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

securityaffairs.co/wordpress/128232/security/recover-files-hive-ransomware.html

February 21, 2022

February 21, 2022 By Pierluigi Paganini

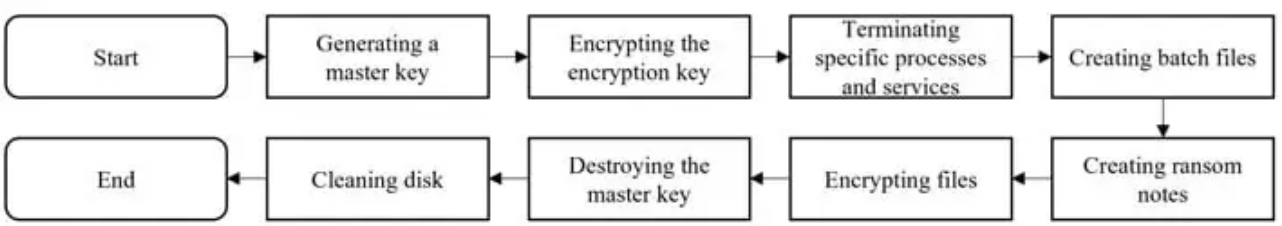
## Researchers discovered a flaw in the encryption algorithm used by Hive ransomware that allowed them to decrypt data.

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.

**Pierluigi Paganini**

**(SecurityAffairs – hacking, ransomware)**

## Experts believe that Russian Gamaredon APT could fuel a new round of DDoS attacks

May 28, 2022 By Pierluigi Paganini

There you can buy or download for free private and compromising data of your competitors. We public schemes, drawings, technologies, political and military secrets, accounting reports and clients databases. All this things were gathered from the largest worldwide companies, conglomerates and concerns with every activity. We gather data using vunlerability in their IT infrastructure. in their IT infrastructure.

Industrial spy team processes huge massives every day to devide you results. You can fid it in their portal:

http://[redacted]

(Tor browser required)

We can save your time gaining your own goals or goals of your company.With our information you could refuse partnership with unscrupulous partner, reveal dirty secrets of your competitors and enemies and earn millions dollars using insider information.

"He who owns the information, owns the world"

Nathan Mayer Rothschild

## The strange link between Industrial Spy and the Cuba ransomware operation

May 28, 2022 By Pierluigi Paganini



Back to top

- Home
- Cyber Crime
- Cyber warfare
- APT

- Data Breach
- Deep Web
- Digital ID
- Hacking
- Hacktivism
- Intelligence
- Internet of Things
- Laws and regulations
- Malware
- Mobile
- Reports
- Security
- Social Networks
- Terrorism
- ICS-SCADA
- EXTENDED COOKIE POLICY
- Contact me