KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | New “Venus Ransomware” targets publicly exposed RDP

Tracker ID: TN1019 **Date:** 28/Oct/2022 **Category:** Malware **Industry:** All **Region**: All

Background

Threat actors are encrypting Windows PCs with a unique "Venus Ransomware" by penetrating into publicly exposed Remote Desktop Services. Venus Ransomware originally emerged in the middle of August 2022 and has since infected targets worldwide. The attacker gained access to a victim's corporate network via the Windows Remote Desktop protocol. It exploited internet-facing RDP for the initial network connection even when the service was running on a non-standard port number. Meanwhile, another ransomware has been identified using the same encrypted file extension since 2021. It's uncertain if they're related.

Once launched, the Venus ransomware will attempt to terminate 39 processes related to database servers and Microsoft Office applications, including “taskkill, msftesql.exe, sqlagent.exe, sqlbrowser.exe, sqlservr.exe, sqlwriter.exe, oracle.exe, ocssd.exe, dbsnmp.exe, synctime.exe, mydesktopqos.exe, agntsvc.exe, isqlplussvc.exe, xfssvccon.exe, mydesktopservice.exe, ocautoupds.exe, agntsvc.exe, agntsvc.exe, agntsvc.exe, encsvc.exe, firefoxconfig.exe, tbirdconfig.exe, ocomm.exe, mysqld.exe, mysqld-nt.exe, mysqld-opt.exe, dbeng50.exe, sqbcoreservice.exe, excel.exe, infopath.exe, msaccess.exe, mspub.exe, onenote.exe, outlook.exe, powerpnt.exe, sqlservr.exe, thebat64.exe, thunderbird.exe, winword.exe, wordpad.exe”.

The malware also deletes shadow copy volumes, disables data execution prevention, and deletes event logs. It appends the ".venus" extension to encrypted files. For example, a file called test.jpg would be encrypted and renamed test.jpg.venus. It will then append the filemarker 'goodgamer' and other metadata to the end of each encrypted file. After the ransomware has finished encrypting the device, it creates an HTA ransom message in the %Temp% folder, which is instantly displayed. It includes a TOX address as well as an email address for contacting the attacker and negotiating a ransom payment. The ransom note ends with a base64 encoded blob, which is most likely an encrypted decryption key.

The Venus ransomware is quite active, with fresh submissions to ID Ransomware being released daily. We advise enterprises to be cautious and ensure that remote desktop services are not publicly exposed. Furthermore, RDP services are firewall-protected and only available via VPN.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | New “Venus Ransomware” targets publicly exposed RDP

Tracker ID: TN1019 **Date:** 28/Oct/2022 **Category:** Malware **Industry:** All **Region**: All

MITRE ATT&CK Tactics

Initial Access, Discovery, Execution, Lateral Movement 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.
- Ensure that Remote Desktop services are behind a firewall, are not publicly exposed, and are only accessible via VPN.
- Apply the principle of least privilege and provide the bare minimum of access or permission required to complete a task.
- 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 deletion of event logs, shadow copy volumes, and disabling of data execution prevention.
- Ensure 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.

References

- Lawrence Abrams, Venus Ransomware targets publicly exposed Remote Desktop services, Bleeping Computer, 16th October 2022, External Link (www.bleepingcomputer.com).
- Cyware Alerts - Hacker News, Venus Ransomware Abuses Remote Desktop Services, 18th October 2022, External Link (cyware.com).

KPMG in India Cyber Response Hotline : +91 9176471471

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 josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | New “Venus Ransomware” targets publicly exposed RDP

Tracker ID: TN1019 **Date:** 28/Oct/2022 **Category:** Malware **Industry:** All **Region**: All

*

SHA-256
6d8e2d8f6aeb0f4512a53fe83b2ef7699513ebaff31735675f46d1beea3a8e05
2e2cef71bf99594b54e00d459480e1932e0230fb1cbee24700fbc2f5f631bf12