HC3: Analyst Note
November 9, 2022 TLP:CLEAR Report: 202211091400

Venus Ransomware Targets Publicly Exposed Remote Desktop Services

Executive Summary
HC3 is aware of at least one healthcare entity in the United States falling victim to Venus ransomware recently. The threat actors behind Venus ransomware operations are known to target publicly exposed Remote Desktop Services to encrypt Windows devices. This report provides additional information, indicators of compromise, techniques and corresponding mitigations associated with Venus ransomware.

Report
Venus ransomware appears to have begun operating in the middle of August 2022 and has since encrypted victims worldwide. When executed, the Venus ransomware will attempt to terminate thirty-nine processes associated with database servers and Microsoft Office applications. As the ransomware appears to be targeting publicly-exposed Remote Desktop services, even those running on non-standard TCP ports, it is vital to put these services behind a firewall. The ransomware will also delete event logs, Shadow Copy Volumes, and disable Data Execution Prevention using the following command. When encrypting files, the ransomware uses AES and RSA algorithms and will append the '.venus' extension. In each encrypted file, a 'goodgamer' filemarker and other information are added to the end of the file.

HC3 recommends the following mitigations for ransomware:

- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, and secure location.
- Implement network segmentation and maintain offline backups of data to ensure limited interruption to the organization.
- Regularly back up data and password-protect backup copies offline. Ensure copies of critical data are not accessible for modification or deletion from the system where the data resides.
- Install and regularly update antivirus software on all hosts and enable real time detection.
- Install updates/patch operating systems, software, and firmware as soon as they are released.
- Consider adding an email banner to emails received from outside your organization.
- Disable hyperlinks in received emails. Disable unused ports.
- Enforce multi-factor authentication (MFA) and consider MFA for securing RDP access while placing RDP behind a Virtual Private Network (VPN).
- Use National Institute for Standards and Technology (NIST) standards for developing and managing password policies. Require administrator credentials to install software.
- Consider implementing rate limiting to slow down the speed that attackers can guess logins.

Analyst Comment
The Venus ransomware variant, also known as GOODGAME, should not be confused with VenusLocker, which uses the '.venusf' file extension during encryption. The operators of Venus ransomware are not believed to operate as a ransomware-as-a-service (RaaS) model, and no associated data leak site (DLS) exists at this time. Despite this, the ransomware uses a wide variety of contact email addresses and TOX IDs, indicating that it is likely that multiple threat actors are distributing the ransomware. Open source reports indicate that initial ransom demands may start around 1 BTC, or less than USD $20,000. *Please note that this report was updated on November 23 to remove potentially false positive IP addresses from the IOCs.*

HC3: Analyst Note
November 9, 2022 TLP:CLEAR Report: 202211091400

Threat Actor Communications

Type	Indicator
Email address	decryptdata[@]onionmail[.]org
Jabber	decryptdata[@]xmpp[.]jp
TOX	9DA3D60F51FB83B539BA0CC79B6D4BE83003F8E7A294B531B6EA05102486855ADEEFFF5A90C8
Email address	skynetwork[@]tutanota[.]com
Email address	skynetwork[@]onionmail[.]org
Email address	skynetwork[@]cock[.]li
Email address	getdecrypt[@]disroot[.]org

Indicators of Compromise (IOCs)

Type	Indicator
File name	venus.exe
File name	yJnZ0N28zU.exe
MD5	eae3f9f84a8b6756db599963aa4f49d1
SHA1	c40909226c102ceb3cf97e9037c590f1623af013
SHA256	0a4e5832841ffff9f8d27ce8216d655c8743b682fff0f90dee6bd3ea83dec028
File name	345.exe
MD5	f5e72bf445387eddec000e0238adf873
SHA1	895eb3047e7a28ce219fdd7e7ad5ce2a61312d93
SHA256	2e2cef71bf99594b54e00d459480e1932e0230fb1cbee24700fbc2f5f631bf12
File name	347.mal
MD5	0d4247600f91e28bd390c91dd61ccd7f
SHA1	ba145483608a4ea567ed3c3c2b7e396098f5386a

SHA256	6d8e2d8f6aeb0f4512a53fe83b2ef7699513ebaff31735675f46d1beea3a8e05
File name	executable.exe
File name	program.exe
MD5	9aa3cc9d7c641ea22cfa3e5233e13c94
SHA1	1970f6c17567d56c3e7840fe33a6959dd887fca2
SHA256	49fd52a3f3d1d46dc065217e588d1d29fba4d978cd8fdb2887fd603320540f71

MITRE ATT&CK Matrix for Venus Ransomware

ATT&CK ID	Tactic	Technique
T1059	Execution	Command and Scripting Interpreter
T1047	Execution	Windows Management Instrumentation
T1106	Execution	Native API
T1053	Execution	Scheduled Task/Job
T1574.002	Persistence	DLL Side-Loading
T1053	Persistence	Scheduled Task/Job
T1547.001	Persistence	Registry Run Keys / Startup Folder
T1574.002	Privilege Escalation	DLL Side-Loading
T1134	Privilege Escalation	Access Token Manipulation
T1055	Privilege Escalation	Process Injection
T1053	Privilege Escalation	Scheduled Task/Job
T1547.001	Privilege Escalation	Registry Run Keys / Startup Folder
T1562.001	Defense Evasion	Disable or Modify Tools
T1140	Defense Evasion	Deobfuscate/Decode Files or Information
T1027	Defense Evasion	Obfuscated Files or Information
T1574.002	Defense Evasion	DLL Side-Loading
T1070.004	Defense Evasion	File Deletion
T1036	Defense Evasion	Masquerading
T1134	Defense Evasion	Access Token Manipulation
T1055	Defense Evasion	Process Injection

T1056	Credential Access	Input Capture
T1124	Discovery	System Time Discovery
T1083	Discovery	File and Directory Discovery
T1082	Discovery	System Information Discovery
T1518.001	Discovery	Security Software Discovery
T1018	Discovery	Remote System Discovery
T1016	Discovery	System Network Configuration Discovery
T1560	Collection	Archive Collected Data
T1114	Collection	Email Collection
T1056	Collection	Input Capture
T1105	Command and Control	Ingress Tool Transfer
T1573	Command and Control	Encrypted Channel
T1095	Command and Control	Non-Application Layer Protocol
T1071	Command and Control	Application Layer Protocol
T1485	Impact	Data Destruction
T1486	Impact	Data Encrypted for Impact
T1490	Impact	Inhibit System Recovery
T1491	Impact	Defacement

References

Venus Ransomware targets publicly exposed Remote Desktop services (October 16, 2022)
https://www.bleepingcomputer.com/news/security/venus-ransomware-targets-publicly-exposed-remote-desktop-services/

Venus ransomware targets remote desktop services (October 20, 2022)
https://www.malwarebytes.com/blog/news/2022/10/venus-ransomware-targets-remote-desktop-services

Venus Ransomware Support & Help topic (.venus & README.html) (October 6, 2022)
https://www.bleepingcomputer.com/forums/t/777945/venus-ransomware-support-help-topic-venus-readmehtml/

Windows Analysis Report for yJnZ0N28zU.exe (October 16, 2022)
https://www.joesandbox.com/analysis/724026/1/html

VirusTotal Report for 2e2cef71bf99594b54e00d459480e1932e0230fb1cbee24700fbc2f5f631bf12

https://www.virustotal.com/gui/file/2e2cef71bf99594b54e00d459480e1932e0230fb1cbee24700fbc2f5f631bf12/summary

VirusTotal Report for 6d8e2d8f6aeb0f4512a53fe83b2ef7699513ebaff31735675f46d1beea3a8e05
https://www.virustotal.com/gui/file/6d8e2d8f6aeb0f4512a53fe83b2ef7699513ebaff31735675f46d1beea3a8e05/summary

VirusTotal Report for 49fd52a3f3d1d46dc065217e588d1d29fba4d978cd8fdb2887fd603320540f71
https://www.virustotal.com/gui/file/49fd52a3f3d1d46dc065217e588d1d29fba4d978cd8fdb2887fd603320540f71/summary

NJCCIC Threat Profile: VenusLocker (December 28, 2016)
https://www.cyber.nj.gov/threat-center/threat-profiles/ransomware-variants/venuslocker

Venus Locker another .NET ransomware (August 12, 2016)
https://www.malwarebytes.com/blog/news/2016/08/venus-locker-another-net-ransomware

Twitter, @linuxct (October 6, 2022)
https://twitter.com/linuxct/status/1577926820636286977

Venus ransomware – Aliases: Goodgamer, Goodgame (May 14, 2021)
https://id-ransomware.blogspot.com/2021/05/venus-ransomware.html

CISA Stop Ransomware Guide
https://www.cisa.gov/stopransomware/ransomware-guide

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback