

## Resumen ejecutivo

Rhysida es un **grupo de tipo ransomware** que, desde 2023, ha demostrado gran capacidad para ejecutar intrusiones con **motivación económica** a través de la doble extorsión. Para ello se apoya en un portal en la red TOR donde lleva a cabo los procesos de negociación y presión operacional sobre la víctima.

Su patrón de ataque incrementa el riesgo para organizaciones públicas y privadas porque combina **acceso inicial por phishing o abuso de credenciales válidas**, con una fase de post-explotación enfocada a dominar el entorno corporativo. En términos de impacto, el riesgo no se limita solo al cifrado de información sensible ya que la fuga de datos eleva la **probabilidad de daño reputacional y sanciones regulatorias**, así como costes de respuesta y recuperación de sistemas. Por tanto, este malware debe considerarse un **riesgo alto** para organizaciones con accesos remotos expuestos, gestión de credenciales débiles, segmentación insuficiente y ausencia de copias de seguridad. Especialmente en sectores como gobierno, educación, sanidad, industrias manufactureras y tecnológicas.

Por todo ello, las medidas clave para mitigar Rhysida serían reforzar el acceso inicial a través de la formación y concienciación; el uso obligatorio de dobles factores de autenticación en servicios de acceso perimetrales (VPN/RDP); limitar la propagación a través de la segmentación de red y políticas de mínimo privilegio; y asegurar los datos a través de backups inmutables y pruebas periódicas de restauración. Además, existe una **herramienta pública de descifrado**, basada en una vulnerabilidad identificada en su implementación, pero su uso está **condicionado por la variante del ransomware y el entorno afectado** (principalmente Windows). Por lo que no debe considerarse una solución, sino una medida de apoyo dentro de la respuesta a incidentes, validando previamente su aplicabilidad en cada caso.

## Grupo de ransomware: Rhysida

Rhysida es un grupo cibercriminal de **motivación principalmente económica**, observada públicamente al menos desde marzo de 2023. Su modelo de fraude se basa en la **doble extorsión**, en la cual además de cifrar sistemas y datos para forzar el pago, el actor exfiltra información sensible y amenaza con publicarla si la víctima no paga. Para ello mantiene un portal en TOR que centraliza la interacción con las víctimas y la publicación de datos.

Un rasgo distintivo de este actor es que se presenta en ocasiones como un supuesto “equipo de ciberseguridad” que “ayuda” a evidenciar debilidades, cuando en realidad su objetivo es la extorsión y el beneficio económico.

Además, su **operativa es de tipo Ransomware-as-a-Service (RaaS)**, un modelo en el que el malware y la infraestructura se facilita a afiliados para ejecutar intrusiones y monetizar rescates.

## Países y sectores afectados

Rhysida no se limita a un ámbito geográfico concreto, sino que **actúa de forma global** con una afectación especialmente visible en Europa y Norteamérica. Entre los países con una mayor actividad asociada destacan Estados Unidos, Reino Unido, Italia, Francia y Alemania.





En cuanto a sectores, Rhysida muestra una victimología amplia, pero con mayor impacto en **educación, sanidad, administración pública, manufactura y tecnologías de la información**. Este patrón es coherente con operaciones de doble extorsión que buscan maximizar la presión y probabilidad de pago en entornos con alta criticidad operativa y datos sensibles.

## Análisis técnico

El ciclo de intrusión asociado a Rhysida suele comenzar con acceso inicial mediante phishing o uso de cuentas válidas comprometidas de servicios VPN o RDP. Una vez obtenida la primera sesión, los operadores tienden a establecer control operativo con frameworks de post-explotación (Cobalt Strike) y a habilitar capacidades de administración remota para su persistencia y despliegue. Tras el acceso, la actividad se orienta a descubrimiento y expansión a través de movimientos laterales mediante servicios remotos y elevación de privilegios. Además, Rhysida lleva a cabo la evasión de defensas, finalizando servicios de seguridad, eliminando backups y realizando cambios en el Directorio Activo.

La fase de cifrado en Rhysida se realiza a través de un esquema híbrido típico de ransomwares modernos, donde utiliza un cifrado asimétrico RSA de 4096 bits para proteger la clave privada y un cifrado simétrico ChaCha20 para el contenido de los ficheros. Además, lleva a cabo el cifrado de ficheros aplicando listas de exclusión para evitar la inestabilidad del sistema.

### Características técnicas principales:

-  **Plataformas:** Rhysida opera contra entornos Windows, Linux y VMware ESXi.
-  **Acceso inicial:** phishing y abuso de credenciales válidas de servicios VPN y RDP
-  **Uso de frameworks post-explotación y herramientas lolbins:** Cobalt Strike, herramienta "DataGrabber.exe para exfiltración, PsExec, AnyDesk como acceso alternativo, WinRM en el marco de scripts, ...
-  **Evasión de defensas:** uso de scripts PowerShell (SILENTKILL) para desactivar sistemas antimalware y borrado de copias de seguridad.

## Técnicas MITRE ATT&CK

Táctica	Técnica más usada
<b>Resource Development</b>	T1587 – Develop Capabilities
<b>Initial Access</b>	T1078 – Valid Accounts T1566 – Phishing
<b>Execution</b>	T1059 – Command and Scripting Interpreter
<b>Persistence</b>	T1547.001 – Boot or Logon Autostart Execution: Registry Run Keys/Startup Folder
<b>Privilege Escalation</b>	T1055.002 – Process Injection: Portable Executable Injection
<b>Defense Evasion</b>	T1070 – Indicator Removal T1564.003 – Hide Artifacts: Hidden Window
<b>Credential Access</b>	T1003.003 – OS Credential Dumping: NTDS T1112 – Modify Registry
<b>Discovery</b>	T1016 – System Network Configuration Discovery T1018 – Remote System Discovery T1033 – System Owner/User Discovery T1069 – Permission Groups Discovery T1087.002 – Account Discovery: Domain Account T1482 – Domain Trust Discovery
<b>Lateral Movement</b>	T1021 – Remote Services
<b>Collection</b>	T1005 – Data from Local System T1119 – Automated Collection
<b>Command and Control</b>	T1219 – Remote Access Software
<b>Exfiltration</b>	T1041 – Exfiltration Over C2 Channel
<b>Impact</b>	T1486 – Data Encrypted for Impact T1657 – Financial Theft

## Medidas de mitigación

### Proactivas

- ❑ Formación continua en concienciación, especialmente en detección de correos y adjuntos sospechosos. (T1566 - Phishing)
- ❑ Implementar autenticación multifactor (MFA) para evitar accesos no autorizados. (T1078 - Valid Accounts)
- ❑ Segmentar la red para limitar el descubrimiento. (T1482 – Domain Trust Discovery)
- ❑ Mantener copias de seguridad seguras y probar restauraciones periódicas. (T1486 – Data Encrypted for Impact)
- ❑ Limitar cuentas con privilegios y mantener sistemas actualizados. (T1069 – Permission Groups Discovery, T1070 – Indicator Removal)
- ❑ Auditar y limitar usuarios RDP, incluso deshabilitar el servicio si no es imprescindible. (T1021 – Remote Services)
- ❑ Monitorizar y proteger claves de inicio automático. (T1547.001 – Registry Run Keys / Startup Folder)

### Reactivas

- ❑ Monitorizar tráfico saliente y bloquear conexiones SMTP/FTP/HTTP no autorizadas usados para exfiltración. (T1041 - Exfiltration Over C2 Channel)
- ❑ Utilizar un antivirus para poner en cuarentena automáticamente archivos sospechosos, desactivar PowerShell cuando no sea necesario o usar el modo "Constrained Language" para restringir el acceso. (T1059 - Command and Scripting Interpreter)

## Conclusiones y recomendaciones

Rhysida debe considerarse una **amenaza global y de alto impacto** para organizaciones de múltiples sectores, en especial sectores como educación, sanidad, administración pública, manufactura y TI. Su ciclo de intrusión combina acceso inicial por phishing o uso de credenciales comprometidas, expansión rápida mediante herramientas comunes y una fase de preparación orientada a debilitar la recuperación y desactivar defensas. Esta combinación eleva el **riesgo de indisponibilidad de servicios críticos, compromiso amplio de organizaciones y pérdida de continuidad operativa**.

En consecuencia, las medidas prioritarias para reducir el riesgo deben centrarse en el uso de dobles factores de autenticación en accesos remotos y cuentas privilegiadas; la segmentación de la red y el uso de políticas de mínimos privilegios para limitar los movimientos laterales; la monitorización continua de patrones anómalos en servicios remotos y ejecución de scripts; y una gestión adecuada y eficiente de las copias de seguridad offline. Además, existe una **herramienta pública de descifrado**, pero su uso está condicionado por la variante del ransomware y el entorno afectado, principalmente Windows.

