There is a tool to decrypt the ransomware that specializes in attacking businesses

This new ransomware is still in development.

Kaspersky recently revealed that they found a flaw in the encryption algorithm of the Yanluowang ransomware. Thanks to that, researchers have found a way to restore files encrypted by this ransomware.

Russian cybersecurity firm has added support for decrypting files encrypted by Yanluowang to its RannohDecryptor utility.

"Kaspersky experts analyzed the ransomware and found a vulnerability that allows decryption of affected users' files through a know-plaintext attack," Kaspersky shared.

This ransomware family encrypts files larger than 3GB and files smaller than 3GB using different methods. Large files are partially encrypted in 5MB strips every 200MB while small files are encrypted end-to-end.

Therefore, if the original file is larger than 3GB, it can decrypt all encrypted files on the system, including large files and small files. But if the original file is smaller than 3GB, it can only decrypt small files.

To decrypt your file, you need at least one original file:

1. To decrypt small files (less than or equal to 3GB), you need a pair of files that are 1024 bytes or larger. This will decrypt all other small files.
2. To decrypt large files (over 3GB), you need a pair of files (encrypted and original) each no less than 3GB in size. This is enough to decrypt both large and small files.

To decrypt files encrypted by the Rannoh ransomware, you need to use the Rannoh decryption tool provided for free by Kaspersky:

King Yama specializes in attacking large businesses.

According to statistics from cybersecurity experts, the King of Hell specializes in attacking large businesses around the world, especially financial institutions. You can learn more about the King of Hell ransomware in the article below:

Recently, Broadcom's Symantec Threat Hunter Team discovered a new ransomware called Yanluowang (Yanluowang, one of the 10 Kings of Hell). Currently, this new ransomware is still in the development stage and its target is to attack businesses.

The Yama Ransomware was discovered when experts were investigating an incident involving a reputable organization. The investigation was launched after they detected suspicious activity involving the command-line Active Directory query tool AdFind.

AdFind is often used by the actors behind ransomware for reconnaissance tasks including accessing information necessary for movement through the victim's network.

Once deployed on the victim's machine, the Yanluowang ransomware encrypts all files and appends the .yanluowang extension. They also leave behind a README.txt file demanding ransom and warning victims not to contact law enforcement or ransomware companies.

If the victim refuses to pay or contacts other parties, the people behind the King of Hell are ready to carry out DDoS attacks, delete data, repeat the attack.

Although still in development, Yama is still considered a dangerous malware. Targeting large companies and businesses, this ransomware can cause unpredictable damage.

Countries around the world are currently very active in cooperating and working together to eradicate ransomware distribution gangs.