KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Sophisticated “Rorschach” Ransomware Hits Firms in Asia, Middle East and Europe

Tracker ID: TN2358 **Date:** April 05, 2023 **Category:** Malware **Industry:** All **Region**: Asia, Middle East, Europe

Background

Researchers have discovered a previously unknown ransomware strain dubbed “Rorschach,” which is both complex and fast. Rorschach is distinguished from other ransomware strains by its high degree of customization and technically novel elements not previously seen in malware. In terms of encryption speed, Rorschach is one of the quickest ransomware strains ever detected. According to the BabLock samples provided to VirusTotal, the gang reportedly carried out attacks in Asia, Middle East and Europe. Additionally, the organization does not encrypt devices that use Russian or other Post-Soviet languages.

In an identified campaign, the malware was being deployed against an unknown U.S.-based business, and no logos or similarities that link it to any previously known ransomware perpetrators were noted. A further investigation of Rorschach's source code resembles Babuk and LockBit 2.0 ransomware. The ransom letters delivered to the victims appear to have been influenced by Yanluowang and DarkSide. The malware payload was loaded using an attack method known as DLL side-loading, which is uncommon in such assaults. The improvement represents a new level of sophistication in the techniques used by monetarily driven attackers to avoid detection.

Furthermore, the malware is said to have been distributed by exploiting Palo Alto Network's Cortex XDR Dump Service Tool (cy.exe) to sideload a file called "winutils.dll." A differentiating trait is its highly configurable nature and the use of direct syscalls to modify files and circumvent defense mechanisms. Rorschach malware is programmed to terminate a preset list of services, delete shadow volumes and backups, clear Windows event logs to remove forensic traces, disable the Windows firewall, and even delete itself once its tasks are completed.

Researchers found that Rorschach encrypted 220,000 files in four minutes and 30 seconds on average, whereas LockBit 3.0 took seven minutes. Its creators used self-propagating capacities, novel anti-analysis, and defense evasion methods to escape detection and make it difficult for security software and experts to analyze and mitigate its effects. Furthermore, Rorschach appears to have combined some of the 'best' features from the top malwares whose code has been leaked publicly.

As the regularity and complexity of these attacks increase, organizations must stay watchful and proactive in their efforts to protect themselves. Organizations should adopt network segmentation and ensure that critical systems are patched against known flaws and that sufficient system backups are in place.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Sophisticated “Rorschach” Ransomware Hits Firms in Asia, Middle East and Europe

Tracker ID: TN2358 **Date:** April 05, 2023 **Category:** Malware **Industry:** All **Region**: Asia, Middle East, Europe

MITRE ATT&CK Tactics

Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Command and Control and Impact.

Indicators of Compromise *

Please refer to the attached sheet for IOCs.

Recommendations

- Check with your existing AV/EDR vendor to validate the detection scope of identified samples.
- Administrators and organizations are encouraged to install critical updates for operating systems and applications on a regular basis against the identified vulnerabilities and exploits as soon as possible.
- Establish strict password rules for both local and domain users. Ensure that separate passwords are used for local admins on all infrastructure hosts.
- Stick to the concept of least privileges in the system when handling access rights, with a particular emphasis on service accounts as well as accounts used for automated chores and remote access.
- Ensure direct RDP access to computers and servers from outside the internal network is prohibited.
- Continuously monitor for anomalous activities, including suspicious activity in the temp folder and the download or installation of unauthorized applications.
- Perform regular data backup procedures and maintain up-to-date incident response.
- Establish a data recovery strategy and routinely backup your files to a secure offsite place. The ability to rescue your data after a ransomware assault is guaranteed by routine data backups.
- Follow multilayered defense solutions and active monitoring to detect threats before operators can launch their attacks.
- Assess your ‘Crown Jewels’ that could help in determining your current security posture. It will aid in deciding ahead of an incident on the data you could afford to have leaked to avoid paying the ransom.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Sophisticated “Rorschach” Ransomware Hits Firms in Asia, Middle East and Europe

Tracker ID: TN2358 **Date:** April 05, 2023 **Category:** Malware **Industry:** All **Region**: Asia, Middle East, Europe

References

- Palo Alto Networks Security Advisories, PAN-SA-2023-0002 Informational Bulletin: Impact of Rorschach Ransomware, PaloAlto, April 04, 2023, External Link (security.paloaltonetworks.com.com).
- Ravie Lakshmanan, Rorschach Ransomware Emerges: Experts Warn of Advanced Evasion Strategies, The Hacker News, April 04, 2023, External Link (thehackernews.com).
- Andrey Zhdanov and Vladislav Azersky, The old way: BabLock, new ransomware quietly cruising around Europe, Middle East, and Asia, Group-IB, April 04, 2023, External Link (www.group-ib.com).

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI

KPMG in India Cyber Response Hotline : +91 9176471471

Hash SHA256	Hash MD5
03c41019faf7e4cc26ca0dd3a2c41b2115e4c4ebd561402079bc4a20256c1813	2237ec542cdcd3eb656e86e43b461cd1
2fd264f58ba82a2675280ec8c6759612def2bcc62aa6160f5e23071f67bb67ab	4a03423c77fe2c8d979caca58a64ad6c
38c610102129be21d8d99ac92f3369c6650767ed513e5744c0cda54e68b33812	6bd96d06cd7c4b084fe9346e55a81cf9
4874d336c5c7c2f558cfd5954655cacfc85bcfcb512a45fb0ff461ce9c38b86d	
66bcad0829a59c424d062b949c2a556b11c509b17515dffecb9cbf65f13f3dc6	
7d62a33e9a2fedff6cf27aaa142ff15838a766ccd4a8d326424611e155442775	
83052cc23c45ecaa09fe5c87fd650c7f8e708aea46756a2b9d452d40ce3b9c00	
88081a21e500e831d86666ca5d7a3d348f7c03bc5c471b6d17d8b18a022f25be	
aa48acaef62a7bfb3192f8a7d6e5229764618ac1ad1bd1b5f6d19a78864eb31f	
b711579e33b0df2143c7cb61246233c7f9b4d53db6a048427a58c0295d8daf1c	
b99d114b267ffd068c3289199b6df95a9f9e64872d6c2b666d63974bbce75bf2	
e14b88795bde45cf736c8363c71a77171aa710a4e7fa9ce38470082cb1bdadbb	
de5a53131225dd97040d48221d9afd98760f7ff2f55613f0d08436891ca632b9	