Informe sobre_ransomware de ThreatLabz 2024

Índice

Resumen ejecutivo_

Los ataques de ransomware han alcanzado nuevos niveles de ambición y audacia durante el año pasado, marcado por un notable aumento de los ataques de extorsión. Además del aumento de los ataques de ransomware, la investigación de ThreatLabz descubrió un **pago de rescate sin precedentes de 75 millones de dolares estadounidenses**, el mayor jamás pagado por una empresa. Esta cantidad es casi el doble del pago de rescate más alto conocido públicamente.[1] Sólo en 2023, los pagos de ransomware superaron los mil millones de dólares, lo que pone de relieve el creciente impacto financiero de estos delitos cibernéticos.

Las tácticas de los autores de amenazas de ransomware se han vuelto cada vez más sofisticadas y audaces. En particular, han superado los límites tradicionales de las corporaciones a las que atacan, llegando incluso a atacar a los hijos de los ejecutivos para provocar rescates más rápidos y mayores.[2] Desde infraestructura crítica[3] y grandes corporaciones[4] hasta pequeñas y medianas empresas, ninguna organización es inmune a encontrarse en el punto de mira de la próxima campaña o evolución de los ataques.

A pesar de que las fuerzas del orden eliminaron a múltiples corredores de acceso inicial en el marco de las operaciones especiales “Operación Endgame” y “Operación Duck Hunt”, muchas de las mayores familias de ransomware activas continúan reagrupándose rápidamente y lanzando nuevos ataques sin apenas perder el ritmo. Desafortunadamente, muchos autores del ransomware están fuera del alcance de las fuerzas del orden, lo que los hace prácticamente inmunes al procesamiento penal. Como se detalla en este informe, los organismos encargados de hacer cumplir la ley han aumentado sus tácticas de presión mediante recompensas monetarias, sanciones, uso de troles y exposición de las personas que ejecutan el ransomware mediante diversas formas de tácticas psicológicas.

Dado que los autores del ransomware evolucionan continuamente en sus tácticas, es fundamental mantenerse al día sobre cómo está cambiando el panorama de amenazas.

El informe sobre ransomware de Zscaler ThreatLabz 2024 ofrece una descripción general del panorama de amenazas de ransomware desde abril de 2023 hasta abril de 2024, y detalla las últimas tendencias, objetivos, familias de ransomware y estrategias de defensa efectivas.

ThreatLabz descubrió que los ataques de ransomware aumentaron un 17,8 % año tras año según los intentos bloqueados en la nube de Zscaler, mientras que los ataques de ransomware identificados a través del análisis de sitios de filtración de datos aumentaron en un 57,8 %. Los objetivos más comunes fueron empresas de los sectores manufacturero, sanitario y tecnológico, poniendo las operaciones e infraestructuras críticas directamente en la línea de ataque.

Los hallazgos presentados en este informe subrayan la necesidad de que las organizaciones prioricen la protección contra la implacable marea de ransomware. Los conocimientos y estrategias del informe sirven como guía crucial para mejorar sus defensas contra el ransomware. Al comprender las últimas tendencias y vulnerabilidades e implementar las mejores prácticas recomendadas, puede reducir significativamente el riesgo de convertirse en víctima de ransomware y proteger mejor los activos y datos críticos de su organización.

[1] Bloomberg, **CNA Financial Paid $40 Million in Ransom After March Cyberattack**, 20 de mayo de 2021.
[2] Business Insider, **Hackers are now targeting the children of corporate executives in ransomware attacks**, 12 de mayo de 2024.
[3] Dark Reading, **Ascension Healthcare Suffers Major Cyberattack**, 10 de mayo de 2024.
[4] CyberScoop, **Boeing confirms attempted $200 million ransomware extortion attempt**, 8 de mayo de 2024.

Principales_ conclusiones

La investigación de Zscaler ThreatLabz descubrió un pago de rescate récord de 75 millones de dólares estadounidenses —el mayor pago de ransomware realizado por una empresa en la historia—casi el doble del pago más alto conocido públicamente.

Los ataques de ransomware bloqueados por la nube Zscaler aumentaron en 17,8 % y el número de empresas extorsionadas en sitios de filtración de datos creció un 57,8 % en el mismo período con respecto al año anterior a pesar de numerosas operaciones policiales, incluida la incautación de infraestructura junto con arrestos, acusaciones penales y sanciones.

Los sectores manufacturero, sanitario y tecnológico fueron los principales objetivos de los ataques de ransomware. Mientras que el sector energético experimentó un aumento interanual del 500 % debido a que la infraestructura crítica y la susceptibilidad a interrupciones operativas lo hacen particularmente atractivo para los ciberdelincuentes.

Estados Unidos sigue siendo el principal objetivo del ransomware, experimentando el 49,95 % de los ataques totales, seguido por el Reino Unido, Alemania, Canadá y Francia.

ThreatLabz identificó 19 nuevas familias de ransomware durante el período de análisis, lo que eleva el número total a 391 desde que comenzó nuestro seguimiento.

Las familias de ransomware más activas fueron **LockBit (22,1 %)**, **BlackCat (también conocido como ALPHV) (9,2 %)** y **8Base (7,9 %)**.

Las vulnerabilidades siguen siendo un vector de ataque de ransomware muy común, lo que pone de manifiesto la importancia de aplicar revisiones oportunas y una gestión unificada de vulnerabilidades, respaldada por una arquitectura de confianza cero para brindar protección incluso cuando las revisiones no están disponibles.

Los ataques de ingeniería social basados en voz se utilizan cada vez más para obtener acceso a redes corporativas, una técnica utilizada por Scattered Spider y el grupo de amenazas Qakbot.

Paisaje de_ransomware: principales tendencias y objetivos

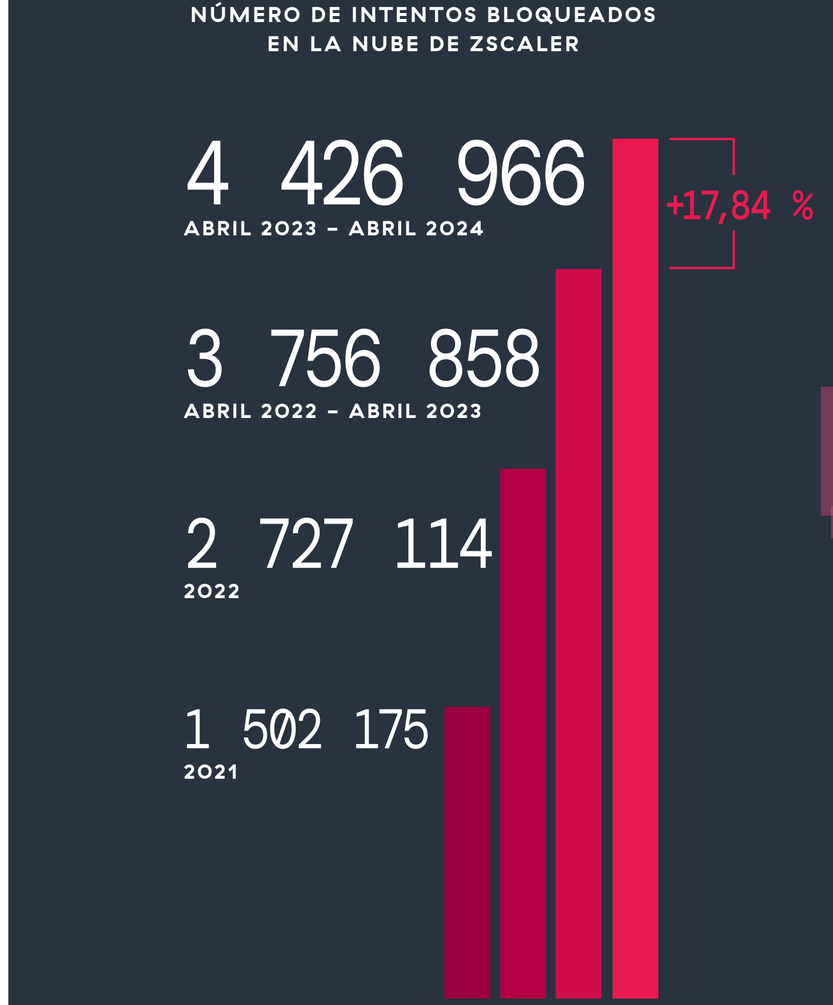
La naturaleza dinámica del ransomware lo ha colocado a la vanguardia de las preocupaciones de seguridad en los últimos años. Los autores de amenazas están evolucionando constantemente sus métodos de ataque y extorsión, aprovechando los avances en la tecnología de inteligencia artificial (IA), el código fuente filtrado y el cifrado avanzado para maximizar su impacto y rentabilidad.

Este informe examina las siguientes tendencias de ataques de ransomware desde abril de 2023 hasta abril de 2024:

- Aumento general de los ataques de ransomware
- Sectores verticales de la industria más afectados por el ransomware
- Distribución geográfica de las organizaciones víctimas
- Mayores medidas policiales contra grupos de ransomware y agentes de acceso inicial
- Principales amenazas de ransomware y pagos de rescate sin precedentes

Aumento general de los ataques de ransomware

El último análisis de ThreatLabz revela una tendencia preocupante, con un aumento interanual del 17,84 % en los ataques de ransomware, datos basados en intentos bloqueados observados en la nube de Zscaler. El aumento de la actividad de ransomware se traduce en importantes interrupciones e impactos financieros para las organizaciones víctimas de todos los tamaños. Estos ataques a menudo interrumpen las operaciones comerciales, provocando tiempos de inactividad prolongados, pérdidas sustanciales de datos y altos costes de recuperación. La carga financiera es considerable; no sólo está en juego una demanda de rescate, sino que la restauración del sistema y el control de daños pueden tener un precio elevado. En vista de estas crecientes amenazas, la necesidad de medidas **potentes de defensa frente al ransomware** nunca ha sido mayor.



Sectores verticales de la industria más afectados por el ransomware

Los ataques de ransomware plantean riesgos importantes para empresas de todos los tamaños y sectores. Estos ataques pueden comprometer datos confidenciales, provocar grandes pérdidas financieras, interrumpir la continuidad del negocio y dañar la reputación. Diferentes sectores industriales se enfrentan a desafíos únicos de ransomware según cómo operan, los datos que manejan y su infraestructura tecnológica.

A pesar de las variables, los ataques de extorsión con ransomware han aumentado constantemente, y el número de empresas que figuran en sitios de filtración de datos aumentó un 57,81 % desde el informe ThreatLabz del año pasado sobre las tendencias del ransomware. La industria manufacturera fue, con diferencia, la más atacada, con 653 ataques, más del doble que cualquier otro sector.

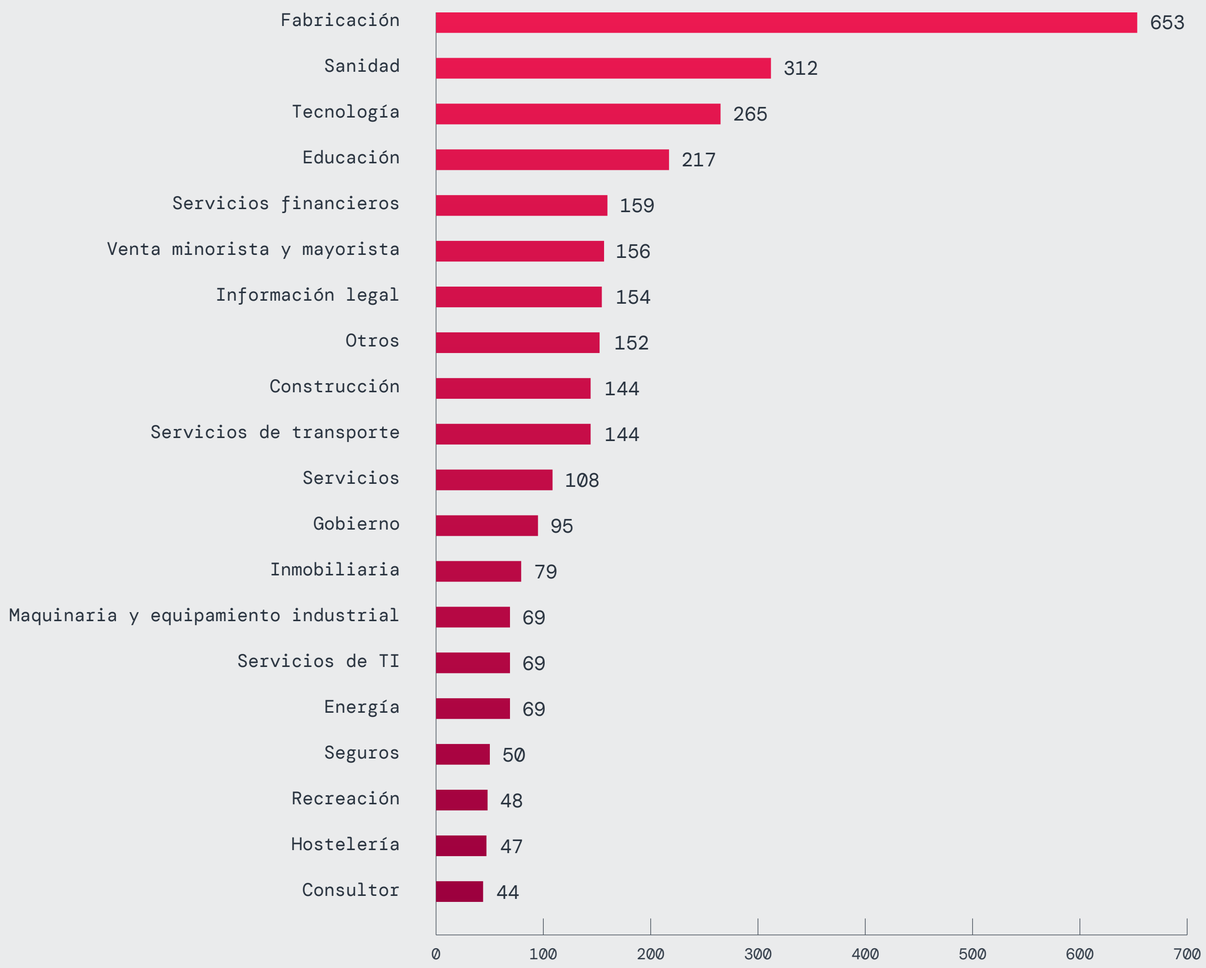


Figura 1: Ataques de ransomware por sector con datos basados en sitios de filtración de datos (sólo los 20 sectores principales).

Tendencias interanuales

El sector energético experimentó un aumento interanual del 527,27 % en los ataques de ransomware, probablemente debido a su naturaleza crítica y al alto potencial de rescate que ofrece a los atacantes.

De manera similar, el sector de restaurantes, bares y servicios de alimentación experimentó un aumento del 333,33 % en este tipo de ataques. Esto puede atribuirse a la rápida digitalización del sector, impulsada por la adopción de sistemas avanzados de punto de venta y plataformas de pedidos en línea. Si bien estas tecnologías pueden agilizar las operaciones y mejorar las experiencias de los clientes, también pueden introducir vulnerabilidades potenciales.

A pesar de que este aumento resalta la prevalencia de los ataques de ransomware, es posible que no capture la magnitud total de los incidentes de ransomware. Muchos ataques no se denuncian o se resuelven de forma privada mediante el pago de un rescate sin divulgación pública. Por lo tanto, estas cifras deben verse como indicativas de tendencias más amplias de ransomware en lugar de una representación integral de todo el panorama de amenazas.

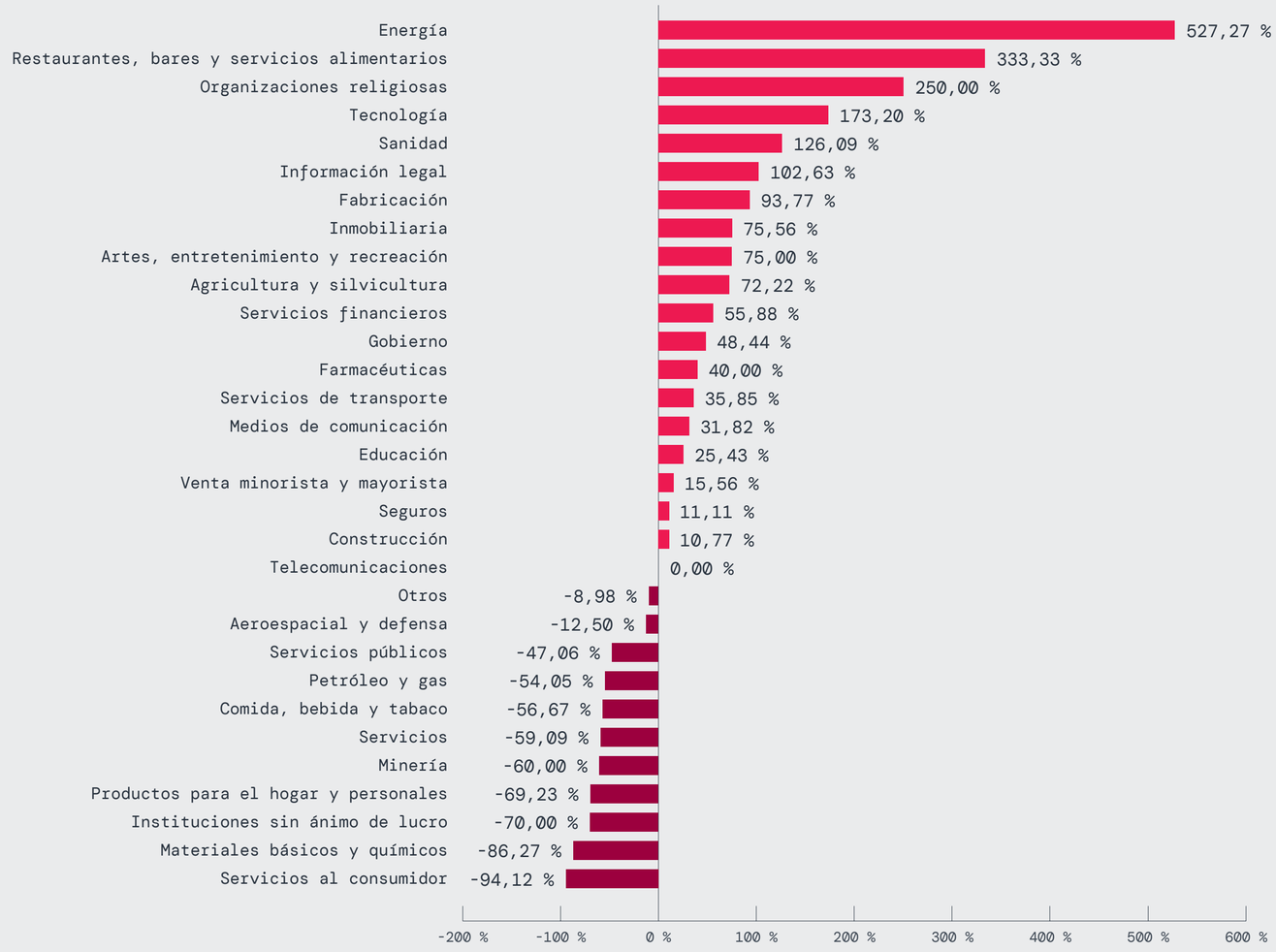


Figura 2: Cambio porcentual año tras año en los ataques de extorsión con ransomware por sector. Tenga en cuenta que algunos sectores tuvieron una base de ataques relativamente baja en el informe del año pasado, lo que hace que su crecimiento parezca más sustancial.

Distribución geográfica de las organizaciones de víctimas

Estados Unidos recibió un volumen notablemente mayor de ataques de ransomware que cualquier otro país con aproximadamente el 50 % de todos los incidentes a nivel mundial. En comparación, el Reino Unido fue el segundo país más atacado, experimentando casi el 6 % de ataques de ransomware, seguido de Alemania (4,09 %), Canadá (3,51 %) y Francia (3,26 %). La Figura 3 muestra un mapa de calor que ilustra los países afectados por extorsiones de rescate entre abril de 2023 y abril de 2024.

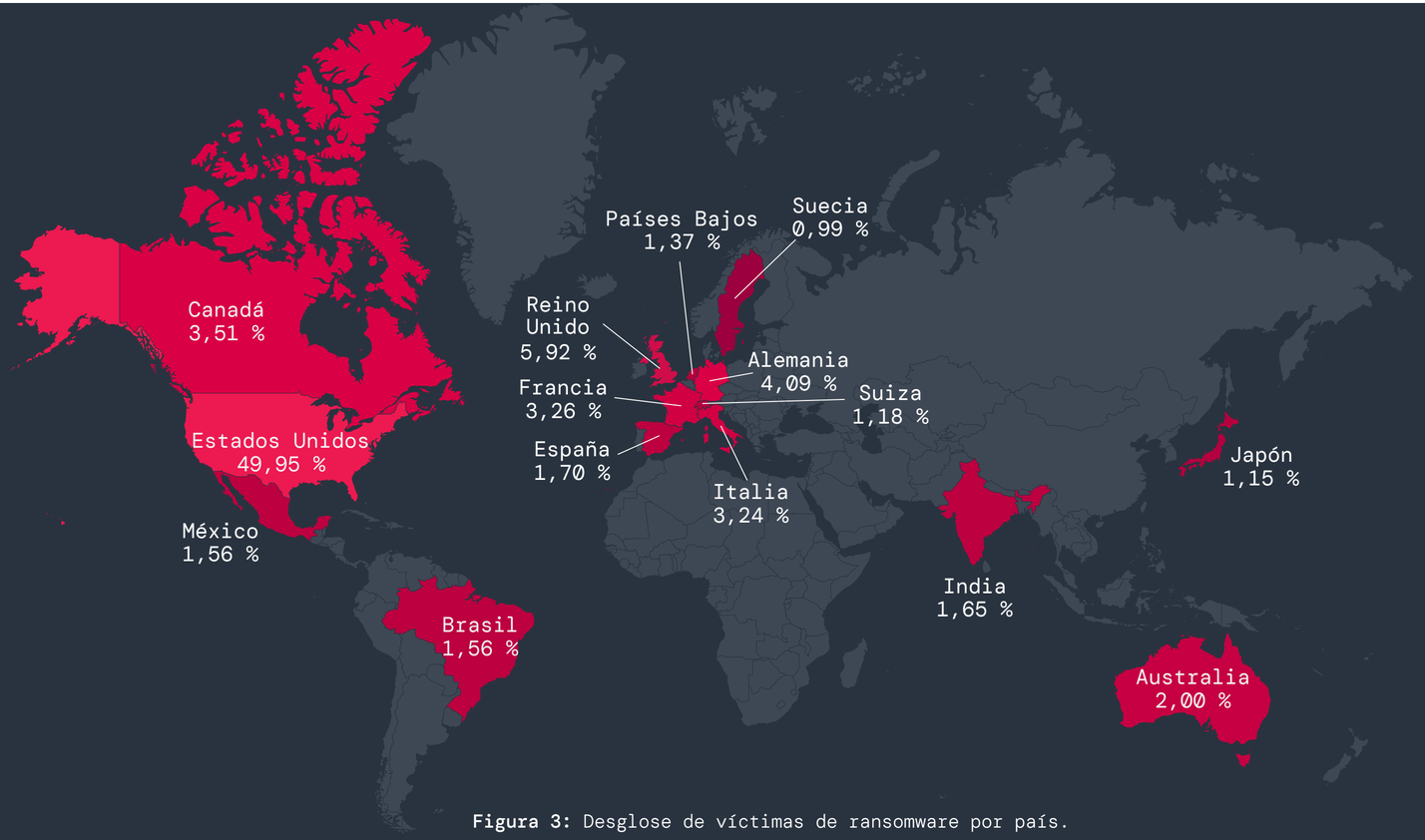


Figura 3: Desglose de víctimas de ransomware por país.

Comprender la distribución de los ataques de ransomware es esencial para la evaluación de riesgos, la asignación de recursos, el desarrollo de políticas, la cooperación internacional y los esfuerzos de concientización pública para combatir las amenazas de ransomware.

Evaluación de riesgos

El análisis de regiones muy atacadas ayuda a las organizaciones de esas áreas a evaluar sus propios niveles de riesgo e implementar una ciberseguridad más potente. En la investigación de ThreatLabz, Estados Unidos representa el 50 % de los ataques globales de ransomware, lo que supone un llamamiento a que las organizaciones dentro de sus fronteras den prioridad a protocolos de seguridad estrictos.

Asignación de recursos

Los datos específicos permiten a los gobiernos y organizaciones asignar recursos estratégicamente, mejorando su postura de seguridad al priorizar el soporte, la financiación y la experiencia en áreas con los niveles de amenaza más altos.

Desarrollo de políticas

Los gobiernos pueden utilizar los conocimientos obtenidos de los ataques regionales de ransomware para fundamentar la legislación, mejorar los estándares de seguridad, promover la cooperación internacional y facilitar el intercambio de información entre los sectores público y privado. Como ejemplo notable reciente, las nuevas reglas de ciberseguridad de la SEC marcan un paso importante para mejorar la transparencia y la rendición de cuentas en medio de amenazas crecientes.

Cooperación internacional

Identificar los países más atacados permite esfuerzos coordinados entre las fuerzas del orden, las organizaciones y los gobiernos para combatir el ransomware a nivel nacional e internacional. La Operación Duck Hunt y la Operación Endgame ejemplifican cómo la cooperación internacional puede interrumpir las actividades cibercriminales.

Conciencia pública

Destacar los países que son objetivos frecuentes puede instar a individuos, organizaciones y gobiernos a tomar medidas más proactivas en lo que respecta a la capacitación en ciberseguridad, la planificación de respuesta a incidentes y la inversión en tecnologías defensivas.

Tendencias interanuales

ThreatLabz comparó los ataques de ransomware del informe de este año con el Informe de ransomware ThreatLabz 2023 para evaluar las tasas de cambio. Entre los 15 países más afectados, Estados Unidos experimentó un notable aumento interanual de 101,88 % y Suecia experimentó un asombroso aumento del 350 %, aunque representó una proporción significativamente menor del total de ataques.

Si bien analizar las tendencias del ransomware a nivel global es indispensable, también es importante examinar los desarrollos específicos en diferentes regiones del mundo. El estudio de los desgloses regionales ayuda a las organizaciones a crear planes de seguridad personalizados y ayuda a los gobiernos a desarrollar políticas de ciberseguridad más efectivas.

CAMBIOS EN LOS ATAQUES DE RANSOMWARE EN LOS 15 PRINCIPALES PAÍSES OBJETIVO

País	Ataques de ransomware por país (2023)	Ataques de ransomware por país (2024)	Cambio porcentual
Estados Unidos de América	902	1,821	101,88 %
Reino Unido	144	216	50,00 %
Alemania	110	149	35,45 %
Canadá	151	128	-15,23 %
Francia	87	119	36,78 %
Italia	63	118	87,30 %
Australia	69	73	5,80 %
Brasil	38	57	50,00 %
España	36	62	72,22 %
México	31	57	83,87 %
Países Bajos	17	50	194,12 %
India	62	60	-3,23 %
Suiza	32	43	34,38 %
Japón	44	42	-4.55 %
Suecia	8	36	350.00 %

Figura 5: Comparación interanual de ataques de ransomware por país.

CAMBIOS EN LAS TASAS DE ATAQUES DE RANSOMWARE EN EMEA

País	Empresas afectadas por ataques de ransomware (2023)	Empresas afectadas por ataques de ransomware (2024)	Cambio porcentual
Reino Unido	144	216	50,00 %
Alemania	110	149	35,45 %
Francia	87	119	36,78 %
Italia	63	118	87,30 %
España	36	62	72,22 %
Países Bajos	17	50	194,12 %
Suiza	32	43	34,38 %
Suecia	8	36	350.00 %
Bélgica	16	34	112,50 %
Sudáfrica	13	24	84,62 %
Austria	15	24	60,00 %
Emiratos Árabes Unidos	12	21	75,00 %

Figura 6: Comparación interanual de ataques de ransomware por país en la región EMEA.

CAMBIOS EN LAS TASAS DE ATAQUES DE RANSOMWARE EN APAC

País	Empresas afectadas por ataques de ransomware (2023)	Empresas afectadas por ataques de ransomware (2024)	Cambio porcentual
Australia	69	73	5,80 %
India	62	60	-3,23 %
Japón	44	42	-4.55 %
Tailandia	13	25	92,31 %
Indonesia	15	23	53,33 %
Malasia	14	20	42,86 %
Taiwan	23	17	-26,09 %
Filipinas	7	16	128,57 %
Singapur	8	16	100,00 %
China	21	15	-28,57 %
Korea del Sur	12	10	-16,67 %
Vietnam	10	10	0,00 %

Figura 7: Comparación interanual de ataques de ransomware por país en la región APAC.

Grupos de ransomware más activos en 2023-2024

LockBit (22,1 %), Black Cat (9,2 %) y 8Base (7,9 %) fueron los grupos de extorsión de ransomware más activos durante el año pasado, cada uno de ellos responsable de una cantidad significativa de ataques. La Figura 8 muestra la cantidad de víctimas de filtración de datos por familia de ransomware durante este período.

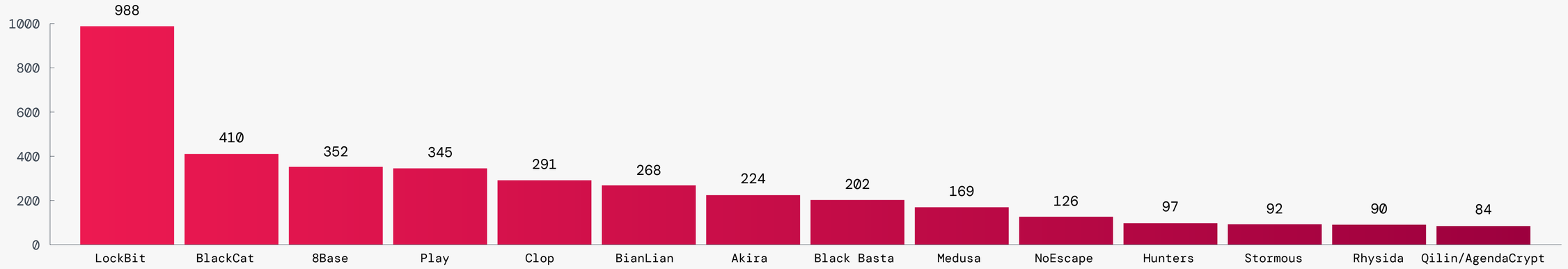


Figura 8: Se revelan ataques de ransomware en sitios web de filtración de datos operados con fines malintencionados.

Los grupos de ransomware más recientes en escena

La Figura 9 muestra una cronología de nuevos grupos de ransomware que comenzaron a publicar datos en sitios de filtración como parte de su estrategia de extorsión.

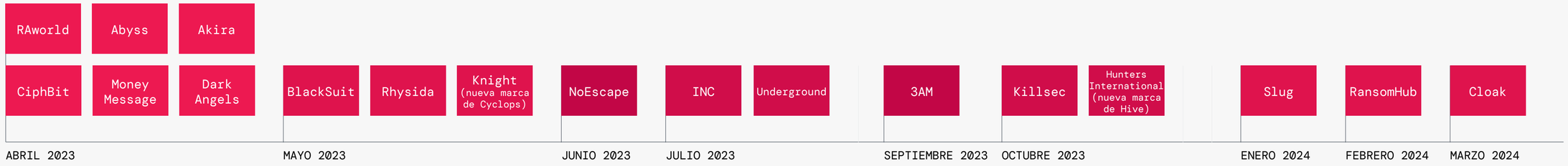


Figura 9: Nuevos grupos de ransomware con sitios de filtración de datos.

Principales vulnerabilidades utilizadas en ataques de ransomware

Las vulnerabilidades en el software, los sistemas y la infraestructura digital en general pueden servir como puntos de entrada críticos para los ataques de ransomware. Las organizaciones deben ser conscientes de estas vulnerabilidades y tomar medidas proactivas para abordarlas.

La Agencia de Ciberseguridad y Seguridad de Infraestructura (CISA) mantiene una lista completa de vulnerabilidades,[5] incluidas aquellas explotadas activamente por grupos de ransomware. Se recomienda encarecidamente que las organizaciones sigan de cerca esta lista y prioricen la mitigación de las vulnerabilidades mencionadas en ella. La gestión proactiva de la vulnerabilidad es esencial para fortalecer la postura general de ciberseguridad de una organización.

En muchos casos, las vulnerabilidades explotadas por los grupos de ransomware afectan los activos conectados a Internet en la superficie de ataque externa de las organizaciones, como puertas de enlace, VPN y otras tecnologías de conectividad remota. Debido a que están orientadas a Internet, estas vulnerabilidades son mucho más fáciles de detectar y explotar para los autores de amenazas. La última guía de CISA[6] enfatiza aún más las vulnerabilidades en las VPN y las soluciones de conectividad remota como puntos críticos de preocupación, y recomienda la adopción de los enfoques más actuales, como la arquitectura de confianza cero, SSE y SASE, que se basan en políticas de control de acceso granular.

Durante el año pasado, destacadas familias de ransomware atacaron y explotaron las vulnerabilidades que se muestran en la figura 10, lo que afectó significativamente a una amplia gama de sistemas.

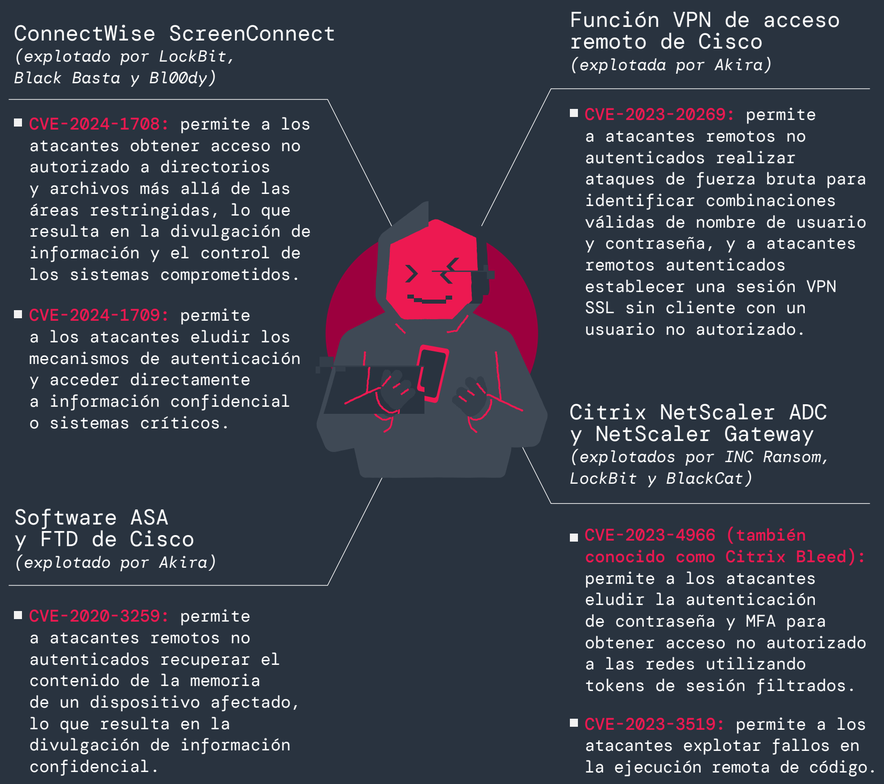


Figura 10: Vulnerabilidades prevalentes entre abril de 2023 y abril de 2024.

Las revisiones disponibles para estas vulnerabilidades deben aplicarse lo antes posible, junto con las siguientes medidas de mitigación:

- Desactive el acceso remoto a servidores
- Utilice contraseñas seguras y autenticación multifactor
- Supervise servidores en busca de actividad sospechosa

[5] Agencia de Ciberseguridad y Seguridad de Infraestructura, **Catálogo de vulnerabilidades explotadas conocidas**, consultado el 25 de junio de 2024.
[6] Agencia de Ciberseguridad y Seguridad de Infraestructura, **Enfoques modernos para la seguridad del acceso a la red**, 18 de junio de 2024.

Resumen de_ransomware: ¿Qué aparece en los titulares?

El ransomware es omnipresente y trasciende los sectores, y cuando un grupo se cierra, otro renace o emerge de nuevo. A continuación se muestran algunas historias recientes que destacan el panorama del ransomware en constante evolución.

La plaga del ransomware en la asistencia sanitaria

La industria de la salud se enfrentó a importantes desafíos a lo largo de 2023 y 2024, ya que fue fuertemente atacada por grupos de ransomware. Las repercusiones de la interrupción de las operaciones de atención médica son graves: se desvían las ambulancias, se retrasan las recetas y es preciso posponer procedimientos médicos esenciales. Además, el robo de datos sanitarios confidenciales puede tener consecuencias de gran alcance, incluido el robo de identidad y el fraude sanitario, lo que exacerba aún más las vulnerabilidades en el ecosistema sanitario.

CONSECUENCIAS IMPREVISTAS DE LOS PAGOS DE RESCATE

Un proveedor de tecnología sanitaria para soluciones de pago fue víctima de un ataque de ransomware orquestado por el grupo BlackCat. A pesar de cumplir con las demandas de los atacantes y pagar una suma asombrosa 22 millones de dólares estadounidesnses de rescate, la terrible experiencia dio un giro inesperado. BlackCat incumplió su promesa de compartir una parte del rescate con el socio que estaba detrás del ataque (la llamada "estafa de salida"), lo que llevó al socio a amenazar al proveedor de atención sanitaria con la divulgación de datos confidenciales.

Este es un claro recordatorio de que el viejo dicho “no hay honor entre los ladrones” es válido para los ataques de ransomware. Incluso si se pagan los rescates, no hay garantía de que el grupo de amenazas no siga publicando o eliminando datos robados. Además, algunas herramientas de descifrado de ransomware contienen errores que impiden la recuperación exitosa de los datos y pueden tardar más en recuperarlos que a partir de una copia de seguridad.

DOBLE EXTORSIÓN, DOBLE VICTIMIZACIÓN

En febrero de 2023, un destacado distribuidor farmacéutico estadounidense confirmó que sus sistemas informáticos se habían visto comprometidos. La infracción afectó a una de las filiales del distribuidor, y los archivos robados fueron filtrados posteriormente por el grupo de ransomware Lorenz.[7] Luego, en febrero de 2024, el mismo distribuidor recibió otro ataque de ransomware.[8] Esto parece ser parte de una tendencia creciente que ThreatLabz ha observado, en la que una empresa ha sido objeto de múltiples incidentes de ransomware en un año.

[7] BleepingComputer, **el distribuidor de medicamentos AmerisourceBergen confirma una infracción de seguridad**, 8 de febrero de 2023.
[8] BleepingComputer, **el gigante farmacéutico Cencora declara que le robaron datos en un ciberataque**, 27 de febrero de 2024.

El impacto del fallo de ciberseguridad de la SEC

En 2023, la SEC introdujo nuevas reglas de divulgación de ciberseguridad para mejorar la transparencia y la responsabilidad entre las empresas que cotizan en bolsa. A partir del 15 de diciembre de 2023, estas reglas exigen la notificación oportuna de incidentes importantes de ciberseguridad y requieren información detallada sobre la gestión, la estrategia y la gobernanza de los riesgos de ciberseguridad de una empresa. Los componentes clave de las resoluciones de la SEC incluyen la incorporación del Artículo 1.05 al 8-K, que requiere informar de los incidentes importantes de ciberseguridad dentro de los cuatro días hábiles posteriores a la determinación de la materialidad por parte de la empresa. Además, el Formulario 10-K ahora exige informes anuales sobre la estrategia y la gestión de riesgos de ciberseguridad, comenzando con los años fiscales que finalizan el 15 de diciembre de 2023 o después. Los emisores privados extranjeros también deben cumplir con comunicaciones comparables en el Formulario 6-K y el Formulario 20-K.

Los fallos presentan un nuevo desafío para los autores de ransomware que ofrecen a las empresas que cotizan en bolsa servicios privados de resolución de pagos, ya que las empresas siguen teniendo que revelar completamente el ataque. En el lado positivo, el nuevo mandato socava los ataques de extorsión sin cifrado, una tendencia emergente mediante la cual los autores de ransomware se basan únicamente en la amenaza de filtrar datos robados para exigir rescates.

CÓMO AFECTAN LAS NUEVAS REGLAS A LAS EMPRESAS

Las normas de ciberseguridad de la SEC pueden plantear serios desafíos para las empresas en términos de cumplimiento y gestión de riesgos. Si bien tienen como objetivo mejorar la transparencia y la protección de los inversores, estas reglas exigen que las empresas cumplan con complejos requisitos de presentación de informes y proporcionen una rápida divulgación de los incidentes importantes.

Un efecto importante es la mayor presión sobre las empresas para cuantificar y evaluar con precisión los incidentes cibernéticos. Determinar la materialidad y el impacto potencial de los incidentes cibernéticos requiere un análisis cuidadoso, que puede ser costoso y puede requerir que las empresas (grandes y pequeñas) reconsideren sus protocolos de respuesta a incidentes y actualicen sus divulgaciones para cumplir con los requisitos de la SEC.

Además, los plazos de cumplimiento varían según el tamaño y el estado de presentación de informes de las empresas, lo que añade otra capa de complejidad. Las empresas más pequeñas que informan a menudo tienen plazos de cumplimiento diferentes y, por lo general, más largos, en comparación con las corporaciones más grandes. Y si bien las corporaciones más grandes deben cumplir con plazos más estrictos, su escala también les brinda más recursos para analizar la materialidad de un incidente de ciberseguridad.

Los nuevos requisitos de divulgación también eliminan la posibilidad de que las empresas públicas paguen rescates silenciosamente sin incurrir en daños a su reputación y la reacción violenta que sigue después de compartir abiertamente información sobre una infracción.

ALGUNAS EMPRESAS YA ESTÁN INFRINGIENDO LAS REGLAS DE LA SEC

A pesar de las claras directrices de la SEC, algunas empresas ya han incumplido con las nuevas normas de ciberseguridad. Las revelaciones recientes de empresas reconocidas han generado preocupaciones sobre el incumplimiento y la idoneidad de sus informes de incidentes.[9] Muchas de estas divulgaciones carecen de "datos cuantitativos y evaluaciones detalladas de las implicaciones financieras y operativas de los incidentes cibernéticos, que es precisamente lo que exige ahora la SEC. Esta tendencia, en la que las empresas proporcionan información deficiente sobre incidentes cibernéticos a pesar del fallo de la SEC, puede requerir una mejor orientación y supervisión regulatoria para garantizar un cumplimiento consistente y efectivo.

Las resoluciones de ciberseguridad de la SEC representan un cambio regulatorio significativo destinado a mejorar la transparencia y la rendición de cuentas en la notificación de incidentes. Adherirse a estas nuevas reglas de manera consistente y de buena fe requerirá una colaboración continua entre los reguladores, las empresas y las partes interesadas de la industria.

[9] Forbes, **algunas empresas ya están incumpliendo las nuevas reglas de divulgación de incidentes de ciberseguridad de la SEC**, 4 de marzo de 2024.

Impacto de las acciones policiales

Qakbot interrumpido por la “Operación Duck Hunt”

El 29 de agosto de 2023, en un esfuerzo multinacional coordinado, la Oficina Federal de Investigaciones (FBI) y el Departamento de Justicia (DOJ) anunciaron la Operación Duck Hunt. Zscaler ThreatLabz brindó importante asistencia técnica a las fuerzas del orden para esta operación.[10] La infraestructura de Qakbot fue diseñada para ser resistente a intentos de eliminación a través de una infraestructura de múltiples niveles, como se muestra en la figura 11.

Esta infraestructura proporcionó varios niveles de resiliencia, y cada nivel requirió un esfuerzo coordinado para desmantelarse. El primer nivel de la infraestructura de Qakbot incluía sistemas infectados que ejecutaban un complemento de supernodo que retransmitía el tráfico a varios servidores proxy diseñados para ocultar el servidor backend maestro de Qakbot.

La Operación Duck Hunt redirigió los servidores proxy ascendentes del supernodo a un conjunto de servidores sumidero para hacerse cargo inmediatamente de la infraestructura de Qakbot, como se muestra en la figura 12.

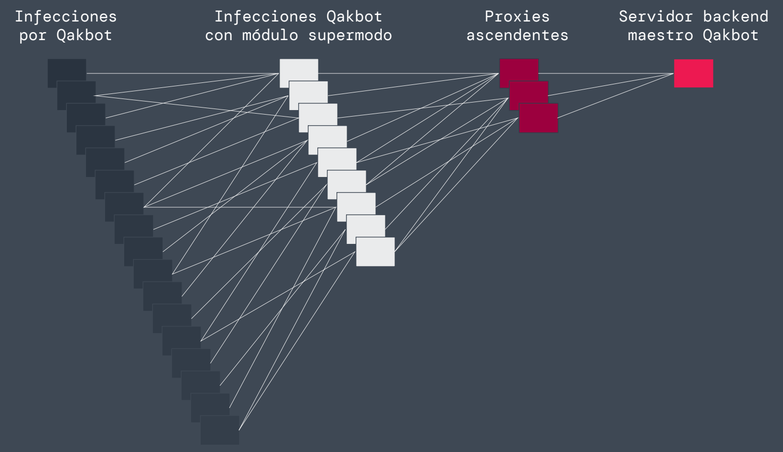


Figura 11: Infraestructura de varios niveles de Qakbot.

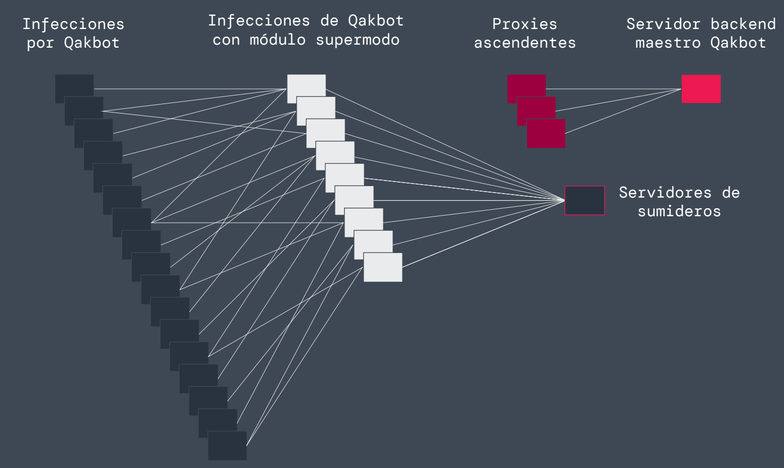


Figura 12: Arquitectura de Qakbot después de redirigir los proxies ascendentes de cada supernodo.

Una vez que el FBI secuestró los supernodos, los servidores del sumidero ordenaron a los ordenadores de las víctimas que descargaran un código shell que cargaba reflexivamente una DLL que neutralizaba el malware. Esto desinfectó con éxito los ordenadores de las víctimas y evitó nuevos ataques.

En el momento de la caída, Qakbot había infectado más de 700 000 ordenadores en todo el mundo, incluidos más de 200 000 solo en los Estados Unidos.[11] Antes de esta operación, Qakbot, originalmente diseñado para facilitar el fraude electrónico y con tarjetas de crédito, estuvo activo durante casi 15 años. En 2019, el grupo pasó a servir como intermediario de acceso inicial para grupos de ransomware, incluidos Conti, ProLock, Egregor, REvil, MegaCortex y Black Basta.

El malware Qakbot normalmente se distribuía a través de correos electrónicos no deseados que contenían archivos adjuntos o enlaces maliciosos. Una vez infectado, se implementaba Cobalt Strike con frecuencia para el movimiento lateral y el eventual despliegue de ransomware.

Desafortunadamente, no hubo arrestos ni acusaciones abiertas contra ninguno de los ciberdelincuentes y Qakbot resurgió en diciembre de 2023. El grupo actualizó el malware para que admitiera versiones de 64 bits de Windows, cambió el formato de configuración interna y modificó la comunicación de red para utilizar cifrado AES. Como veremos más adelante en el informe, el autor de amenazas Qakbot ha cambiado significativamente sus TTP desde la Operación Duck Hunt.

[10] Departamento de Justicia de EE. UU., **Malware Qakbot interceptado en un esfuerzo cibernético internacional**, 29 de agosto de 2023.

[11] TechCrunch, **Cómo el FBI derribó la famosa botnet Qakbot**, 1 de septiembre de 2023.

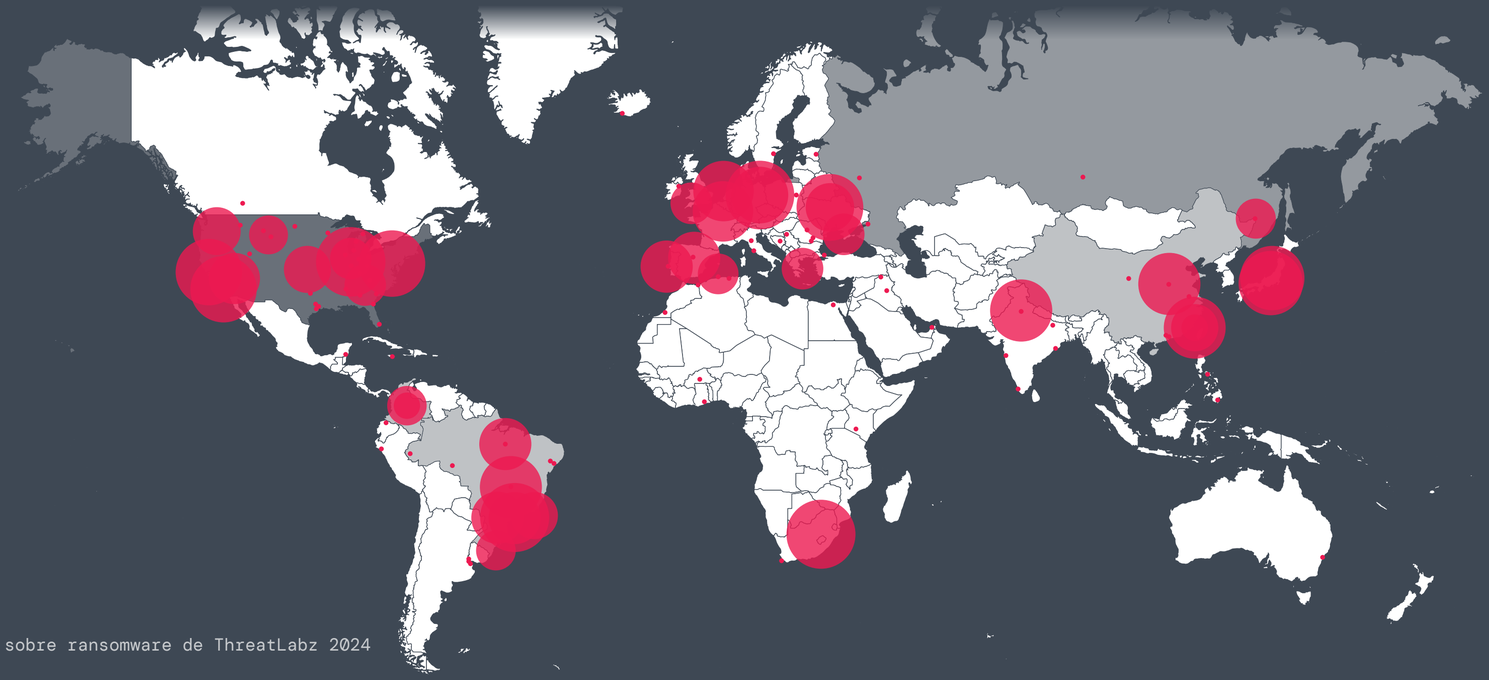
La “Operación Endgame” se dirigía simultáneamente a múltiples intermediarios de acceso inicial

El 28 de mayo de 2024, en colaboración con numerosos organismos internacionales encargados de hacer cumplir la ley, Europol anunció la Operación Endgame, dirigida simultáneamente a múltiples intermediarios de acceso inicial. Esto provocó más de una docena de búsquedas globales, varios arrestos y el cierre de más de 100 servidores utilizados para actividades delictivas. Estos servidores eran parte integral de las operaciones de varios descargadores de malware (también conocidos como "cargadores") que se habían utilizado para infiltrarse en los ordenadores de las víctimas, implementando software malicioso, incluido ransomware.

Las familias de malware objetivo de esta operación fueron responsables de infectar millones de ordenadores en todo el mundo, incluso en instalaciones de asistencia sanitaria y servicios de infraestructura crítica. Como parte de la operación, se tomaron medidas contra SmokeLoader, Pikabot, Bumblebee e IcedID.

Zscaler ThreatLabz brindó asistencia técnica crítica para el sumidero SmokeLoader de la Operación Endgame y los esfuerzos de corrección.

SmokeLoader, activo desde 2011, fue utilizado por varios intermediarios de acceso inicial para ransomware, incluidos Raspberry Robin y la banda de ransomware Stop (también conocido como DJVU). Operation Endgame se apoderó de más de 1000 dominios de SmokeLoader utilizados por estos grupos de amenazas. Posteriormente, se redirigieron los dominios a un servidor sumidero controlado por las fuerzas del orden. El mapa de la figura 13 muestra los sistemas infectados que se comunicaron con el sumidero de SmokeLoader.



Este mapa muestra el impacto de gran alcance que tuvo SmokeLoader en todo el mundo, con infecciones significativas en América Latina, Asia, América del Norte y Europa.

Figura 13: Mapa de infecciones de SmokeLoader que se comunican con el sumidero de Operación Endgame. (Fuente: Zscaler ThreatLabZ)

Cuando los sistemas infectados con SmokeLoader se conectaban al servidor del sumidero, recibían el comando de desinstalación integrado del malware. Hasta la fecha, se han limpiado más de 40 000 sistemas infectados con SmokeLoader, como se muestra en la figura 14.

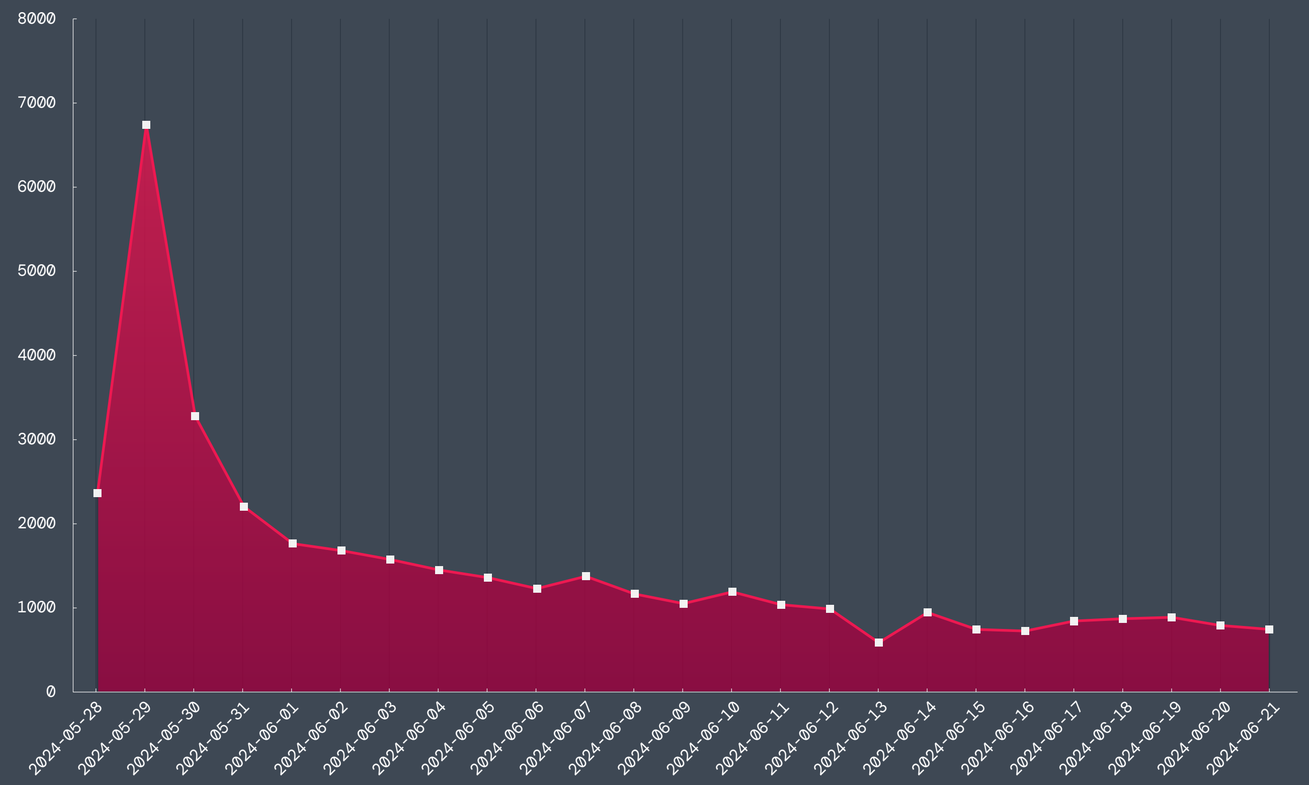


Figura 14: Sistemas SmokeLoader limpiados por Operation Endgame.

Pikabot surgió originalmente a principios de 2023 y exhibió una actividad significativa en la segunda mitad del año. Este aumento se debió a que el malware se convirtió en el intermediario de acceso inicial elegido para el ransomware Black Basta después de que la Operación Duck Hunt interrumpiera Qakbot. En febrero de 2024, **Pikabot resurgió con cambios significativos** en la estructura y la base de su código. ThreatLabz observó a Pikabot implementando regularmente **Cobalt Strike** y Meterpreter **de Metasploit**.

Bumblebee se presentó en marzo de 2022 y tenía vínculos con el antiguo grupo de ransomware Conti. El malware fue el sucesor de la herramienta de malware BazarLoader del grupo, que utilizaron para el acceso inicial a los ataques de ransomware Conti y Diavol. ThreatLabz observó con frecuencia que tanto BazarLoader como Bumblebee desplegaban cargas útiles de Cobalt Strike para movimiento lateral. Bumblebee también se ha asociado con los ataques de ransomware Akira y Black Basta.

Al igual que Qakbot, IcedID se diseñó originalmente como un troyano bancario cuando apareció en 2017. Sin embargo, más tarde el grupo cambió su enfoque para servir como intermediario de acceso inicial para ransomware. A lo largo de los años, el código de malware de IcedID se ha bifurcado y modificado para diversos fines. Además, los mismos desarrolladores crearon un nuevo cargador de malware conocido como Latrodectus, lanzado en noviembre de 2023, que probablemente también se utilizó para implementar ransomware.

Después de la Operación Endgame, ha habido una actividad mínima para la mayoría de estos intermediarios de acceso inicial **con la excepción de Latrodectus**, que resurgió en menos de un mes. Sin embargo, es probable que la pausa sea de corta duración a medida que los autores de la amenaza se reagrupen.

El ransomware Hive renace como Hunters International

En enero de 2023, se cerró la infraestructura del grupo de ransomware Hive. Después de una operación encubierta de siete meses, el FBI se infiltró con éxito en los servidores de Hive y recuperó más de 300 claves de descifrado que impidieron aproximadamente 130 millones de dólares estadounidenses en pagos de rescate. En funcionamiento desde junio de 2021, el colectivo Hive apuntó y atacó a más de 1500 organizaciones en todo el mundo, acumulando más de 100 millones de dólares estadounidenses en pagos de rescate.[12] Las víctimas incluyeron hospitales, distritos escolares, instituciones financieras y varias otras entidades. Sin embargo, no se realizaron arrestos asociados con Hive y el grupo pasó a llamarse Hunters International en octubre de 2023. Los ciberdelincuentes suelen utilizar esta estrategia de cambio de marca después de una interrupción importante.

El grupo hizo un cambio notable en su operación: ya no ofrecerán descuentos ni negociarán con las víctimas a partir de la demanda inicial de rescate, como se muestra en la figura 15.

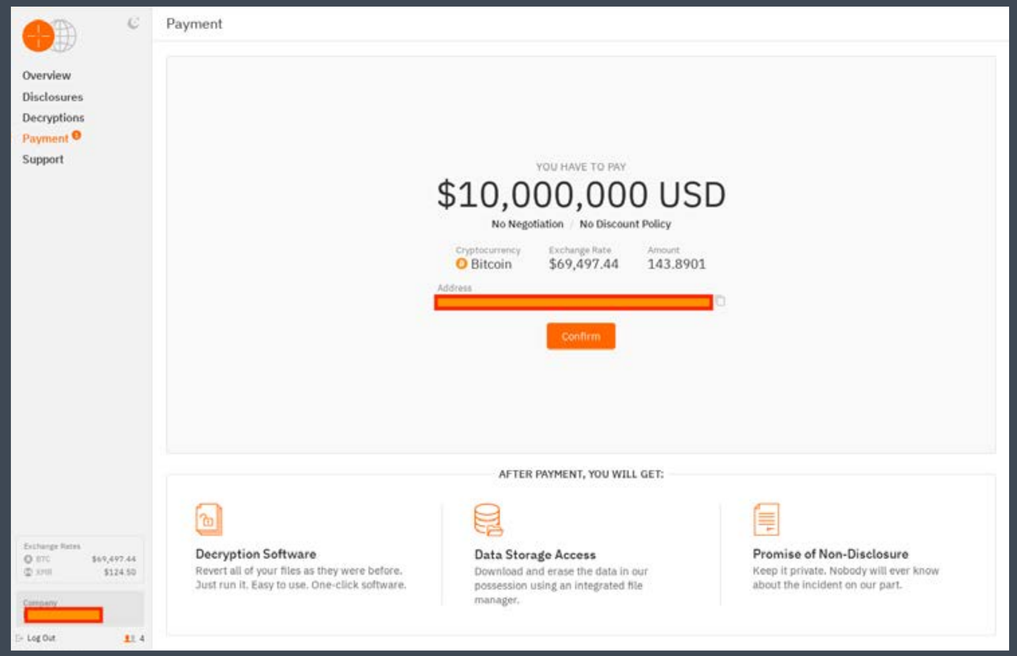


Figura 15: Portal de víctimas de Hunters International sin descuentos ni negociaciones de precios.

La política de precios no negociables es **muy poco común** entre los grupos de ransomware, que frecuentemente ofrecen importantes descuentos sobre la demanda de rescate original. Esta decisión del equipo de Hunters probablemente conducirá a un volumen de pago general más bajo, pero a montos de pago generales más altos.

Hunters International continúa lanzando nuevos ataques y es probable que siga siendo una amenaza formidable sin más arrestos ni acusaciones penales.

[12] Departamento de Justicia de EE. UU., **el Departamento de Justicia de EE. UU. desmantela una variante del ransomware Hive**, 26 de enero de 2023.

Las 5 principales familias de ransomware a tener en cuenta en 2024-2025

A medida que el ransomware y otras ciberamenazas continúan evolucionando en complejidad y sofisticación, mantenerse informado sobre las familias de ransomware más frecuentes y peligrosas es crucial para mantener una postura de seguridad eficaz. Esta sección destaca cinco familias de ransomware que plantean algunos de los riesgos más importantes para las empresas y proporciona información sobre sus tácticas, impacto potencial y actividad reciente.

Nº1 Dark Angels

El grupo de ransomware Dark Angels, que opera el sitio de filtración de datos Dunghill, surgió alrededor de mayo de 2022. El grupo ha llevado a cabo algunos de los mayores ataques de ransomware, pero ha logrado atraer muy poca atención. A principios de 2024, ThreatLabz descubrió una víctima que pagó a Dark Angels 75 millones de dólares estadounidenses, más que cualquier otra cantidad conocida públicamente, un logro que seguramente atraerá el interés de otros atacantes que buscan replicar tal éxito adoptando sus tácticas clave (que describimos a continuación). Dark Angels se dirige a diversos sectores, incluidos la asistencia sanitaria, el gobierno, las finanzas y la educación. Más recientemente, se les ha observado lanzando ataques contra grandes empresas industriales, tecnológicas y de telecomunicaciones.

El grupo Dark Angels emplea un enfoque muy específico, normalmente atacando a una sola gran empresa a la vez. Esto contrasta marcadamente con la mayoría de los grupos de ransomware, que atacan a las víctimas de forma indiscriminada y subcontratan la mayor parte del ataque a redes afiliadas de intermediarios de acceso inicial y equipos de pruebas de penetración. Una vez que Dark Angels han identificado y comprometido un objetivo, deciden selectivamente si cifran los archivos de la empresa. En la mayoría de los casos, el grupo Dark Angels roba una gran cantidad de información, normalmente entre 1 y 10 TB. Para las grandes empresas, el grupo ha extraído entre 10 y 100 TB de datos, cuya transferencia puede tardar de días a semanas.

El ataque de más alto perfil realizado por Dark Angels se produjo en septiembre de 2023, cuando el grupo irrumpió en un conglomerado internacional que ofrece soluciones para sistemas de automatización de edificios, entre otros servicios. Dark Angels exigió 51 millones de dólares estadounidenses de rescate, afirmó haber robado más de 27 TB de datos corporativos y cifrado las máquinas virtuales VMware ESXi de la empresa. Se utilizó una variante del ransomware RagnarLocker para cifrar los archivos de la empresa durante el ataque. La relación entre RagnarLocker y Dark Angels no está clara, pero el grupo ya usaba el ransomware antes de la acción policial contra RagnarLocker,[13] que resultó en el arresto de un miembro clave en octubre de 2023. Hay que tener en cuenta que cuando Dark Angels apareció por primera vez, implementó una variante de Babuk antes de cambiar a RagnarLocker.

La estrategia del grupo de ransomware Dark Angels de atacar a un pequeño número de empresas de alto valor para obtener grandes pagos es una tendencia que vale la pena supervisar. Zscaler ThreatLabz predice que otros grupos de ransomware tomarán nota del éxito de Dark Angels y pueden adoptar tácticas similares, centrándose en objetivos de alto valor y aumentando la importancia del robo de datos para maximizar sus ganancias financieras.

[13] Europol, **la banda de ransomware Ragnar Locker derribada por una redada policial internacional**, 20 de octubre de 2023.

Nº 2 LockBit

LockBit surgió por primera vez en septiembre de 2019 y rápidamente saltó a la fama gracias a la gran red de afiliados de ransomware del grupo. LockBit aprovecha una gran red de afiliados para realizar infracciones, filtrar datos e implementar su ransomware. La infiltración suele comenzar a través de correos electrónicos no deseados que contienen archivos adjuntos o enlaces maliciosos. Otros métodos incluyen la ejecución de ataques de fuerza bruta a contraseñas dirigidos al Protocolo de escritorio remoto (RDP) o credenciales VPN, la compra de credenciales robadas comprometidas a través de intermediarios de acceso inicial y la explotación de aplicaciones públicas. La red cibercriminal de LockBit ha atacado a sectores críticos como la fabricación, la asistencia sanitaria y la logística. El grupo ha atacado colectivamente a más de 2000 sistemas en todo el mundo y extorsionado más de 120 millones de dólares estadounidenses a sus víctimas.

Durante el último año, LockBit se ha mantenido en la cima en términos de volumen de ataques. Utilizando una estrategia marcadamente diferente a la de Dark Angels, el grupo LockBit alienta a sus afiliados a atacar tantas organizaciones como sea posible, independientemente de la recompensa potencial. Este gran volumen de ataques a menudo resulta en que las pequeñas empresas sean objeto de demandas de rescate relativamente bajas.

LockBit ransomware se implementa en sistemas basados en Windows y Linux. Hay tres versiones de LockBit para Windows: LockBit Red (el original), LockBit Black (basado en el código fuente de BlackMatter) y LockBit Green (basado en el código fuente de Conti filtrado). Como se menciona en el **Informe de ransomware ThreatLabz 2023**, el constructor LockBit Black se filtró y muchos grupos de ciberdelincuentes no afiliados a LockBit lo han utilizado para sus propios ataques de ransomware. Curiosamente, LockBit Black sigue siendo la variante más utilizada por el grupo. La variante específica del ransomware LockBit utilizada para cifrar los archivos de una víctima ahora se muestra en la nota de rescate junto al ID de la víctima. Esto permite al autor de amenazas que realiza el ataque identificar fácilmente la variante LockBit implementada para ayudarle a proporcionar la herramienta de descifrado adecuada cuando se paga un rescate. Consulte la figura 16 para ver un ejemplo de una nota de rescate reciente de LockBit Black.

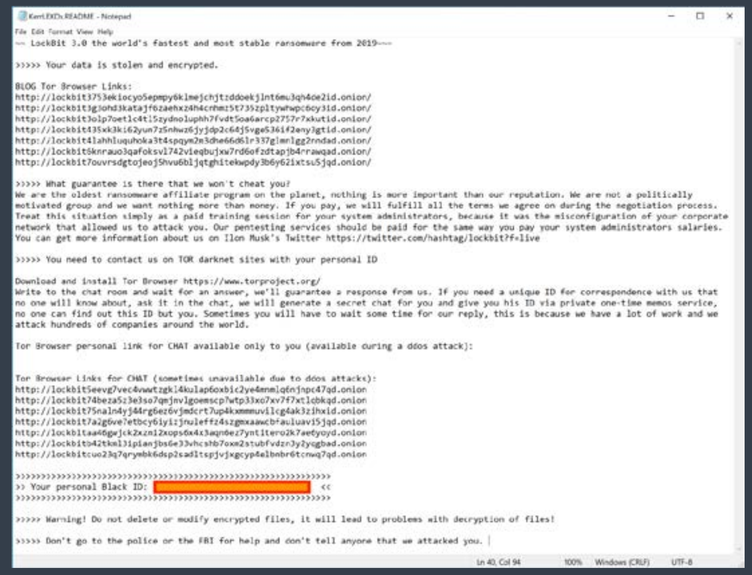


Figura 16: Ejemplo de una nota de rescate reciente de LockBit Black.

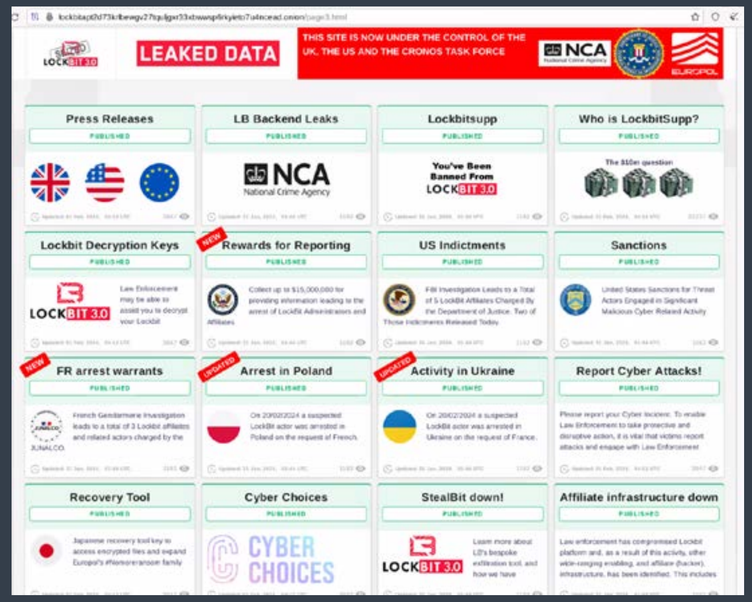


Figura 17: Incautación por parte de las fuerzas del orden del sitio de filtración de datos de LockBit.

El 20 de febrero de 2024, el FBI y las fuerzas del orden del Reino Unido confiscaron partes de la infraestructura de LockBit, que incluían aproximadamente 7000 claves de descifrado de víctimas. Después de la incautación, las fuerzas del orden se apoderaron del sitio web de filtración de datos LockBit y se burlaron de los ciberdelincuentes con una interpretación similar del sitio anterior que mostraba varios artículos y temporizadores de cuenta regresiva hasta que se publicara nueva información, como se muestra en la figura 17 a continuación.

Desafortunadamente, a los pocos días de la caída, **ThreatLabz identificó nuevos ataques de ransomware** perpetrados por LockBit y un nuevo sitio de filtración de datos. El grupo se ha mantenido activo y ha atacado a docenas de nuevas entidades desde la acción policial.

El 7 de mayo de 2024, el FBI anunció la acusación contra el desarrollador y operador de LockBit, Dmitry Yuryevich Khoroshev. Sin embargo, el operador de LockBit rápidamente negó que el FBI lo hubiera identificado correctamente. Sin más arrestos, los ataques de LockBit probablemente continuarán en el futuro previsible, aunque en algún momento ThreatLabz espera que la marca LockBit se retire y la operación resucite con otro nombre debido almayor control al que está sometido.

Nº 3 BlackCat

El ransomware BlackCat (también conocido como ALPHV) introducido en noviembre de 2021, fue una de las amenazas más notorias hasta que se cerró en marzo de 2024. Al igual que LockBit, BlackCat aprovechaba una red de afiliados para lanzar ataques y compartía un porcentaje de los pagos del rescate.

Podría decirse que el socio de BlackCat más infame es un grupo conocido como Scattered Spider[14] (también conocido como Star Fraud). Compuesto por miembros de habla inglesa, este grupo es muy eficaz en ataques de ingeniería social, a menudo haciéndose pasar por personal de TI o de soporte técnico en llamadas de voz y llevando a cabo ataques de intercambio de SIM para anular la autenticación multifactor. El 15 de junio de 2024, el presunto cabecilla[15] de Scattered Spider, un ciudadano británico de 22 años, fue arrestado. Sin embargo, es demasiado pronto para decir qué impacto tendrá este arresto en la capacidad del grupo para continuar sus ataques.

BlackCat era una de las familias de ransomware más compatibles con varias plataformas, en parte porque utiliza el lenguaje de programación Rust. La Figura 18 muestra las herramientas de descifrado disponibles para todas las plataformas compatibles con el ransomware BlackCat justo antes de que el grupo cerrara sus operaciones. Las plataformas incluían Windows, ESXi, FreeBSD y numerosas variantes de arquitecturas y sistemas operativos Linux, como ARM, x86/x64 y PowerPC.

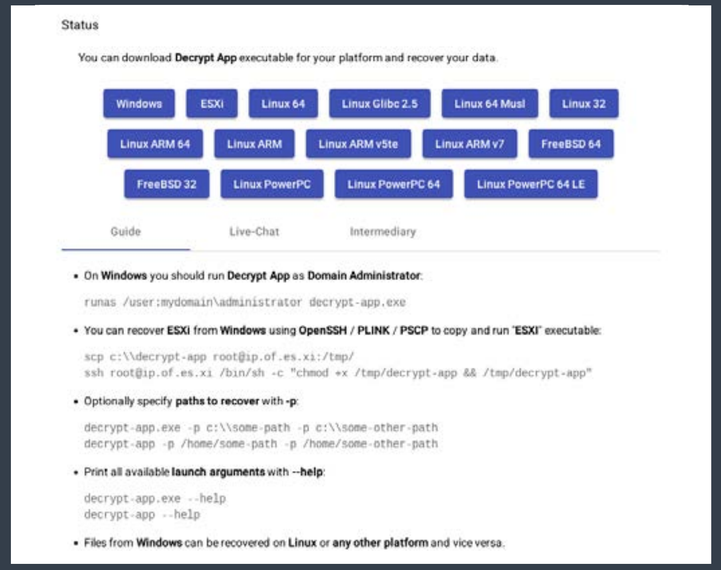


Figura 18: Se proporcionaron herramientas de descifrado de BlackCat para 15 sistemas operativos, arquitecturas y plataformas diferentes.

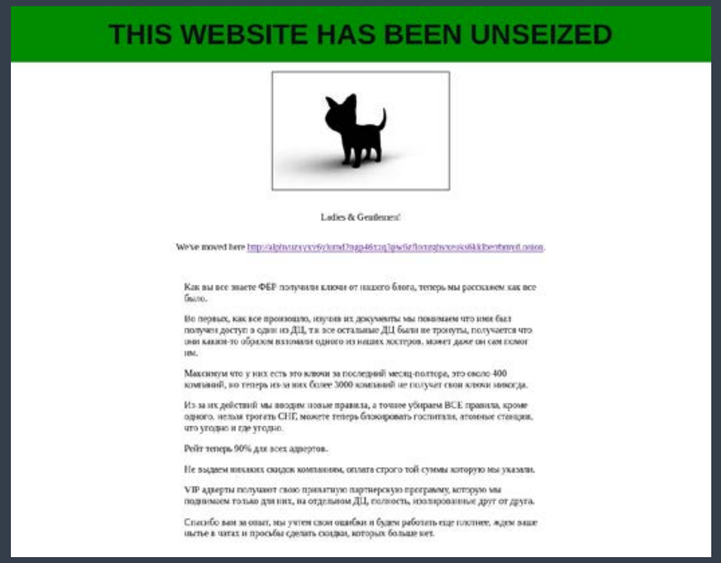


Figura 19: Sitio de filtración de datos "no incautados" de BlackCat después de una acción policial.

Este nivel de compilación multiplataforma es inusual en comparación con otras familias de ransomware que normalmente sólo admiten Windows, ESXi y una pequeña cantidad de plataformas basadas en Linux. Esto indica que es posible que los socios de BlackCat hayan solicitado soporte para plataformas adicionales a fin de cifrar archivos en tantos sistemas como sea posible.

En diciembre de 2023, el FBI obtuvo acceso a parte de la infraestructura de BlackCat. El FBI intentó apoderarse de los sitios web del grupo basados en Tor, incluidos los portales de negociación de rescates y los sitios de filtración de datos. Sin embargo, en un rápido giro de los acontecimientos, BlackCat publicó un mensaje indicando que habían "desmantelado" el sitio web de filtración de datos y proporcionó un enlace a un nuevo sitio web de filtración de datos que el FBI no pudo manipular, como se muestra en la figura 19 a continuación.

Este tira y afloja entre el FBI y BlackCat se produjo durante unos días hasta que BlackCat consideró que el nuevo sitio de filtración de datos estaba suficientemente publicitado. Tenga en cuenta que "apoderarse" de un sitio web basado en Tor no es tan trivial como un sitio web tradicional basado en DNS porque depende de secretos criptográficos en lugar de una autoridad central sujeta a órdenes judiciales.

En marzo de 2024, el grupo BlackCat anunció su disolución, argumentando que su infraestructura se había visto comprometida por parte del FBI, lo que supuestamente les impedía continuar con sus operaciones. Sin embargo, surgieron sospechas debido a que el momento de su cierre se produjo inmediatamente después de recibir un rescate por valor de 22 millones de dólares estadounidenses y luego realizar una estafa de salida a un socio que los ayudó a atacara un proveedor de asistencia sanitaria (comentado anteriormente en este informe).

Si bien el ransomware BlackCat ya no está activo, los socios que estaban detrás de los ataques del grupo probablemente hayan migrado a otras redes de ransomware como servicio como RansomHub (donde los datos robados del proveedor de asistencia sanitaria que pagó el rescate de 22 millones de dólares se ha filtrado desde entonces). Además, es poco probable que el propio grupo de ransomware BlackCat haya cesado realmente sus operaciones y probablemente resurja bajo una nueva marca.

[14] Agencia de Ciberseguridad y Seguridad de Infraestructuras, **Aviso de ciberseguridad: Scattered Spider**, 16 de noviembre de 2023.
[15] Krebs sobre seguridad, **presunto jefe del grupo de piratería 'Scattered Spider' arrestado**, 15 de junio de 2024.

Nº 4 Akira

El ransomware Akira irrumpió en escena en abril de 2023 y rápidamente se convirtió en tristemente famoso por el volumen de ataques realizados por sus socios. El grupo de amenazas Akira es probablemente otra rama del desaparecido grupo Conti. De hecho, el código del ransomware Akira originalmente compartía muchas similitudes con el código fuente filtrado de Conti. Sin embargo, el grupo ha desarrollado más recientemente un ransomware basado en Rust que contiene referencias a personajes de Power Rangers como Megazord.

Los socios del ransomware Akira han empleado varios mecanismos de acceso inicial, incluso mediante la explotación de CVE-2023-20269.[16] También se sabe que el grupo de amenazas que opera Bumblebee, que tiene vínculos con el ransomware Conti, es un intermediario de acceso inicial para Akira. Como se ha mencionado anteriormente en el informe, la Operación Endgame desmanteló Bumblebee pero tuvo un impacto mínimo en las operaciones de Akira.

Para comprender mejor los ataques de Akira, podemos aprender directamente de la información que Akira proporciona a las víctimas que pagan un rescate. ThreatLabz capturó el siguiente mensaje de chat de Akira, que contiene detalles sobre cómo obtuvieron acceso inicialmente a la red de la empresa a través de un intermediario de acceso inicial, y en el que también se ofrecían consejos para prevenir ataques de ransomware en el futuro:

El acceso inicial a su red se compró en la web oscura. Luego se llevó a cabo kerberoasting y obtuvimos hashes de contraseñas. Luego simplemente los eliminamos y obtuvimos la contraseña de administrador del dominio. Al pasar semanas dentro de su red, hemos logrado detectar algunos fallos que recomendamos eliminar:

1. Ninguno de sus empleados debe abrir correos electrónicos sospechosos, enlaces sospechosos ni descargar archivos, y mucho menos ejecutarlos en su ordenador.

2. Utilice contraseñas seguras y cámbielas con la mayor frecuencia posible (al menos 1 o 2 veces al mes). Las contraseñas no deben coincidir ni repetirse en diferentes recursos.

3. Instale 2FA siempre que sea posible.

4. Utilice las últimas versiones de los sistemas operativos, ya que son menos vulnerables a los ataques.

5. Actualice todas las versiones de software.

6. Utilice soluciones antivirus y herramientas de seguimiento del tráfico.

7. Cree un host de salto para su VPN. Utilice credenciales únicas que difieran del dominio uno.

8. Utilice software de respaldo con almacenamiento en la nube que admita una clave token.

9. Instruya a sus empleados con la mayor frecuencia posible sobre las precauciones de seguridad en línea. El punto más vulnerable es el factor humano y la irresponsabilidad de sus empleados, administradores de sistemas, etc. Le deseamos seguridad, tranquilidad y muchos beneficios en el futuro. Gracias por trabajar con nosotros y su actitud cuidadosa hacia su seguridad.

Aunque este consejo proviene directamente de Akira, las recomendaciones son válidas y proporcionan una base para comprender y frustrar tales ataques.

Akira es uno de los únicos grupos importantes de ransomware que no se ha visto interrumpido directamente por las fuerzas del orden. Como resultado, Akira es ahora uno de los grupos de ransomware más activos y probablemente continuará lanzando nuevos ataques durante el próximo año.

[16] https://nvd.nist.gov/vuln/detail/CVE-2023-20269

Nº 5 Black Basta

El ransomware Black Basta, identificado por primera vez en abril de 2022, es otro sucesor del grupo de ransomware Conti. Los socios de Black Basta han empleado diversos métodos para obtener acceso a las redes corporativas. Antes de la Operación Duck Hunt (agosto de 2023), Qakbot era un importante intermediario de acceso inicial para Black Basta. Como se mencionó anteriormente, Pikabot intervino para llenar el vacío después de su caída. Sin embargo, Pikabot se cerró tras la Operación Endgame en mayo de 2024.

Desde entonces, ThreatLabz ha estado rastreando nuevas actividades del grupo de amenazas Qakbot, que ha girado y cambiado significativamente sus TTP. En lugar de utilizar correo electrónico no deseado para infectar sistemas con Qakbot, el grupo de amenazas utiliza actualmente una combinación de técnicas de ingeniería social. En vez de enviar correos electrónicos no deseados a millones de direcciones, el grupo de amenazas realiza ataques dirigidos. Estos ataques comienzan cuando el grupo de amenazas envía correos electrónicos no deseados a una pequeña cantidad de empresas objetivo. Luego, el grupo llama a un empleado de estas empresas haciéndose pasar por su propio departamento de TI. La persona que llama le indica a la víctima que se una a una sesión de pantalla compartida utilizando un software de escritorio remoto como Quick Assist de Microsoft para "actualizar los filtros de spam de la empresa" para el empleado. Una vez que el empleado da acceso al autor de la amenaza, se ejecuta un script por lotes de Windows para realizar reconocimiento, robar credenciales e instalar una puerta trasera en el sistema de la víctima. La puerta trasera sigue cambiando, pero incluye Qakbot, Cobalt Strike y una herramienta proxy SOCKS. El script por lotes contiene una interfaz de línea de comandos similar a la que se muestra en la figura 20.

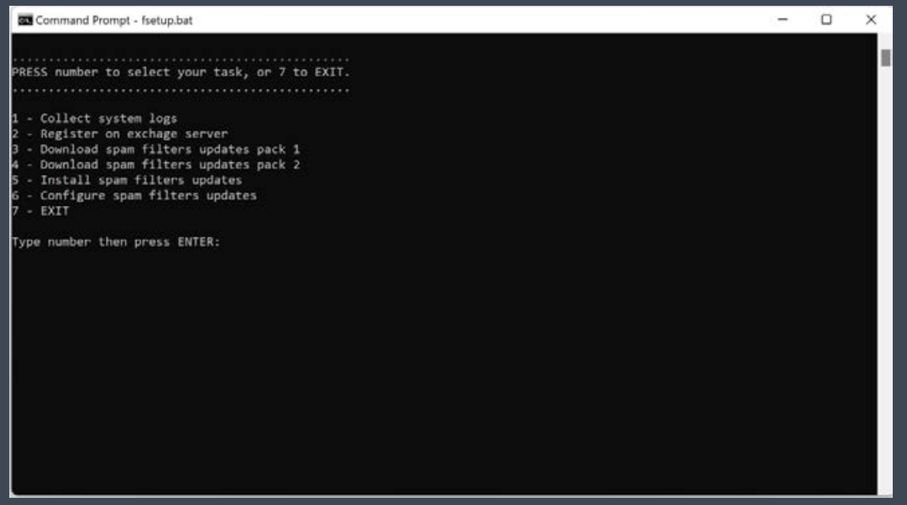


Figura 20: Interfaz de script por lotes malicioso de Windows utilizada para establecer una puerta trasera en el sistema de la víctima como precursor de un ataque de ransomware Black Basta.

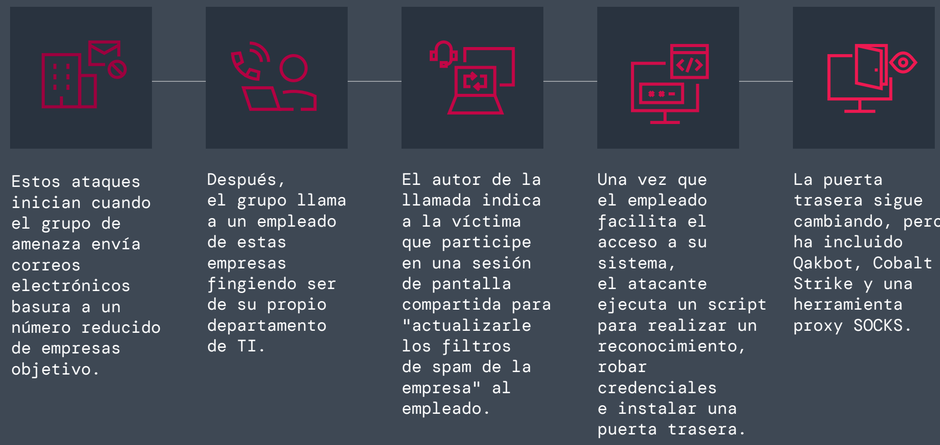


Figura 21: Cadena de ataque del ransomware Black Basta con acceso inicial gestionado por el grupo de amenazas Qakbot.

Una vez que se ha establecido este acceso de puerta trasera, el grupo de amenazas Qakbot cede el acceso a un equipo de pruebas de penetración responsable del movimiento lateral y la implementación final del ransomware Black Basta.

Si bien la Operación Duck Hunt tuvo un impacto significativo a corto plazo, el grupo de amenazas permanece activo y continúa innovando y experimentando con nuevas técnicas para comprometer a las organizaciones. Durante el próximo año, es probable que el grupo de amenazas Qakbot siga siendo un importante intermediario de acceso inicial para ataques de ransomware como Black Basta.

ThreatLabz
Notas de_ransomware
Archivo

Zscaler ThreatLabz ha estado manteniendo un **depósito público en GitHub** que, al momento de escribir este artículo, rastrea 391 familias de ransomware y contiene un total de 945 notas de rescate, habiendo agregado 19 familias y 55 notas de rescate entre abril de 2023 y abril de 2024. Este archivo puede ser valioso para el seguimiento de grupos de ransomware a lo largo del tiempo, incluidos sus sitios web de filtración de datos y tácticas de negociación, y para vincular grupos de ransomware que cambian de marca mediante el uso de análisis estilométrico.

La Figura 22 muestra una comparativa estilométrica entre un chat de rescate de Conti (arriba) y un chat de rescate de Black Basta (abajo). Esto demuestra que es casi seguro que los miembros de Black Basta son ex miembros de Conti, como se desprende de las similitudes en la estructura de sus oraciones, la elección de palabras e incluso instrucciones específicas.

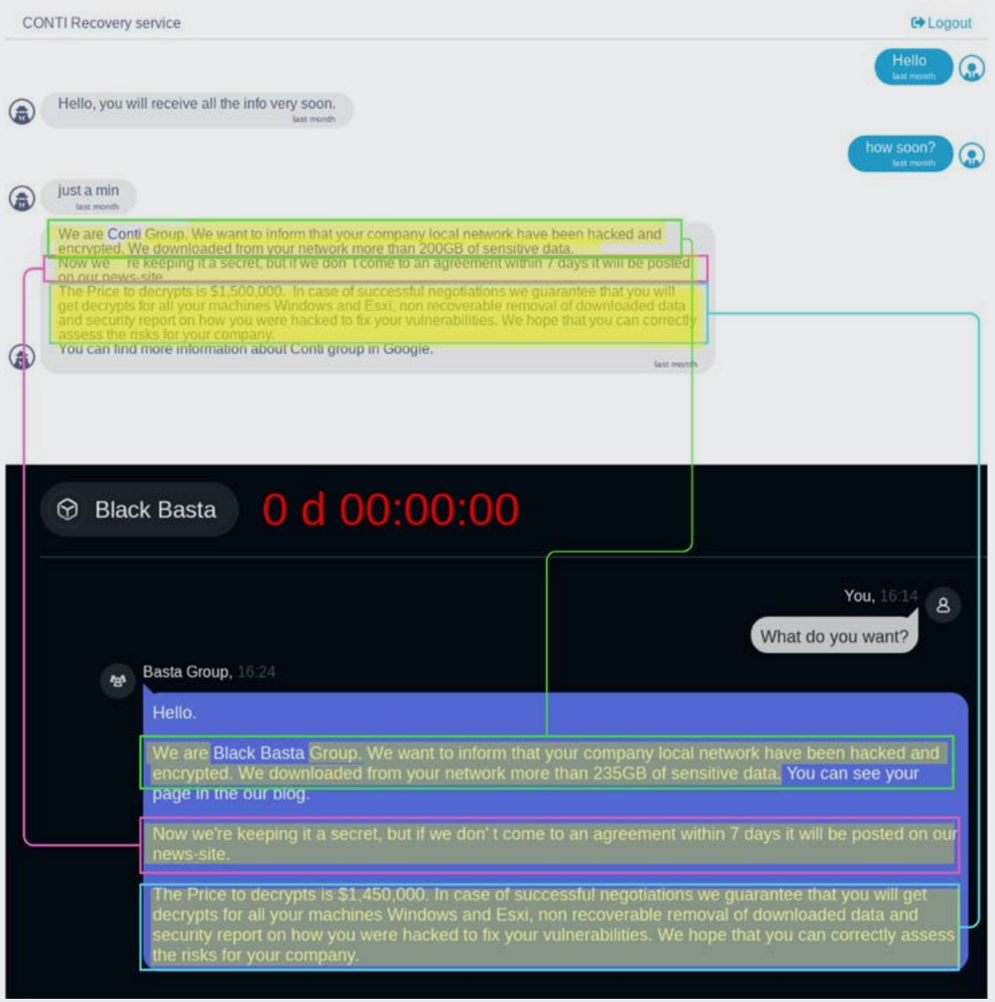


Figura 22: Comparativa estilométrica entre los chats de rescate de Conti (arriba) y Black Basta (abajo).

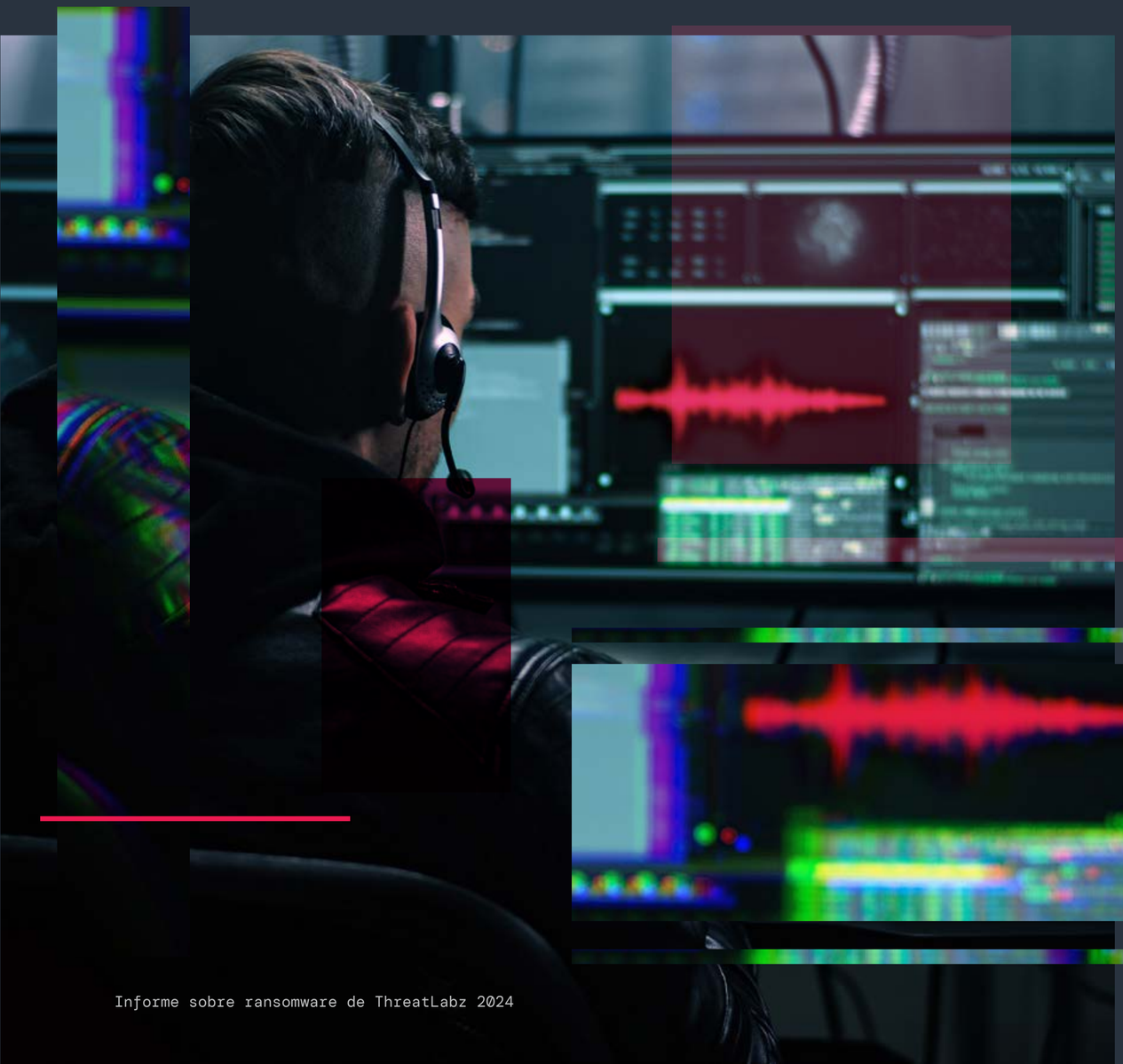
2025_ Predicciones

1. Los autores de amenazas de ransomware adoptarán estrategias de ataque muy específicas.

Durante el último año, Dark Angels ha sido uno de los grupos de ransomware más exitosos y menos conocidos, con una estrategia distinta de atacar a un pequeño número de empresas multimillonarias y extorsionarlas para obtener rescates sustanciales. Esta estrategia tiene un doble propósito: reducir el escrutinio por parte de las autoridades y el sector de la seguridad, y al mismo tiempo gastar más recursos para infiltrarse en grandes empresas que están dispuestas a pagar rescates significativos para proteger enormes volúmenes de datos robados. Esto ha llevado al grupo a recibir el mayor pago de rescate conocido (75 millones de dólares estadounidenses), lo que seguramente atraerá el interés de otros autores de amenazas de ransomware en 2025 que quieran replicar su éxito.

2. Los ataques dirigidos implicarán cada vez más ingeniería social basada en voz.

En 2025, esperamos ver un aumento de los ataques dirigidos facilitados por intermediarios de acceso inicial especializados. Estos intermediarios, ejemplificados por las actividades de Qakbot y Scattered Spider, emplean técnicas sofisticadas para asegurar la entrada, en particular utilizando ataques de ingeniería social basados en voz (“vishing”) para engañar a las personas para que les concedan acceso a un entorno corporativo, que luego se utiliza en última instancia para extraer datos e implementar ransomware. Esta tendencia emergente destaca las colaboraciones dentro del ecosistema cibercriminal y subraya la necesidad de una mayor vigilancia y medidas de seguridad avanzadas para contrarrestar estas amenazas en evolución.



3. Los atacantes de ransomware adoptarán cada vez más la inteligencia artificial generativa para crear campañas más efectivas, personalizadas y localizadas.

La creciente adopción de la IA generativa en 2025 y más allá permitirá a los autores de amenazas crear correos electrónicos no deseados con gramática y ortografía precisas, así como utilizar la clonación de voz para hacerse pasar por el personal y obtener acceso privilegiado. En los próximos años, es posible que las voces generadas por IA se adapten con acentos y dialectos locales para mejorar la credibilidad y aumentar la probabilidad de éxito, y convertirse en un excelente ejemplo de cómo los autores de amenazas de ransomware harán que los ataques sean más convincentes y difíciles de detectar.

4. Se informará de más incidentes de ciberseguridad de acuerdo con las nuevas reglas de la SEC.

Con el fallo de la SEC que exige informes más estrictos sobre incidentes de ciberseguridad, en 2025 se seguirá presenciando un aumento en el número de organizaciones que divulgan incidentes de ransomware. Es de esperar que esto dé como resultado una mayor transparencia y promueva una cultura de responsabilidad y defensas proactivas, impulsando mejoras en las prácticas de ciberseguridad.

5. Los ataques de ransomware de filtración de datos de gran volumen irán en aumento.

Los ataques que filtran grandes cantidades de datos, incluidos más incidentes sin cifrado, aumentarán significativamente en el próximo año. Esta tendencia, que comenzó a ganar impulso en 2022, hace que los autores de amenazas se centren únicamente en extraer datos sin cifrar sistemas. El enfoque permite operaciones oportunistas más rápidas y aprovecha el miedo a que se divulguen datos confidenciales para obligar a las víctimas a pagar rescates. Subraya un cambio continuo en las estrategias de ransomware hacia métodos más eficientes y de alto impacto.

6. Las empresas del sector sanitario, especialmente, seguirán enfrentándose a ataques persistentes por parte de grupos de ransomware.

El alto valor de los datos sanitarios seguirá atrayendo la atención en 2025. Muchas empresas de asistencia médica tardan en reemplazar los sistemas heredados con medidas de seguridad modernas y avanzadas, lo que las hace particularmente vulnerables. Como resultado, es probable que estas organizaciones se enfrenten a infracciones e intentos de extorsión reiterados. Aquellos que no tomen las medidas adecuadas para priorizar las estrategias de defensa de confianza cero pueden verse atacados por grupos de ransomware.

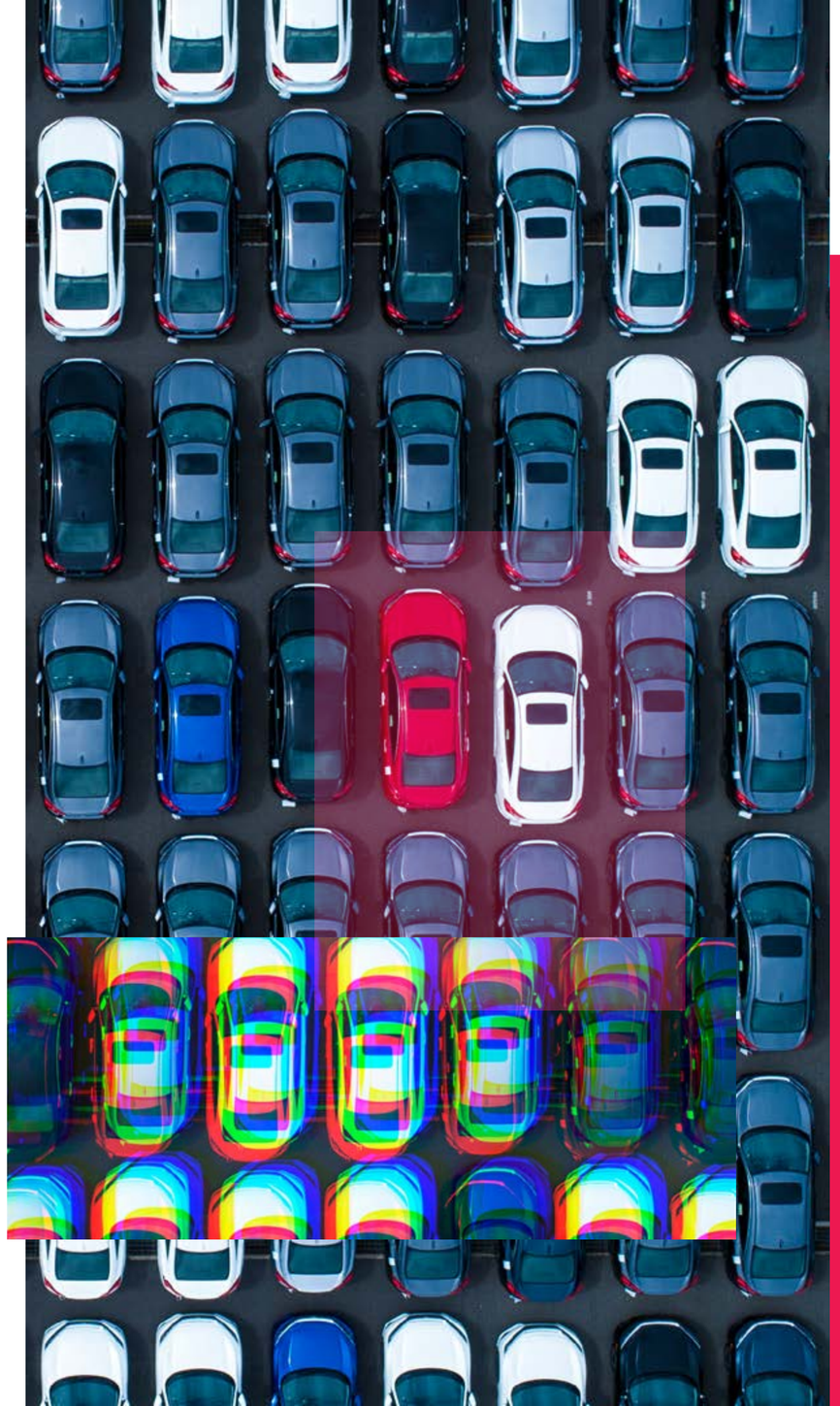
7. La colaboración internacional contra las organizaciones de delitos cibernéticos se basará en los esfuerzos existentes.

Las fuerzas del orden y la industria privada seguirán colaborando en los esfuerzos para combatir los ataques de ransomware, como el bloqueo de los principales intermediarios de acceso inicial y grupos de ransomware. La colaboración internacional será cada vez más vital a medida que crezca la interconexión global, lo que facilitará que los ciberdelincuentes operen a nivel transnacional. Al compartir inteligencia y experiencia, estas acciones coordinadas alterarán de manera más efectiva las redes globales de ransomware. Durante el último año, Zscaler ThreatLabz ha estado a la vanguardia y ha sido fundamental al brindar asistencia técnica para varias de estas operaciones.

Cómo Zscaler simplifica la protección contra ransomware

La creciente complejidad y el coste de los ataques de ransomware subraya la necesidad de contar con defensas integrales de confianza cero. La plataforma Zscaler Zero Trust Exchange™ simplifica el desafío y ofrece un enfoque holístico para detener el ransomware.

Zero Trust Exchange permite a las empresas implementar defensas más inteligentes en cada etapa de un ataque. Esto comienza con evitar que los atacantes descubran o exploten usuarios y aplicaciones haciendo que dichos usuarios y aplicaciones sean invisibles y accesibles únicamente para usuarios o dispositivos autorizados. Inspecciona todo el tráfico entrante y saliente en línea, esté cifrado o no. Los usuarios y dispositivos autenticados se conectan directamente a las aplicaciones que necesitan, nunca a la red, por lo que incluso si un atacante logra entrar, no puede moverse lateralmente para robar o cifrar datos.



POR QUÉ LA CONFIANZA CERO ES ESENCIAL PARA LA PROTECCIÓN CONTRA RANSOMWARE

Las arquitecturas de seguridad heredadas son ineficaces para detener los ataques de ransomware.

FUERA LO VIEJO: Las medidas de seguridad tradicionales y las soluciones puntuales, incluidos los cortafuegos y VPN de "próxima generación", a menudo introducen puntos ciegos, complejidad y costes significativos. Estos enfoques heredados no logran inspeccionar de manera rentable los archivos y el tráfico cifrados, lo que deja a las organizaciones vulnerables a movimientos laterales y ataques de ransomware que explotan las brechas en la visibilidad y el control, a menudo con consecuencias devastadoras.

DENTRO LA CONFIANZA CERO: Una arquitectura de confianza cero supone que cada usuario, dispositivo y conexión está potencialmente comprometido. Este enfoque exige una verificación continua y un estricto control de acceso. Al verificar constantemente las identidades e inspeccionar todo el tráfico, incluidos los datos cifrados, la confianza cero reduce significativamente el riesgo de que los ataques se propaguen dentro de la red, neutralizando las amenazas de ransomware antes de que puedan causar daños.

ZSCALER DETIENE EL RANSOMWARE EN CADA ETAPA DEL CICLO DE ATAQUE, desde el reconocimiento y el peligro iniciales hasta el movimiento lateral, el robo de datos y la ejecución de la carga útil.

Minimice la superficie de ataque: construido sobre una arquitectura de confianza cero, Zero Trust Exchange reemplaza las arquitecturas de cortafuegos y VPN heredadas explotables que amplían la superficie de ataque. Zscaler minimiza eficazmente la superficie de ataque al ocultar usuarios, aplicaciones y dispositivos detrás de un proxy en la nube, donde no son visibles ni detectables desde Internet. De manera similar a una centralita que enruta llamadas a destinos autorizados, Zscaler sólo conecta al usuario o dispositivo correcto y autorizado a una aplicación en particular.

Evite el compromiso inicial: Zero Trust Exchange emplea una amplia inspección TLS/SSL, aislamiento del navegador, zona de pruebas en línea avanzada y controles de acceso basados en políticas para evitar que los usuarios accedan a sitios web maliciosos, así como detectar amenazas desconocidas antes de que lleguen a su red. Esto minimiza el riesgo de verse comprometido en primer lugar.

Elimine el movimiento lateral: aprovechando la segmentación de usuario a aplicación o de aplicación a aplicación, los usuarios se conectan directamente a las aplicaciones (y las aplicaciones a otras aplicaciones), no a la red, eliminando el riesgo de movimiento lateral. Al centralizar la gestión de políticas de control de acceso, Zscaler actúa como un punto de control de seguridad para el tráfico de Internet, eliminando vías de movimiento lateral. Zscaler también puede identificar y evitar que atacantes potenciales se muevan lateralmente, ya sean amenazas externas o personas internas maliciosas, a través de capacidades de detección y respuesta a amenazas de identidad (ITDR) y engaño.

Detenga la pérdida de datos: las medidas de prevención de pérdida de datos en línea, combinadas con total inspección TLS/SSL, frustran eficazmente los intentos de robo de datos. Zscaler garantiza que los datos estén protegidos tanto en tránsito como en reposo.

LUCHAR CONTRA LAS AMENAZAS IMPULSADAS POR IA CON INNOVACIÓN DE IA + ZERO TRUST

Estas capacidades impulsadas por IA permiten a Zscaler ofrecer una protección sólida frente al ransomware, garantizando una seguridad integral para las empresas en el panorama de amenazas en evolución:

- ***La detección de phishing y C2 impulsada por IA*** utiliza la detección basada en IA en línea desde Zscaler Secure Web Gateway para identificar y bloquear sitios de phishing e infraestructura de comando y control (C2) nunca antes vistos.
- ***El sandboxing impulsado por IA*** ofrece prevención integral de malware y amenazas de día cero mediante el análisis de archivos sospechosos en un entorno controlado.
- ***La segmentación impulsada por IA*** proporciona recomendaciones de políticas de acceso automatizadas para minimizar la superficie de ataque y evitar el movimiento lateral, utilizando el contexto, el comportamiento, la ubicación y la telemetría de aplicaciones privadas del usuario.
- ***La política dinámica basada en riesgos*** analiza continuamente el riesgo asociado con los usuarios, dispositivos y aplicaciones para aplicar políticas dinámicas de acceso y seguridad.
- El aislamiento ***del navegador impulsado por IA*** crea una brecha segura entre los usuarios y el contenido web malicioso al representar las páginas como flujos de imágenes perfectas, evitando filtraciones de datos y la entrega de amenazas activas.
- ***El descubrimiento y la clasificación de datos impulsados por IA*** brindan visibilidad y clasificación de datos instantánea y lista para usar en datos de terminales, en línea y en la nube, lo que dificulta que el ransomware ataque y cifre datos confidenciales.

Prevención integral en cada etapa de la cadena de ataque

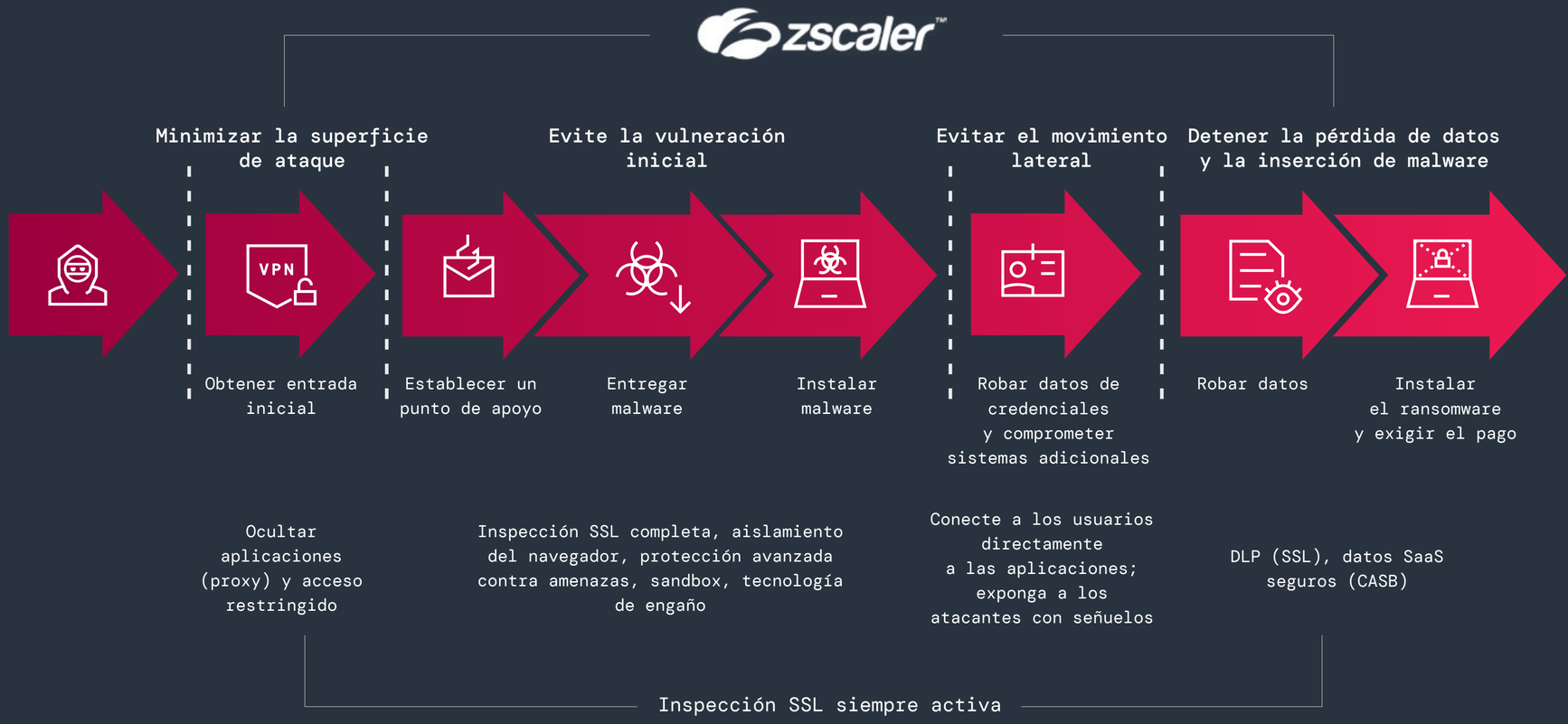


Figura 23: asignación de arquitectura de confianza cero a lo largo de la cadena de ataque de ransomware

Productos Zscaler relacionados

Zscaler Internet Access™ (ZIA™) proporciona acceso seguro y directo a Internet y ofrece protección contra amenazas en línea. Las capacidades avanzadas de prevención de amenazas y zona de pruebas de ZIA ayudan a frustrar las descargas de ransomware y las comunicaciones de comando y control (C2), evitando la infiltración de ransomware.

Zscaler Private Access™ (ZPA™) permite el acceso seguro a aplicaciones internas sin exposición a Internet, empleando un modelo de confianza cero. ZPA garantiza que sólo los usuarios y dispositivos autorizados puedan acceder a aplicaciones críticas, reduciendo así la superficie de ataque y previniendo intentos de ransomware.

Zscaler Zero Trust Firewall intercepta e inspecciona el tráfico TLS/SSL para detectar malware oculto en el tráfico cifrado, evitando su infiltración en la red.

Zscaler Deception detecta y contiene a los atacantes que intentan moverse lateralmente o escalar privilegios atrayéndolos con servidores, aplicaciones, directorios y cuentas de usuario señuelo.

Zscaler Sandbox analiza archivos y ejecutables sospechosos en un entorno virtual controlado, ayudando a identificar y bloquear códigos maliciosos, manteniendo a las organizaciones por delante del ransomware basado en archivos y los ataques de día cero.

Zscaler Cloud Browser aísla las sesiones web y transmite solo píxeles a los dispositivos para eliminar de manera efectiva el riesgo de descargas no autorizadas y vulneraciones de día cero que pueden utilizar los operadores de ransomware.

Zscaler ITDR (Identity Threat Detection and Response) detecta ataques basados en la identidad, como el robo de credenciales y el abuso de privilegios, ataques de Active Directory y asignaciones arriesgadas de derechos, y proporciona protección contra estos.

Zscaler Data Protection proporciona seguridad unificada y consistente para los datos en movimiento y en reposo en aplicaciones SaaS y de nube pública, lo que reduce la probabilidad de filtración de datos y al mismo tiempo mitiga el impacto potencial de los ataques de ransomware.

Guía de prevención de ransomware

Una estrategia de defensa basada en una arquitectura de confianza cero es una medida de seguridad comprobada para detener el ransomware, pero abordar esta amenaza multifacética exige una planificación proactiva, colaboración continua e inversiones estratégicas.

Los expertos de ThreatLabz han recopilado las mejores y más recientes prácticas para ayudar a reducir los riesgos de ransomware y proteger su organización contra amenazas existentes y emergentes.

- **Implementar copias de seguridad de datos periódicas y seguras.** Asegúrese de que se realicen copias de seguridad de todos los datos de forma periódica y segura, incluidas las copias de seguridad fuera de línea. Adapte las estrategias de copia de seguridad en función de las amenazas en evolución.
- **Mantener el software actualizado.** Aplique las últimas revisiones de seguridad rápidamente para abordar las vulnerabilidades conocidas. Utilice plataformas de información sobre amenazas basadas en IA para priorizar y gestionar revisiones de seguridad de forma eficaz.
- **Habilitar la autenticación multifactor (MFA).** Agregue una capa adicional de seguridad a las cuentas de usuario con MFA para mitigar el riesgo de acceso no autorizado. Integre soluciones MFA para detectar y prevenir la apropiación de cuentas de manera efectiva.
- **Establecer una política de seguridad corporativa consistente.** Asegúrese de que todos los usuarios sigan procedimientos de seguridad coherentes, incluida MFA y actualizaciones de seguridad periódicas, para ayudar a evitar compromisos iniciales. Con un personal distribuido, es aún más importante implementar una arquitectura de perímetro del servicio de seguridad (SSE) para proteger a los usuarios sin importar dónde se encuentren.
- **Reforzar la seguridad de las aplicaciones.** Elimine aplicaciones de la Internet pública para evitar que los autores de ransomware aprovechen las vulnerabilidades. Implemente una arquitectura de confianza cero para las aplicaciones internas para protegerlas contra intentos de ransomware.
- **Hacer cumplir el acceso con privilegios mínimos.** Implemente políticas con privilegios mínimos para restringir el acceso de los usuarios exclusivamente a los recursos necesarios para sus funciones. Utilice soluciones impulsadas por IA para analizar dinámicamente el comportamiento del usuario y adaptar los privilegios de acceso en consecuencia.
- **Fortalecer la protección de la identidad.** Utilice herramientas ITDR para obtener visibilidad de las configuraciones erróneas de identidad, remediar vulnerabilidades en Active Directory que los adversarios aprovechan para escalar privilegios y moverse lateralmente así como detectar amenazas de identidad sigilosas.
- **Inspeccione todo el tráfico.** Hoy en día, el 86 % de las amenazas se transmiten a través de canales cifrados, que a menudo no se inspeccionan, lo que facilita que incluso los atacantes moderadamente sofisticados eludan los controles de seguridad. Es esencial inspeccionar todo el tráfico, cifrado o no, para evitar compromisos.
- **Implementar acceso a la red de confianza cero (ZTNA).** Implemente una segmentación granular de usuario a aplicación y de aplicación a aplicación, intermediando el acceso a través de controles de acceso con privilegios mínimos para eliminar el movimiento lateral, minimizar la exposición de los datos y mejorar su postura de seguridad general.

- **Utilizar el aislamiento del navegador impulsado por IA.** Proteja a los usuarios de las amenazas web con aislamiento basado en IA de contenido de Internet sospechoso y usuarios de alto riesgo. Al aislar la experiencia del navegador y restringir acciones potencialmente dañinas (como ingresar credenciales), los usuarios pueden acceder de manera segura a URL y archivos sospechosos sin poner en riesgo la seguridad de su sistema.

- **Emplear sandboxing avanzado impulsado por IA.** Detenga el malware esquivo y nunca antes visto con un entorno de pruebas que detecta y pone en cuarentena automáticamente amenazas desconocidas y archivos sospechosos aprovechando el análisis de IA/ML.

- **Implementar prevención de pérdida de datos (DLP) en línea.** Proteja contra la filtración y exposición de datos mediante la implementación de medidas DLP en línea.

- **Aprovechar la tecnología del engaño.** Emplee herramientas de engaño y trampas para desviar a los atacantes, fortaleciendo las defensas contra la infiltración del sistema.

- **Utilizar un agente de seguridad de acceso a la nube (CASB).** Controle y supervise el uso de aplicaciones en la nube con un CASB para evitar actividades maliciosas como descargas de archivos y filtración de datos.

- **Proporcionar capacitación continua a los empleados.** Realice sesiones periódicas de concientización sobre seguridad para educar a los empleados sobre las amenazas de ransomware. Emplee simulaciones de escenarios de ransomware del mundo real para mejorar la preparación de los empleados.

- **Desarrollar un plan integral de respuesta al ransomware.** Cree un plan de respuesta que abarque recuperación de datos, respuesta a incidentes y protocolos de comunicación para actuar con rapidez y eficacia en caso de un ataque de ransomware.

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

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

X @ThreatLabz | Blog de investigación de seguridad de ThreatLabz

Metodología del informe

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 del informe recopiló datos de una variedad de fuentes entre abril de 2023 y marzo de 2024, que incluyen:

- **La nube de seguridad global de Zscaler,** que 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.

- **Fuentes de inteligencia externas.** También recopilamos datos de fuentes de inteligencia externas, como fuentes de inteligencia sobre amenazas, investigaciones de código abierto e informes de aplicación de la ley, que proporcionaron información adicional sobre los atacantes de ransomware, sus objetivos y sus métodos.

- **El propio análisis del equipo de ThreatLabz de muestras de ransomware y datos de ataques.** El equipo de ThreatLabz Threat Intelligence rastrea familias de ransomware a escala mediante ingeniería inversa y automatización del análisis de malware para desarrollar estrategias de respuesta efectivas. ThreatLabz también trabaja en estrecha colaboración con agencias internacionales de aplicación de la ley y ha desempeñado un papel importante en acciones recientes, incluidas la Operación Duck Hunt y la Operación Endgame.

Acerca de ThreatLabz

ThreatLabZ es la división de investigación de seguridad de Zscaler. Este equipo de primera clase es responsable de buscar nuevas amenazas y garantizar que las miles de organizaciones que usan la plataforma global Zscaler estén siempre protegidas. Además de investigar el malware y de analizar los comportamientos, los miembros del equipo participan en la investigación y el desarrollo de nuevos módulos prototipo para la protección avanzada contra las amenazas en la plataforma Zscaler. Asimismo, realizan habitualmente auditorías de seguridad internas para garantizar que los productos y la infraestructura de Zscaler satisfacen los estándares de cumplimiento de seguridad. ThreatLabZ publica regularmente análisis detallados de amenazas nuevas y emergentes en su portal **research.zscaler.com**.

Acerca de Zscaler

Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, resilientes 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 150 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.es.**