Ransomware Roundup: Gwisin, Kriptor, Cuba, and More

August 18, 2022

On a bi-weekly basis, FortiGuard Labs gathers data on ransomware variants of interest that have been gaining traction within the OSINT community and within our datasets. The Ransomware Roundup report aims to provide readers with brief insights into the evolving ransomware landscape and the Fortinet solutions that protect against those variants.

This latest edition of the Ransomware Roundup covers the DarkyLock, Gwisin, vvyu, Kriptor, and Cuba ransomware families.

Affected platforms: Microsoft Windows
Impacted parties: Microsoft Windows Users
Impact: Encrypts files on the compromised machine and demands ransom for file decryption
Severity level: High

DarkyLock ransomware

DarkyLock is a Babuk variant that appears to be new for 2022. Should this variant execute on a victim's system, files will be encrypted and changed to have a ".darky" file extension.

Figure 1. Files encrypted by DarkyLock ransomware.

Locations where files are encrypted will also have a ransom note deposited in them named "Restore-My-Files.txt".

Figure 2. DarkyLock ransom note.

The ransom note demands 0.005BTC (approximately $120.00USD) to decrypt the files on an affected system. At the time of writing, there have been no transactions observed using the Bitcoin wallet mentioned in the ransom note.

An interesting string appears in the DarkyLock executable that references LockBit 3.0, also known as Lockbit Black ransomware.

Figure 3. Interesting string contained within the DarkyLock executable.

It's currently unknown why the reference to LockBit 3.0 is includes "colorful" language.

Fortinet Protections

Fortinet customers running the latest (AV) definitions are protected against known DarkyLock ransomware variants by the following signatures:

- W32/FilecoderProt.F183!tr.ransom
- W32/CoinMiner.NBH!tr

Gwisin ransomware

Gwisin is ransomware variant that was reportedly used to target companies in South Korea. It encrypts files on compromised machines and adds a file extension named after the target company to the affected files.

In order to become infected, an MSI (Windows installer) file is delivered to the target machine. Contained within that is a Windows DLL file that requires a specific set of criteria to be met via the installer package to execute, making it difficult to detect in an environment. It is likely that the circumstances for installation are unique to each victim organization.

Figure 4. Some of the variables that need to be satisfied by the MSI installer.

Fortinet Protections

Fortinet customers running the latest (AV) definitions are protected against known Gwisin ransomware variants by the following signature:

W32/PossibleThreat

vvyu ransomware

vvyu is a variant of the STOP/DJVU ransomware family designed to encrypt files on a victim's machine. Should the ransomware be successful in running, a ransom note will be deposited in every location where files are encrypted.

Figure 5. vvyu ransom note

It demands a price of $980USD to have software provided to decrypt the affected files on the system, although a discount is promised for payment within the first 72 hours. Support e-mail addresses and a unique ID are also provided for contact with the operators. Files encrypted by vvyu will have a ".vvyu" file extension appended to them.

Figure 6. Files encrypted by vvyu ransomware.

Fortinet Protections

Fortinet Customers running the latest (AV) definitions are protected against known vvyu ransomware variants by the following signature:

W32/Stealer.3389!tr

Kriptor ransomware

At first glance, the ransom note and screen from Kriptor appear very similar to those of the infamous WannaCry ransom attack from 2017. There's even a reference to it, "Wannacry@Kozisis," in a WannaCry-like ransom screen. Unlike Wannacry, however, there is no mechanism for self-propagation to spread to other machines.

As with Wannacry and other ransomware families, Kriptor will encrypt files of interest on a victim machine and demand a ransom of $300USD worth of Bitcoin (0.012BTC) to be sent to a wallet controlled by the malware authors. At the time of this writing, there have been no transactions observed using the Bitcoin wallet mentioned in the ransom note.

Figure 7. Kriptor ransom note.

Files will be encrypted and appended with a ".Kriptor" file extension. A running clock will count down from 72 hours, after which point the malware authors threaten to double the ransom and/or prevent decryption permanently from that point onwards.

Figure 8. Files encrypted by Kriptor ransomware.

Figure 9. File properties for Kriptor ransomware show further callbacks to WannaCry.

Fortinet Protections

Fortinet customers running the latest (AV) definitions are protected against known Kriptor ransomware variants by the following signature:

W32/Filecoder.OAE!tr.ransom

Cuba ransomware

The Cuba ransomware family has been observed since 2019. They use the now ubiquitous “double extortion” method of threatening to release a victim’s data on the Internet if they do not pay the requested ransom.

Figure 10. Cuba ransomware TOR site.

Once the ransomware has executed, a ransom note will be deposited in any directory where files have been encrypted. The ransom note will be named “!! READ ME !!.txt” and contain a unique ID to contact the ransomware controllers to pay. The primary contact channel is Tox (a peer-to-peer instant messaging protocol) with a backup e-mail address if a victim cannot make contact. Files encrypted by Cuba will have a “.cuba” file extension appended.

Figure 11. The ransom note for Cuba ransomware.

Figure 12. Files encrypted by Cuba ransomware.

Fortinet Protections

Fortinet customers running the latest (AV) definitions are protected against known Cuba ransomware variants by the following signatures:

- W32/Filecoder.OAE!tr.ransom
- W32/GenKryptik.EMOA!tr
- W32/Kryptik.HGXH!tr
- W32/Filecoder.OAE!tr.ransom
- W32/Injector.EQGY!tr
- JS/Agent.5646!tr
- W32/GenKryptik.FSCS!tr

Best practices include not paying a ransom

Organizations such as CISA, NCSC, the FBI, and HHS caution ransomware victims against paying a ransom, partly because payment does not guarantee files will be recovered. Ransom payments may also embolden adversaries to target additional organizations, encourage other criminal actors to distribute ransomware, and/or fund illicit activities that could potentially be illegal, according to a U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) advisory. The FBI has a Ransomware Complaint page, where victims can submit samples of ransomware activity via the Internet Crimes Complaint Center (IC3).

Learn more about Fortinet’s FortiGuard Labs threat research and intelligence organization and the FortiGuard Security Subscriptions and Services portfolio.