free-decryption/