Master Key for Hive Ransomware Retrieved Using a Flaw in its Encryption Algorithm

thehackernews.com/2022/02/master-key-for-hive-ransomware.html

February 19, 2022

Researchers have detailed what they call the "first successful attempt" at decrypting data infected with **Hive ransomware** without relying on the private key used to lock access to the content.

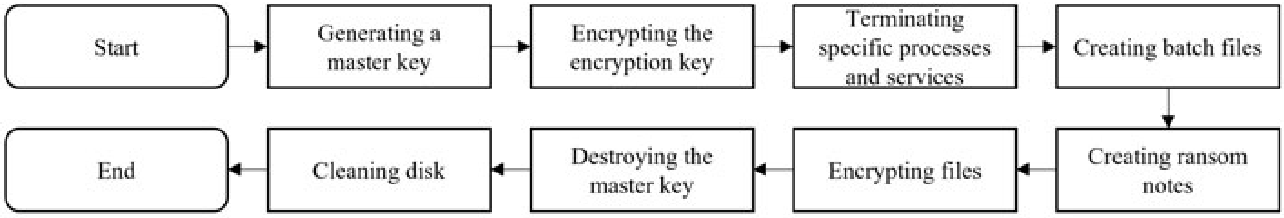
"We were able to recover the master key for generating the file encryption key without the attacker's private key, by using a cryptographic vulnerability identified through analysis," a group of academics from South Korea's Kookmin University said in a new paper dissecting its encryption process.

Hive, like other cybercriminal groups, operates a ransomware-as-a-service that uses different mechanisms to compromise business networks, exfiltrate data, and encrypt data on the networks, and attempts to collect a ransom in exchange for access to the decryption software.

GitProtect.io
by Xopero ONE
SOC 2 and ISO 27001 compliant backup
for GitHub, Bitbucket, GitLab, and Jira
Start trial

It was first observed in June 2021, when it struck a company called Altus Group. Hive leverages a variety of initial compromise methods, including vulnerable RDP servers, compromised VPN credentials, as well as phishing emails with malicious attachments.

The group also practices the increasingly lucrative scheme of double extortion, wherein the actors go beyond just encryption by also exfiltrating sensitive victim data and threatening to leak the information on their Tor site, "**HiveLeaks**."



Entire encryption process of Hive ransomware

As of October 16, 2021, the Hive RaaS program has victimized at least 355 companies, with the group securing the eighth spot among the top 10 ransomware strains by revenue in 2021, according to blockchain analytics company Chainalysis.

The malicious activities associated with the group have also prompted the U.S. Federal Bureau of Investigation (FBI) to release a Flash report detailing the attacks' modus operandi, noting how the ransomware terminates processes related to backups, anti-virus, and file copying to facilitate encryption.

The cryptographic vulnerability identified by the researchers concerns the mechanism by which the master keys are generated and stored, with the ransomware strain only encrypting select portions of the file as opposed to the entire contents using two keystreams derived from the master key.

"For each file encryption process, two keystreams from the master key are needed," the researchers explained. "Two keystreams are created by selecting two random offsets from the master key and extracting 0x100000 bytes (1MiB) and 0x400 bytes (1KiB) from the selected offset, respectively."

The encryption keystream, which is created from an XOR operation of the two keystreams, is then XORed with the data in alternate blocks to generate the encrypted file. But this technique also makes it possible to guess the keystreams and restore the master key, in turn enabling the decode of encrypted files sans the attacker's private key.

The researchers said that they were able to weaponize the flaw to devise a method to reliably recover more than 95% of the keys employed during encryption.

"The master key recovered 92% succeeded in decrypting approximately 72% of the files, 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," the researchers said.

SHARE □ □ □ □
SHARE □