Informe de Ransomware

ThreatLabz 2025



©2025 Zscaler, Inc. Todos los derechos reservados.

Índice



Resumen ejecutivo 3

Hallazgos clave 4

Panorama del ransomware: principales tendencias y objetivos 6

- Los ataques de ransomware alcanzan nuevos máximos 6
- La tendencia de exfiltración de datos aumenta un 92.7 % 7
- Puntos críticos globales y regionales 11
- Grupos de ransomware más activos en 2024–2025 14
- Nuevos grupos de ransomware 15
- Principales vulnerabilidades explotadas en campañas de ransomware 16

Resumen sobre ransomware: lo que llega a los titulares 17

- Black Basta utiliza ChatGPT para actividades delictivas 17
- ¿Hola? Ransomware: el manual de estrategias de ataque en múltiples etapas 18
- LockBit con filtraciones: mecanismos de RaaS expuestos en una brecha en la Dark Web 20
- La sanidad bajo asedio: la era del robo masivo de datos 22
- Cambiando la tendencia del ransomware: desde el frente 23

Las principales 5 familias de ransomware a vigilar en 2025–2026 24

- Nº 1 Dark Angels 24
- Nº2 Clop/ClOp 25
- Nº 3 DragonForce 26
- Nº 4 Akira 26
- Nº 5 Interlock 27

Archivo Notas de ransomware de ThreatLabz 28

Predicciones para 2026 29

Cómo Zscaler detiene el ransomware con Zero Trust + AI 31

Lista de comprobación de prevención de ransomware 33

Metodología de investigación 35

- Acerca de Zscaler 35
- Acerca de ThreatLabZ 35

©2025 Zscaler, Inc. Todos los derechos reservados.

Resumen ejecutivo

El ransomware ha sido una constante en el panorama de amenazas desde hace mucho tiempo, pero su forma de operar cambia constantemente. Las campañas actuales son más específicas, automatizadas y eficientes, impulsadas en parte por el uso creciente de IA generativa que mejora y acelera todo, desde los señuelos de phishing hasta el desarrollo de malware. Esta evolución se ha traducido en un aumento significativo de la actividad y el impacto del ransomware.

Entre abril de 2024 y abril de 2025, la nube de Zscaler bloqueó más intentos de ransomware que en cualquier año anterior (más de 10.8 millones de accesos), lo que marca un aumento interanual del 145.9 % y el mayor volumen registrado desde que comenzó el seguimiento. Al mismo tiempo, el número de organizaciones incluidas en sitios de filtración de ransomware aumentó un 70.1 %, lo que pone de relieve un cambio más amplio hacia ataques basados en la extorsión. Las campañas actuales son de alta frecuencia y alto impacto, diseñadas para extraer el máximo efecto, a menudo sin necesidad de cifrado. Un número cada vez mayor de operadores de ransomware están abandonando por completo el cifrado en favor de la extorsión pura de datos, una evolución reflejada en un aumento del 92.7 % en los volúmenes de exfiltración de datos durante el año pasado.

Incluso frente a iniciativas de eliminación de alto perfil como Operation Endgame, los grupos de ransomware no muestran signos de desaceleración. En todo caso, es posible que la disrupción esté impulsando una reinvención. Durante el período de análisis de este informe surgieron treinta y cuatro nuevas familias de ransomware. Mientras tanto, grupos establecidos como DragonForce, Akira y Clop se colocaron en la cima de las tablas de actividad, lo que demuestra la resistencia de las operaciones de ransomware maduras.

El informe sobre ransomware ThreatLabz 2025 de Zscaler analiza en profundidad estos desarrollos y hallazgos, cubriendo los principales sectores y regiones atacados, familias de ransomware a tener en cuenta, metodologías de ataque en evolución y orientación práctica para los defensores. Más allá del seguimiento de amenazas, conozca cómo ThreatLabz desempeña un papel activo en la protección de empresas de todo el mundo, desde la creación de herramientas personalizadas para la recuperación de ataques de ransomware hasta la contribución a los esfuerzos globales que exponen e interrumpen los ecosistemas de malware y ransomware a gran escala.

©2025 Zscaler, Inc. Todos los derechos reservados.

Hallazgos clave

Los intentos de ransomware bloqueados por la nube Zscaler aumentaron un 145.9 % año tras año (abril de 2024–abril de 2025), lo que marca el aumento más significativo que hemos visto en tres años.

Los volúmenes de exfiltración de datos de 10 familias principales de ransomware aumentaron un 92.7 % año tras año hasta alcanzar los 238.5 terabytes (TB) robados, lo que indica un cambio más amplio hacia el robo de datos como principal táctica de extorsión.

Los casos de extorsión pública aumentaron un 70.1 % según el análisis de sitios con filtraciones de datos, lo que demuestra que la amenaza de daño a la reputación o consecuencias regulatorias suele ser más convincente que el cifrado por sí solo.

Las industrias manufactureras, tecnológicas y de asistencia sanitaria fueron las más atacadas y el sector de petróleo y gas experimentó un aumento del 935.3 % en ataques.

©2025 Zscaler, Inc. Todos los derechos reservados.

Estados Unidos sigue siendo el primer objetivo global, que experimenta el 50.8 % de los ataques totales, seguido de Canadá, el Reino Unido, Alemania y la India.

La IA generativa se está convirtiendo en un multiplicador de fuerza para los actores de amenazas de ransomware, ayudándoles a crear rápidamente señuelos de phishing, escribir código malicioso, automatizar la extracción de datos y más.

RansomHub (833), Akira (520) y Clop (488) surgieron como las familias de ransomware más activas, colectivamente responsables de la mayor parte de los ataques.

El vishing (phishing basado en voz) se integra cada vez más en los ataques de ransomware a medida que las estafas de voz se vuelven más convincentes y más efectivas para obtener acceso inicial.

ThreatLabz identificó 34 familias de ransomware recientemente activasdurante el período de análisis, lo que eleva el número total rastreado a 425 desde que comenzó nuestra investigación.

A pesar de la creciente actividad de ransomware, los esfuerzos coordinados de aplicación de la ley, respaldados por expertos de la industria como Zscaler ThreatLabz, han logrado avances significativos en la interrupción de la principal infraestructura de ransomware, como lo demuestra la Operación Endgame.

©2025 Zscaler, Inc. Todos los derechos reservados.

Panorama del ransomware: principales tendencias y objetivos

Si bien las infracciones que aparecen en los titulares ilustran la escala global del ransomware, la información más valiosa surge del análisis de los patrones de segmentación y los comportamientos operativos que utilizan los actores de amenazas en sus campañas.

Esta sección va más allá de los titulares para examinar dónde el ransomware está teniendo el impacto más significativo (por sector y región), identificar qué familias de ransomware están liderando la carga y poner de manifiesto el surgimiento de nuevos grupos durante el año pasado.

Los ataques de ransomware alcanzan nuevos máximos

El crecimiento constante de la actividad de ransomware ya no sorprende, pero los últimos datos muestran un aumento drástico en el volumen de ataques: los intentos de ataques de ransomware en la nube de Zscaler aumentaron un 145.9 % interanual y se han sextuplicado desde 2021. Este aumento refleja más que simplemente un mayor volumen; señala un cambio hacia campañas más rápidas y deliberadas dirigidas a entornos de alto impacto.

Para los equipos de seguridad, las tácticas de ransomware pueden resultar familiares en su mayor parte, pero la creciente omnipresencia, precisión y eficiencia operativa de las campañas recientes apuntan a una evolución, impulsada en parte por la IA generativa, que acelera el desarrollo del ransomware en un modelo de negocio cibercriminal más sofisticado y escalable.

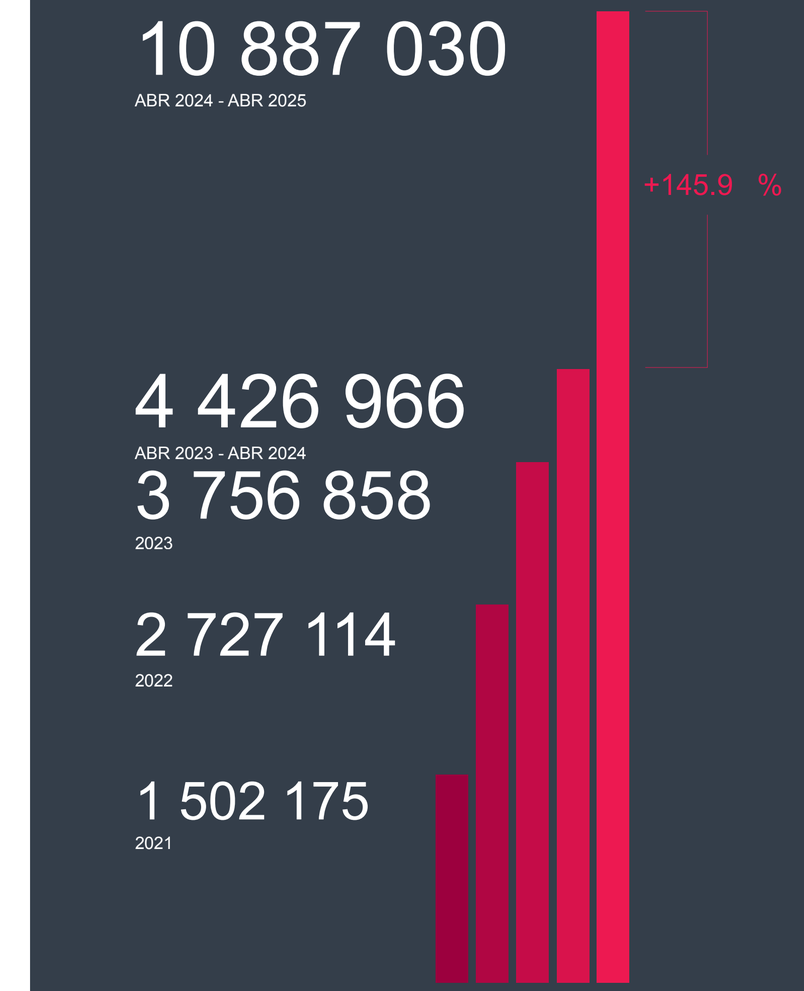


Figura 1: Ataques de ransomware bloqueados por Zscaler anualmente



©2025 Zscaler, Inc. Todos los derechos reservados.



La tendencia de exfiltración de datos aumenta un 92.7 %

Durante el último año, los grupos de ransomware han convertido el robo de datos de un acto secundario en el evento principal. Cada vez es más frecuente que el cifrado por sí solo (si es que existe) no sea la solución final. Los actores de amenazas están exfiltrando cantidades masivas de datos para aumentar la presión y aumentar los riesgos para las víctimas.

Un reciente aumento en la exfiltración de datos refleja esta tendencia. El análisis de ThreatLabz revela que el volumen total de datos robados aumentó año tras año en 10 grupos principales de ransomware. El volumen total de datos exfiltrados por estos grupos aumentó 92.7%, de 123.8 TB (abril de 2023–marzo de 2024) a 238.5 TB (abril de 2024–marzo de 2025). Esto excluye una única vulneración en el período 2023–2024 que involucró 100 TB de datos exfiltrados (la mayor exfiltración observada en todo el conjunto de datos), lo que sesga considerablemente el total anual. La eliminación de ese valor atípico proporcionó una visión más precisa de las tendencias más amplias en la actividad de robo de datos.

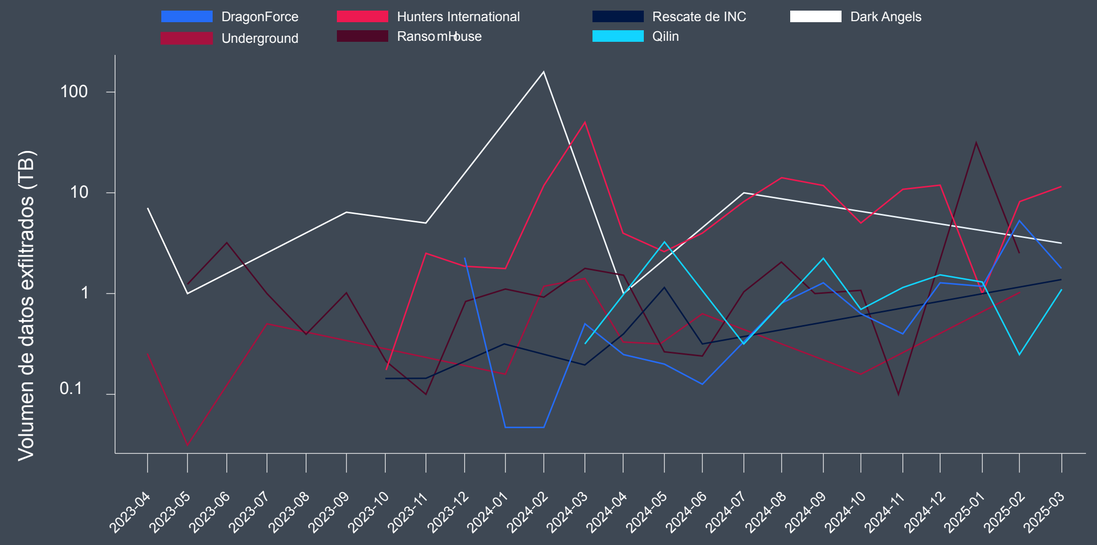


Figura 2: Exfiltración de datos por parte de grupos clave de ransomware

- **Hunters International** aumentó significativamente el total de datos robados año tras año, un 224,3%, de 37,7 TB a 122,1 TB. La pérdida media de datos por víctima también aumentó de aproximadamente 300 GB a 359 GB año tras año, un incremento del 19,6% por víctima. La siguiente sección (“Pasando a la extorsión de datos únicamente”) explora cómo el grupo decidió alejarse por completo del cifrado de archivos.
- **DragonForce** logró el mayor salto porcentual en el volumen total de exfiltración, con un aumento del 382,6 %, de 4,2 TB a 20,3 TB. Aunque la mediana se mantuvo mayormente estable con un ligero descenso, el aumento del volumen general sugiere que el grupo ha estado comprometiendo a más víctimas.
- **Los Ángeles Oscuros** tuvieron el mayor impacto medio por víctima: un aumento del 132,6 %, de 2,15 TB a 5 TB. Esto coincide con el enfoque continuo del grupo en objetivos grandes y de alto valor a pesar de haber registrado menos incidentes en general.
- **RansomHub** exfiltró un 86,2 % más de datos año tras año, con un total de 22,4 TB desde abril de 2024 hasta marzo de 2025. La pérdida media de datos por víctima del grupo aumentó más del doble, pasando de 50 GB a 118 GB.
- **RansomHouse** aumentó su volumen total robado en un 83,1% año tras año, de 17,2 TB a 31,6 TB. La pérdida media de datos por víctima también aumentó de 425 GB a 500 GB.

©2025 Zscaler, Inc. Todos los derechos reservados.

Pasando únicamente a la extorsión de datos

El informe sobre ransomware Zscaler ThreatLabz 2024 examinó cómo el grupo de ransomware Hive cambió su nombre a Hunters International en octubre de 2023, tras una operación dirigida por el FBI que se confiscó la infraestructura del grupo a principios de ese año. Desde la aparición de Hunters International, el grupo ha sido muy activo y se ha centrado principalmente en el robo de datos con fines de cifrado. De hecho, desde la creación del grupo, han robado casi 160 TB de datos. Cada víctima de Hunters International perdió un promedio de 698 GB y la pérdida media de datos fue de 317 GB. La figura 3 muestra los volúmenes de datos robados por mes desde la formación del grupo.

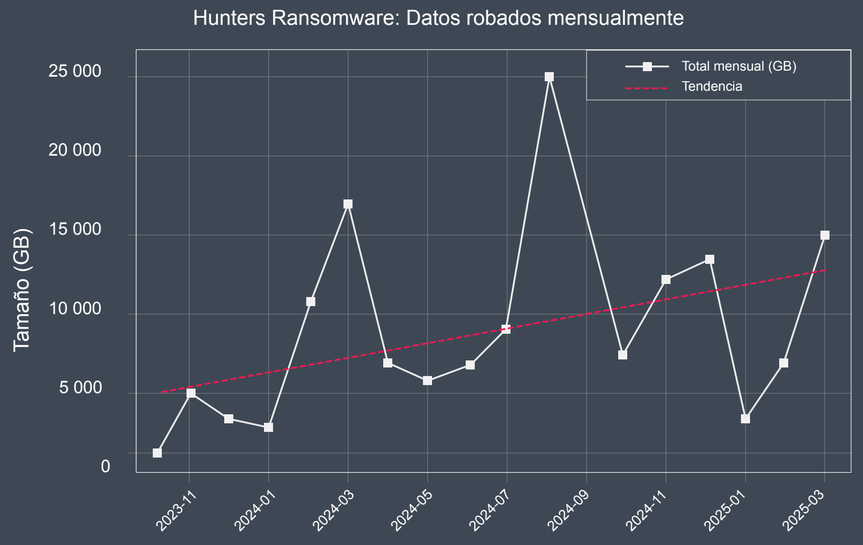


Figura 3: GB de datos robados al mes por Hunters International

En mayo de 2025, surgió un nuevo grupo bajo la marca World Leaks, que lanzaba ataques sin utilizar ransomware y optaba por centrarse exclusivamente en la extorsión de datos. El sitio World Leaks es visual y programáticamente similar a Hunters International (ver figura 4), lo que indica que es probable que el mismo grupo esté detrás de ambos.

Desde que World Leaks comenzó sus ataques en mayo de 2025, el grupo ha robado más de 25 TB de datos. Las estadísticas de robo de datos son muy similares a las de Hunters International: cada víctima perdió de media 769 GB, con una pérdida mediana de 452 GB.

Por cierto, el 3 de julio de 2025, Hunters International anunció su cierre a través de un mensaje en su sitio de filtraciones, afirmando que el grupo estaba cerrando operaciones y proporcionando herramientas de descifrado gratuitas (ver figura 5).

Este cambio del cifrado de archivos al robo de datos no es algo sin precedentes. Otros grupos como BianLian y Clop también han dejado de lado el ransomware para centrarse en la extorsión de datos, una tendencia que exploramos con más detalle más adelante en este informe.

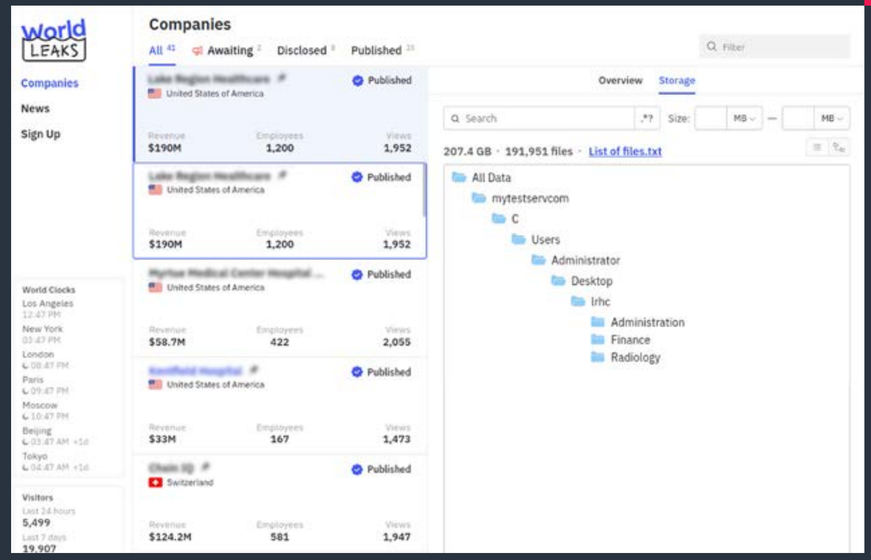


Figura 4: Sitio web del grupo de ransomware World Leaks

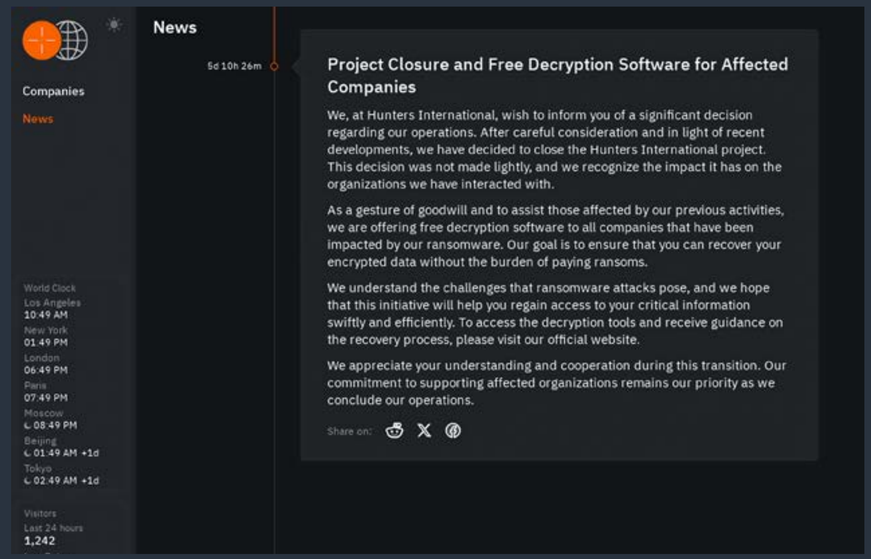


Figura 5: Aviso de cierre de Hunters International

©2025 Zscaler, Inc. Todos los derechos reservados.

Sectores que hacen frente a más ataques

Los atacantes siguieron priorizando las industrias en las que la presión para pagar es mayor, ya sea por el potencial de interrupción operativa, la sensibilidad de los datos robados y el potencial relacionado de daño a la reputación o la exposición regulatoria.

La figura 6 muestra la cantidad de incidentes de ransomware por industria según los datos del sitio de filtración, y ofrece una instantánea de los ataques confirmados en los que los actores de amenazas exfiltraron datos y aplicaron presión de extorsión. Los sectores manufacturero, tecnológico y de atención sanitaria siguieron siendo los más atacados y representan entornos de alto riesgo propicios para la extorsión y el apalancamiento.

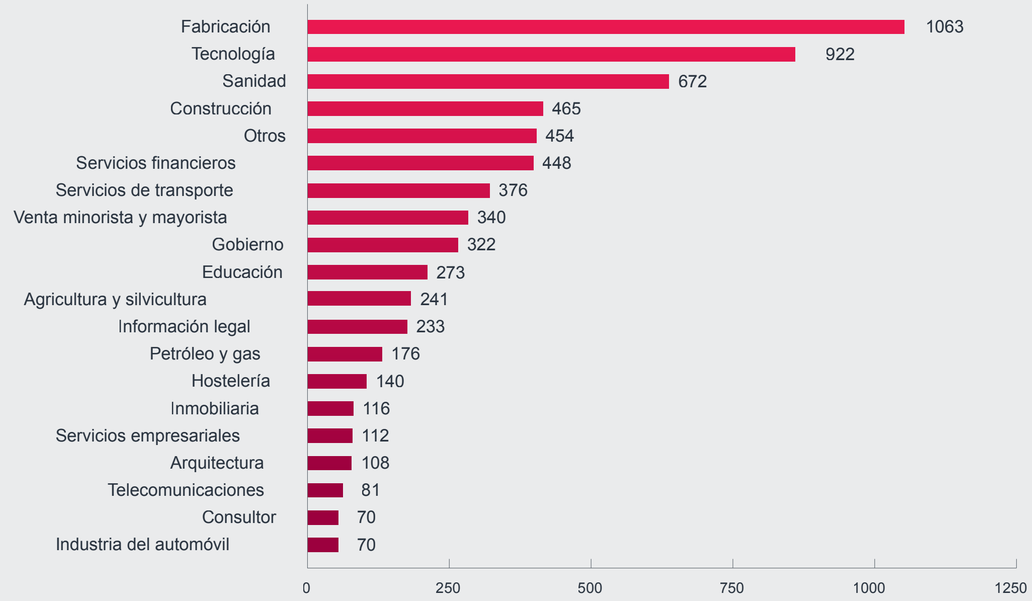


Figura 6: Ataques de ransomware por sector según sitios de filtración de datos (los 20 sectores principales)



©2025 Zscaler, Inc. Todos los derechos reservados.

Tendencias interanuales

La figura 7 muestra los cambios porcentuales interanuales en los ataques de ransomware por sector.

Los ataques de ransomware en el sector de petróleo y gas se han disparado más de un 900 % interanual, probablemente impulsados por una combinación de mayor automatización, desde las plataformas de perforación hasta los oleoductos, que amplía la superficie de ataque y prácticas de seguridad obsoletas. En 2025, la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) advirtió[1] que incluso los actores de amenazas "poco sofisticados" están explotando vulnerabilidades en los sistemas de control industrial (ICS) y la tecnología SCADA, que son esenciales para las operaciones de petróleo y gas.

El sector agrícola también vio cómo los ataques de ransomware se disparaban un 677.4%. Las operaciones agrícolas se están volviendo cada vez más digitalizadas (pensemos en tractores inteligentes y sensores habilitados para IoT), pero las defensas de seguridad no han seguido el mismo ritmo. Aun así, hay señales de progreso y reconocimiento de que los sistemas agrícolas ahora son los principales objetivos del ransomware: John Deere, un importante fabricante de maquinaria agrícola, organizó un hackathon 2025 donde los estudiantes trabajaron para exponer vulnerabilidades en sus tractores inteligentes.[2]

La atención médica sigue siendo uno de los ataques más frecuentes y constantes, con un aumento constante del 115,4 % año tras año. Según The HIPAA Journal,[3] investigadores de la Universidad Estatal de Michigan, la Universidad de Yale y la Universidad Johns Hopkins descubrieron que el ransomware es ahora una de las principales causas de violaciones de datos de atención médica. Este riesgo se volvió dolorosamente real para varias importantes organizaciones de atención médica afectadas por ataques de ransomware atribuidos a la banda de ransomware Interlock (en nuestra **lista de vigilancia de familias de ransomware**). Obtenga más información en la sección **"La atención médica bajo asedio: la era del robo masivo de datos".**

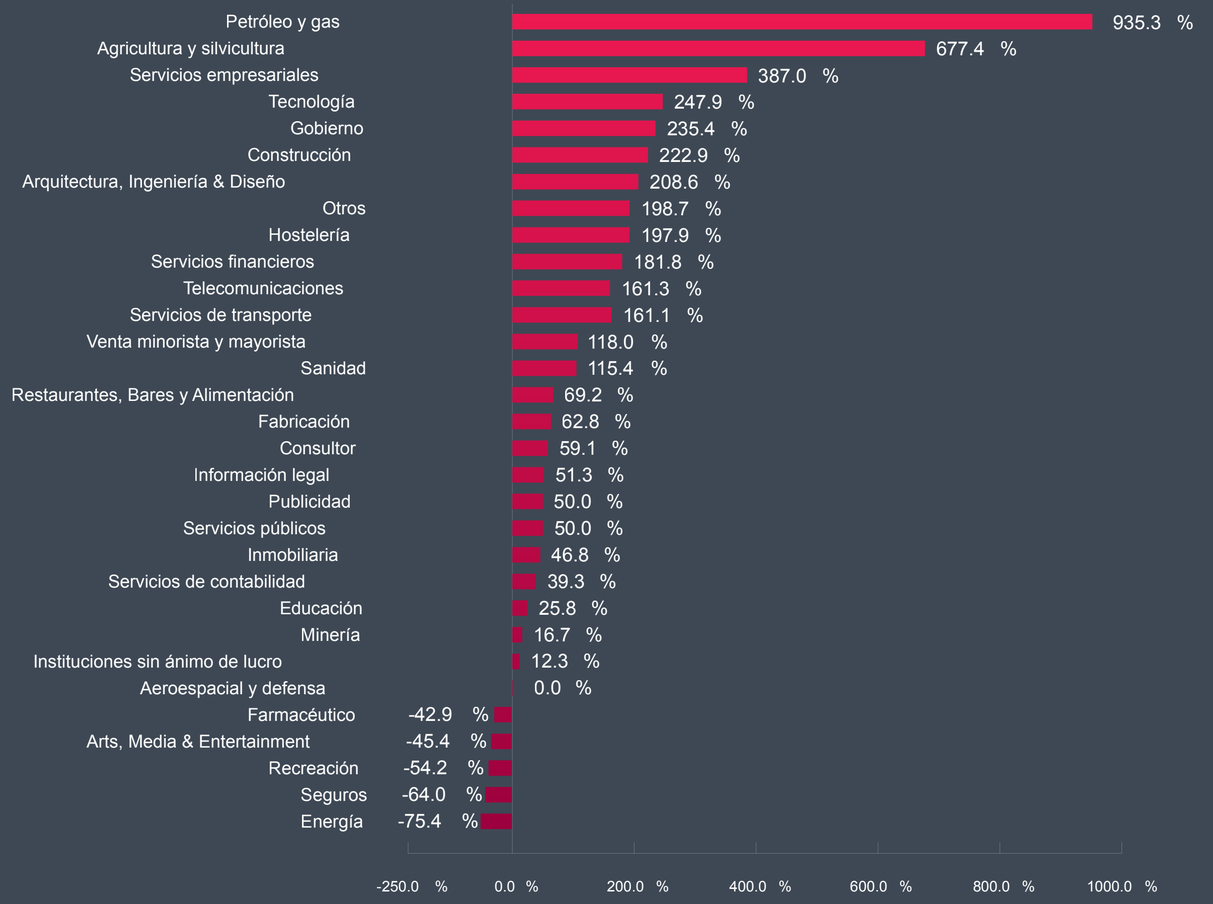


Figura 7: Cambio porcentual interanual en los ataques de extorsión mediante ransomware por sector (se excluyeron sectores con menos de 10 ataques notificados en el conjunto de datos del año pasado para evitar exagerar el crecimiento debido a una línea de base baja)

[1] CISA, **Actores cibernéticos poco sofisticados que atacan la tecnología operativa**, 6 de mayo de 2025.
[2] Axios, **John Deere invita a los estudiantes a hackear tractores**, 24 de junio de 2025.
[3] El **estudio de HIPAA Journal, explora el alcance de los ataques de piratería y ransomware en la atención médica**, 16 de mayo de 2025.

©2025 Zscaler, Inc. Todos los derechos reservados.

Puntos críticos globales y regionales

Los datos del sitio de filtración revelan una clara concentración geográfica, con una proporción dominante de ataques dirigidos a organizaciones en los Estados Unidos (50.8 %), muy por delante de países como Canadá (5.2 %) y el Reino Unido (4.6 %). Esto refleja cómo los ciberdelincuentes continúan priorizando las economías de alto valor y concentradas digitalmente. La Figura 8 desglosa los 15 países más atacados por proporción de ataques de ransomware registrados en sitios de filtración de datos.

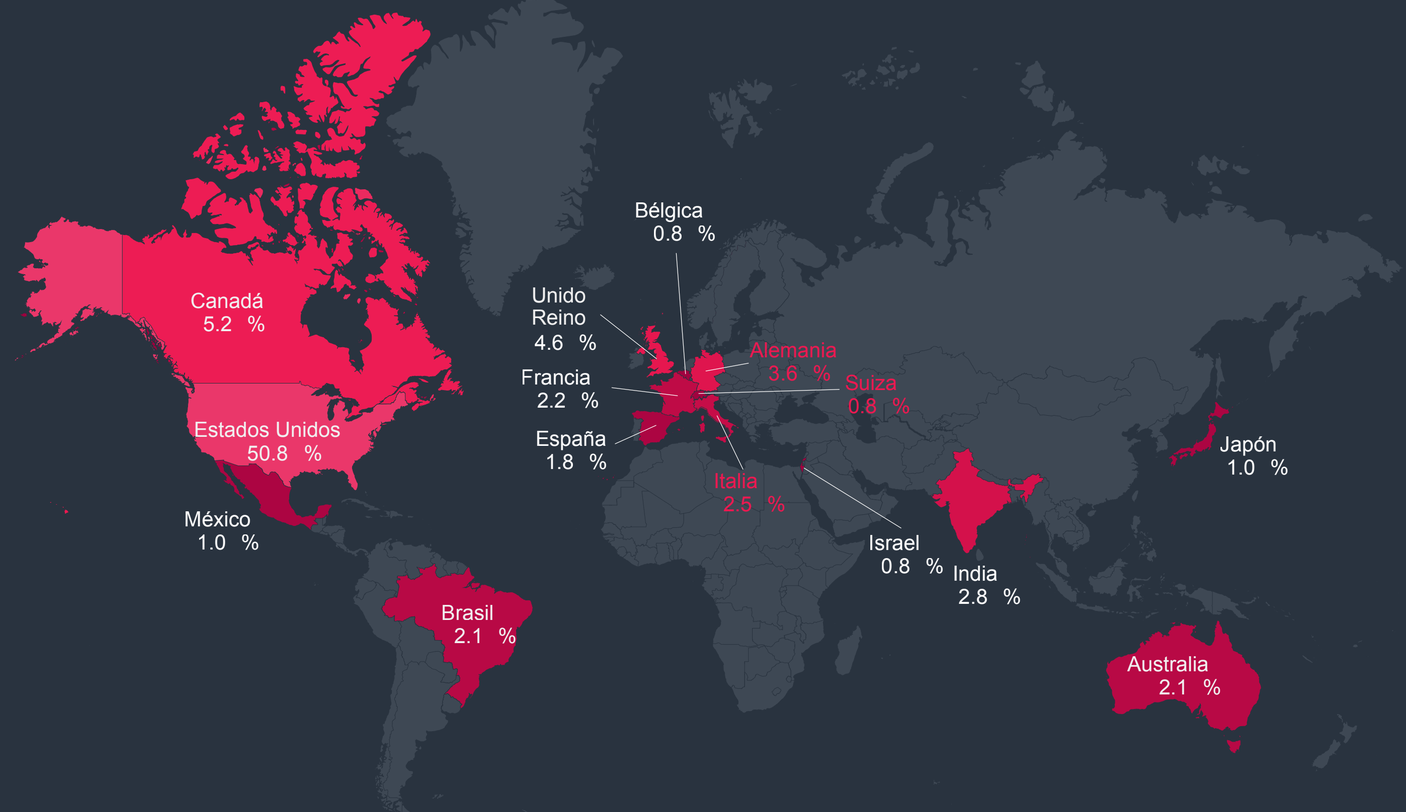


Figura 8: Los 15 países con mayor proporción de ataques de ransomware

©2025 Zscaler, Inc. Todos los derechos reservados.

Tendencias interanuales

El impacto del ransomware varía ampliamente de una región a otra. Comprender dónde se están acelerando los ataques ayuda a predecir dónde es probable que los actores de amenazas ataquen a continuación y respalda estrategias de defensa con mayor información regional.

TOP 15 MUNDIAL: PICOS MASIVOS EN EE. UU.

Los ataques de ransomware aumentaron en todo el mundo, y los 15 países principales por número de ataques de ransomware experimentaron aumentos porcentuales de dos y tres dígitos (ver figura 9). Los ataques en Estados Unidos aumentaron más del doble hasta alcanzar los 3671, superando el total combinado de los 15 países más atacados restantes. El aumento del 194,5% en Canadá refuerza la forma en que los actores de amenazas se están expandiendo por América del Norte, con un enfoque creciente en los sectores vulnerables. La Evaluación Nacional de Amenazas Cibernéticas 2025–2026 del Centro Canadiense para la Seguridad Cibernética nombra al ransomware como la principal amenaza cibernética para la infraestructura crítica del país, citando la escalada de ataques a organizaciones del sector sanitario, industrial y público[4]

País	Ataques de ransomware (informe de 2024)	Ataques de ransomware (informe de 2025)	Cambio porcentual
Estados Unidos	1821	3671	101.6 %
Canadá	128	377	194.5 %
Reino Unido	216	333	54,2 %
Alemania	149	260	74.5 %
India	60	199	231.7 %
Italia	118	181	53.4 %
Francia	119	159	33.6 %
Australia	73	152	108.2 %
Brasil	57	149	161.4 %
España	62	134	116.1 %
Japón	42	75	78.6 %
Méjico	57	74	29.8 %
Suiza	43	60	39,5 %
Bélgica	34	59	73.5 %
Israel	11	59	436.4 %

Figura 9: Comparación interanual de ataques de ransomware por país



[4] Centro Canadiense de Seguridad Cibernética, Evaluación Nacional de Amenazas Cibernéticas 2025–2026, consultado el 14 de julio de 2025.

©2025 Zscaler, Inc. Todos los derechos reservados.

EMEA: INTENSIFICACIÓN DE LOS ATAQUES EN EUROPA Y MÁS ALLÁ

La región de Europa, Medio Oriente y África (EMEA) experimentó aumentos generalizados en la actividad de ransomware, como se muestra en la figura 10. Los picos interanuales notables incluyeron economías importantes como España (+116.1 %) y Alemania (+74.5 %) así como mercados más pequeños como Bélgica (+73.5 %). Israel experimentó un aumento del 436.4 %, un marcado incremento relativo que, si bien parte de una línea de base más pequeña de ataques, probablemente refleja crecientes tensiones geopolíticas y un aumento de las operaciones de ransomware vinculadas a estados.

País	Ataques de ransomware (informe de 2024)	Ataques de ransomware (informe de 2025)	Cambio porcentual
Reino Unido	216	333	54,2 %
Alemania	149	260	74.5 %
Italia	118	181	53.4 %
Francia	119	159	33.6 %
España	62	134	116.1 %
Suiza	43	60	39,5 %
Bélgica	34	59	73.5 %
Israel	11	59	436.4 %
Emiratos Arabes Unidos	21	52	147.6 %
Países Bajos	50	52	4 %

Figura 10: Comparativa interanual de ataques de ransomware por país en la región de EMEA

APAC: CRECIMIENTO EXPLOSIVO EN MERCADOS EMERGENTES Y ESTABLECIDOS

La región Asia–Pacífico (APAC) registró algunos de los mayores aumentos interanuales a nivel mundial. Como muestra la figura 11, los actores de ransomware ampliaron su presencia en una región caracterizada por una rápida transformación digital y niveles inconsistentes de madurez cibernética. El impacto se sintió en toda la región APAC, abarcando centros regionales de tecnología y logística como Singapur. (+237.5 %) y Taiwán (+147.1 %) a economías de gran escala como China (+186.7 %) y la India (+231.7 %).

País	Ataques de ransomware (informe de 2024)	Ataques de ransomware (informe de 2025)	Cambio porcentual
India	60	199	231.7 %
Australia	73	153	109.6 %
Japón	42	75	78.6 %
Singapur	16	54	237.5 %
Indonesia	23	43	86.9 %
China	15	43	186.7 %
Taiwán	17	42	147.1 %
Tailandia	25	32	28 %
Malasia	20	27	35 %
Hong Kong	7	23	228.6 %

Figura 11: Comparativa interanual de ataques de ransomware por país en la región de APAC

©2025 Zscaler, Inc. Todos los derechos reservados.

Grupos de ransomware más activos en 2024-2025

Varios grupos altamente activos continuaron dominando el ecosistema de ransomware, con RansomHub a la cabeza, al reclamar el mayor número de víctimas identificadas públicamente: 833. Esto posicionó al grupo como la operación de ransomware más prolífica según la actividad reportada durante el último año. Curiosamente, el grupo decidió cesar sus operaciones y desapareció en abril de 2025.

Akira y Clop han ascendido en el ranking de ataques de ransomware desde el año pasado. Akira, asociada con 520 víctimas, ha ampliado constantemente su alcance a través de numerosos afiliados y corredores de acceso inicial. Clop, conocido por centrarse en los ataques a la cadena de suministro, le sigue de cerca con 488 víctimas, lo que destaca su estrategia de focalizar las aplicaciones de software de terceros que muchas empresas utilizan para maximizar el impacto.

La figura 12 muestra los grupos de ransomware con más víctimas durante el último año.

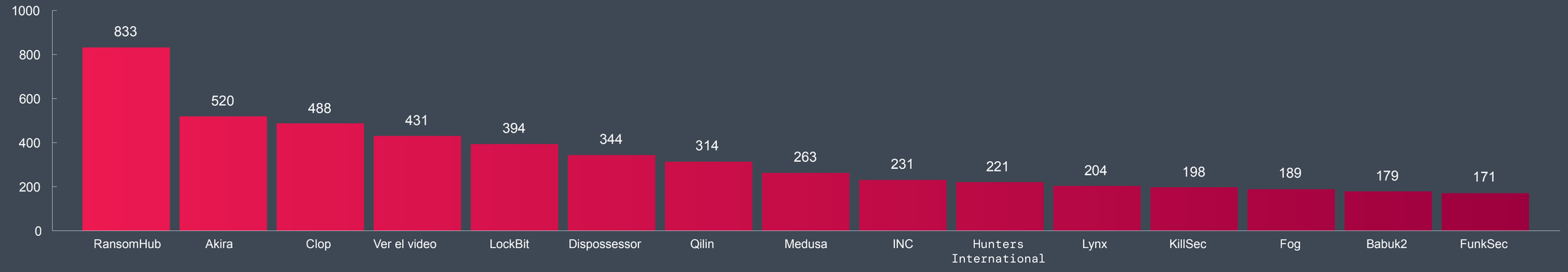


Figura 12: Ataques de ransomware reportados en sitios web con fugas de datos

©2025 Zscaler, Inc. Todos los derechos reservados.

Nuevos grupos de ransomware

El panorama del ransomware cambia constantemente: algunos grupos tradicionales desaparecen y surgen otros nuevos. Esto puede ser un cambio de marca estratégico para eludir sanciones o un esfuerzo de un nuevo grupo para llenar un vacío dejado por otros. De todos modos, los afiliados de grupos de ransomware desaparecidos cambian periódicamente de operaciones y emplean sus metodologías de ataque establecidas. La línea de tiempo en la figura 13 muestra los grupos de ransomware que se activaron y comenzaron a publicar datos sobre sitios de fugas entre abril de 2024 y abril de 2025.

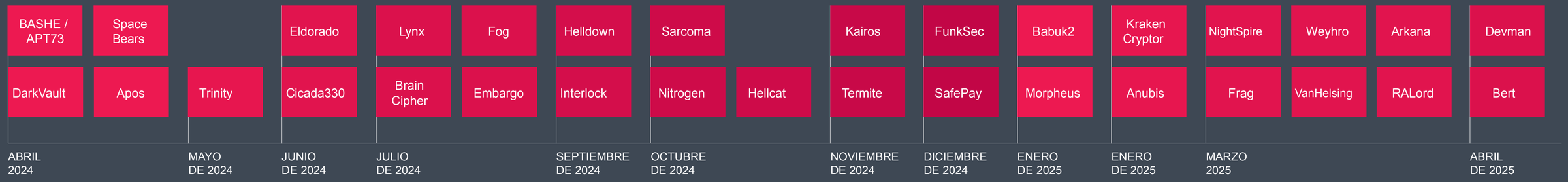


Figura 13: Nuevos grupos de ransomware con sitios de fuga de datos



©2025 Zscaler, Inc. Todos los derechos reservados.

Principales vulnerabilidades explotadas en campañas de ransomware

Los grupos de ransomware aprovechan cada vez más las vulnerabilidades de las tecnologías empresariales críticas para ejecutar ataques impactantes. La explotación de estas vulnerabilidades proporciona a los atacantes vías directas para moverse lateralmente, robar información confidencial y propagar ransomware en entornos de red. Casi todas estas vulnerabilidades son fáciles de explotar porque son aplicaciones que operan en Internet y que pueden descubrirse mediante técnicas básicas de escaneo. Los objetivos clave incluyen VPN, sistemas de respaldo, hipervisores, herramientas de acceso remoto y aplicaciones de transferencia de archivos: tecnologías que están omnipresentes en las organizaciones y son esenciales para las operaciones.

VPN

Las vulnerabilidades de las redes privadas virtuales (VPN) generalmente brindan a los atacantes acceso directo a la red interna de una organización, lo que permite a los actores de amenazas realizar reconocimientos, moverse lateralmente y comprometer sistemas críticos para robar datos y desplegar ransomware.

Algunos ejemplos de estas vulnerabilidades incluyen **CVE-2024-55591** (que afecta a los dispositivos VPN SSL de FortiProxy) y **CVE-2024-40766** (que afecta a los dispositivos VPN SSL de SonicWall).

Soluciones de respaldo

Las tecnologías de respaldo y replicación se han convertido en vectores de ataque fundamentales para los operadores de ransomware. Las vulnerabilidades en estos sistemas permiten el acceso directo para robar información y deshabilitar soluciones de respaldo antes del cifrado de archivos.

Un ejemplo de vulnerabilidad que ha sido explotada por actores de amenazas de ransomware es **CVE-2023-27532** (Replicación y copia de seguridad de Veeam).

Los hipervisores de software de virtualización

como VMware ESXi concentran las cargas de trabajo, lo que los convierte en objetivos de ransomware de alto valor. Los exploits contra ESXi pueden comprometer entornos virtualizados completos.

Por ejemplo, la vulnerabilidad **CVE-2024-37085** permite a los atacantes manipular el grupo de administradores de ESX para obtener el control de un servidor. En los últimos años, los grupos de ransomware también han desarrollado cada vez más compilaciones de ransomware personalizadas exclusivamente para cifrar archivos en entornos ESXi.

Herramientas de acceso remoto

Las herramientas de monitoreo y administración remota (RMM) son fundamentales en los entornos de TI corporativos para administrar puntos finales e infraestructura. Sin embargo, también son objetivos comunes de los grupos de ransomware, especialmente cuando el software subyacente es vulnerable.

Ejemplos de estas vulnerabilidades son **CVE-2024-57726**, **CVE-2024-57727** y **CVE-2024-57728** (SimpleHelp RMM), que han permitido a los actores de amenazas de ransomware obtener acceso a entornos corporativos.

Aplicaciones de transferencia de archivos

Las empresas utilizan aplicaciones de transferencia de archivos para compartir archivos de manera eficiente entre sistemas internos y entre socios externos, proveedores o clientes. Sin embargo, cuando se expone a Internet, cualquier vulnerabilidad presente en la aplicación subyacente puede ser explotada para acceder a los datos de la organización. Este grupo de aplicaciones ha sido el objetivo principal del grupo de ransomware Clop, del que hablaremos más adelante en el informe.

Solo durante el último año, el grupo aprovechó múltiples vulnerabilidades de día cero en aplicaciones de transferencia de archivos (**CVE-2024-50623** y **CVE-2024-55956**) para robar datos de cientos de organizaciones.

Reforzar los sistemas vulnerables

Para combatir las campañas de ransomware impulsadas por estas vulnerabilidades, los defensores deben adoptar un enfoque de seguridad en capas:

1. **Aplicación de revisiones como prioridad:** agilizar las reparaciones de los servicios de borde (firewalls, VPN y sistemas de respaldo).
2. **Segmentación y Zero Trust:** bloquee el movimiento lateral imponiendo la segmentación de usuarios y aplicaciones, la gestión de la postura del dispositivo, controles de acceso estrictos y la supervisión de cuentas privilegiadas.
3. **Protección avanzada contra amenazas con cobertura de día cero:** aproveche las tecnologías de aislamiento y sandbox en línea para evitar la explotación de día cero. Realice una inspección TLS para bloquear cargas maliciosas y aplique controles de prevención de pérdida de datos (DLP) para detener la exfiltración de datos.

Al cerrar proactivamente estas brechas de seguridad, los defensores pueden reducir la capacidad de los actores de ransomware de explotar vulnerabilidades y fortalecer significativamente su resiliencia organizativa.

©2025 Zscaler, Inc. Todos los derechos reservados.

Resumen sobre ransomware: lo que llega a los titulares

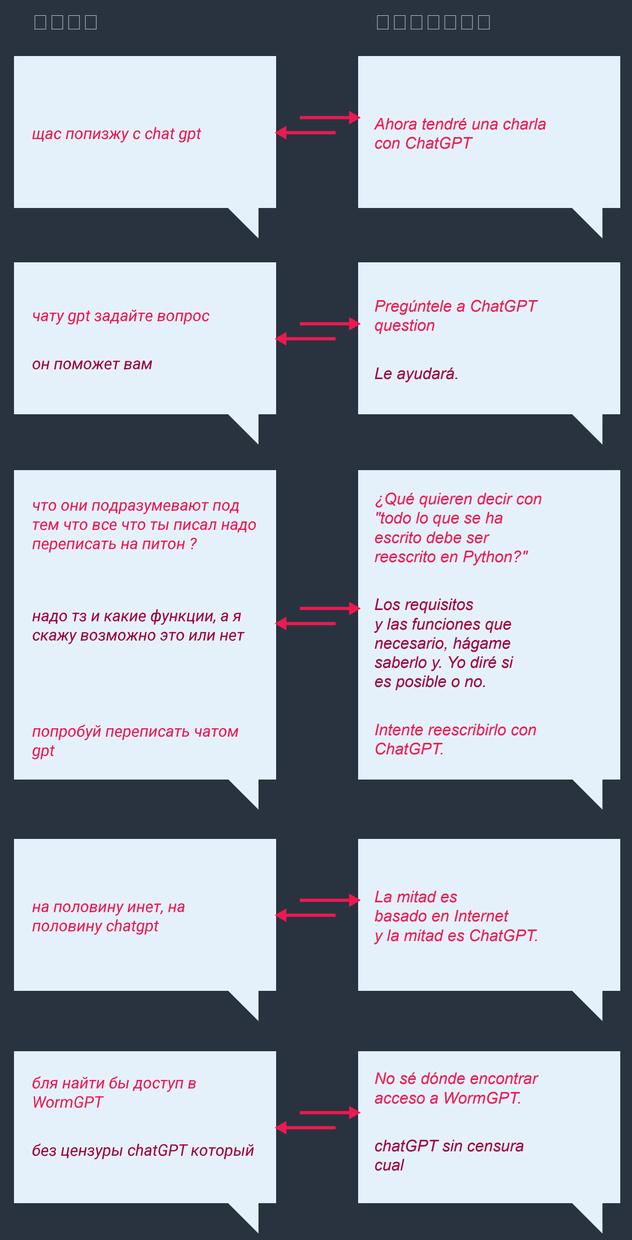
Black Basta utiliza ChatGPT para actividades delictivas

En febrero de 2025, un tesoro de mensajes del servidor de chat interno Matrix del grupo de ransomware **Black Basta** se filtró en línea, lo que permitió a los investigadores obtener una visión de primera mano de las operaciones del grupo. Estas charlas, que abarcan desde septiembre de 2023 hasta septiembre de 2024, arrojan luz sobre la estructura interna del grupo, las estrategias de ataque y los procesos. Lo más notable es que revelan cómo Black Basta utiliza ChatGPT, lo que no sorprende dada su gran popularidad. Según el **Informe de seguridad de IA de ThreatLabz 2025**, ChatGPT domina el panorama de la IA y representa aproximadamente el 45 % de todas las transacciones relacionadas con la IA.

Debido a la gran popularidad y saturación de ChatGPT en el panorama de la IA, ThreatLabz concentró su análisis en cómo Black Basta integra ChatGPT en sus operaciones rutinarias.

Nuestros hallazgos revelan que el grupo de ransomware emplea ChatGPT de varias maneras:

- **Reescritura de código:** los registros de chat mencionan explícitamente el uso de ChatGPT para reescribir scripts en Python.
- **Dependencia de la IA:** el grupo se refiere a confiar parcialmente en ChatGPT junto con los recursos de Internet, lo que sugiere su integración en su flujo de trabajo más amplio. Además, los registros de chat muestran que los miembros se animan entre sí a resolver problemas utilizando ChatGPT.
- **Interés en modelos de IA sin restricciones:** el debate sobre WormGPT refleja un interés en explorar herramientas de IA sin censura, que pueden ofrecer capacidades no limitadas por las reglas legales y éticas integradas en ChatGPT.



©2025 Zscaler, Inc. Todos los derechos reservados.

¿Hola? Ransomware: el manual de estrategias de ataque en múltiples etapas

Se ha producido un alejamiento de los intermediarios de acceso inicial que utilizan campañas de spam a gran escala como vector de infección inicial. En cambio, en los dos últimos años se han empleado con eficacia ataques más específicos utilizando la metodología ilustrada en la figura 14.

Los actores de amenazas detrás de estos ataques primero realizan un reconocimiento utilizando sitios como ZoomInfo para comprar información de contacto sobre los empleados de una empresa objetivo. Se puede obtener información adicional sobre los empleados a través de sitios como LinkedIn, lo que permite a los ciberdelincuentes identificar al personal para suplantar su identidad, especialmente los que trabajan en el departamento de TI de la empresa. Empleados específicos con acceso privilegiado (normalmente en RR.HH., nóminas y finanzas) son objetivos habituales de los ataques.

Una vez obtenida la información de contacto de la víctima, el ataque comienza con un bombardeo de spam para inundar la bandeja de entrada de la víctima. Posteriormente, el actor de la amenaza realiza una llamada telefónica a ese empleado (con la información obtenida previamente) y se hace pasar por otro empleado del departamento de TI de la empresa, un ejemplo clásico de vishing (phishing de voz). Las personas que efectúan la llamada son elegidos para que coincidan con el empleado de TI suplantado (hombre, mujer, hablante nativo). El actor de amenazas informa a la víctima que trabaja en el departamento de TI de la empresa y se comunica con la víctima para ayudarla a "actualizar su filtro de spam", y solicita acceso remoto a través de una herramienta RMM como Microsoft Teams, Quick Assist, Team Viewer, AnyDesk, etc. Si la víctima cae en la trampa, el ciberdelincuente realiza una serie de acciones para instalar una puerta trasera en el sistema de la víctima mientras proporciona suficiente credibilidad como para afirmar que los filtros de spam de la víctima se han "actualizado". La figura 15 muestra un sitio web real operado por un agente de acceso inicial de ransomware que utiliza esta táctica.



Figura 14: Metodología de ataque de ransomware de múltiples etapas

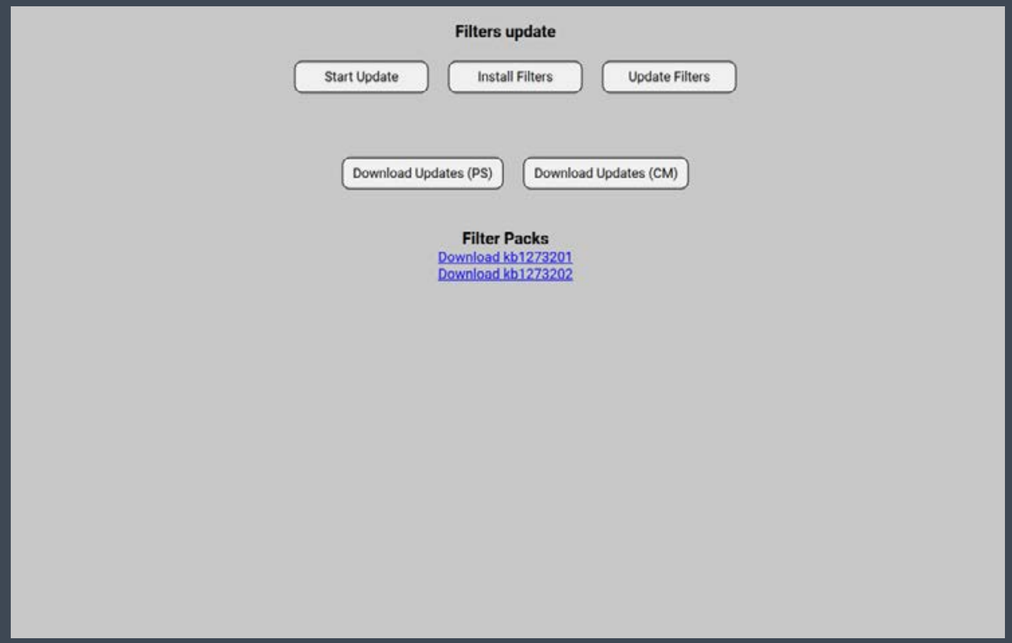


Figura 15: Sitio web falso de "Actualización de filtros" de un agente de acceso inicial de ransomware

©2025 Zscaler, Inc. Todos los derechos reservados.

Estos sitios web, a menudo alojados en Azure o Amazon Web Services, son engañosamente simples pero pueden emplear numerosas técnicas especialmente diseñadas para evadir entornos sandbox de antivirus y malware. Por ejemplo:

- Los enlaces de Filter Packs son en realidad un archivo ZIP de varias partes (dividido en dos partes, por ejemplo, kbxxxxxxx) cifrado con una frase de contraseña.

- Los botones Descargar actualizaciones copian comandos de PowerShell o de shell de Windows al portapapeles de la víctima, que luego se ejecutan. Estos comandos solicitan al actor de amenazas la contraseña del archivo ZIP. Además, los comandos establecen valores de registro con la información de comando y control de la carga útil del malware. Por lo tanto, el ejecutable de malware por sí solo no funcionará correctamente en un entorno sandbox con este paso de inicialización previo.

- Una vez descifrado y descomprimido el archivo ZIP, se utiliza un ejecutable legítimo (por ejemplo, Microsoft OneDrive) para descifrar e implementar una carga maliciosa a través de la carga lateral de DLL.

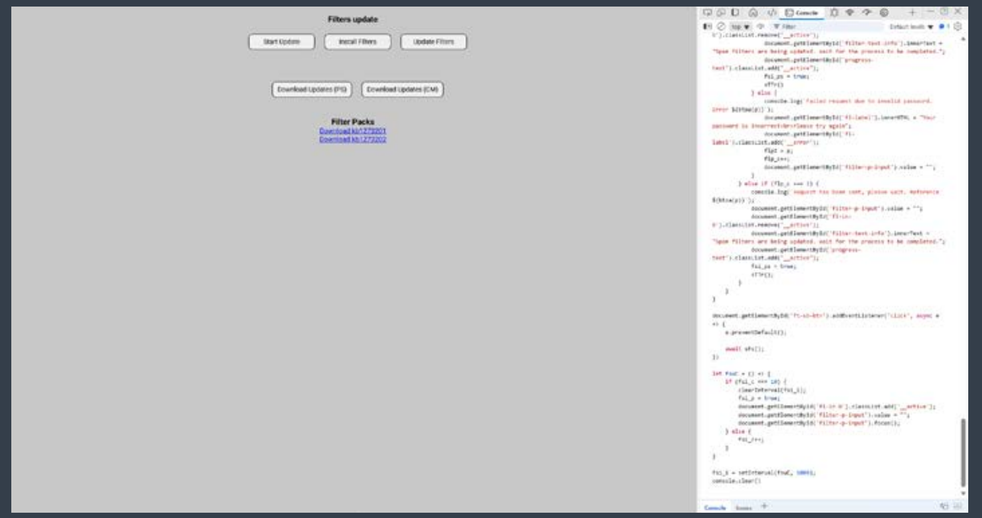


Figura 16: Acceso a la consola en el extremo de una víctima

Los tres botones superiores están diseñados para robar la contraseña de Microsoft 365 de la víctima. Al hacer clic, cada botón copia el contenido de JavaScript al portapapeles de la víctima. A continuación, el actor de amenazas abre las herramientas de desarrollo del navegador web para acceder a la consola como se muestra en la figura 16.

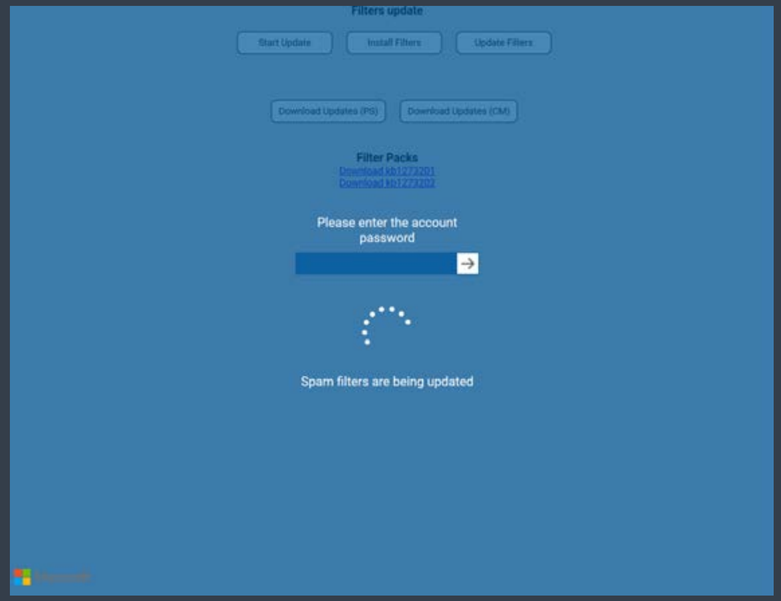


Figura 17: Un campo de entrada de contraseña maliciosa

Luego, el contenido de JavaScript del portapapeles se pega en la consola y se ejecuta, mostrando una superposición que solicita a la víctima que ingrese su contraseña, como en la figura 17.

Después de que se roba la contraseña de la cuenta de la víctima y se instala la puerta trasera del malware, el actor de amenazas intenta moverse lateralmente dentro de la organización para robar información e implementar ransomware.
Este nuevo estilo de ataques de ransomware dirigidos a menudo tiene éxito y un alto índice de víctimas caen en estas trampas.

©2025 Zscaler, Inc. Todos los derechos reservados.

LockBit con filtraciones: mecanismos de RaaS expuestos en una brecha en la Dark Web

En mayo de 2025, los paneles de afiliados y de administración de LockBit fueron desconfigurados con un enlace para descargar la base de datos del grupo (ver figura 18).

La base de datos MySQL filtrada proporciona a los investigadores, incluido ThreatLabz, una vista detallada de las operaciones internas de LockBit luego de una importante **operación policial internacional** conocida como Operación Cronos en febrero de 2024, que llevó a que el líder del grupo fuera acusado públicamente. Incluso después del desmontaje, LockBit **se recuperó en cuestión de días**, lanzando nuevos ataques con un nuevo sitio de filtración. La base de datos filtrada incluye las actividades del grupo en el momento del **lanzamiento de LockBit 4.0**, del 18 de diciembre de 2024 al 29 de abril de 2025. La información expone 75 nombres de afiliados, 4423 mensajes de chat de rescate y alrededor de 60 000 direcciones de billeteras bitcoin. De los 75 afiliados, 54 crearon compilaciones de ransomware LockBit para 246 víctimas en 156 organizaciones. A cada afiliado se le asignó un nivel de confianza específico, como se muestra en la figura 19.



Figura 18: Panel de administración de LockBit desfigurado

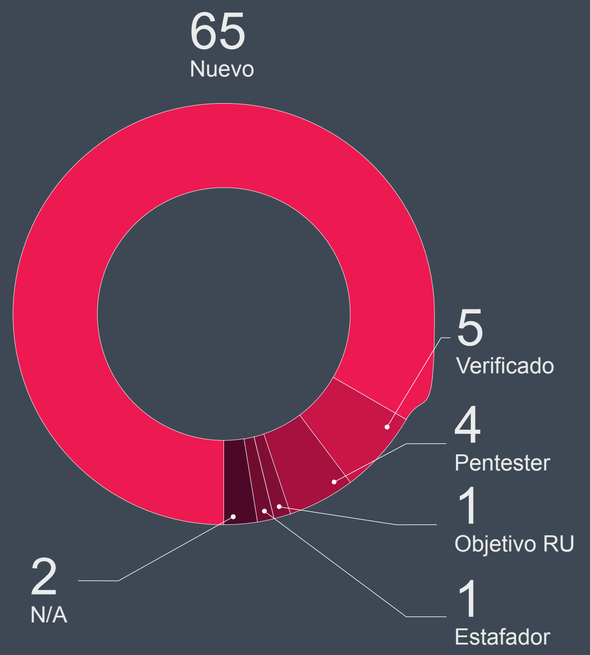


Figura 19: Número de afiliados de LockBit por "nivel de confianza"

Había 35 afiliados con estado de pausa, presumiblemente aquellos que estaban inactivos o suspendidos. Curiosamente, un afiliado que utilizaba el nombre de BaleyBeach pasó a utilizar LockBit después del cierre de su rival RansomHub (del que hablaremos más adelante). A continuación se muestra un mensaje de chat enviado por este afiliado a una víctima.

> "Éramos afiliados de RansomHub, ahora RansomHub ha cerrado, nos mudamos aquí. Así que las empresas existentes (incluida la suya) con las que tuvimos que tratar aún tienen la oportunidad [sic] de evitar la filtración de sus datos."

©2025 Zscaler, Inc. Todos los derechos reservados.

La Figura 20 muestra la cantidad de compilaciones de LockBit generadas por los afiliados con la mayor cantidad de compilaciones.

Ni los usuarios admin ni matrix777 tenían niveles de confianza asignados y estaban registrados con el mismo ID TOX, lo que indica que probablemente sean la misma persona.

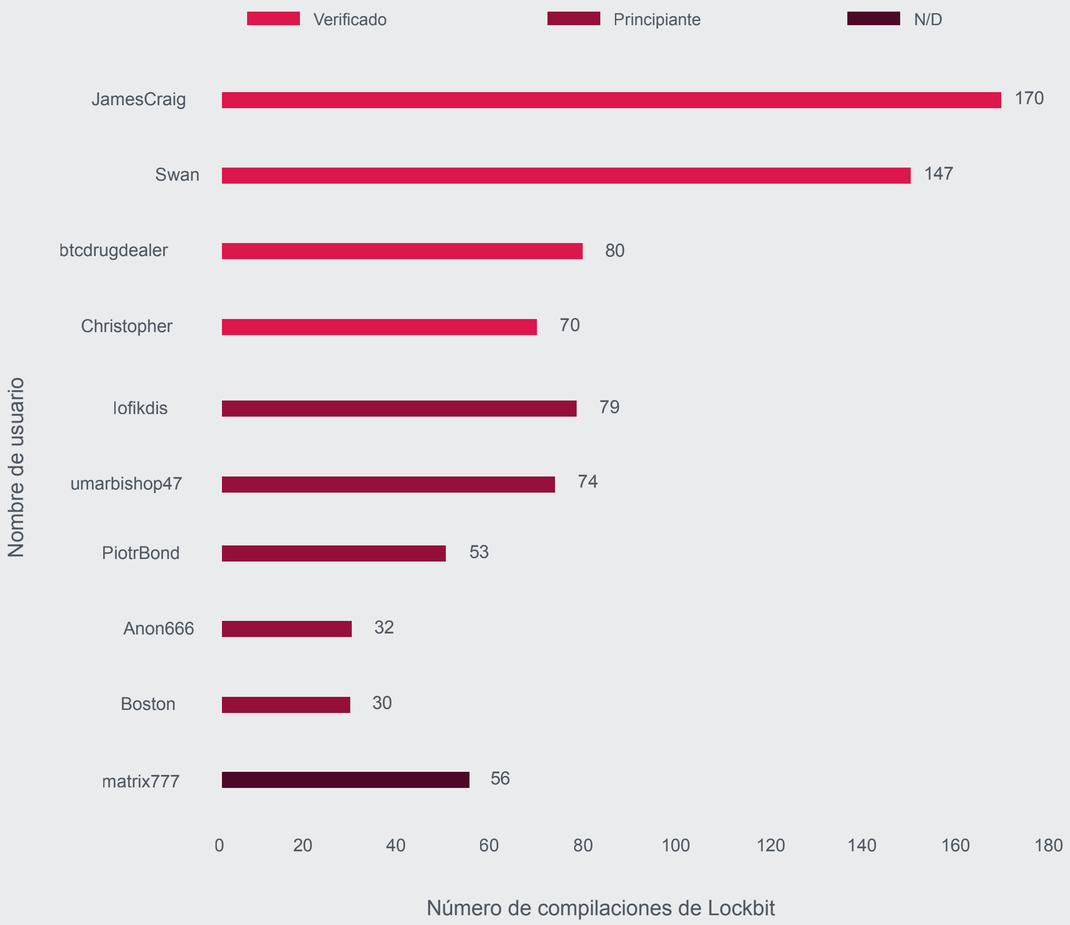


Figura 20: Número de compilaciones de LockBit por afiliado

En total, 208 víctimas participaron en chats para pedir rescate y 20 pagaron un rescate. Solo 10 afiliados de LockBit recibieron pagos de rescate durante este período de casi seis meses, como se muestra en la figura 21.

En un caso*, una víctima acordó pagar a Swan, afiliada de LockBit $2 millones, pero los registros de chat terminaron justo antes de que se proporcionara la información de pago. Sin embargo, podemos inferir que el pago en realidad se realizó a través de otra billetera bitcoin en la base de datos, controlada por el grupo LockBit, quienes recibieron una comisión del 20 % por esa víctima. Así, sólo dos afiliados, Swan y Christopher, ganaron más de US$100,000. En total, todos los afiliados de LockBit obtuvieron un total combinado de 2 334 615 de dólares (1 867 692 dólares después de las comisiones) en pagos de rescate. El grupo LockBit recibió el 20 % de esa cantidad o aproximadamente 466 923 dólares. Si bien no son insignificantes, estos pagos de rescate son mucho más bajos que los de muchos de los principales grupos de ransomware, que con frecuencia reciben muchos pagos multimillonarios. Por lo tanto, esta base de datos filtrada de LockBit indica que la interrupción de febrero de 2024 debilitó significativamente al grupo.

Nombre de usuario	Pagos aproximados recibidos (US$)	Número de víctimas pagadas	Chats de víctimas totales
Cisne	2 021 000 dólares estadounidenses*	2*	17
Christopher	231 015 dólares estadounidenses	8	44
umarbishop47	40 000 dólares estadounidenses	1	10
PiotrBond	13 000 dólares estadounidenses	2	16
Arryn Baird	10 000 dólares estadounidenses	1	5
Iofikdis	6000 dólares estadounidenses	1	12
Riccardo Bond	4400 dólares estadounidenses	1	4
Brown	3600 dólares estadounidenses	1	5
James Craig	3600 dólares estadounidenses	2	17
btcdrugdealer	2000 dólares estadounidenses	1	6

Figura 21: Pagos derescate recibidos por los afiliados de LockBit

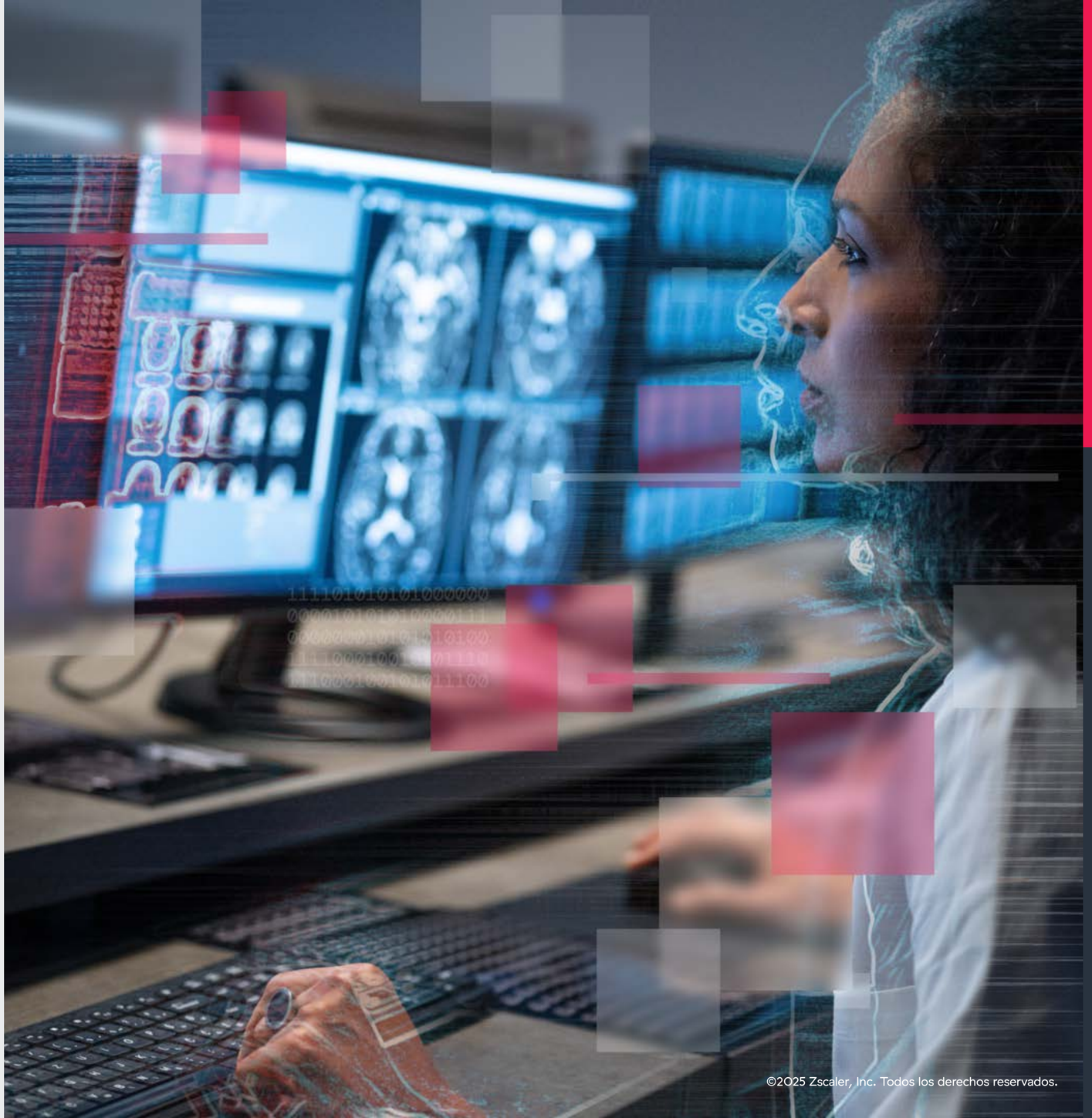
©2025 Zscaler, Inc. Todos los derechos reservados.

La sanidad bajo asedio: la era del robo masivo de datos

La estrategia del ransomware en el sector sanitario ha evolucionado con una nueva receta: primero exfiltrar, luego interrumpir. En la actualidad, los actores de amenazas priorizan el robo de datos como fuente principal de apalancamiento y, como las instituciones de salud poseen vastos repositorios de información sanitaria protegida (PHI), se han convertido en objetivos lucrativos para los operadores de ransomware que buscan maximizar la presión. Dado que la confianza del paciente es fundamental en la asistencia sanitaria, una violación pública puede ser tan perjudicial como el tiempo de inactividad.

A nivel mundial, el sector de la salud experimentó un aumento sustancial año tras año en los ataques de ransomware. Estos ataques a menudo combinaban la exfiltración de grandes volúmenes de datos con encriptación, dejando a las instituciones lidiando con el caos operativo, pérdidas financieras y daños a la reputación. En 2024, la Oficina de Derechos Civiles (OCR) del Departamento de Salud y Servicios Humanos de EE. UU. informó 725 infracciones que involucraron a 500 o más personas, con alrededor de 275 millones de registros de atención médica expuestos.[5]

El ransomware en el ámbito sanitario ya no se limita a causar interrupciones. Se trata de apalancamiento, y eso empieza con los datos. Al robar y exponer millones de registros, los operadores de ransomware pueden duplicar la presión sobre las víctimas de la atención médica. Datos recientes de varias familias de ransomware subrayan una tendencia crítica: la escala del robo de datos se está acelerando rápidamente. Entre los grupos que impulsan esta evolución se encuentra Interlock, que aparece en la sección **“Las 5 principales familias de ransomware a tener en cuenta en 2025–2026”.**



[5] The HIPAA Journal, **Informe sobre infracciones de datos**de atención médicade 2024, 30 de enero de 2025..

©2025 Zscaler, Inc. Todos los derechos reservados.

Cambiando la tendencia del ransomware: desde el frente

A pesar del aumento significativo de los ataques de ransomware durante el último año, hay historias de éxito que contar en la lucha contra el ransomware. La colaboración entre las fuerzas de seguridad internacionales y los investigadores de la industria privada ha demostrado ser eficaz para desmantelar algunos elementos clave de las operaciones de ransomware y apoyar la recuperación de las víctimas.

Por ejemplo, a principios de 2025, ThreatLabz descubrió una vulnerabilidad en RansomHub que hacía posible el descifrado de archivos sin tener que pagar un rescate. Basándose en este descubrimiento, el equipo de ThreatLabz desarrolló *DecryptHub* (ver figura 22), un portal especializado diseñado para ayudar a las organizaciones afectadas por los ataques de ransomware de RansomHub.

El portal DecryptHub de ThreatLabz ayudó a docenas de organizaciones víctimas a recuperar archivos, ahorrándoles potencialmente millones de dólares en pagos de rescate.

RansomHub fue uno de los grupos de ransomware más grandes y activos antes de cerrar en abril de 2025. Muchos de los afiliados del grupo estuvieron anteriormente asociados con la extinta operación de ransomware BlackCat. Al igual que BlackCat, RansomHub utilizó el lenguaje de programación Rust para desarrollar y compilar ransomware para numerosas arquitecturas, entre ellas:

- Ventanas (x86, x64, ARM, ARM64)
- FreeBSD (x64)
- Linux (x86, x64, ARM, ARM64, ARMv5, ARMv5-64, ARMv6, ARMv6-64, ARMv7, ARMv7-64)
- ESXi (x64)

Otro logro notable del año pasado es la operación policial a gran escala, llamada en código **Operación Endgame**, ejecutada en coordinación con socios de la industria, incluido Zscaler (ver figura 23).

Operation Endgame es una iniciativa global destinada a desmantelar las organizaciones cibercriminales y el ecosistema de malware que facilita los ataques de ransomware. El éxito más reciente fue el desmantelamiento de **DanaBot**, una poderosa familia de malware modular que operaba una plataforma de malware como servicio (MaaS) con vínculos a varios grupos de ransomware. Esto se basa en una serie de victorias en 2024, cuando la Operación Endgame apuntó a familias de malware conocidas como **SmokeLoader**, IcedID, SystemBC, Pikabot y Bumblebee.

Zscaler ThreatLabz ha estado apoyando la Operación Endgame durante los últimos dos años, proporcionando recursos e inteligencia vitales para identificar campañas de malware, desmantelar la infraestructura criminal y exponer a los ciberdelincuentes. ThreatLabz también ha lanzado herramientas gratuitas a través de **GitHub** que pueden usarse para detectar y remediar infecciones, lo que subraya la importancia de la colaboración en la lucha contra el ransomware.



Figura 22: El portal de víctimas de DecryptHub

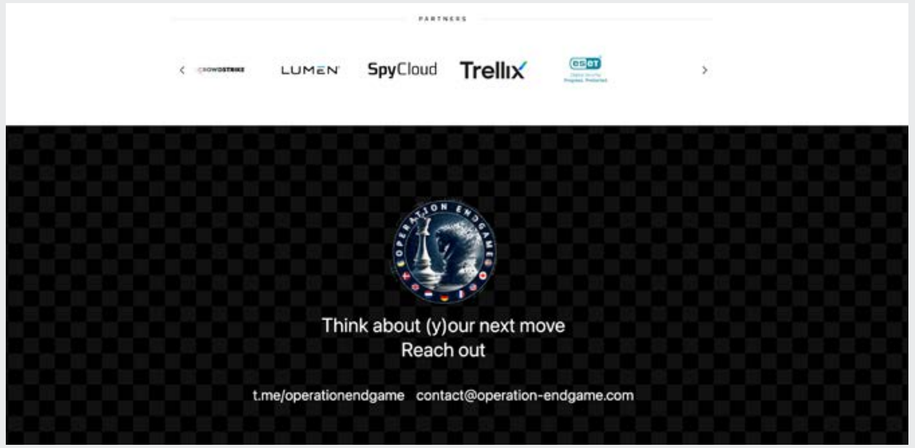


Figura 23: Datos de contacto de Operation Endgame

©2025 Zscaler, Inc. All rights reserved.

Las principales 5 familias de ransomware a vigilar en 2025-2026

Nº 1 Dark Angels

El grupo de ransomware Dark Angels, activo desde abril de 2022, es una de las familias de ransomware más exitosas hasta la fecha. El grupo ha ganado notoriedad por sus ataques altamente lucrativos, con un pago de rescate récord de 75 millones de dólares que ThreatLabz reveló en 2024. El grupo se destaca del resto por una variedad de razones. A diferencia de otros grupos de amenazas, Dark Angels no subcontrata ataques a afiliados externos (es decir, intermediarios de acceso inicial). El número de ataques lanzados por los Ángeles Oscuros es limitado y se centra en grandes organizaciones. Dark Angels exfiltra grandes cantidades de datos de las víctimas, con un promedio de 9,6 TB y una mediana de 2,35 TB. Luego, el grupo decide si implementará ransomware y cifrará los datos de una organización. Dark Angels intenta evitar debilitar a las organizaciones con ransomware para evitar los titulares de las noticias y pasar desapercibidos.

El grupo publica datos de víctimas robadas en un sitio web llamado Dunghill Leak y en un canal de Telegram, ninguno de los cuales menciona a Dark Angels, probablemente en parte para distanciarse (desde el punto de vista de la atribución) de los ataques.

Dark Angels se infiltra en las redes corporativas utilizando una variedad de técnicas, incluidos correos electrónicos de phishing y a través de aplicaciones expuestas públicamente que contienen vulnerabilidades como CVE-2023-22069. El grupo escanea redes comprometidas y aprovecha los entornos de Microsoft Active Directory. Los objetivos principales son los usuarios con privilegios de administrador de dominio para facilitar el movimiento lateral y el acceso a los controladores de dominio de la organización.

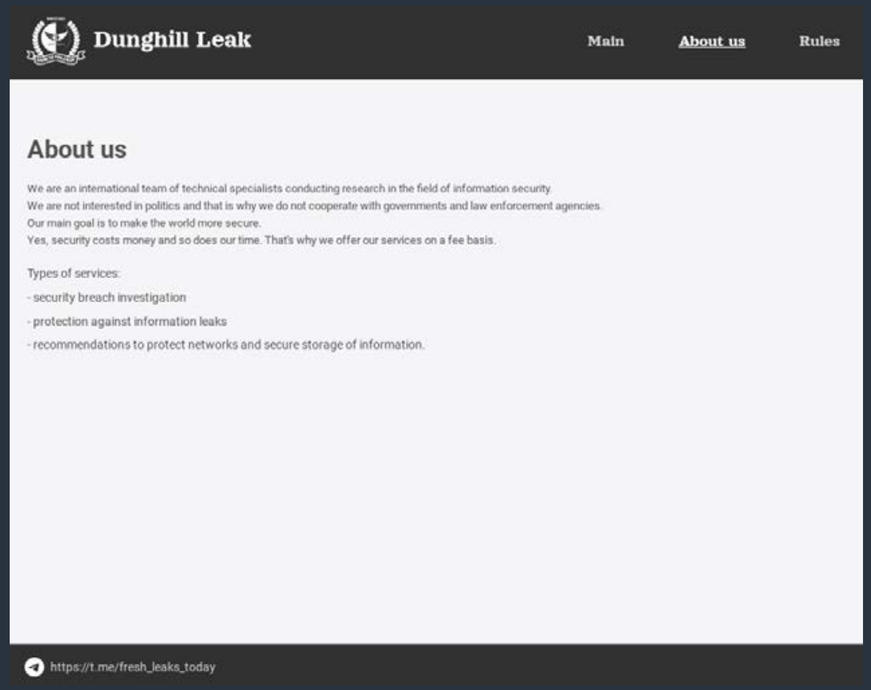


Figura 24: Sitio de la fuga de Dunghill del grupo Dark Angels

Curiosamente Dark Angels no ha desarrollado su propio ransomware. En cambio, el grupo se basa en compilaciones personalizadas de familias de ransomware de terceros, entre las que se incluyen Babuk, Read the Manual (RTM) Locker y una variante de RagnarLocker. Dark Angels apunta a archivos en Windows, Linux, ARM y ESXi para el cifrado de archivos.

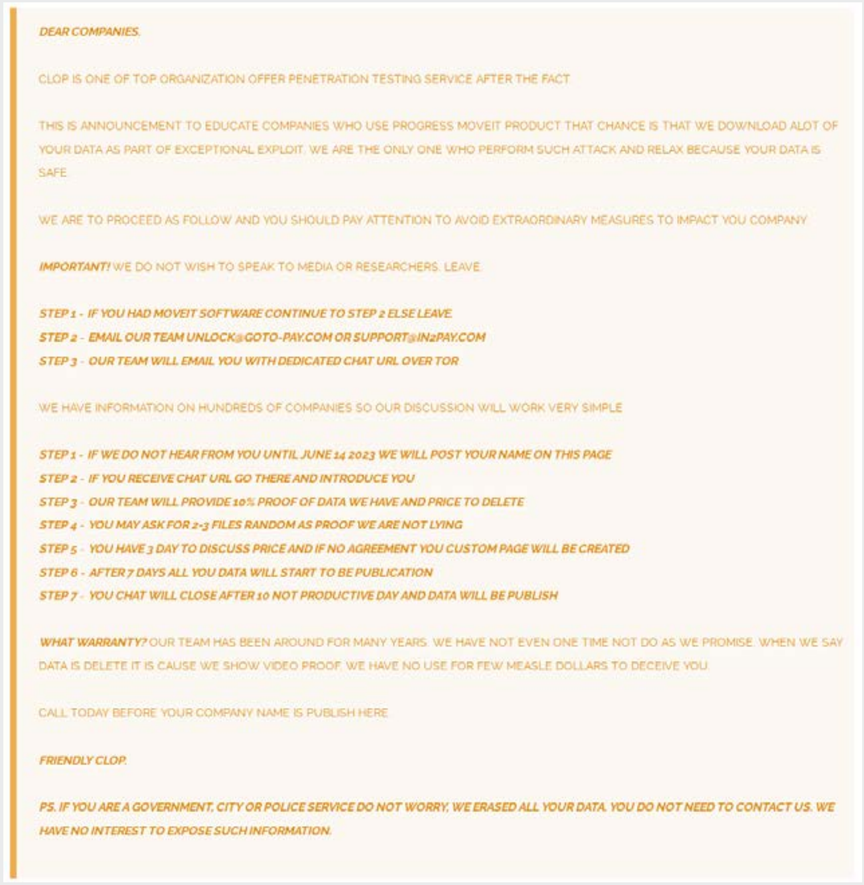


©2025 Zscaler, Inc. Todos los derechos reservados.

Nº2 Clop/Cl0p

Clop, también conocido como ClOp, es un grupo de ransomware que ha estado activo desde 2019. Clop se ha alejado en gran medida del cifrado de archivos y se ha centrado en cambio en la extorsión de datos a través de ataques a la cadena de suministro que explotan vulnerabilidades de día cero, especialmente en plataformas de aplicaciones de transferencia segura de archivos basadas en la web populares que les permiten acceder y robar datos confidenciales de cientos o incluso miles de organizaciones a la vez. Una de las primeras aplicaciones de transferencia de archivos que fue explotada fue la antigua aplicación de transferencia de archivos (FTA) de Acellion en diciembre de 2020. El antiguo Acellion FTA tenía numerosas vulnerabilidades (CVE-2021-2710, CVE-2021-27102, CVE-2021-27103 y CVE-2021-27104) que Clop explotó para implementar un webshell personalizado para robar datos de docenas de organizaciones. En julio de 2021, Clop explotó CVE-2021-35211 en las **aplicaciones Serv-U Managed File Transfer y Serv-U Secure FTP**. En estos casos, Clop utilizó la vulnerabilidad para obtener acceso a las redes internas de las organizaciones, lo que provocó la exfiltración de datos y el cifrado de archivos.

A principios de 2023, Clop llevó a cabo otro ataque a la cadena de suministro dirigido a la aplicación de transferencia de archivos administrada (MFT) de GoAnywhere. Este ataque explotó CVE-2023-0669, permitiendo la ejecución remota de código no autenticado y el robo de datos. Clop aprovechó la vulnerabilidad de día cero para robar datos **de más de 100 empresas**. En mayo de 2023, solo unos meses después del incidente de GoAnywhere MFT, Clop explotó una vulnerabilidad de inyección SQL de día cero (**CVE-2023-34362**) en la aplicación MOVEit Transfer para robar datos de empresas que tenían instancias con acceso a Internet. Este fue uno de los mayores ataques a la cadena de suministro de ransomware hasta la fecha, que afectó a más de 2500 organizaciones y provocó la pérdida de información personal de **millones de personas**. Clop anunció este ataque en su sitio de filtración de datos, como se muestra en la figura 25.



DEAR COMPANIES,

CLOP IS ONE OF TOP ORGANIZATION OFFER PENETRATION TESTING SERVICE AFTER THE FACT.

THIS IS ANNOUNCEMENT TO EDUCATE COMPANIES WHO USE PROGRESS MOVEIT PRODUCT THAT CHANCE IS THAT WE DOWNLOAD ALOT OF YOUR DATA AS PART OF EXCEPTIONAL EXPLOIT. WE ARE THE ONLY ONE WHO PERFORM SUCH ATTACK AND RELAX BECAUSE YOUR DATA IS SAFE.

WE ARE TO PROCEED AS FOLLOW AND YOU SHOULD PAY ATTENTION TO AVOID EXTRAORDINARY MEASURES TO IMPACT YOU COMPANY.

IMPORTANT! WE DO NOT WISH TO SPEAK TO MEDIA OR RESEARCHERS. LEAVE.

STEP 1 - IF YOU HAD MOVEIT SOFTWARE CONTINUE TO STEP 2 ELSE LEAVE.
STEP 2 - EMAIL OUR TEAM UNLOCK@GOTO-PAY.COM OR SUPPORT@IN2PAY.COM
STEP 3 - OUR TEAM WILL EMAIL YOU WITH DEDICATED CHAT URL OVER TOR

WE HAVE INFORMATION ON HUNDREDS OF COMPANIES SO OUR DISCUSSION WILL WORK VERY SIMPLE.

STEP 1 - IF WE DO NOT HEAR FROM YOU UNTIL JUNE 14 2023 WE WILL POST YOUR NAME ON THIS PAGE
STEP 2 - IF YOU RECEIVE CHAT URL GO THERE AND INTRODUCE YOU
STEP 3 - OUR TEAM WILL PROVIDE 10% PROOF OF DATA WE HAVE AND PRICE TO DELETE
STEP 4 - YOU MAY ASK FOR 2-3 FILES RANDOM AS PROOF WE ARE NOT LYING
STEP 5 - YOU HAVE 3 DAY TO DISCUSS PRICE AND IF NO AGREEMENT YOU CUSTOM PAGE WILL BE CREATED
STEP 6 - AFTER 7 DAYS ALL YOU DATA WILL START TO BE PUBLICATION
STEP 7 - YOU CHAT WILL CLOSE AFTER 10 NOT PRODUCTIVE DAY AND DATA WILL BE PUBLISH

WHAT WARRANTY? OUR TEAM HAS BEEN AROUND FOR MANY YEARS. WE HAVE NOT EVEN ONE TIME NOT DO AS WE PROMISE. WHEN WE SAY DATA IS DELETE IT IS CAUSE WE SHOW VIDEO PROOF. WE HAVE NO USE FOR FEW MEASLE DOLLARS TO DECEIVE YOU.

CALL TODAY BEFORE YOUR COMPANY NAME IS PUBLISH HERE.

FRIENDLY CLOP.

PS. IF YOU ARE A GOVERNMENT, CITY OR POLICE SERVICE DO NOT WORRY, WE ERASED ALL YOUR DATA. YOU DO NOT NEED TO CONTACT US. WE HAVE NO INTEREST TO EXPOSE SUCH INFORMATION.

Figura 25: Anuncio de Clop sobre la explotación de la vulnerabilidad CVE-2023-34362 MOVEit

Los ataques a la cadena de suministro a gran escala más recientes de Clop fueron en octubre de 2024, que explotaron dos vulnerabilidades CVE-2024-50623 y CVE-2024-55956 en las aplicaciones de transferencia de archivos Harmony, VLTrader y LexiCom de Cleo. Estas vulnerabilidades permitían a un usuario no autenticado importar y **ejecutar comandos arbitrarios de Bash o PowerShell**. Una vez más, Clop utilizó estas vulnerabilidades para robar datos de organizaciones que utilizaban las aplicaciones de transferencia de archivos de Cleo que estaban expuestas a Internet. ThreatLabz capturó un ejemplo de nota de rescate de Clop proporcionada a una víctima de estos ataques de Cleo y está disponible aquí.

La amplitud de los ataques de Clop es significativa y algunas víctimas fueron objeto de múltiples infracciones por parte del grupo. De hecho, ThreatLabz identificó a una víctima del ataque MOVEit de Clop, que previamente pagó $1 millones en rescate, siendo luego víctima del ataque Cleo del grupo.

©2025 Zscaler, Inc. Todos los derechos reservados.

Nº 3 DragonForce

DragonForce surgió como un grupo RaaS en diciembre de 2023. Las primeras versiones del ransomware de DragonForce utilizaban el constructor filtrado LockBit, y el grupo luego creó su propio ransomware basado en el código fuente filtrado de Conti. A principios de 2025, DragonForce anunció un nuevo modelo de negocio de "cártel" en un foro sobre delitos cibernéticos y en su sitio web de noticias, como se muestra en la figura 26.

Este nuevo modelo permite a los afiliados de ransomware utilizar la infraestructura, las herramientas y los servicios del grupo para sus propios ataques con un esquema del 80/20 de participación porcentual en las ganancias. Los afiliados del grupo han robado más de 30 TB de datos y cada víctima ha perdido aproximadamente 156 GB en promedio, con una mediana de 72 GB.

DragonForce recibió una atención relativamente modesta hasta abril de 2025, cuando el grupo anunció que se iba a "fusionar" con RansomHub, uno de los mayores y más activos grupos de ransomware en ese momento. RansomHub negó la afirmación y acusó a los miembros de DragonForce de trastocar su infraestructura y desfigurar su sitio web. Tanto si la afirmación era correcta como una coincidencia, RansomHub cerró sus operaciones y muchos de los afiliados del grupo migraron a DragonForce. Entre estos afiliados se encuentra Scattered Spider (también conocido como "The Com"), que ha llevado a cabo ataques importantes contra grandes organizaciones utilizando diversas técnicas de ingeniería social dirigidas a los departamentos de TI para eludir la autenticación multifactor (MFA). Se cree que Scattered Spider está detrás de los ataques DragonForce dirigidos a varios minoristas del Reino Unido en abril y mayo de 2025.

Nº 4 Akira

Desde que surgió en abril de 2023, Akira se ha establecido como uno de los grupos de ransomware más activos. Las versiones iniciales de Akira se basaron en el código fuente filtrado de Conti. Posteriormente, el grupo desarrolló un ransomware basado en Rust llamado Megazord. Sin embargo, el grupo abandonó Megazord en favor de la variante basada en C/C++, que ahora se compila para las versiones ESXi 6 y 7, así como para Windows x86 y x64. La última variante utiliza la biblioteca aritmética de precisión múltiple GNU (GMP) para el cifrado RSA en lugar de las API nativas de Windows que se encontraban en versiones anteriores. Es interesante señalar que Black Basta utilizó anteriormente la misma biblioteca GMP para el cifrado asimétrico en su ransomware (antes de migrar a la Crypto++ biblioteca).

Los afiliados de Akira continúan concentrándose principalmente en el cifrado de archivos en lugar de robar grandes cantidades de datos. Los volúmenes de exfiltración de datos por parte de los afiliados de Akira suelen ser más bajos en promedio que los de muchos otros grupos de ransomware que roban terabytes de datos o más de víctimas individuales. De hecho, en el sitio de filtración de datos de Akira (ver figura 27), los volúmenes promedio y mediano de robo de datos fueron 44.87 GB y 14.33 GB, respectivamente. El robo de datos más voluminoso fue de aproximadamente 370 GB, mucho más pequeño que el de muchas de las principales familias de ransomware. Sin embargo, a pesar de no centrarse en el robo de datos, Akira tiene un número significativo de víctimas y es responsable de más de 13 TB de pérdida de datos en total.

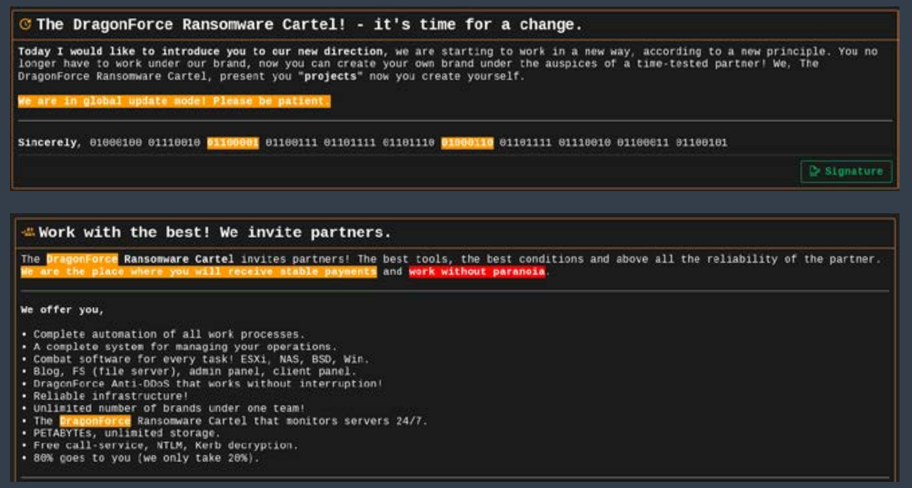


Figura 26: Anuncio del "cartel" de DragonForce



Figura 27: Sitio de filtración de datos del grupo Akira

©2025 Zscaler, Inc. Todos los derechos reservados.

Nº 5 Interlock

Interlock es un grupo de ransomware más nuevo que ha estado realizando ataques desde al menos septiembre de 2024, comprometiendo alrededor de 50 organizaciones víctimas. Los ataques de Interlock abarcan diversos sectores, incluidos la salud, la educación, las finanzas, el gobierno y la manufactura. Los dos primeros sectores se han visto especialmente afectados por el Interlock. Es probable que esta segmentación se deba al profundo conocimiento del grupo de los marcos de cumplimiento como GDPR, HIPAA, CCPA, NYDFS y GLBA. Interlock intenta aprovechar estas regulaciones para presionar a las víctimas a pagar un rescate. De hecho, **las notas de rescate** de Interlock mencionan específicamente las sanciones financieras por tales violaciones.

El grupo ha desarrollado variantes de ransomware para Windows, Linux y FreeBSD. El ransomware no es digno de mención, salvo que es relativamente poco común crear compilaciones específicas para este último. Sin embargo, dado que muchas grandes organizaciones utilizan FreeBSD para ejecutar infraestructura de servidor crítica, no es sorprendente y seguirá siendo un objetivo.

Al igual que Dark Angels, Interlock roba volúmenes significativos de datos de las organizaciones. En un caso, Interlock robó más de 11 TB de datos de una sola víctima. Otra víctima en la industria de la salud perdió más de 5 TB de datos y pagó de más 2.5 millones de dólares en rescate. En total, el grupo ha robado más de 73.5 TB de datos solo en los últimos nueve meses. En promedio, cada víctima perdió 1.6 TB de datos, y la pérdida media fue de alrededor de 700 GB.

La sección Acerca de del sitio de filtración de datos de Interlock, que se muestra en la figura 28, destaca la postura del grupo hacia las víctimas. Interlock culpa a las víctimas de “imprudencia” y “negligencia” como las causas fundamentales que llevan a los ataques de ransomware del grupo.

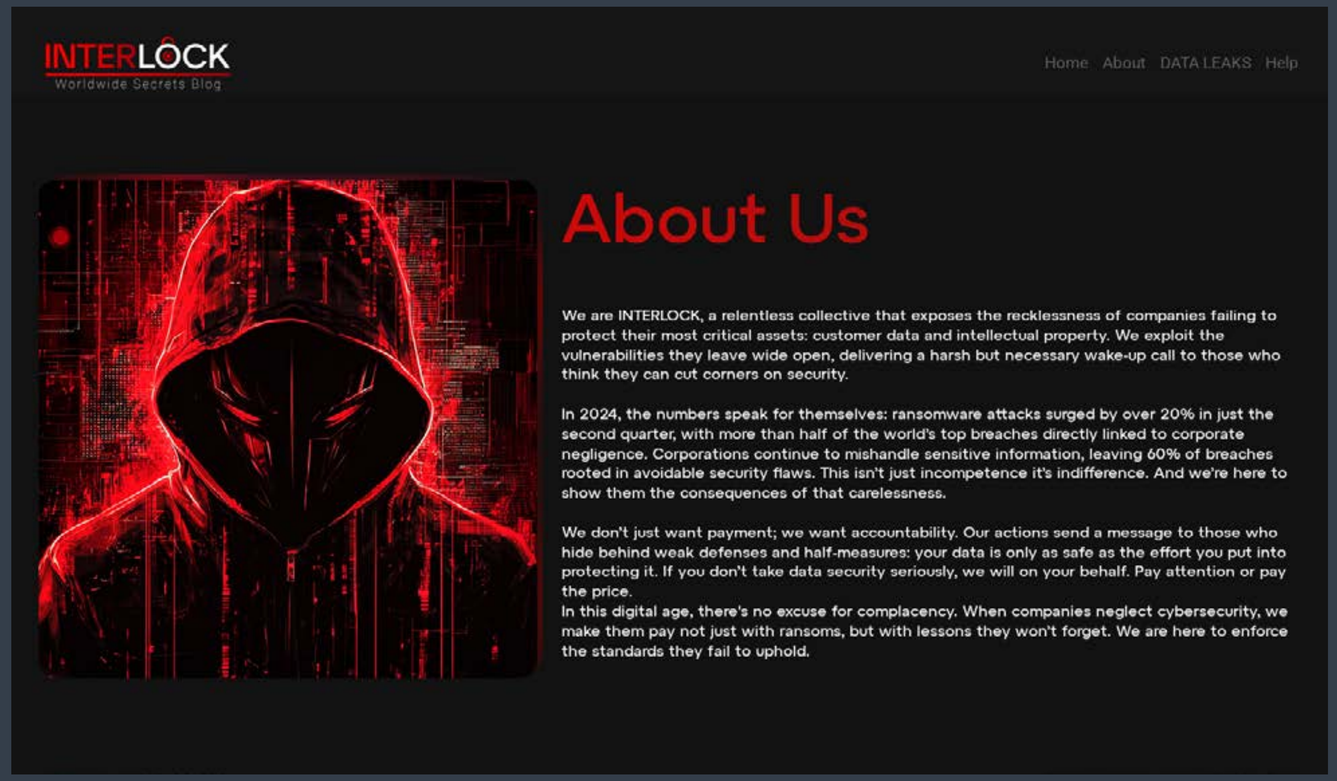


Figura 28: Página “Acerca de nosotros” del grupo Interlock

©2025 Zscaler, Inc. Todos los derechos reservados.

Archivo Notas de ransomware de ThreatLabz

Zscaler ThreatLabz mantiene un **repositorio público de GitHub** que, al momento de escribir este artículo, agregó otras 73 nuevas notas de ransomware durante el año pasado, lo que eleva el total a 1018. Este archivo puede ser valioso para rastrear grupos de ransomware a lo largo del tiempo, incluidos sus sitios web de fuga de datos y sus tácticas de negociación, así como para utilizar el análisis estilométrico para vincular grupos de ransomware que cambian de nombre.



©2025 Zscaler, Inc. Todos los derechos reservados.



Predicciones para 2026

1. Los grupos de ransomware utilizarán GenAI como arma para campañas de extorsión escalables y de múltiples fases.

La IA generativa se convertirá cada vez más en una infraestructura central para las operaciones de ransomware. Las comunicaciones filtradas del grupo Black Basta revelan cómo los actores de amenazas de ransomware ya están utilizando herramientas como ChatGPT para generar señuelos de phishing y documentos falsos, depurar y reescribir malware y crear contenido deepfake. De cara al futuro, se espera que las operaciones de ransomware amplíen este modelo, con amplias posibilidades, incluido el uso de LLM para analizar y resumir datos confidenciales robados. Además, a medida que las empresas aumentan la cantidad de datos que recopilan para fines de entrenamiento de IA, estos datos se convertirán en objetivos lucrativos para las bandas de ransomware.

2. Los grupos de ransomware seguirán empleando ataques de ingeniería social de múltiples etapas.

Los operadores de ransomware duplicarán los ataques dirigidos y abandonarán las campañas de spam masivo en favor de una ingeniería social de alta precisión. Al utilizar plataformas como LinkedIn y ZoomInfo, identificarán a los empleados con acceso privilegiado, saturarán las bandejas de entrada con spam y luego se harán pasar por personal de TI a través de llamadas telefónicas para poder ingresar.

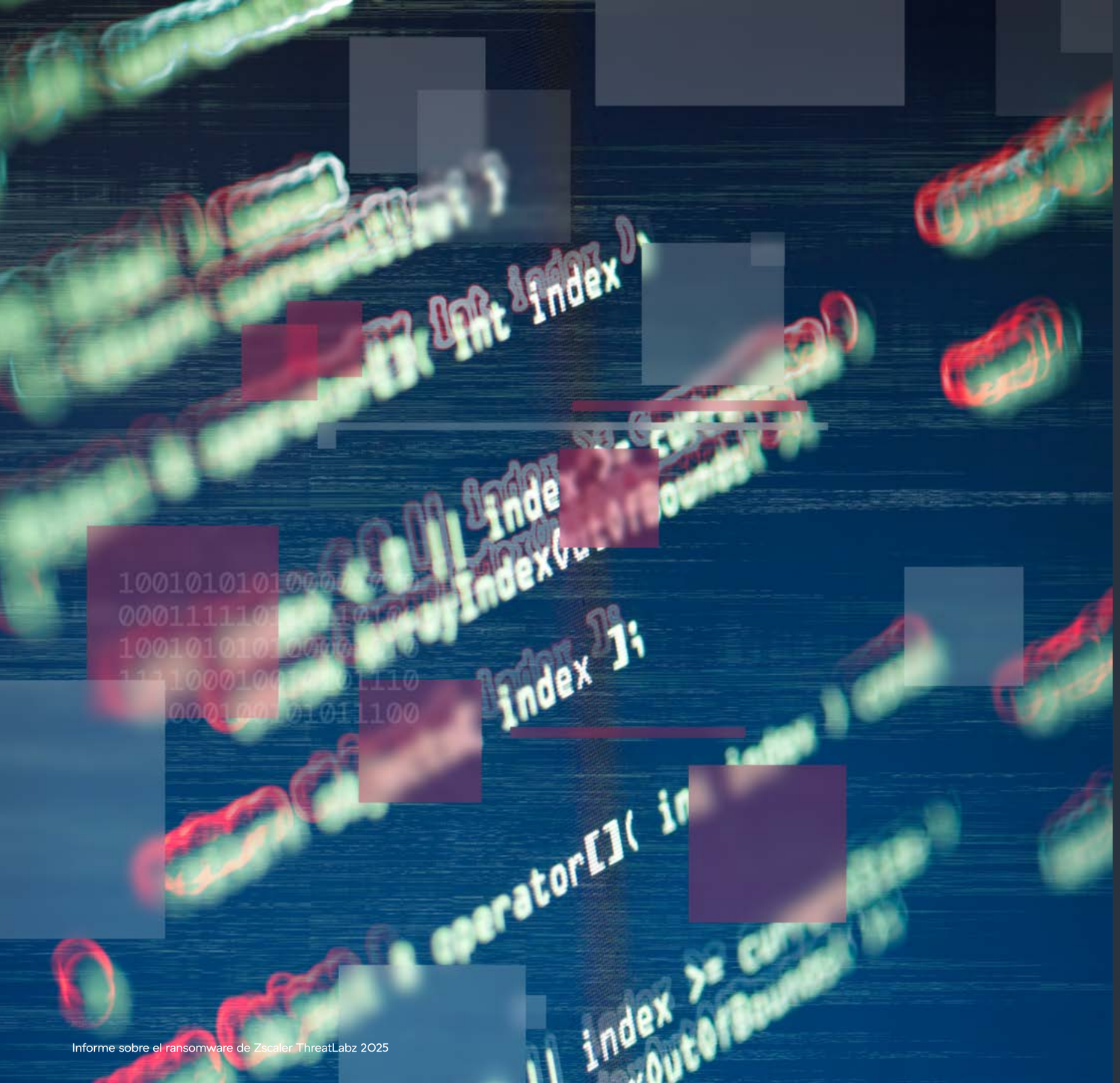
3. Los ataques basados en voz aumentarán a medida que los operadores de ransomware perfeccionen sus tácticas de ingeniería social.

Los grupos de ransomware seguirán aprovechando vectores de ataque basados en voz a través de phishing de voz o “vishing” y audio generado por IA para obtener acceso a las organizaciones víctimas. Estas tácticas explotan la confianza y la urgencia humanas, a menudo haciéndose pasar por ejecutivos o personal de TI para manipular a los empleados para que revelen sus credenciales o concedan acceso a los sistemas internos. A medida que las herramientas de inteligencia artificial generativa se vuelven más accesibles, los actores de amenazas de ransomware esencialmente pondrán el vishing en piloto automático, aprovechando tácticas como la clonación de voz multilingüe y los scripts de llamadas adaptativos para engañar a los empleados de la empresa y abrir la puerta al cifrado y la extorsión.

4. La extorsión de datos seguirá siendo un factor clave para el pago de rescates, con un aumento en los volúmenes de robo.

El robo de datos se está convirtiendo en la principal palanca de las campañas de ransomware y esta tendencia se acelerará. Grupos como Clop, BianLian y Hunters International han liderado el cambio hacia operaciones puramente de extorsión, abandonando por completo el cifrado. ThreatLabz observó que varios de estos grupos ahora roban cientos de gigabytes por víctima en promedio. A medida que las organizaciones mejoran sus capacidades de respaldo y recuperación, los actores de amenazas utilizarán cada vez más los datos robados para presionar a las organizaciones víctimas a pagar.

©2025 Zscaler, Inc. Todos los derechos reservados.



5. Las filtraciones del código fuente del ransomware y de sus creadores impulsarán la próxima generación de ataques.

A medida que las herramientas de creación de ransomware y el código fuente continúan filtrándose (intencionadamente o no), surgirá una nueva ola de ataques de bajo esfuerzo y alto impacto. Las filtraciones de los principales grupos de ransomware ya han alimentado operaciones derivadas, variantes con nuevo nombre y campañas de imitación. Los grupos emergentes se basarán en bases de código filtradas, modificando cargas útiles y técnicas de entrega mientras evaden las firmas de detección existentes.

6. Las fuerzas del orden ampliarán su enfoque para centrarse en quienes facilitan el ransomware.

Las operaciones internacionales de aplicación de la ley son cada vez más audaces y específicas, y destruyen no solo los grupos de ransomware, sino también la infraestructura y los servicios que posibilitan sus ataques. Operation Endgame demostró que las plataformas de distribución de malware pueden desmantelarse a gran escala.

7 Los afiliados de ransomware continuarán moviéndose entre grupos.

El modelo de ransomware como servicio (RaaS) brinda flexibilidad a los afiliados y crea volatilidad en el panorama de amenazas. Los afiliados cambian con frecuencia de grupo en función de las presiones de eliminación, las condiciones de pago, las herramientas o la reputación. Este movimiento constante conduce a una infraestructura reciclada, tácticas superpuestas y cambios rápidos de marca cuando se interrumpen las operaciones. Mientras los modelos de afiliados sigan siendo rentables con bajo riesgo, este patrón continuará.

©2025 Zscaler, Inc. Todos los derechos reservados.

Cómo Zscaler detiene el ransomware con Zero Trust + AI

El ransomware prospera en entornos donde la seguridad está fragmentada, la visibilidad es limitada y la confianza es implícita. Sin embargo, muchas organizaciones aún dependen de herramientas de seguridad tradicionales (cortafuegos de última generación, VPN y productos puntuales como antimalware) que no fueron diseñados para manejar amenazas modernas.

Estas arquitecturas heredadas crean más riesgos de los que mitigan. Dejan brechas críticas en la protección contra el ransomware, desde puntos ciegos en el tráfico cifrado hasta visibilidad aislada de amenazas y gestión de políticas complejas e inconsistentes. Y lo que es peor, estas arquitecturas se basan en modelos de acceso amplios y excesivamente permisivos que exponen los recursos internos. Una vez que los atacantes logran establecerse, pueden moverse lateralmente a través de los sistemas, lo que hace que sea más fácil para los actores de amenazas de ransomware propagarse, escalar privilegios y acceder a datos confidenciales sin ser detectados.

Zscaler Zero Trust Exchange™ elimina estos riesgos al reemplazar modelos obsoletos centrados en la red con una arquitectura de confianza cero impulsada por IA y nativa de la nube. Ofrece una plataforma unificada y escalable que minimiza el riesgo y simplifica la protección contra ransomware entre usuarios, dispositivos y aplicaciones, sin importar dónde residan.

ZSCALER DETIENE EL RANSOMWARE EN CADA ETAPA DEL CICLO DE VIDA DEL ATAQUE:

- **Minimizar la superficie de ataque:** eliminar de forma eficaz la infraestructura expuesta a la que el ransomware puede apuntar ocultando usuarios, aplicaciones y dispositivos detrás de un proxy en la nube, donde no son visibles ni detectables desde Internet, lo que crea una superficie de ataque mucho más pequeña. No hay IP públicas ni acceso directo a la red: los actores de amenazas de ransomware no pueden encontrar ni acceder a los recursos internos. La tecnología de predicción de infracciones aprovecha la IA para simular escenarios de ataque y señalar las posibles rutas que los actores de amenazas podrían explotar, lo que permite a los equipos de seguridad remediar antes de que ocurra un ataque.

- **Prevenir el compromiso inicial:** proteja a los usuarios para que no accedan a contenido malicioso y detecte amenazas desconocidas antes de que lleguen a su red mediante una protección completa. TLS/SSL Inspección, sandboxing y aislamiento en línea. Estas capacidades detienen el ransomware antes de que pueda ejecutarse, minimizando así el riesgo de que se produzca una vulneración en primer lugar.

- **Eliminar el movimiento lateral:** conecta a los usuarios directamente con las aplicaciones (y las aplicaciones con otras aplicaciones), no con la red en sí, eliminando así el riesgo de movimiento lateral. La segmentación impulsada por IA adapta el acceso en función del comportamiento del usuario, la postura del dispositivo y el contexto de la aplicación. Los actores de amenazas de ransomware no pueden propagarse de un sistema a otro, incluso si un punto final está comprometido. La inteligencia artificial y la detección y respuesta a amenazas de identidad (ITDR) ayudan a revelar patrones de acceso anómalos, mientras que la tecnología de engaño y los señuelos atraen a los actores de amenazas de ransomware a trampas monitoreadas.

- **Bloquear la exfiltración de datos:** las campañas de ransomware que priorizan la extorsión se basan en el robo de datos confidenciales. Las capacidades de protección contra pérdida de datos en línea (DLP), CASB e inspección de tráfico bloquean transferencias no autorizadas a aplicaciones en la nube autorizadas, TI en la sombra e infraestructura de comando y control (C2).



©2025 Zscaler, Inc. Todos los derechos reservados.

LAS PRINCIPALES PROTECCIONES CONTRA RANSOMWARE IMPULSADAS POR IA DE ZSCALER INCLUYEN:

- **La predicción** de infracciones anticipa posibles escenarios de infracciones mediante IA generativa y modelos predictivos multidimensionales.
- **La detección de phishing y C2** utiliza detección basada en IA en línea de Zscaler Secure Web Gateway para identificar y bloquear sitios de phishing e infraestructura C2 nunca antes vistos.
- **El sandbox en línea** ofrece una prevención integral contra malware y amenazas de día cero mediante el uso de modelos de inteligencia artificial avanzados para analizar archivos sospechosos en un entorno controlado.
- **Zero Trust Browser** aprovecha la inteligencia artificial para identificar y aislar contenido web malicioso, evitando fugas de datos y la distribución de malware.
- **La segmentación** utiliza el aprendizaje automático para generar automáticamente recomendaciones para segmentos y políticas de aplicaciones, lo que en última instancia minimiza la superficie de ataque y evita el movimiento lateral.
- **La política dinámica basada en riesgos evalúa** continuamente la postura de riesgo de los usuarios, dispositivos y aplicaciones utilizando análisis de comportamiento impulsado por IA para aplicar políticas de acceso y seguridad dinámicas.
- **El descubrimiento y la clasificación de datos escanean y clasifican** instantáneamente datos confidenciales en puntos finales, tráfico en línea y aplicaciones en la nube, lo que hace que sea más difícil para el ransomware atacar y cifrar datos confidenciales.
- **Los controles de prevención de pérdida de datos (DLP)** bloquean transferencias de datos no autorizadas, respaldados por la inspección de contenido basada en inteligencia artificial y la aplicación de políticas, lo que evita que los operadores de ransomware roben datos confidenciales para extorsionar.



A MEDIDA QUE EVOLUCIONAN LAS TÁCTICAS DE RANSOMWARE, TAMBIÉN DEBEN EVOLUCIONAR LAS DEFENSAS. ZSCALER ZERO TRUST EXCHANGE ES FUNDAMENTAL PARA AYUDAR A LAS ORGANIZACIONES A REDUCIR SU SUPERFICIE DE ATAQUE, DETENER AMENAZAS DE RANSOMWARE NUEVAS Y EVASIVAS, PREVENIR EL MOVIMIENTO LATERAL (INCLUSO DESPUÉS DE UNA VULNERACIÓN) E INTERRUMPIR LOS INTENTOS DE EXTORSIÓN ANTES DE QUE SE FILTREN LOS DATOS.

©2025 Zscaler, Inc. Todos los derechos reservados.

Lista de comprobación de prevención de ransomware

Zero Trust es imprescindible cuando se trata de detener el ransomware, pero la defensa eficaz contra el ransomware no termina allí. También depende de capas operativas más amplias, incluida la capacitación de los empleados, copias de seguridad seguras y un plan de respuesta bien preparado.

Basada en los conocimientos de los expertos de ThreatLabz, esta lista de verificación reúne los pasos más efectivos que puede tomar ahora mismo para reducir el riesgo de ransomware y desarrollar una resiliencia duradera.

Realice copias de seguridad de los datos periódicamente

- [ ] Mantenga copias de seguridad cifradas y rutinarias, tanto en línea como fuera de línea.
- [ ] Pruebe los procedimientos de recuperación con frecuencia y adapte las estrategias de respaldo a medida que evolucionan las tácticas de ransomware.

Implementar la autenticación multifactor (MFA)

- [ ] Exigir MFA en todas las cuentas de usuario, especialmente para el acceso privilegiado.
- [ ] Integre con la protección de identidad para detectar y bloquear la apropiación de cuentas de manera efectiva.

Reforzar la seguridad de las aplicaciones

- [ ] Eliminar aplicaciones de la exposición pública para evitar que los actores de ransomware exploten vulnerabilidades.
- [ ] Implemente una arquitectura de confianza cero para las aplicaciones internas para protegerlas contra el ransomware.

Mantenga el software y los sistemas actualizados

- [ ] Aplique las últimas revisiones de seguridad rápidamente para cerrar las vulnerabilidades conocidas.
- [ ] Utilice inteligencia sobre amenazas basada en IA para priorizar la aplicación de revisiones en función del riesgo del mundo real.

Estandarizar las políticas de seguridad corporativa

- [ ] Asegúrese de que todos los usuarios sigan procedimientos de seguridad consistentes, incluida MFA, actualizaciones de software y controles de acceso.
- [ ] Adopte una arquitectura de servicio de seguridad de borde (SSE) para proteger a los usuarios, ya sea en las instalaciones o de forma remota.

Aplicar controles de acceso con privilegios mínimos

- [ ] Implementar políticas de mínimo privilegio para limitar el acceso de los usuarios estrictamente a los datos y sistemas necesarios para sus funciones.
- [ ] Utilice soluciones impulsadas por IA para analizar dinámicamente el comportamiento y ajustar los privilegios en consecuencia.



©2025 Zscaler, Inc. Todos los derechos reservados.

Fortalecer la protección de la identidad

- [ ] Utilice las herramientas ITDR para monitorear configuraciones incorrectas de identidad, remediar vulnerabilidades en Active Directory que los adversarios explotan para escalar privilegios y moverse lateralmente, y detectar amenazas de identidad ocultas.

Utilice el aislamiento del navegador impulsado por IA

- [ ] Aísle de forma segura las sesiones de usuario de la web para evitar descargas automáticas, phishing y robo de credenciales.
- [ ] Permita que los usuarios accedan a sitios sospechosos en un entorno contenido y de solo lectura.

Aproveche la tecnología del engaño

- [ ] Coloque trampas (por ejemplo, honeypots, credenciales falsas) para detectar, desviar y retrasar a los atacantes en las primeras etapas de la cadena de ataque.
- [ ] Utilice alertas de sistemas de engaño para acelerar la respuesta a incidentes.

Proporcione formación continua a los empleados

- [ ] Eduque periódicamente a los usuarios sobre las técnicas de ransomware, incluido el phishing, la ingeniería social y las actualizaciones de software falsas.
- [ ] Simule escenarios de ataques del mundo real para mejorar la preparación de los empleados.

Inspeccione todo el tráfico, especialmente el cifrado.

- [ ] El 87% de las amenazas se esconden en canales cifrados: inspeccione todo el tráfico, cifrado o no, para descubrir amenazas ocultas y evitar vulneraciones.

Implemente un entorno sandbox impulsado por IA

- [ ] Detecte y bloquee malware evasivo nunca antes visto mediante IA y análisis de comportamiento con aprendizaje automático
- [ ] Ponga en cuarentena los archivos sospechosos antes de que lleguen a los puntos finales.

Controle el acceso a SaaS con un CASB

- [ ] Supervise y administre el uso de aplicaciones en la nube para bloquear actividades maliciosas como descargas de archivos y exfiltración de datos.
- [ ] Haga cumplir las políticas sobre el uso compartido y las descargas de datos.

Cree un plan de respuesta al ransomware probado

- [ ] Incluya procedimientos para recuperación de datos, respuesta a incidentes y protocolos de comunicación.
- [ ] Realice ejercicios de mesa periódicamente para evaluar la preparación y cerrar brechas.

Implemente el acceso a la red de confianza cero (ZTNA)

- [ ] Reemplace el acceso amplio a la red con una segmentación precisa basada en la identidad (de usuario a aplicación y de aplicación a aplicación).
- [ ] Acceso al intermediario a través de controles de acceso con privilegios mínimos para evitar el movimiento lateral y reducir la superficie de ataque.

Implemente la prevención de pérdida de datos en línea (DLP)

- [ ] Evite la exfiltración de datos y las transferencias de archivos confidenciales implementando medidas DLP en línea.
- [ ] Aplique políticas en todos los canales web, en la nube y por correo electrónico.

©2025 Zscaler, Inc. Todos los derechos reservados.

Metodología de investigación

La metodología de investigación para este informe es un proceso integral que utiliza múltiples fuentes de datos para identificar y rastrear las tendencias de ransomware. El equipo de ThreatLabz recopiló datos entre abril de 2024 y abril de 2025 de fuentes que incluyen:

- **La nube de seguridad global de Zscaler.** La nube de Zscaler procesa más de 500 billones de señales diarias, bloquea más de 9 mil millones de amenazas e infracciones de políticas por día y ofrece más de 250 000 actualizaciones de seguridad diarias a los clientes de Zscaler. Analizamos estos datos, que incluyen información sobre direcciones IP de origen, direcciones IP de destino y tipos de archivos asociados con ataques de ransomware, para identificar la actividad de ransomware.
- **Análisis propio del equipo de ThreatLabz de muestras de ransomware y datos de ataques.** ThreatLabz rastrea familias de ransomware y actores de amenazas, junto con la telemetría de ataque correspondiente. El equipo realiza ingeniería inversa profunda para comprender las herramientas utilizadas por los intermediarios de acceso inicial, así como el ransomware en sí, incluidos los algoritmos de cifrado de archivos. En varios casos, el equipo ha descubierto fallas criptográficas que pueden explotarse para descifrar archivos sin pagar un rescate y ha creado herramientas de descifrado. El equipo proporciona estas herramientas a los organismos internacionales encargados de hacer cumplir la ley para que las ofrezcan a las víctimas de forma gratuita. ThreatLabz también ha creado una plataforma patentada de automatización de malware que puede detectar y detener automáticamente las amenazas en la nube de Zscaler.
- **Fuentes de inteligencia externas.** También recopilamos y comparamos nuestros propios datos con investigaciones de fuentes abiertas cuando fue posible.

Acerca de ThreatLabZ

ThreatLabz es la división de investigación de seguridad de Zscaler. Este equipo de clase mundial es responsable de localizar nuevas amenazas y asegurar que las miles de organizaciones que utilizan la plataforma global de Zscaler estén siempre protegidas. Además de la investigación de malware y el análisis de comportamiento, los miembros del equipo participan en la investigación y el desarrollo de nuevos módulos prototipo para la protección avanzada contra amenazas en la plataforma Zscaler y realizan regularmente auditorías de seguridad internas para garantizar que los productos y la infraestructura de Zscaler cumplen con los estándares de cumplimiento de seguridad. ThreatLabz publica regularmente análisis detallados de amenazas nuevas y emergentes en su portal, **research.zscaler.com**.

***Siga a Zscaler ThreatLabz* para obtener información periódica sobre las últimas amenazas y desarrollos de ransomware, incluidos los indicadores de compromiso (IOC) publicados y MITRE ATT. & Mapeos CK. Esta información se puede utilizar para capacitar a su equipo, mejorar su postura de seguridad y ayudar a prevenir ataques de ransomware.**

ThreatLabz también mantiene depósitos de GitHub con IOC, herramientas (incluidas herramientas de descifrado de ransomware de prueba de concepto) y un archivo de notas de ransomware de todos los grupos principales de ransomware.

X @ThreatLabzBlog
de investigación de seguridad
de ThreatLabz

Acerca de Zscaler

Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, sólidos y seguros. Zscaler Zero Trust Exchange™ protege a miles de clientes de ciberataques y de la pérdida de datos gracias a la conexión segura de usuarios, dispositivos y aplicaciones ubicados en cualquier lugar. Distribuida en más de 160 centros de datos en todo el mundo, Zero Trust Exchange basada en SASE es la mayor plataforma de seguridad en línea en la nube del mundo. Para obtener más información, visite www.zscaler.com/es.

©2025 Zscaler, Inc. Todos los derechos reservados.



zscaler™ | Zero Trust Everywhere

Acerca de Zscaler

Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, potentes y seguros. La plataforma Zscaler Zero Trust Exchange™ protege a miles de clientes de ciberataques y de pérdidas de datos gracias a la conexión segura de usuarios, dispositivos y aplicaciones ubicados en cualquier lugar. Distribuido en más de 160 centros de datos en todo el mundo, Zero Trust Exchange™ basado en SSE es la mayor plataforma de seguridad en línea en la nube del mundo. Obtenga más información en **zscaler.com/es** o síganos en Twitter **@zscaler**.

©2025 Zscaler, Inc. Todos los derechos reservados Zscaler™ y otras marcas comerciales enumeradas en **zscaler.es/legal/trademarks** son (i) marcas comerciales registradas o marcas de servicio o (ii) marcas comerciales o marcas de servicio de Zscaler, Inc. en los Estados Unidos y/u otros países. Cualquier otra marca registrada es propiedad de sus respectivos dueños.

+1 408.533.0288 **Zscaler, Inc. (Sede) • 120 Holger Way • San José, CA 95134** **zscaler.com/es**

