Rorschach

Threat: **Ransomware**

Author: **Jeffrey Farnan**

Date Originally Published: **April 30th, 2023**

1. SUMMARY

- A new and highly sophisticated ransomware strain has come on the scene called Rorschach, it stands out for its ability to encrypt data more quickly than other ransomware types. This ransomware is partially autonomous capable of spreading itself automatically when executed on a domain controller. Rorschach was deployed using the DLL side-loading technique, its rare in ransomware attacks and incredibly difficult technique to defend against. The developers have made this malware extremely flexible making it capable of changing its behavior to suit an attacker's needs providing it with optional arguments.

2. MALWARE FAMILY

- **Type** = Ransomware.

- **Ransomware Family:** A type of malware which secretly encrypts victim's files holds those files for ransom until a sum of money is paid. The attackers can threaten the victim with publishing the victim's data or block access to the device until the ransom is paid.

3. MALWARE CHARATERISTICS

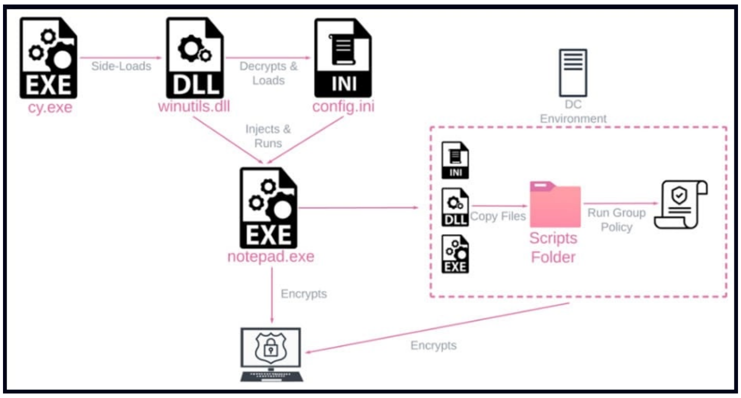
- **Suspected country of origin** = Unknown
- **First seen date/period** = June 2022.
- **Still active** = Yes.
- **Last submitted sample as of writing this article** = April 26th, 2023.

4. MALWARE HISTORY

- Rorschach was first discovered in June 2022 by Check Point Research who responded to an Incident at a company in the U.S. Rorschach got its name because everyone who analyzed it saw something different.
- This ransomware is unique as it shares characteristics with other types of ransomware, including Babuk, Darkside and LockBit, but it has no overlaps that can link it with any other ransomware strain.

5. MALWARE DESCRIPTION

- Rorschach is also known as BabLock, is based on the LockBit ransomware, but is has also has the best features from other strains. Security researchers don't believe this is from the same ransomware developers who created LockBit. This malware extremely flexible making it capable of changing its behavior to suit an attacker's needs thanks to the numerous optional arguments. Some of the options available to the attacker are drop a ransom note, create log files, do not self-delete on execution, encrypt the following path, do not change wallpaper, do not encrypt shares, explicitly state the loader DLL, etc. These options are hidden and can't be accessed without reverse engineering the malware.
- **Encryption speed:** The encryption speed was compared to another ransomware variants known as Lockbit which is considered a fast encryptor. Lockbit has a speed of 420 seconds while Rorschach has a speed of 270 seconds. The encryption scheme blends the curve25519 and eSTREAM cipher hc-128 algorithms and it encrypts the files only partially, leading to increased processing speed. Its speed of encryption is makes it one of the sophisticated ransomware types we have seen so far which speaks to the rapidly changing nature of cyber-attacks today.
- **DLL side-loading:** DLL side-loading is not a new technique, but it's rare in ransomware attacks and incredibly difficult technique to defend against. DLL side-loading is the proxy execution of a malicious DLL via a benign executable planted in the same directory. This abused the Windows behavior of loading the DLL from the application (e.g. the benign, planted binary) was loaded prior to other locations as system directories. The benefits for the Threat actors of using this technique is that the executables used are often trusted, signed and in use within an organization. The payload is embedded within the DLL and may often be encrypted or obfuscated to defeat anti-virus or basic scanning.



- This attack consists of using the Cortex XDR Dump Service Tool (cy.exe) to sideload the Rorschach loader and injector (winutils.dll) leading to launching the ransomware payload called config.ini into a Notepad process. The loader file features UPX-style anti-analysis protection, while the main payload is protected against reverse engineering and detection by virtualizing parts of the code using the VMProtect software.
- Rorschach adds a random strig of characters and a two-digit number (ranging from 00 to 98) to the end of filenames. An example of how Rorschach modifies filenames: it changes "**1.jpg**" to "**1.jpg.slpqne.37**", "**2.png**" to "**2.png.slpqne.39**", and so forth. The appended string of random characters may vary depending on the ransomware variant. A ransom note is dropped ("**_r_e_a_d_m_e.txt**") and changes the desktop wallpaper.
- **Evasion:** Like other strains of ransomware Rorschach displays anti-analysis and evasion techniques to avoid detection making it harder for malware analysists to analyze. After a machine has been compromised the malware erases four event logs (Application, Security, System and Windows Powershell) to wipe its trace. This malware also incorporates an unusual technique to evade defense mechanisms, it makes direct system calls using the "syscall" instruction.

6. POTENTIAL CUSTOMER DEFENSE

- When a ransomware attack happens there are two basic options:
    - **Recovery:** In some cases, victims may be able to recover their files by using decryption tools. If the ransomware uses strong encryption and the decryption is unavailable may be impossible without paying the ransom. Which is never advised as there is no guarantee that the decryption key / tool will be provided.
    - **Restore from backups:** The fastest way to recover from ransomware is to restore your systems from backups. You must have a recent version of your data and applications backed up on an uninfected machine.

Research Sources:

- https://www.cybersecuritydive.com/news/rorschach-ransomware-encryption-speed/647693/
- https://www.trendmicro.com/en_us/research/23/d/an-analysis-of-the-bablock-ransomware.html
- https://www.siliconrepublic.com/enterprise/rorschach-ransomware-fast-research
- https://businessinsights.bitdefender.com/tech-explainer-what-is-dll-sideloading
- https://www.crowdstrike.com/blog/dll-side-loading-how-to-combat-threat-actor-evasion-techniques/
- https://www.bleepingcomputer.com/news/security/new-rorschach-ransomware-is-the-fastest-encryptor-seen-so-far/
- https://www.computerweekly.com/news/365534897/Quick-acting-Rorschach-ransomware-appears-out-of-nowhere
- https://www.pcrisk.com/removal-guides/26437-rorschach-ransomware

Disclaimer: All opinions expressed in this article are the opinions solely of the author.