The Rhysida Ransomware: Activity Analysis and Ties to Vice Society

research.checkpoint.com/2023/the-rhysida-ransomware-activity-analysis-and-ties-to-vice-society/

August 8, 2023

Introduction

The Rhysida ransomware group was first revealed in May this year, and since then has been linked to several impactful intrusions, including an attack on the Chilean Army. Recently the group was also tied to an attack against Prospect Medical Holdings, affecting 17 hospitals and 166 clinics across the United States. After this attack, the US Department of Health and Human Services defined Rhysida as a significant threat to the healthcare sector.

While responding to a recent Rhysida ransomware case against an educational institution, the Check Point Incident Response Team (CPIRT), in collaboration with Check Point Research (CPR), observed a set of unique Techniques, Tactics and Tools (TTPs). During our analysis, we identified significant similarities to the TTPs of another ransomware group – Vice Society. Vice Society was one of the most active and aggressive ransomware groups since 2021, mostly targeting the education and healthcare sectors. For example, Vice Society was responsible for the attack against the Los Angeles Unified School District.

As a connection between Vice Society and Rhysida was suggested recently, we bring forth technical evidence to strengthen the connection. Our analysis shows both a technical similarity between the two groups, and a clear correlation between the emergence of

Rhysida and the disappearance of Vice Society. In addition, the two groups share a focus on two main sectors which stand out in the ransomware ecosystem: education and healthcare.

As Vice Society was observed deploying a variety of commodity ransomware payloads, this link does not suggest that Rhysida is exclusively used by Vice Society, but shows with at least medium confidence that Vice Society operators are now using Rhysida ransomware.

Tactics, Techniques and Procedures

As the Rhysida ransomware payload was thoroughly analyzed before, we will focus on the TTPs leading to its deployment, specifically on Lateral Movement, Credential Access, Defense Evasion, Command and Control, and Impact.

Based on the evidence we have, the time to ransom (TTR) of the actors employing Rhysida ransomware is relatively low. It has been eight days from the first signs of lateral movement to the widespread ransomware deployment.

Lateral Movement

The attackers used a variety of tools to perform lateral movement, including:

- **Remote Desktop Protocol** – Throughout the intrusion, the threat actor initiated RDP connections, and took additional steps to deliberately remove associated logs and registry entries to harden detection and analysis efforts (as described in the Defense Evasion section). RDP remains an effective approach to performing lateral movement within the environment.
- **Remote PowerShell Sessions (WinRM)** – While connected remotely via RDP, the threat actor was observed initiating remote PowerShell connections to servers within the environment. This happened in the days before the ransomware payload was deployed.
- **PsExec** – The ransomware payload itself was deployed using PsExec from a server within the environment. The deployment happened in two phases.
    - Copying the malicious payload using the command `PsExec.exe -d \\VICTIM_MACHINE -u "DOMAIN\ADMIN" -p "Password" -s cmd /c COPY "\\path_to_ransomware\payload.exe" "C:\windows\temp"`.
    - Executing the malicious payload using the command `PsExec.exe -d \\VICTIM_MACHINE -u "DOMAIN\ADMIN"" -p "Password" -s cmd /c c:\windows\temp\payload.exe`.

Credential Access

Most notably, the threat actor used ntdsutil.exe to create a backup of NTDS.dit in a folder name `temp_l0gs`. This path was utilized by the actor multiple times. In addition to those, the threat actor has enumerated Domain Administrator accounts and attempted to log in using

some of them.

Command and Control

The threat actors have utilized several backdoors and tools for persistence, including:

- **SystemBC –** In a successful PowerShell session, the attacker executed a SystemBC PowerShell implant (very similar to the implant described here) which maintains persistence by installing a registry run key named socks to execute the script on startup. The implant reaches out to `5.255.103[.]7`. Additionally, the threat actor set up a firewall rule named Windows Update to allow outbound traffic to another server, `5.226.141[.]196`.
- **AnyDesk –** The threat actor was observed using the remote management tool AnyDesk.

Defense Evasion

Throughout the activity, the threat actors consistently deleted logs and forensic artifacts following their activity. This includes:

- Deleting the history of recently used files and folders.
- Deleting a list of recently executed programs.
- Deleting the history of recently typed paths in File Explorer.
- Deleting PowerShell console history file.
- Deleting all files and folders within the current user's temporary folder.

Following RDP sessions, the threat actor also deleted RDP-specific logs by:

- Searching for all subkeys under "`HKCU:\Software\Microsoft\Terminal Server Client`" in the Windows Registry, and for each subkey, removing the "`UsernameHint`" value if it exists.
- Deleting `Default.rdp` from the users' Documents folder.

Impact

On the day of ransomware deployment, the threat actor utilized the access provided by AnyDesk to widely deploy the ransomware payload in the environment using PsExec:

- **Account Access Removal** – The threat actor initiated a password change for tens of thousands of accounts in the domain to harden remediation efforts.

- **Inhibit System Recovery** – Before deploying the ransomware payload, the threat actor attempted to deploy a PowerShell script with a wide variety of capabilities, including:
    - Changing all local passwords to a predefined password.
    - Killing services related to database systems, backup software, and security products.
    - Disabling Windows Defender and creating exclusions for it.
    - Deleting shadow copies with both wmic.exe and vssadmin.exe.
    - Changing the default RDP port to 4000 and creating a firewall rule for it.
    - Deleting all Windows event logs and PowerShell history.
- **Data Encryption** – The threat actor ended up deploying the Rhysida ransomware payload using PsExec, as described above.

The Vice Society Connection

Throughout our analysis of Rhysida ransomware TTPs and infrastructure, we found several similarities to another infamous ransomware group: Vice Society, which was observed changing ransomware payloads over time. A possible link between Vice Society and Rhysida has been recently suggested. Here we will present additional evidence supporting this claim.

Techniques, Tools and Infrastructure

Many of the techniques described above are highly correlated with previous Vice Society intrusions as described by Microsoft and Intrinsec. Some of them might appear quite generic for Ransomware operators, but were utilized in very specific ways, including specific paths, which are not common:

- Utilization of NTDSUtil the create a backup of `NTDS.dit` to a folder named `temp_l0gs`. The same path was reported to be used by Vice Society.
- Creation of a local Firewall rule using `New-NetFirewallRule` named Windows Update to facilitate traffic relaying using SystemBC, a commodity malware. SystemBC was executed through the registry Run key, stored under the value socks.
- Initiation of a domain-wide password change process before deployment of ransomware payload.
- Analysis of infrastructure related to a Rhysida incident surfaced a set of PortStarter samples, some of them previously attributed to Vice Society. Although PortStarter is often described as a commodity tool, its usage has been linked almost exclusively to Vice Society in public reports.

Victimology

In addition to technical similarity, there is also a correlation between the emergence of Rhysida and a significant decline in Vice Society activity. Based on information from both Rhysida and Vice Society leak sites, we constructed a timeline displaying extortion announcements of the two groups.

Ever since Rhysida first appeared, Vice Society has only published two victims. It's likely that those were performed earlier and were only published in June. Vice Society actors stopped posting on their leak site since June 21, 2023.

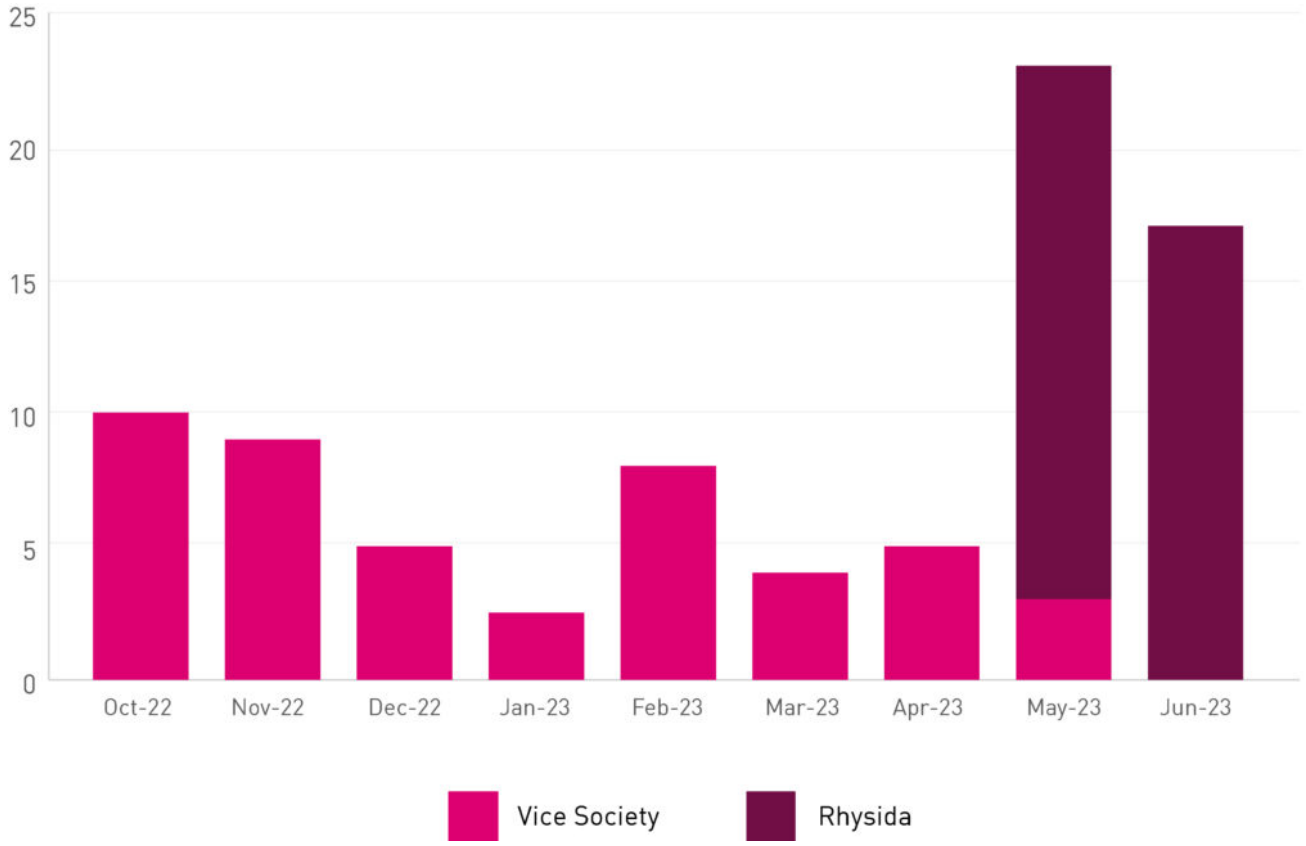

Figure 1 – Distribution of Rhysida and Vice Society victims over time.

In addition, we also noticed similarities in the targeted sectors affected by the two groups, which are well known for targeting the education and healthcare industries. The high portion of victims in the education industry stands out as unique for both groups in the entire ransomware ecosystem:

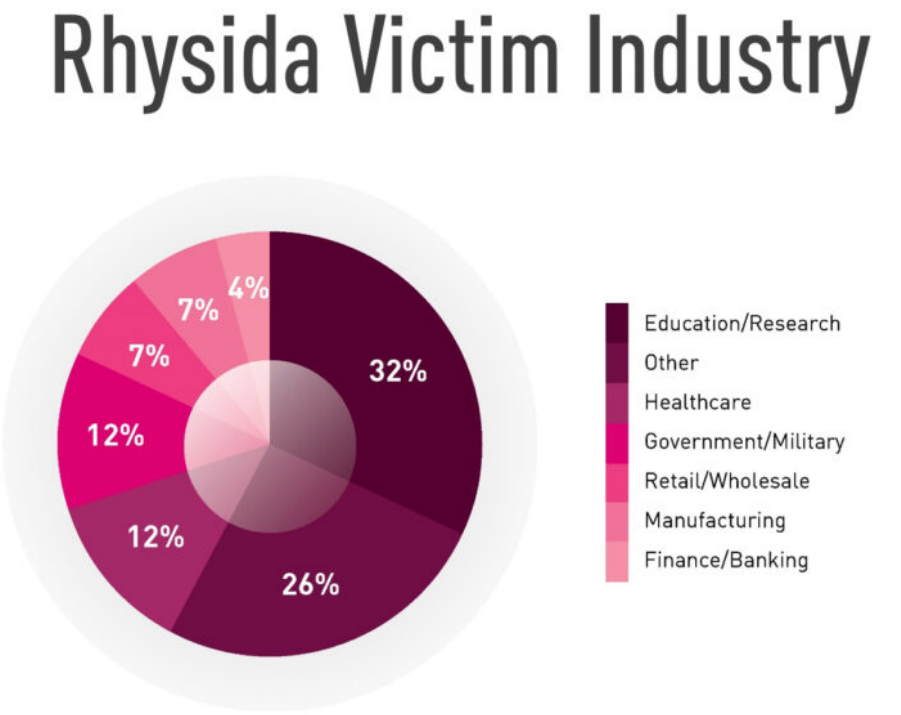

Figure 2 – Distribution of Rhysida victims per industry sector.

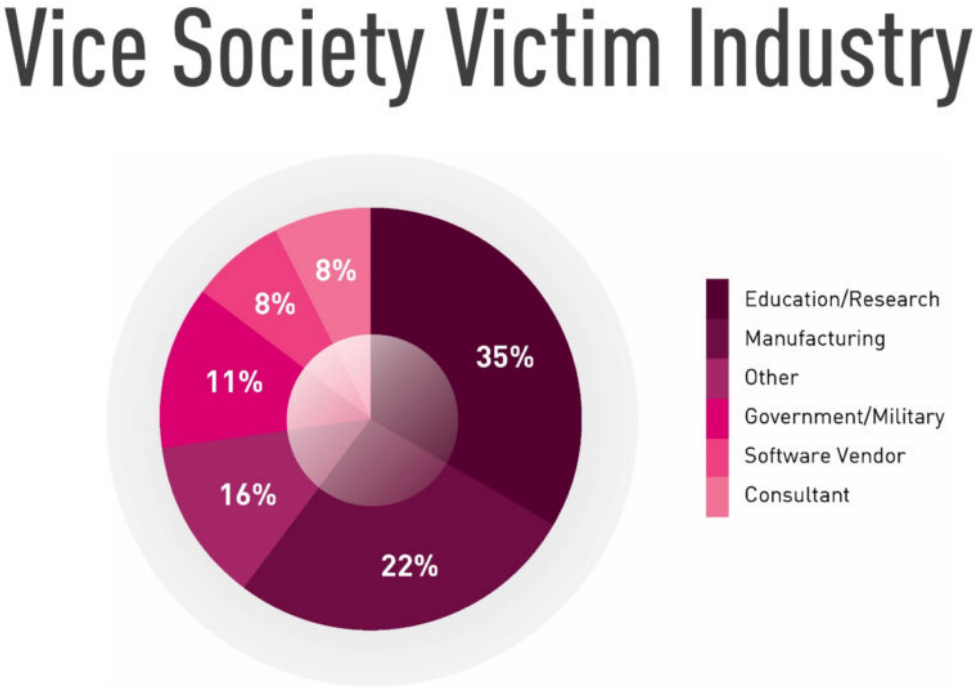

Figure 3 – Distribution of Vice Society victims per industry sector.

Conclusion

Our analysis of Rhysida ransomware intrusions reveals clear ties between the group and the infamous Vice Society, but it also reveals a grim truth – the TTPs of prolific ransomware actors remain largely unchanged. Major portions of the activity we've observed could have been used, and have been used, to deploy any ransomware payload by any ransomware group.

This highlights the importance of understanding not just the operation of a ransomware payload, but the entire process leading to its deployment. From the usage of remote management tools such as AnyDesk to the deployment of ransomware through PsExec, threat actors leverage a variety of tools to facilitate such attacks. Closely monitoring the activity of those could help in preventing the next ransomware attack.

Check Point Software customers remain protected against Rhysida ransomware.

Check Point Threat Emulation and Harmony Endpoint provide comprehensive coverage of attack tactics and file types and is protecting against the type of attacks and threats described in this report.

GO UP
BACK TO ALL POSTS