Rorschach Ransomware

UPDATE

Separately, Palo Alto Networks issued an informational security advisory discussing Rorschach ransomware operators using the Cortex XDR Dump Service Tool (cydump.exe) to load untrusted dynamic link libraries (DLLs) using DLL-sideloading. This is true only when the tool is removed from its installation directory; it is not possible to side-load DLLs when Cortex XDR agent is installed on Windows and is running from the installation path because Cortex XDR's security permissions and protections prevent it. In the advisory, Palo Alto verified that Cortex XDR 7.7, and newer versions, with content update version 240 (released Nov 2021), and later content updates, detect and block the ransomware. New versions of Cortex XDR agent, capable of blocking the DLL side-loading technique, will be released next week to prevent future misuse of the software. Mac OS and Linux platforms are not affected by this issue.

Reference:
https://security.paloaltonetworks.com/PAN-SA-2023-0002

Security researchers have discovered a new ransomware strain, called Rorschach, with unique technical features. The malware is deployed using the dynamic link library (DLL) side-loading technique via a signed component in Cortex XDR, a threat detection and incident response tool from Palo Alto Networks. Rorschach features UPX-style anti-analysis protection and virtualizes parts of its code using VMProtect software to protect against reverse engineering and detection. Its encryption scheme uses the curve25519 and eSTREAM cipher hc-128 algorithms and intermittently encrypts files, making it faster than other ransomware strains. Rorschach also creates a Group Policy when executed on a Windows Domain Controller to propagate to other hosts on the domain and erases four event logs to wipe its trace. The ransomware strain has no branding or known operators.
The lack of branding and unknown operators of Rorschach is a rare occurrence in the ransomware scene. Security researchers note that Rorschach seems to have implemented the best features from some of the leading ransomware strains leaked online, including Babuk, LockBit v2.0, and DarkSide. The self-propagating capabilities of Rorschach are expected to raise the bar for ransom attacks. It is not yet clear who is behind Rorschach, but its technically advanced features suggest that it may pose a significant threat to organizations that fall victim to it.

The Critical Start Cyber Threat Intelligence (CTI) team will continue to monitor the situation and work closely with the Threat Detection Engineering (TDE) team and the SOC to implement any relevant detections. For future updates, the CTI team will post via ZTAP® Bulletins and on the Critical Start Intelligence Hub.

References:

1. https://research.checkpoint.com/2023/rorschach-a-new-sophisticated-and-fast-ransomware/
2. https://www.bleepingcomputer.com/news/security/new-rorschach-ransomware-is-the-fastest-encryptor-seen-so-far/

Critical Start's Threat Detection Engineer Team has implemented detections within ZTAP® that address this malicious activity.