HC3: Sector Alert

August 4, 2023 TLP:CLEAR Report: 202308041500

Rhysida Ransomware

Executive Summary

Rhysida is a new ransomware-as-a-service (RaaS) group that has emerged since May 2023. The group drops an eponymous ransomware via phishing attacks and Cobalt Strike to breach targets' networks and deploy their payloads. The group threatens to publicly distribute the exfiltrated data if the ransom is not paid. Rhysida is still in early stages of development, as indicated by the lack of advanced features and the program name Rhysida-0.1. The ransomware also leaves PDF notes on the affected folders, instructing the victims to contact the group via their portal and pay in Bitcoin. Its victims are distributed throughout several countries across Western Europe, North and South America, and Australia. They primarily attack education, government, manufacturing, and technology and managed service provider sectors; however, there has been recent attacks against the Healthcare and Public Health (HPH) sector.

Overview of Rhysida

First oberved on May 17, 2023, following the emergence of their victim support chat portal, hosted via TOR (.onion), Rhysida describes itself as a "cybersecurity team" that aims to help victims highlight potential security issues and secure their networks. While not much is known about the group's origins or country affiliations, the name Rhysida is a reference to the Rhysida genus of centipede and is reflected as the logo on their victim blog. The TOR page also shows the current auctions and total number of victims. The group's website also serves as a portal for Rhysida-centric news and media coverage, as well as details on how to contact the group should journalists, recovery firms, or fans be inclined to do so.

Rhysida is a 64-bit Portable Executable (PE) Windows cryptographic ransomware application compiled using MINGW/GCC. In each sample analyzed, the application's program name is set to Rhysida-0.1, suggesting the tool is in early stages of development. A notable characteristic of the tool is its plain-text strings revealing registry modification commands.

Rhysida ransomware is deployed in multiple ways. Primary methods include breaching targets' networks via phishing attacks, and by dropping payloads across compromised systems after first deploying Cobalt Strike or similar command-and-control frameworks. Of note, a previous HC3 product on Russian-speaking RaaS group, Black Basta, detailed how both threat groups, Black Basta and FIN7 (aka Carbanak/Cobalt Group/Carbon Spider), share a TTP in their employment of Cobalt Strike.

When Rhysida runs, one cybersecurity firm observed a process of getting output from the command line, which apparently scans the files, runs the "file_to_crypt" function, and if successful, changes the file extension to ".rhysida":

HC3: Sector Alert

August 4, 2023 TLP:CLEAR Report: 202308041500

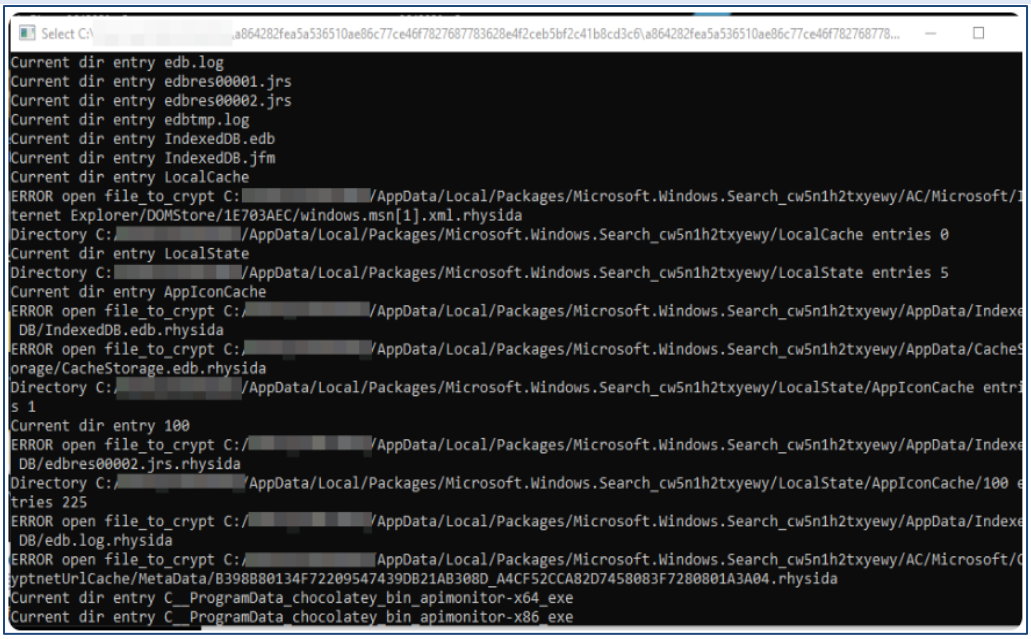

Figure 1: Script outputs that appear on cmd[.] exe when Rhysida runs. *(Source: SOCRadar)*

For the encryption phase, Rhysida uses a 4096-bit RSA key with the ChaCha20 algorithm. After the encryption details are established, Rhysida enumerates files and folders connected to the system. The main function ends by calling PowerShell to delete the binary after encryption has completed.

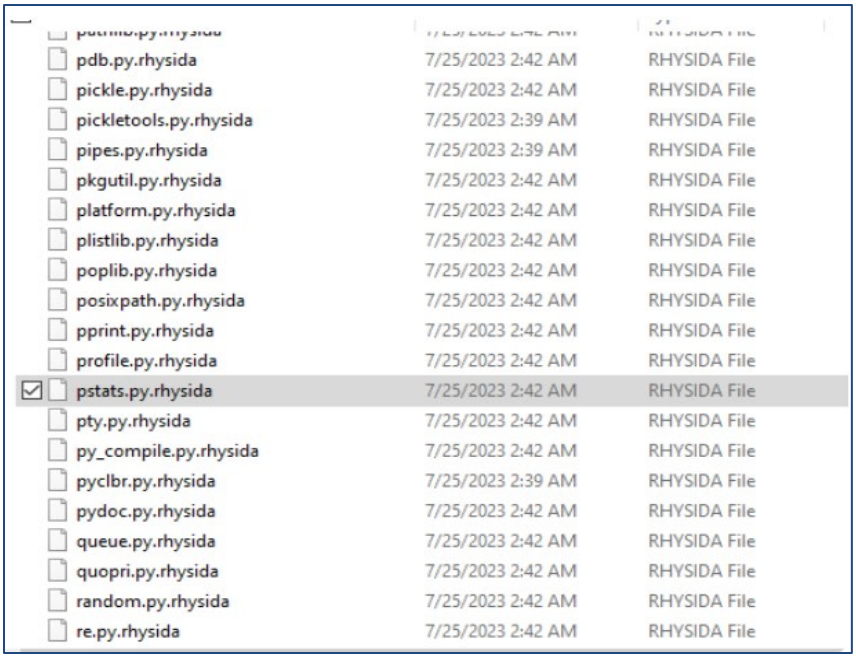

Figure 2: Some files in test environment have changed to ".rhysida" extension. *(Source: SOCRadar)*

Rhysida uses a file exclusion list to avoid encrypting certain files. This check occurs in the isFileExcluded function, which compares the current file extension against exclude_extensions, an array that contains the following excluded file extensions. This function initializes two variables, exclude_i as 0 and exclude_c as 11, which iterate through the array of 27 excluded file extensions and the length of the current file name.

Extended features beyond encrypting files are still not present in current variations of Rhysida. The most recent of analyzed samples continue to lack commodity features like VSS Removal, multiple persistence mechanisms, process termination or unhooking.

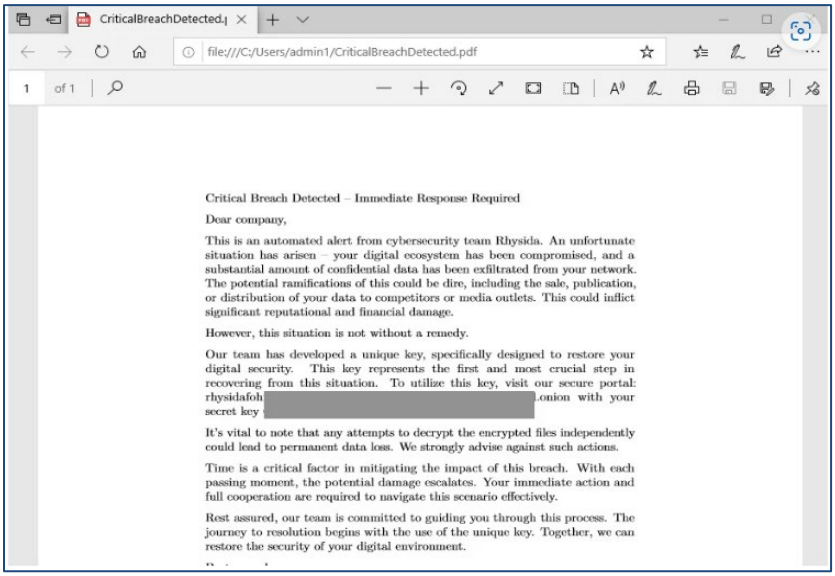

Figure 3: Rhysida ransom note, CriticalBreachDetected.pdf. *(Source: SentinelOne)*

The group then threatens victims in a ransom note with public distribution of the exfiltrated data, bringing them in line with modern-day double-extortion groups. Rhysida ransom notes are written as PDF documents to affected folders on targeted drives, with the content of the document embedded in the binary in clear text. This potentially provides some insight into the types of systems or networks that the threat group targets, as the presence of these ransom notes could indicate that the targeted systems have the capability to handle PDF documents. This also indicates that the group is not targeting command-line operating systems used on network devices or servers.

Victims are instructed to contact the attackers via their TOR-based portal, utilizing their unique identifier providers in the ransom note. Rhysida accepts payment in Bitcoin only, providing information on the purchase and use of Bitcoin on the victim portal as well. Upon providing their unique ID to the payment portal, another form is presented that allows victims to provide additional information to the attackers, such as authentication and contact details.

HC3: Sector Alert

August 4, 2023 TLP:CLEAR Report: 202308041500

Targets of Rhysida

Despite being an ostensibly independent ransomware group and showing no observed overt connections to existing ransomware operations, the geopolitical ramifications of the attack on the Chilean government remain unclear. However, its victims are distributed throughout several countries across Western Europe, North and South America, and Australia, loosely aligning the group's targeting with other ransomware operations that avoid targeting former Soviet Republic or bloc countries in Eastern Europe and Central Asia's Commonwealth of Independent States. When the country distributions are analyzed, one cybersecurity firm concluded that the United States, Italy, Spain, and the United Kingdom are targeted more than other countries.

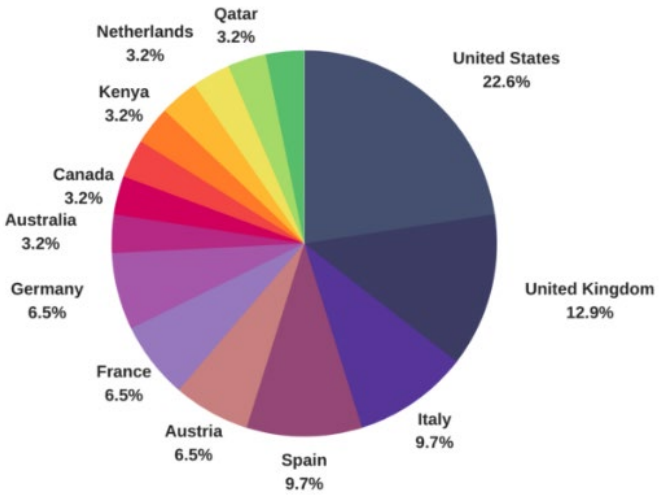

Figure 4: Distribution of affected countries by Rhysida ransomware. *(Source: SOCRadar)*

Since June, the threat actor has already added at least eight victims to its dark web data leak site and has published all stolen files for five of them. The cyberattack on the Chilean army targeted victims from the education, government, manufacturing, and technology and managed service provider sectors, but overall, Rhysida prefers to target other sectors. When observing Rhysida's past attacks, it can be inferred that it mostly targets organizations operating in the education and manufacturing sectors.

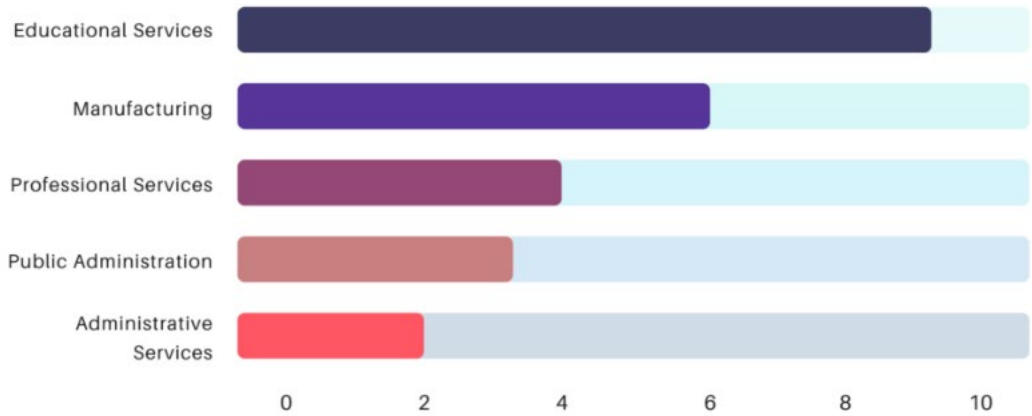

Figure 5: Distribution of affected sectors by Rhysida ransomware. *(Source: SOCRadar)*

Relationships to Other Threat Groups

Recently, security researchers have alleged that there is a relationship between the threat actors Rhysida and Vice Society. In terms of commonalities, both groups mainly target the education sector. 38.4% of Vice Society's attacks targeted the education sector, compared to 30% of Rhysida's. Of note, Vice Society mainly targets both educational and healthcare institutions, preferring to attack small-to-medium organizations. If there is indeed a linkage between both groups, then it is only a matter of time before Rhysida could begin to look at the healthcare sector as a viable target.

HC3: Sector Alert

August 4, 2023 TLP:CLEAR Report: 202308041500

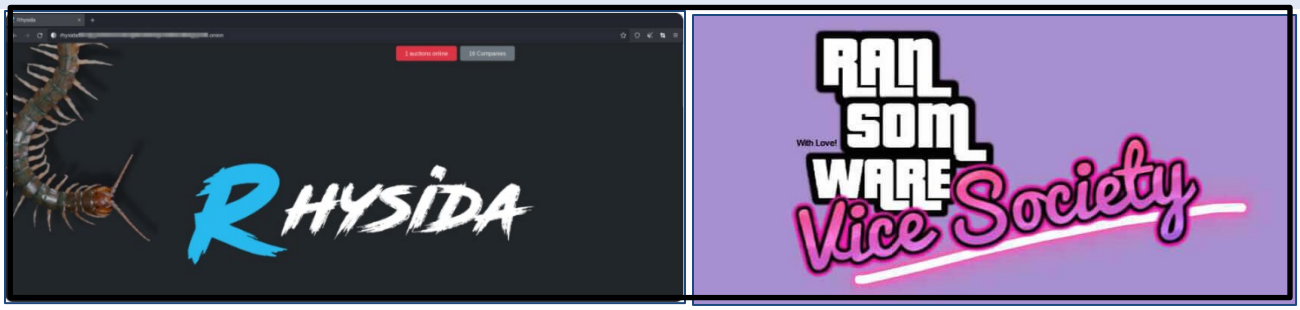

Figure 6: Logos for both Rhysida and Vice City RaaS Threat Groups. *(Source: SOCRadar and Fortra)*

Security Recommendations Against Rhysida

Given the severity of Rhysida's attacks, it is crucial for organizations to take proactive measures to protect their systems and data. Here are some security recommendations to defend against Rhysida ransomware:

- **Virtual Patching**: Rhysida exploits known vulnerabilities in software to gain access to systems. Virtual patching can help by providing an immediate layer of protection against known vulnerabilities that the ransomware might exploit. This is especially important when a vendor-supplied patch is not immediately available or cannot be applied right away due to testing requirements.

- **Phishing Awareness Training**: Since Rhysida often uses phishing campaigns to deliver its ransomware, it is important to provide regular phishing awareness training to all employees. This can help them recognize and avoid phishing attempts.

- **Use of Endpoint Security Solutions**: Endpoint security tools can help fight against ransomware by continuously checking all points of entry in a network, spotting and stopping malicious software, reviewing all incoming data, and giving the option to separate or delete data from afar, which helps prevent the spread of ransomware throughout the network.

- **Immutable Backups**: Utilizing the inherent stability of immutable backups, which are distinguished by their resistance to modification and deletion, organizations can construct a robust protective barrier against potential ransomware incursions. These backups guarantee that, despite the presence of such cyber risks, the restoration of data remains a feasible and efficient approach, thereby negating the necessity to comply with ransom requisitions.

- **Network Segmentation**: By segmenting your network, you can limit the spread of ransomware if one part of your network is compromised.

- **Use of Firewalls and Intrusion Detection Systems**: Firewalls and intrusion detection systems can help detect and block suspicious activity, potentially stopping an attack before it can do significant damage.

- **Incident Response Plan**: Having a well-defined incident response plan can help your organization respond quickly and effectively to a ransomware attack, minimizing downtime and damage.

- **Least Privilege Principle**: Limit the access rights of users and applications as much as possible. This can help prevent ransomware from gaining the access it needs to encrypt files or spread throughout your network.

MITRE ATT&CK Tactics Techniques and Procedures (TTPs) of Rhysida Ransomware

Technique	ID
Reconnaissance	
Active Scanning	T1595
Phishing for Information	T1598
Resource Development	
Acquire Infrastructure	T1583
Develop Capabilities	T1587
Initial Access	
Phishing	T1566
Abuse Elevation Control Mechanism: Bypass User Account Control	T1548.002
Execution	
Command and Scripting Interpreter	T1059
Shared Modules	T1129
Persistence	
Registry Run Keys / Startup Folder	T1547.001
Privileged Escalation	
Process Injection	T1055
Thread Execution Hijacking	T1055.003
Registry Run Keys / Startup Folder	T1547.001
Defense Evasion	
Obfuscated Files or Information	T1027
Indicator Removal from Tools	T1027.005
Masquerading	T1036
Process Injection	T1055
Thread Execution Hijacking	T1055.003
Virtualization/Sandbox Evasion	T1497
Hide Artifacts	T1564
NTFS File Attributes	T1564.004
Reflective Code Loading	T1620
Discovery	
Application Window Discovery	T1010
Process Discovery	T1057
System Information Discovery	T1082
File and Directory Discovery	T1083
Virtualization/Sandbox Evasion	T1497
Security Software Discovery	T1518.001
Collection	
Data from Local System	T1005
Automated Collection	T1119
Command and Control	
Application Layer Protocol	T1071
Web Protocols	T1071.001
Exfiltration	

Exfiltration Over C2 Channel	T1041
Impact	
Data Encrypted for Impact	T1486

Indicators of Compromise

SentinelOne's Indicators of Compromise	
SHA1	Description
69b3d913a3967153d1e91ba1a31ebed839b297ed	Rhysida PE first reported by MalwareHunterTeam
338d4f4ec714359d589918cee1adad12ef231907	Rhysida PE used in attack against Chilean Army
b07f6a5f61834a57304ad4d885bd37d8e1badba8	Rhysida PE, crashes during analysis

SOCRadar's Indicators of Compromise	
IOC Type	IOC
URL	https://ipapi.com/json/
Hash (SHA-256)	a864282fea5a536510ae86c77ce46f7827687783628e4f2ceb5bf2c41b8cd3c6
Hash (SHA-256)	6903b00a15eff9b494947896f222bd5b093a63aa1f340815823645fd57bd61de
Hash (SHA-1)	7abc07e7f56fc27130f84d1c7935a0961bd58cb9
Hash (SHA-256)	3bc0340007f3a9831cb35766f2eb42de81d13aeb99b3a8c07dee0bb8b000cb96
Hash (SHA-256)	2a3942d213548573af8cb07c13547c0d52d1c3d72365276d6623b3951bd6d1b2
Hash (MD-5)	59a9ca795b59161f767b94fc2dece71a
Hash (SHA-256)	250e81eeb4df4649ccb13e271ae3f80d44995b2f8ffca7a2c5e1c738546c2ab1
Hash (SHA-256)	2a3942d213548573af8cb07c13547c0d52d1c3d72365276d6623b3951bd6d1b2

Way Forward

In only a short time, Rhysida has proven itself to be a significant threat to organizations worldwide. With its strong encryption techniques and double extortion tactics, and a focus on multi-sector targets (military, government, education, and manufacturing), it is likely they will continue to pose a significant threat to these and possibly other sectors. By understanding the group's TTPs, organizations can take a proactive approach to protect their systems and data. This includes patching known vulnerabilities, implementing robust security measures, and training staff to recognize and avoid phishing attempts.

In addition to previous HC3 product recommendations on how to safeguard against ransomware/extortion attacks, some cyber security professionals advise that the healthcare industry acknowledge the ubiquitous threat of cyberwar against them and recommend that their cybersecurity teams implement the following steps:

- Educate and train staff to reduce the risk of social engineering attacks via email and network access.
- Assess enterprise risk against all potential vulnerabilities and prioritize implementing the security plan with the necessary budget, staff, and tools.
- Develop a cybersecurity roadmap that everyone in the healthcare organization understands.

At no cost, Cybersecurity & Infrastructure Security Agency (CISA) also offers Cyber Hygiene Vulnerability Scanning services to federal, state, local, tribal and territorial governments, as well as public and private sector critical infrastructure organizations. This service helps organizations monitor and evaluate their

external network posture.

Furthermore, the HHS OCR provides links to online government resources (general information, frequently asked questions, tips, and a ransomware readiness self-assessment) to proactively and reactively aid healthcare organizations.

The probability of cyber threat actors targeting the healthcare industry remains high. Prioritizing security by maintaining awareness of the threat landscape, assessing their situation, and providing staff with tools and resources necessary to prevent an cyberattack remains the best way forward for healthcare organizations.

Relevant HHS Reports

HC3: Alert – 2021 Trends Show Increased Globalized Threat of Ransomware (February 9, 2022)

HC3: Threat Profile – Black Basta (March 15, 2023)

References

"Dark Web Profile: Vice Society Ransomware Group." SOCRadar. August 4, 2022. https://socradar.io/dark-web-profile-vice-society/

Delamotte, Alex and Jim Walter. "Rhysida Ransomware: RaaS Crawls Out of Crimeware Undergrowth to Attack Chilean Army." SentinelOne. June 29, 2023. https://www.sentinelone.com/blog/rhysida-ransomware-raas-crawls-out-of-crimeware-undergrowth-to-attack-chilean-army/

Gatlan, Sergui. "Rhysida ransomware leaks documents stolen from Chilean Army." Bleeping Computer. June 15, 2023. https://www.bleepingcomputer.com/news/security/rhysida-ransomware-leaks-documents-stolen-from-chilean-army/

"Latin American Governments Targeted by Ransomware." Recorded Future. June 14, 2022. https://www.recordedfuture.com/latin-american-governments-targeted-by-ransomware

"Threat Profile: Rhysida Ransomware." SOCRadar. August 3, 2023. https://socradar.io/threat-profile-rhysida-ransomware/

"Warning issued about Vice Society ransomware gang after attacks on schools." Fortra. September 8, 2022. https://www.tripwire.com/state-of-security/warning-issued-vice-society-ransomware-gang

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