Rhysida Ransomware: History, TTPs and Adversary Emulation Plans

fourcore.io/blogs/rhysida-ransomware-history-ttp-adversary-emulation

Article

Last Updated on Mon Dec 12, 2023

Written by **Swapnil**

Co-founder @ FourCore

Rhysida is a new player in the Ransomware space, first appearing in May 2023, and has been targeting industries all across the globe. In recent months, Rhysida has run campaigns compromising and extorting organizations from the government, education, healthcare, IT, and manufacturing sectors. Rhysida emerged in the Ransomware Space with a high-profile attack on the Chilean army. The group currently has more than 50 victims listed on its leak site.

Rhysida Ransomware History

Rhysida Ransomware is an independent group that was first observed on May 23. The group presents itself as a cybersecurity team favouring its victims by highlighting the security issues and the potential ramifications. The TTPs used by Rhysida have significant similarities with another ransomware group, Vice Society. Vice Society has been active since 2021 and follows an opportunistic attack methodology. The group exploits vulnerable web-facing applications or uses valid accounts to gain access to organisations. Vice Society's last attacks were seen between July and October 2022.

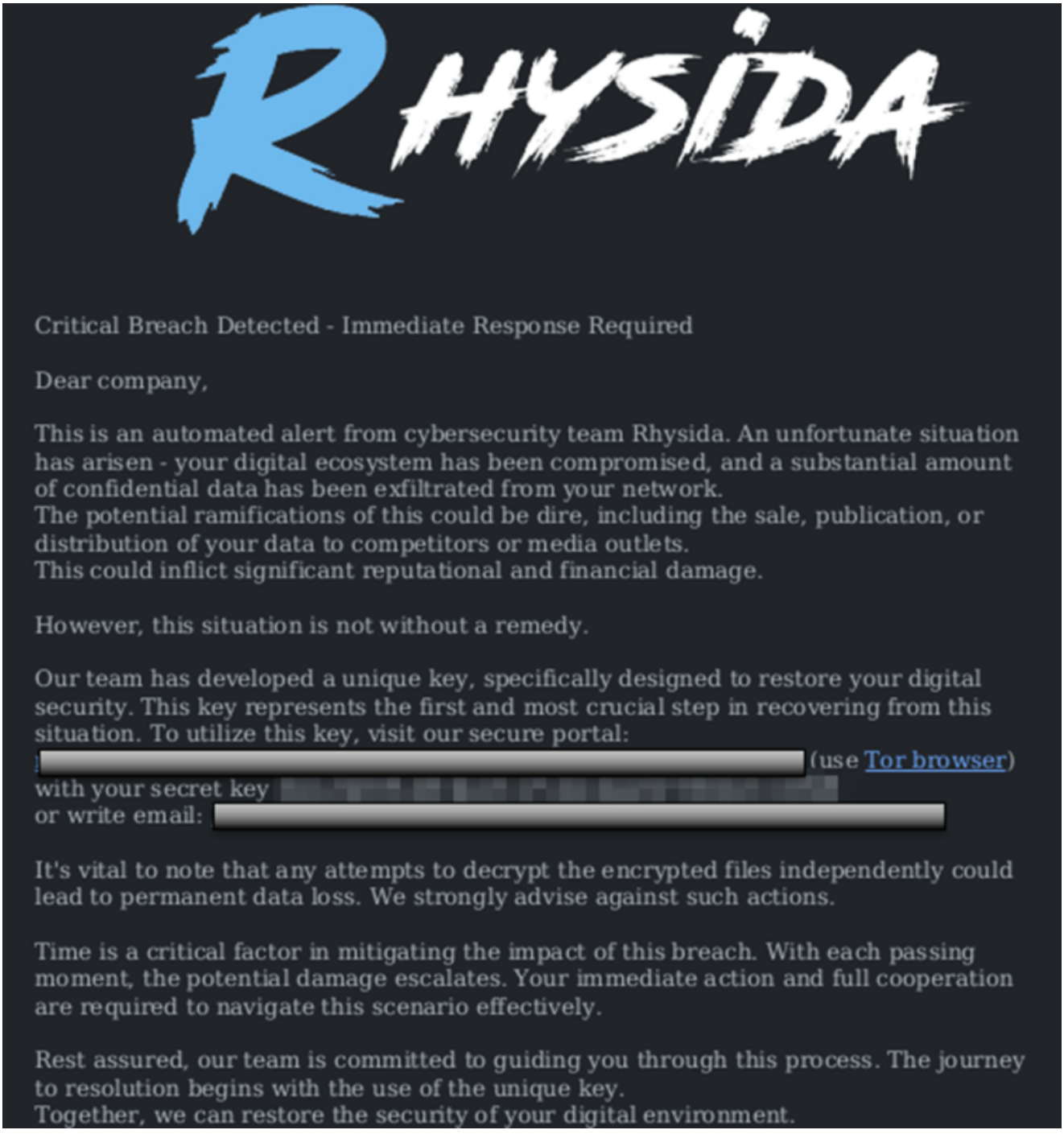
During the emergence of Rhysida, many similarities in TTPs were noted between Rhysida and Vice Society groups—usage of the same folder name, Utilisation of SystemBC, malware for sale, and the exact name of the registry run key used for persistence—**all point to the rebranding of Vice Society to Rhysida Group**. Vice Society's activities have significantly reduced after the emergence of Rhysida, and they have only published two victims on their leak site since. The two groups have also targeted similar industries, i.e. Healthcare and Education, revealing ties among Rhysida and Vice Society members.

Rhysida Ransomware Behavior

During Encryption, Rhysida uses a 4096-bit RSA key with the ChaCha20 algorithm. It uses an exclusion list to avoid encrypting certain files.

```
1bat, bin, cab, cmd, com, cur, diagcab, diagcfg, diagpkg, drv, dll, exe, hlp, hta, ico,
2ini, iso, lnk, msi, ocx, ps1, psm1, scr, sys,  Thumbs-db, url
```

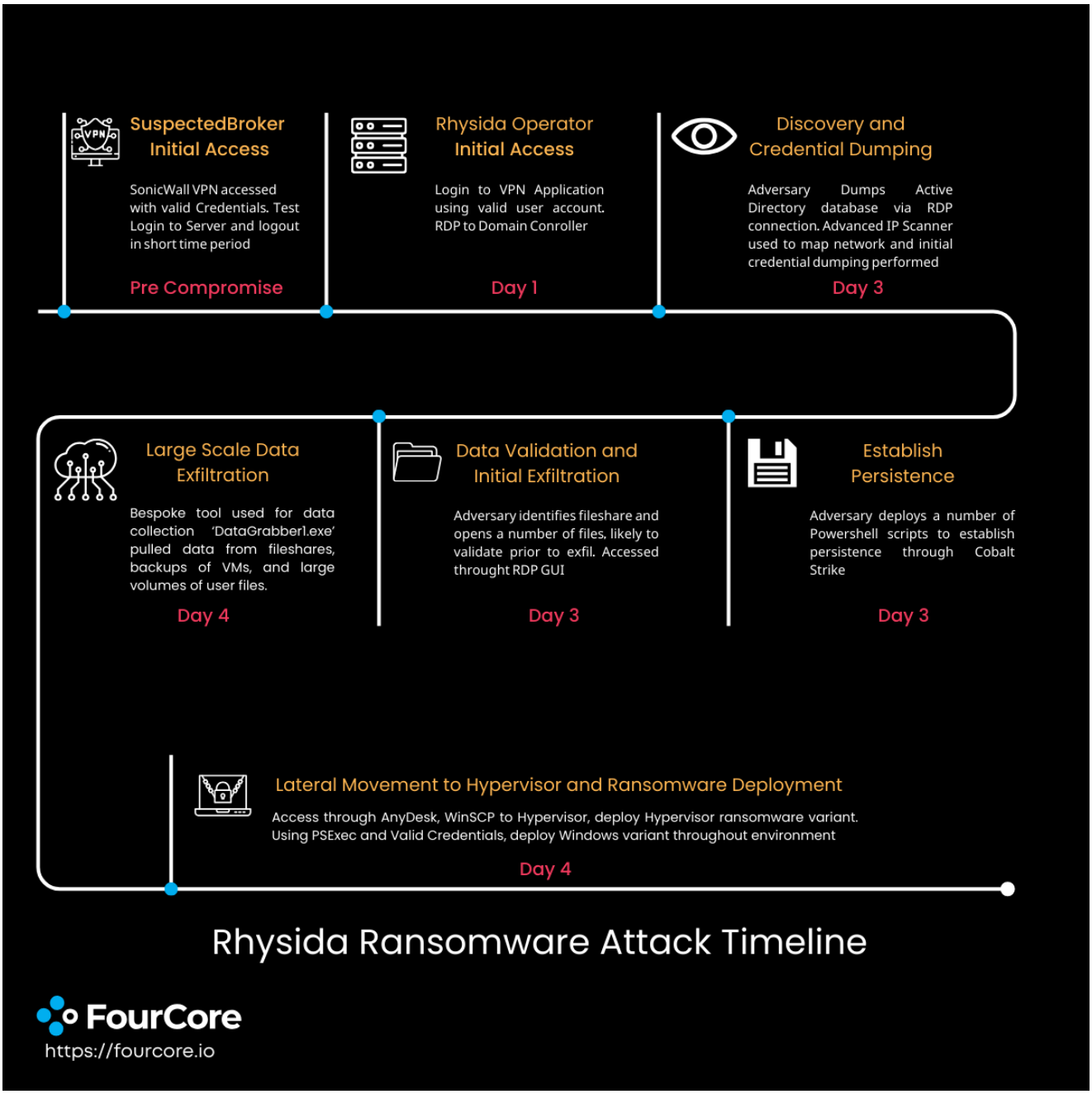
After encryption, Rhysida appends the **.rhysida extension** to the names of the encrypted files. It changes the wallpaper and drops a Ransom note as a PDF document.



Rhysida Ransom Note as a PDF document

Rhysida Ransomware TTPs

The Rhysida Ransomware operators compromise their victims opportunistically using recent exploits or utilising Valid Credentials bought on the dark web marketplace by Initial Access Brokers. During the encryption phase of their chain, they utilise either their own Rhysida payload or other ransomware payloads available in the RaaS ecosystem, such as QuantumLocker, BlackCat, and Zepplin, among others. There have been a few cases where the group did not encrypt the victim's files but performed extortion using only exfiltrated stolen data.



Rhysida's Infection Chain

Initial Access

Rhysida Operators perform initial access using multiple methods. They opportunistically target vulnerable web applications or acquire Valid RDP accounts or VPN Credentials by Initial Access Brokers. They have also been observed conducting successful Phishing attacks

Technique	Description
T1078: Valid Accounts	Rhysida operators utilise valid account credentials or VPN credentials to gain access to organisations
T1190: Exploit Public Facing Applications	Rhysida operators opportunistically target vulnerable Web Facing applications and exploit them to gain access to organisations
T1566: Phishing	Rhysida operators are known to conduct phishing attacks with malicious Excel payloads

Execution

After the initial access, Rhysida Operators have been seen utilising bat scripts, PS1 files and scheduled tasks to execute their payloads. The group deploys commodity tools and malware, such as CobaltStrike beacons and SystemBC, on the compromised systems.

Technique	Description
T1059.001: Command and Scripting Interpreter: Powershell	Rhysida operators drop a variety of PowerShell scripts and execute commands using Powershell
T1059.003: Command and Scripting Interpreter: Windows Command Shell	Rhysida operators use batch scripting and execute commands using the Windows command prompt

Privilege Escalation

Rhysidia operators escalate their privileges by utilising process injection to become NT Authority/System or become Domain Admin by utilising exploits such as ZeroLogon

Technique	Description
T1055.002: Process Injection: Portable Executable Injection	Rhysida operators inject 64-bit PE ransomware into running processes to escalate its privileges.
T1068: Exploitation for Privilege Escalation	Rhysida operators exploit vulnerable machines in the environment, such as Windows Servers, to escalate their privileges to Domain Admin

Defence Evasion

During their infection chain, Rhysida Operators continuously remove any indicators of compromise. They regularly clear Windows Event logs, Delete files, and create Hidden Artifacts.

Technique	Description
T1070.001: Indicator Removal: Clear Windows Event Logs	Rhysida operators use wevtutil.exe to clear system, application, and security event logs to avoid detection
T1070.004: Indicator Removal: File Deletion	Rhysida operators utilise PowerShell and scheduled tasks to delete any artifacts created on the system to prevent forensic scrutiny
T1564.003: Hide Artifacts: Hidden Window	Rhysida operators execute commands in hidden PowerShell windows

Credential Dumping

Once they have the right privileges, Rhysida Operators try to find credentials to spread across the organisation. They dump lsass memory, NTDS database and scour for credentials in the registry.

Technique	Description
T1003.003: OS Credential Dumping: NTDS	Rhysida operators dump credentials using tools like secretsdump to extract credentials and dump NTDS database
T1003.001: OS Credential Dumping: LSASS Memory	Rhysida operators dump lsass.exe using a variety of methods, such as using procdump or even dumping the whole RAM to extract NTLM hashes
T1003.004: OS Credential Dumping: LSA Secrets	Rhysida operators try to extract LSA secrets by dumping SAM and SECURITY Key from the registry

Discovery

During the course of the infection, Rhysidia operators discover details that may help accomplish further goals, such as lateral movement. They discover remote systems, current user permissions, and any trusts they can utilise to further their objectives.

Technique	Description
T1016: System Network Configuration Discovery	Rhysida operators use the ipconfig command to enumerate system network configurations

Technique	Description
T1018: Remote System Discovery	Rhysida operators use net group domain computers /domain to enumerate servers on the victim domain
T1033: System Owner/User Discovery	Rhysida operators utilise whoami and various net commands to identify logged in users and their associated privileges and groups
T1069.001: Permission Groups Discovery: Local Groups	Rhysida operators used the command net localgroup administrators to identify accounts with local administrator rights
T1069.002: Permission Groups Discovery: Domain Groups	Rhysida operators used the command net group “domain admins” /domain to identify domain administrators
T1087.002: Account Discovery: Domain Account	Rhysida operators used the command net user [username] /domain to identify account information
T1482: Domain Trust Discovery	Rhysida operators used the Windows utility nltest to enumerate domain trusts.

Lateral Movement

Rhysida Operators spread through the organisation by utilising RDP and SSH connections. They also utilise tools such as PsExec to execute commands and gain a foothold into other systems.

Technique	Description
T1021.001: Remote Services: Remote Desktop Protocol	Rhysida operators utilise compromised user credentials with RDP for lateral movement.
T1021.004: Remote Services: Remote Desktop Protocol	Rhysida operators utilise compromised user credentials with SSH using PuTTY for lateral movement.

Command and Control

Rhysida Operators leave Anydesk services running on compromised systems to obtain remote access and maintain persistence

Technique	Description
T1219: Remote Access Software	Rhysida operators have been observed using the AnyDesk software to obtain remote access to victim systems and maintain persistence.

Exfiltration

Rhysida Operators exfiltrate victim data using tools like DataGrabber1 and upload it to their cloud systems. The data is leaked or sold to the highest bidder if the victim doesn't pay the ransom.

Technique	Description
T1567.002: Exfiltration to Cloud Storage	Rhysida operators exfiltrate victim user data using tools such as DataGrabber1 and upload it to their cloud VMs

Impact

Rhysida Operators are financially motivated and utilise double extortion attacks to force their victims to pay. Along with encrypting victim data, they also exfiltrate the data and threaten to publish sensitive information if the ransom is not paid

Technique	Description
T1486: Data Encrypted for Impact	Rhysida operators encrypt victim data using a 4096-bit RSA encryption key that implements a ChaCha20 algorithm.
T1657: Financial Theft	Rhysida operators 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
T1490: Inhibit System Recovery	Rhysida Operators delete shadow copies using wmic and vssadmin, kill services related to backup software and change the default RDP port to 4000.

Rhysida Ransomware Hunting & Detection

Rhysida Ransomware can be hunted for in your environment via the following rules.

The following YARA rule can be utilize for hunting Rhysidia ransomware binaries.

```
rule rw_rhysida {

      meta:
              author = "Alex Delamotte"
              description = "Rhysida ransomware detection."
              sample = "69b3d913a3967153d1e91ba1a31ebed839b297ed"
              reference = "https://s1.ai/rhys"
      strings:
              $typo1 = { 63 6D 64 2E 65 78 65 20 2F 63 20 72 65 67 20 64 65 6C 65 74 65 20 22 48 4B 43 55
5C 43 6F 6E 74 74 6F 6C 20 50 61 6E 65 6C 5C 44 65 73 6B 74 6F 70 22 }
              $cmd1 = { 63 6D 64 2E 65 78 65 20 2F 63 20 72 65 67 20 61 64 64 20 22 48 4B 43 55 5C 53 6F
66 74 77 61 72 65 5C 4D 69 63 72 6F 73 6F 66 74 5C 57 69 6E 64 6F 77 73 5C 43 75 72 72 65 6E 74 56 65 72 73
69 6F 6E 5C 50 6F 6C 69 63 69 65 73 5C 41 63 74 69 76 65 44 65 73 6B 74 6F 70 }
              $cmd2 = { 63 6D 64 2E 65 78 65 20 2F 63 20 72 65 67 20 61 64 64 20 22 48 4B 4C 4D 5C 53 6F
66 74 77 61 72 65 5C 4D 69 63 72 6F 73 6F 66 74 5C 57 69 6E 64 6F 77 73 5C 43 75 72 72 65 6E 74 56 65 72 73
69 6F 6E 5C 50 6F 6C 69 63 69 65 73 5C 53 79 73 74 65 6D 22 20 2F 76 20 57 61 6C 6C 70 61 70 65 72 20 2F 74
20 52 45 47 5F 53 5A 20 2F 64 20 22 43 3A 5C 55 73 65 72 73 5C 50 75 62 6C 69 63 5C 62 67 2E 6A 70 67 22 20
2F 66 }
              $byte1 = { 48 8D 05 72 AA 05 00 48 8B 00 8B 95 }
              $byte2 = { 48 8D 15 89 CF 03 00 48 89 C1 E8 F9 1C 03 00 44 }
      condition:
              2 of them
}
```

The following Fortinet hunting rule can hunt for the persistence method utilized by Rhysida operators.

```
Type: ("Value Created") AND Registry.Name:"socks" AND Registry.Path:
("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run") AND Registry.Data: ("Powershell.exe \-
windowstyle hidden \-ExecutionPolicy Bypass \-File ")
```

Following detection rules can be utilized to detect LSASS Memory dumping by Rhsyida Operators.

Rule	Link
Procdump Execution	Link
Renamed ProcDump Execution	Link
Potential LSASS Process Dump Via Procdump	Link

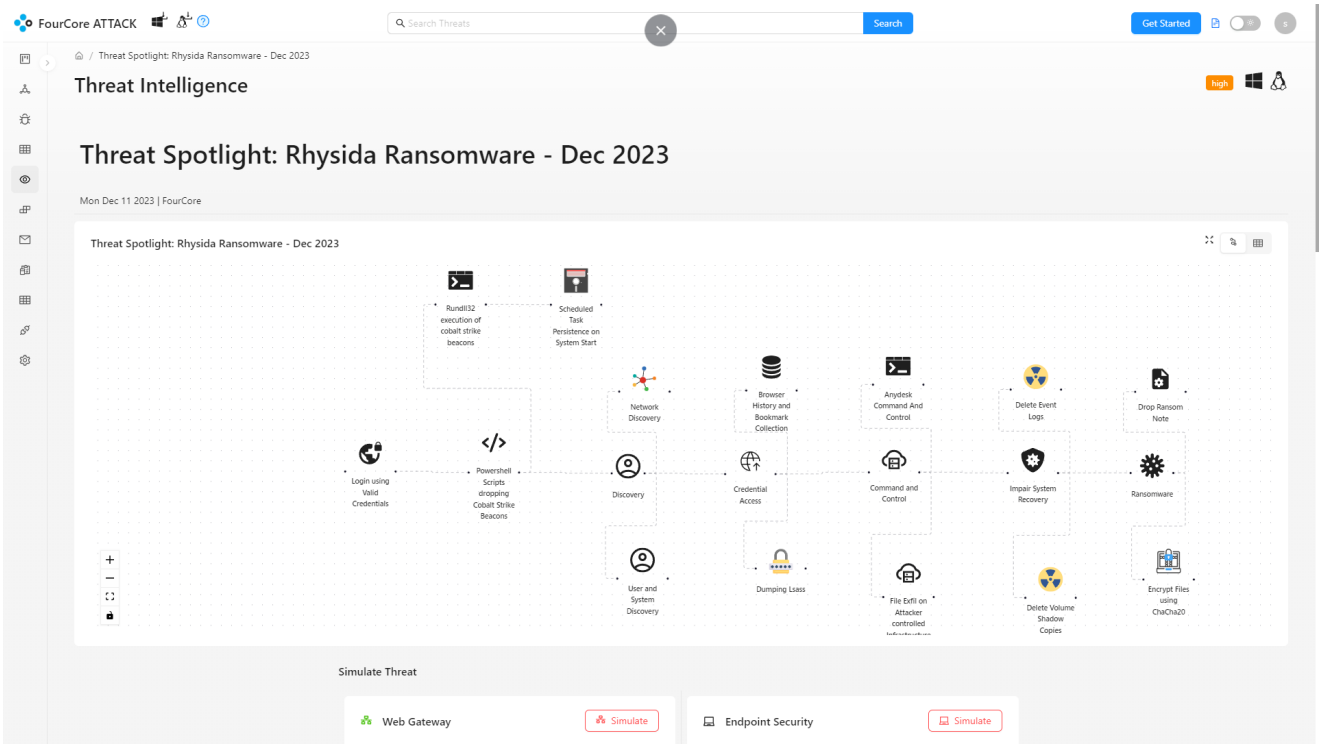
Defend Against Rhysida Ransomware

Most of the TTPs employed by Rhysida operators during the intrusion are typical for these ransomware intrusions, and no novel techniques were observed. This highlights the importance of understanding not just the operation of a ransomware payload but the

entire process leading to its deployment. There are hallmarks of a less seasoned actor, such as the unobfuscated registry modification and PowerShell commands seen throughout the activity.

The actors leverage various tools, from the usage of remote management tools such as AnyDesk to the deployment of ransomware through PsExec, to facilitate such attacks. Closely monitoring those activities could help prevent the next ransomware attack.

Our Threat Research Team has developed adversary emulation plans for the Rhysida Ransomware utilizing analyst reports, TTPs and threat intelligence. These plans validate the effectiveness of your various security controls by emulating the TTPs and behaviours utilized by the Rhysida Ransomware group.



Emulate threats continuously on the FourCore ATTACK Platform and achieve Threat-informed Defense.

References

- CISA #StopRansomware: Rhysida Ransomware
- Rhysida Incident Response
- Checkpoint: Activity Analysis and Ties to Vice Society
- SentinelOne: Rhysida Ransomware
- Sophos: Vice Society and Rhysida Ransomware

- Microsoft: Vice Society opportunistic ransomware campaigns
- SOC Radar Threat Profile: Rhysida Ransomware

FourCore ATTACK Adversary Emulation Platform