Free decryptor released for Yanluowang ransomware victims

By Sergiu Gatlan

Published: 2022-04-18 · Archived: 2026-04-05 14:30:29 UTC

Kaspersky today revealed it found a vulnerability in Yanluowang ransomware's encryption algorithm, which makes it possible to recover files it encrypts.

The Russian cybersecurity firm has added support for decrypting files locked by the Yanluowang ransomware strain to its RannohDecryptor utility.

"Kaspersky experts have analyzed the ransomware and found a vulnerability that allows decrypting files of affected users via a known-plaintext attack," the company said today.


DIE LINKE.
0:00

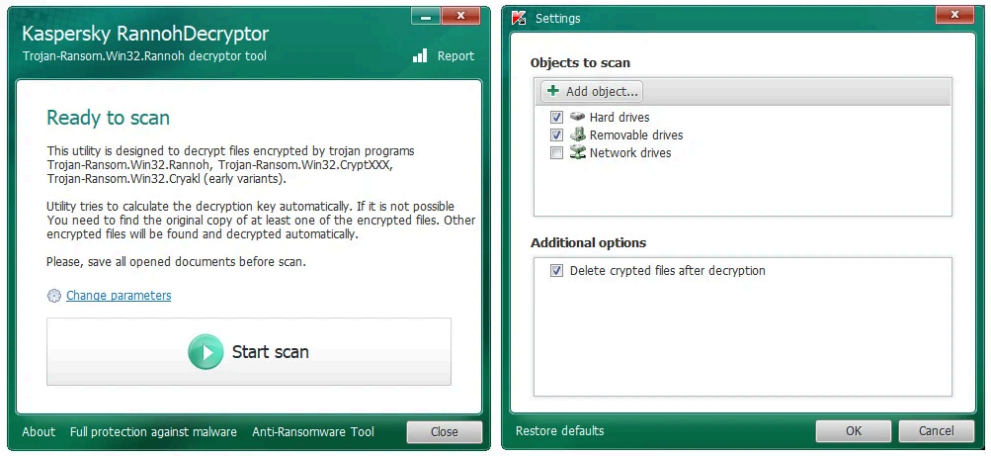
This ransomware strain encrypts files bigger than 3GB and those smaller than 3GB using different methods: larger ones are partially encrypted in 5MB stripes after every 200MB, while smaller ones are entirely encrypted from start to end.

Because of this, "if the original file is larger than 3 GB, it is possible to decrypt all files on the infected system, both big and small. But if there is an original file smaller than 3 GB, then only small files can be decrypted."

To decrypt your files, you need at least one of the original files:

- To decrypt small files (less than or equal to 3 GB), you need a pair of files with a size of 1024 bytes or more. This is enough to decrypt all other small files.
- To decrypt big files (more than 3 GB), you need a pair of files (encrypted and original) no less than 3 GB in size each. This will be enough to decrypt both big and small files.

To decrypt files encrypted by Yanluowang ransomware, you have to use the Rannoh decryption tool available for download from Kaspersky's servers.



Kaspersky RannohDecryptor (BleepingComputer)

Yanluowang attacks high-profile enterprise targets

Yanluowang ransomware, first spotted in October 2021, has been used in human-operated, highly targeted attacks against enterprise entities.

One month later, one of its affiliates was observed attacking US organizations in the financial sector since at least August, using the BazarLoader malware for reconnaissance.

Based on the tactics, techniques, and procedures (TTPs) used in these attacks, this Yanluowang affiliate was linked to the Thieflock ransomware operation developed by the Fivehands group (tracked by Mandiant as UNC2447).

Once deployed on compromised networks, Yanluowang stops hypervisor virtual machines, ends all processes, and encrypts files appending the .yanluowang extension.

It also drops ransom notes named README.txt that warn victims not to contact law enforcement or ask any ransomware negotiation firms for help.

If the attackers' requests are not met, the ransomware operators threaten to launch distributed denial of service (DDoS) attacks against the victims' networks and inform their employees and business partners they were breached.

They also say they'll breach the victims' networks again "in a few weeks" and delete their data, a common tactic ransomware gangs use to pressure their victims into paying the ransom.

Source: https://www.bleepingcomputer.com/news/security/free-decryptor-released-for-yanluowang-ransomware-victims/