Rhysida Ransomware and the Detection Opportunities

By SIMKRA

Published: 2024-11-18 · Archived: 2026-04-05 16:20:43 UTC

Robust Detection and Analytical Scoring countering Cy-X threat actor like Ryhsida

While it was a hypothesis just a few months ago, it has now been confirmed that the Cy-X threat actors of Rhysida are affiliates of the former ransomware group Vice Society.

Our research team assessed the exact extent of this relationship and could actually follow one of the following hypotheses:

> Due to increased scrutiny from law enforcement, the threat group behind Vice Society fully disbanded their operation and migrated their efforts towards their newly created Rhysida operation (**rebrand**). In this case, this specific new encryption payload could have been developed directly by them or by a contracted developer exclusively for them (more likely).
>
> In continuation with their regular shifts of payloads, the threat actors behind Vice Society affiliated themselves to a new private third-party RaaS called Rhysida, that advertises the victims through its own leak site and no longer on the Vice Society leak site (new RaaS **affiliation**). In this case, the former Vice Society group might not be the only ones deploying Rhysida in the future.

Rhysida has also focused on big game hunting the last year, attacking targets such as the British Library, Ministry of Finance of Kuwait and various hospitals in the US.

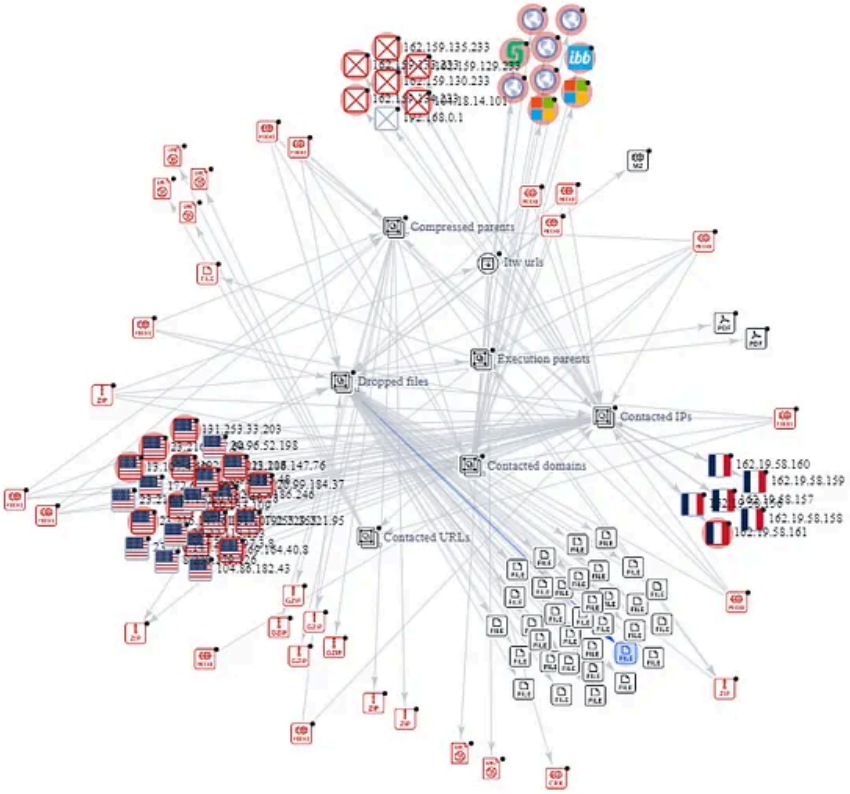
Just a few days ago, the news broke that the Royal family's sensitive data had been stolen by Rhysida in one of these attacks. Now the criminals are threatening to publish them.

In the following article, I have summarized one of the main indicators that I also presented at the SANS European DFIR Summit this summer for Rhysida and how to detect and hunt for the TTPs. The goal is to detect the top indicators in time or to harden the systems accordingly, as well as to prevent the spread of Ryhsida during an attack with the help of developing VIP detections in the event of a running incident. To find artifacts accordingly after the incident has happened helps to put the most important systems into operation again as quickly as possible.

In order to fully understand the TTPs and thus also the intention, the capabilities and an advantage in detection, I take therefore the findings from various CTI reports and my own Orange Cyberdefense analysis and those of my colleagues. These results give us the main MITRE ATT&CK techniques that Rhysida uses, including the tools also

of affiliates, various sources of artifact and the attacker's infrastructure. Here is a picture from Virus Total with the Infrastructure for Rhysida, published a few days ago:

Press enter or click to view image in full size

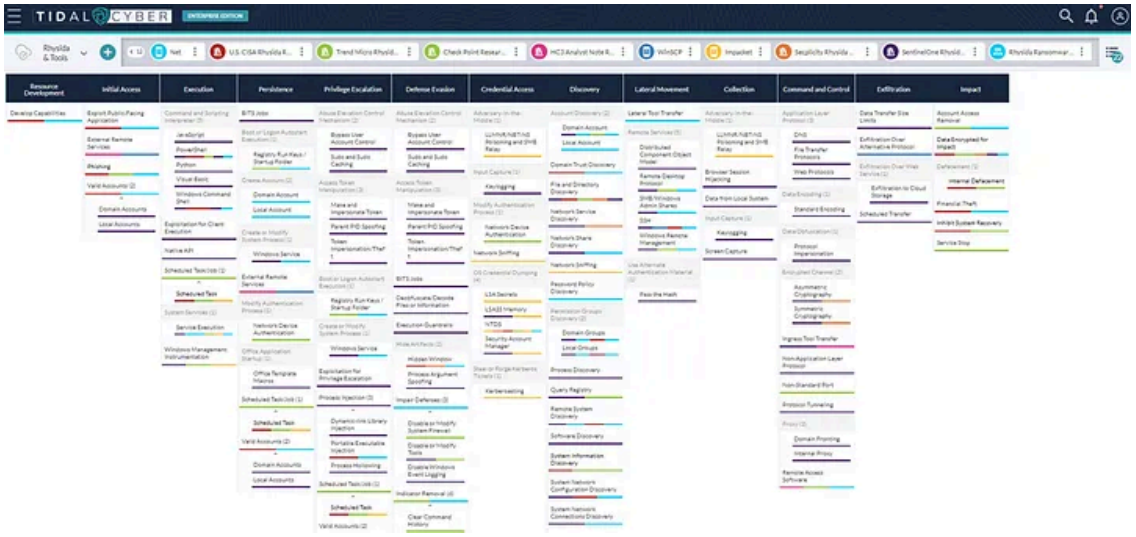


The graph shows us not only the execution of the ransomware but the contacted domains, IPs, URLs and more files that could be also interesting for the detection engineering and hunting. We see for example **fury.exe** as artifact and older version of the ransomware. In the article Scratching the Surface of Rhysida Ransomware for example you will find the executable as SHA1 **69b3d913a3967153d1e91ba1a31ebed839b297ed** for **fury_ctm1042.bin** and a great analysis of the executable reverse engineered. Such artifacts helps us to identify not only the ransomware group, but also to develop robust detection like we will see in the following analysis.

Therefore, first we take a look at the MITRE ATT&CK matrix with multilayering in Tidal Cyber Enterprise, the constellations of ransomware groups such as Rhysida, Vice Society and the associated tools that they use. The relationship of the ransomware groups and affiliates is described in the article from Sophos Same threats, different ransomware. In this article Sophos researcher cluster Vice Society with Rhysida. In addition to the cluster, other CTI reports such as those from SOCRadar, Trendmicro, Microsoft Threat Intelligence, Secplicity, Talos, Fortinet, SentinelOne, Checkpoint, CISA etc. and my own findings will be helpful to write **robust detection.**

All these information results in the following MITRE mapped TTP matrix including the capabilities means the tools from Rhysida:

Press enter or click to view image in full size



The analysis revealed the top tools and MITRE ATT&CK technique, which are recommended to be analyzed. Of course, there are more tools the threat actor has as capabilities, but it's just a starting point for **robust detection**.

Following tools are recommended to be prevented or detected specifically during an attack of the threat actor Rhysida:

· **PsExec** and other **Sysinternals tools** like in the CISA alert AA23–319A described

· The script **PortStarter**. PortStarter is a backdoor written in Go. According to Microsoft, this malware is capable of modifying firewall settings and opening ports to connect to pre-configured C2 servers

· The remote tool **AnyDesk**, very popular in the ransomware "scene" to get remotely access

· **SystemBC** is a post-compromise commodity RAT and proxy tool, used by numerous ransomware groups

· **Secretdump** for credential dumping

PowerShell & CMD executing the tools

T1059.001 PowerShell is executing **secretdump** or **ntdsutil.exe** observed for Vice Society. Command & Control can be detected as an artifact via **sock.ps** like describe for DEV-0832 or with the artifact **Sock5.sh** as mentioned in the CISA alert AA23–319A.

T1059.003 Windows Command Shell can also be used primarily in VIP detection **during the encryption** as an opportunity to **prevent further spread** in the event of an attack. *Normally, you should find ways to NOT have the situation of such an event, but be prepared!*

Therefore, here is a list of commands that Rhysida ransomware would execute via cmd.exe and reg.exe:

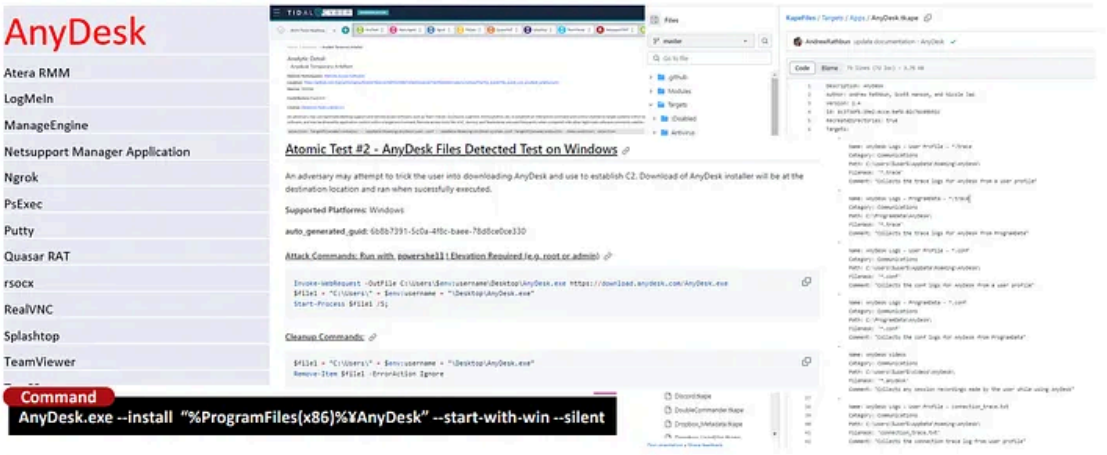
```
cmd.exe /c reg delete "HKCU\Conttol Panel\Desktop" /v WallpaperStyle /f

reg.exe delete "HKCU\Conttol Panel\Desktop" /v WallpaperStyle /f

cmd.exe /c reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop" /v NoChan
```

```
reg.exe add "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop" /v NoChangingWal
cmd.exe /c reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop" /v NoChan
reg.exe add "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop" /v NoChangingWal
cmd.exe /c reg add "HKCU\Control Panel\Desktop" /v Wallpaper /t REG_SZ /d "C:\Users\Public\bg.jpg" /
reg.exe add "HKCU\Control Panel\Desktop" /v Wallpaper /t REG_SZ /d "C:\Users\Public\bg.jpg" /f
reg.exe add "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v Wallpaper /t REG_SZ
cmd.exe /c reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v WallpaperStyl
reg.exe add "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v WallpaperStyle /t RE
cmd.exe /c reg add "HKCU\Control Panel\Desktop" /v WallpaperStyle /t REG_SZ /d 2 /f
reg.exe add "HKCU\Control Panel\Desktop" /v WallpaperStyle /t REG_SZ /d 2 /f
cmd.exe /c reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v Wallpaper /t
cmd.exe /c cmd.exe /c reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v Wa
```

PsExec

Executing PsExec with the specific parameters **-d -u** and **-s cmd c/ COPY** and copying the files to the **C:\Windows\Temp** folder is another specific indicator of the ransomware group. This also includes the T1569.002 Services Execution including PsExec with the specific parameters for Rhysida mentioned above. The behavior itself can be tested, as I described at the SANS's European DFIR Summit with the Atomic Red Team Test#2 T1219 as shown in the picture below:

Press enter or click to view image in full size

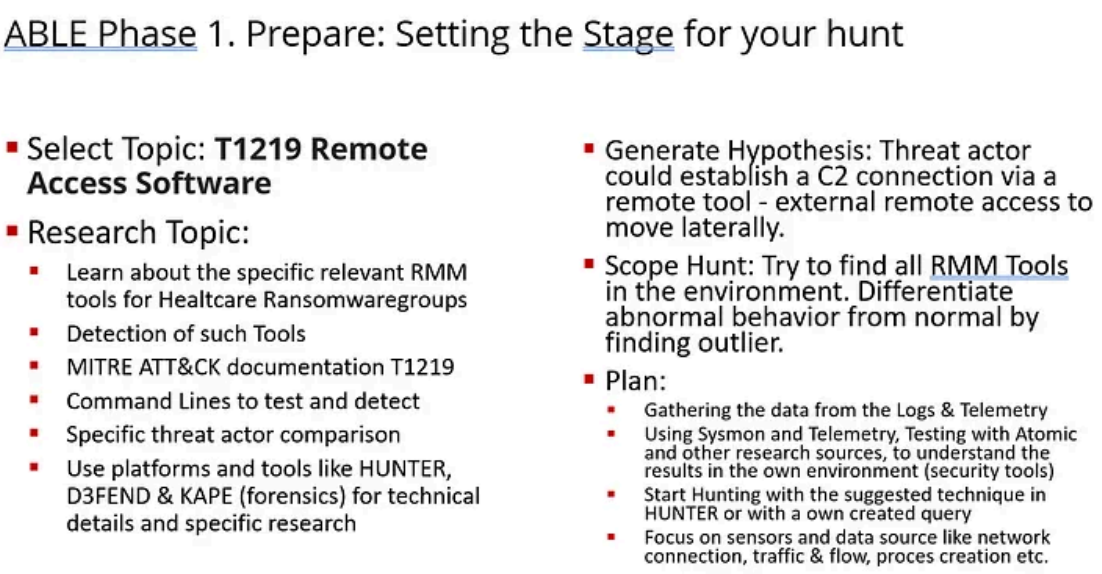


Threat Hunting Any Desk with David Bianco's PEAK Threat Hunting Framework

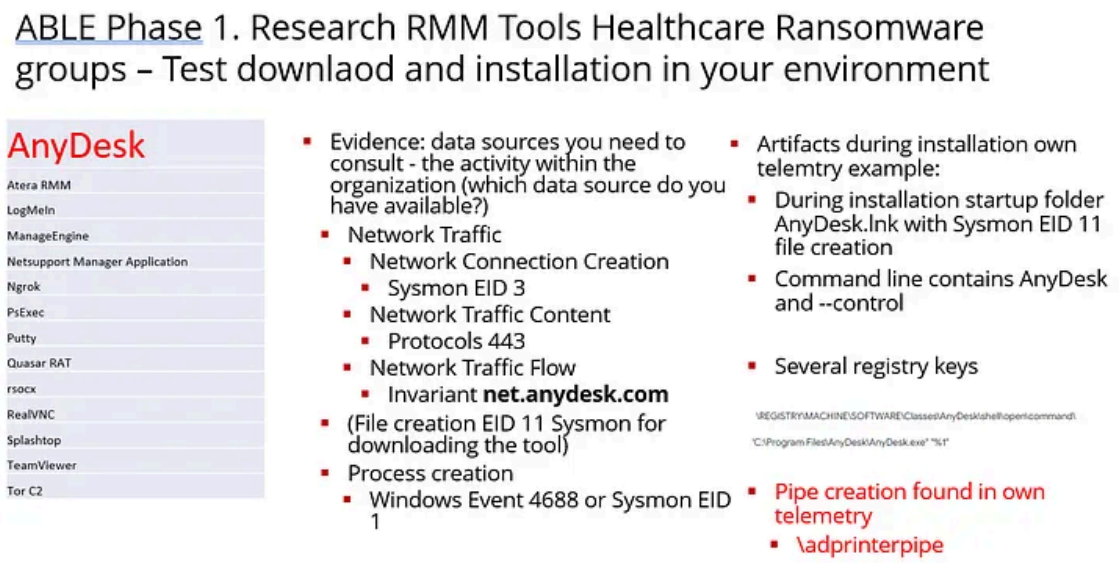
To systematically analyze and hunt for AnyDesk or RMM tools you can take for the research the outstanding [PEAK approach]of David Bianco.

A very short high level description for PEAK is: with ABLE you analyze systematically **actor, behavior, location and evidence**. In the first phase of PEAK (**Prepare, Execute, Act and Knowledge)** you set the stage for your hunt like shown in the picture above, after that you gather and escalate your critical findings to preserve and in the last phase of your hunt you document your finding. I think I will write another article about the PEAK Threat Hunting Framewok in the future with another example and dive a little bit deeper into it. Let's do it now with a short summary for AnyDesk with the following pictures:

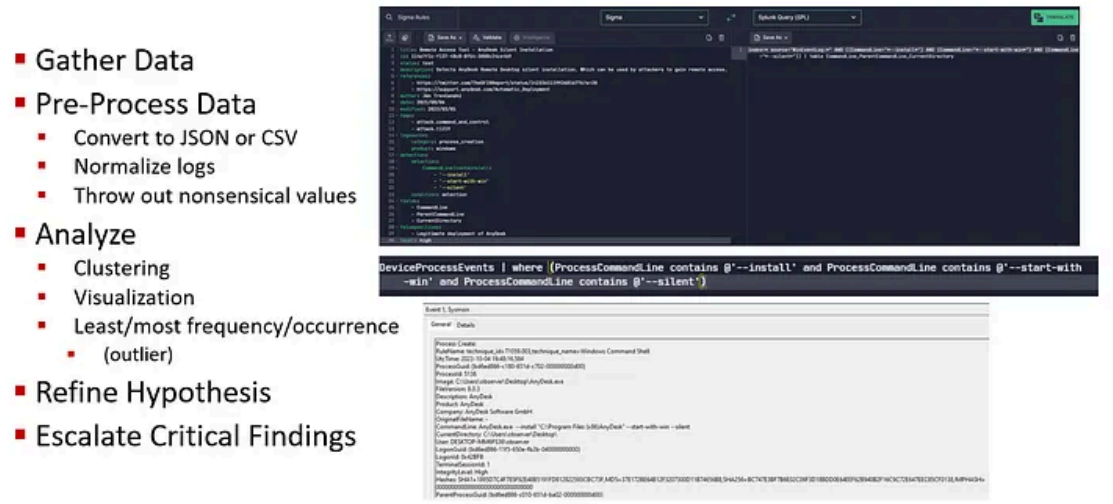
Press enter or click to view image in full size



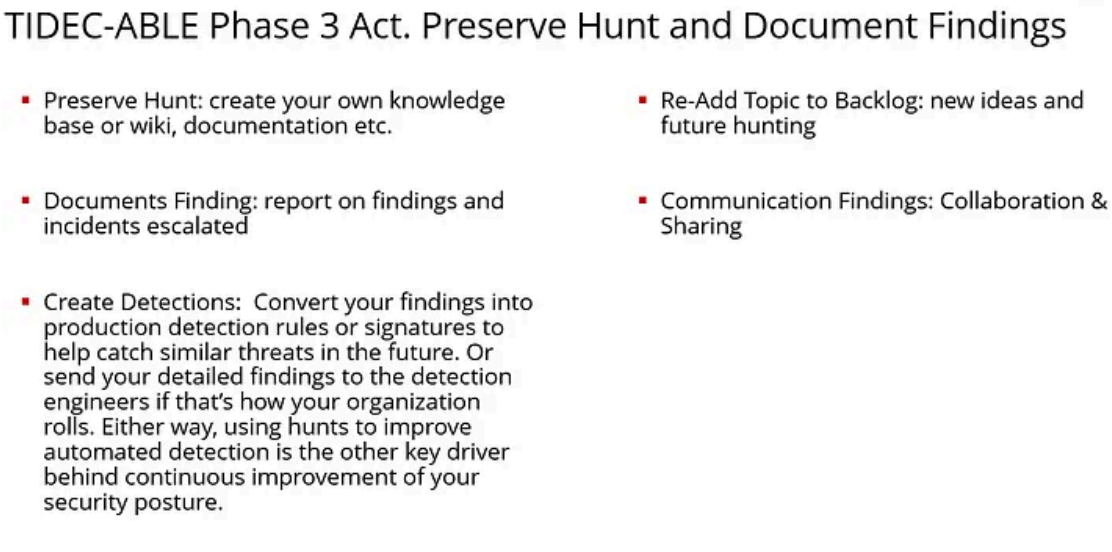
Press enter or click to view image in full size



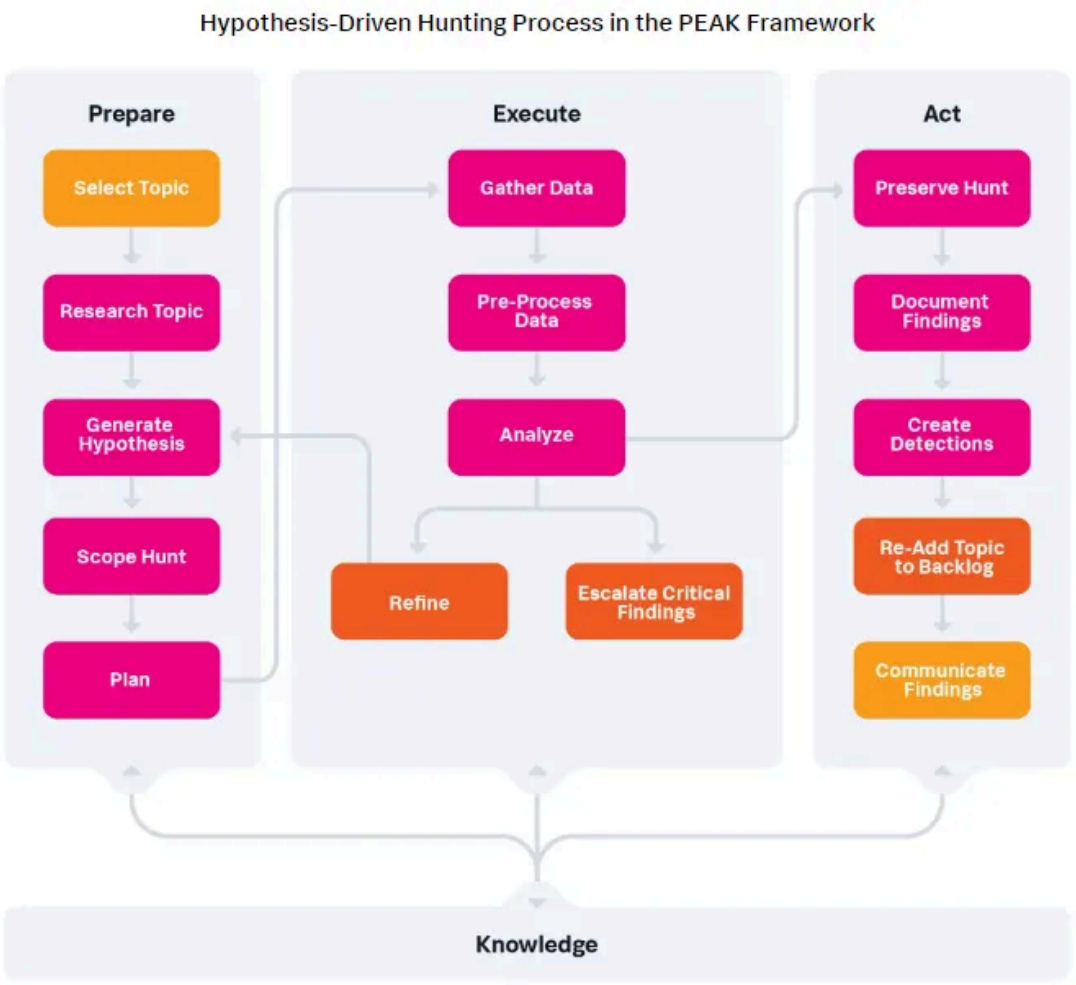
Press enter or click to view image in full size



Press enter or click to view image in full size



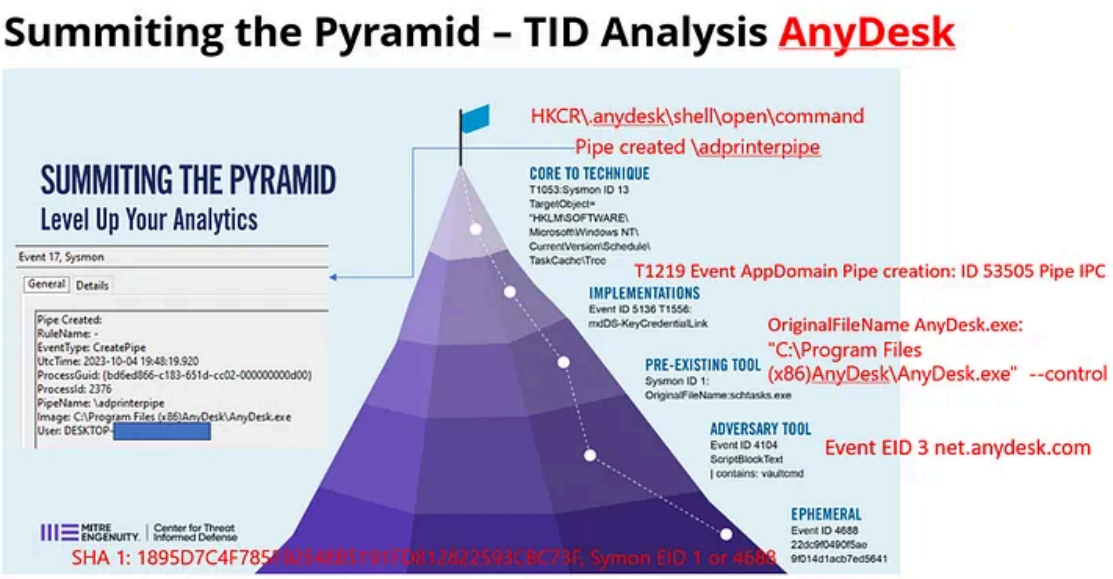
This results into knowledge (picture originally from David Bianco for Hypothesis-Driven Hunting Process:



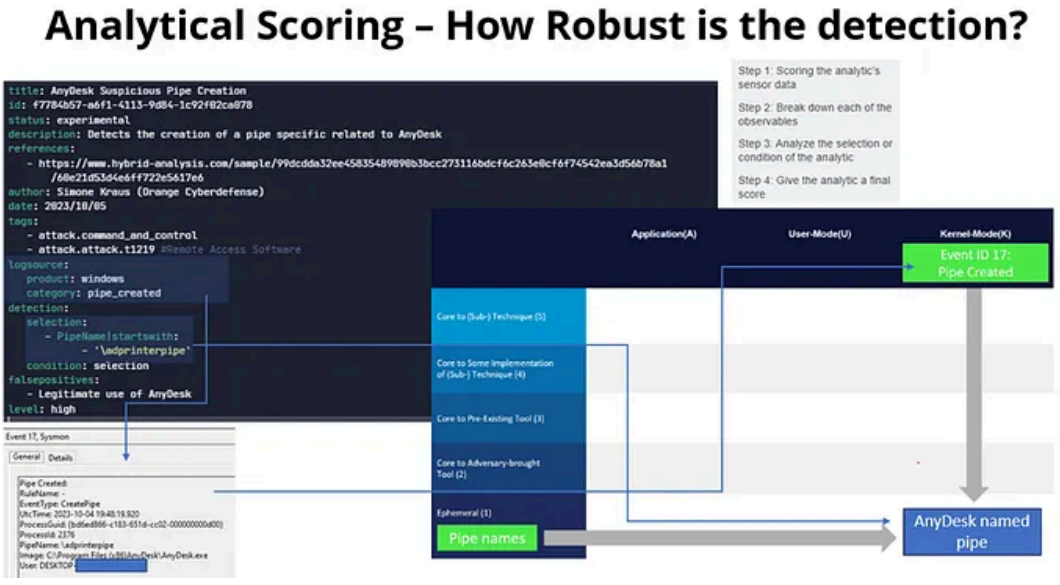
Hunting Rhysida AnyDesk

For the installation process independent of the **anydesk.exe**, *which would no longer be detected by a name change*, it is recommended to use a robust detection such for named pipe like we've seen in the pictures before for **\adprinterpip**, which could be detected during the installation of AnyRun via Sysmon, for example. You can take the detection and score it with the Summiting of the Pyramid approach, a thread informed defense approach that is developed by the MITRE Center for Threat Informed Defense to score detection systematically.

Press enter or click to view image in full size



Press enter or click to view image in full size



I have described a detailed summary of the brilliant approach in my article Summiting the Pyramid — A new Dimension of Cyber Analytics Engineering. I highly recommend to read the article about it like the original documentation you can find here.

Open Source Community Edition Detection Engineering Tools

imede.ai

Further Sigma Rules for AnyDesk regarding installation are available from the legendary **The DFIR Report** team in the imede.ai community edition. Imede.ai is a relatively new detection engineering platform with built-in Sigma Rules and attack simulation for which you need the enterprise version I unfortunately don't have right now. In the community edition Sigma Rules are available for the entire kill chain as well as specifically for Sysmon, Zeek and Azure. I'm excited to see how the platform will evolve. At the moment it is still relatively little input, but this will

certainly improve over time with increasing awareness that such a detection engineering platform exists and offers another opportunity to search for specific hunting queries.

uncoder.ai

In uncoder.ai for example you can get even more Sigma Rules for AnyDesk like the Sigma Rule from frack113 “Anydesk Temporary Artefact”. In this Sigma Rule AnyDesk would be detected for the the **user.conf** and **system.conf** in **.temp**. The Sigma Rules are also availabe on github.

Example Query KQL for Microsoft Defender for Endpoint:

DeviceFileEvents | where ((FolderPath contains @’\AppData\Roaming\AnyDesk\user.conf’ or FolderPath contains @’\AppData\Roaming\AnyDesk\system.conf’) and FolderPath endswith @’.temp’)

PortStarter Rhysida C2 Script

PortStarter, a tool that uses Ryhsida to establish a C2 backdoor communication, the detection opportunity is the **main.dll** with the hash **b25b87cfcedc69e27570afa1f4b1ca85aab07fd416c5d0228f1fe32886e0a9a6in** path **C:\Users\Public\main.dll**.

Analysis Sophos Schedule Task Living off the Land Rundll32 for PortStarter

To execute the PortStarter backdoor, the attackers were observed creating a scheduled task called ‘System’ for persistence to run **C:\Users\Public\main.dll**:

```
C:\Windows\system32\schtasks.exe /create /sc ONSTART /tn System /tr “rundll32 C:\Users\Public\main.d
```

Similarly, the threat actors were also observed creating a scheduled task called ‘*SystemCheck* for persistence to run a PortStarter DLL (**C:\ProgramData\schk.dll**).

```
C:\Windows\Tasks\windows32u.dll

C:\Windows\Tasks\windows32u.ps1
```

Over the course of several cases PortStarter backdoor was observed in different file paths reaching out to the following IPs:

C:\Windows\System32\config\main.dll

156.96.62[.]58

146.70.104[.]249

51.77.102[.]106

c:\users\public\main.dll

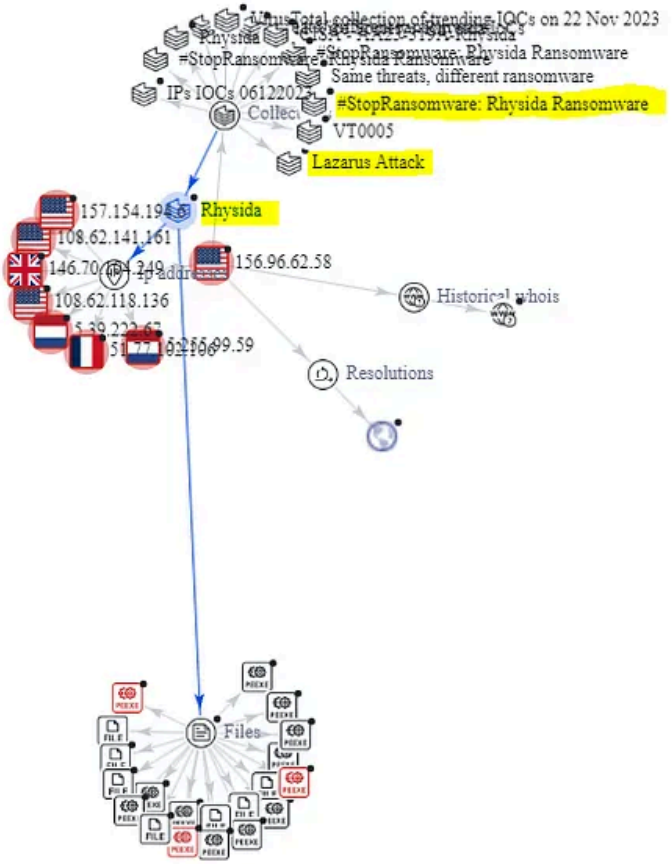
108.62.141[.]161

C:\ProgramData\schk.dll

157.154.194[.]6

And especially for the IP address **156.96.62.58** we can also see that this IP address was abused by the threat actor *Lazarus*, too.

Press enter or click to view image in full size



Credential Access

Rhysida's credential access tactic is similar to Vice Society's approach via NTDS.dit with the MITRE ATT&CK technique T1003.003.

Here you can hunt on the command **powershell 'ntdsutil.exe' 'ac i ntds' 'ifm' 'create full c:\temp_l0gs' Q q'** as well as on the tool **secretdump**. If you find secretdump, it may also be an indicator that Rhysida has successfully used the exploit **Zerologon** as mentioned in the note of exploit-db as a 3rd point and described in various CTI reports such as CISA alert AA23–319A.

```
NOTE - Exploitation will break the DC until restored, recommended guidelines:

    1. Check the DC - usually ~300 attempts, use the NETBIOS name not the FQDN:
        cve-2020-1472.py -do check -target <NETBIOS NAME> -ip <IP>

    2. Exploit the DC - this will break the DC until restored:
        cve-2020-1472.py -do exploit <NETBIOS NAME> -ip <IP>

    3. Dump the DC - for the DA hashes, this will not contain the
machine hex-pass:
        secretsdump.py -just-dc -no-pass <NETBIOS NAME>\$@<IP>

    4. Dump the DC again - use the DA hash to get the machines hex-pass:
        secretsdump.py -no-pass -hashes <LMHASH>:<NTHASH> <DOMAIN>/<ADMIN>@<IP>

    5. Restore target - this fixes the DC:
        cve-2020-1472.py -do restore -target <NETBIOS NAME> -ip <IP>
-hex <HEXPASS>
```

Special reference should also be made here to the artifact **temp_l0gs**. Both Vice Society and Rhysida generate this file **during credential dumping**.

As always, there are different sources to create your own Sigma Rules or to use hunting packages from HUNTER or impede.ai as well as Tidal Cyber and SOC Prime. All platforms offer a community edition. Uncoder.ai has the advantage of being able to immediately optimize specific sigma rules for the respective attacker himself while Tidal Cyber gives you a great overview which Sigma Rule to use for a specific MITRE ATT&CK technique.

Especially for Rhysida, Cyborg Security HUNTER offers the following hunting packages in the community edition for free

Wevtutil Cleared Log

Remote Desktop Protocol (RDP) port manipulation

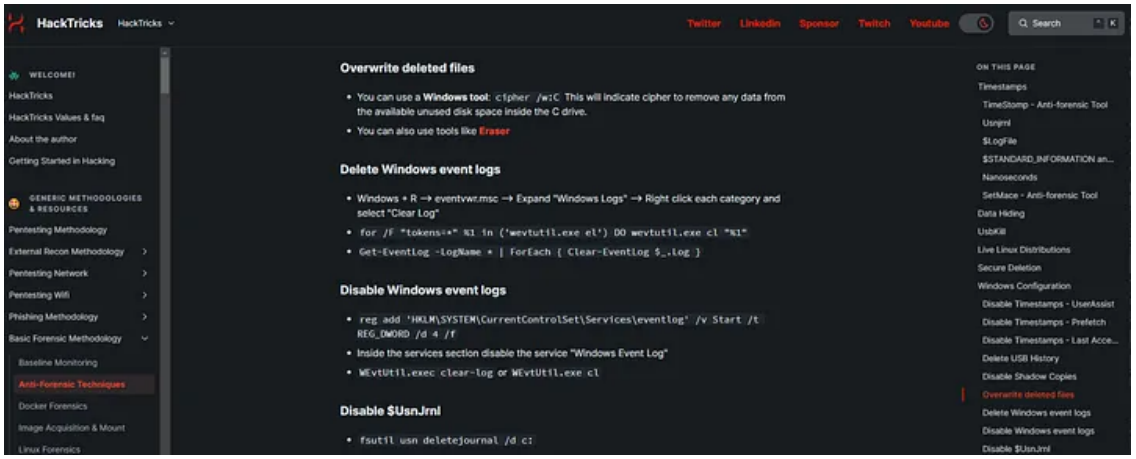
Autorun or ASEP Registry Key Modification

Shadow Copies Deletion Using Operating System Utilities

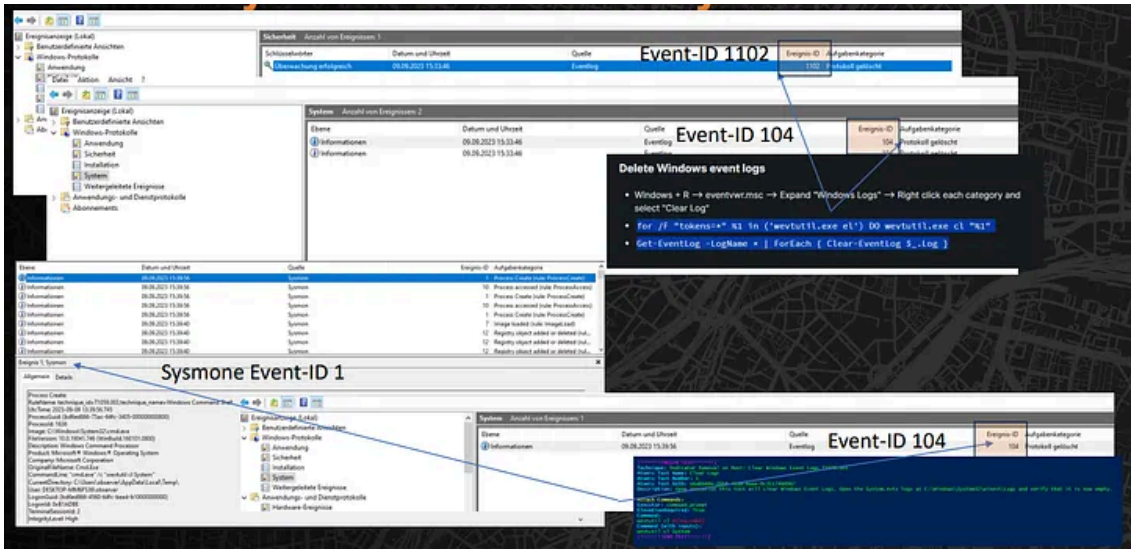
Deletion of Windows Event Logs

Regarding **wevtutil** you can test it in your own environment in several ways to understand your telemetry as shown in the following picture:

Press enter or click to view image in full size



Press enter or click to view image in full size

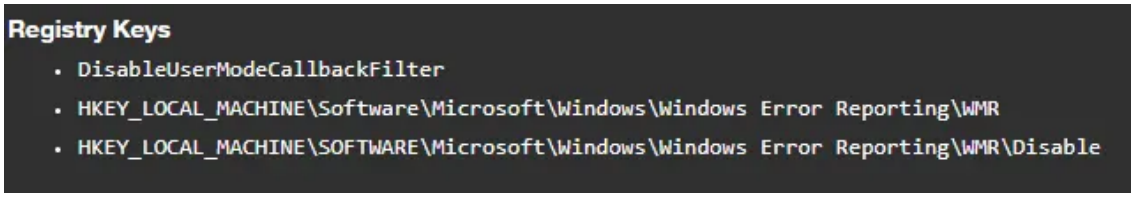


It is the same way Rhysida would delete your events.

Another detection opportunity is that Ryhsida drops as ransom not the **CriticalBreachDetected.pdf**. And it removes the subkey under **HKCU:\Software\Microsoft\Terminal Server Client** like it removes **UsernameHint.**

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

During the encryption Rhysida changes the registry to disable Windows error reporting. This is another specific IOC you can take as a VIP detection.



During your investigation following IOCs are recommended by CISA:

Sock5.sh 48f559e00c472d9ffe3965ab92c6d298f8fb3a3f0d6d203cd2069bfca4bf3a57
PsExec64.exe edfae1a69522f87b12c6dac3225d930e4848832e3c551ee1e7d31736bf4525ef
PsExec.exe 078163d5c16f64caa5a14784323fd51451b8c831c73396b967b4e35e6879937b
PsGetsid64.exe 201d8e77ccc2575d910d47042a986480b1da28cf0033e7ee726ad9d45ccf4daa
PsGetsid.exe a48ac157609888471bf8578fb8b2aef6b0068f7e0742fccf2e0e288b0b2cfdfb
PsInfo64.exe de73b73eeb156f877de61f4a6975d06759292ed69f31aaf06c9811f3311e03e7
PsInfo.exe 951b1b5fd5cb13cde159cebc7c60465587e2061363d1d8847ab78b6c4fba7501
PsLoggedon64.exe fdadb6e15c52c41a31e3c22659dd490d5b616e017d1b1aa6070008ce09ed27ea
PsLoggedon.exe d689cb1dbd2e4c06cd15e51a6871c406c595790ddcdcd7dc8d0401c7183720e
PsService64.exe 554f523914cdbaed8b17527170502199c185bd69a41c81102c50dbb0e5e5a78d
PsService.exe d3a816fe5d545a80e4639b34b90d92d1039eb71ef59e6e81b3c0e043a45b751c
Eula.txt 8329bcbadc7f81539a4969ca13f0be5b8eb7652b912324a1926fc9bfb6ec005a
psfile64.exe be922312978a53c92a49fefd2c9f9cc098767b36f0e4d2e829d24725df65bc21
psfile.exe 4243dc8b991f5f8b3c0f233ca2110a1e03a1d716c3f51e88faf1d59b8242d329
pskill64.exe 7ba47558c99e18c2c6449be804b5e765c48d3a70ceaa04c1e0fae67ff1d7178d
pskill.exe 5ef168f83b55d2cbd2426afc5e6fa8161270fa6a2a312831332dc472c95dfa42
pslist64.exe d3247f03dcd7b9335344ebba76a0b92370f32f1cb0e480c734da52db2bd8df60
pslist.exe ed05f5d462767b3986583188000143f0eb24f7d89605523a28950e72e6b9039a
psloglist64.exe 5e55b4caf47a248a10abd009617684e969dbe5c448d087ee8178262aaab68636
psloglist.exe dcdb9bd39b6014434190a9949dedf633726fdb470e95cc47cdaa47c1964b969f
pspasswd64.exe 8d950068f46a04e77ad6637c680cccf5d703a1828fbd6bdca513268af4f2170f
pspasswd.exe 6ed5d50cf9d07db73eaa92c5405f6b1bf670028c602c605dfa7d4fcb80ef0801
psping64.exe d1f718d219930e57794bdadf9dda61406294b0759038cef282f7544b44b92285
psping.exe 355b4a82313074999bd8fa1332b1ed00034e63bd2a0d0367e2622f35d75cf140
psshutdown64.exe 4226738489c2a67852d51dbf96574f33e44e509bc265b950d495da79bb457400
psshutdown.exe 13fd3ad690c73cf0ad26c6716d4e9d1581b47c22fb7518b1d3bf9cfb8f9e9123
pssuspend64.exe 4bf8fbb7db583e1aacbf36c5f740d012c8321f221066cc68107031bd8b6bc1ee
pssuspend.exe 95a922e178075fb771066db4ab1bd70c7016f794709d514ab1c7f11500f016cd
PSTools.zip a9ca77dfe03ce15004157727bb43ba66f00ceb215362c9b3d199f000edaa8d61
Pstools.chm 2813b6c07d17d25670163e0f66453b42d2f157bf2e42007806ebc6bb9d114acc
psversion.txt 8e43d1ddbd5c129055528a93f1e3fab0ecdf73a8a7ba9713dc4c3e216d7e5db4
psexesvc.exe This artifact is created when a user establishes a connection using psexec. It is removed after the connection is terminated, which is why there is no hash available for this executable.

To detect the deployment you can take following IOCs

psexec.exe 078163d5c16f64caa5a14784323fd51451b8c831c73396b967b4e35e6879937b
A file used to execute a process on a remote or local host.
S_0.bat 1c4978cd5d750a2985da9b58db137fc74d28422f1e087fd77642faa7efe7b597
A batch script likely used to place 1.ps1 on victim systems for ransomware staging purposes [T1059.003].
1.ps1 4e34b9442f825a16d7f6557193426ae7a18899ed46d3b896f6e4357367276183
Identifies an extension block list of files to encrypt and not encrypt.
S_1.bat
97766464d0f2f91b82b557ac656ab82e15cae7896b1d8c98632ca53c15cf06c4
A batch script that copies conhost.exe (the encryption binary) on an imported list of host names within the **C:\Windows\Temp** directory of each system.
S_2.bat
918784e25bd24192ce4e999538be96898558660659e3c624a5f27857784cd7e1
Executes conhost.exe on compromised victim systems, which encrypts and appends the extension of .Rhysida across the environment.

The file extension for the encryption is **.Rhysida** and *additionally, third-party researcher identified evidence of Rhysida actors developing custom tools with program names set* ***Rhysida-0.1***.

Conclusion

Rhysida was first an underestimated ransomware group. Over the last months we can see that the threat actor is not only attacking critical infrastructure like the healthcare system but is developing capabilities similar to other big hunting threat actors.

The mere fact that Rhysida is targeting healthcare and is not afraid to blackmail the British royal family should make it clear that neither Vice Society nor Ryhsida affiliates will stop enriching themselves from other people’s misery. For this reason, companies as well as healthcare and government agencies should take measures to detect an attack.
