# Rhysida Ransomware Attacking Windows Machine Through VPN Devices and RDP

By **Tushar Subhra Dutta** - November 21, 2023

Rhysida, a new ransomware group, hit its first victim in May 2023. They use their ransomware, offered as RaaS

(Ransomware-as-a-Service), with at least 50 global victims listed on their website.

In May 2023, they made headlines for deploying ransomware in systems linked to the Chilean Army.

Recently, the cybersecurity researchers at Fortinet identified that Rhysida ransomware attacks Windows machines through VPN devices and RDP.

## Ransomware Attacking Windows Machine

Rhysida targets diverse industries with a focus on education and manufacturing. However, schools with similar network setups and limited security are frequent victims.

The consistent security posture across schools makes intrusion tactics more effective. Geographically, victims span major regions, with the following countries topping the list:-

- The USA
- France
- Germany
- England

Find us On Google News

Latest News

PoC Published for VMWare vCenter Server RCE Vulnerability CVE-2024-38812
**Guru Baran** - October 28, 2024

- Italy

While attacks are widespread, a notable concentration in Europe is observed, especially in the top five countries.

*Attack timeline (Source – Fortinet)*

The FortiGuard MDR team flagged a 'Sensitive Information Access' event, revealing an attempt to dump lsass.exe memory (T1003.001). The attacker used taskmgr.exe, but FortiEDR prevented the attempt.

*FortiEDR blocked taskmgr.exe access to system credentials (Source – Fortinet)*

FortiEDR identified 'svchost.exe' linked to a remote connection from IP 10.x.x.10, likely hosting a Remote Registry service. An attempt to access the SAM database was blocked.

A third event involved the legitimate tool 'ProcDump' trying to dump LSASS memory, blocked by FortiEDR. Despite no FortiEDR on the IP device, the indicators point

Canadian Cyber Centre Warns Of Chinese Hackers Scanning IT Systems
October 29, 2024

INE Launches Initiative to Optimize Year-End Training Budgets with Enhanced Cybersecurity and Networking Programs
October 28, 2024

Wi-Fi Test Suite Command Injection Vulnerability Found in Arcadyan Routers
October 26, 2024

Realtek SD Card Reader Driver Flaws Impact Dell, Lenovo, And Other Laptops
October 28, 2024

to a SAM dumping attempt via remote registry (T1003.002).

After detecting the incident, the FortiGuard IR team was fully investigated while the MDR team continued monitoring. The IR team found an RDP connection to HOST_A from 10.x.x.231 using a legitimate admin account from the SonicWall VPN range.

Experts found no brute force or known vulnerability evidence, suggesting prior access with compromised credentials.

The first compromised RDP session to HOST_A occurred in early July 2023 (Day 1), where the threat actor accessed Active Directory.

On Day 3, after an RDP session, the threat actor copied the Active Directory database on server HOST_A. Then, they downloaded and ran Advanced Port Scanner to scan the network internally, creating a registry entry with a scanned IP range.

Here below, we have mentioned the IPs:-

- 207.38.72.0/24
- 10.10.0.0/16
- 10.30.0.0/16
- 10.143.0.0/16
- 192.168.0.0/16

The threat actor, unaware of FortiEDR blocking, tried various tools and techniques for credential access. Their use of hash analysis on the endpoint instead of copying dumps gave detection chances.

After failed attempts, they created another RDP session to HOST_FILESERVER1, continuing internal discovery with port scanning.

Attempts to execute PowerShell scripts via PowerShell ISE were blocked, but the actor switched to PsExec.exe for a different approach on HOST_DC2, HOST_DC4, HOST_E, and HOST_FILESERVER1.

Six hours later, the threat actor used RDP to authenticate to HOST_DC4, creating 'DataGrabber1.exe' for data extraction; after that, AnyDesk and WinSCP for file transfer were downloaded and executed on HOST_F. PuTTY connected to ESXi servers to deploy Linux ransomware '67'.

The threat actor then deployed a Windows variant of Rhysida ransomware ('fury.exe') on HOST_FILESERVER1, encrypting user files across multiple systems and displaying Rhysida ransom notes.

*Ransom note (Source – Fortinet)*

## IOCs

*IOCs (Source – Fortinet)*

TAGS cyber security

**Tushar Subhra Dutta**

Tushar is a Cyber security content editor with a passion for creating captivating and informative content. With years of experience under his belt in Cyber Security, he is covering Cyber Security News, technology and other news.