

## Resumen ejecutivo

Desde su aparición a principios de 2024, el grupo **RansomHub** se ha consolidado como una de las amenazas de ransomware más activas y con mayor capacidad de expansión dentro del modelo **ransomware como servicio (RaaS)**.

RansomHub ha logrado posicionarse rápidamente gracias a un **ecosistema de afiliados muy activo**, al que ofrece condiciones especialmente rentables. Este modelo ha permitido al grupo realizar intrusiones simultáneas en distintos países y sectores, acumulando víctimas en industrias como tecnología, sanidad, manufactura o servicios financieros, y consolidándose como un grupo altamente oportunista y orientado al beneficio económico.

Técnicamente opera con cargas dañinas adaptadas a entornos **Windows, Linux y ESXi**, lo que le permite atacar infraestructuras híbridas. Su acceso inicial suele lograrse mediante **credenciales comprometidas, servicios VPN vulnerables o phishing**. Una vez dentro, emplea herramientas legítimas y técnicas de **“living off the land”** para moverse lateralmente, evadir defensas y preparar la exfiltración y el cifrado.

El grupo ejecuta una estrategia de **dobles extorsión**, publicando los datos robados en su portal si la víctima no paga. RansomHub representa un **riesgo muy alto** para organizaciones y administraciones públicas debido a su elevada capacidad operativa, su profesionalización y su rápida expansión. Por todo ello, se recomienda reforzar los **controles de acceso remoto, la monitorización de actividad sospechosa y la segmentación de red**, además de apoyarse en **capacidades de ciberinteligencia para anticipar sus campañas**.

## Grupo de ransomware: RansomHub

RansomHub es un grupo de ransomware operado bajo el **modelo RaaS**, activo desde principios de 2024. Su rápida expansión se atribuye a un programa muy rentable para afiliados y a la posible incorporación de actores procedentes de otros grupos disueltos, lo que ha reforzado sus capacidades técnicas desde el inicio.

A principios de 2025, la infraestructura de RansomHub fue absorbida por el **grupo DragonForce**, y el grupo se considera actualmente inactivo como marca, aunque sus afiliados y herramientas siguen representando un **riesgo relevante**.

## Países y sectores afectados

RansomHub ha atacado a organizaciones de múltiples regiones, con especial afectación en Estados Unidos, Reino Unido, Europa y Australia, incluyendo varias empresas españolas en 2025.

En España, los ataques se han concentrado principalmente en los sectores tecnológico, sanitario, alimentación y manufactura, así como en servicios profesionales.

A nivel global, sus víctimas pertenecen principalmente a los sectores **tecnológico, construcción, financiero, sanitario y manufactura**.






Además, la mayoría de las víctimas de RansomHub son **pequeñas empresas**, lo que refleja un enfoque oportunista y orientado a objetivos con menor capacidad de defensa.

## Análisis técnico

Desde una perspectiva técnico-operativa, RansomHub se caracteriza por utilizar múltiples vectores de ataque iniciales, como el uso de vulnerabilidades conocidas, técnicas de ingeniería social y malware complementario para establecer acceso inicial y persistencia.

En la fase de ejecución y movimiento lateral, RansomHub combina herramientas administrativas legítimas con utilidades de red y frameworks ofensivos para desplegar payloads, ejecutar scripts remotos y pivotar entre sistemas. Además, el grupo utiliza payloads compatibles con Windows, Linux y ESXi, permitiéndole atacar entornos corporativos híbridos y virtualizados con alta eficacia.

### Características técnicas principales:

-  **Carga útil** escrita en **Golang**, optimizada para portabilidad entre sistemas Windows y Linux.
-  Esquema de cifrado híbrido que combina **AES-256 para el cifrado de archivos** y **RSA-2048 para la protección de claves**.
-  Acceso inicial mediante **phishing** dirigido, **explotación de vulnerabilidades** en VPNs (como Fortinet, SonicWall) y **abuso de credenciales comprometidas**.
-  **Movimientos laterales y exfiltración** usando **herramientas legítimas** (LOLBAS), como AnyDesk, WinSCP, y RClone. También se ha detectado uso de PowerShell y WMI para persistencia y ejecución remota
-  Evasión de EDR y tampering mediante **desactivación de servicios**, **manipulación de logs** y uso de **binarios ofuscados**. Algunas variantes implementan técnicas anti-debugging y anti-sandbox

## Técnicas MITRE ATT&CK

Táctica	Técnica más usada
<b>Resource Development</b>	<b>T1588.005</b> – Obtain Capabilities: Exploits
<b>Initial Access</b>	<b>T1566</b> – Phishing <b>T1190</b> – Exploit Public-Facing Application
<b>Execution</b>	<b>T1059</b> – Command and Scripting Interpreter <b>T1047</b> – Windows Management Instrumentation
<b>Persistence</b>	<b>T1136</b> – Create Account <b>T1098</b> – Account Manipulation
<b>Defense Evasion</b>	<b>T1070</b> – Indicator Removal on Host <b>T1222</b> – File and Directory Permissions Modification <b>T1036</b> – Masquerading <b>T1562</b> – Impair Defenses: Disable or Modify Tools
<b>Credential Access</b>	<b>T1003</b> – OS Credential Dumping
<b>Discovery</b>	<b>T1082</b> – System Information Discovery <b>T1018</b> – Remote System Discovery <b>T1057</b> – Process Discovery <b>T1083</b> – File and Directory Discovery <b>T1046</b> – Network Service Discovery
<b>Lateral Movement</b>	<b>T1021.001</b> – Remote Services: Remote Desktop Protocol
<b>Command and Control</b>	<b>T1219</b> – Remote Access Software
<b>Exfiltration</b>	<b>T1048</b> – Exfiltration Over Alternative Protocol
<b>Impact</b>	<b>T1486</b> – Data Encrypted for Impact <b>T1489</b> – Service Stop <b>T1490</b> – Inhibit System Recovery

## Medidas de mitigación

### Proactivas

- ❑ Proteger y centralizar logs, impidiendo su borrado y monitorizando cambios en permisos de archivos/directorios. (T1070 - Indicator Removal, T1222 - Permissions Modification)
- ❑ Segmentar la red y limitar visibilidad entre hosts, reduciendo el descubrimiento de procesos, sistemas y directorios. (T1057 - Process Discovery, T1018 - Remote System Discovery, T1083 - File/Directory Discovery, T1082 - System Information Discovery)
- ❑ Implementar backups offline/inmutables y proteger servicios críticos, con alertas ante paradas sospechosas o intentos de inhibir la recuperación. (T1486 – Data Encrypted for Impact, T1489 - Service Stop, T1490 - Inhibit System Recovery)
- ❑ Auditar y limitar usuarios RDP, deshabilitar el servicio si no es necesario, usar gateways y MFA. (T1021.001 - Remote Services: Remote Desktop Protocol)

### Reactivas

- ❑ Usar sandbox y microsegmentación, bloquear drivers vulnerables y aplicar protección contra exploits; mantener software actualizado y usar inteligencia de amenazas. (T1203 - Exploitation for Client Execution)
- ❑ Utilizar un antivirus para poner en cuarentena automáticamente archivos sospechosos y desactivar PowerShell cuando no sea necesario. (T1059 - Command and Scripting Interpreter: PowerShell, T1047 – WMI)

## Conclusiones y recomendaciones

RansomHub se ha consolidado como uno de los grupos de ransomware con mayor crecimiento y actividad en 2024-2025, destacando por su modelo RaaS altamente rentable para afiliados y por su capacidad para comprometer organizaciones de distintos tamaños, especialmente pequeñas y medianas empresas. Su flexibilidad técnica, con cargas capaces de operar en Windows, Linux y ESXi, y su enfoque oportunista en la explotación de accesos remotos y credenciales comprometidas lo sitúan como una amenaza especialmente relevante en el panorama actual.

La actividad creciente de RansomHub, unida a la profesionalización del ecosistema RaaS, eleva de forma notable el riesgo para organizaciones de todos los tamaños, especialmente aquellas con accesos remotos expuestos o una gestión débil de credenciales. En este contexto, resulta esencial reforzar la defensa en profundidad, mejorar la detección temprana de actividad sospechosa y asegurar planes sólidos de respuesta y recuperación. Además, el apoyo en capacidades de ciberinteligencia permite anticipar campañas y reducir de forma significativa el impacto potencial de futuros ataques.

