



Rorschach Ransomware Hits the Middle East

CRITICALITY



06/04/2023

Recommendations



Prevention



Detection



Remediation



Response



MITRE ATT&CK

Summary

Rorschach ransomware is currently targeting small and medium businesses and industrial firms in Asia, Europe and the Middle East.



Threat Details

Researchers at Check Point have identified a new ransomware variant called Rorschach, which has the fastest encryption speed among known ransomware threats. The malware has been detected in Asia, Europe, and the Middle East and was deployed by exploiting a vulnerability in a threat detection and incident response tool.

The attackers used the DLL side-loading technique through a signed component in Palo Alto Networks' Cortex XDR product. They leveraged the Cortex XDR Dump Service Tool (cy.exe) version 7.3.0.16740 to deploy the Rorschach loader and injector (winutils.dll), which launched the ransomware payload named "config.ini" into a Notepad process. Upon execution, the malware creates a Group Policy to propagate to other hosts on the domain.

However, it has been confirmed by Palo Alto Networks that Cortex XDR agent version 7.7 and later, along with content update version and later updates have the ability to detect and block the spread of the ransomware.



Recommendations



Prevention

- **Appendix A** contains the recommendations to prevent such attacks.

References

New Rorschach ransomware is the fastest encryptor seen so far. (2023). Retrieved from Bleeping Computer: <https://www.bleepingcomputer.com/news/security/new-rorschach-ransomware-is-the-fastest-encryptor-seen-so-far/>

PAN-SA-2023-0002 Informational Bulletin: Impact of Rorschach Ransomware. (2023). Retrieved from Palo Alto: <https://security.paloaltonetworks.com/PAN-SA-2023-0002>

Rorschach Ransomware Emerges: Experts Warn of Advanced Evasion Strategies. (2023). Retrieved from The Hacker News: <https://thehackernews.com/2023/04/rorschach-ransomware-emerges-experts.html>



Contact Us

Bahrain National CERT - National Cyber Security Center “NCSC”

Email: CERT@ncsc.gov.bh



Appendix A – Prevention

The National Cyber Security Centre recommends all the entities to apply the latest available patches.

Affected Products	
Cortex XDR Agent 5.0	All agents on Windows
Cortex XDR Agent 7.5 CE	All agents on Windows
Cortex XDR Agent 7.8	Agents with content update earlier than CU-240 on Windows
Cortex XDR Agent 7.9 CE	Agents with content update earlier than CU-240 on Windows
Cortex XDR Agent 8.0	Agents with content update earlier than CU-240 on Windows



Appendix B – Best Practices

Bahrain National CERT team recommends organizations to implement the following security best practices.

- Daily backups of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes.
- Patch operating systems. Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.
- Patch applications e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications.
- Restrict administrative privileges to operating systems and applications based on user role. Regularly reassess the need for privileges. Don't use privileged accounts for reading email and web browsing.
- Configure Microsoft Office macro settings to block macros from the Internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.
http://www.asd.gov.au/publications/protect/Microsoft_Office_Macro_Security.pdf
- Application whitelisting of approved/trusted programs to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers.
- User application hardening. Configure web browsers to block Flash (ideally uninstall it), ads and Java on the Internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers.
- Multi-factor authentication for VPNs, Outlook Web Access (OWA), RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive or high-availability) data repository.
- Implement CIS Critical Security Controls, while prioritizing the implementation of the Top 5 CIS Controls. (<https://www.cisecurity.org/critical-controls.cfm>)
- Implement Strategies to mitigate cyber security incidents.
(<http://www.asd.gov.au/infosec/mitigationstrategies.htm>)



CERT.bh recommends organizations to implement the following strategies to detect and respond to cyber security incidents:

- Network-based intrusion detection/prevention system using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.
- Host-based intrusion detection/prevention system to identify anomalous behaviour during program execution e.g. process injection, keystroke logging, driver loading and persistence mechanisms.
- Endpoint detection and response software on all computers to centrally log systems' behaviour and facilitate incident response. Microsoft's free SysMon tool is an entry level option.
- Enhance visibility through PowerShell logging to provide investigators a detection mechanism for malicious activity and a historical record of how PowerShell was used on systems.
https://www.fireeye.com/blog/threat-research/2016/02/greater_visibility.html
- Hunt to discover incidents using threat intelligence consisting of analyzed threat data with indicators of compromise and mitigating threats based on behaviour patterns.
- Capture network traffic to and from internal systems that store important data or are considered critical assets, and network traffic traversing the network perimeter, to assist with incident detection and analysis.
- Continuous incident detection and response with automated immediate analysis of centralised time-synchronised logs of permitted and denied: computer events, authentication, file access, network activity.
- MITRE Corporation provides a public repository that includes a model and framework for describing the actions attackers may take while operating within an enterprise network. These details can aid organizations in detecting attacker activities.
 - https://attack.mitre.org/wiki/Main_Page
 - https://car.mitre.org/wiki/Full_Analytic_List
 - <https://car.mitre.org/caret/#/>



Appendix C – TLP Definitions

RED

For the eyes and ears of individual recipients only, no further disclosure. Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting.

AMBER

Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Note that **TLP:AMBER+STRICT** restricts sharing to the organization only. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may 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: if the source wants to restrict sharing to the organization only, they must specify TLP:AMBER+STRICT.

GREEN

Limited disclosure, recipients can spread this within their community. Sources may use TLP:GREEN when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. Note: when “community” is not defined, assume the cybersecurity/defense community.

CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction