KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Clop utilizes Raspberry Robin Worm for pre-ransomware activity

Tracker ID: TN1103 **Date:** 07/Nov/2022 **Category:** Malware **Industry:** All **Region**: All

Background

A recent activity has been identified that indicates the Raspberry Robin worm is part of a sophisticated and interconnected malware ecosystem, with linkages to other malware families and additional infection techniques beyond its original USB drive propagation. DEV-0950 was discovered employing Clop ransomware to encrypt a victim's network that had been infiltrated by the Raspberry Robin worm. This malicious behavior linked with DEV-0950 is similar to those of financially motivated cybercrime organizations known as FIN11 and TA505, which are known for installing Clop payloads ransomware on targets' systems.

In addition to delivering ransomware, Raspberry Robin has been used to deploy IcedID, Bumblebee, and Truebot as second-stage payloads onto victim systems. In October 2022, researchers observed Raspberry Robin infections followed by Cobalt Strike activity from DEV-0950. This operation, which included Truebot infections in certain cases, finally led to the deployment of the Clop ransomware. This suggests that Raspberry Robin's operators are selling initial access to compromised enterprise systems to ransomware gangs and affiliates, who now have another route into their targets' networks in addition to phishing emails and malicious advertising.

Moreover, in late July, Microsoft also discovered Evil Corp pre-ransomware behaviour on networks where an access broker identified as DEV-0206 installed the FakeUpdates (aka SocGholish) backdoor on Raspberry Robin-infected devices. On September 2021, Red Canary discovered Raspberry Robin spreading to other systems via compromised USB devices containing a malicious .LNK file. Once the USB is connected and the user clicks on the LNK file, the worm executes a a msiexec process to load a second malicious file stored on the infected drive. Then, it connects with its command-and-control servers (C2) on infected Windows devices. Furthermore, after bypassing UAC (User Account Control) it exploits several trusted Windows programs on compromised systems to deliver and execute additional payloads like fodhelper, msiexec, and odbcconf.

The Raspberry Robin malware infestation was discovered on the networks of hundreds of enterprises from different industries. Nearly 1,000 firms have been hit by the worm. Raspberry Robin's infection chain is intricate, with several infection spots that can result in various outcomes. To prevent the impact of these complex and highly interrelated cybercriminal threats, organisations should build a robust prevention and detection strategy, ensure credential hygiene, least privileges, and network segmentation.

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

KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Clop utilizes Raspberry Robin Worm for pre-ransomware activity

Tracker ID: TN1103 **Date:** 04/Nov/2022 **Category:** Malware **Industry:** All **Region**: All

MITRE ATT&CK Tactics

Initial Access, Execution 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.
- Prevent drives from using autorun and execution code on insertion or mount.
- Continuously monitor for anomalous activities, including suspicious process launched using cmd.exe or suspicious behavior by msiexec.exe. Collect and review relevant logs, data, and artifacts to identify any threat in the network.
- Enforce periodic password changes and key rotation. Make sure the credentials are complex, unique, and not reused on another platform. Apply the principle of least privilege and provide the bare minimum of access or permission required to complete a task.
- Ensure security software components are up-to-date and 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.

References

- Microsoft, Raspberry Robin worm part of larger ecosystem facilitating pre-ransomware activity, Microsoft Security Threat Intelligence, 27th October 2022, External Link (www.microsoft.com).
- Sergiu Gatlan, Microsoft links Raspberry Robin worm to Clop ransomware attacks, Bleeping Computer, 27th October 2022, External Link (www.bleepingcomputer.com).
- Tara Seals, Raspberry Robin's Cyber Worm Infects Thousands of Endpoints, Dark Reading, 28th October 2022, External Link (www.darkreading.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

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

KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Clop utilizes Raspberry Robin Worm for pre-ransomware activity

Tracker ID: TN1103 **Date:** 07/Nov/2022 **Category:** Malware **Industry:** All **Region**: All

*

SHA256 Hash	IP	Domain	URL
d1224c08da923517d65c164932ef8d931633e5376f74bf0655b72d559cc32fd2	146[.]70[.]93[.]10	ads[.]softupdt[.]com	hxxps://codeload[.]github[.]com/downloader2607/download64_12/zip/refs/heads/main
0b214297e87360b3b7f6d687bdd7802992bc0e89b170d53bf403e536e07e396e		aviadronazhed[.]com	hxxps://spideroak[.]com/storage/OVPXG4DJMRSXE33BNNPWC5LUN5PTSMRTGAZTG/shared/5392194-1-1040/Setup_64_1.zip?b6755c86e52ceecf8d806bf814690691
0c435aadaa3c42a71ad8ff80781def4c8ce085f960d75f15b6fee8df78b2ac38		guteyutur[.]com	hxxps://dsfdsfgb[.]azureedge[.]net/332_332/universupdatepluginx84.zip
f18a54ba72df1a17daf21b519ffeee8463cfc81c194a8759a698709f1c9a3e87			hxxps://cdn[.]discordapp[.]com/attachments/1004390520904220838/1008127492449648762/Setup_64_11.zip
5c15151a29fab8a2d58fa55aa6c88a58a456b0a6bc959b843e9ceb2295c61885			
7e39dcd15307e7de862b9b42bf556f2836bf7916faab0604a052c82c19e306ca			

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