Ransomware Roundup: Redeemer, Beamed, and More

fortinet.com/blog/threat-research/ransomware-roundup-redeemer-beamed-and-more

August 4, 2022

Over the past few weeks, FortiGuard Labs has observed several new ransomware variants of interest that have been gaining traction within the OSINT community, along with activity from our datasets. This isn't a new phenomenon. This is part of a pattern of behavior that dates back several years—a pattern that is likely to continue for some time to come.

Ransomware infections continue to have a significant impact on organizations, including—but not limited to—disruptions to operations, theft of confidential information, monetary loss due to ransom payout, and more. It's why we feel it's imperative that we increase our efforts to raise awareness about existing and emerging ransomware variants.

This new Ransomware Roundup report aims to provide readers with brief insights into the evolving ransomware landscape and the Fortinet solutions that protect against these variants.

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

This latest edition of the Ransomware Roundup covers the Redeemer, Beamed, and Araicrypt ransomware families.

Redeemer Ransomware

Redeemer is a ransomware variant that was first discovered in June 2021. It encrypts files on a compromised machine and demands a ransom in Monero cryptocurrency (XMR) to decrypt the affected files. As of this writing (July 29, 2022), there are four public versions of Redeemer ransomware; versions 1.0, 1.5, 1.7, and 2.0. This indicates that the Redeemer threat actors have been applying constant effort to improve the ransomware.

Figure 1. Change log for Redeemer ransomware version 1.0

Figure 2. Change log for Redeemer ransomware versions 1.5 and 1.7

Figure 3. Change log for Redeemer ransomware version 2.0

Files encrypted by Redeemer ransomware typically have a ".redeem" file extension. The malware also leaves a ransom note in Read Me.TXT.

Figure 4. Files encrypted by Redeemer ransomware and ransom note

Figure 5. Redeemer ransomware's ransom note

Redeemer has its own web page on TOR that provides instructions on how to use the Redeemer ransomware and toolkit. The instructions are broken down into six sections.

1. Part zero is for crypto usage and lists process names that affiliates should not use.
2. Part one is how to build Redeemer ransomware, including generating a private build key, setting a ransom amount in Monero, adding contact information, adding a campaign ID, and enabling and disabling self-deletion.
3. Part two states that the ransomware is designed to delete logs and shadow copies twice, before and after the encryption process, and to leave a ransom note in all directories where affected files reside. This section warns affiliates that the ransomware must be executed with administrator privilege or else it will not run. This indicates that Redeemer ransomware either uses social engineering to trick victims into running the ransomware or uses exploits for vulnerabilities in software or hardware to elevate privileges to do so. Note that the latter has not been observed.

4. Part three describes how to communicate with victims. Affiliates are recommended to use privacy-oriented services to negotiate with victims to avoid identifying the attacker's IP. The Redeemer threat actors also advise against giving discounts to victims as they believe such an ask typically comes from professional negotiators.
5. Part four is on file decryption, providing instructions on using the Affiliate Toolkit to obtain the Redeemer affiliate key using the Redeemer public key received from the victim and the previously generated private build key (see part one). Affiliates will receive a Redeemer master key for file decryption once the Redeemer affiliate key is passed to the developer and the decryption fee (20% of the ransom amount) is deposited to the developer's Monero wallet.
6. Part five covers how victims run the Redeemer decrypter to recover the encrypted files.

Figure 6. Affiliate instructions on the Redeemer page

Figure 7. Files inside Redeemer version 2.0 package

As previously mentioned, the decryption fee is currently set at 20%, giving affiliates 80% of the profit. The developer also provides a Tox chat address to communicate with affiliates.

Figure 8. Decryption fee payment and developer's Tox Chat ID on the Redeemer page

Fortinet protections

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

- W32/Filecoder.OHI!
- W32/Filecoder.OHI!tr
- W32/Filecoder.050E!tr.ransom
- W32/Filecoder.OHI!tr.ransom
- W32/RedLineStealer.A!tr
- W32/Malicious_Behavior.VEX

Beamed ransomware

Beamed is ransomware that encrypts files on a compromised machine and demands that victims pay a ransom in Bitcoin for file decryption. Encrypted files have a ".beamed" file extension. It leaves a ransom note in "RIP YO DOCUMENTS.txt", which contains the attacker's Bitcoin address. The ransom fee is set at $200 worth of Bitcoin. As of this writing, no transaction has been observed in the Bitcoin wallet.

Figure 9. Beamed ransomware's "colourful" ransom note

Fortinet Protections

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

MSIL/Filecoder.TA!tr

Araicrypt ransomware

Araicrypt appears to be a variant of the Thanos ransomware family that encrypts files on a victim's machine. It leaves a ransom note in "READ_TO_RESTORE_YOUR_FILES.txt". In the ransom note, Araicrypt claims to have deleted shadow copies, which makes file recovery difficult. It also claims to have stolen information from the victim, who is given 48 hours to contact the attacker via email. The attacker threatens to publish the stolen data if the victim fails to make contact. Files encrypted by Araicrypt ransomware have a ".araicrypt" file extension.

Figure 10. Arai ransomware's ransom note

Fortinet Protections

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

- MSIL/Filecoder.Thanos.A!tr
- MSIL/Filecoder_Thanos.A!tr.ransom
- MSIL/Filecoder_Thanos.B!tr

Best practices include not paying a ransom

Ransomware victims are cautioned against paying ransom by organizations such as CISA, NCSC, the FBI, and HHS, partly because payment does not guarantee that 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.