Rhysida: Evading Detection, One Service at a Time

Archived: 2026-04-05 20:07:04 UTC

During a recent engagement, At-Bay Security analysts observed artifacts showing a threat actor operating under the Rhysida ransomware brand attempting to hide their network activity prior to ransomware deployment.

Based on these observations, actionable steps organizations can take to protect themselves include:

- Educate users on how to identify social engineering tactics such as search engine optimization (SEO) Poisoning which may falsely elevate malicious URLs in search engine results.
- Detections built around the disabling of, or tampering with security controls and services, including changes or modifications to security settings (e.g. Windows Defender).
- Enforce Multi-Factor Authentication for all remote connections.
- Leverage a managed version of Endpoint Detection and Response (EDR) so that alerts are identified and actioned in real-time.

About Rhysida Ransomware

Rhysida Ransomware, first detected in May 2023, has impacted hundreds of victim networks across the globe, with a particular focus on sectors such as healthcare, government, education and manufacturing.

This group operates on a double extortion model, exfiltrating data and encrypting networks prior to asking for a financial demand. Rhysida is also known to use a variety of methods to infiltrate systems including the exploitation of external remote services (e.g. VPNs) and phishing.

Key Findings

In a case observed by At-Bay, a user at an organization fell victim to a tactic known as Search Engine Optimization (SEO) poisoning and downloaded a trojanized version of Putty.exe which helped Rhysida gain access and persistence into the network. Once inside, the actor moved laterally through the network using Remote Desktop Protocol (RDP). During the threat actor's time in the system, forensics identified the use of the tool Advanced Port Scanner for network enumeration and exfiltration via azcopy commands, successfully transferring over a hundred thousand files into a threat actor-controlled Azure storage. After exfiltration, but prior to ransomware deployment, the threat actor was observed clearing security logs across numerous systems, the details of which will be discussed in the next sections.

Rhysida Evasion Techniques

At-Bay Security reviewed access to a client environment after encryption with Rhysida ransomware (.rhysida). Investigation identified that the threat actor was diligent in clearing logs and other techniques to hide their tactics, techniques and procedures. However, investigators identified that a script meant to clear logs during the intrusion failed to complete the process, giving At-Bay analysts visibility into how the script worked.

This article will break down each section of this code to reveal insights into threat actor obfuscation.

In the Beginning

The discovered script starts with the declaration of variables which can and will likely be changed per environment.

Here we start with the threat actor hard-coding an SMB IP address, which can be a share that already exists or that the threat actor sets prior to the execution. They also define a password later used to reset the 'Administrator' account, as well as change the text shown to a user prior to logging in.

▶ Show code snippet

Evasion

Services

In the next section of the script, the threat actor coded the name of services potentially running on a host that could hamper their exfiltration or encryption efforts.

The Function 's' defines a list of services names and if they are present on the host it will attempt to set these services to disabled and stop them. Most services will attempt to auto restart if they crash or are closed, this is what the disabling part of the script is trying to address. After the services have been set to be disabled, they then attempt to stop those processes.

▶ Show code snippet

Processes

The next step attempts to identify and stop already running processes. This list targets both base server applications as well as AV processes, Backup processes, Remote Management processes, ERP Applications and Administration tooling. Using Windows Management Instrumentation Command-Line (WMIC) the TA will look for running processes with specific names and terminate the process using the "delete" function. Following that the threat actor uses powershell to terminate specific processes if they are currently running.

After the threat actor shuts down these services and processes they move on to active changes within the system.

▶ Show code snippet

Configuration Changes

In the next section of code, the threat actor sets an exception in Windows Defender to allow execution of any .exe file. After that the threat actor sets the extension '.Readme' to be a text file which will aid in the compromised user being able to easily open any file with a '.Readme' extension such as the ransom note. The last part of this section copies the computer name from the environment variable to a variable named '$name', to be used later in the script.

▶ Show code snippet

Wakey-Wakey Eggs and Bakey

The threat actor uses the ARP table of the computer to compile a list of MAC addresses the computer knows about and crafts a Wake-On-Lan magic packet to those systems in an attempt to bring any of those systems that might have been offline back online, aiding in lateral movement inside an organization.

▶ Show code snippet

Enable Remote Access

The threat actor enables RDP within the windows registry and within the windows firewall enables any rule associated with the ‘Remote Desktop’ group.

▶ Show code snippet

Local Account Modification

Here in this section, the threat actor gathers a list of all local accounts on a windows system. With this list of users it builds new passwords for the accounts, which is the first 13 characters of a MD5 hash. The hash is created by combining the username with the word ‘zero’.

▶ Show code snippet

Elevation

Here in this section the local built-in ‘Administrator’ has its password set to the password set at the beginning of the script named ‘$LOCAL_ADMIN_PASS’. It will then make sure the local ‘Administrator’ account is part of the local security group ‘Administrators’ ensuring the account has administrative privileges on the host. The threat actor also adds the same account to the local ‘Remote Desktop Users’ security group, in combination with the previous edits to the remote desktop setting the threat actor should now have remote access to this host using the local ‘Administrator’ account.

▶ Show code snippet

No Way Back

In this section of the script, the threat actor takes steps to inhibit restoration of this host after the encryption event. The threat actor removes any Windows backups, or any shadow copies and restore points which might exist on the system.

▶ Show code snippet

Here the threat actor attempts to remove the feature ‘Windows Defender’ from the host.

▶ Show code snippet

Evade, Evade, Evade

Next, the function ‘Uninstall-App’ attempts to remove protections on installed applications and perform an uninstall by either utilizing msiexec or cmd.exe.

▶ Show code snippet

Blocking Restoration

This part of the script changes the boot policies for a Windows host and turns off recovery options if the host has issues during boot. This poses a hindrance to any restoration options presented to the user at boot time. Next, the script enables Windows remote management and turns on the ability to execute Powershell commands on this host from a remote system.

▶ Show code snippet

Check-in and Welcome Message

The script will then check to see if Windows Defender is still present. If the process is running, a text file named the computer name will be written to the share identified in variables at the beginning of the script and write ‘NO’ conversely if Windows Defender is not currently running it does the same but writes ‘OK’ to the text file. Next the script will modify the text displayed to an end user prior to logging on to the computer, with the content of the variables set at the beginning of the script.

▶ Show code snippet

Stealth Check

Now, the script clears all files located in C:\Windows\Temp. Next for every user profile on the system it will remove any files in the per user temp directory. After removing these temporary files, the script then will clear Event Logs for the Security, Application and System events. It will remove any Powershell commands which might be present in the Powershell Console History log. Inserted here amongst the evidence tampering techniques is another removal instruction for uninstalling Trend-Micro. It then clears the Powershell window and removes the history typed within.

▶ Show code snippet

File List, Achieved

The last of the recovered script we have here enumerates the file paths for all drives, providing the threat actor with insight into the data contained across the network.

▶ Show code snippet

Conclusion & Mitigation Tactics

This article highlights the lengths ransomware groups such as Rhysida will go to to hide their tracks while in a network. It is vital for organizations to use multi-layered security controls to prevent threat actors from accessing the network and to detect and eject them should one make it past first-line defenses.

Practical suggestions to prevent ransomware attacks such as Rhysida include:

1. Enforce Multi-Factor Authentication for remote services such as Virtual Private Networks (VPN) or Remote Desktop Protocol (RDP).
2. Maintain a regular schedule for patching to ensure critical systems are running the latest versions of commercial software.
3. Educate and inform users on how to identify suspicious emails or web search results prompting them to download software. Software should only be obtained from the official company domain.
4. Utilize Managed Detection and Response service to help identify and stop threat actor activity.

At-Bay policyholders have access to meetings with Cyber Advisors through the Stance Advisory Services in their policy. At-Bay's expert Cyber Advisors can assist with advanced assessments, security training, and provide personalized recommendations for your organization. At-Bay also offers 24×7 monitoring and remediation through Stance Managed Detection and Response services.
