# Academics publish method for recovering data encrypted by the Hive ransomware

By Catalin Cimpanu

Published: 2023-01-17 · Archived: 2026-04-06 01:14:27 UTC

A team of South Korean researchers has published an academic paper on Thursday detailing a method to recover files encrypted by the Hive ransomware without paying the attackers for the decryption key.

"By analyzing the encryption process of [the] Hive ransomware, we confirmed that vulnerabilities exist by using their own encryption algorithm," four scientists from Seoul's Kookmin University said yesterday.

"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," they added.

Starting from this premise, researchers said they were able to recover a large portion of the "**master key**" that was used as the base to encrypt a victim's files.

The researchers said the technique they developed recovers around 95% of the master key, but even in this incomplete state, the key can be used to decrypt encrypted data, ranging from 82% to 98% of the victim's files, depending on how much of the original master key is recovered.

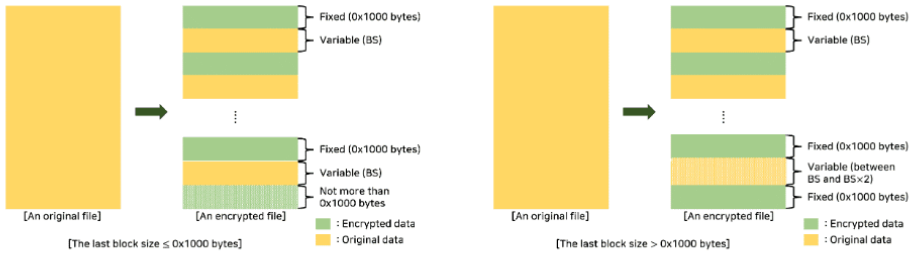
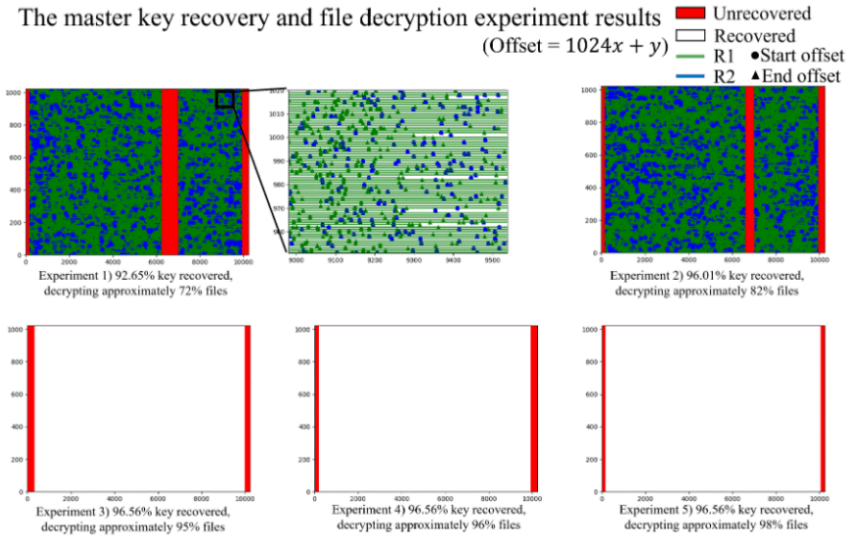



Figure 6: Encrypted file structure




The research team published a technical breakdown of their findings in a whitepaper titled "A Method for Decrypting Data Infected with Hive Ransomware."

The work was done by members of the Dept. of Financial Information Security and the Dept. of Information Security, Cryptology, and Mathematics from the Kookmin University, in Seoul, South Korea.

Their work was sponsored by a grant from the Korean government and supported by Korea's Information Security Agency (KISA).

Together with their US and European counterparts, South Korean law enforcement has been extremely active in chasing down and dealing with the current ransomware problem, having contributed to the arrest of several members of the Clop ransomware gang.

The Hive ransomware gang first appeared in June 2021 and has become one of the most active ransomware groups today, after the shutdowns of gangs like REvil, Darkside, BlackMatter, and Avaddon.

In August 2021 and January 2022, the FBI and Spain's INCIBE agencies released reports [FBI, INCIBE] detailing the Hive ransomware group's operations after seeing spikes in activity from the gang.

The Hive ransomware group did not list a contact method on their "leak site and couldn't be contacted for comment on the release of the academic paper.

> Leak site for new Hive ransomware looks pretty snazzy. Looks like some ransomware group have discovered ThemeForest pic.twitter.com/VVli1TPyzr
>
> — Catalin Cimpanu (@campuscodi) June 29, 2021

Researchers from at least two security firms—Bitdefender and Kaspersky—are currently analyzing the paper to see if they can create a free Hive decrypter based on the Korean researchers' findings.

[Catalin Cimpanu]

is a cybersecurity reporter who previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.

---