
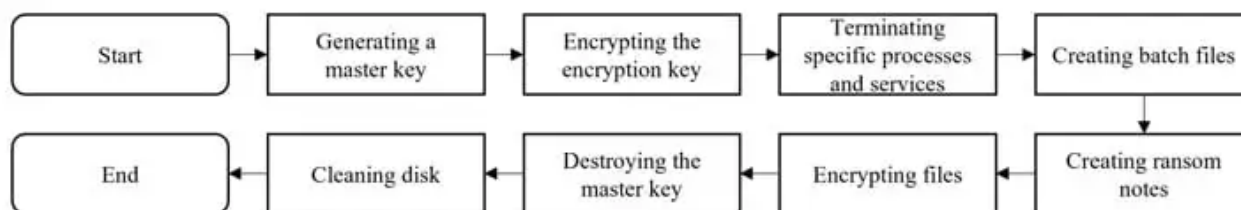


A flaw in the encryption algorithm of Hive Ransomware allows retrieving encrypted files

By Pierluigi Paganini

Published: 2022-02-21 · Archived: 2026-04-05 23:00:59 UTC

 [Pierluigi Paganini](#)  February 21, 2022



Entire encryption process of Hive ransomware

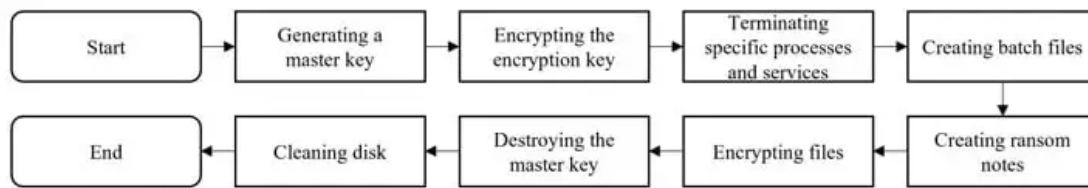
Researchers discovered a flaw in the encryption algorithm used by Hive ransomware that allowed them to decrypt data.

Researchers discovered a flaw in the encryption algorithm used by [Hive ransomware](#) that allowed them to decrypt data without knowing the private key used by the gang to encrypt files.

The Hive ransomware operation has been active since June 2021, it provides Ransomware-as-a-Service Hive and adopts a double-extortion model threatening to publish data stolen from the victims on their leak site (HiveLeaks). In April 2021, the Federal Bureau of Investigation (FBI) has [released a flash alert](#) on the [Hive ransomware](#) attacks that includes technical details and indicators of compromise associated with the operations of the gang. According to a [report](#) published by blockchain analytics company Chainalysis, the Hive ransomware is one of the top 10 ransomware strains by revenue in 2021. The group used a variety of attack methods, including malspam campaigns, vulnerable RDP servers, and compromised VPN credentials.

“Hive ransomware uses a hybrid encryption scheme, but uses its own symmetric cipher to encrypt files. We were able to recover the master key for generating the file encryption key without the attacker’s private key, by using a cryptographic vulnerability identified through analysis. As a result of our experiments, encrypted files were successfully decrypted using the recovered master key based on our mechanism.” reads the [paper](#) published by researchers from Kookmin University (South Korea). “To the best of our knowledge, this is the first successful attempt at decrypting the Hive ransomware. We experimentally demonstrated that more than 95% of the keys used for encryption could be recovered using the method we suggested.”

The technique devised by the team of academics was able to recover more than 95% of the keys used for the encryption process that is represented in the following image:



Entire encryption process of Hive ransomware

The experts detailed the process used by Hive ransomware to generate and store master key for victim files. The ransomware generates 10MiB of random data, and uses it as a master key. The malware extracted from a specific offset of the master key 1MiB and 1KiB of data for each file to be encrypted and uses as a keystream. The offset is stored in the encrypted file name of each file. This means that experts were able to determine the offset of the keystream stored in the filename and decrypt the file.

“Hive ransomware encrypts files by XORing the data with a random keystream that is different for each file. We found that this random keystream was sufficiently guessable.” continues the paper. “Hive ransomware generates a data encryption keystream (EKS) that appears random for each file, and encrypts the file by XORing EKS with the file. However, EKS is created using two keystreams extracted from the previously created master key During the encryption process, only the part of the file, not the entire area, is encrypted.”

The results of the tests demonstrated the efficiency of the method, the master key recovered 92% succeeded in decrypting approximately 72% of the files, while the master key restored 96% succeeded in decrypting approximately 82% of the files, and the master key restored 98% succeeded in decrypting approximately 98% of the files.

Follow me on Twitter: [@securityaffairs](#) and [Facebook](#)

[adrotate banner="9"]	[adrotate banner="12"]
-----------------------	------------------------

[Pierluigi Paganini](#)

([SecurityAffairs](#) – hacking, ransomware)

[adrotate banner="5"]

[adrotate banner="13"]



Source: <https://securityaffairs.co/wordpress/128232/security/recover-files-hive-ransomware.html>