Orion Team

Monthly Ransomware Activity

Written by: Maor Huli

October, 2022
Contents

RedKrypt ................................................................................................................................................................................. 5
RONALDIHNO ............................................................................................................................................................................. 6
CMLOCKER .................................................................................................................................................................................. 7
Killnet .......................................................................................................................................................................................... 8
Executive Summary

As an integral department in Cynet’s research team, Orion works around the clock to track threat intelligence resources, analyze payloads and automate labs to ensure our customers are protected against the newest ransomware variants. In these monthly reports, Orion reviews the latest trends identified in Bleeping Computer — the most up-to-date website that summarizes the newest ransomware variants — and shares how Cynet detects these threats.
Cynet 360 AutoXDR™ VS Ransomware
RedKrypt Ransomware
- Observed since: Oct 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .redkrypt
- Ransomware note: RedKrypt-Notes-README.txt
- Sample hash: 16764b17314ddee73431f8a7b33166a31947647b4f7b315c53c4f0be9ed43a20

RedKrypt Overview
RedKrypt ransomware renames the encrypted files with .redkrypt in the extension.

Once a computer’s files have been encrypted and renamed, it drops a note as “RedKrypt-Notes-README.txt”:

The ransomware note contains general information, warnings and the attacker’s email address:
Ronaldinho Ransomware

- Observed since: Oct 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .r7
- Ransomware note: READ_THIS.txt
- Sample hash: 568ea8c7d3f1ad39e975fac562fc4af41e983f289af092a104c2ec99e8259586

The ransomware note contains general information and warnings:

- **DROP THE CRYPTO-KEYS:**
  - Repetition: 456 times

  **Important:** You are only required to pay for the software key. If you do not have the software key, you may refuse to pay for the ransomware.

  **However,** if you are required to pay for the software key, you may refuse to pay for the ransomware.

  **WARNING:** If you do not have the software key, you may refuse to pay for the ransomware.

  **Important:** You are only required to pay for the software key. If you do not have the software key, you may refuse to pay for the ransomware.

  **WARNING:** If you do not have the software key, you may refuse to pay for the ransomware.

The attacker's contact information will eventually appear as a desktop background:

- **Questions?** - dupex876@gmail.com
- **you have 24h to pay us**
- **we accept all crypto methods**
- **For Poland we have BLIK**
CMLOCKER Ransomware

- Observed since: 2022
- Ransomware encryption method: AES + RSA
- Ransomware extension: .CMLOCKER
- Ransomware note: HELP_DECRYPT_YOUR_FILES.txt
- Sample hash: 5fef2acf0b0289500ddfcbcbe45c95973c37d30eeb2f25f0f894a6f5b43ef31

Once a computer's files have been encrypted and renamed, it drops a note named "HELP_DECRYPT_YOUR_FILES.txt" (screenshot has been taken from an outsource sandbox):

Upon execution, it immediately encrypts the endpoint and drops the ransomware note. The ransomware note contains general information, warnings and several attacker's links (a screenshot has been taken from an outsource sandbox):
Killnet Ransomware

• Observed since: 2022
• Ransomware encryption method: AES + RSA
• Ransomware extension: .killnet
• Ransomware note: Ru.txt
• Sample hash: db1c8ddcdfea93031a565001366ffa9fdb41a689bddab46aec7611a46bb4dc50

Once a computer’s files have been encrypted and renamed, it drops a note named “Ru.txt”.

The ransomware also changes the desktop wallpaper:

Google Translate:

The ransomware also changes the desktop wallpaper.
Thank you!

October, 2022