

INDUSFACE™


Live Webinar

Detect and Protect : Strategies for Malware-Free Websites and APIs

📅

Thurs 7<sup>th</sup> November 2024 | 3:00 PM to 4:00 PM (IST) | 11:30 AM to 12:30 PM (CET)

Register Now



indusface.com



FORRESTER TEI STUDY

426% ROI DELIVERED BY CYNET

Presented

The Total Economic Impact™ Of Cynet All in One Security

Cost Savings And Business Benefits Enabled By Cynet All in One Security

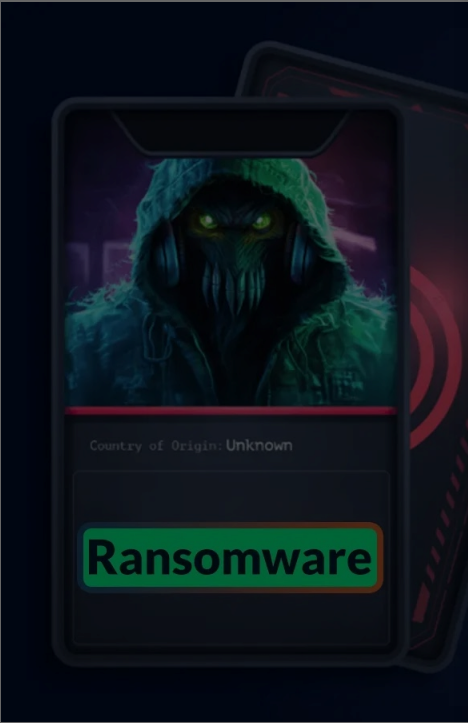
FREE

DOWNLOAD

computer Security   Cyber Security News

# Rhysida Ransomware Attacking Windows Machine Through VPN Devices and RDP

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



Rhysida, a new ransomware, has been identified by researchers. The group, who created their ransomware, offered a ransom of \$100,000. They have already attacked 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.

Welcome


This site asks for consent to use your data



Personalised advertising and content, advertising and content measurement, audience research and services development



Store and/or access information on a device



Learn more

Your personal data will be processed and information from your device (cookies, unique identifiers, and other device data) may be stored by, accessed by and shared with **134 TCF vendor(s) and 63 ad partner(s)**, or used specifically by this site or app.

Some vendors may process your personal data on the basis of legitimate interest, which you can object to by managing your options below. Look for a link at the bottom of this page to manage or withdraw consent in privacy and cookie settings.

Manage options

Consent

Find us On Google News

Page 1 of 5

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
- 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 first identified the attack, revealing an attempt to download taskmgr.exe, but FortiEDR blocked the download.

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

Latest News



Operation Magnus Disrupted Redline and Meta Infostealer Malware

Dhivya - October 28, 2024

NVIDIA GPU Vulnerabilities Allow Attackers To Execute Remote Code on Windows & Linux

October 28, 2024

IBM Flexible Service Processor Vulnerability Lets Attackers Gain Service Privileges

October 30, 2024

Hackers Exploiting SharePoint RCE Vulnerability to Compromise Entire Domain

November 1, 2024

Top 10 Best Server Monitoring Tools in 2025

October 26, 2024

Welcome

This site asks for consent to use your data



Personalised advertising and content, advertising and content measurement, audience research and services development



Store and/or access information on a device

Your personal data will be processed and information from your device (cookies, unique identifiers, and other device data) may be stored by, accessed by and shared with [134 TCF vendor\(s\)](#) and [63 ad partner\(s\)](#), or used specifically by this site or app.

Some vendors may process your personal data on the basis of legitimate interest, which you can object to by managing your options below. Look for a link at the bottom of this page to manage or withdraw consent in privacy and cookie settings.



Free Webinar

Live API Attack Simulation Webinar

In the upcoming webinar, Karthik Krishnamoorthy, CTO and Vivek Gopalan, VP of Products at Indusface demonstrate how APIs could be hacked. The session will

cover: an exploit of OWASP API Top 10 vulnerability, a brute force account take-over (ATO) attack on API, a DDoS attack on an API, how a WAAP could bolster security over an API gateway

Register for Free



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 used a legitimate admin account.

On Day 3, after an RDP session to HOST\_A, the threat actor used a Port Scanner to scan the new scanned IP range.

Here below, we have mentioned the IP ranges scanned:

- 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'.

Welcome

This site asks for consent to use your data



Personalised advertising and content, advertising and content measurement, audience research and services development



Store and/or access information on a device

Your personal data will be processed and information from your device (cookies, unique identifiers, and other device data) may be stored by, accessed by and shared with [134 TCF vendor\(s\)](#) and [63 ad partner\(s\)](#), or used specifically by this site or app.

Some vendors may process your personal data on the basis of legitimate interest, which you can object to by managing your options below. Look for a link at the bottom of this page to manage or withdraw consent in privacy and cookie settings.



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)

Experience how StorageGuard eliminates the security blind spots in your storage systems by trying a **14-day free trial**.

TAGS

cyber security

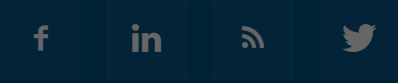


Tushar Subhra Dutta

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.


Cyber Security News

Cyber Security News Is a Dedicated News Channel For Hackers And Security Professionals. Get Latest Hacker News & Cyber Security Newsletters update Daily.




Welcome

This site asks for consent to use your data



Personalised advertising and content, advertising and content measurement, audience research and services development



Store and/or access information on a device

Your personal data will be processed and information from your device (cookies, unique identifiers, and other device data) may be stored by, accessed by and shared with [134 TCF vendor\(s\)](#) and [63 ad partner\(s\)](#), or used specifically by this site or app.

Some vendors may process your personal data on the basis of legitimate interest, which you can object to by managing your options below. Look for a link at the bottom of this page to manage or withdraw consent in privacy and cookie settings.