See All Posts

RANSOMWARE

Emulating the Controversial and Intriguing Rhysida Ransomware

Published September 20, 2023

AttackIQ has released two new attack graphs that seek to emulate the various activities carried out by the controversial Ransomware-as-a-Service (RaaS) known as Rhysida against multiple targets worldwide since its discovery in May 2023.

Rhysida is a Ransomware-as-a-Service (RaaS) that has been active since at least May 2023 and, despite being a newcomer, has quickly established itself as a significant fully-fledged ransomware operation.

The operators behind Rhysida present themselves as a "Cybersecurity Team" who help their victims find security weaknesses in their networks and systems. In reality, the operators conduct double-extortion activities in which

Contributors

Francis Guibernau

More by this author

ADVERSARY EMULATION

Response to CISA Advisory (AA24-290A): Iranian Cyber Actors' Brute Force and Credential Access Activity Compromises Critical Infrastructure Organizations

Read More →

ADVERSARY EMULATION

Emulating the Opportunistic

they threaten victims with public distribution of the extracted data if the demanded ransom is not provided. Rhysida operators have a victim support chat portal hosted on TOR (.onion), where they also list for sale the information of those victims who do not comply with their demands.

Rhysida was initially known for targeting sectors such as Education, Government, Manufacturing, and Technology. However, more recently, it has expanded its activities to include Healthcare and Public Health organizations. As a result of this, in August 2023, the U.S. Department of Health and Human Services issued a warning to the healthcare industry about Rhysida ransomware activity.

A connection between the adversary known as Vice Society, also known as Vanilla Tempest, and the operators of Rhysida was suggested due to the clear correlation between the emergence of Rhysida and the disappearance of the former. Additionally, both groups focus on two main sectors that stand out in the ransomware ecosystem: Education and Healthcare. This connection does not suggest that Rhysida is exclusively used by Vice Society, but it shows with at least medium confidence that Vice Society operators are now users of Rhysida ransomware.

AttackIQ has released two new attack graphs aimed at emulating the activities carried out by this infamous Ransomware and its operators to help customers validate their security controls and their ability to defend against similar threats.

Validating your security program performance against these behaviors is vital in reducing risk. By using these new attack graphs in the AttackIQ Security Optimization Platform, security teams will be able to:

- Evaluate the performance of security controls against a highly active threat worldwide.
- Assess your security posture against the Tactics, Techniques and Procedures (TTPs) employed by Rhysida operators.
- Continually validate detection and prevention pipelines against a highly active and financially motivated threat.

and Lightweight Lumma Stealer

Read More →

ADVERSARY EMULATION

Emulating the Surging Hadooken Malware

Read More →

Rhysida Ransomware – 2023-08 – Global Campaign against Multiple Sectors and Regions

The following emulations aim to emulate all the Tactics, Techniques, and Procedures (TTPs) employed by Rhysida Ransomware, and its operators, since its discovery in May 2023 through August 2023.

During the identified activities, Rhysida arrived at the victim's system via phishing lures, after which a second-stage payload such as Cobalt Strike or SystemBC is deployed and executed in order to assist in Discovery and Lateral Movement activities within the system and network.

Prior to the deployment of Rhysida, the perpetrators used a PowerShell script known as SILENTKILL to identify security software and disable it or create exclusion rules to bypass it. Additionally, the script is capable of changing local account passwords, modifying the local Firewall, and deleting system backups to delay recovery tasks.

According to public reports, Rhysida operators were observed using different mechanisms for lateral movement such as PsExec, Remote Desktop Protocol (RDP) and Windows Remote Management (WinRM) with the objective of deploying the payload itself.

Upon deployment, Rhysida will seek to identify and list all files on all local drives on the compromised system. Once completed, it will perform the task of encrypting the files using a 4096-bit RSA key and ChaCha20 and append the extension ".rhysida".

Striving to offer the broadest possible range of intrusion chains on this threat, AttackIQ has created two variants of the emulation that are intended to group together those behaviors employed by Rhysida in different periods of activity.

Rhysida Ransomware – 2023-08 – Global Campaign against Multiple Sectors and Regions [SystemBC Version]

(Click for Larger)

On August 8, 2023, CheckPoint reported the analysis of the activities carried out by Rhysida in recent months. During the reported activities, CheckPoint observed Rhysida operators employing SystemBC, a commodity malware, as a second-stage payload.

Furthermore, the perpetrator achieved persistence through the creation of a Registry Run Key and leveraged Remote Desktop Protocol (RDP) and Windows Remote Management (WinRM) mechanisms to move laterally throughout the compromised environment.

(Click for Larger)

The first stage of the attack begins with the download and saving of a compressed ZIP file which is usually distributed via phishing. Subsequently, a PowerShell version of SystemBC, which is contained within the ZIP file, is saved to the system.

SystemBC is then executed via Code Injection and, in the case of failure, it will be executed secondarily via the Reflective DLL Injection technique. Finally, the implant acquires persistence through the creation of a Registry Run Key called "socks".

> **Ingress Tool Transfer (T1105):** This scenario downloads to memory and saves to disk in two separate scenarios to test network and endpoint controls and their ability to prevent the delivery of known malicious content.
>
> **Process Injection (T1055):** This scenario injects a DLL file into another running process and validates if a canary file can be created.

Reflective DLL Injection (T1620): This scenario takes a default AttackIQ DLL and loads it into the memory space of its own process in order to execute the desired DLL function.

Logon Autostart Execution: Registry Run Keys (T1547.001): This scenario creates a registry entry named `socks` under the `HKLM\Software\Microsoft\Windows\CurrentVersion\Run` key that Windows uses to identify what applications should be run at system startup.

(Click for Larger)

In this stage, SystemBC will acquire system information, such as operating system information, active processes, CPU properties, installed security software, and administrator accounts.

System Information Discovery (T1082): The native `systeminfo` command is executed to retrieve all of the Windows system information.

Process Discovery (T1057): Window's built-in `tasklist` command is executed as a command process and the results are saved to a file in a temporary location.

Windows Management Instrumentation (T1047): This scenario uses `wmic` commands to collect information regarding the CPU properties.

Security Software Discovery (T1518.001): A native Microsoft Windows Management Instrumentation Command (WMIC) is executed to determine which software has been installed as an `AntiVirusProduct` class.

Account Discovery: Domain Account (T1087.002): The system command `net group` is used to list Domain and Enterprise Admins accounts.

(Click for Larger)

In the third stage of the attack, the adversary will attempt to move laterally to other systems within the network via Remote Desktop Protocol (RDP) and Windows Remote Management (WinRM).

Once accomplished, the deployment of SILENTKILL, a PowerShell script designed to terminate AV-related processes and services, delete Volume Shadow Copies, and modify RDP configurations, will be conducted.

After SILENTKILL is deployed and executed, the emulation will attempt to disable Windows Defender by modifying the DisableAntiSpyware registry key.

> **Remote Services: Remote Desktop Protocol (T1021.001):** Remote Desktop is the built-in remote access utility used by Windows. This scenario attempts to remotely connect to another accessible asset with stolen credentials.
>
> **Remote Services: Windows Remote Management (T1021.006):** This scenario will attempt to move laterally to any available asset inside the network through the use of WinRM.
>
> **Impair Defenses: Disable or Modify Tools (T1562.001):** The registry key `HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware` is set to 1 that will disable Windows Defender from being enabled at next reboot.

(Click for Larger)

The fourth stage has the objective of evading defenses by creating a firewall rule via the Net-NewFirewallRule PowerShell cmdlet, inhibiting system recovery by deleting Volume Shadow Copies via VSSAdmin and delaying forensic analysis and incident response activities by deleting Windows event logs via Wevutil and erasing Remote Desktop Protocol (RDP) logs.

> **Impair Defenses: Disable or Modify System Firewall (T1562.004):** The scenario will use the `New-NetFirewallRule` PowerShell function to create a new rule into the Windows System Firewall to allow outbound traffic.

Inhibit System Recovery (T1490): This scenario executes `vssadmin.exe` to delete a recent Volume Shadow Copy created by the emulation.

Indicator Removal: Clear Windows Event Logs (T1070.001): The scenario will use the `wevtutil.exe` binary to clear event logs from the system.

Indicator Removal on Host: File Deletion (T1070.004): This scenario deletes a recently created file from the filesystem.

(Click for Larger)

The last stage of the attack begins with the deployment of Rhysida Ransomware, which is executed through a scheduled task called "Rhsd". Subsequently, Rhysida will proceed to identify relevant files to be encrypted, change the desktop background of the system via registry keys and then encrypt the selected files using a 4096-bit RSA + ChaCha20 cryptographic combination.

Scheduled Task/Job: Scheduled Task (T1053.005): This scenario creates a new scheduled task named `Rhsd` using the `schtasks` utility.

File and Directory Discovery (T1083): The actors used the PowerShell `dir` cmdlet to recursively query a drive and list all of the files.

Modify Registry (T1112): This scenario will attempt the Rhysida registry key modifications to replace the desktop background.

Data Encrypted for Impact (T1486): This scenario performs the file encryption routines used by common ransomware families. Files matching an extension list are identified and encrypted in place using the same encryption algorithms used by Rhysida ransomware.

Rhysida Ransomware – 2023-08 – Global Campaign against Multiple Sectors and Regions [Cobalt Strike Version]

(Click for Larger)

On August 9, 2023, Trend Micro reported details on new Rhysida ransomware activities targeting the Healthcare sector. Rhysida's operators were recently involved in an incident in early August against Pospect Medical Holdings, a California-based healthcare system, that affected 17 hospitals and 166 clinics across the United States.

During this activity, Rhysida operators used Cobalt Strike as a second-stage payload rather than SystemBC, and leveraged PsExec to deploy PowerShell scripts and the Rhysida ransomware payload itself.

(Click for Larger)

The first stage of the attack begins with the download and saving of a compressed ZIP file which is usually distributed via phishing. Subsequently, a Cobalt Strike Beacon is saved to the filesystem.

Cobalt Strike is then executed via Code Injection and, in the case of failure, it will be executed secondarily via the Reflective DLL Injection technique.

(Click for Larger)

In this stage, Cobalt Strike will acquire system information, such as operating system information, active processes, CPU properties, installed security software, and administrator accounts.

(Click for Larger)

In the third stage of the attack, the adversary will attempt to move laterally to other systems within the network via PsExec.

Once accomplished, the deployment of SILENTKILL, a PowerShell script designed to terminate AV-related processes and services, delete Volume Shadow Copies, and modify RDP configurations, will be conducted.

After SILENTKILL is deployed and executed, the emulation will attempt to disable Windows Defender by modifying the DisableAntiSpyware registry key. In case of being unable to do so, the emulation will add extensions to Defender's exclusion list, with the objective of avoiding detection.

(Click for Larger)

This stage has the objective of evading defenses by creating a firewall rule via the Net-NewFirewallRule PowerShell cmdlet, inhibiting system recovery by deleting Volume Shadow Copies via VSSAdmin or Windows Management Instrumentation Command (WMIC) and delaying forensic analysis and incident response activities by deleting Windows event logs via Wevutil and erasing Remote Desktop Protocol (RDP) logs.

(Click for Larger)

The last stage of the attack begins with the deployment of Rhysida Ransomware, which is executed through a scheduled task called "Rhsd". Subsequently, Rhysida will proceed to identify relevant files to be encrypted, change the desktop background of the system via registry keys and then encrypt the selected files using a 4096-bit RSA + ChaCha20 cryptographic combination.

Detection and Mitigation Opportunities

Given the vast number of techniques used by these adversaries, it can be difficult to know which to prioritize for prevention and detection assessment. AttackIQ recommends first focusing on the following techniques emulated in our scenarios before moving on to the remaining techniques.

1. Process Injection (T1055) and Reflective DLL Injection (T1620):

Rhysida operators were observed using techniques that obscure the true source of malicious activity. By injecting code into another active process or reflectively load code into its own process, with the aim of loading malicious code, the adversary may try to hide in the normal operating noise of the system or abuse overzealous whitelisting:

1a. Detection

Searching for common processes that are performing uncommon actions can help identify when a process has been compromised. It would be uncommon for these processes to be executing additional process or performing discovery techniques. You can look for similar activity using a signature like:

```
Parent Process Name CONTAINS (‘explorer.exe’ OR ‘svchost.exe’)
Command Line CONTAINS (‘set’ OR ‘whoami’ OR ‘ping’ OR ‘dir’)
```

1b. Mitigation

- M1040 – Behavior Prevention on Endpoint
- M1026 – Privileged Account Management

2. Logon Autostart Execution: Registry Run Keys (001):

Preventing an actor from maintaining a foothold in your environment should always be one of the top priorities. During these activities, the adversary used registry keys to achieve persistence.

1a. Detection

Using a SIEM or EDR Platform to see modifications to the Run and RunOnce keys will alert when unauthorized users or software makes modifications to the keys that allow programs to run   after startup.

```
Process Name == reg.exe
Command Line Contains (“ADD” AND “\CurrentVersion\Run”)
```

1b. Mitigation

MITRE ATT&CK does not have any direction mitigations as this is abusing legitimate Windows functionality. They recommend monitoring registry changes and process execution that may attempt to add these keys.

Wrap-up

In summary, these attack graphs will evaluate security and incident response processes and support the improvement of your security control posture against a highly active and sophisticated threat. With data generated from continuous testing and use of these attack graphs, you can focus your teams on achieving key security outcomes, adjust your security controls, and work to elevate your total security program effectiveness against a known and dangerous threat.

AttackIQ stands at the ready to help security teams implement this attack graph and other aspects of the AttackIQ Security Optimization Platform, including through our fully managed service, AttackIQ Ready!, and our co-managed security service, AttackIQ Enterprise.

TAGS:

Education , Financial Services , Government , Healthcare & Life Sciences , Manufacturing , Professional Services , Retail , Technology

About the Author

Francis Guibernau

Francis Guibernau is an Adversary Research Engineer and member of the Adversary Research Team (ART) at AttackIQ. Francis conducts in-depth threat research and analysis to design and create highly sophisticated and realistic adversary emulations. He also coordinates the Cyber Threat Intelligence (CTI) project which focuses on the research, analysis, tracking and documentation of adversaries, malware families and cybersecurity incidents. Francis has extensive experience in adversary intelligence, encompassing both Nation-State and eCrime threats, as well as in vulnerability assessment and management, having previously worked at Deloitte and BNP Paribas. Learn More