KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | New Ransomware Ransom Cartel linked with REvil

Tracker ID: TN1021 **Date:** 27/Oct/2022 **Category:** Malware **Industry:** All **Region**: All

Background

A new "Ransom Cartel" ransomware operation has been discovered, which appears to be in collaboration with the infamous REvil gang. The links are based on the code similarities in both operations' encryptors, which include double-extortion attempts, hefty ransom demands, and a data leak site to coerce victims into paying a ransom. REvil reached dominance in the first half of 2021, compromising thousands of organizations via a Kaseya MSP supply-chain attack, extorting Apple using stolen designs for future goods, and even demanding $50 million from computer manufacturer Acer.

The REvil group was disbanded in October 2021 by law enforcement, and in January 2022, the Russian authorities announced the arrests of eight gang members, the confiscation of their assets, and the filing of criminal charges. However, the discovery of the Ransom Cartel alters the battleground. The new ransomware from Ransom Cartel is either a rebrand or a novel operation initiated by a core member of the original gang as it uses code identical to REvil's encrypting malware. Another ransomware used identical ransom notes and named itself "Sodinokibi," another name for REvil, on their Tor payment sites in a previous case. It should be noted that the source code for REvil's encrypting malware was never disclosed on hacker forums, confirming that the operation was carried out by a member of the original gang.

Although the storage locations change, when the Ransom Cartel's encryptors were examined, several similarities in the configuration's structure were uncovered. Some configuration settings are missing in the Ransom Cartel, indicating that the authors are either attempting to make the malware leaner or are using an earlier version of the REvil as their base. The similarities are strongest in the encryption method, with the Ransom Cartel samples producing multiple pairs of public/private keys and session secrets, a REvil system that was very effective in the Kaseya attacks. Both use the file encryption techniques Salsa20 and Curve25519, and the structure of the encryption routines is also very similar. The Ransom Cartel clones lack REvil's powerful obfuscation, which is a fascinating discovery because it could imply that the new malware developers do not have access to REvil's original obfuscation engine.

The Windows Data Protection API (DPAPI) is one of the identified Ransom Cartel methods that is not found in REvil attacks. It instead uses a tool named "DonPAPI" to search hosts for DPAPI blobs containing Wi-Fi keys, credentials saved in web browsers, and RDP passwords. The blobs are then downloaded and decrypted locally on the workstation. These credentials are subsequently used to access the vCenter web interfaces of the compromised Linux ESXi systems. Threat actors terminate all critical functions, shut down virtual machines, and encrypt all data connected to VMware (.log, .vmdk, .vmem, .vswp, .vmsn). The use of DonPAPI, an extremely unique technology, demonstrates that the Ransom Cartel's operators are sophisticated threat actors.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

This document is for e-communication only.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | New Ransomware Ransom Cartel linked with REvil

Tracker ID: TN1021 **Date:** 27/Oct/2022 **Category:** Malware **Industry:** All **Region**: All

MITRE ATT&CK Tactics

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

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.
- Ensure only authorized personnel are using enterprise VPN and critical RDP, Citrix, or VNC credentials. Enforce periodic password changes and key rotation. Make sure the credentials are complex, unique, and not reused on another platform.
- As a protective measure, prevent unnecessary PowerShell execution by implementing policies and standards that permit only signed scripts to execute.
- Apply the principle of least privilege and provide the bare minimum of access or permission required to complete a task.
- Immediately identify the systems vulnerable to the Print Nightmare vulnerability and apply the vendor-provided patches ASAP.
- Check for any modifications made in the registry to disable UAC remote restrictions that set SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy to 1.
- Continuously monitor for suspicious or anomalous activities. Collect and review relevant logs, data, and artifacts to identify any threat in the network.
- Lookout for suspicious activities, including usage of "wevtutil" to clear the Windows event logs or deletion of rules in the Windows Defender Firewall exception list related to AnyDesk.
- Check that all security software components are enabled on all systems and that a policy is in place requiring the administrator password to be entered in the event of attempts to disable protection.
- 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.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

This document is for e-communication only.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | New Ransomware Ransom Cartel linked with REvil

Tracker ID: TN1021 **Date:** 27/Oct/2022 **Category:** Malware **Industry:** All **Region**: All

References

- Bill Toulas, Ransom Cartel linked to notorious REvil ransomware operation, Bleeping Computer, 18th October 2022, External Link (www.bleepingcomputer.com).
- Amer Elsad, Ransom Cartel Ransomware: A Possible Connection With Revil, Palo Alto Networks 14th October 2022, External Link (unit42.paloaltonetworks.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

*

SHA-256 Hash	IPs
55e4d509de5b0f1ea888ff87eb0d190c328a559d7cc5653c46947e57c0f01ec5	108.62.103.193
2411a74b343bbe51b2243985d5edaaabe2ba70e0c923305353037d1f442a91f5	179.43.151.115
	185.129.62.62
	185.143.223.13
	185.239.222.240
	185.253.163.23
	80.85.155.17
	80.85.157.8

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

This document is for e-communication only.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia