THREAT ANALYSIS

April 10, 2023

Rorschach Ransomware and its Evasion Capabilities

SUMMARY

Rorschach Ransomware is a highly customizable strain that was recently uncovered by Check Point Software Technologies. There is currently no known overlap with other ransomware strains. Its ability to very quickly encrypt files on targeted systems contributes to its uniqueness. Check Point further noted that the first victim was likely a U.S.-based organization.

TECHNICAL DETAILS

Check Point found that Rorschach-based ransomware attacks were primarily reported in Asia, Europe, and the Middle East. The malware uses direct syscalls and is highly customizable. The ransomware then encrypts target files and presents the victim with a ransom note in a format similar to the Yanluowang ransom note. The Cortex XDR Dump Service tool's DLL side-loading vulnerability is used to spread the ransomware, which is believed to be developed from the Babuk ransomware's leaked source code and is partially influenced by LockBit 2.0.

The ransomware attempts to stop a predefined list of services within target hosts as soon as it is executed, then attempts to delete backups and shadow volumes using authorized Windows tools. On a Windows Domain Controller host, the ransomware automatically creates a Group Policy in order to spread to other machines in the domain. Rorschach encryption uses a combination of the curve25519 and eSTREAM encryption hc-128 algorithms.

The speed and capabilities of the Rorschach ransomware highlights the value of resilience and recovery strategies, offline backups, and the visibility and capability for detection and response for blue teams.

INDICATORS OF COMPROMISE (IOCs)

Hashes:

- 2237ec542cdcd3eb656e86e43b461cd1
- 4a03423c77fe2c8d979caca58a64ad6c
- 6bd96d06cd7c4b084fe9346e55a81cf9

REFERENCES

- https://research.checkpoint.com/2023/rorschach-a-new-sophisticated-and-fast-ransomware/
- https://www.bleepingcomputer.com/news/security/new-rorschach-ransomware-is-the-fastest-encryptor-seen-so-far/
- https://thehackernews.com/2023/04/rorschach-ransomware-emerges-experts.html