Informe sobre el ransomware de ThreatLabz 2024

Índice

Resumen ejecutivo_

Los ataques de ransomware han alcanzado nuevos niveles de ambición y audacia durante el pasado año, 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 dólares, el mayor pagado nunca por una empresa. Esta cantidad es casi el doble del mayor pago de rescate conocido públicamente.[1] Solo en 2023, los pagos por ransomware superaron los 1000 millones de dólares, lo que pone de relieve la escalada del impacto financiero de estos ciberdelitos.

Las tácticas de los actores de las amenazas de ransomware se han vuelto cada vez más sofisticadas y audaces. En particular, han sobrepasado los límites tradicionales de las corporaciones a las que atacan, llegando incluso a dirigirse a los hijos de los ejecutivos para provocar rescates más rápidos y elevados.[2] Desde las infraestructuras críticas[3] y las grandes corporaciones[4] hasta las pequeñas y medianas empresas, ninguna organización está exenta de encontrarse en la mira de la próxima campaña o evolución de los ataques.

A pesar de que las fuerzas del orden han desmantelado varios intermediarios de acceso inicial en el marco de las operaciones especiales "Operación Endgame" y "Operación Duck Hunt", muchas de las principales familias de ransomware activas siguen reagrupándose rápidamente y lanzando nuevos ataques sin inmutarse. Lamentablemente, muchos actores de 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, las fuerzas del orden han aumentado sus tácticas de presión mediante recompensas monetarias, sanciones, troleo y exposición de las personas detrás del ransomware mediante diversas formas de tácticas psicológicas.

A medida que los actores de ransomware evolucionan continuamente en sus tácticas, es fundamental mantenerse actualizado sobre cómo está cambiando el panorama de amenazas.

El Informe Zscaler ThreatLabz 2024 sobre ransomware ofrece una visión general del panorama de las amenazas de ransomware desde abril de 2023 hasta abril de 2024, detallando las últimas tendencias, objetivos, familias de ransomware y estrategias de defensa eficaces.

ThreatLabz descubrió que los ataques de ransomware aumentaron un 17.8 % interanual basándose en los intentos bloqueados en la nube de Zscaler, mientras que los ataques de ransomware identificados a través del análisis de sitios de fuga de datos aumentaron un 57.8 %. Los objetivos más comunes fueron empresas de los sectores de fabricación, sanitario y tecnológico, poniendo las operaciones e infraestructuras críticas directamente en la línea de ataque.

Las conclusiones presentadas en este informe subrayan la necesidad de que las organizaciones den prioridad a la protección contra la incesante oleada de ransomware. Los conocimientos y estrategias del informe sirven como guía esencial para mejorar sus defensas contra el ransomware. Si conoce las últimas tendencias y vulnerabilidades, y aplica las mejores prácticas recomendadas, podrá reducir significativamente el riesgo de convertirse en víctima del 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.

Hallazgos clave

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

Los ataques de ransomware bloqueados por la nube de Zscaler aumentaron un 17.8 %, y el número de empresas extorsionadas en sitios de fuga de datos creció un 57.8 % en el mismo período interanual, a pesar de las numerosas operaciones de las fuerzas del orden, incluida la incautación de infraestructuras junto con detenciones, acusaciones penales y sanciones.

Los sectores de fabricación, sanitario y tecnológico fueron los principales objetivos de los ataques de ransomware, mientras que el sector energético experimentó un repunte interanual del 500 %, ya que las infraestructuras críticas y su susceptibilidad a las interrupciones operativas lo hacen especialmente atractivo para los ciberdelincuentes.

Estados Unidos sigue siendo el principal objetivo del ransomware, con un 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 demasiado común, lo que subraya la importancia de aplicar parches a tiempo y de una gestión unificada de las vulnerabilidades, respaldada por una arquitectura Zero Trust para ofrecer protección incluso cuando los parches no estén disponibles.

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

El panorama del ransomware: Principales tendencias y objetivos

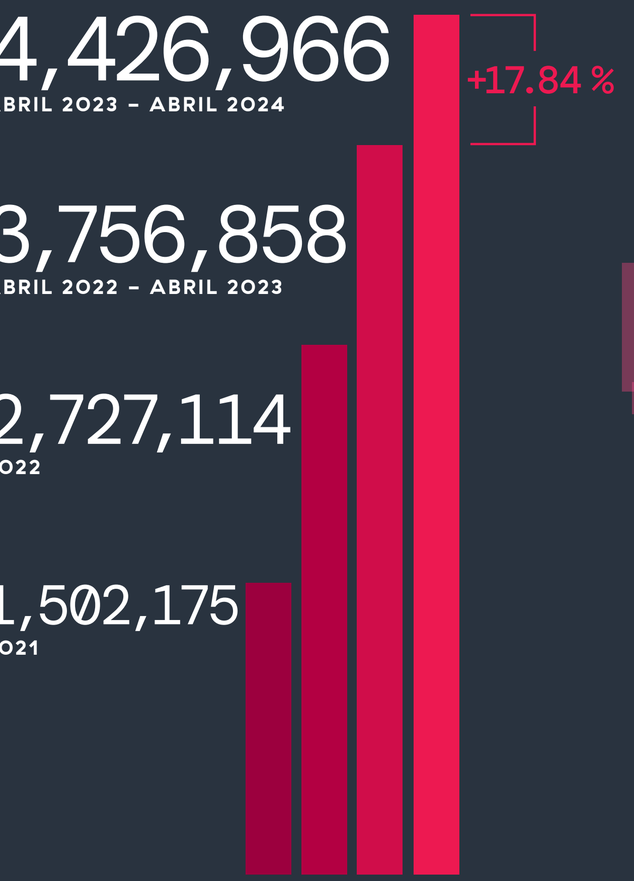
La naturaleza dinámica del ransomware lo ha situado en primera línea de las preocupaciones de seguridad en los últimos años. Los malintencionados desarrollan constantemente sus métodos de ataque y extorsión, aprovechando los avances de la tecnología de inteligencia artificial (IA), el código fuente fugado 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
- Mayor acción de las fuerzas del orden contra los grupos de ransomware y los intermediarios 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 basados en intentos bloqueados observados en toda la nube de Zscaler. El aumento de la actividad de ransomware se traduce en interrupciones significativas e impactos financieros para las organizaciones víctimas de todos los tamaños. Estos ataques a menudo interrumpen las operaciones empresariales, causando un tiempo de inactividad prolongado, una pérdida sustancial de datos y elevados costos de recuperación. El impacto financiero es considerable; no solo hay una petición de rescate en juego, sino que la restauración del sistema y el control de daños pueden tener un precio elevado. A raíz de estas amenazas crecientes, la necesidad de **sólidas medidas de defensa contra el software malicioso** 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 e industrias. Estos ataques pueden comprometer datos confidenciales, provocar grandes pérdidas financieras, interrumpir la continuidad de la actividad y dañar la reputación. Los distintos sectores se enfrentan a desafíos únicos en materia de ransomware en función de su manera de operar, los datos que manejan y su infraestructura tecnológica.

A pesar de las variables, los ataques de extorsión por ransomware no han dejado de aumentar, y el número de empresas víctimas que aparecen en los sitios de fuga de datos ha incrementado en un 57.81 % desde el informe de ThreatLabz del año pasado sobre las tendencias del ransomware. El sector de la fabricación fue por mucho el más atacado, con 653 ataques, más del doble que cualquier otro sector.

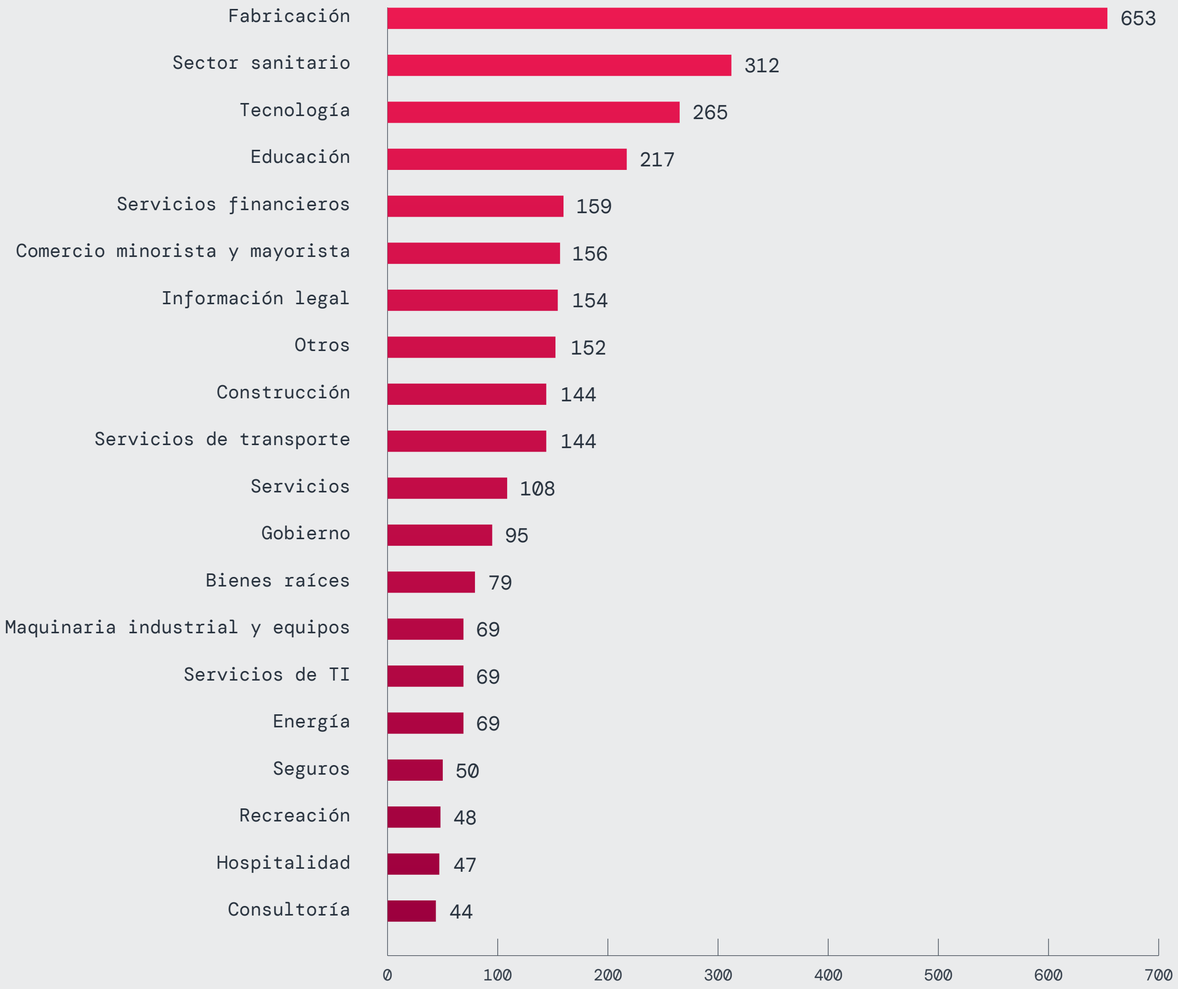


Figura 1: Ataques de ransomware por sector según los sitios de fuga de datos (solo los 20 sectores principales).

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 elevado potencial de rescate que ofrece a los atacantes.

Del mismo modo, 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 avanzados sistemas de punto de venta y plataformas de pedidos en línea. Aunque estas tecnologías pueden agilizar las operaciones y mejorar la experiencia de los clientes, también pueden introducir vulnerabilidades potenciales.

Aunque este aumento pone de relieve la prevalencia de los ataques de ransomware, puede que no capte el alcance total de los incidentes de ransomware. Muchos ataques no se denuncian o se resuelven en privado mediante el pago de rescates sin divulgación pública. Por lo tanto, estas cifras deben considerarse como indicativas de tendencias más amplias del ransomware y no como una representación exhaustiva de todo el panorama de amenazas.

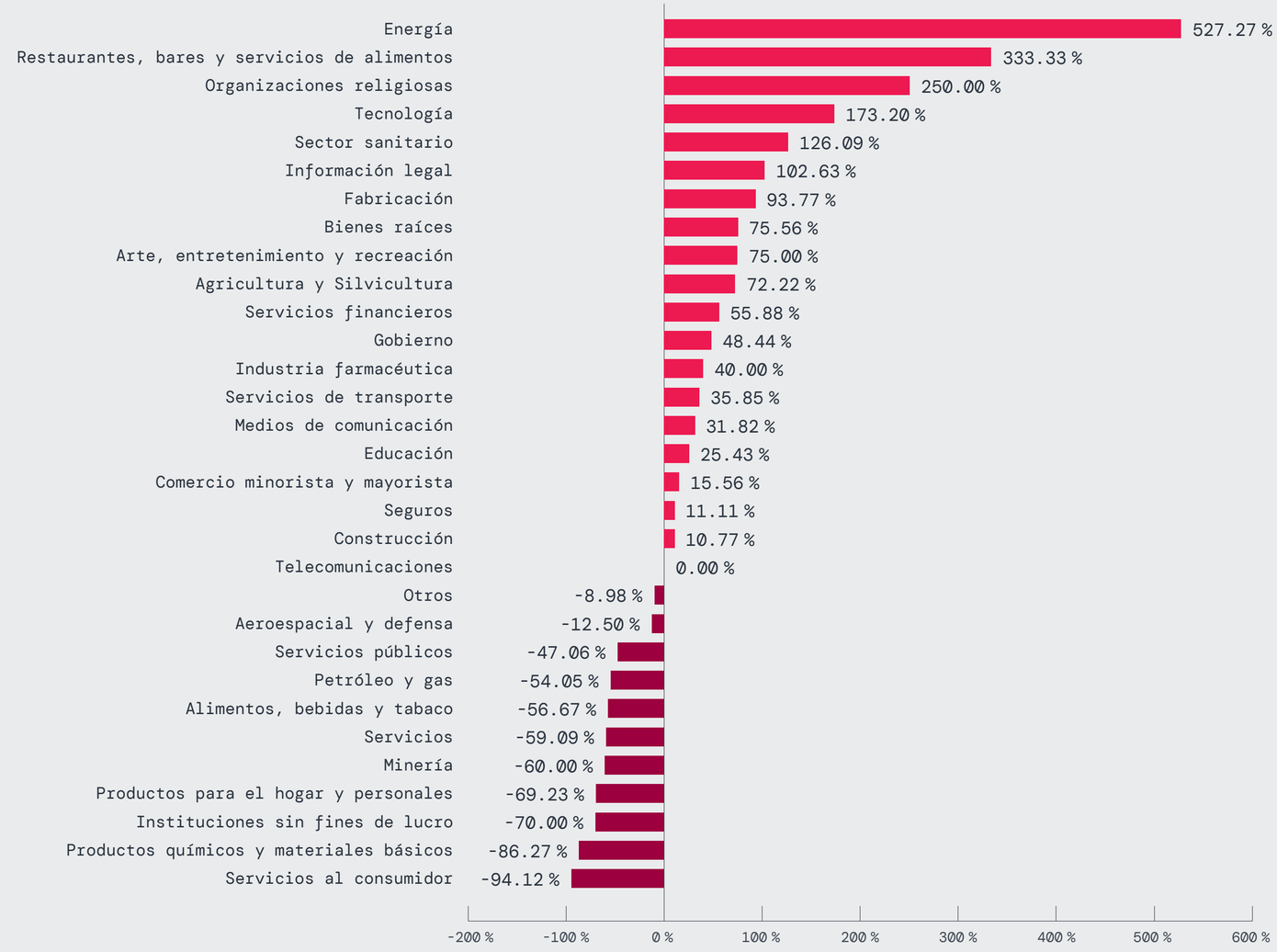


Figura 2: Variación porcentual interanual de los ataques de extorsión de ransomware por sectores. Observe que algunos sectores tenían una base relativamente baja de ataques en el informe del año pasado, lo que hace que su crecimiento parezca más sustancial.

Distribución geográfica de las organizaciones víctimas

Estados Unidos se enfrentó a un volumen considerablemente mayor de ataques de ransomware que cualquier otro país, representando alrededor del 50 % de todos los incidentes a nivel mundial. En comparación, el Reino Unido fue la segunda nación más atacada, experimentando casi el 6 % de los 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 las extorsiones de rescate entre abril de 2023 y abril de 2024.

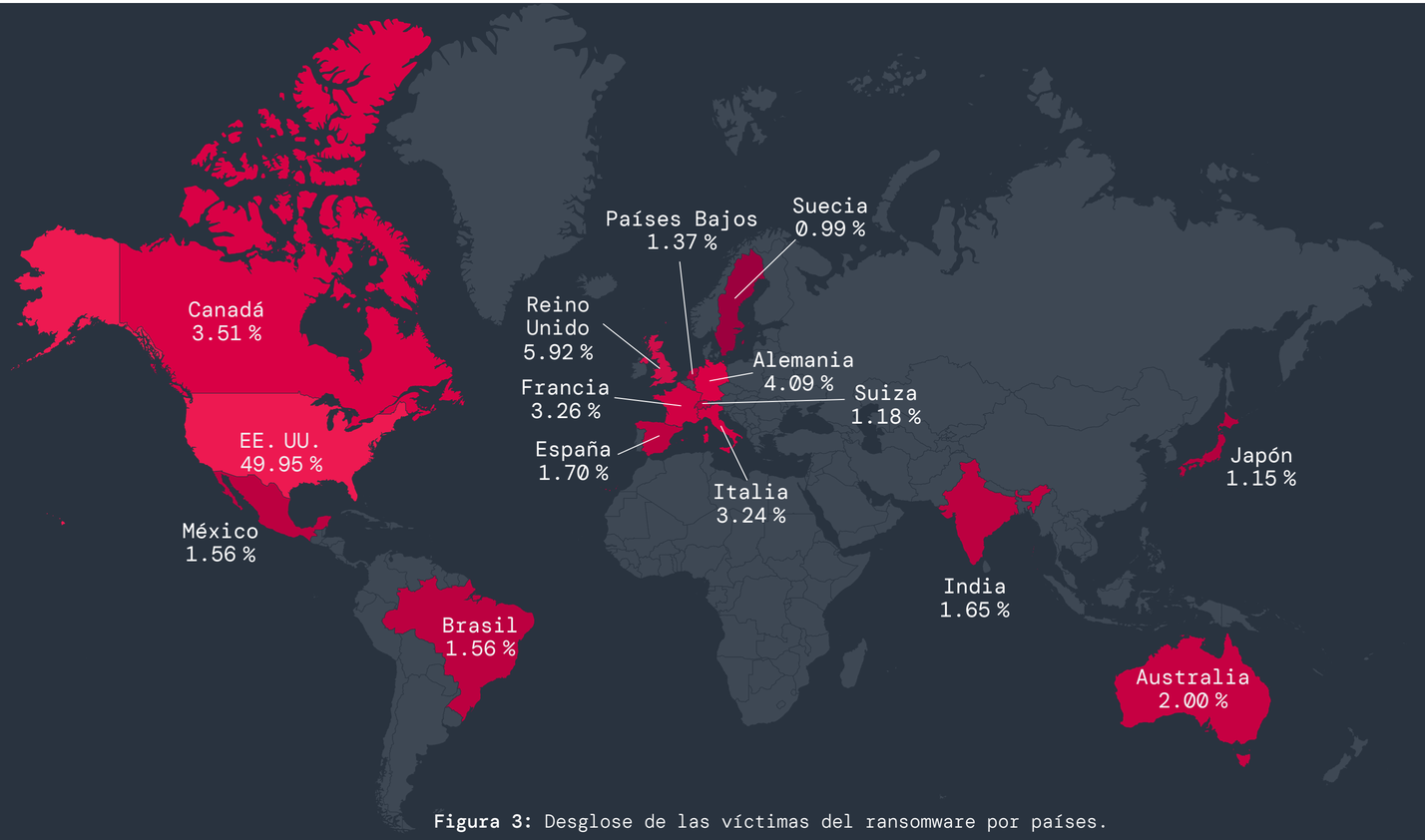


Figura 3: Desglose de las víctimas del ransomware por países.

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 en la lucha contra las amenazas de ransomware.

Evaluación de riesgos

El análisis de las regiones más atacadas ayuda a las organizaciones de esas zonas a evaluar sus propios niveles de riesgo e implementar una ciberseguridad más sólida. Según la investigación de ThreatLabz, los EE. UU. son responsables del 50 % de los ataques mundiales de ransomware, lo que exige 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 a las organizaciones asignar estratégicamente los recursos, mejorando su postura de seguridad al priorizar la asistencia, la financiación y la experiencia en las áreas con los niveles de amenaza más elevados.

Desarrollo de políticas

Los gobiernos pueden utilizar la información obtenida de los ataques regionales de ransomware para informar la normativa, mejorar los estándares de seguridad, promover la cooperación internacional y facilitar el intercambio de información entre los sectores público y privado. Un ejemplo destacado reciente son las nuevas normas de ciberseguridad de la SEC, que suponen un gran paso para mejorar la transparencia y la rendición de cuentas en medio de las crecientes amenazas.

Cooperación internacional

La identificación de los países más afectados permite coordinar los esfuerzos entre las fuerzas del orden, las organizaciones y los gobiernos para combatir el ransomware a escala nacional e internacional. La Operación Duck Hunt y la Operación Endgame ejemplifican cómo la cooperación internacional puede desarticular las actividades de los ciberdelincuentes.

Concientización del público

Señalar los países que suelen ser objetivo de ataques puede instar a particulares, organizaciones y gobiernos a tomar medidas más proactivas en lo que respecta a la capacitación en ciberseguridad, la planificación de la respuesta a incidentes y la inversión en tecnologías de defensa.

Tendencias interanuales

ThreatLabz comparó los ataques de ransomware del informe de este año con el Informe sobre ransomware de ThreatLabz 2023 para evaluar los ritmos del cambio. Entre los 15 países más atacados, los Estados Unidos experimentaron un notable incremento interanual del 101.88 %, y Suecia experimentó un asombroso aumento del 350 %, aunque representó una parte significativamente menor del total de ataques.

Si bien analizar las tendencias del ransomware a nivel global es invaluable, también es importante examinar los desarrollos específicos en diferentes regiones del mundo. Analizar los desgloses regionales ayuda a las organizaciones a crear planes de seguridad a la medida y a los gobiernos a desarrollar políticas de ciberseguridad más eficaces.

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 los ataques de ransomware por países.

CAMBIOS EN LOS ÍNDICES 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 los ataques de ransomware por países en la región EMEA.

CAMBIOS EN LOS ÍNDICES 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%
Taiwán	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 los ataques de ransomware por países en la región APAC.

Grupos de ransomware más activos en 2023-2024

LockBit (22.1 %), BlackCat (9.2 %) y 8Base (7.9 %) fueron los grupos de extorsión de ransomware más activos durante el año pasado, cada uno responsable de un número importante de ataques. La figura 8 muestra el número de víctimas de fuga de datos por familia de ransomware durante este período.

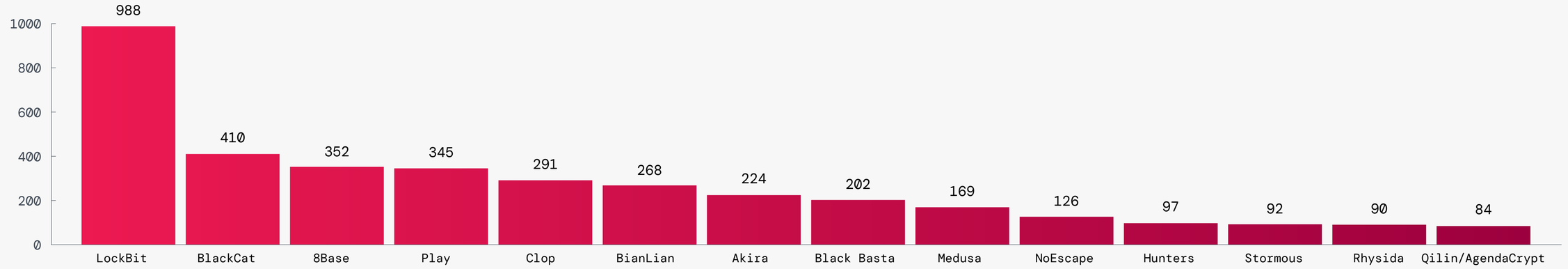


Figura 8: Ataques de ransomware revelados en sitios web de fuga de datos operados de manera maliciosa.

Los grupos de ransomware más nuevos en la escena

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

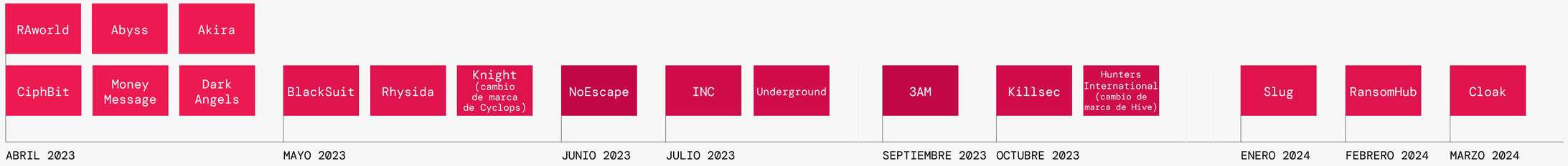


Figura 9: Nuevos grupos de ransomware con sitios de fuga de datos.

Vulnerabilidades importantes 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 las Infraestructuras (CISA) mantiene una lista exhaustiva de vulnerabilidades,[5] que incluye las que explotan activamente los grupos de ransomware. Es muy recomendable que las organizaciones sigan de cerca esta lista y den prioridad a la mitigación de las vulnerabilidades mencionadas en ella. La gestión proactiva de las vulnerabilidades es esencial para reforzar la postura general de ciberseguridad de una organización.

En muchos casos, las vulnerabilidades explotadas por los grupos de ransomware afectan a 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 significativamente más fáciles de escanear y explotar para los malintencionados. La nueva guía de CISA[6] enfatiza aún más las vulnerabilidades en las VPN y las soluciones de conectividad remota como puntos críticos de atención, aconsejando la adopción de enfoques más actuales, como la arquitectura Zero Trust, SSE y SASE, que se basan en políticas de control de acceso granular.

Durante el último año, las principales familias de ransomware han atacado y explotado las vulnerabilidades que se muestran en la figura 10, afectando considerablemente a una gran variedad de sistemas.

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

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

- Desactivar el acceso remoto a servidores
- Utilizar contraseñas seguras y autenticación multifactor
- Supervisar servidores en busca de actividad sospechosa

[5] Cybersecurity & Infrastructure Security Agency, **Known Exploited Vulnerabilities Catalog**, consultado el 25 de junio, 2024.
[6] Cybersecurity & Infrastructure Security Agency, **Modern Approaches to Network Access Security**, 18 de junio, 2024.

Boletín de ransomware: Las últimas noticias

El ransomware es omnipresente y trasciende las industrias, y cuando se cierra un grupo, otro renace o vuelve a surgir. A continuación se muestran algunas historias recientes que destacan el panorama del ransomware en constante evolución.

La plaga del ransomware en el sector sanitario

El sector sanitario se enfrentó a importantes desafíos a lo largo de 2023 y en 2024, ya que fue blanco de los grupos de ransomware. Las repercusiones de la interrupción de las operaciones sanitarias son graves: las ambulancias se desvían, las recetas se retrasan y hay que posponer intervenciones médicas esenciales. Además, el robo de datos sanitarios confidenciales puede tener consecuencias de gran alcance, como el robo de identidad y el fraude sanitario, lo que agrava aún más las vulnerabilidades del 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 exigencias de los atacantes y pagar un alucinante rescate de 22 millones de dólares, la terrible situación dio un giro inesperado. BlackCat incumplió su promesa de compartir una parte del rescate con el afiliado que estaba detrás del ataque (lo que se conoce como "estafa de salida"), lo que llevó al afiliado a amenazar al proveedor de servicios sanitarios con la divulgación de datos confidenciales.

Este es un claro recordatorio de que el viejo dicho "cada ladrón juzga por su condición" es válido para los ataques de ransomware. Aunque se paguen rescates, no hay garantías de que el grupo de la amenaza no siga publicando o borrando los datos robados. Además, algunas herramientas de descifrado de ransomware contienen fallas que impiden recuperar los datos con éxito, y pueden tardar más en recuperarlos que a partir de una copia de seguridad.

DOBLE EXTORSIÓN, DOBLE VICTIMIZACIÓN

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

[7] BleepingComputer, **Drug distributor AmerisourceBergen confirms security breach**, 8 de febrero, 2023.
[8] BleepingComputer, **Pharmaceutical giant Cencora says data was stolen in a cyberattack**, 27 de febrero, 2024.

El impacto de la decisión de la SEC sobre ciberseguridad

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 normas obligan a informar puntualmente de los incidentes importantes de ciberseguridad y exigen 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 adición del punto 1.05 al formulario 8-K, que exige informar de los incidentes importantes de ciberseguridad en un plazo de cuatro días laborables a partir de la determinación de materialidad por parte de la empresa. Además, el formulario 10-K exige ahora la presentación de informes anuales sobre la gestión y la estrategia de los riesgos de ciberseguridad, a partir de los ejercicios fiscales que terminen el 15 de diciembre de 2023 o después. Los emisores privados extranjeros también deben cumplir con divulgaciones comparables en el Formulario 6-K y el Formulario 20-K.

Las resoluciones suponen 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 ahora éstas siguen estando obligadas a revelar completamente el ataque. El aspecto positivo es que el nuevo mandato socava los ataques de extorsión sin cifrado, una tendencia emergente por la que los actores del ransomware se basan únicamente en la amenaza de fugar los datos robados para exigir rescates.

CÓMO IMPACTAN LAS NUEVAS REGLAS A LAS EMPRESAS

Las resoluciones de la SEC en materia de ciberseguridad pueden plantear serios desafíos a las empresas en términos de cumplimiento y gestión de riesgos. Aunque su objetivo es aumentar la transparencia y la protección de los inversores, estas normas exigen a las empresas que se enfrenten a complejos requisitos de información y que divulguen rápidamente los incidentes importantes.

Uno de los principales efectos es el aumento de la presión sobre las empresas para que cuantifiquen y evalúen con precisión los ciberincidentes. Determinar la materialidad y el impacto potencial de los ciberincidentes requiere un análisis cuidadoso, que puede ser costoso y puede requerir que las empresas (grandes y pequeñas) se replanteen sus protocolos de respuesta a incidentes y actualicen sus divulgaciones para cumplir con los requisitos de la SEC.

Además, los plazos de cumplimiento varían en función del tamaño y la situación informativa de las empresas, lo que añade otra capa de complejidad. Las pequeñas empresas declarantes suelen tener plazos de cumplimiento diferentes, y normalmente más largos, que las grandes corporaciones. Y aunque las grandes empresas deben cumplir plazos más estrictos, su escala también les permite disponer de 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 discretamente sin incurrir en daños a su reputación y en la reacción violenta que se produce tras compartir abiertamente información sobre una violación.

ALGUNAS EMPRESAS YA ESTÁN VIOLANDO LAS RESOLUCIONES DE LA SEC

A pesar de las claras directrices de la SEC, algunas empresas ya han incumplido las nuevas normas de ciberseguridad. Recientes divulgaciones de empresas muy conocidas han suscitado preocupación por el incumplimiento y la idoneidad de sus informes sobre incidentes.[9] Muchas de estas divulgaciones carecen de datos cuantitativos y de evaluaciones detalladas de las implicaciones financieras y operativas de los ciberincidentes, que es precisamente lo que ahora exige la SEC. Esta tendencia, en la que las empresas proporcionan divulgaciones deficientes sobre ciberincidentes a pesar de la resolución de la SEC, puede exigir una mayor orientación y supervisión reglamentaria para garantizar un cumplimiento uniforme y eficaz.

Las resoluciones de la SEC en materia de ciberseguridad representan un importante cambio normativo destinado a mejorar la transparencia y la responsabilidad en la notificación de incidentes. Adherirse a estas nuevas reglas de manera uniforme y de buena fe requerirá una colaboración continua entre los reguladores, las empresas y las partes interesadas de la industria.

[9] Forbes, **Companies Are Already Not Complying With The New SEC Cybersecurity Incident Disclosure Rules**, 4 de marzo, 2024.

Impacto de las acciones de las fuerzas del orden

Qakbot desarticulado por la “Operación Duck Hunt”

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

Esta infraestructura brindaba varios niveles de resistencia, y cada nivel requería un esfuerzo coordinado para ser desmantelado. El primer nivel de la infraestructura de Qakbot incluía sistemas infectados que ejecutaban un complemento de supernodo que retransmitía el tráfico ascendente a varios proxies 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 sinkhole o sumidero para apoderarse inmediatamente de la infraestructura de Qakbot, como se muestra en la figura 12.

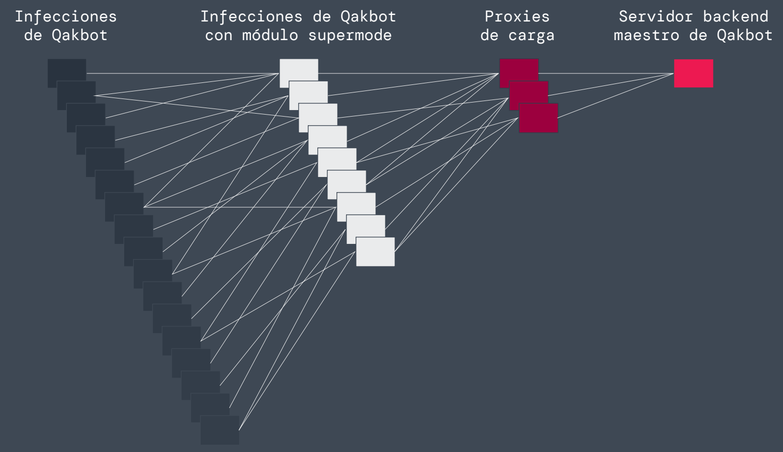


Figura 11: Infraestructura de varios niveles de Qakbot.

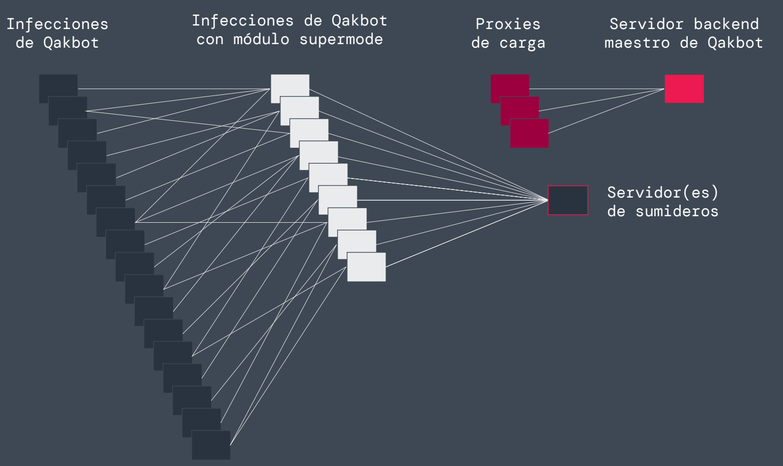


Figura 12: Arquitectura de Qakbot después de redirigir los proxies ascendentes de cada supernodo.

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

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

El malware Qakbot se distribuía normalmente a través de correos electrónicos de spam que contenían archivos adjuntos o enlaces maliciosos. Una vez infectado, Cobalt Strike se implementaba con frecuencia para el movimiento lateral y la eventual implementación de ransomware.

Lamentablemente, no se produjeron detenciones ni se levantaron cargos contra ninguno de los atacantes, y Qakbot resurgió en diciembre de 2023. El grupo actualizó el malware para que fuera compatible con las versiones de 64 bits de Windows, cambió el formato de configuración interna y modificó la comunicación de red para utilizar el cifrado AES. Como comentaremos más adelante en el informe, el atacante Qakbot ha cambiado significativamente sus TTP desde la Operación Duck Hunt.

[10] US Department of Justice, **Qakbot Malware Disrupted in International Cyber Takedown**, 29 de agosto, 2023.
[11] TechCrunch, **How the FBI took down the notorious Qakbot botnet**, 1 de septiembre, 2023.

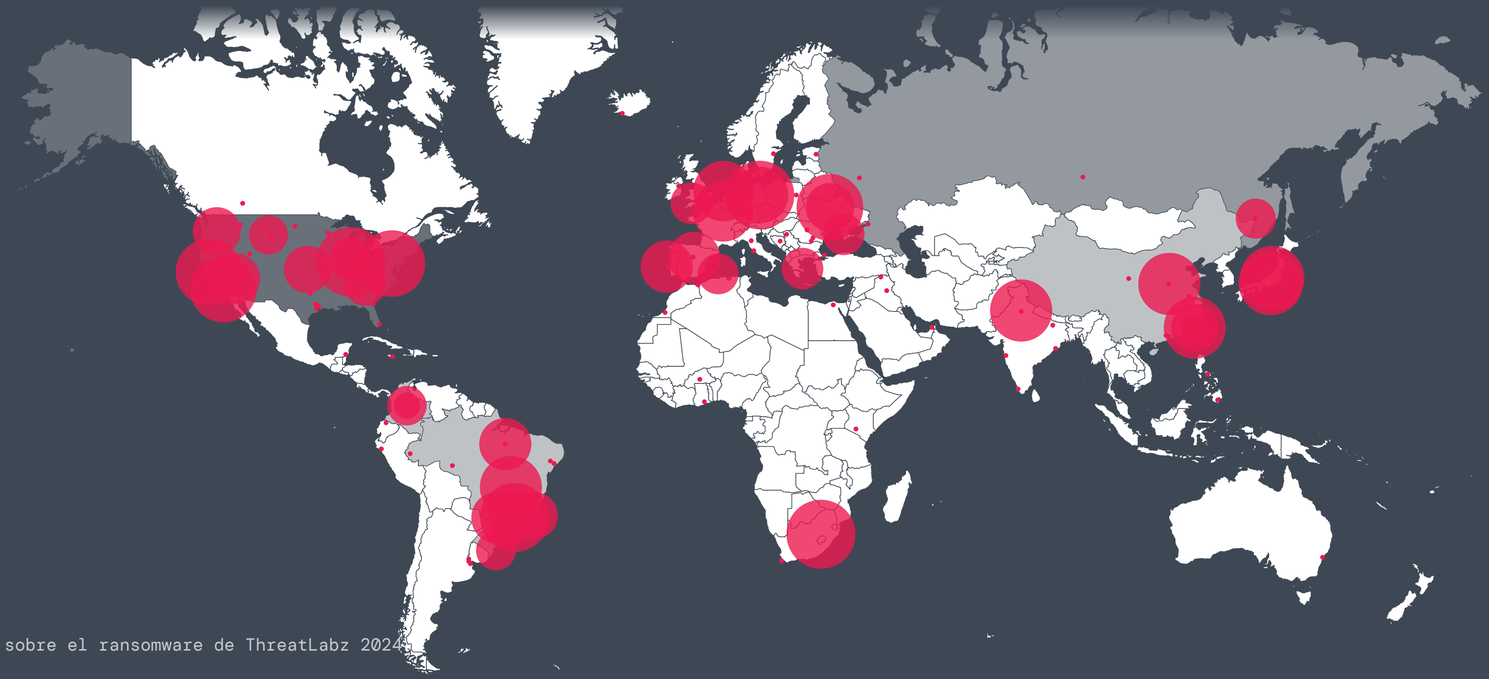
"Operación Endgame" se dirigió simultáneamente a múltiples intermediarios de acceso inicial

El 28 de mayo de 2024, en colaboración con numerosos organismos internacionales encargados de la aplicación de la ley, Europol anunció la Operación Endgame, dirigida simultáneamente contra múltiples intermediarios de acceso inicial. Esto condujo a más de una docena de registros globales, varias detenciones y el cierre de más de 100 servidores utilizados para actividades delictivas. Estos servidores formaban parte integral de las operaciones de varios descargadores de malware (también conocidos como "cargadores") que se habían utilizado para infiltrarse en las computadoras de las víctimas, implementando software malicioso que incluía ransomware.

Las familias de malware atacadas en esta operación fueron responsables de infectar millones de computadoras en todo el mundo, incluso en instalaciones sanitarias y servicios de infraestructuras críticas. Como parte de la operación, se tomaron medidas contra SmokeLoader, Pikabot, Bumblebee e IcedID.

Zscaler ThreatLabz proporcionó asistencia técnica crítica para el sinkhole de SmokeLoader de la Operación Endgame y los esfuerzos de remediación.

SmokeLoader, activo desde 2011, fue utilizado por varios intermediarios de acceso inicial para ransomware, entre ellos Raspberry Robin y la banda de ransomware Stop (también conocida como DJVU). La Operación Endgame incautó más de 1000 dominios SmokeLoader utilizados por estos grupos de amenazas. Posteriormente, los dominios fueron redirigidos a un servidor sumidero controlado por las fuerzas del orden. El mapa de la figura 13 muestra los sistemas infectados que se comunicaban con el sumidero SmokeLoader.



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

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

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

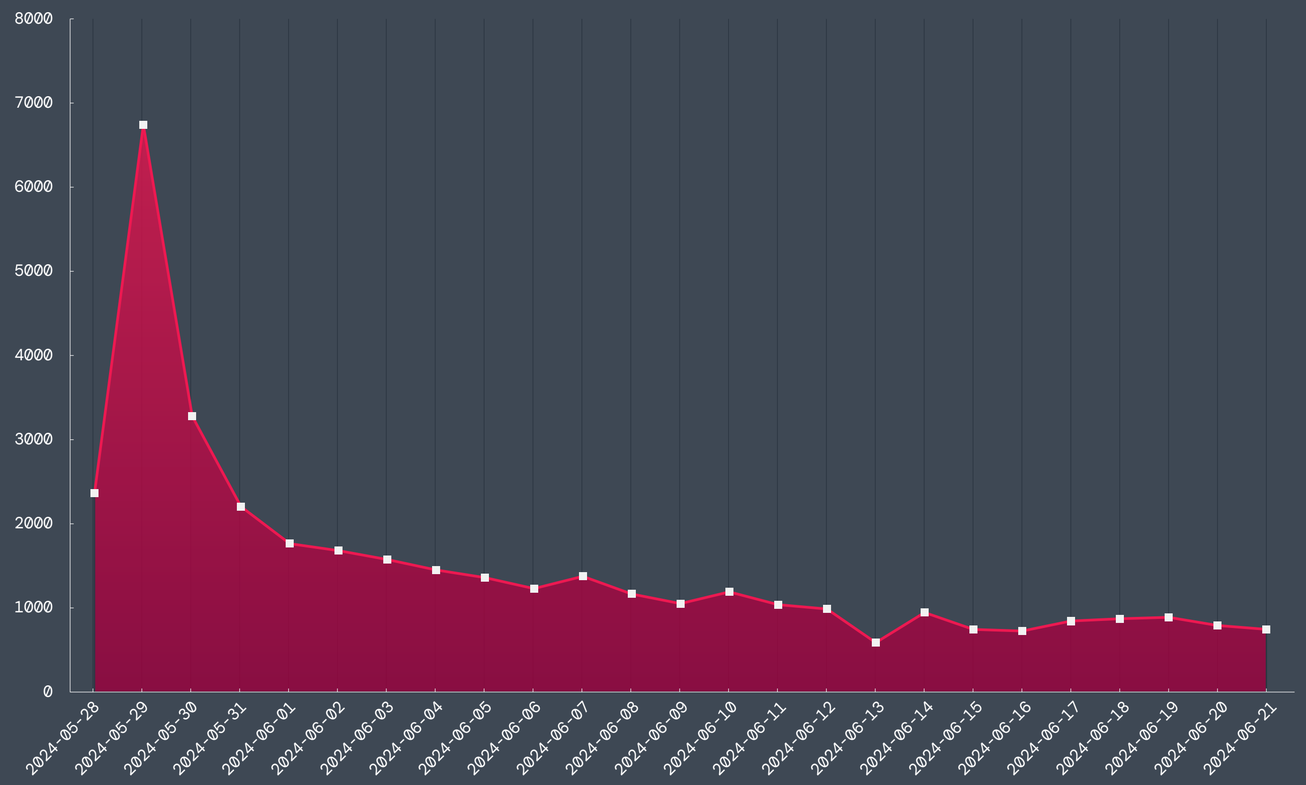


Figura 14: Sistemas SmokeLoader depurados por la Operación Endgame.

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

Bumblebee se introdujo 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 implementaban cargas útiles de Cobalt Strike para el movimiento lateral. Bumblebee también se ha asociado con los ataques de ransomware Akira y Black Basta.

De manera similar a Qakbot, IcedID fue diseñado 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 malicioso de IcedID ha sido bifurcado y modificado con 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 el ransomware.

Tras la Operación Endgame, la actividad de la mayoría de estos intermediarios de acceso inicial ha sido mínima, **con la excepción de Latrodectus**, que resurgió en menos de un mes. Sin embargo, es probable que la tregua dure poco, mientras los malintencionados se reagrupan.

El ransomware Hive renace como Hunters International

En enero de 2023, la infraestructura del grupo de ransomware Hive fue desactivada. Tras una operación encubierta de siete meses, el FBI se infiltró con éxito en los servidores de Hive, recuperando más de 300 claves de descifrado que evitaron aproximadamente 130 millones de dólares en pagos de rescates. Operando desde junio de 2021, el colectivo Hive tuvo como objetivo y víctima a más de 1500 organizaciones de todo el mundo, acumulando más de 100 millones de dólares en pagos de rescates. [12] Entre las víctimas se encontraban hospitales, distritos escolares, instituciones financieras y otras entidades diversas. Sin embargo, no se produjeron detenciones asociadas a Hive, y el grupo se rebautizó como Hunters International en octubre de 2023. Los ciberdelincuentes suelen utilizar esta estrategia de cambio de marca después de un ataque importante.

El grupo realizó un cambio notable en su funcionamiento: ya no ofrecen descuentos ni negocian con las víctimas a partir de la petición de rescate inicial, como se muestra en la figura 15.

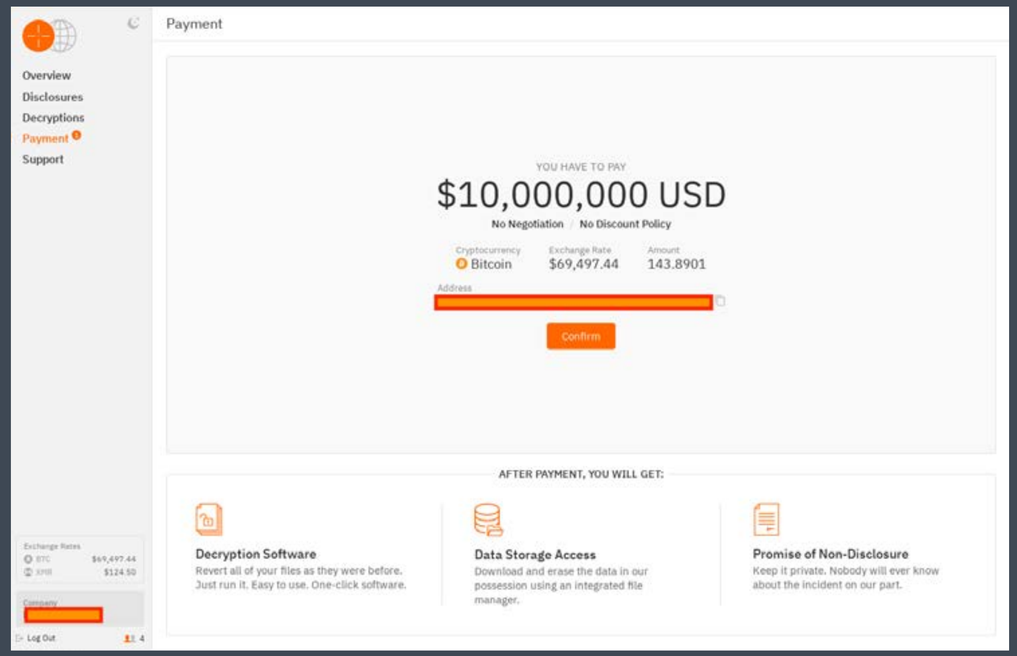


Figura 15: Portal de víctimas de Hunters International que no recibieron descuentos ni negociaron los precios.

La política de precios no negociables es **muy poco común** entre los grupos de ransomware, que suelen ofrecer descuentos significativos respecto a la petición de rescate original. Esta decisión del equipo de Hunters conducirá probablemente a un menor volumen global de pagos, pero a importes globales más elevados.

Hunters International sigue lanzando nuevos ataques y es probable que siga siendo una amenaza formidable si no se producen más detenciones y acusaciones penales.

[12] US Department of Justice, **U.S. Department of Justice Disrupts Hive Ransomware Variant**, 26 de enero, 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, proporcionando información sobre sus tácticas, impacto potencial y actividad reciente.

#1 Dark Angels

El grupo de ransomware Dark Angels, que opera el sitio de fuga 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 a una víctima que pagó a Dark Angels 75 millones de dólares, una cantidad superior a cualquier otra conocida públicamente, un logro que sin duda atraerá el interés de otros atacantes que busquen replicar tal éxito adoptando sus tácticas clave (que describimos a continuación). Dark Angels se centra en varios sectores, como la sanidad, 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 con la mayoría de los grupos de ransomware, que atacan a las víctimas de manera 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 los 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 del orden de 1 a 10 TB. En el caso de las grandes empresas, el grupo ha exfiltrado entre 10 y 100 TB de datos, cuya transferencia puede llevar de días a semanas.

El ataque de más alto perfil llevado a cabo por Dark Angels fue en septiembre de 2023, cuando el grupo vulneró un conglomerado internacional que proporciona soluciones para sistemas de automatización de edificios, entre otros servicios. Dark Angels exigió un rescate de 51 millones de dólares, afirmó haber robado más de 27 TB de datos corporativos y cifró 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 utilizaba el ransomware antes de la acción de las fuerzas del orden contra RagnarLocker,[13] que concluyó con la detención de un miembro clave en octubre de 2023. Tenga 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 dirigirse a un pequeño número de empresas de alto valor para obtener grandes pagos es una tendencia que conviene seguir de cerca. Zscaler ThreatLabz prevé que otros grupos de ransomware tomarán nota del éxito de Dark Angels y podrían adoptar tácticas similares, centrándose en objetivos de alto valor y aumentando la importancia del robo de datos para maximizar sus ganancias financieras.

[13] Europol, **Ragnar Locker ransomware gang taken down by international police swoop**, 20 de octubre, 2023.

#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 a sus afiliados para llevar a cabo violaciones, exfiltrar datos e implementar su ransomware. La infiltración suele comenzar a través de correos electrónicos de spam que contienen archivos adjuntos o enlaces maliciosos. Otros métodos incluyen la ejecución de ataques de fuerza bruta contra contraseñas dirigidas a credenciales de Protocolo de Escritorio Remoto (RDP) o VPN, la compra de credenciales robadas comprometidas a través de intermediarios de acceso inicial y la explotación de aplicaciones orientadas al público. La red de ciberdelincuentes de LockBit ha apuntado a sectores críticos como la fabricación, la sanidad y la logística. El grupo ha atacado colectivamente más de 2000 sistemas en todo el mundo y ha obtenido más de 120 millones de dólares de sus víctimas.

Durante el último año, LockBit se ha mantenido a la cabeza en cuanto a volumen de ataques. Utilizando una estrategia notablemente diferente a la de Dark Angels, el grupo LockBit anima a sus afiliados a atacar a 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.

El ransomware LockBit se implementa en sistemas basados en Windows y Linux. Existen tres versiones de LockBit para Windows: LockBit Red (la original), LockBit Black (basada en el código fuente de BlackMatter) y LockBit Green (basada en el código fuente fugado de Conti). Como se menciona en el Informe sobre ransomware deThreatLabz 2023, el ensamblador de LockBit Black se fugó 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 implementada del grupo. La variante específica del ransomware LockBit utilizada para cifrar los archivos de una víctima se muestra ahora en la nota de rescate junto a la identificación de la víctima. Esto permite al actor que lleva a cabo el ataque identificar fácilmente la variante de LockBit implementada para ayudarle a proporcionar la herramienta de descifrado adecuada cuando se pague el rescate. Véase en la figura 16 un ejemplo de una nota de rescate reciente de LockBit Black.

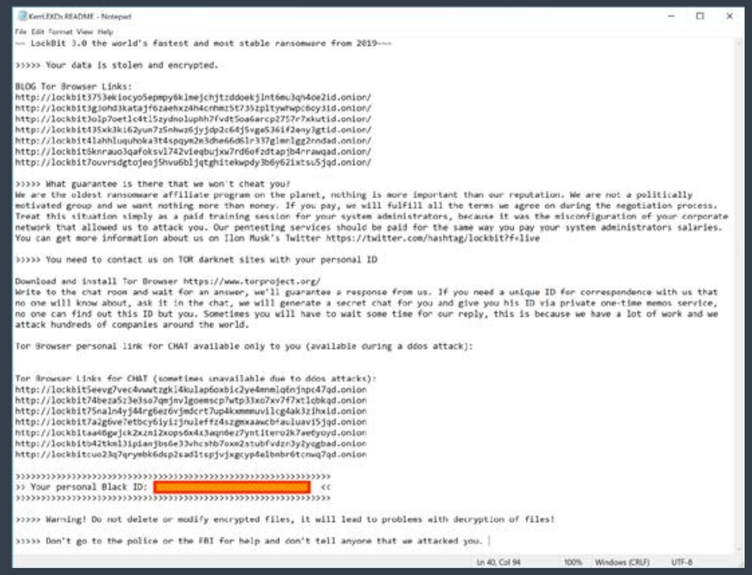


Figura 16: Ejemplo de una nota de rescate reciente de LockBit Black.

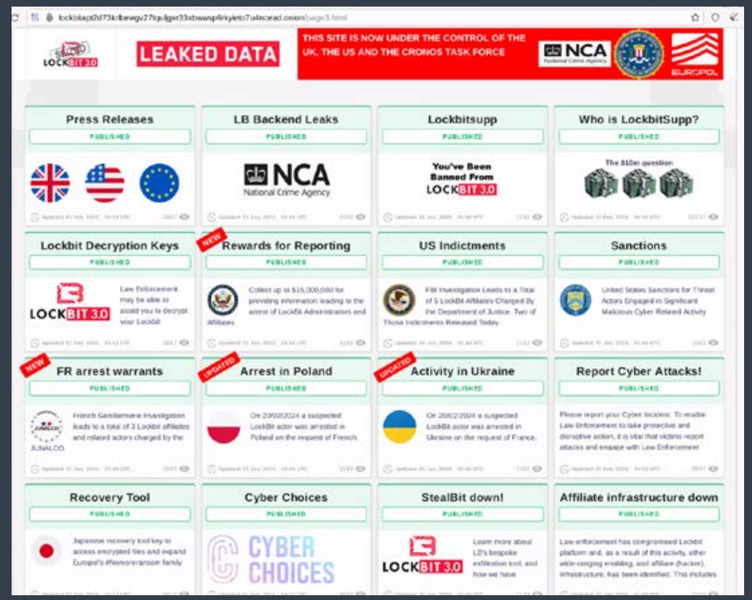


Figura 17: Incautación por parte de las fuerzas del orden del sitio de fuga de datos de LockBit.

El 20 de febrero de 2024, el FBI y las fuerzas del orden del Reino Unido incautaron parte de la infraestructura de LockBit, que incluía aproximadamente 7000 claves de descifrado de víctimas. Tras la incautación, las fuerzas del orden requisaron el sitio web de la fuga de datos de LockBit y engañaron a los ciberdelincuentes con una versión similar al sitio anterior en la que se mostraban varios artículos y temporizadores de cuenta atrás hasta que se publicara nueva información, como se muestra en la figura 17 a continuación.

Lamentablemente, pocos días después del desmantelamiento, ThreatLabz identificó nuevos ataques de ransomware perpetrados por LockBit y un nuevo sitio de fuga de datos. El grupo ha permanecido activo y ha atacado a docenas de nuevas entidades desde la actuación de las fuerzas del orden.

El 7 de mayo de 2024, el FBI anunció la imputación del desarrollador y operador de LockBit, Dmitry Yuryevich Khoroshev. Sin embargo, el operador de LockBit negó rápidamente que el FBI le hubiera identificado correctamente. Sin nuevas detenciones, es probable que los ataques de LockBit continúen en un futuro previsible, aunque en algún momento ThreatLabz espera que la marca LockBit sea retirada y la operación resucitada bajo otro nombre debido a un mayor escrutinio.

#3 BlackCat

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

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

BlackCat fue una de las familias de ransomware más compatibles entre plataformas, en parte porque utiliza el lenguaje de programación Rust. En la figura 18 se muestran las herramientas de descifrado disponibles para todas las plataformas que eran compatibles con el ransomware BlackCat justo antes de que el grupo cesara sus operaciones. Las plataformas incluían Windows, ESXi, FreeBSD y numerosas variantes de sistemas operativos Linux y arquitecturas, como ARM, x86/x64 y PowerPC.

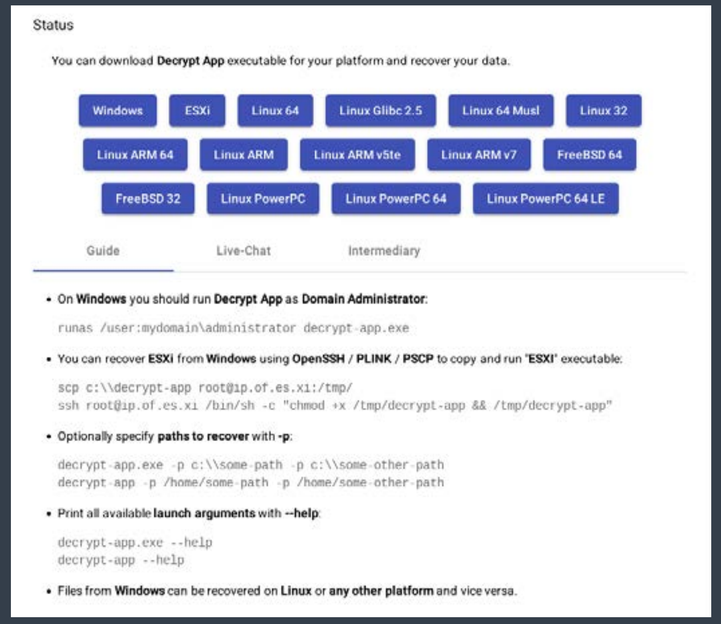


Figura 18: Se proporcionaron herramientas de descifrado BlackCat para 15 sistemas operativos, arquitecturas y plataformas diferentes.

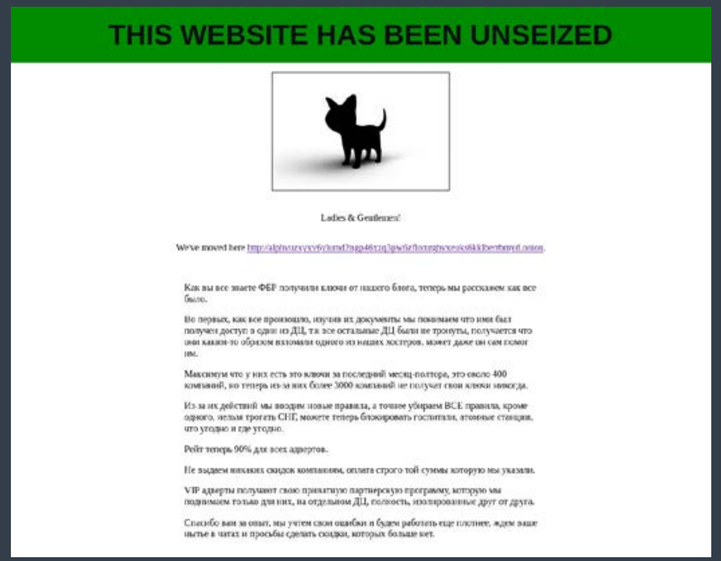


Figura 19: Sitio de fuga de datos "no incautados" de BlackCat después de una acción de las fuerzas del orden.

Este nivel de compilación multiplataforma es inusual en comparación con otras familias de ransomware que normalmente solo son compatibles con Windows, ESXi y un pequeño número de plataformas basadas en Linux. Esto indica que los afiliados de BlackCat pueden haber solicitado soporte para plataformas adicionales con el fin de cifrar archivos en el mayor número de sistemas posible.

En diciembre de 2023, el FBI obtuvo acceso a parte de la infraestructura de BlackCat. El FBI intentó confiscar los sitios web del grupo basados en Tor, incluidos los portales de negociación de rescates y los sitios de fuga de datos. Sin embargo, tras un rápido giro de los acontecimientos, BlackCat publicó un mensaje en el que informaba de que había "desincautado" el sitio web de fuga de datos y proporcionaba un enlace a un nuevo sitio web que el FBI no podía manipular, como se muestra en la figura 19 a continuación.

Este tira y afloja entre el FBI y BlackCat se prolongó durante varios días hasta que BlackCat tuvo la certeza de que el nuevo sitio de fuga de datos tenía suficiente publicidad. Tenga en cuenta que "incautar" un sitio web basado en Tor no es tan sencillo como un sitio web tradicional basado en DNS porque se basa en secretos criptográficos en lugar de en una autoridad central sujeta a órdenes judiciales.

En marzo de 2024, el grupo BlackCat anunció su disolución, alegando el compromiso de su infraestructura por parte del FBI, lo que supuestamente les imposibilitó continuar con sus operaciones. Sin embargo, surgieron sospechas debido al momento en que se produjo su cierre, inmediatamente después de recibir un rescate de 22 millones de dólares y, posteriormente, realizar una estafa de salida a un afiliado que les ayudó a vulnerar un proveedor de servicios sanitarios (de lo que ya se ha hablado anteriormente en este informe).

Aunque el ransomware BlackCat ya no está activo, es probable que los afiliados que estaban detrás de los ataques del grupo hayan migrado a otras redes de ransomware como servicio, como RansomHub (donde desde entonces se han fugado los datos robados al proveedor sanitario que pagó el rescate de 22 millones de dólares). Además, es poco probable que el propio grupo de ransomware BlackCat realmente haya cesado sus operaciones y es probable que resurja bajo una nueva marca.

[14] Cybersecurity & Infrastructure Security Agency, **Cybersecurity Advisory: Scattered Spider**, 16 de noviembre, 2023.
[15] Krebs on Security, **Alleged Boss of 'Scattered Spider' Hacking Group Arrested**, 15 de junio, 2024.

#4 Akira

El ransomware Akira irrumpió en escena en abril de 2023 y rápidamente ganó infamia por el volumen de ataques realizados por sus afiliados. 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 fugado 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 afiliados del ransomware Akira han empleado varios mecanismos de acceso inicial, incluso a través de la explotación de CVE-2023-20269.[16] El grupo de amenazas que opera Bumblebee, vinculado al ransomware Conti, también ha sido conocido por ser un intermediario de acceso inicial para Akira. Como se mencionó 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 accedieron inicialmente a la red de la empresa a través de un intermediario de acceso inicial, y también ofreció 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 algunas fallas que recomendamos eliminar:

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

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 un software de copia de seguridad con almacenamiento en la nube que funcione con 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 por su cautela en materia de seguridad.

Aunque estos consejos proceden directamente de Akira, las recomendaciones son válidas y proporcionan una base para comprender y frustrar este tipo de ataques.

Akira es uno de los únicos grupos importantes de ransomware que no ha sido objeto directo de una intervención de 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

#5 Black Basta

El ransomware Black Basta, identificado por primera vez en abril de 2022, es otro sucesor del grupo de ransomware Conti. Los afiliados 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 ya se ha mencionado, Pikabot intervino para llenar el vacío tras su caída. Sin embargo, Pikabot se cerró después de la Operación Endgame en mayo de 2024.

Desde entonces, ThreatLabz ha estado rastreando nuevas actividades del grupo de amenazas Qakbot, que ha pivotado 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 lugar 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. El autor de la llamada 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 malintencionado, se ejecuta un script por lotes de Windows para realizar un reconocimiento, robar credenciales e instalar una puerta trasera en el sistema de la víctima. La puerta trasera continúa 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.

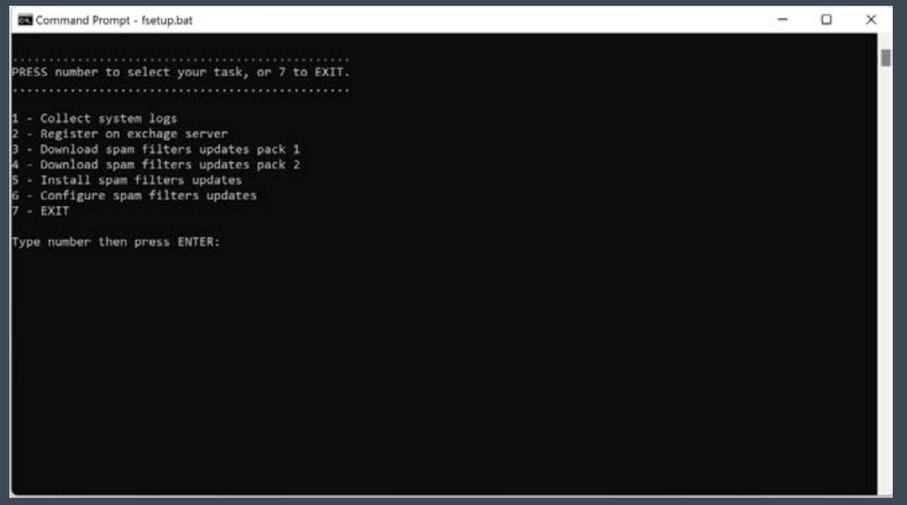


Figura 20: Interfaz de script por lotes malicioso de Windows utilizada para establecer una puerta trasera en el sistema de la víctima como precursor de un ataque de ransomware Black Basta.

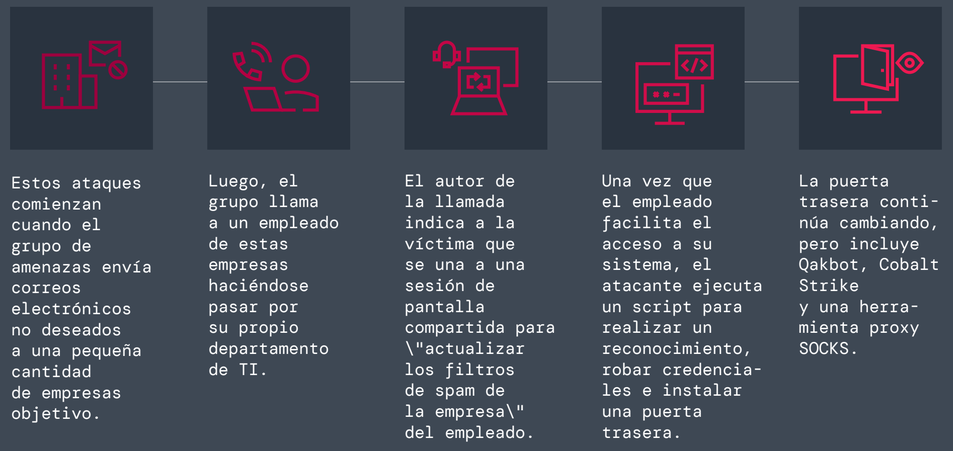


Figura 21: Cadena de ataque del ransomware Black Basta con acceso inicial gestionado por el grupo de amenazas Qakbot.

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.

Repositorio de notas de ransomware de ThreatLabz

Zscaler ThreatLabz ha estado manteniendo un **repositorio público en GitHub** que, en el momento de la redacción de este informe, rastrea 391 familias de ransomware y contiene un total de 945 notas de rescate, añadiendo 19 familias y 55 notas de rescate entre abril de 2023 y abril de 2024. Este repositorio 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 relacionar grupos de ransomware que cambian de marca mediante el análisis estilométrico.

La figura 22 muestra una comparación estilométrica entre un chat de rescate de Conti (arriba) y un chat de rescate de Black Basta (abajo). Esto demuestra que los miembros de Black Basta son casi con toda seguridad antiguos miembros de Conti, tal y como se evidencia en las semejanzas en la estructura de sus frases, la elección de palabras e incluso las instrucciones específicas.

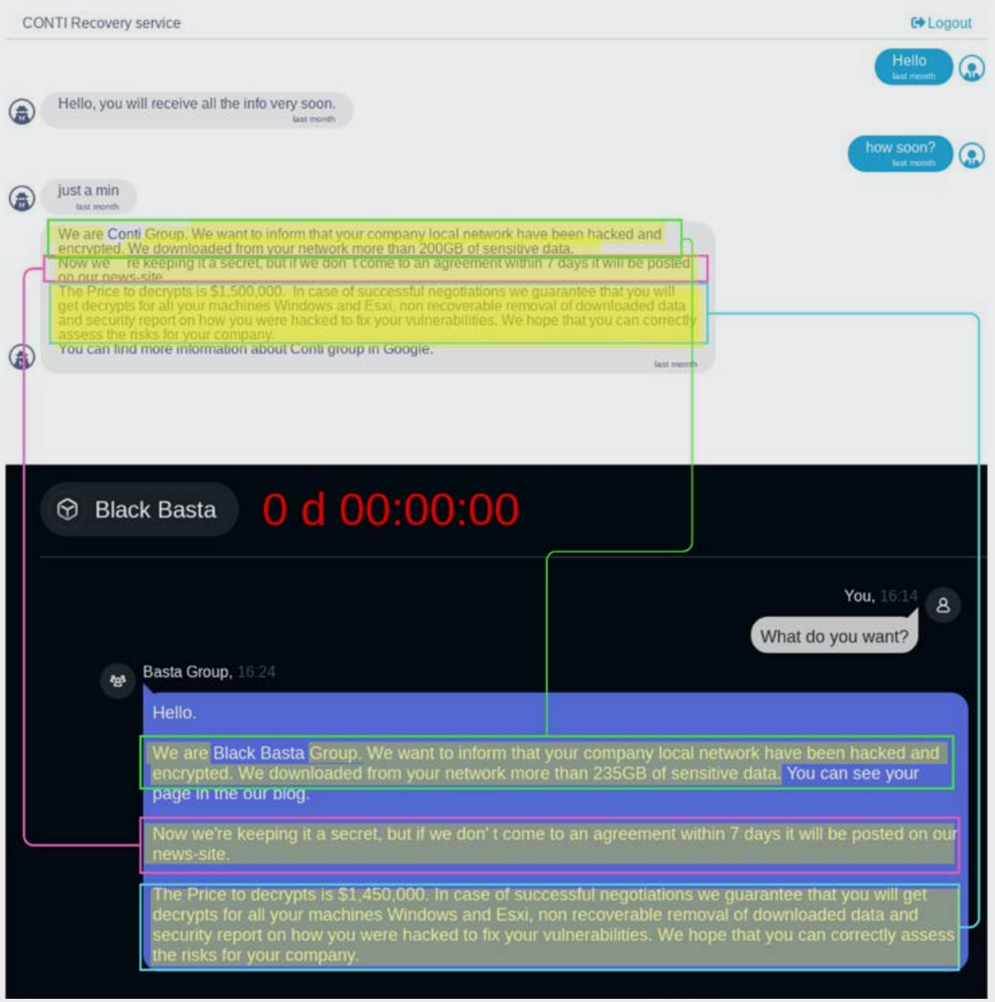


Figura 22: Comparación estilométrica entre los chats de rescate de Conti (arriba) y Black Basta (abajo).

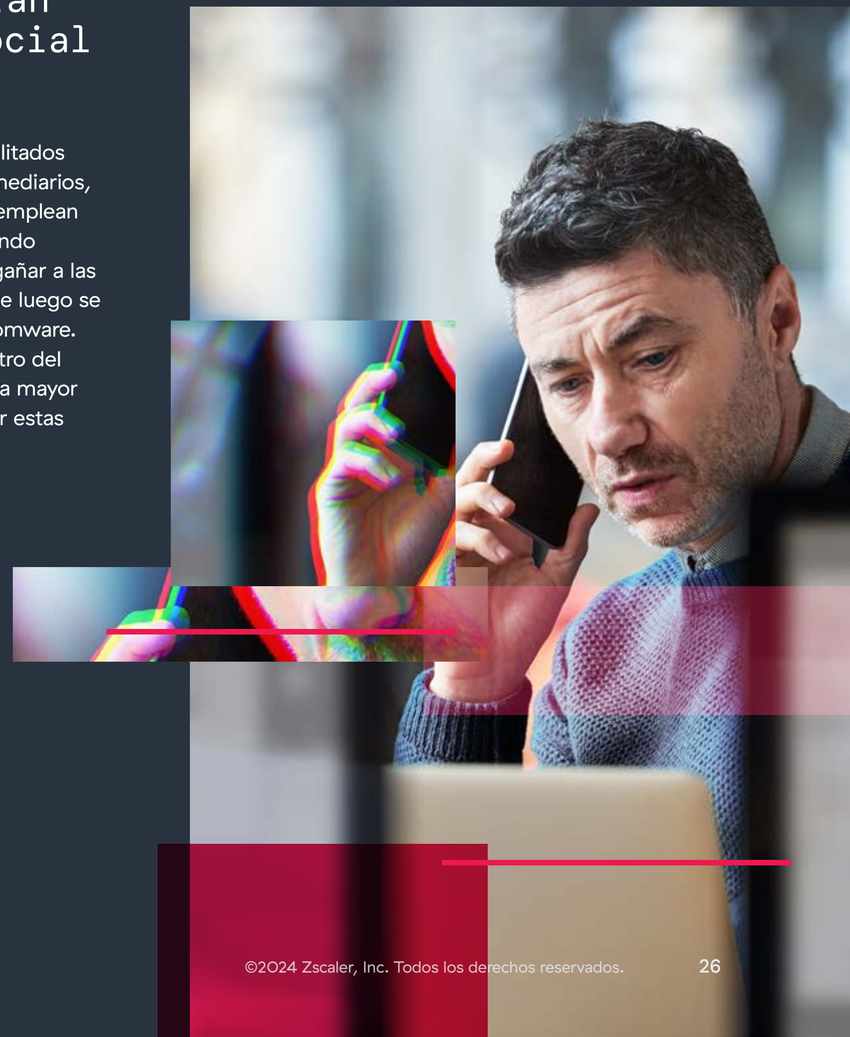
Predicciones para 2025

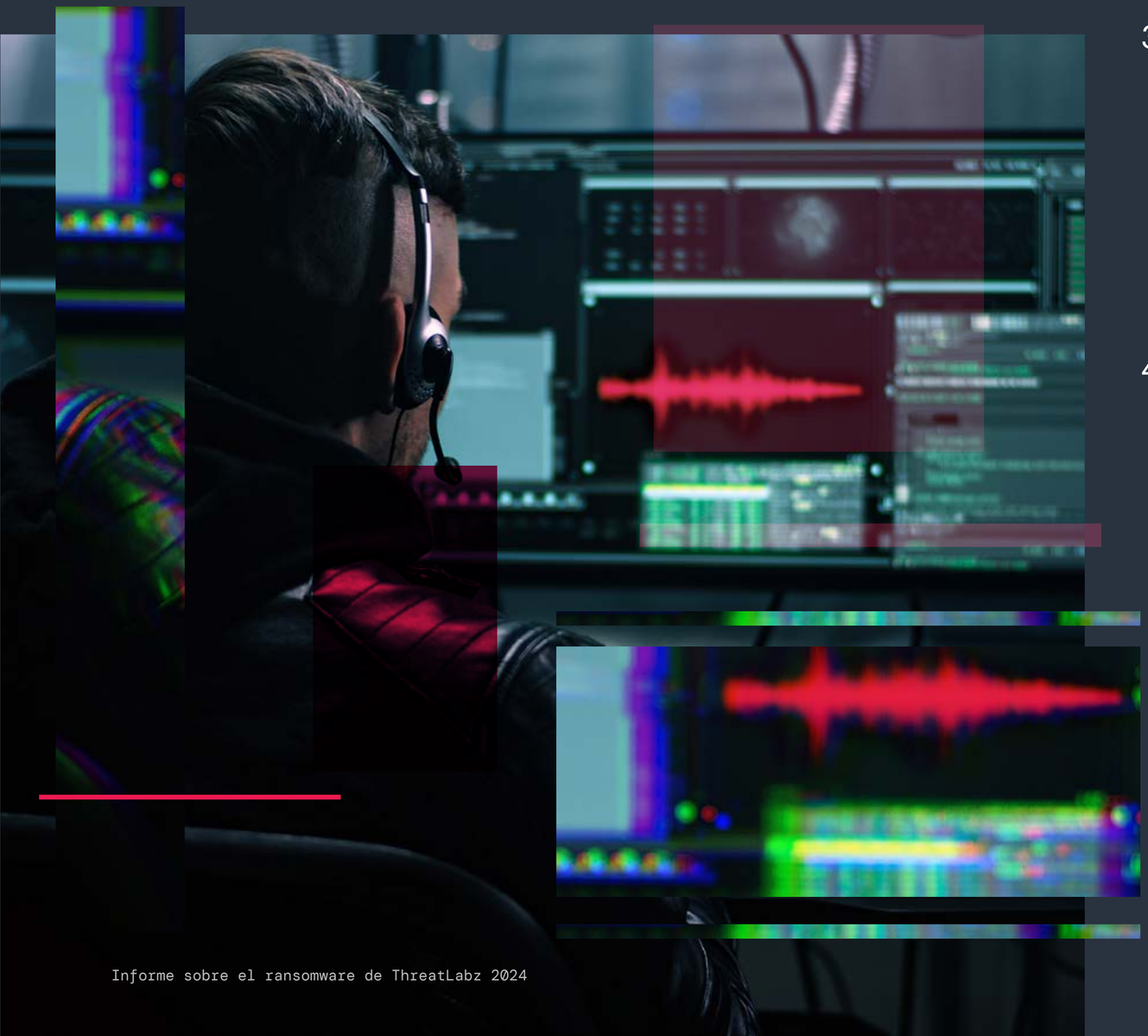
1. Los actores de amenazas de ransomware adoptarán estrategias de ataque muy selectivas.

Durante el último año, Dark Angels ha sido uno de los grupos de ransomware más exitosos y menos conocidos, con una clara estrategia que consiste en dirigirse a un pequeño número de empresas multimillonarias y extorsionarlas para obtener sustanciosos rescates. Esta estrategia tiene un doble objetivo: reducir el escrutinio de las fuerzas del orden y del sector de la seguridad, al tiempo que se destinan más recursos para infiltrarse en grandes empresas dispuestas a pagar importantes rescates para proteger enormes volúmenes de datos robados. Esto ha llevado al grupo a recibir el mayor pago de rescate conocido, 75 millones de dólares, lo que sin duda atraerá el interés de otros actores de amenazas de ransomware en 2025 que podrían querer replicar su éxito.

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

En 2025, esperamos ver un aumento de los ataques dirigidos facilitados por intermediarios especializados en el acceso inicial. 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 la voz ("vishing") para engañar a las personas para que concedan acceso a un entorno corporativo, que luego se utiliza en última instancia para exfiltrar datos y implementar ransomware. Esta tendencia emergente pone de relieve las colaboraciones dentro del ecosistema de los ciberdelincuentes y subraya la necesidad de una mayor vigilancia y de medidas de seguridad avanzadas para contrarrestar estas amenazas en evolución.





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

La creciente adopción de la IA generativa en 2025 y más allá permitirá a los actores malintencionados elaborar correos electrónicos de spam con gramática y ortografía precisas, así como utilizar la clonación de voz para hacerse pasar por personal con el fin de obtener acceso privilegiado. En los próximos años, es posible que las voces generadas por la IA se personalicen con acentos y dialectos locales para mejorar la credibilidad y aumentar las probabilidades de éxito, y se conviertan en un ejemplo de cómo los actores 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 normas de la SEC.

Con la resolución de la SEC que obliga a informar de manera más estricta sobre los incidentes de ciberseguridad, en 2025 seguirán aumentando las organizaciones que revelen incidentes de ransomware. Es de esperar que esto se traduzca en una mayor transparencia y promueva una cultura de responsabilidad y defensa proactiva, fomentando mejoras en las prácticas de ciberseguridad.

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

Los ataques que exfiltran grandes cantidades de datos, incluidos más incidentes sin cifrado, aumentarán considerablemente en el próximo año. Esta tendencia, que empezó a cobrar fuerza en 2022, muestra cómo los malintencionados se centran únicamente en la exfiltración de datos sin cifrar los sistemas. Este enfoque permite realizar operaciones más rápidas y oportunistas y aprovecha el miedo a que se divulguen datos confidenciales para coaccionar a las víctimas a pagar rescates. Destaca un cambio continuo en las estrategias del ransomware hacia métodos más eficaces y de mayor impacto.

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

El gran valor de los datos sanitarios seguirá atrayendo miradas en 2025. Muchas empresas sanitarias se retrasan en la sustitución de los sistemas heredados por medidas de seguridad modernas y avanzadas, lo que las hace especialmente vulnerables. Como resultado, es probable que estas organizaciones se enfrenten a repetidas violaciones e intentos de extorsión. Aquellos que no tomen las medidas adecuadas para dar prioridad a las estrategias de defensa Zero Trust pueden encontrarse en el punto de mira de los grupos de ransomware.

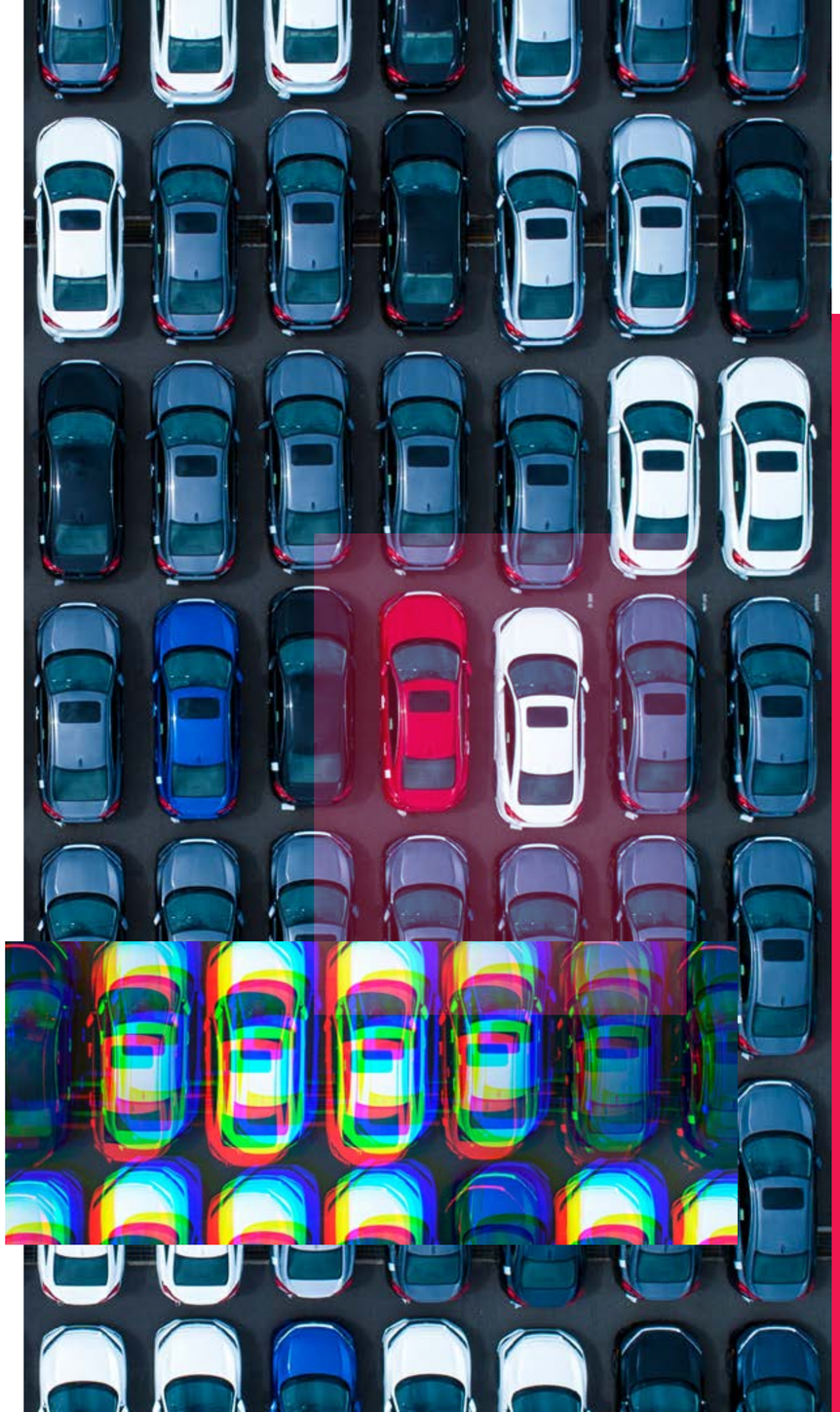
7. La colaboración internacional contra las organizaciones de ciberdelincuentes se basará en los esfuerzos existentes.

Las fuerzas del orden y la industria privada seguirán colaborando en los esfuerzos para combatir los ataques de ransomware, como la desarticulación de los principales intermediarios de acceso inicial y grupos de ransomware. La colaboración internacional será cada vez más vital a medida que aumente la interconexión mundial, lo que facilitará a los ciberdelincuentes operar a escala transnacional. Al compartir inteligencia y experiencia, estas acciones coordinadas desarticularán con mayor eficacia las redes mundiales de ransomware. Zscaler ThreatLabz ha estado a la vanguardia y ha desempeñado un papel decisivo en la prestación de asistencia técnica para varias de estas operaciones durante el último año.

Cómo Zscaler simplifica la protección contra ransomware

La creciente complejidad y costo de los ataques de ransomware subraya la necesidad de defensas Zero Trust integrales. La plataforma Zscaler Zero Trust Exchange™ simplifica las dificultades, ofreciendo un enfoque integral para detener el ransomware.

Zero Trust Exchange permite a las empresas implementar defensas más inteligentes en cada fase de un ataque. Esto empieza por impedir que los atacantes descubran o exploten usuarios y aplicaciones haciendo que dichos usuarios y aplicaciones sean invisibles, accesibles solo para usuarios o dispositivos autorizados. Además, inspecciona todo el tráfico entrante y saliente en línea, cifrado o no. Los usuarios y dispositivos autenticados se conectan directamente a las aplicaciones que necesitan y nunca a la red, por lo que, aunque un atacante consiga entrar, no podrá desplazarse lateralmente para robar o cifrar datos.



POR QUÉ ZERO TRUST ES ESENCIAL PARA LA PROTECCIÓN CONTRA EL 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 firewalls de "nueva generación" y las VPN, a menudo introducen puntos ciegos, complejidad y costos significativos. Estos enfoques heredados no consiguen inspeccionar de manera rentable los archivos y el tráfico cifrados, lo que deja a las organizaciones vulnerables a los movimientos laterales y a los ataques de ransomware que aprovechan las brechas de visibilidad y control, a menudo con consecuencias devastadoras.

BIENVENIDA ZERO TRUST:
Una arquitectura Zero Trust asume que cada usuario, dispositivo y conexión está potencialmente comprometido. Este enfoque exige una verificación continua y un control de acceso estricto. Al verificar sistemáticamente las identidades e inspeccionar todo el tráfico, incluidos los datos cifrados, Zero Trust reduce significativamente el riesgo de que los ataques se propaguen por la red, neutralizando las amenazas de ransomware antes de que puedan infligir daños.

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

Minimice la superficie de ataque: Creado con una arquitectura Zero Trust, el Zero Trust Exchange sustituye a las arquitecturas explotables de VPN y firewalls heredadas que amplían la superficie de ataque. Zscaler minimiza eficazmente la superficie de ataque ocultando usuarios, aplicaciones y dispositivos tras un proxy en la nube, donde no son visibles ni detectables desde Internet. Del mismo modo que una centralita enruta las llamadas a los destinos autorizados, Zscaler solo conecta al usuario o dispositivo correcto y autorizado a una aplicación concreta.

Evitar el compromiso inicial: Zero Trust Exchange implementa una amplia inspección SSL/TLS, aislamiento del navegador, sandboxing avanzado en línea y controles de acceso basado en políticas para evitar que los usuarios accedan a sitios web maliciosos y detectar amenazas desconocidas antes de que lleguen a su red. Esto minimiza el riesgo de compromiso inicial.

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 puesto de control de seguridad para el tráfico de Internet, eliminando las vías para el movimiento lateral. Zscaler también puede identificar y detener el movimiento lateral de posibles atacantes, ya sean amenazas externas o personal interno malintencionado, a través de las capacidades de detección y respuesta a amenazas de identidad (ITDR) y de engaño.

Detenga la pérdida de datos: Las medidas de prevención de pérdida de datos en línea, combinadas con la inspección completa TLS/SSL, frustran eficazmente los intentos de robo de datos. Zscaler garantiza la seguridad de los datos tanto en tránsito como en reposo.

COMBATIR LAS AMENAZAS IMPULSADAS POR LA IA CON IA + INNOVACIÓN ZERO TRUST

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

- ***La detección de phishing y C2 potenciada por IA*** utiliza la detección en línea basada en la IA de Zscaler Secure Web Gateway para identificar y bloquear sitios de phishing nunca vistos e infraestructuras de comando y control (C2).
- ***El sandboxing impulsado por la 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 la IA*** ofrece recomendaciones automatizadas de políticas de acceso para minimizar la superficie de ataque y evitar el movimiento lateral, utilizando el contexto del usuario, el comportamiento, la ubicación y la telemetría de aplicaciones privadas.
- ***La política dinámica basada en el riesgo analiza*** continuamente el riesgo asociado a los usuarios, los dispositivos y las aplicaciones para aplicar políticas dinámicas de seguridad y acceso.
- ***El aislamiento del navegador basado*** en IA crea una brecha segura entre los usuarios y los contenidos web maliciosos al renderizar las páginas como flujos de imágenes perfectas, lo que evita las filtraciones de datos y la propagación de amenazas activas.
- ***El descubrimiento y la clasificación de datos impulsados por la IA*** proporcionan visibilidad y clasificación instantáneas de los datos desde el primer momento en los datos de los puntos finales, en línea y en la nube, lo que dificulta que el ransomware apunte a los datos confidenciales y los cifre.

Prevención integral en cada etapa de la cadena de ataque

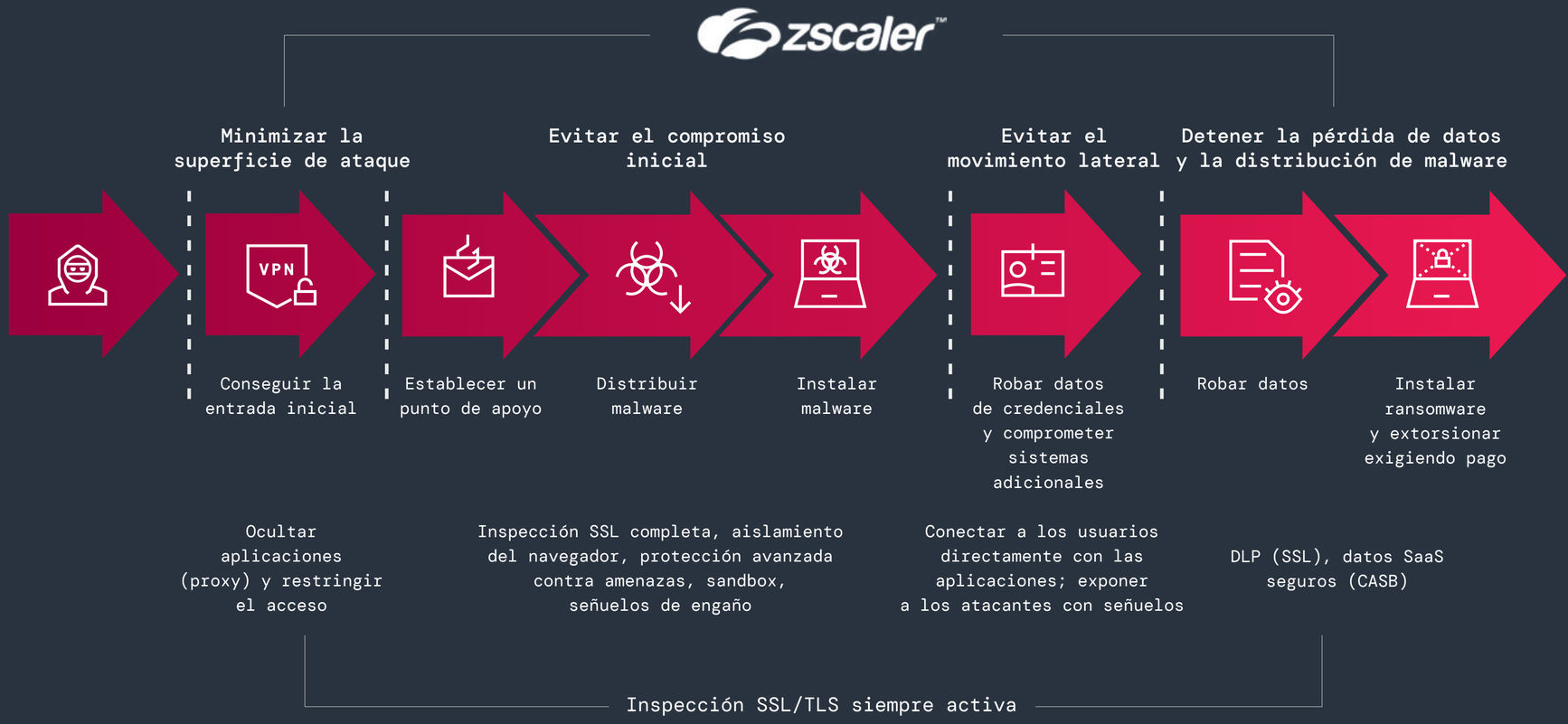


Figura 23: Mapeo de la arquitectura Zero Trust a lo largo de la cadena de ataque del ransomware

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 Zero Trust. ZPA garantiza que solo los usuarios y dispositivos autorizados puedan acceder a las aplicaciones críticas, reduciendo así la superficie de ataque y evitando los intentos de ransomware.

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

Zscaler Deception el servicio de engaño de Zscaler 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 los archivos y ejecutables sospechosos en un entorno virtual controlado, ayudando a identificar y bloquear el código malicioso, 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 exploits de día cero que pueden utilizar los operadores de ransomware.

Zscaler ITDR (detección y respuesta a amenazas a la identidad por sus siglas en inglés) detecta y protege contra ataques basados en la identidad, como el robo de credenciales y el abuso de privilegios, asaltos a Active Directory y autorizaciones peligrosas.

Zscaler Data Protection proporciona una seguridad consistente y unificada para los datos en movimiento y los datos en reposo a través de SaaS y aplicaciones de nube pública, reduciendo la probabilidad de exfiltración de datos al tiempo que mitiga el impacto potencial de los ataques de ransomware.

Guía para la prevención del ransomware

Una estrategia de defensa basada en una arquitectura Zero Trust es una medida de seguridad probada para detener el ransomware, pero hacer frente a esta amenaza multifacética exige una planificación proactiva, una colaboración continua e inversiones estratégicas.

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

- **Implemente copias de seguridad periódicas y seguras de los datos.** Asegúrese de que se realicen copias de seguridad periódicas y seguras de todos los datos, incluidas las copias de seguridad fuera de línea. Adapte las estrategias de copia de seguridad en función de la evolución de las amenazas.
- **Mantenga el software actualizado.** Aplique los últimos parches de seguridad rápidamente para abordar las vulnerabilidades conocidas. Utilice plataformas de inteligencia sobre amenazas basadas en IA para priorizar y gestionar parches de seguridad de manera eficaz.
- **Active 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.
- **Establezca una política de seguridad corporativa uniforme.** Asegúrese de que todos los usuarios sigan procedimientos de seguridad uniformes, incluyendo MFA y actualizaciones regulares de seguridad, para ayudar a prevenir compromisos iniciales. Con una fuerza de trabajo distribuida, es aún más importante implementar una arquitectura de perímetro de servicio de seguridad (SSE) para proteger a los usuarios estén donde estén.
- **Refuerce la seguridad de las aplicaciones.** Elimine aplicaciones de la Internet pública para evitar que los actores de amenazas de ransomware aprovechen las vulnerabilidades. Implemente una arquitectura Zero Trust para las aplicaciones internas para protegerlas contra intentos de ransomware.
- **Implemente el acceso con privilegios mínimos.** Implemente políticas de privilegios mínimos para restringir el acceso de los usuarios únicamente a los recursos necesarios para sus funciones. Utilice soluciones basadas en IA para analizar dinámicamente el comportamiento de los usuarios y adaptar los privilegios de acceso en consecuencia.
- **Refuerce la protección de identidades.** Utilice las herramientas ITDR para obtener visibilidad de las configuraciones erróneas de identidad, remediar las vulnerabilidades en Active Directory que los adversarios aprovechan para escalar privilegios y desplazarse lateralmente, y detectar las amenazas de identidad sigilosas.
- **Inspeccione todo el tráfico.** Actualmente, 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.
- **Implemente el acceso a la red Zero Trust (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.

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

- **Emplee un sandboxing avanzado impulsado por la IA.** Detenga el malware inédito y elusivo con un sandbox que detecta y pone en cuarentena automáticamente las amenazas desconocidas y los archivos sospechosos aprovechando el análisis de IA/ML.

- **Implemente la prevención de pérdida de datos (DLP) en línea.** Protéjase contra la exfiltración y exposición de datos implementando medidas de DLP en línea.

- **Aproveche la tecnología del engaño.** Emplee herramientas de engaño y honeypots para desviar a los atacantes, fortificando las defensas contra la infiltración en el sistema.

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

- **Imparta capacitación continua a los empleados.** Ofrezca capacitación periódica de concientización sobre seguridad para educar a los empleados sobre las amenazas del ransomware. Realice simulaciones de escenarios reales de ransomware para mejorar la preparación de los empleados.

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

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

ThreatLabz también mantiene repositorios de GitHub con IOC, herramientas (incluidas herramientas de descifrado de ransomware de prueba de concepto) y un repositorio 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 consiste en un proceso exhaustivo que utiliza varias fuentes de datos para identificar y rastrear las tendencias del 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 y violaciones 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 maliciosa.

- **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 las fuerzas del orden, que proporcionaron información adicional sobre los atacantes de ransomware, sus objetivos y sus métodos.

- **El análisis de muestras de ransomware y datos de ataques realizado por el propio equipo de ThreatLabz.** El equipo de Inteligencia de Amenazas de ThreatLabz rastrea familias de ransomware a escala mediante ingeniería inversa y automatizando el análisis de malware para desarrollar estrategias de respuesta eficaces. ThreatLabz también colabora estrechamente con las fuerzas del orden internacionales y ha desempeñado un papel importante en acciones recientes, como la Operación Duck Hunt y la Operación Endgame.

Acerca de ThreatLabZ

ThreatLabz es la rama de investigación de seguridad de Zscaler. Este equipo de primer nivel es responsable de la búsqueda de nuevas amenazas y de garantizar que las miles de organizaciones que utilizan la plataforma global de Zscaler estén siempre protegidas. Además de la investigación de malware y el análisis conductual, los miembros del equipo están involucrados en la investigación y el desarrollo de nuevos módulos de prototipo para la protección avanzada contra amenazas en la plataforma Zscaler, y realizan auditorías de seguridad internas regularmente para garantizar que los productos e infraestructura de Zscaler cumplan con los estándares 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, resistentes y seguros. Zero Trust Exchange™ protege a miles de clientes contra ciberataques y pérdida de datos al conectar usuarios, dispositivos y aplicaciones de manera segura en cualquier ubicación. Distribuido en más de 150 centros de datos en todo el mundo, Zero Trust Exchange, basado en SASE, es la plataforma de seguridad en la nube en línea más grande del mundo.
Para obtener más información, visite **www.zscaler.com.**

Experience your world, secured.™