JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP:CLEAR

Product ID: AA23-319A

November 15, 2023

#StopRansomware: Rhysida Ransomware

SUMMARY

Note: *This joint Cybersecurity Advisory (CSA) is part of an ongoing #StopRansomware effort to publish advisories for network defenders detailing various ransomware variants and ransomware threat actors. These #StopRansomware advisories include recently and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware. Visit stopransomware.gov to see all #StopRansomware advisories and to learn more about other ransomware threats and no-cost resources.*

Actions to take today to mitigate malicious cyber activity:

- Prioritize remediating known exploited vulnerabilities.
- Enable multifactor authentication (MFA) for all services to the extent possible, particularly for webmail, VPN, and accounts that access critical systems.
- Segment networks to prevent the spread of ransomware.

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) are releasing this joint CSA to disseminate known Rhysida ransomware IOCs and TTPs identified through investigations as recently as September 2023. Rhysida—an emerging ransomware variant—has predominately been deployed against the education, healthcare, manufacturing, information technology, and government sectors since May 2023. The information in this CSA is derived from related incident response investigations and malware analysis of samples discovered on victim networks.

FBI, CISA, and the MS-ISAC encourage organizations to implement the recommendations in the Mitigations section of this CSA to reduce the likelihood and impact of Rhysida ransomware and other ransomware incidents.

To report suspicious or criminal activity related to information found in this joint Cybersecurity Advisory, contact your local FBI field office or CISA's 24/7 Operations Center at Report@cisa.gov or (888) 282-0870. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. SLTT organizations should report incidents to the MS-ISAC (866-787-4722 or SOC@cisecurity.org).

TECHNICAL DETAILS

Note: This advisory uses the MITRE ATT&CK® for Enterprise framework, version 14. See the ATT&CK Tactics and Techniques section for tables mapped to the threat actors' activity.

Overview

Threat actors leveraging Rhysida ransomware are known to impact "targets of opportunity," including victims in the education, healthcare, manufacturing, information technology, and government sectors. Open source reporting details similarities between Vice Society (DEV-0832)[1] activity and the actors observed deploying Rhysida ransomware. Additionally, open source reporting[2] has confirmed observed instances of Rhysida actors operating in a ransomware-as-a-service (RaaS) capacity, where ransomware tools and infrastructure are leased out in a profit-sharing model. Any ransoms paid are then split between the group and the affiliates.

For additional information on Vice Society actors and associated activity, see the joint CSA #StopRansomware: Vice Society.

Initial Access

Rhysida actors have been observed leveraging external-facing remote services to initially access and persist within a network. Remote services, such as virtual private networks (VPNs), allow users to connect to internal enterprise network resources from external locations. Rhysida actors have commonly been observed authenticating to internal VPN access points with compromised valid credentials [T1078], notably due to organizations lacking MFA enabled by default. Additionally, actors have been observed exploiting Zerologon (CVE-2020-1472)—a critical elevation of privileges vulnerability in Microsoft's Netlogon Remote Protocol [T1190]—as well as conducting successful phishing attempts [T1566]. **Note:** Microsoft released a patch for CVE-2020-1472 on August 11, 2020.[3]

Living off the Land

Analysis identified Rhysida actors using living off the land techniques, such as creating Remote Desktop Protocol (RDP) connections for lateral movement [T1021.001], establishing VPN access, and utilizing PowerShell [T1059.001]. Living off the land techniques include using native (built into the operating system) network administration tools to perform operations. This allows the actors to evade detection by blending in with normal Windows systems and network activities.

`Ipconfig` [T1016], `whoami` [T1033], `nltest` [T1482], and several `net` commands have been used to enumerate victim environments and gather information about domains. In one instance of using compromised credentials, actors leveraged `net` commands within PowerShell to identify logged-in users and performed reconnaissance on network accounts within the victim environment. **Note:** The following commands were not performed in the exact order listed.

- `net user [username] /domain` [T1087.002]
- `net group "domain computers" /domain` [T1018]
- `net group "domain admins" /domain` [T1069.002]

- `net localgroup administrators` [T1069.001]

Analysis of the master file table (MFT)[4] identified the victim system generated the `ntuser.dat` registry hive, which was created when the compromised user logged in to the system for the first time. This was considered anomalous due to the baseline of normal activity for that particular user and system. **Note:** The MFT resides within the New Technology File System (NTFS) and houses information about a file including its size, time and date stamps, permissions, and data content.

Leveraged Tools

Table 1 lists legitimate tools Rhysida actors have repurposed for their operations. The legitimate tools listed in this joint CSA are all publicly available. Use of these tools should not be attributed as malicious without analytical evidence to support they are used at the direction of or controlled by threat actors.

Table 1: Tools Leveraged by Rhysida Actors

Disclaimer: Organizations are encouraged to investigate and vet use of these tools prior to performing remediation actions.

Name	Description
cmd.exe	The native command line prompt utility.
PowerShell.exe	A native command line tool used to start a Windows PowerShell session in a Command Prompt window.
PsExec.exe	A tool included in the PsTools suite used to execute processes remotely. Rhysida actors heavily leveraged this tool for lateral movement and remote execution.
mstsc.exe	A native tool that establishes an RDP connection to a host.
PuTTY.exe	Rhysida actors have been observed creating Secure Shell (SSH) PuTTy connections for lateral movement. In one example, analysis of PowerShell console host history for a compromised user account revealed Rhysida actors leveraged PuTTy to remotely connect to systems via SSH [T1021.004].
PortStarter	A back door script written in Go that provides functionality for modifying firewall settings and opening ports to pre-configured command and control (C2) servers.[1]
secretsdump	A script used to extract credentials and other confidential information from a system. Rhysida actors have been observed using this for NTDS dumping [T1003.003] in various instances.
ntdsutil.exe	A standard Windows tool used to interact with the NTDS database. Rhysida actors used this tool to extract and dump the `NTDS.dit` database from the domain controller containing hashes for all Active Directory (AD) users.

Name	Description
	Note: It is strongly recommended that organizations conduct domain-wide password resets and double Kerberos TGT password resets if any indication is found that the `NTDS.dit` file was compromised.
AnyDesk	A common software that can be maliciously used by threat actors to obtain remote access and maintain persistence [T1219]. AnyDesk also supports remote file transfer.
wevtutil.exe	A standard Windows Event Utility tool used to view event logs. Rhysida actors used this tool to clear a significant number of Windows event logs, including system, application, and security logs [T1070.001].
PowerView	A PowerShell tool used to gain situational awareness of Windows domains. Review of PowerShell event logs identified Rhysida actors using this tool to conduct additional reconnaissance-based commands and harvest credentials.

Rhysida Ransomware Characteristics

Execution

In one investigation, Rhysida actors created two folders in the C:\ drive labeled `in` and `out`, which served as a staging directory (central location) for hosting malicious executables. The `in` folder contained file names in accordance with host names on the victim's network, likely imported through a scanning tool. The `out` folder contained various files listed in Table 2 below**Error! Reference source not found.**. Rhysida actors deployed these tools and scripts to assist system and network-wide encryption.

Table 2: Malicious Executables Affiliated with Rhysida Infections

File Name	Hash (SHA256)	Description
conhost.exe	6633fa85bb234a75927b23417313e51a4c155e12f71da3959e168851a600b010	A ransomware binary.
psexec.exe	078163d5c16f64caa5a14784323fd51451b8c831c73396b967b4e35e6879937b	A file used to execute a process on a remote or local host.
S_0.bat	1c4978cd5d750a2985da9b58db137fc74d28422f1e087fd77642faa7efe7b597	A batch script likely used to place `1.ps1` on victim systems for ransomware staging purposes [T1059.003].
1.ps1	4e34b9442f825a16d7f6557193426ae7a18899ed46d3b896f6e4357367276183	Identifies an extension block list of files to encrypt and not encrypt.

File Name	Hash (SHA256)	Description
S_1.bat	97766464d0f2f91b82b557ac656ab82e15cae7896b1d8c98632ca53c15cf06c4	A batch script that copies `conhost.exe` (the encryption binary) on an imported list of host names within the `C:\Windows\Temp` directory of each system.
S_2.bat	918784e25bd24192ce4e999538be96898558660659e3c624a5f27857784cd7e1	Executes `conhost.exe` on compromised victim systems, which encrypts and appends the extension of `.Rhysida` across the environment.

Rhysida ransomware uses a Windows 64-bit Portable Executable (PE) or common object file format (COFF) compiled using MinGW via the GNU Compiler Collection (GCC), which supports various programming languages such as C, C++, and Go. The cryptographic ransomware application first injects the PE into running processes on the compromised system [T1055.002]. Additionally, third-party researchers identified evidence of Rhysida actors developing custom tools with program names set to "Rhysida-0.1" [T1587].

Encryption

After mapping the network, the ransomware encrypts data using a 4096-bit RSA encryption key with a ChaCha20 algorithm [T1486]. The algorithm features a 256-bit key, a 32-bit counter, and a 96-bit nonce along with a four-by-four matrix of 32-bit words in plain text. Registry modification commands [T1112] are not obfuscated, displayed as plain-text strings and executed via `cmd.exe`.

Rhysida's encryptor runs a file to encrypt and modify all encrypted files to display a `.rhysida` extension.[5] Following encryption, a PowerShell command deletes the binary [T1070.004] from the network using a hidden command window [T1564.003]. The Rhysida encryptor allows arguments `-d` (select a directory) and `-sr` (file deletion), defined by the authors of the code as parseOptions.[6] After the lines of binary strings complete their tasks, they delete themselves through the control panel to evade detection.

Data Extortion

Rhysida actors reportedly engage in "double extortion" [T1657]—demanding a ransom payment to decrypt victim data and threatening to publish the sensitive exfiltrated data unless the ransom is paid.[5],[7] Rhysida actors direct victims to send ransom payments in Bitcoin to cryptocurrency wallet addresses provided by the threat actors. As shown in Figure 1, Rhysida ransomware drops a ransom note named "CriticalBreachDetected" as a PDF file—the note provides each company with a unique code and instructions to contact the group via a Tor-based portal.

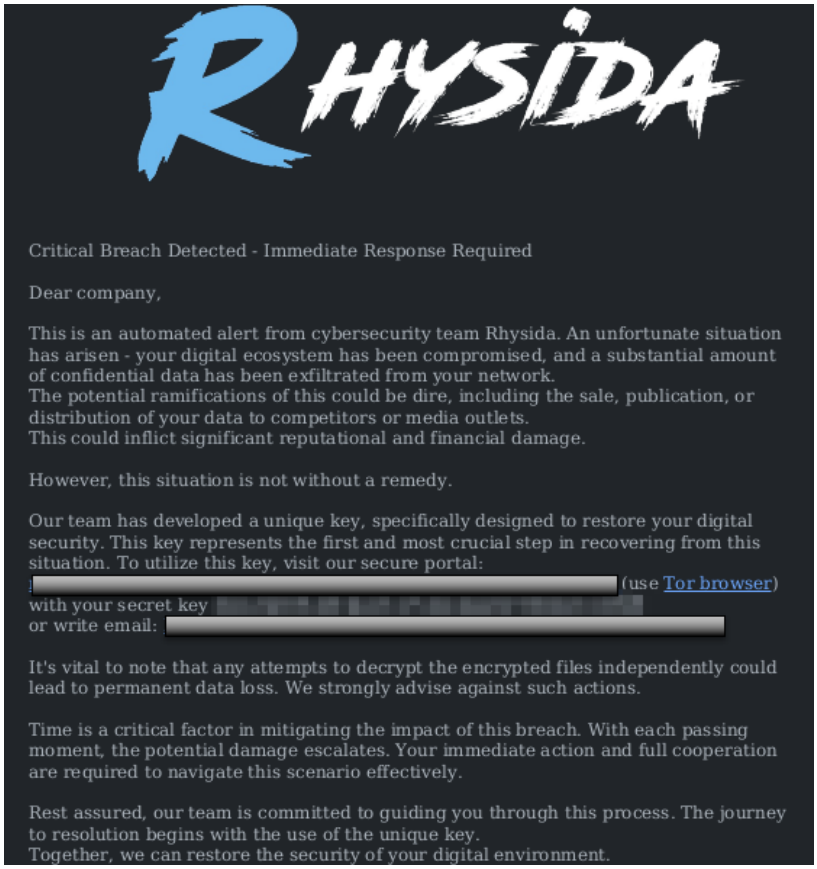

Figure 1: Rhysida Ransom Note

Identified in analysis and also listed in open source reporting, the contents of the ransom note are embedded as plain-text in the ransom binary, offering network defenders an opportunity to deploy string-based detection for alerting on evidence of the ransom note. Rhysida threat actors may target systems that do not use command-line operating systems. The format of the PDF ransom notes could indicate that Rhysida actors only target systems that are compatible with handling PDF documents.[8]

INDICATORS OF COMPROMISE

On November 10, 2023, Sophos published TTPs and IOCs identified from analysis conducted for six separate incidents.[9] The C2 IP addresses listed in Table 3 were derived directly from Sophos' investigations and are listed on GitHub among other indicators.[10]

Table 3: C2 IP Addresses Used for Rhysida Operations

C2 IP Address
5.39.222[.]67
5.255.99[.]59
51.77.102[.]106

108.62.118[.]136
108.62.141[.]161
146.70.104[.]249
156.96.62[.]58
157.154.194[.]6

Additional IOCs were obtained from FBI, CISA, and the MS-ISAC's investigations and analysis. The email addresses listed in Table 4 are associated with Rhysida actors' operations. Rhysida actors have been observed creating Onion Mail email accounts for services or victim communication, commonly in the format: `[First Name][Last Name]@onionmail[.]org`.

Table 4: Email Addresses Used to Support Rhysida Operations

Email Address
rhysidaeverywhere@onionmail[.]org
rhysidaofficial@onionmail[.]org

Rhysida actors have also been observed using the following files and executables listed in Table 5 to support their operations.

Table 5: Files Used to Support Rhysida Operations

Disclaimer: Organizations are encouraged to investigate the use of these files for related signs of compromise prior to performing remediation actions.

File Name	Hash (SHA256)
Sock5.sh	48f559e00c472d9ffe3965ab92c6d298f8fb3a3f0d6d203cd2069bfca4bf3a57
PsExec64.exe	edfae1a69522f87b12c6dac3225d930e4848832e3c551ee1e7d31736bf4525ef
PsExec.exe	078163d5c16f64caa5a14784323fd51451b8c831c73396b967b4e35e6879937b
PsGetsid64.exe	201d8e77ccc2575d910d47042a986480b1da28cf0033e7ee726ad9d45ccf4daa
PsGetsid.exe	a48ac157609888471bf8578fb8b2aef6b0068f7e0742fccf2e0e288b0b2cfdfb
PsInfo64.exe	de73b73eeb156f877de61f4a6975d06759292ed69f31aaf06c9811f3311e03e7
PsInfo.exe	951b1b5fd5cb13cde159cebc7c60465587e2061363d1d8847ab78b6c4fba7501
PsLoggedon64.exe	fdadb6e15c52c41a31e3c22659dd490d5b616e017d1b1aa6070008ce09ed27ea
PsLoggedon.exe	d689cb1dbd2e4c06cd15e51a6871c406c595790ddcdcd7dc8d0401c7183720ef

File Name	Hash (SHA256)
PsService64.exe	554f523914cdbaed8b17527170502199c185bd69a41c81102c50dbb0e5e5a78d
PsService.exe	d3a816fe5d545a80e4639b34b90d92d1039eb71ef59e6e81b3c0e043a45b751c
Eula.txt	8329bcbadc7f81539a4969ca13f0be5b8eb7652b912324a1926fc9bfb6ec005a
psfile64.exe	be922312978a53c92a49fefd2c9f9cc098767b36f0e4d2e829d24725df65bc21
psfile.exe	4243dc8b991f5f8b3c0f233ca2110a1e03a1d716c3f51e88faf1d59b8242d329
pskill64.exe	7ba47558c99e18c2c6449be804b5e765c48d3a70ceaa04c1e0fae67ff1d7178d
pskill.exe	5ef168f83b55d2cbd2426afc5e6fa8161270fa6a2a312831332dc472c95dfa42
pslist64.exe	d3247f03dcd7b9335344ebba76a0b92370f32f1cb0e480c734da52db2bd8df60
pslist.exe	ed05f5d462767b3986583188000143f0eb24f7d89605523a28950e72e6b9039a
psloglist64.exe	5e55b4caf47a248a10abd009617684e969dbe5c448d087ee8178262aaab68636
psloglist.exe	dcdb9bd39b6014434190a9949dedf633726fdb470e95cc47cdaa47c1964b969f
pspasswd64.exe	8d950068f46a04e77ad6637c680cccf5d703a1828fbd6bdca513268af4f2170f
pspasswd.exe	6ed5d50cf9d07db73eaa92c5405f6b1bf670028c602c605dfa7d4fcb80ef0801
psping64.exe	d1f718d219930e57794bdadf9dda61406294b0759038cef282f7544b44b92285
psping.exe	355b4a82313074999bd8fa1332b1ed00034e63bd2a0d0367e2622f35d75cf140
psshutdown64.exe	4226738489c2a67852d51dbf96574f33e44e509bc265b950d495da79bb457400
psshutdown.exe	13fd3ad690c73cf0ad26c6716d4e9d1581b47c22fb7518b1d3bf9cfb8f9e9123
pssuspend64.exe	4bf8fbb7db583e1aacbf36c5f740d012c8321f221066cc68107031bd8b6bc1ee
pssuspend.exe	95a922e178075fb771066db4ab1bd70c7016f794709d514ab1c7f11500f016cd
PSTools.zip	a9ca77dfe03ce15004157727bb43ba66f00ceb215362c9b3d199f000edaa8d61
Pstools.chm	2813b6c07d17d25670163e0f66453b42d2f157bf2e42007806ebc6bb9d114acc
psversion.txt	8e43d1ddbd5c129055528a93f1e3fab0ecdf73a8a7ba9713dc4c3e216d7e5db4
psexesvc.exe	This artifact is created when a user establishes a connection using `psexec`. It is removed after the connection is terminated, which is why there is no hash available for this executable.

MITRE ATT&CK TACTICS AND TECHNIQUES

See Tables 6-15 for all referenced threat actor tactics and techniques in this advisory. For assistance with mapping malicious cyber activity to the MITRE ATT&CK framework, see CISA and MITRE's Best Practices for MITRE ATT&CK Mapping and CISA's Decider Tool.

Additional notable TTPs have been published by the Check Point Incident Response Team.[11]

Table 6: Resource Development

Technique Title	ID	Use
Develop Capabilities	T1587	Rhysida actors have been observed developing resources and custom tools, particularly with program names set to "Rhysida-0.1" to gain access to victim systems.

Table 7: Initial Access

Technique Title	ID	Use
Valid Accounts	T1078	Rhysida actors are known to use valid credentials to access internal VPN access points of victims.
Exploit Public-Facing Application	T1190	Rhysida actors have been identified exploiting Zerologon, a critical elevation of privilege vulnerability within Microsoft's Netlogon Remote Protocol.
Phishing	T1566	Rhysida actors are known to conduct successful phishing attacks.

Table 8: Execution

Technique Title	ID	Use
Command and Scripting Interpreter: PowerShell	T1059.001	Rhysida actors used PowerShell commands (`ipconfig`, `nltest`, `net`) and various scripts to execute malicious actions.
Command and Scripting Interpreter: Windows Command Shell	T1059.003	Rhysida actors used batch scripting to place `1.ps1` on victim systems to automate ransomware execution.

Table 9: Privilege Escalation

Technique Title	ID	Use
Process Injection: Portable Executable Injection	T1055.002	Rhysida actors injected a Windows 64-bit PE cryptographic ransomware application into running processes on compromised systems.

Table 10: Defense Evasion

Technique Title	ID	Use
Indicator Removal: Clear Windows Event Logs	T1070.001	Rhysida actors used `wevtutil.exe` to clear Windows event logs, including system, application, and security logs.
Indicator Removal: File Deletion	T1070.004	Rhysida actors used PowerShell commands to delete binary strings.
Hide Artifacts: Hidden Window	T1564.003	Rhysida actors have executed hidden PowerShell windows.

Table 11: Credential Access

Technique Title	ID	Use
OS Credential Dumping: NTDS	T1003.003	Rhysida actors have been observed using `secretsdump` to extract credentials and other confidential information from a system, then dumping NTDS credentials.
Modify Registry	T1112	Rhysida actors were observed running registry modification commands via `cmd.exe`.

Table 12: Discovery

Technique Title	ID	Use
System Network Configuration Discovery	T1016	Rhysida actors used the `ipconfig` command to enumerate victim system network settings.
Remote System Discovery	T1018	Rhysida actors used the command `net group “domain computers” /domain` to enumerate servers on a victim domain.

Technique Title	ID	Use
System Owner/User Discovery	T1033	Rhysida actors leveraged `whoami` and various `net` commands within PowerShell to identify logged-in users.
Permission Groups Discovery: Local Groups	T1069.001	Rhysida actors used the command `net localgroup administrators` to identify accounts with local administrator rights.
Permission Groups Discovery: Domain Groups	T1069.002	Rhysida actors used the command `net group "domain admins" /domain` to identify domain administrators.
Account Discovery: Domain Account	T1087.002	Rhysida actors used the command `net user [username] /domain` to identify account information.
Domain Trust Discovery	T1482	Rhysida actors used the Windows utility `nltest` to enumerate domain trusts.

Table 13: Lateral Movement

Technique Title	ID	Use
Remote Services: Remote Desktop Protocol	T1021.001	Rhysida actors are known to use RDP for lateral movement.
Remote Services: SSH	T1021.004	Rhysida actors used compromised user credentials to leverage PuTTy and remotely connect to victim systems via SSH.

Table 14: Command and Control

Technique Title	ID	Use
Remote Access Software	T1219	Rhysida actors have been observed using the AnyDesk software to obtain remote access to victim systems and maintain persistence.

Table 15: Impact

Technique Title	ID	Use
Data Encrypted for Impact	T1486	Rhysida actors encrypted victim data using a 4096-bit RSA encryption key that implements a ChaCha20 algorithm.
Financial Theft	T1657	Rhysida actors reportedly engage in "double extortion"—demanding a ransom payment to decrypt victim data and threatening to publish the sensitive exfiltrated data unless the ransom is paid.

MITIGATIONS

FBI, CISA, and the MS-ISAC recommend that organizations implement the mitigations below to improve your organization's cybersecurity posture. These mitigations align with the Cross-Sector Cybersecurity Performance Goals (CPGs) developed by CISA and the National Institute of Standards and Technology (NIST). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful threats, and TTPs. Visit CISA's Cross-Sector Cybersecurity Performance Goals for more information on the CPGs, including additional recommended baseline protections.

These mitigations apply to all critical infrastructure organizations and network defenders. FBI, CISA, and the MS-ISAC recommend incorporating secure-by-design and -default principles, limiting the impact of ransomware techniques and strengthening overall security posture. For more information on secure by design, see CISA's Secure by Design webpage.

- **Require phishing-resistant MFA** for all services to the extent possible, particularly for webmail, VPN, and accounts that access critical systems [CPG 2.H].
- **Disable command-line and scripting activities and permissions.** Privilege escalation and lateral movement often depend on software utilities running from the command line. If threat actors are not able to run these tools, they will have difficulty escalating privileges and/or moving laterally [CPG 2.N].
- **Implement verbose and enhanced logging within processes** such as command line auditing[12] and process tracking[13].
- **Restrict the use of PowerShell** using Group Policy and only grant access to specific users on a case-by-case basis. Typically, only those users or administrators who manage the network or Windows operating systems should be permitted to use PowerShell [CPG 2.E].
- **Update Windows PowerShell or PowerShell Core to the latest version** and uninstall all earlier PowerShell versions. Logs from Windows PowerShell prior to version 5.0 are either non-existent or do not record enough detail to aid in enterprise monitoring and incident response activities [CPG 1.E, 2.S, 2.T].

- **Enable enhanced PowerShell logging** [CPG 2.T, 2.U].
  - PowerShell logs contain valuable data, including historical operating system and registry interaction and possible TTPs of a threat actor's PowerShell use.
  - Ensure PowerShell instances (using the latest version) have module, script block, and transcription logging enabled (e.g., enhanced logging).
  - The two logs that record PowerShell activity are the PowerShell Windows event log and the PowerShell operational log. FBI, CISA, and the MS-ISAC recommend turning on these two Windows event logs with a retention period of at least 180 days. These logs should be checked on a regular basis to confirm whether the log data has been deleted or logging has been turned off. Set the storage size permitted for both logs to as large as possible.
- **Restrict the use of RDP and other remote desktop services to known user accounts and groups.** If RDP is necessary, apply best practices such as [CPG 2.W]:
  - Implement MFA for privileged accounts using RDP.
  - Use Remote Credential Guard[14] to protect credentials, particularly domain administrator or other high value accounts.
  - Audit the network for systems using RDP.
  - Close unused RDP ports.
  - Enforce account lockouts after a specified number of attempts.
  - Log RDP login attempts.
- Secure remote access tools by:
  - **Implementing application controls** to manage and control execution of software, including allowlisting remote access programs. Application controls should prevent the installation and execution of portable versions of unauthorized remote access and other software. A properly configured application allowlisting solution will block any unlisted application execution. Allowlisting is important as antivirus solutions may fail to detect the execution of malicious portable executables when the files use any combination of compression, encryption, or obfuscation.
  - Apply the recommendations in CISA's joint Guide to Securing Remote Access Software.

In addition, FBI, CISA, and the MS-ISAC recommend network defenders apply the following mitigations to limit potential adversarial use of common system and network discovery techniques, and to reduce the impact and risk of compromise by ransomware or data extortion actors:

- **Keep all operating systems, software, and firmware up to date.** Timely patching is one of the most efficient and cost-effective steps an organization can take to minimize its exposure to cybersecurity threats. Prioritize patching known exploited vulnerabilities in internet-facing systems [CPG 1.E].
- **Segment networks** to prevent the spread of ransomware. Network segmentation can help prevent the spread of ransomware by controlling traffic flows between—and access to—various subnetworks and by restricting adversary lateral movement [CPG 2.F].
- **Identify, detect, and investigate abnormal activity and potential traversal of the indicated ransomware with a network monitoring tool.** To aid in detecting ransomware, implement a tool that logs and reports all network traffic, including lateral movement activity on a network. Endpoint detection and response (EDR) tools are particularly useful for detecting

lateral connections as they have insight into common and uncommon network connections for each host [CPG 3.A].

- **Audit user accounts** with administrative privileges and configure access controls according to the principle of least privilege (PoLP) [CPG 2.E].
- **Implement time-based access for accounts set at the admin level and higher** [CPG 2.A, 2.E]. For example, the just-in-time (JIT) access method provisions privileged access when needed and can support the enforcement of PoLP (as well as the zero trust model). This is a process where a network-wide policy is set in place to automatically disable admin accounts at the AD level when the account is not in direct need. Individual users may submit their requests through an automated process that grants them access to a specified system for a set timeframe when they need to support the completion of a certain task.
- **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 (e.g., hard drive, storage device, or the cloud).
- **Maintain offline backups of data** and regularly maintain backups and their restoration (daily or weekly at minimum). By instituting this practice, organizations limit the severity of disruption to business operations [CPG 2.R].
- **Ensure all backup data is encrypted, immutable** (i.e., cannot be altered or deleted), and covers the entire organization's data infrastructure [CPG 2.K, 2.L, 2.R].
- **Forward log files to a hardened centralized logging server,** preferably on a segmented network [CPG 2.F]. Review logging retention rates, such as for VPNs and network-based logs.
- **Consider adding an email banner to emails** received from outside your organization [CPG 2.M].
- **Disable hyperlinks** in received emails.

VALIDATE SECURITY CONTROLS

In addition to applying mitigations, FBI, CISA, and the MS-ISAC recommend exercising, testing, and validating your organization's security program against the threat behaviors mapped to the MITRE ATT&CK for Enterprise framework in this advisory. FBI, CISA, and the MS-ISAC recommend testing your existing security controls inventory to assess how they perform against the ATT&CK techniques described in this advisory.

To get started:

1. Select an ATT&CK technique described in this advisory (see Tables 6-15).
2. Align your security technologies against the technique.
3. Test your technologies against the technique.
4. Analyze your detection and prevention technologies' performance.
5. Repeat the process for all security technologies to obtain a set of comprehensive performance data.
6. Tune your security program, including people, processes, and technologies, based on the data generated by this process.

FBI, CISA, and the MS-ISAC recommend continually testing your security program, at scale, in a production environment to ensure optimal performance against the MITRE ATT&CK techniques identified in this advisory.

RESOURCES

- CISA: #StopRansomware
- CISA: #StopRansomware Vice Society
- CISA: Known Exploited Vulnerabilities Catalog
- NIST: CVE-2020-1472
- CISA, MITRE: Best Practices for MITRE ATT&CK Mapping
- CISA: Decider Tool
- CISA: Cross-Sector Cybersecurity Performance Goals
- CISA: Secure by Design
- CISA: Implementing Phishing-Resistant MFA
- CISA: Guide to Securing Remote Access Software

REPORTING

FBI is seeking any information that can be shared, to include boundary logs showing communication to and from foreign IP addresses, a sample ransom note, communications with Rhysida actors, Bitcoin wallet information, decryptor files, and/or a benign sample of an encrypted file.

Additional details requested include: a targeted company point of contact, status and scope of infection, estimated loss, operational impact, transaction IDs, date of infection, date detected, initial attack vector, and host and network-based indicators.

FBI and CISA do not encourage paying ransom as payment does not guarantee victim files will be recovered. Furthermore, payment may also embolden adversaries to target additional organizations, encourage other threat actors to engage in the distribution of ransomware, and/or fund illicit activities. Regardless of whether you or your organization have decided to pay the ransom, FBI and CISA urge you to promptly report ransomware incidents to the FBI's Internet Crime Complaint Center (IC3) at Ic3.gov, a local FBI Field Office, or CISA via the agency's Incident Reporting System or its 24/7 Operations Center at report@cisa.gov or (888) 282-0870.

REFERENCES

[1] Microsoft: DEV-0832 (Vice Society) Opportunistic Ransomware Campaigns Impacting US Education Sector
[2] FortiGuard Labs: Ransomware Roundup - Rhysida
[3] Microsoft: Security Update Guide - CVE-2020-1472
[4] Microsoft: Master File Table (Local File Systems)
[5] SentinelOne: Rhysida
[6] Secplicity: Scratching the Surface of Rhysida Ransomware

[7] Cisco Talos: What Cisco Talos Knows about the Rhysida Ransomware
[8] SOC Radar: Rhysida Ransomware Threat Profile
[9] Sophos: A Threat Cluster's Switch from Vice Society to Rhysida
[10] Sophos: Vice Society - Rhysida IOCs (GitHub)
[11] Check Point Research: Rhysida Ransomware - Activity and Ties to Vice Society
[12] Microsoft: Command Line Process Auditing
[13] Microsoft: Audit Process Tracking
[14] Microsoft: Remote Credential Guard

ACKNOWLEDGEMENTS

Sophos contributed to this CSA.

DISCLAIMER

The information in this report is being provided "as is" for informational purposes only. FBI, CISA, and the MS-ISAC do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by FBI, CISA, and the MS-ISAC.

VERSION HISTORY

November 15, 2023: Initial version.