

 BRIEF

REDKRYPT RANSOMWARE

ZEROFOX INTELLIGENCE

B-2022-10-20b

Classification: TLP:AMBER

Criticality: High

Intelligence Requirements: Ransomware

October 20, 2022



Scope Note

*ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 08:00 AM (EDT) on October 18, 2022**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

RedKrypt Ransomware

Executive Summary

ZeroFox Intelligence has discovered a previously-unknown ransomware family calling itself RedKrypt. Not much is known about its infection vector, as the sample was discovered on VirusTotal. The ransomware was created in Microsoft's .NET framework and does not appear to use any sort of obfuscation. One key is generated per victim, and that key is then encrypted via RSA1024. Plaintext (.txt) and Markdown (.md) files are fully encrypted, while all other files are only encrypted up to the first 1024 bytes. To ensure it can recover a victim's files, RedKrypt sends the operators a uniquely-generated ID and a RSA1024 private key via Telegram.

Capabilities

Communicates via Telegram

Though RedKrypt does not exfiltrate files, it does exfiltrate the generated private RSA1024 key and victim ID to the operators via Telegram so they can provide a key to the victim when contacted.

Creates Unique Victim IDs

Using a combination of the victim's hardware information, a unique ID is created per victim.

Encrypts Key

Although a standard encryption method is not used on file contents, the key used to modify file contents is encrypted using RSA1024. The encrypted key is stored in %APPDATA%\DONTDELETEME.redkrypt. This file serves two purposes:

- Signifies RedKrypt has previously run
- Stores an encrypted version of the key



Includes Decryptor

RedKrypt, straying from the usual trend, includes the decryptor as part of the infection. The decryptor is an embedded resource inside the ransom payload and is extracted to the victim's desktop to be run at the end of the encryption process. Despite the decryptor being included, the victim still needs the private RSA1024 key sent to the operators to decrypt a password stored in DONTDELETEME.redkrypt.

Modifies Files (Without Encryption)

Rather than using a full encryption scheme, RedKrypt generates a random password (key) per victim. The bytes from this password are then combined with bytes from the target file to transform the original file contents.

Runs Once

RedKrypt attempts to create a mutex when it starts to ensure that only one instance is running at a time on the victim's machine. It also checks for the existence of DONTDELETEME.redkrypt to know if the ransomware has already been run previously.

Runs on Start

RedKrypt's decryptor adds an entry for itself to the Windows Run key in the registry under the name "REDKRYPTDecryptor."

Runs Quickly

To ensure quick runs, RedKrypt only fully-encrypts files with the ".md" (Markdown) or ".txt" (Plaintext) file extensions. All other files are only processed up to and including the first 1024 bytes. Only files in the %USERPROFILE% directory are targeted.

Protects Against Termination

RedKrypt uses security descriptors to protect itself against being stopped before execution completes.



Appendix 1: Indicators of Compromise (IOCs)

Files

- %APPDATA%\DONTDELETEME.redkrypt
- %APPDATA%\publicEncryptionKey.redkrypt
- %APPDATA%\rnsKey.txt
- Desktop\RedKryptDecryptor.exe
- Desktop\RedKrypt-Notes-README.txt
- *.f.redkrypt
- *.p.redkrypt

Registry

- SOFTWARE\Microsoft\Windows\CurrentVersion\Run\REDKRYPTDecryptor

SHA256 Hashes

- a851d387648348b23d00c555f2a3db866088289dfcf7eb20a593f94dfc63ad7b
- 16764b173314ddeb7341f18a7b33066a319476847ba715c53c4f0f8e9ed43a20

URLs

- hXXps://api.telegram[.]org/bot



Appendix 2: YARA Rules

```
rule RedKrypt : dotnet ransomware
{
    meta:
        author = "@_FirehaK <yara@firehak.com>"
        date = "2022-10-18"
        description = "Detects RedKrypt ransomware"
        modified = "2022-10-18"
        reference =
            "https://www.virustotal.com/gui/file/a851d387648348b23d00c555f2a3db866088289dfcf7eb20a593f94dfc63ad7b"
            tlp = "TLP:AMBER"

    strings:
        $method_main = { 28??000006 00 1F1A 28??00000A 72??????70 28??00000A 0B 07
        28??00000A 16 FE01 0D 09 2C08 00 28??000006 00 00 2A }
        $method_GetFiles = { 00 73??00000A 0A 00 06 02 03 16 28??00000A 6F??00000A 00 00 02
        28??00000A 0B 16 0C 2B16 07 08 9A 0D 06 09 03 28??000006 6F??00000A 00 08 17 58 0C 08 07 8E
        69 32E4 00 DE05 26 00 00 DE00 06 1304 2B00 1104 2A }
        $method_EncodeAob = { 00 03 8E 69 8D??000001 0A 16 0B 16 0C 2B25 00 06 08 03 08 91 04
        07 91 58 D2 9C 04 07 17 58 91 16 FE01 0D 09 2C04 16 0B 2B04 07 17 58 0B 00 08 17 58 0C 08 03 8E 69
        FE04 1304 1104 2DCF 06 1305 2B00 1105 2A }
        $method_DecodeAob = { 00 03 8E 69 8D??000001 0A 16 0B 16 0C 2B25 00 06 08 03 08 91 04
        07 91 59 D2 9C 04 07 17 58 91 16 FE01 0D 09 2C04 16 0B 2B04 07 17 58 0B 00 08 17 58 0C 08 03 8E 69
        FE04 1304 1104 2DCF 06 1305 2B00 1105 2A }

    condition:
        uint16(0) == 0x5a4d
        and 3 of them
}
```



Appendix 3: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.