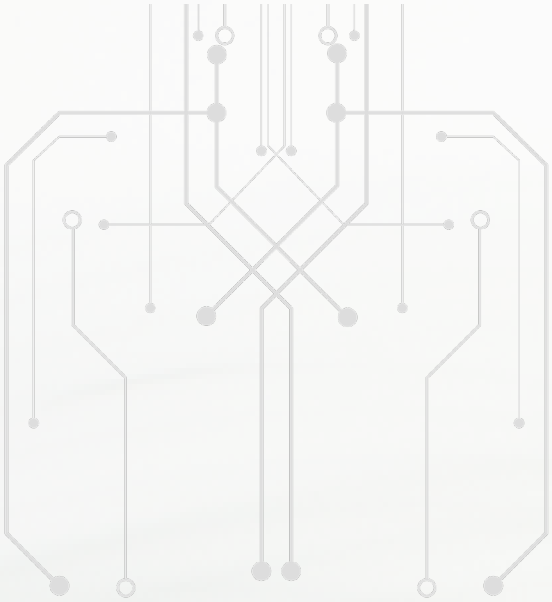
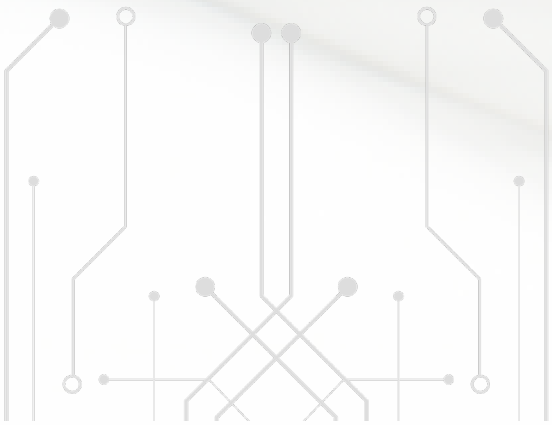
Panorama del Ransomware 2024

Informe de Ciberinteligencia

Lab52

Tabla de contenidos





INTRODUCCIÓN

Uno de los tipos de malware que más ha contribuido a la actividad cibercriminal es el Ransomware. En particular, el Ransomware as a Service (RaaS) ha supuesto un nuevo tipo de negocio, que se adapta a los nuevos cambios y golpes que recibe dicha industria por parte de los cuerpos y fuerzas de seguridad. El hecho es, que esta industria del ciberdelito sufre también sus propios problemas de seguridad, con diferentes fugas de su activo más preciado: herramientas propietarias usadas para proteger su código y dificultar su análisis. Estos problemas permiten que actores que podrían invertir menos en desarrollo de malware y su protección, se vean beneficiados y apliquen medidas de protección robustas.

En todo este contexto actual, la atribución, considerando lo anterior, se complica más aún. Pese a que existen esfuerzos conjuntos de fuerzas y cuerpos de seguridad a escala internacional para desmantelar la infraestructura de los grupos más fuertes y realizar arrestos de sus principales integrantes, nada parece frenar esta actividad. Sirva de ejemplo la Operación Cronos, llevada a cabo por la NCA (National Crime Agency, UK) en cooperación con el FBI (Federal Bureau of Investigation, USA), que en febrero de 2024 intervino la infraestructura de LockBit. LockBit fue, con diferencia, el ransomware de más impacto de 2023, conforme al último informe de S2 Grupo sobre el panorama del ransomware[1].

Dos días tras Operación Cronos fueron publicadas nuevas víctimas de LockBit[2][3]. Dadas las fugas sufridas por la banda durante todo este tiempo (por ejemplo, la filtración del builder de LockBit 3.0 en septiembre de 2022), los expertos no descartan que estos nuevos ataques sean fruto de otros actores[4] y que no se pueda atribuir directamente a la banda principal.

Este informe se centra en el panorama del ransomware tomando como punto de partida el informe previo sobre panorama del ransomware, y destacando las novedades sobre la evolución de los grupos. Los datos mostrados provienen del servicio de ciberinteligencia de S2 Grupo, que se nutre a su vez del análisis geopolítico y de los análisis y seguimiento de ransomware necesario para mantener al día MicroClaudia, la herramienta de vacunación contra el ransomware del CCN-CERT.

1 https://home.s2grupo.es/informe-ransomware-2023
2 https://www.bleepingcomputer.com/news/security/lockbit-ransomware-returns-restores-servers-after-police-disruption/
3 https://www.bleepingcomputer.com/news/security/police-arrest-lockbit-ransomware-members-release-decryptor-in-global-crackdown/
4 Ransomware associated with LockBit still spreading 2 days after server takedown | Ars Technica

RAAS – DESPLIEGUE DE UNA INFECCIÓN

Una característica comúnmente obviada sobre el RaaS, es que, aunque recibe su nombre del Ransomware, dicho tipo de malware no es más que la última parte de un plan de despliegue mayor, en el que desempeñan un rol fundamental tanto las infraestructuras de despliegue y herramientas seleccionadas como los diferentes actores de la cadena de operadores y afiliados que dan vida al RaaS.

La Ilustración 1 ofrece una descripción general del despliegue de ransomware cuando hay un modelo RaaS detrás.

Tomando como base dicha cadena de sucesos podríamos, tal vez, anticiparnos a un despliegue efectivo de ransomware.

La primera parte del flujo es siempre la vinculada tanto al factor humano como a vulnerabilidades. Mientras que el factor humano puede intentar minimizarse por medio **de planes de concienciación y salud digital,** las vulnerabilidades 0-day suponen un problema únicamente resoluble mediante la **inversión en el descubrimiento de éstas vulnerabilidades antes que los atacantes,** algo no siempre posible para las entidades que emplean los componentes.

Una vez que los atacantes consiguen acceso a la infraestructura, éste puede **venderse a otros actores para el despliegue del ransomware.** Cabe destacar en este punto el análisis de riesgos que pueden hacer los cibercriminales, y el estudio sobre si la entidad es interesante como víctima.

En un modelo RaaS, donde los cibercriminales están organizados, **cada ataque es una inversión en recursos,** comprendiendo: herramientas, infraestructura, tiempo de operadores humanos y también software ad-hoc de los atacantes en los casos más dirigidos.

Desde el punto de vista del análisis del malware, necesario para detener el avance de la infección, **la gestión de las infraestructuras que hace el atacante es crucial.** En ocasiones, un despliegue exitoso priorizando la ejecución en memoria y evitando la persistencia en disco permitiría a los atacantes reducir las posibilidades de detección. Además, proteger su infraestructura es también una medida de durabilidad.

Durante este informe la imagen previa se tomará en varios puntos como base para explicar la evolución del RaaS, los grupos más destacados, y también **cómo podemos usar el conocimiento que tenemos de su operativa para frenar la actividad lo antes posible,** o recuperarnos de un ataque.

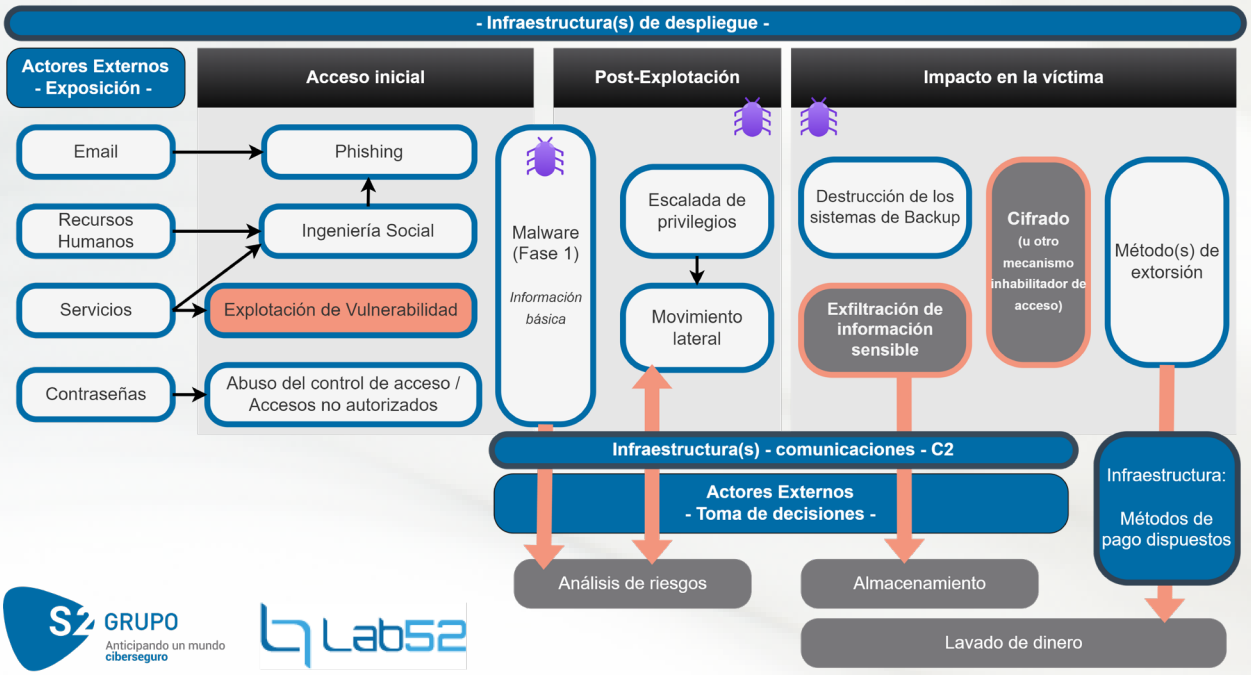


Ilustración 1. Despliegue de Ransomware

1 ACTIVIDAD Y ECONOMÍA DEL RAAS

El gran impulsor del RaaS como modelo es el beneficio económico. En esta sección se describen los principales puntos observados que podrían impactar en el negocio del RaaS.

1.1 ECONOMÍA DEL RANSOMWARE

Uno de los éxitos del RaaS es que consigue adaptarse a las medidas de seguridad que ya implementan sus víctimas potenciales. Si bien durante un ataque se procura eliminar o dañar las copias de seguridad de un sistema, aún cuando esto no es posible han comprobado que con la extorsión también es posible obtener ganancias.

Algunos datos se muestran a continuación. Por ejemplo, conforme a Chainanalysis, los pagos por ransomware excedieron el billón de dólares en 2023. Esto puede ser debido a dos factores: el incremento de la actividad (y del éxito) de los grupos RaaS, pero, también, a la adaptación de su operativa.

En el informe de Chainanalysis atribuyen el descenso de 2022 a una anomalía, y a la negativa de algunas organizaciones a pagar los rescates debido a posibles sanciones, junto con la actividad de las fuerzas y cuerpos de seguridad en la desarticulación de grupos como Hive. Pese a que el anuncio de la intervención de Hive se produjo en enero de 2022, las infiltraciones en la infraestructura de la organización se remontan a Julio de 2022, conforme al comunicado oficial de los involucrados[6].

Sin embargo, las diferentes intervenciones y esfuerzos durante 2023 parecen no haber afectado a la recaudación del ransomware en términos generales, probablemente en parte debido a que éstas se produjeron mayoritariamente a final de año. Cabe destacar también que, conforme investigadores, Hunters International es la nueva marca de Hive, siguiendo dicho grupo activo en el momento de la elaboración de este informe.

La siguiente gráfica procedente del análisis de datos de Coveware muestra un descenso de pagos durante el último trimestre de 2024. Sin embargo, este descenso también se alinea en parte con el tamaño medio de las compañías víctimas de los grupos. Podría comprenderse que a menor tamaño de compañía los pagos demandados también decrecen.

Esta actividad destacada en dicha fuente podría deberse a actividad de grupos específicos, abordados durante este informe.

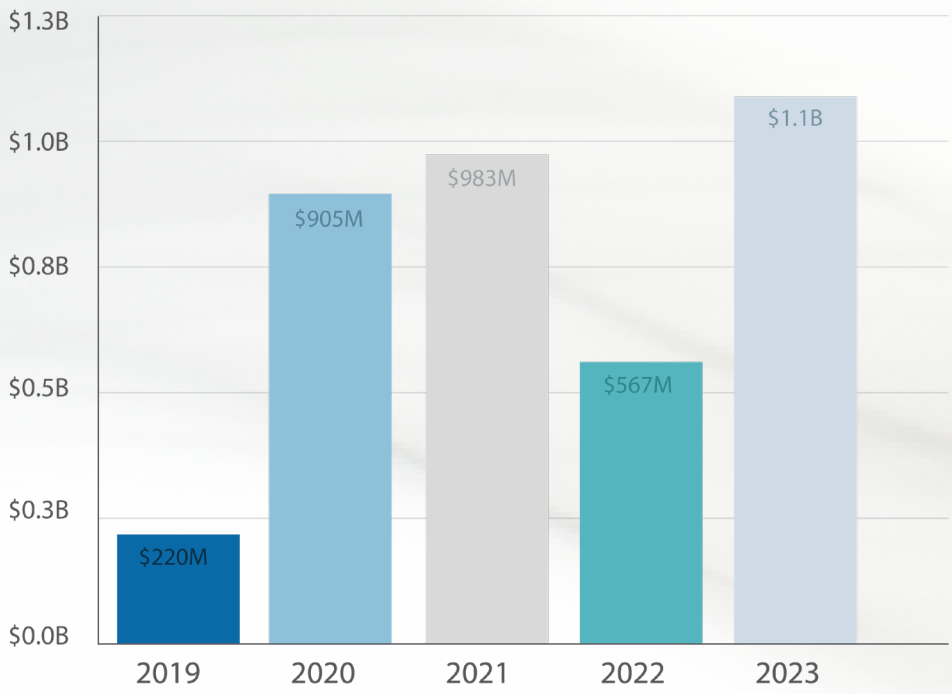


Ilustración 2. Ganancias del ransomware: 2019-2023. Fuente: Chainalysis[5]

5 https://www.trendmicro.com/vinfo/us/security/news/ransomware-by-the-numbers/lockbit-and-black-basta-are-the-most-active-raas-groups-as-victim-count-rises-ransomware-in-q2-and-q3-2022
6 https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant

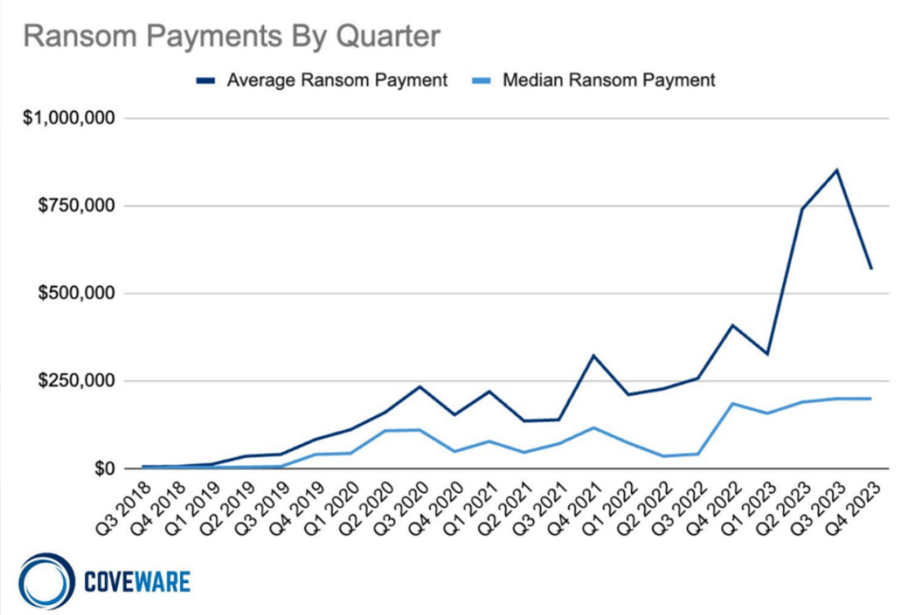


Ilustración 3. Evolución de los pagos de ransomware por cuartil. Fuente: Coveware[7]

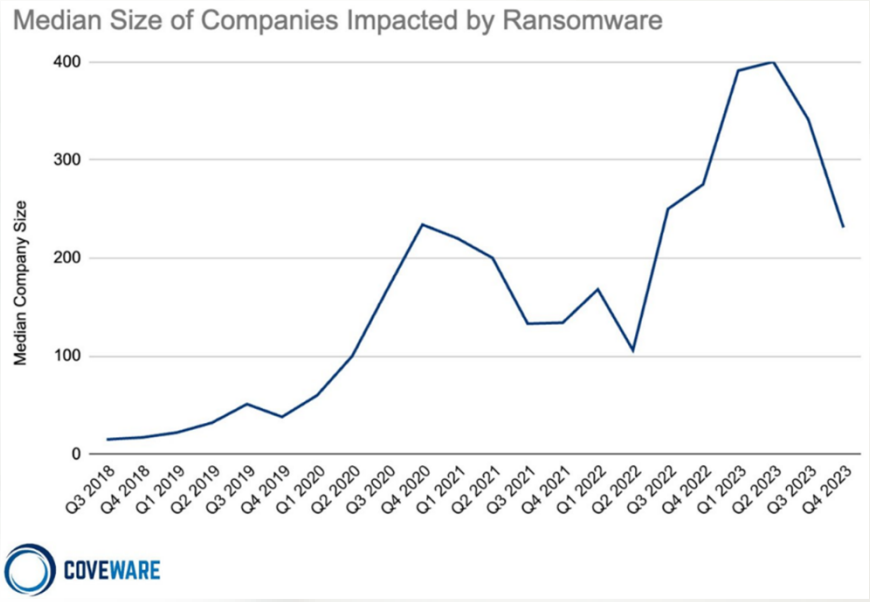


Ilustración 4. Evolución del tamaño medio de compañía atacada por cuartil. Fuente: Coveware[8]

7 - 8 https://www.coveware.com/blog/2024/1/25/new-ransomware-reporting-requirements-kick-in-as-victims-increasingly-avoid-paying

1.2 RAAS EN EL MAR DEL CIBERCRIMEN

Un aspecto fundamental para entender la progresión del ransomware y también los esfuerzos por detenerlo, es el coste del cibercrimen a nivel mundial. El coste del cibercrimen se estima en constante aumento conforme fuentes como Statista, que calculan que en 2024 el coste superará los 9 trillones de dólares.

Conforme a dicha fuente, tan sólo el ransomware ocupa en torno al 68,42% de los ciberataques a nivel mundial, lo que implica que es, destacadamente, uno de los factores que más está impactando en el aumento de las cifras. Además, indica también que es un modelo muy rentable para los cibercriminales.

Considerando, además, la cadena de despliegue del ransomware ya mencionada, tanto las fugas de datos como los accesos indebidos a redes contribuyen al éxito del RaaS.

Estos datos reflejan la importancia del Ransomware en el ecosistema del cibercrimen, y la importancia de detenerlo. Pero para poder ser efectivos en estas operaciones, es más necesario que nunca poder entenderlo.

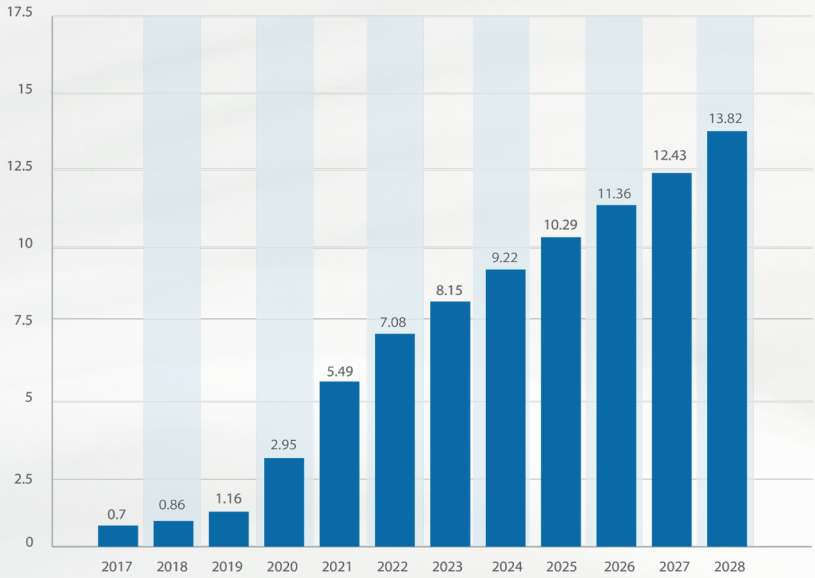


Ilustración 5. Estimación del coste del cibercrimen a nivel mundial. Fuente: Statista[9]

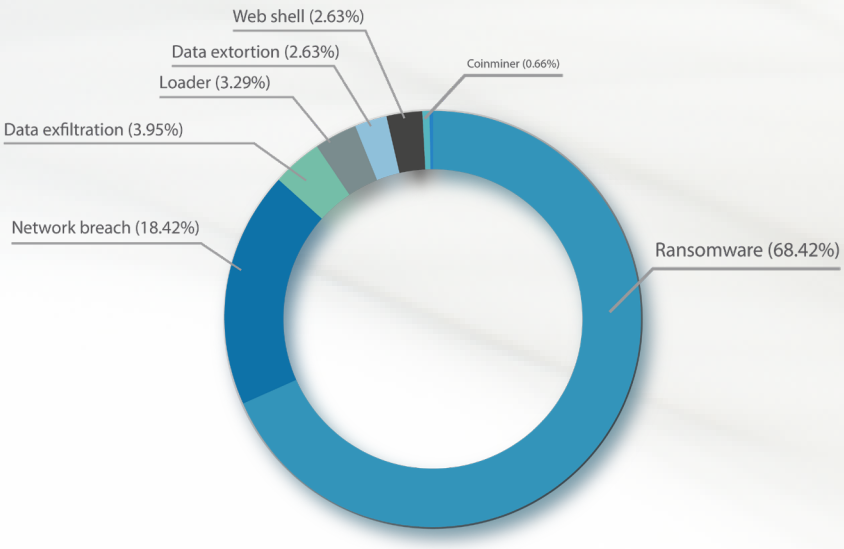


Ilustración 6. Ransomware en comparación con otros ciberataques. Fuente: Statista[10]

9 https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide
10 https://www.statista.com/statistics/1382266/cyber-attacks-worldwide-by-type/

1.3 PRINCIPALES SECTORES AFECTADOS

Si bien existen grupos que evitan el ataque a infraestructuras críticas, lo cierto es que cada vez más sectores se ven afectados por la actividad del RaaS. Considerando el sector financiero y, dentro del mismo el bancario, cabe destacar un mayor incremento de ataques efectivos de ransomware durante 2023. Esta tendencia ya se indicó en el informe previo.

En este sentido, en la Ilustración 7 se muestran los sectores más azotados por el ransomware durante los dos últimos trimestres, ordenados conforme a los últimos valores de T1 2024.

Respecto a tales resultados, cabe destacar que el sector de la construcción adelanta al tecnológico y al educativo durante este último trimestre. Además, el sector finanzas ocupa el décimo puesto, desplazado por los sectores legal, alimentos y consultoría.

A su vez, es necesario destacar la predominancia aún en este trimestre sobre el sector manufacturero. **Las organizaciones pertenecientes al sector manufacturero están compuestas por cadenas de suministro con alta complejidad.** Este hecho implica que sean más vulnerables contra ataques que puedan venir de terceras partes o proveedores.

Las cadenas de suministro dentro del sector manufacturero son muy relevantes porque, si una parte de la cadena de suministro queda inoperativa, esto genera un impacto directo en el producto final. Cuanto mayor efecto en cadena pueda tener un ataque de ransomware en la cadena de suministro, mayores probabilidades hay de que la víctima acceda a pagar un rescate.

También cabe mencionar que los ataques de ransomware no solo afectan a la eficiencia operativa, sino que también generan costos financieros y de reputación, ya que normalmente, los atacantes suelen tener un doble objetivo, llevar a cabo un robo de información confidencial y dejar inoperativo el proceso de producción manufacturero. Con ello pretenden incrementar las probabilidades de pago del rescate.

En lo relativo al **sector de "atención al cliente",** cabe destacar el gran impacto que estos ataques puede tener especialmente sobre los usuarios finales. Las víctimas pertenecientes al sector de atención al cliente tienen una importante dependencia de los datos almacenados en sus sistemas, sobre todo para poder ejercer su operativa diaria normal. Esta situación incrementa las probabilidades de ser una potencial víctima por parte de los grupos de ransomware. Además, los datos que contienen información personal ostentan un elevado valor dentro de los mercados de la darkweb, lo cual es de interés para los actores de ransomware.

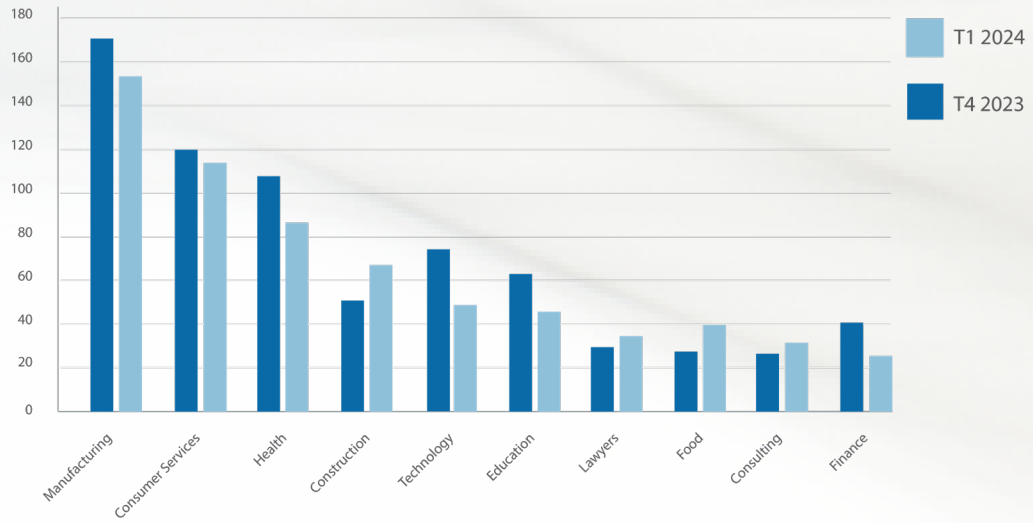


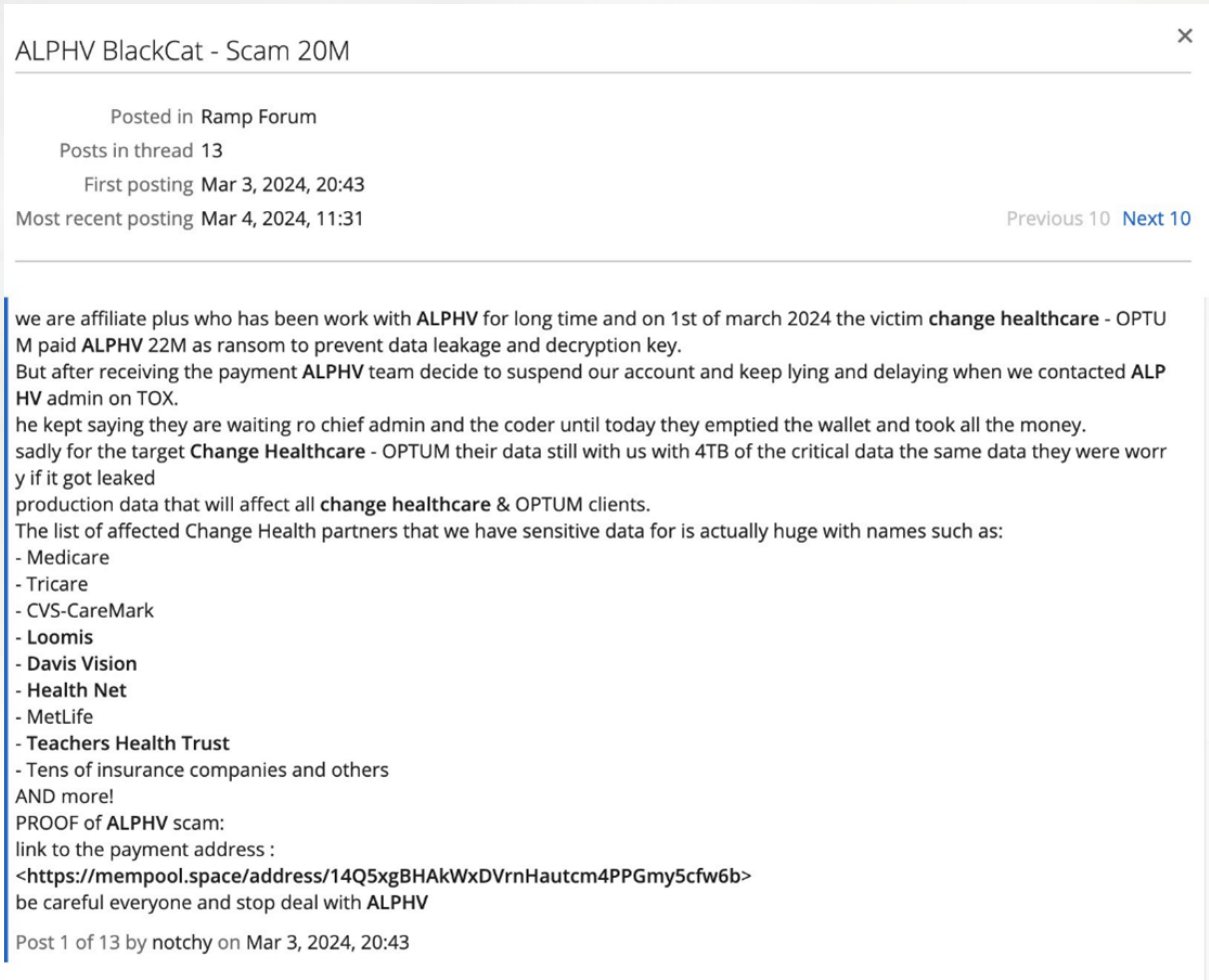
Ilustración7. Top-10 afectados por ransomware T1 2024 y T4 2023. Fuente: Lab52 (S2 Grupo)

Con relación a los ataques de ransomware contra organizaciones del **sector de la salud,** cabe mencionar que es uno de los ámbitos que presenta una mayor criticidad debido al gran impacto que supone la posibilidad de crear una disrupción en servicios sanitarios críticos, que genere a su vez un daño directo a pacientes. En este sentido, los servicios de emergencia de un centro sanitario están considerados unos de los más claves.

Por otro lado, la violación de los datos personales y clínicos de los pacientes podría conllevar graves consecuencias en lo que respecta a las operativas médicas de la organización sanitaria receptora del ciberataque. Los efectos que estos hechos puedan generar, podrían ser los objetivos que los atacantes de ransomware pretendan conseguir del sector sanitario.

A modo de ejemplo, el ataque de Rhysida sobre el hospital infantil Lurie Children en Chicago[11] causó gran conmoción por el sector en particular al que afectó. Amenazar a un sector como el sanitario está más allá de la barrera que no están dispuestos a cruzar determinados grupos de ciberdelincuentes, y que no supuso ningún problema moral para Rhysida. El ataque se produjo a finales de febrero, y el grupo vendió los datos sustraídos por 60 BTC a un tercero. Más allá de las filtraciones, la actividad del hospital se vio interrumpida por el ciberataque.

Uno de los incidentes más notorios por varios motivos, es la infección de BlackCat sobre la empresa UnitedHealth Group, empresa estadounidense de seguros de salud. En particular, la infección de ransomware se produjo sobre Change Healthcare[12] que es una


ALPHV BlackCat - Scam 20M

Posted in Ramp Forum
Posts in thread 13
First posting Mar 3, 2024, 20:43
Most recent posting Mar 4, 2024, 11:31
Previous 10 Next 10

we are affiliate plus who has been work with **ALPHV** for long time and on 1st of march 2024 the victim **change healthcare** - OPTUM paid **ALPHV** 22M as ransom to prevent data leakage and decryption key.
But after receiving the payment **ALPHV** team decide to suspend our account and keep lying and delaying when we contacted **ALPHV** admin on TOX.
he kept saying they are waiting ro chief admin and the coder until today they emptied the wallet and took all the money.
sadly for the target **Change Healthcare** - OPTUM their data still with us with 4TB of the critical data the same data they were worry if it got leaked
production data that will affect all **change healthcare** & OPTUM clients.
The list of affected Change Health partners that we have sensitive data for is actually huge with names such as:
- Medicare
- Tricare
- CVS-CareMark
- **Loomis**
- **Davis Vision**
- **Health Net**
- MetLife
- **Teachers Health Trust**
- Tens of insurance companies and others
AND more!
PROOF of **ALPHV** scam:
link to the payment address :
<https://mempool.space/address/14Q5xgBHAkWxDVrnHautcm4PPGmy5cfw6b>
be careful everyone and stop deal with **ALPHV**

Post 1 of 13 by notchy on Mar 3, 2024, 20:43

Ilustración 8. Nota de afiliados. Publicada por el analista Dmitry Smilyanets

11 Rhysida ransomware wants $3.6 million for children's stolen data (bleepingcomputer.com)
12 https://therecord.media/change-healthcare-blackcat-alphv-incident-drags-on

firma de servicios IT dentro de la compañía. Uno de los motivos que hacen destacable este incidente es que **BlackCat había sido ya intervenida meses antes de que se produjese el ataque,** un hecho más que demuestra que no deben descartarse futuros ataques tras una intervención. Pero, principalmente, al margen de eso, el impacto que tuvo este ataque desde el punto de vista social y humano es importante, dado que **afecta a un sector crítico como lo es el sector salud, a través de la aseguradora.** Tras recibir el pago de 22 millones de dólares por parte de Change Healthcare, el grupo anunció su retirada estafando al parecer a sus afiliados, y publicando, una nota aparentemente falsa en su portal[13].

El sector financiero también forma parte de los sectores afectados de forma notoria. Además de los ataques directos sobre el sector financiero, **al ser un sector que tiene dependencias también con otros, se ve afectado igualmente por otros ataques.** Un ejemplo de ataque de ransomware efectivo sobre una entidad de Tecnologías de la Informacion (TI) y cómo se vincula en dicho caso con el sector financiero es el sufrido en noviembre de 2023 por la multinacional InfoSy. En particular, la unidad de negocio en Estados Unidos, se vio afectada por un ataque de ransomware tras el que estaba LockBit[14]. Entre la información sustraída por los ciberdelincuentes se encuentran: nombres, números de la seguridad social, residencia, cuentas bancarias, números de tarjetas de crédito / débito, códigos de acceso, contraseñas, valores PIN de acceso a cuentas, fechas de nacimiento.

13 Ransomware group behind Change Healthcare attack goes dark | CyberScoop
14 Fidelity financial info feared stolen in cyberattack • The Register

1.4 INTERVENCIONES Y FUGAS DESTACADAS SUFRIDAS POR LOS GRUPOS

La lucha contra el ransomware requiere necesariamente la cooperación entre cuerpos y fuerzas de seguridad a escala internacional. Se describen aquí tanto intervenciones que han permitido asestar algún golpe a los grupos de cibercriminales, como fugas sufridas por los grupos, de diverso tipo que tienen impactos muy diversos en este ecosistema.

Se destacan a modo de ejemplo las siguientes intervenciones a grupos de ransomware o a parte de su infraestructura durante 2023 y principios de 2024:

Fecha	Grupo	Descripción
26 Enero 2023	Hive	El FBI, en colaboración con autoridades alemanas y holandesas. Fue posible la obtención de claves de descifrado. El grupo Hunters Interantional mantiene gran similitud con Hive, y los investigadores apuntan a que es su continuación[15].
7 Marzo 2023	Entropy (DoppelPaymer)	Arrestos producidos por acciones coordinadas de Europol, FBI y Países Bajos.
15 Marzo 2023	ChipMixer	Empleada como parte de la infraestructura de grupos de ransomware y otras actividades delictivas como fraude y robos de criptomonedas.
23 Octubre 2023	Ragnar Locker	Acción coordinada de Europol y Eurojust que permitió el arresto de un desarrollador de malware presuntamente vinculado con este grupo.
19 Diciembre 2023	BlackCat (ALPHV / Noberus)	FBI, en colaboración con autoridades alemanas, Dinamarca y Europol. Herramienta de descifrado para la restauración de los datos.
29 Enero 2024	BlogXXX (SugarLocker)	Operación de FACCT (organización Rusa) por la que se produjo el arresto de miembros presuntamente vinculados con este grupo. BlogXXX es una variante de SugarLocker y, a su vez, se vincula con REvil.
20 Febrero 2024	LockBit	Colaboración internacional para la captura de infraestructura empleada por el grupo LockBit (p.ej. control de servidores empleados por administradores) y arresto de varios potenciales involucrados. También se colaboró para la creación de descifradores de datos.

15 https://socradar.io/dark-web-profile-play-ransomware/

Aunque no forma parte de intervenciones a grupos, también es interesante mencionar en este punto el ataque sobre Trigona por parte de un grupo pro-ucraniano en octubre de 2023.

En el caso de Trigona, el grupo de ransomware vio toda su infraestructura destruida tras el ataque del grupo hacktivista proucraniano Ukranian Cyber Alliance, donde estos borraron 10 servidores de la banda Trigona, desfiguraron su sitio web y exfiltraron datos sobre la operación de cibercrimen.

En el segundo caso, referente al grupo Trickbot, tanto Estados Unidos como Reino Unido impusieron varias sanciones económicas a once miembros de la banda, debido a las numerosas pérdidas millonarias así como daños causados a entidades críticas que Trickbot, con sede en Rusia, habrían causado en todo el mundo.

Por otro lado, cuando un grupo organizado de ransomware sufre fugas, otros grupos menores se aprovechan de la inversión realizada para mejorar su propio software.

Las fugas de grupos contribuyen a la proliferación de ransomware, al aumento de víctimas y con ello al incremento de la probabilidad de recibir pagos de rescate. Asimismo, podría dar cabida a la mayor contribución en el desarrollo de malware en sus diferentes facetas. Por ejemplo, según un informe publicado por SentinelLabs, a principios de 2023 se identificaron muestras de familias que aprovechaban la fuga del código de Babuk ocurrida en 2021[16]. En particular, se observó cómo se aprovechaban otros grupos para la adaptación de código para entornos ESXi. Entre las familias identificadas, se destacaron: Play, Mario, Conti y REvil. También otras familias consideradas por ahora menores como Ra world (antiguamente conocido como Ra group) han aprovechado el código de Babuk[17]. En este último caso, se ha visto su uso en ataques dirigidos, dado que incluye valores específicos de la víctima como parte de su código, en las diferentes fases. Es en la última fase de la infección, la correspondiente al ransomware en sí mismo, donde Ra world emplea el código de Babuk filtrado.

A modo de ejemplo, se destacan a continuación algunas fugas producidas durante 2023 y hasta la fecha de este informe.

Fecha	Grupo	Descripción
9 Octubre 2023	HelloKitty	Publicación del código fuente de la primera versión del ransomware en un foro de hacking de habla rusa.
25 Enero 2024	Zeppelin	Venta del builder y ficheros empleados por el grupo por parte de un afiliado. Esta oferta se produce una vez el grupo no sigue su curso. Grupos como ViceSociety podrían tener variantes de su ransomware basadas en Zeppelin[18].
19 Febrero 2024	Knight	Venta del código fuente de Knight en la dark web.

Importante es también destacar que los operadores de BlackCat (ALPHV) anunciaron en Marzo de 2024 la posible venta del código fuente tras su denotado “exit scam”, aunque durante la elaboración de este informe aún no se confirma que se haya producido.

Por último, un ejemplo de cómo los grupos de ransomware también se ven afectados por las vulnerabilidades software es el caso de Ransomed.vc. La migración de la web del grupo a WordPress, y en particular la vulnerabilidad CVE-2017-5487 (versiones WordPress 4.7 anteriores a la 4.7.1), expuso la IP original empleada por el grupo, así como un conjunto de entradas DNS asociadas[19].

16 https://www.sentinelone.com/labs/hypervisor-ransomware-multiple-threat-actor-groups-hop-on-leaked-babuk-code-to-build-esxi-lockers/
17 https://therecord.media/ra-ransomware-group-using-leaked-code
18 https://www.sentinelone.com/anthology/vice-society/
19 https://socradar.io/on-the-horizon-ransomed-vc-ransomware-group-spotted-in-the-wild/

2 FAMILIAS DE RANSOMWARE

A continuación, se destacan los principales grupos de ransomware conforme a las fuentes de ciberinteligencia de S2 Grupo. En particular, se ha puesto el foco en la actividad destacada de 2023 y principios de 2024.

2.1 EVOLUCIÓN DE FAMILIAS DURANTE 2023 Y T1 2024

La Ilustración 9 resume los principales grupos de 2023 en base al número total de víctimas acumuladas durante todo el año. Como puede apreciarse, LockBit tuvo un impacto significativo continuado durante todo 2023, mientras que Cl0p, el segundo grupo en dicho listado tuvo el mayor impacto en el tercer trimestre del año, aunque en el último trimestre se ha percibido un descenso notable de la actividad.

En el último informe de S2 Grupo sobre el panorama del ransomware[20] se proporcionaron fichas para LockBit, BlackCat (ALPHV), BianLian, Cl0p, Royal y BlackBasta. Desde entonces se ha visto la progresión de los grupos, hasta completar el listado de los más destacados como queda en la gráfica previa.

Por su parte, la Ilustración 10 compara los dos últimos trimestres, en aras de vislumbrar la última actividad de grupos de ransomware que, si bien no destacan en el gráfico anterior podrían hacerlo durante 2024, dependiendo de cómo evolucionen los actores principales. En este caso los datos se encuentran ordenados conforme a volumetría de víctimas en T1 2024. Los datos trimestrales deben tomarse no obstante con cautela, porque nos muestran una ventana de tiempo muy específica.

Si bien Lockbit fue intervenido en febrero de 2024, como se ha mencionado continuó su actividad y se mantiene en T1 2024 como el grupo que ha impactado en mayor número de víctimas. Puede decirse lo mismo de BlackCat (ALPHV), que ha continuado registrando nuevos incidentes.

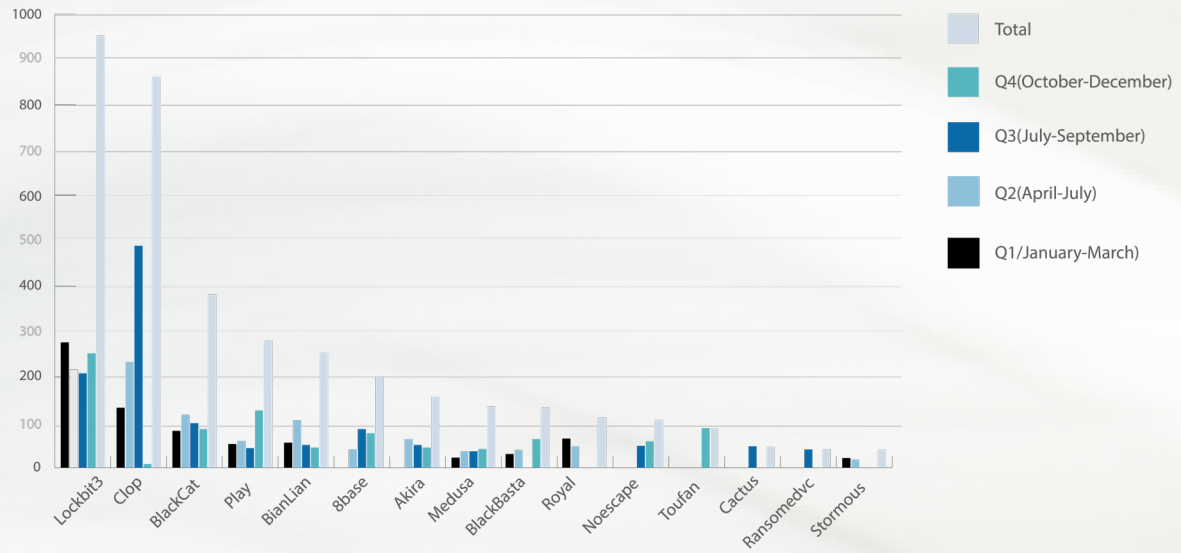


Ilustración 9. Principales grupos en base al número de víctimas 2023. Fuente: Lab52 (S2 Grupo)

20 https://home.s2grupo.es/informe-ransomware-2023

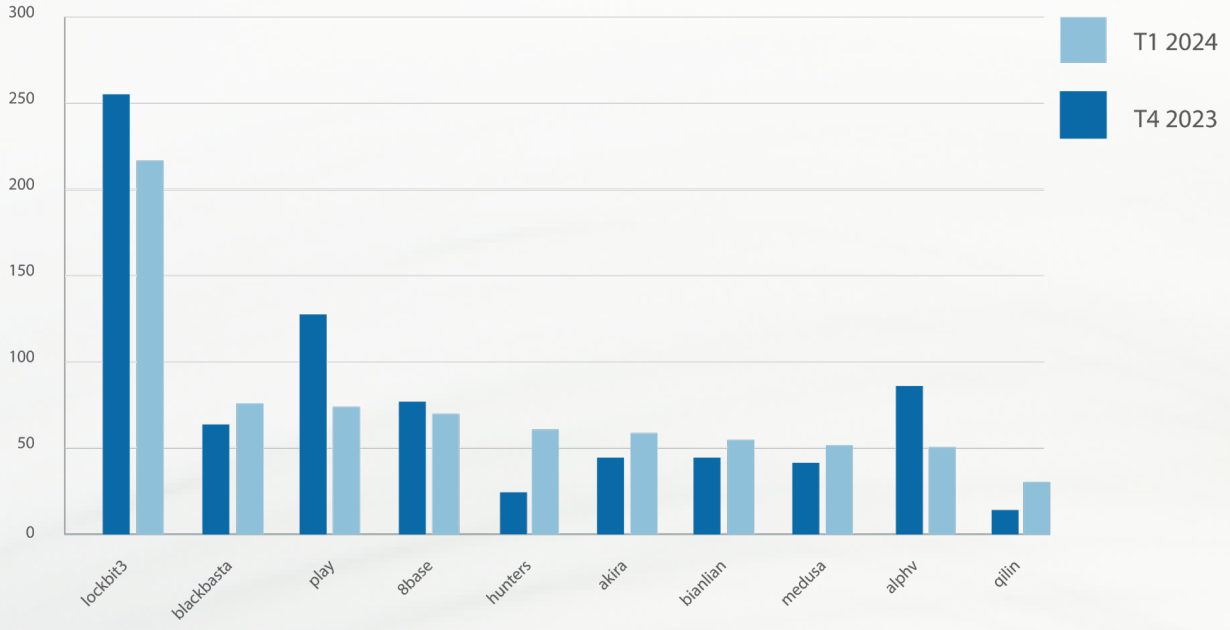


Ilustración 10. Top-10 grupos de ransomware T1 2024 y T4 2023. Fuente: Lab52 (S2 Grupo)

Nuevamente cabe destacar patrones comunes entre artefactos de ransomware. Tal y como destaca TrendMicro en un informe sobre LockBit publicado a final de febrero de 2024[21], el código de LockbBit 3.0 compartiría similitudes con muestras de DarkSide y BlackMatter. En particular, la resolución de APIs necesarias para funcionar, entre otras características. Esto demuestra una vez más que el análisis de malware sobre las diferentes muestras es crucial para entender la variabilidad en el software, identificar evoluciones novedosas y preparar las defensas futuras.

Entre los primeros puestos también destaca Play, que ya había aumentado su volumen de víctimas respecto a otras familias en T4 2023. Play es una de las familias que minimiza las evidencias en el sistema para minimizar su detección, evitando por ejemplo la generación de comandos identificables por herramientas como sysmon.

BlackBasta ocupaba en el ranking de 2023 uno de los 10 primeros puestos. Considerando únicamente los datos de los dos últimos trimestres se sitúa entre los primeros puestos y, de hecho, comparte puesto junto con Play. Recordemos que, tal y como se mencionaba en la ficha del último informe sobre ransomware, BlackBasta está formado por integrantes de la desarticulada Conti.

Por su parte, 8base es un malware de la familia Phobos que cuenta con grandes similitudes también con RansomHouse[22]. Phobos cuenta con multitud de variantes que, no obstante, comparten en su mayor parte las reglas de detección. Pese a esto, conforme a los datos previos se encuentra como uno de los ransomware que han provocado mayor número de víctimas.

Destacable es también la subida en número de víctimas del ransomware Hunters respecto al trimestre previo. Hunters International es un grupo que, aunque data de 2023, comparte código con Hive, desarticulada en 2023.

21 https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-lockbit
22 https://www.hhs.gov/sites/default/files/8base-ransomware-analyst-note.pdf

2.2 REPERCUSIÓN DE GRUPOS DESTACADOS DE RANSOMWARE EN SECTORES

Mientras que los grupos tienen impacto en múltiples sectores en mayor o menor medida, es destacable que, dependiendo del grupo, puedan verse afectados algunos sectores más que otros. A modo de ejemplo, se muestran los sectores más atacados por grupos destacados como LockBit, BlackCat, Play y Bianlian durante T4 2023 y T1 2024.

Cabe destacar no sólo que diferentes actores tienen un impacto distinto en los sectores mencionados, sino también que este impacto en grupos como LockBit, suponen un aumento del número de ataques por ransomware contra dichos sectores. **En los grupos anteriores, que suman mayores casos durante el periodo seleccionado, el sector "Manufactura" forma parte del Top-5 de sectores afectados.**

Sin embargo, este impacto en los diferentes sectores puede variar con el tiempo. Considerando datos globales en periodos comprendidos desde 2021 a 2022 ofrecidos por TrendMicro[23], se observa un claro impacto en el sector salud por parte de LockBit. Esta variabilidad puede deberse a múltiples factores, que involucran aspectos sociales (p.ej. pandemia, contexto geopolítico) y también tecnológicos (p.ej. vulnerabilidades explotables sobre software que afecten a la cadena de suministro).

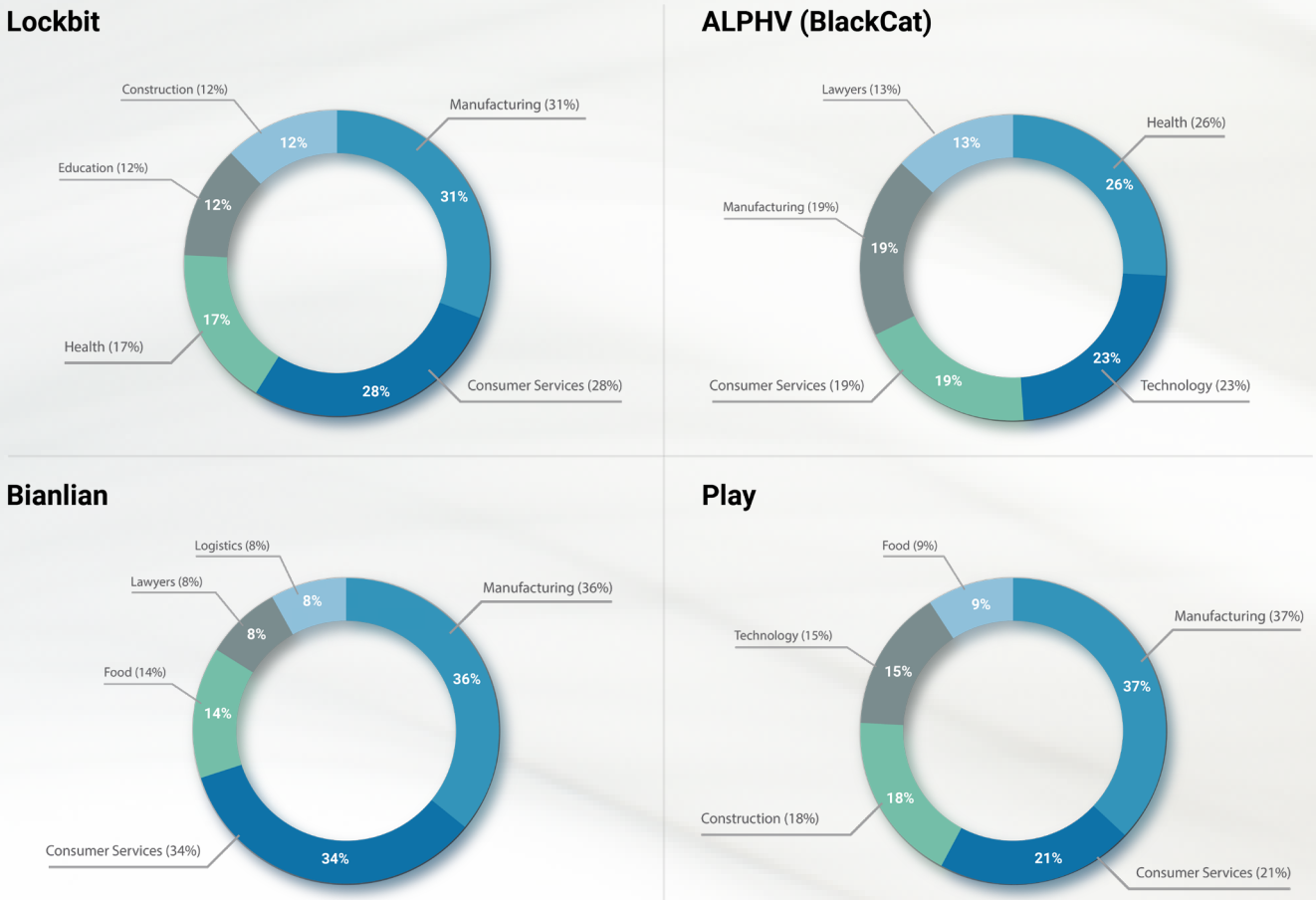


Ilustración 11. Top-5 sectores atacados por LockBit, BlackCat, Play y BianLian – T4 2023 y T1 2024. Fuente: Lab52 (S2 Grupo)

23 https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-lockbit

3 GEOPOLÍTICA Y RANSOMWARE

El análisis geopolítico es fundamental para comprender la manera en la que el panorama internacional impacta en las actuaciones llevadas a cabo por grupos de ransomware, dado que diversos actores internacionales podrían usar este tipo de malware como arma para afectar a sus objetivos. La Ilustración 12 ofrece de forma esquemática los principales factores que se ven afectados por el contexto geopolítico.

Por ello es crucial conocer la motivación de los atacantes para comprender cómo los eventos sociales impactan en la necesidad del uso del ransomware. El alineamiento de diferentes grupos de ransomware para el desarrollo de un conflicto posterior, se vio enormemente reflejado en los meses previos a la invasión rusa de Ucrania, así como durante los meses siguientes del comienzo de dicho enfrentamiento[24].

Por ejemplo, durante la campaña electoral estadounidense de 2020 se publicaron numerosas informaciones en varios medios del país[25], sobre una supuesta campaña de ransomware que habría afectado a sistemas críticos y servicios telefónicos del condado de Georgia durante las elecciones de dicho año. Por otro lado, CISA habría alertado previamente de la posible actividad que cabría esperar durante ese período electoral, por parte del grupo Energetic Bear con supuesta vinculación a Rusia. No obstante, en la nota emitida por CISA[26] no se detectó el empleo del ransomware como una de las herramientas empleadas por dicho grupo para efectuar sus acciones.

Durante el transcurso de 2024 se prevé un incremento de procesos electorales. Varios de ellos son altamente significativos como es el caso de Estados Unidos, elecciones al Parlamento Europeo y Rusia entre otros. De este modo, se incluye un mapa a continuación, donde se pueden observar todos aquellos países en los que ya se habrían celebrado elecciones o en los que aún tienen que hacerse durante este 2024.

De este modo, se puede confirmar la importancia que tiene la ciberseguridad a nivel global durante este 2024, ya que tomando como referencia casos previos de injerencias externas mediante el supuesto posible uso de herramientas maliciosas como el ransomware y, teniendo en cuenta además, la importancia estratégica de muchos países en los que se celebran elecciones, es probable que exista un incremento de campañas maliciosas en las que se pudiera emplear el ransomware como herramienta mediante la cual coaccionar y obtener beneficios económicos de los datos filtrados.

Ilustración 12. Principales factores que se ven afectados por el contexto geopolítico. Fuente: Lab52 (S2Grupo)

24 https://home.s2grupo.es/informe-de-inteligencia-conflicto-rusia-ucrania
25 https://apnews.com/article/virus-outbreak-elections-georgia-voting-2020-voting-c191f128b36d1c0334c9d0b173daa18c
26 https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-296a

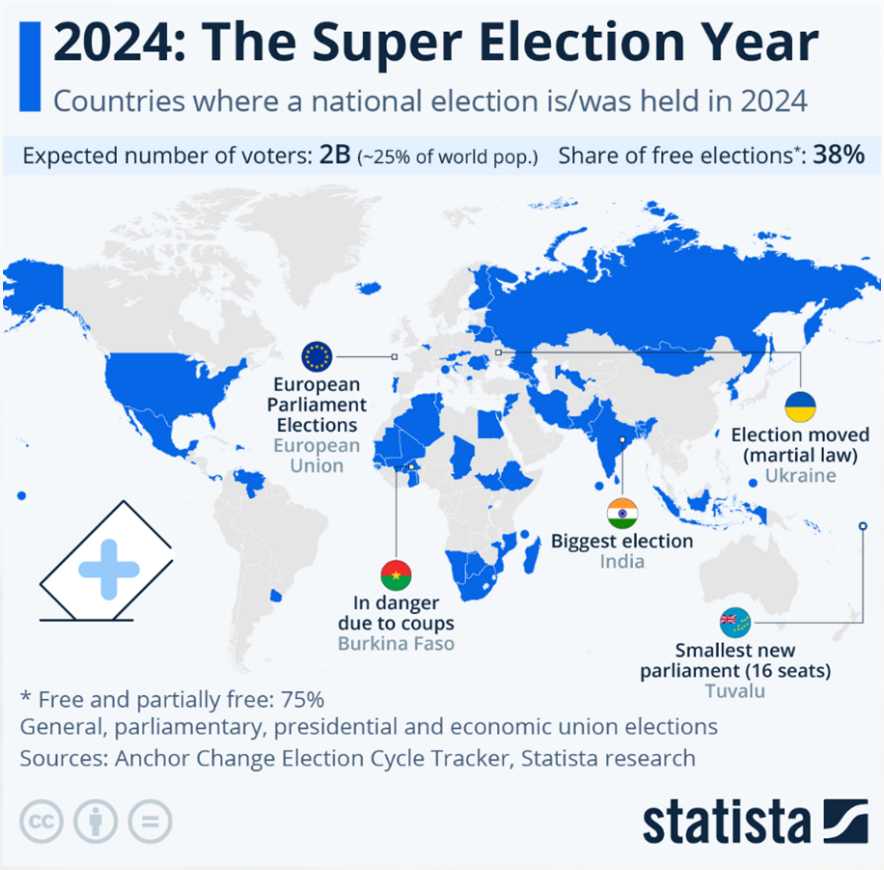
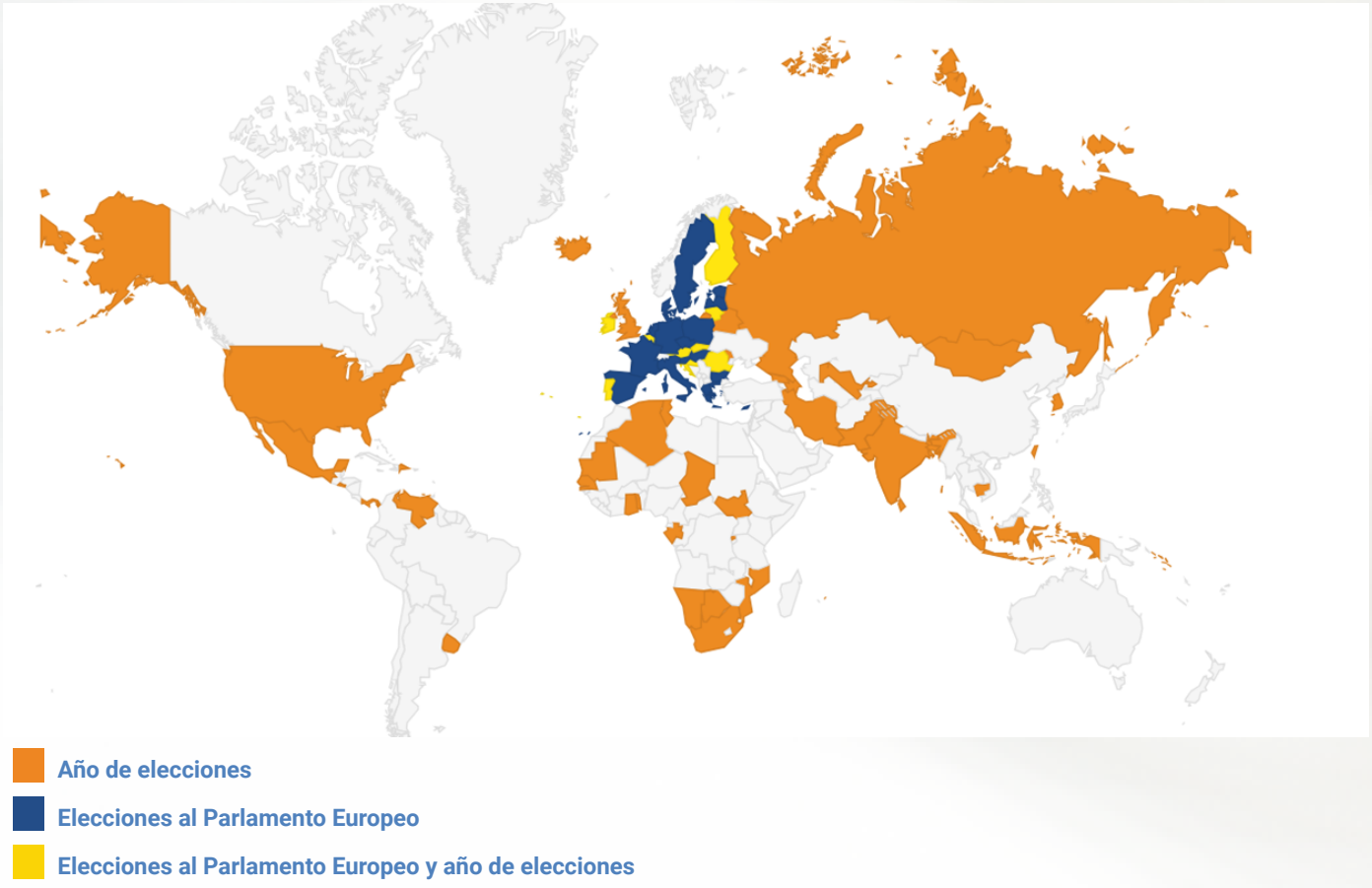


Ilustración 13. Mapa electoral a nivel mundial en 2024. Fuente: Statista[27]



27 https://www.statista.com/chart/31604/countries-where-a-national-election-is-was-held-in-2024/

3.1 PAÍSES MÁS AFECTADOS

En términos generales, la Ilustración 14 muestra los países más afectados por ransomware en los últimos dos trimestres. El orden de selección se basa en los países más afectados en T1 2024. Estados Unidos se mantiene como el país más afectado por ataques de ransomware, seguido de Canadá y Reino Unido.

En esta ocasión la afectación de países principalmente occidentales puede explicarse desde una perspectiva geopolítica, teniendo en cuenta que el posible desarrollo e inversión que estos países hacen en industrias como puedan ser la manufacturera, el sector sanitario o todo lo relacionado con nuevos avances tecnológicos, supone un gran interés en términos de beneficios económicos para los grupos de ransomware.

En este sentido cabe mencionar cómo el hecho de que **Estados Unidos,** así como **Canadá, Reino Unido** y otros países europeos, sean potencias mundiales y presenten cierta **estabilidad financiera e inversión en desarrollo tecnológico,** puede suponer una de las causas principales por las que estos países se encuentren entre los objetivos de grupos de ransomware, ya que dicha estabilidad puede otorgar una determinada certeza a los grupos cibercriminales de que exista un elevado número de empresas, tanto medianas como grandes, que cuenten con elevados ingresos y a los que sea posible acceder a través de técnicas no muy elaboradas de ataque, mediante los cuales conseguir datos relevantes de las mismas que acaben transformando en dinero.

Asimismo, la presencia de países de la región iberoamericana como **Brasil,** afectados también por campañas de ransomware, se entiende teniendo en cuenta que es uno de los más extensos de la zona, por lo que cuenta con una amplia **expectativa de desarrollo como potencia mundial y país influyente (actualmente forma parte de los BRICS).** Esto puede llamar la atención de diversos grupos de cibercrimen ya que la existencia de comercios y compañías brasileñas clave a nivel internacional incluso regional presenta una buena oportunidad de la que obtener beneficio económico mediante distintas campañas de ataque. Además, considerando este procedimiento de avance y desarrollo, puede que los protocolos de ciberseguridad no estén ampliamente instaurados en la región, lo que facilitaría aún más las operaciones de cibercrimen.

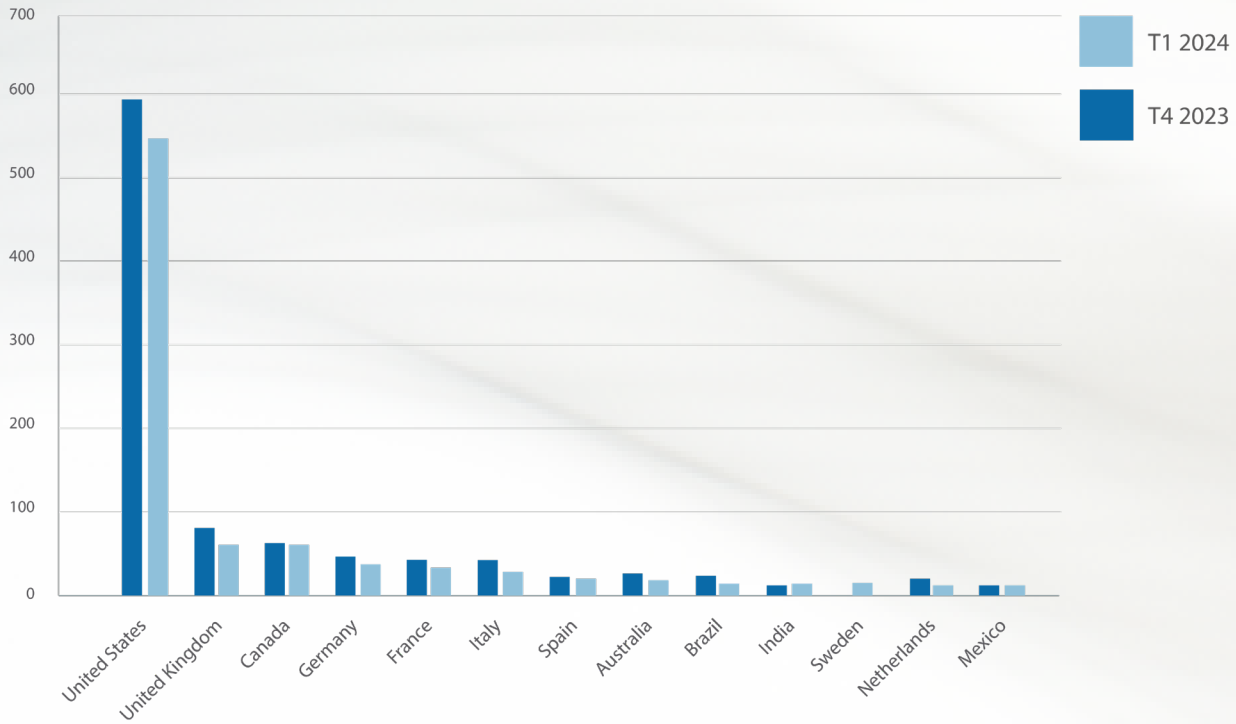


Ilustración 14. Comparativa de países más afectados por ransomware.
Fuente: Lab52 (S2 Grupo)

3.2 RECURSO OFENSIVO DE GRUPOS APT

A priori los grupos APT se centran en llevar a cabo campañas de explotación, es decir, acciones de espionaje y en algunas ocasiones, campañas de ataque o sabotaje acordes a los objetivos estratégicos marcados por los gobiernos. Sin embargo, **con la aparición del conflicto ruso-ucraniano, se habrían empleado diversas herramientas, entre ellas el ransomware y los wipers, como forma de mostrar las debilidades más inminentes en materia de ciberseguridad que presentan los sectores críticos y estratégicos ucranianos.** Estas informaciones pueden consultarse en los anexos del informe de inteligencia, relativo al impacto que el ciberespacio tiene en el conflicto ruso-ucraniano, elaborado por Lab52[28].

De igual modo, el hecho de que **países como Corea del Norte se encuentren en una situación grave de crisis económica y alimentaria en el país ha supuesto una mayor implicación de grupos, presuntamente vinculados a Estados-Nación.** Estos grupos realizarían actividades propias de los grupos de cibercrimen en cuanto a la obtención de beneficios puramente financieros y el empleo de herramientas maliciosas tales como el ransomware. Además, algunos de estos grupos APT podrían emplear el ransomware en sus **ataques de falsa bandera.**

A modo de ejemplo, se muestra más abajo un cuadro con grupos APT que mantienen dentro de su *toolkit* el ransomware como recurso ofensivo:

- **El grupo Carabanak** habría llevado a cabo campañas en las que empleó el ransomware CL0P contra numerosas víctimas.
- **Doppel Spider:** Dos miembros de este grupo, que ha llevado a cabo numerosos ataques de ransomware contra grandes compañías de diversos sectores, como por ejemplo, KIA Motors America, el Instituto Holandés de Investigación Científica (NWO) o PEMEX, habrían sido detenidos por la policía alemana y agentes del servicio secreto de los EE.UU por sus implicaciones en las campañas de cibercrimen realizadas en los últimos años.
- **Lazarus Group:** Este grupo principalmente identificado como APT, habría empezado a llevar a cabo campañas de cibercrimen mediante las cuales obtener beneficios económicos. Más concretamente el subgrupo de Lazarus, Andariel, habría sido detectado empleando entre otras herramientas, el ransomware Maui.
- **TA577 (WaterCurupia)** es un actor que recientemente ha sido vinculado con el uso del ransomware BlackBasta.

Amenaza Persistente Avanzada	País presuntamente atribuido
Carbanak, Anunak[29]	Ukraine
Doppel Spider[30]	Russia
Andariel (Lazarus)	North Korea
TA577 (WaterCurupia)[31]	-

28 https://home.s2grupo.es/informe-de-inteligencia-conflicto-rusia-ucrania
29 https://www.bleepingcomputer.com/news/security/microsoft-notorious-fin7-hackers-return-in-clop-ransomware-attacks/
30 https://www.malwarebytes.com/blog/news/2023/09/doppelpaymer-ransomware-group-suspects-identified
31 https://www.proofpoint.com/us/blog/threat-insight/first-step-initial-access-leads-ransomware

Por otro lado, y aunque no de manera directa, se ha podido observar que grupos APT estarían empleando malware que también utilizan los grupos de ransomware, ya que se ha detectado profesionalización y vinculación con los mismos.

Ilustración 15. Publicación en twitter relacionando TA577 y ransomware[32]

32 https://twitter.com/1ZRR4H/status/1765048348057247931

3.3 NACIONES UNIDAS: NUEVO TRATADO INTERNACIONAL SOBRE LA UTILIZACIÓN DE LAS TIC CON FINES DELICTIVOS

A la hora de analizar el planteamiento del nuevo **Tratado Internacional sobre la Utilización de las TIC con fines Delictivos en el marco de Naciones Unidas,** es interesante conocer la posición de Rusia, dada la conocida vinculación de grupos de ransomware con dicho país puesta de manifiesto durante el conflicto Ruso-Ucraniano.

Se espera que este nuevo tratado contribuya minimizar la actividad cibercriminal a través de puntos comunes de cooperación entre los diferentes países que conforman este proyecto bajo el marco de Naciones Unidas. Es un tratado que, si bien no es exclusivo de ransomware, sí podría permitir, por ejemplo, realizar acciones que permitan acelerar las intervenciones sobre sus grupos. Es por ello que estudiar este posicionamiento desde el punto de vista geopolítico es sumamente interesante para poder realizar estimaciones sobre los siguientes movimientos que impacten en la industria del ransomware.

Rusia, aunque es miembro del Consejo de Europa, ha mostrado sus discrepancias con respecto al Convenio de Budapest, que legisla también sobre cibercrimen.

Durante la última década, Rusia habría estado defendiendo la creación de un nuevo tratado de alcance mundial sobre ciberdelincuencia, a pesar de la existencia del Convenio de Budapest, Tratado internacional que ya aborda aspectos relativos a la ciberdelincuencia, que fue negociado en el Consejo de Europa en 2001 y cuya entrada en vigor tuvo lugar en 2004. Esta Convención ha sido ratificada hasta el momento por 66 países de diversas regiones del mundo. No obstante, Rusia no ratificó la Convención de Budapest, ya que considera que dicho Tratado supone una violación de los principios relativos a la soberanía estatal al permitir operaciones transfronterizas de ciberdelincuencia.

Por ello, habría estado preparando desde 2019 y con el apoyo de China, Camboya, Bielorrusia, Corea del Norte, Myanmar, Irán y Venezuela, un borrador para plantear la creación de un nuevo tratado a la Asamblea General de las Naciones Unidas.

Uno de los sucesos a tener en cuenta en lo relativo a la tipificación de los delitos cibernéticos puede ser la evolución del actual conflicto entre Rusia y Ucrania. Así pues, el 24 de febrero de 2022, día en el que estaba prevista la primera sesión organizativa del Comité Ad Hoc para abordar cuestiones relativas al posible nuevo tratado, se producía al mismo tiempo la entrada de las tropas rusas en el territorio ucraniano, lo que daba lugar al enfrentamiento armado que continúa durante la redacción de este informe.

Actualmente y tras dos años de reuniones y negociaciones, sigue sin haber consenso entre los Estados participantes en este proyecto por falta de acuerdos sobre los puntos conflictivos fundamentales relativos a la forma que debería adoptar una convención de la ONU contra el cibercrimen: si debiera ser un tratado tradicional contra el cibercrimen o un tratado más amplio que cubra todos los delitos cometidos utilizando tecnologías de la información y las comunicaciones. Por ello y tras la última sesión celebrada en febrero de 2024 en Nueva York, y ante la falta de consenso, se decidió posponer la reunión para otra fecha en la que por fin todos los participantes puedan acercar posturas.

Por consiguiente, si bien la firma del nuevo tratado permitiría acercar posturas y unir el frente común contra la lucha del cibercrimen y por ende del ransomware, la tendencia actual parece sugerir que **este tipo de malware está desempeñando un rol nada desdeñable en los conflictos actuales entre países.**

4 LATINOAMÉRICA

El caso de Latinoamérica sirve como ejemplo para comprender mejor las vías de actuación contra el ransomware. Si bien en las secciones anteriores el foco se pone en familias de ransomware de impacto internacional (incluyendo cómo no Latinoamérica), dicha evaluación no es suficiente para la priorización en cuanto a estudio de amenazas.

En los datos globales del último trimestre analizado Brasil y México son países latinoamericanos que están en el Top-14, estando Brasil en noveno lugar y México en catorceava posición. Este es un dato muy significativo.

Este informe destaca datos para Latinoamérica, en aras de comprender mejor porqué el estudio del ransomware debe adaptarse también al contexto para su priorización y entendimiento.

4.1 PAÍSES MÁS AFECTADOS

La Ilustración 16 muestra los países Latinoamericanos más afectados por ransomware. Se realiza la ordenación en base al total de casos acumulados desde T4 2023. Considerando dicho orden, los países en el Top-5 serían: Brasil, México, Argentina, Colombia y Perú.

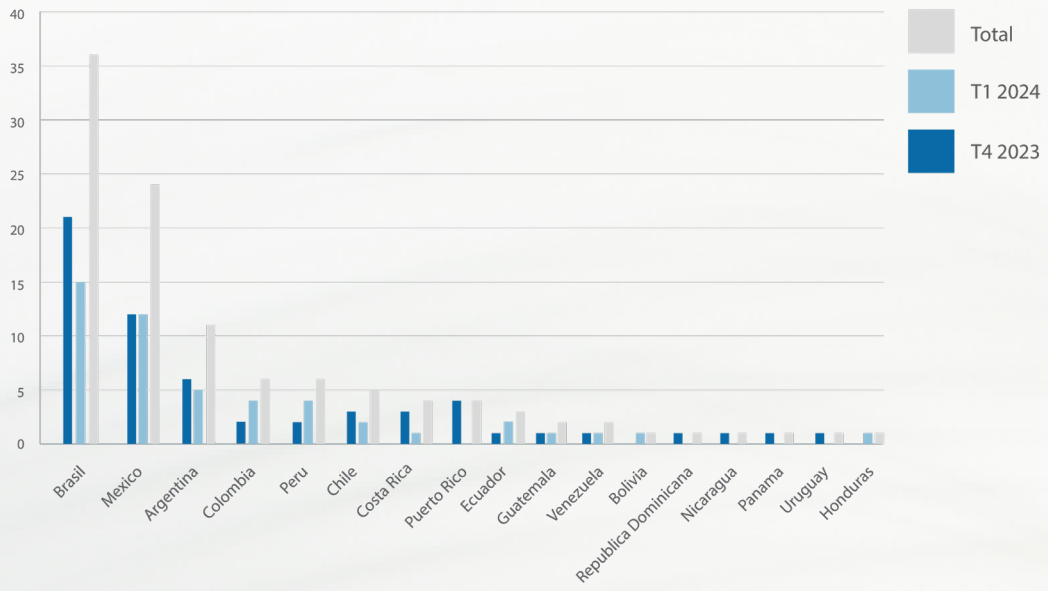


Ilustración 16 Países Latinoamericanos afectados por Ransomware – T4 2023 y T1 2024. Fuente: Lab52 (S2 Grupo)

El hecho de que Brasil, México, Argentina, Colombia y Perú se encuentren dentro de los cinco países más afectados por Ransomware durante el último trimestre de 2023 así como durante el primer trimestre de 2024 puede deberse a diferentes razones.

En primer lugar, hay que tener en cuenta que tanto Brasil, México, Argentina y Colombia, ocupan actualmente la misma posición en el ranking de las **economías latinoamericanas con el mayor PIB de la región**, según el FMI[33], tal y como se puede ver en la imagen 17.

En segundo lugar, otro factor importante a tener en cuenta es el hecho de que en la gran mayoría de estos países ha habido **cambios recientes de Gobierno**, lo cual suele generar ciertas **incertidumbres en los ámbitos empresariales** respecto a qué nuevas directrices económicas podrá tomar ese nuevo Gobierno y qué impacto podrá tener en sus compañías. Con lo que este tipo de situaciones, pueden ser aprovechadas por los grupos de ransomware para actuar con mayor facilidad ante empresas que presenten ciertas inseguridades.

Finalmente, en tercer lugar, la mayoría de estos países presentan **grandes reservas de diversos recursos naturales**, explotados por diversas compañías objeto de interés de posibles grupos de ransomware, debido a las grandes cantidades de dinero que dichos negocios pueden generar.

Ilustración 17 Mayores economías latinoamericanas en base a su PIB. Fuente: Statista.

33 https://es.statista.com/grafico/26372/paises-latinoamericanos-con-el-mayor-pib-a-traves-del-tiempo/

4.2 SECTORES MÁS AFECTADOS

En cuanto a los sectores más afectados es necesaria la comparación con datos globales, aún teniendo en cuenta que los casos registrados en Latinoamérica son inferiores en número. En el caso de Latinoamérica el sector más afectado es el de servicios, seguido por educación y tecnología, ocupando el sector manufacturas un cuarto lugar, mientras que en los datos globales dicho sector se sitúa en el primer puesto.

A su vez, cabe destacar que por el momento el sector salud no forma parte de los primeros sectores afectados por ransomware en Latinoamética, al menos en cuanto a los datos agrupados por trimestre.

Ejemplos de ataques de ransomware que han afectado a empresas tecnológicas en Latinoamérica son, por ejemplo, la infección del ransomware **Akira** sobre VitalT, un integrador y proveedor de servicios de IT con sede en SaoPaulo (Brasil) y es subsidiaria de Telefonica S.A. (ES)[34], así como el ciberataque a CLARO en Mexico por parte del grupo **Trigona**, que se ha extendido a Guatemala, El Salvador, Honduras, Nicaragua y Costa Rica[35]. Es importante destacar que este ataque no se refleja en los datos de este informe, al pertenecer por temporalidad al T2 2024.

El caso del proveedor de servicios IXmetro Powerhost de Chile también es reseñable, ocurrido el 1 de abril de 2024. IXmetro es un proveedor de servicios de datacenter, infraestructura y conectividad afectado por un incidente de ransomware aún en curso de resolución durante la redacción de este informe[36]. No es el primer centro de datos que se ve afectado por un ataque de ransomware, ya el pasado 23 e octubre de 2023 el datacenter GTD fue afectado por un ataque de ransomware.

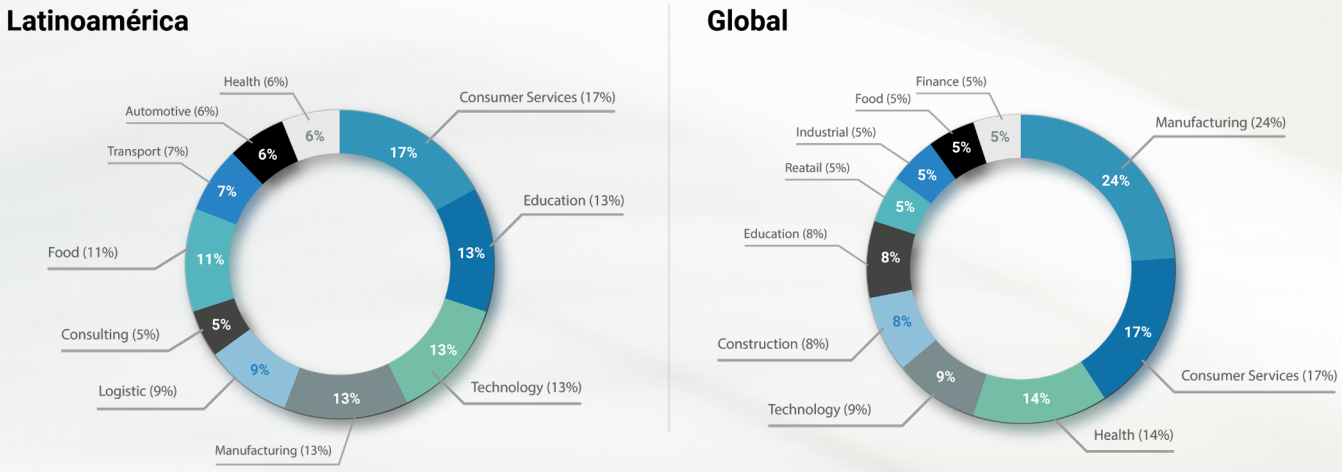


Ilustración 18. Sectores afectados por ransomware Latinoamérica.T4 2023 y T1 2024. Fuente: Lab52 (S2 Grupo)

34 https://x.com/_venarixES_/status/1772322266111426897?s=20
35 https://ciberprisma.org/2024/02/02/ataque-de-ransomware-a-claro-desata-caos-en-america-central-y-pone-en-alerta-a-la-region/
36 https://twitter.com/1ZRR4H/status/1774768945003696245?t=rCVcNR4XzjlQ3H2mRb1cNw&s=08

Tan sólo en marzo de 2024 se registran algunos ejemplos de impacto como lo son: el ataque de Rysida contra el medio de comunicación Debate de Culiacán Sinaloa[37], la infección de 8base sobre HC Querétaro (industria manufacturera en México)[38], y el ataque de RansomHub en el que fue víctima Industrial de Alimentos EYL SA. en Honduras[39].

Aunque no formen parte del Top-5, hay otros incidentes también destacables, como la infección de INCRansomware que afectó al Ejército del Perú, exfiltrándose 500 GBde datos. En paralelo, el grupo #RansomEXX anunció al Ministerio de Defensa en su sitio en la Dark Web 757.5 GB exfiltrados[40].

Ilustración 19.Imagen de la web de Trigona

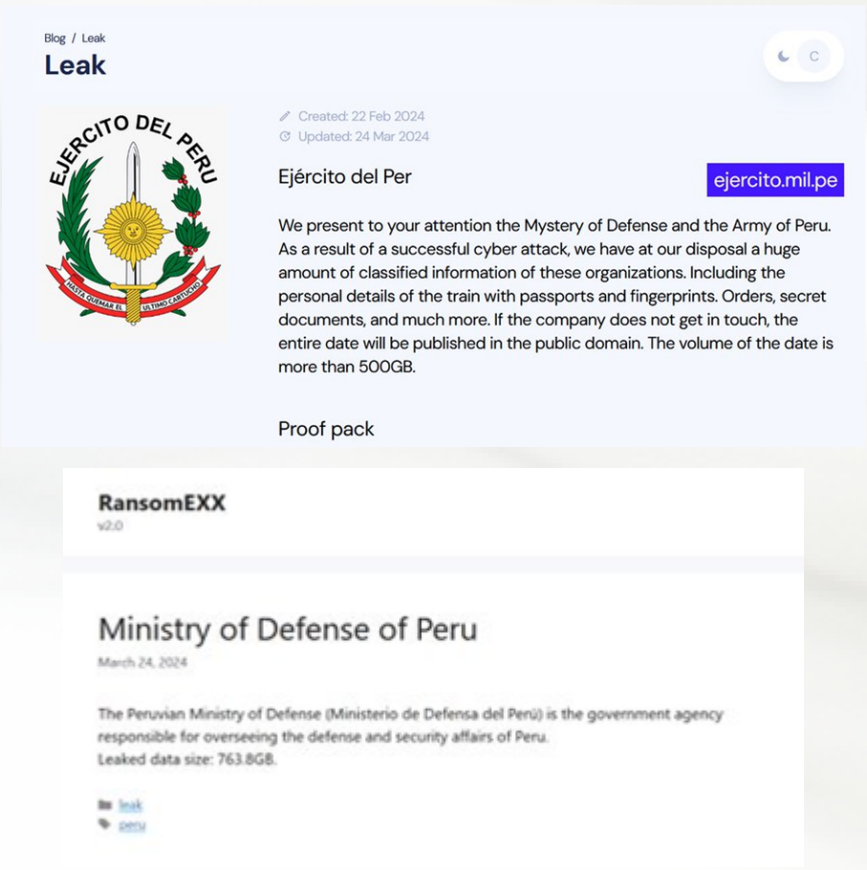


Ilustración 20. Casos de ransomware afectando a defensa

36 https://twitter.com/victor_ruiz/status/1772839560768061689?t=2mjSop_ciWuFbpj536seUw&s=19
37 https://twitter.com/CTIabs/status/1773000767835660646?t=3ohAiXW5ohc8mTMKMrcSUg&s=19
38 https://twitter.com/chum1ng0/status/1773071154430800107?t=0CMjWV_CE72-Tf1GoPnBxg&s=19
40 https://twitter.com/Cronup_CyberSec/status/1772295734366245141?t=LHwYx1M4ed8j-DI-gwRjog&s=08

4.3 PRINCIPALES GRUPOS

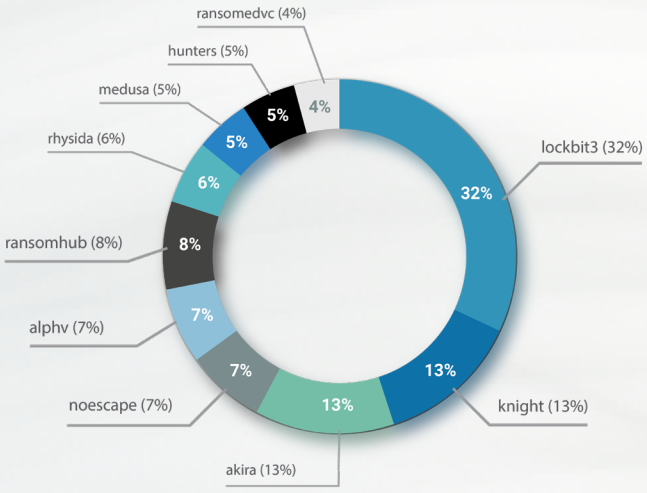
Nuevamente se realiza una comparativa entre Latinoamérica y los datos globales para determinar los grupos de ransomware que más impactan en los dos últimos trimestres a la región (Ilustración 21).

Estos datos nos permiten apreciar que, mientras que Lockbit ocupa el primer puesto en ambos, luego existen variaciones entre los grupos. Por este motivo es muy importante que la priorización de análisis para la defensa de los sistemas se haga en base al contexto de protección, y no se rija únicamente por métricas a nivel global. **La ciberinteligencia desempeña un rol fundamental en comprender el contexto de una organización o de un país de cara a mejorar sus líneas de defensa y optimizar la utilización de sus recursos.**

La existencia de porcentajes de afectación en la región de Latinoamérica puede entenderse como parte de un **proceso en desarrollo donde aún están acercándose posturas sobre el establecimiento de organismos comunes y centrales**, que regulen y aborden todas las cuestiones relativas a ciberamenazas y ciberataques en la zona de América Latina e Iberoamérica.

La concienciación de la población a gran escala puede ser otra de las causas que motiven estos resultados, ya que pueden existir zonas que bien por cuestiones de carácter natural (como pueda ser la ubicación en entornos de gran vegetación, en zonas de gran altitud, etc) o por cuestiones económicas, no tengan el mismo acceso a la información sobre cómo proceder en el ámbito cibernético.

Latinoamérica



Global

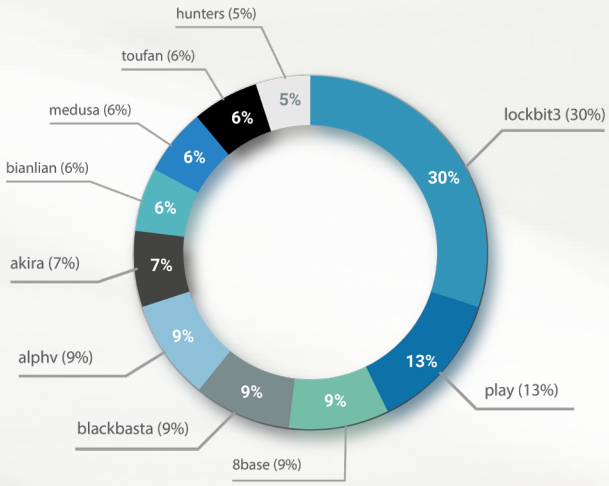


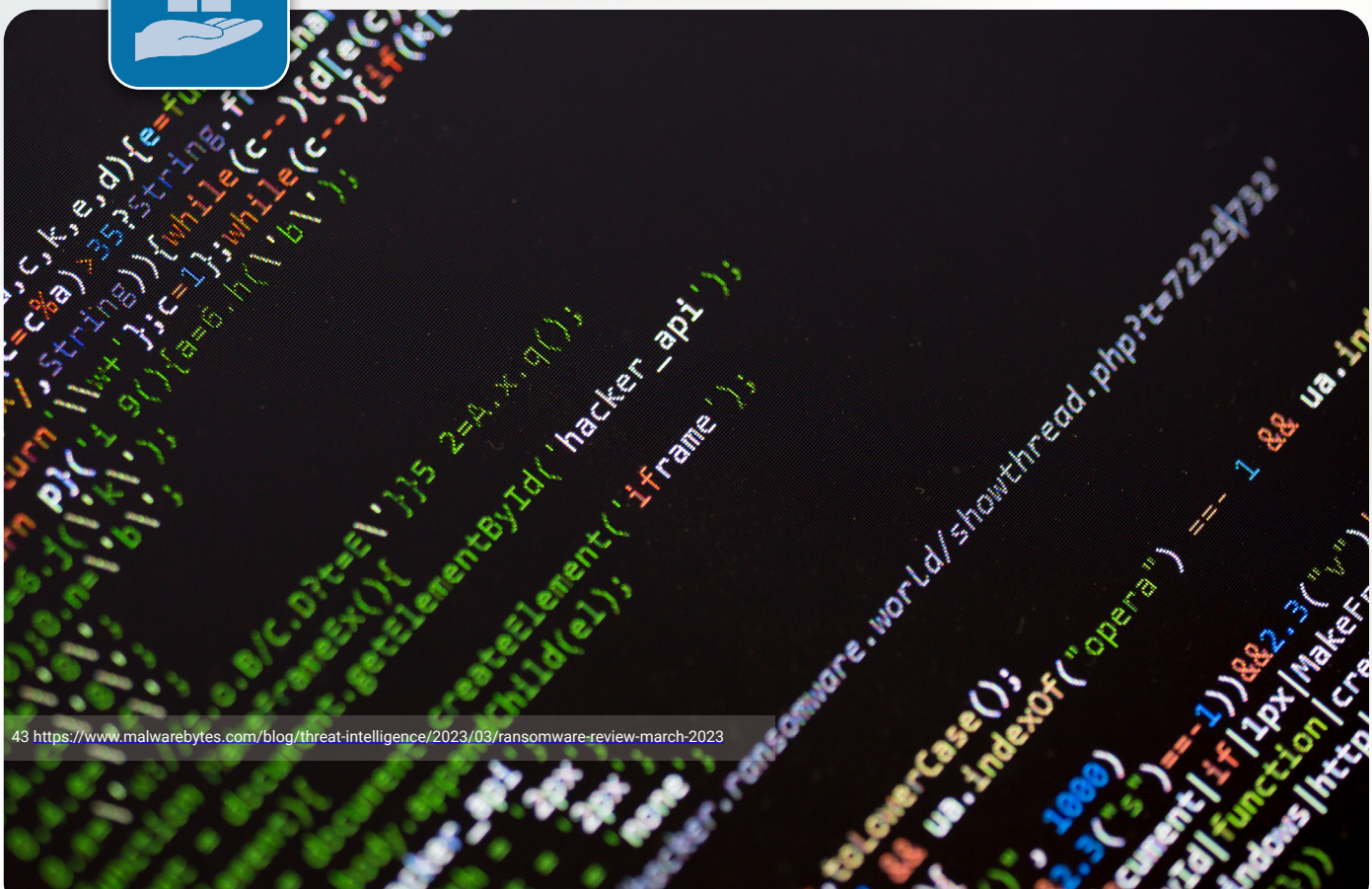
Ilustración 21. Top-10 grupos de ransomware Latinoamérica.T4 2023 y T1 2024. Fuente: Lab52 (S2 Grupo)

38 https://github.com/cert-orangecyberdefense/ransomware_map/blob/main/OCD_WorldWatch_Ransomware-ecosystem-map.pdf
39 https://www.europol.europa.eu/media-press/newsroom/news/cybercriminals-stung-hive-infrastructure-shut-down
40 https://github.com/cert-orangecyberdefense/ransomware_map/blob/main/OCD_WorldWatch_Ransomware-ecosystem-map.pdf


TITLE RED HAT ENTERPRISE LINUX SERVER (2.6.32-696
ROOT (HD0,0)
KERNEL /VMLINUZ-2.6.32-696.6.3.EL6.X86_64 RO ROOT
ANG=EN_US.UTF-8 RD_LVM_LV=OS_VG/SWAP_01_LV RD_NO_DM
OT_LV KEYBOARDTYPE=PC KEYTABLE=US RD_NO_DM
ADLINE TRANSPARENT_HUGEPAGE=NEVER DEBUG
LV=OS_VG/ROOT_LV KEYBOARDTYPE=PC KEYTABLE=US
TITLE RED HAT ENTERPRISE LINUX SERVER (2.6.32-696
ROOT (HD0,0)
KERNEL /VMLINUZ-2.6.32-696.6.3.EL6.X86_64 RO ROOT
ANG=EN_US.UTF-8 RD_LVM_LV=OS_VG/SWAP_01_LV RD_NO_DM
OT_LV KEYBOARDTYPE=PC KEYTABLE=US RD_NO_DM
ADLINE TRANSPARENT_HUGEPAGE=NEVER DEBUG
LV=OS_VG/ROOT_LV KEYBOARDTYPE=PC KEYTABLE=US
TITLE RED HAT ENTERPRISE LINUX SERVER (2.6.32-573
ROOT (HD0,0)
KERNEL /VMLINUZ-2.6.32-573.1.1.EL6.X86_64 RO ROOT
N_US.UTF-8 RD_LVM_LV=OS_VG/SWAP_01_LV RD_NO_DM
DTYPE=PC KEYTABLE=US RD_NO_DM ELEVATOR=NOOP
OARDTYPE=PC KEYTABLE=US RD_NO_DM ELEVATOR=DEADLINE
TITLE RED HAT ENTERPRISE LINUX SERVER (2.6.32-573
ROOT (HD0,0)
KERNEL /VMLINUZ-2.6.32-573.1.1.EL6.X86_64 RO ROOT
N_US.UTF-8 RD_LVM_LV=OS_VG/SWAP_01_LV RD_NO_DM
DTYPE=PC KEYTABLE=US RD_NO_DM ELEVATOR=NOOP
OARDTYPE=PC KEYTABLE=US RD_NO_DM ELEVATOR=DEADLINE

5 METODOLOGÍA DEL RANSOMWARE

En esta sección se destacan los aspectos más significativos en cuanto a las metodologías que siguen los grupos RaaS para el despliegue del ransomware. Si bien en el informe previo se hizo una descripción exhaustiva de porqué es importante considerar las fases de: acceso inicial, post-explotación, exfiltración y cifrado, en este informe se ha visto necesario destacar aquellas vulnerabilidades más explotadas por los grupos de ransomware y su relación con otro malware.



43 https://www.malwarebytes.com/blog/threat-intelligence/2023/03/ransomware-review-march-2023

5.1 PRINCIPALES VECTORES DE ENTRADA

Los principales vectores de entrada conforme las TTPs analizadas y las fuentes consultadas continúan siendo, considerando los datos conocidos, el aprovechamiento de accesos RDP, las campañas de phishing y la explotación de vulnerabilidades.

Es notable sin embargo la información del informe de Coveware obre Q3 2023, en el que ya se observa un aumento notable del vector de entrada etiquetado como "Unknown" (desconocido). Este dato refleja aquellos casos para los cuales **no se pudo identificar el vector de entrada, dado que cuando se materializa la amenaza no quedan rastros suficientes de su origen.** Este dato es muy importante y casa perfectamente con la operativa dividida en fases destacada al inicio del documento. **Mientras que los ataques de ransomware pueden ser llamativos y rápidos en cuanto a efecto, hay ataques, en aumento, que no se desencadenarán hasta pasado un tiempo.**

Este hecho no afecta únicamente a la imposibilidad de conocer más sobre el despliegue de las muestras, o la vinculación entre diferentes muestras, sino que también se da en las últimas fases de despliegue, en las que la ejecución en memoria dificulta notoriamente la

De los vectores de entrada anteriormente señalados, la explotación de vulnerabilidades es aquel que debería azotar únicamente cuando estas vulnerabilidades sean 0-day o muy recientes, aunque desafortunadamente no es así en muchos casos. Siguen registrándose vulnerabilidades con años de antigüedad empleadas por los atacantes.

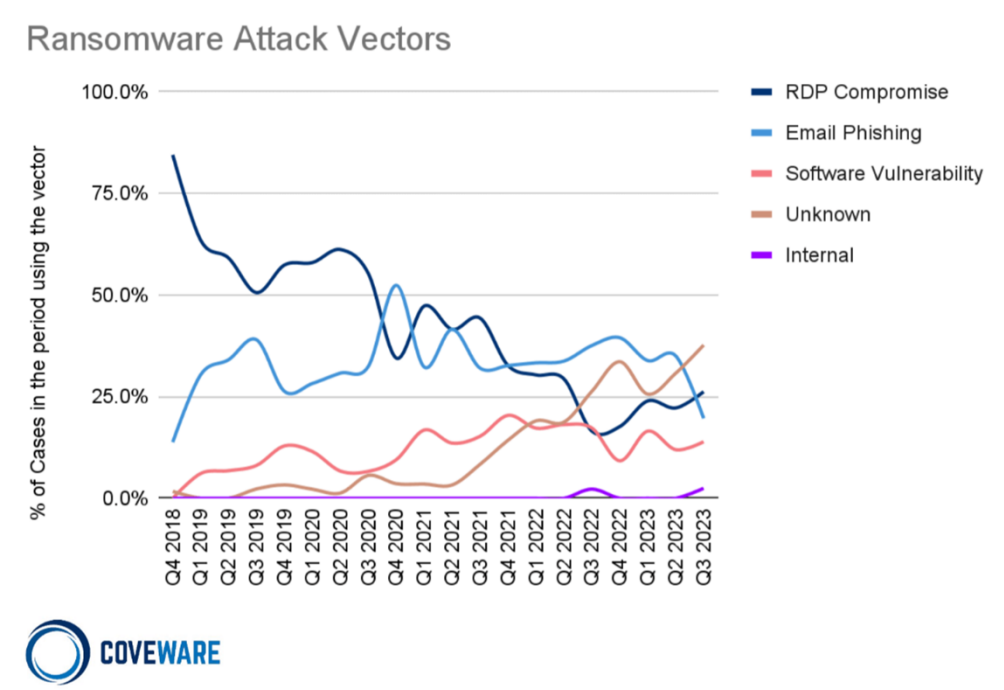


Ilustración 22. Progresión de los vectores de entrada más comunes. Fuente: Coveware[41]

41 https://www.coveware.com/blog/2023/10/27/scattered-ransomware-attribution-blurs-focus-on-ir-fundamentals

5.2 VULNERABILIDADES EXPLOTADAS

El conjunto de vulnerabilidades explotadas por los grupos de ransomware es variable. A lo largo de los años diferentes grupos de impacto han empleado vulnerabilidades que permitían el control de los sistemas afectados. El informe de RecordedFuture incluye un conjunto de vulnerabilidades explotadas por los grupos de ransomware desde 2017 a 2023[42] considerando esta y otras fuentes, a continuación, se incluye un resumen sobre las vulnerabilidades explotadas por los grupos de ransomware más destacados conforme los datos de ciberinteligencia de Lab52.

En particular, la Ilustración 23 resume el número de vulnerabilidades directamente vinculadas por diversas fuentes a los grupos de ransomware destacados. Por legibilidad se han considerado únicamente grupos con al menos 4 vulnerabilidades explotadas conocidas. Las vulnerabilidades pueden ser explotadas para el acceso y también para la explotación o el movimiento lateral, dependiendo del contexto.

Respecto a las vulnerabilidades más empleadas por más de cuatro familias diferentes de ransomware, la Ilustración 24 ofrece un ejemplo de algunas de ellas respecto a las fuentes públicas registradas por Lab52.

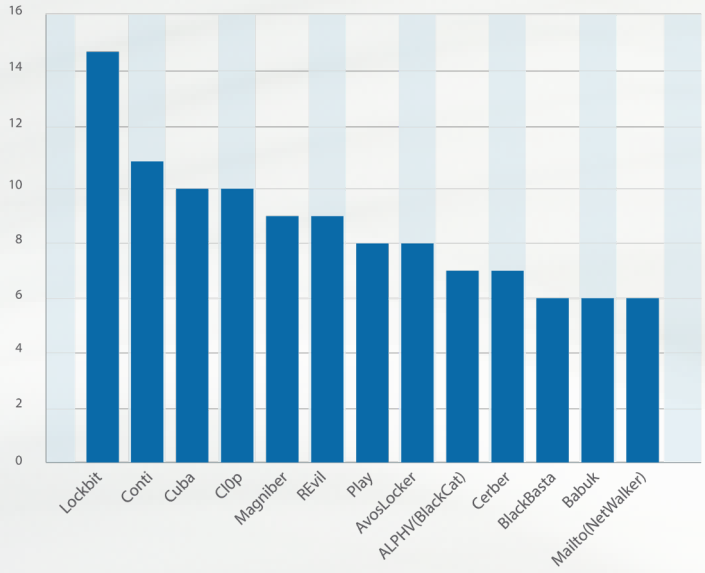


Ilustración 23. Vulnerabilidades conocidas explotadas por grupos[43]. Fuente: Lab52

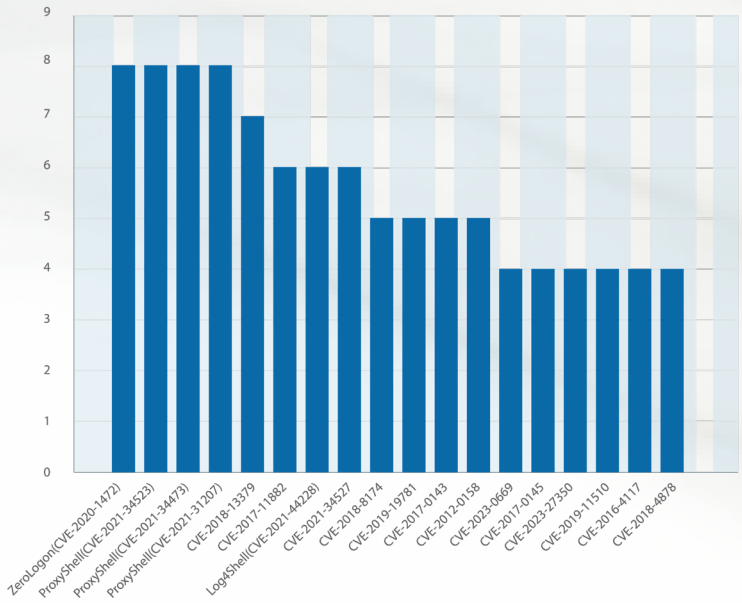


Ilustración 24. Vulnerabilidades explotadas por grupos de ransomware.

42 https://www.recordedfuture.com/patterns-targets-ransomware-exploitation-vulnerabilities-2017-2023
43 Se consideran grupos para los que conste en alguna de las fuentes consultadas como mínimo 4 vulnerabilidades explotadas.

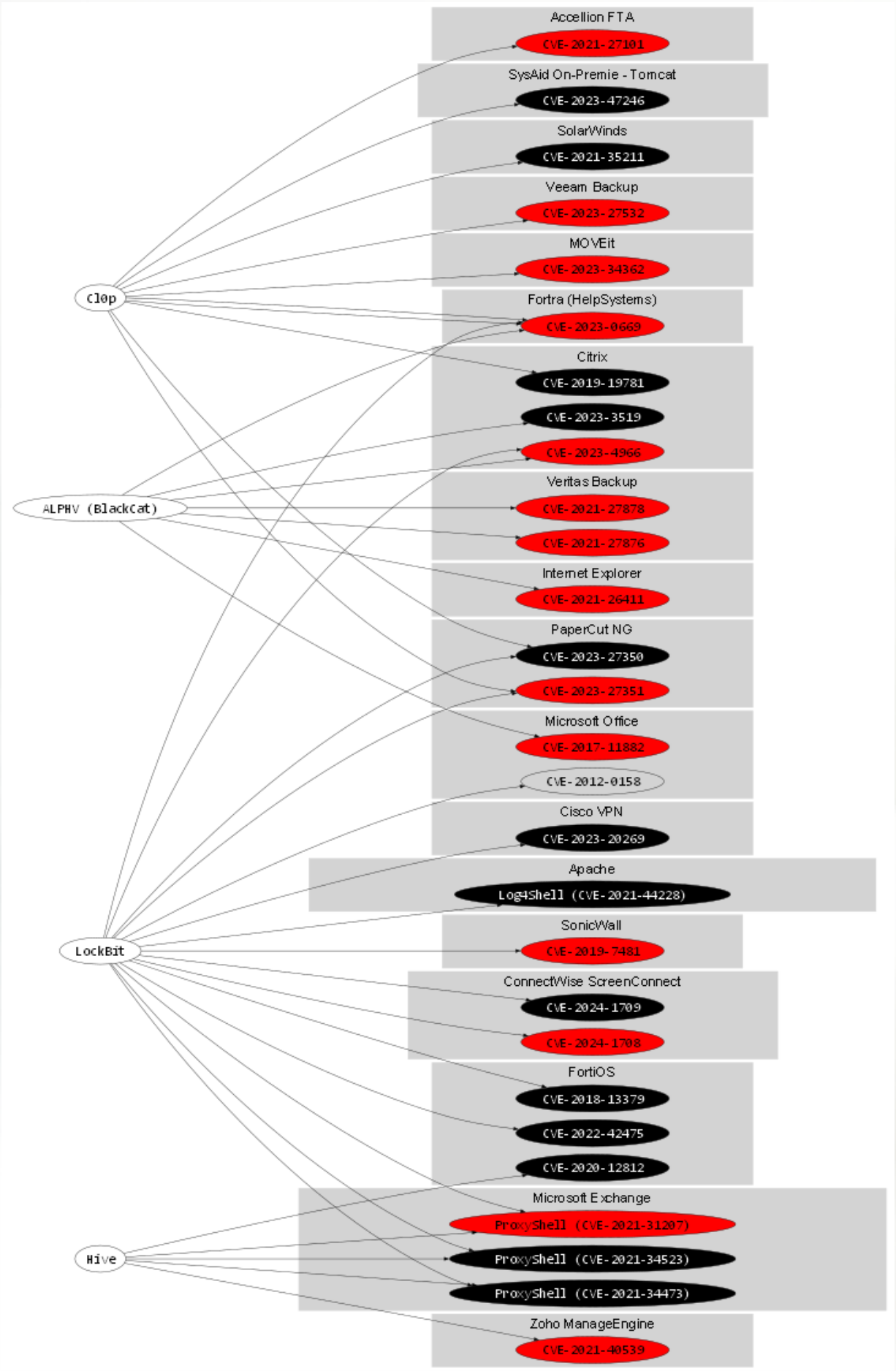


Ilustración 25. Relación entre vulnerabilidades y familias. Fondo Negro: Vulnerabilidad Crítica (NIST), Fondo Rojo: Vulnerabilidad Alta (NIST).

En dicho listado pueden observarse vulnerabilidades que han sido explotadas y que podrían seguir siendo explotadas por muestras de ransomware que aprovechen la exposición de plataformas sin las actualizaciones correspondientes.

También es imperativo recalcar **el uso de vulnerabilidades por parte de varios grupos que han ocasionado gran impacto.** No todas las vulnerabilidades son aprovechadas por cualquier grupo y dependería de los objetivos de los atacantes. Actualmente es esperable que los grupos de mayor impacto abarquen mayor volumetría de vulnerabilidades explotadas. La Ilustración 25 se ofrece a modo de ejemplo gráfico, en el que se relacionan las vulnerabilidades explotadas por cuatro grupos de gran impacto como son Cl0p, BlackCat, LockBit y Hive.

Durante febrero de 2024, además, Sophos anunciaba mediante un comunicado que había observado cómo LockBit estaba explotando también las vulnerabilidades que afectan al software ConnectWise ScreenConnect CVE-2024-1708 y CVE-2024-1709[44]. En particular, CVE-2024-1709 es una vulnerabilidad considerada crítica que permitiría sortear la autenticación y crear cuentas con permisos de administrador en instancias expuestas. No es descartable que estas vulnerabilidades estén siendo empleadas también por otros grupos.

Atendiendo únicamente a vulnerabilidades publicadas durante 2023 y 2024, la

Ilustración 26 sintetiza el numero de grupos de ransomware explotando la vulnerabilidad.

Algunas de ellas, nuevamente, son compartidas por grupos como Cl0p, LockBit y BlackCat. La Ilustración 27 se hace eco de vulnerabilidades reportadas en 2023 y 2024, cuya explotación por parte de los grupos está confirmada.

Además de las ya mencionadas vulnerabilidades sobre ScreenConnect que está explotando LockBit, debe sumarse la explotación de la vulnerabilidad CVE-2024-23334 por parte del grupo ShadowSyndicate[45]. Esta vulnerabilidad explota un fallo de validación en la biblioteca de Python AioHttp (Asynchronous Input Output HTTP) empleada en aplicaciones web de alto rendimiento. El exploit para la vulnerabilidad se hizo público a finales de febrero de 2024 y algunos ejemplos de explotación paso a paso estuvieron disponibles durante el mes de marzo. Conforme investigadores, el código de ShadowSyndicate podría estar vinculado con actores como BlackCat, Cl0p y Play, entre otros.

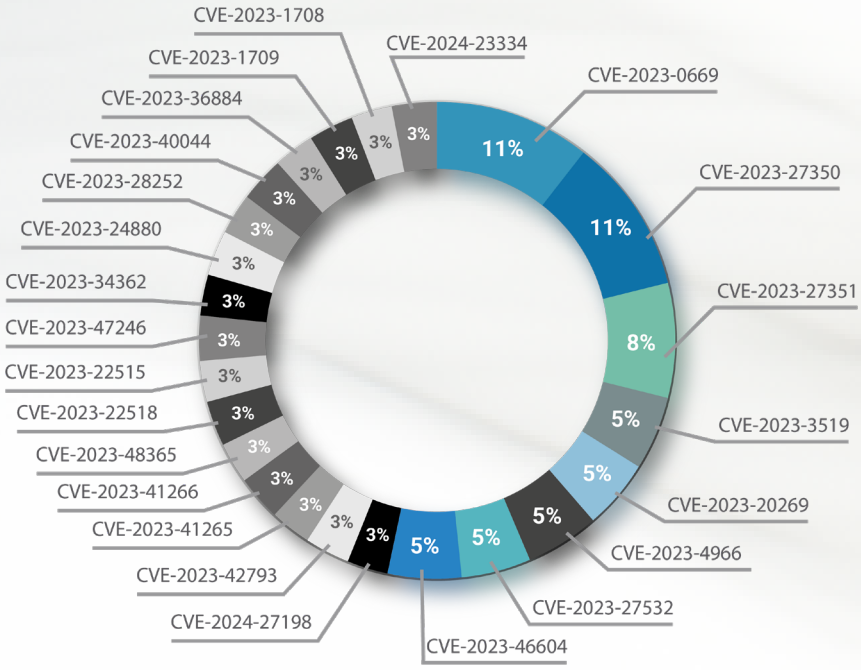


Ilustración 26. Vulnerabilidades de 2023 explotadas por los grupos de ransomware.

44 https://infosec.exchange/@SophosXOps/111975043941611370
45 https://www.bleepingcomputer.com/news/security/hackers-exploit-aiohttp-bug-to-find-vulnerable-networks/

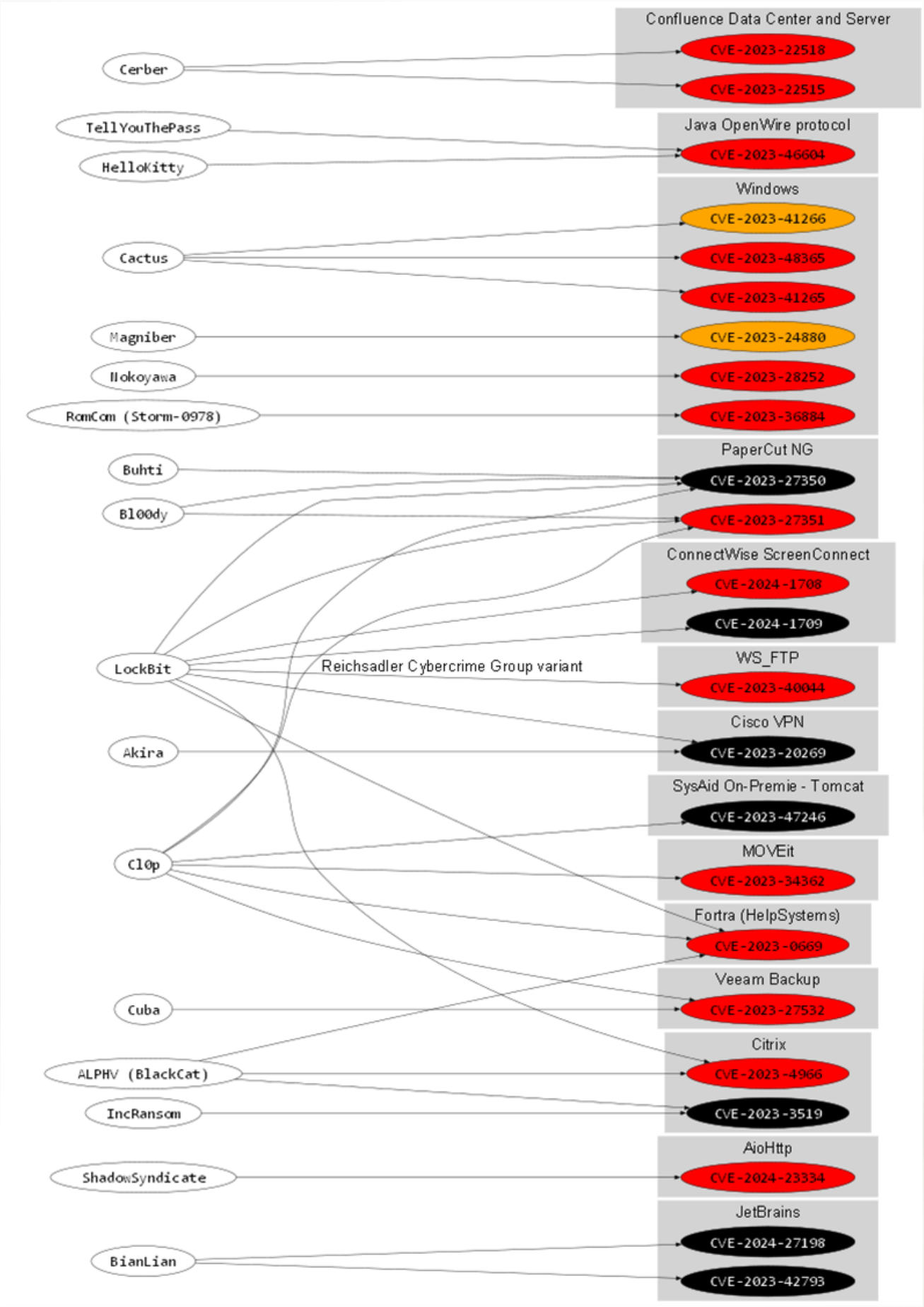


Ilustración 27. Uso de vulnerabilidades de 2023 por parte de ransomware

Tampoco hay que olvidar que las anteriores son vulnerabilidades de las que se conoce, en base a fuentes públicas, su explotación por parte de los grupos de ransomware. Sin embargo, cada día surgen nuevas vulnerabilidades que pueden ser potencialmente aprovechadas por los atacantes.

Por ejemplo, dado que los principales grupos ya cuentan con versiones para sistemas Linux, no sería de extrañar que aprovechasen la vulnerabilidad **CVE-2024-3094**, código asignado al código backdoor embebido en las utilidades XZ para versiones 5.6.0 y 5.6.1 que afecta a Linux y que fue descubierta a finales de marzo.

5.3 HERRAMIENTAS DEL RANSOMWARE

Como se adelantaba en el informe de panorama del ransomware 2023, los grupos de ransomware pueden desarrollar sus propias herramientas para la exfiltración de datos (p.ej. StealBit empleada por Lockbit[46]), además del software empleado para el cifrado. Más allá de estos desarrollos propietarios, también pueden emplear herramientas legítimas del sistema para realizar sus operaciones. En cualquier caso, el objetivo es siempre el mismo: minimizar el riesgo de exposición, detección y análisis. A continuación, se incluyen ejemplos de técnicas empleadas actualmente por el ransomware con dichos objetivos.

5.3.1 MINIMIZAR EL RIESGO DE EXPOSICIÓN

El despliegue del malware de forma modular es una táctica encaminada a minimizar el riesgo de exposición de dicho activo, además de mejorar también las posibilidades de que pase desapercibido. Esta modularización en fases permite, además, particularizar mejor el código. La interactuación con el nodo de comando y control (C2) podría permitir descargar software específico para un sistema. Esto dependerá siempre del grupo que haya detrás del ataque.

La Ilustración 28 muestra dos vías de operativa observada en los grupos de ransomware, la automatizada y la manual[47]. La automatizada es la que podrían seguir grupos menores que no realicen una discriminación necesariamente entre víctimas, o que en el propio código del malware incluyan un listado de objetivos u otra característica.

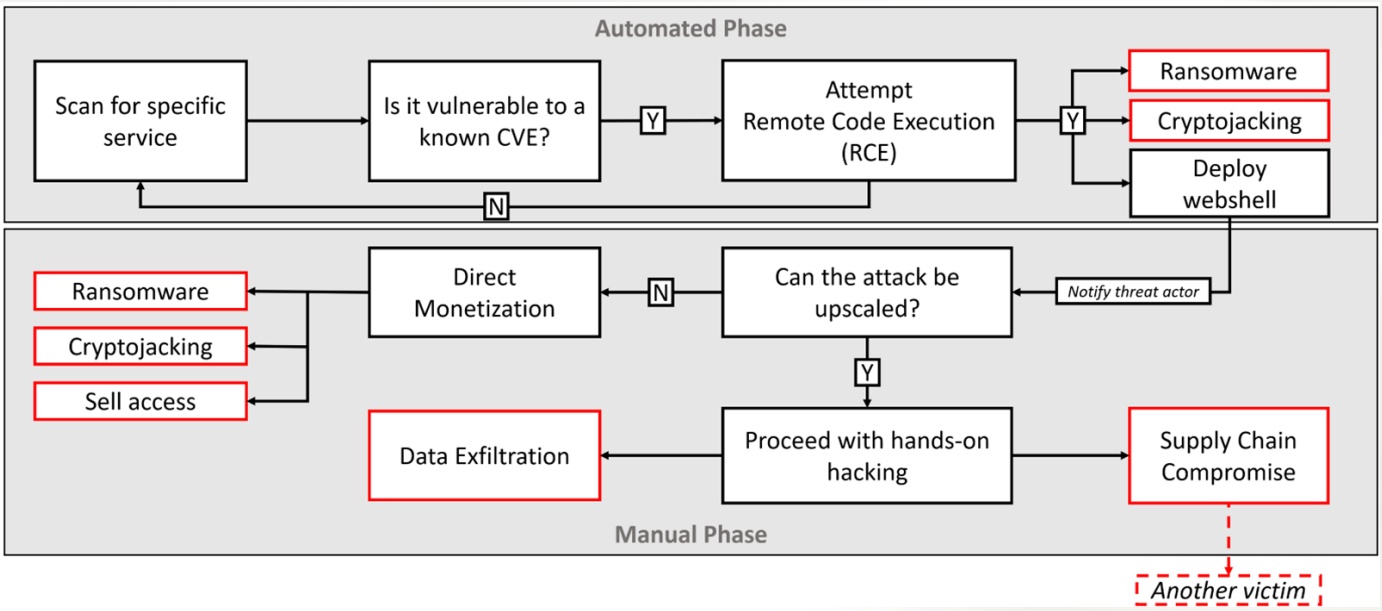


Ilustración 28. Despliegue de ransomware automatizado vs manual. Fuente: BitDefender[44]

46 https://www.cybereason.com/blog/research/threat-analysis-report-inside-the-lockbit-arsenal-the-stealbit-exfiltration-tool
47 https://www.bitdefender.com/blog/businessinsights/tech-advisory-manageengine-cve-2022-47966/
48 https://www.bitdefender.com/blog/businessinsights/tech-advisory-manageengine-cve-2022-47966/

Tampoco es descartable que en un equipo comprometido con ransomware se identifiquen otras muestras de malware, pudiendo ser el acceso al sistema aprovechado por varios actores, como se indica en el artículo de Talos sobre un caso de infección de Avos Locker en el que se identificaron muestras no relacionadas de DarkComet[49].

Por último, la mejora del software empleado por los grupos es fundamental para su éxito. Los analistas de malware buscarán cualquier fallo para tomar ventaja, ya sea para la construcción de defensas o para llevar a cabo la recuperación de los datos. A este respecto, una novedad importante introducida por LockBit fue el **programa de recompensas ante el descubrimiento de vulnerabilidades en su software o en sus procedimientos que llevase a poner en riesgo su operativa.** Este tipo de incentivos permite mejorar el software malicioso.

Entre las mejoras necesarias también se encuentra el disponer de utilidades que mejoren la exfiltración de datos, en aquellos grupos que empleen la extorsión múltiple. LockBit vuelve a ser un ejemplo en este sentido, jactándose de los tiempos de exfiltración conseguidos por su utilidad StealBit en comparación con otras[50]. Entre sus características está el **aprovechar funcionalidades nativas de Windows para ser más eficiente en la exfiltración** minimizando además el tiempo de exposición. Por ejemplo, paralelizando las tareas de exfiltración cuando es posible para finalizar antes, o por medio de integrar el soporte para comunicación interproceso, que permitiría la comunicación entre múltiples procesos StealBit. Esta característica estuvo presente desde LockBit 2.0, aunque puede variar dependiendo de la campaña.

La adaptabilidad de los grupos es crítica en todo este proceso. La Ilustración 29 muestra el despliegue de LockBit 2.0 empleando StealBit antes del despliegue de ransomware, mientras que la Ilustración 30 ofrece un despliegue diferente, identificado para muestras LockBit 3.0, en el que se hace uso del malware SecGolish, vinculado al grupo APT EvilCorp[51].

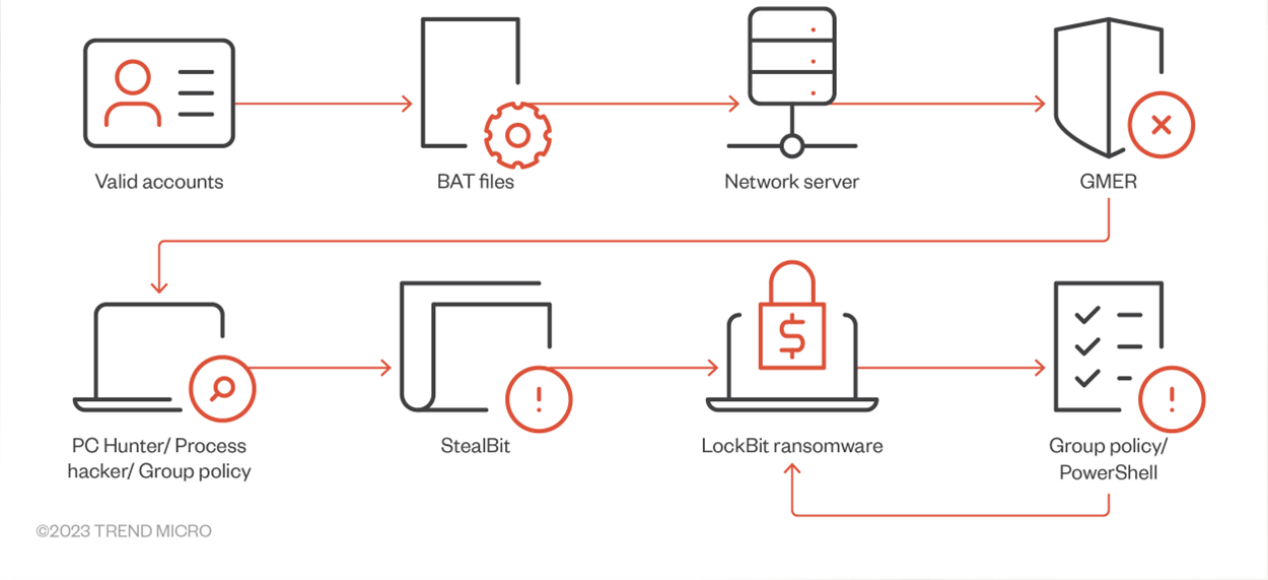


Ilustración 29. Infección de LockBit 2.0 – Fuente: TrendMicro[52]

49 https://blog.talosintelligence.com/avoslocker-new-arsenal/
50 https://www.cybereason.com/blog/research/threat-analysis-report-inside-the-lockbit-arsenal-the-stealbit-exfiltration-tool
51 https://redcanary.com/threat-detection-report/threats/socgholish/
52 https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-lockbit

Esta tendencia hacia la profesionalización de las operaciones y al uso cada vez más notable de herramientas empleadas por grupos APT, hacen que los grupos RaaS bien organizados tengan una operativa cada vez más efectiva.

5.3.2 EVASIÓN DE DEFENSAS

La evasión de defensas es una característica recurrente presente en todo despliegue de malware, y el ransomware no es una excepción. Por lo general, en una infección el software malicioso puede comprobar las herramientas presentes en el sistema, deshabilitarlas, o incluso aprovecharlas. El ransomware, si está en el paso final de la infección podría depender de otro malware previo que facilite la deshabilitación de dichas utilidades, o de las habilidades de operadores humanos que, empleando la comunicación con el C2, evalúen las utilidades a ser deshabilitadas.

Algunas comprobaciones habituales antes del despliegue de ransomware son las siguientes:

- Deshabilitación de sistemas antivirus y, en su caso, Windows defender u otros sistemas empleados para la monitorización y detección.
- Búsqueda de software como BloodHound, SeatBelt, ProcessHacker u otras herramientas de análisis.
- Modificaciones en políticas de grupo.
- Inclusión de nuevos usuarios y obtención de privilegios.

El uso de herramientas propietarias supone un riesgo para los cibercriminales en el caso de que éstas sean identificadas. El software nativo al sistema operativo puede despertar menos sospechas, aunque no esté diseñado exprofeso para minimizar los rastros de la operativa o realizar otras actuaciones.

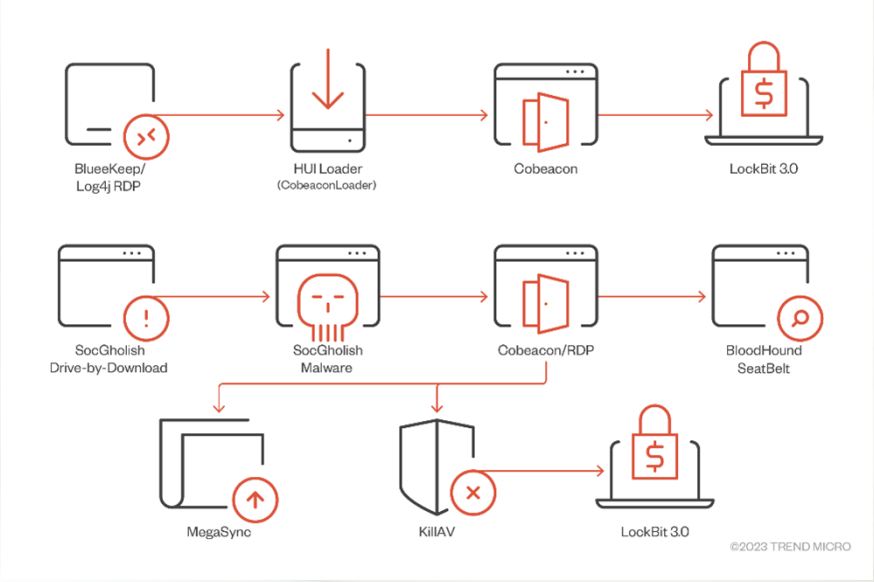


Ilustración 30. Infección de LockBit 3.0. Fuente: TrendMicro[53]

53 https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-lockbit

5.3.3 ANTI-ANÁLISIS

Volviendo a StealBit, dicha utilidad también tiene características anti-análisis, como comprobar por ejemplo el contexto de ejecución para identificar la presencia del debugger, o la carga de librerías con nombres previamente ofuscados[54].

En general, los mecanismos anti-análisis aplicados a nivel de código persiguen evitar que el malware, una vez identificado y capturado, pueda ser comprendido por los analistas. Es una protección que resulta habitual para la protección del software, y los desarrolladores de malware mínimamente profesionales la aplican.

A este fin contribuyen mucho las fugas de código de los grupos fuertes de ransomware, que permiten que desarrolladores no tan avanzados puedan particularizar y proteger sus muestras antes de liberar la campaña.

Por ejemplo, Play cuenta entre sus técnicas anti-análisis a nivel de código las siguientes[55]:

- Dificultar conocer la dirección de retorno en las funciones, para evitar que el decompilador pueda realizar una adecuada interpretación de las funciones.
- Código basura, para retrasar y dificultar el entendimiento del código por parte de los analistas.
- API Hahsing – los nombres de las funciones se encuentran ofuscados y solo son visibles en tiempo de ejecución, en memoria.
- Cifrado de cadenas – las cadenas relevantes se encuentran cifradas y se descifran en memoria, cuando van a ser usadas.

Estas técnicas no son exclusivas de ransomware. Play, además, es un ransomware que se ha observado en despliegue como parte de una cadena mayor, y que puede tener malware que lo precede. Aún así, se encuentra protegido. Es sólo un ejemplo, pero la tendencia actual es que el código del ransomware se encuentre mínimamente protegido para evitar su análisis.

54 https://www.cybereason.com/blog/research/threat-analysis-report-inside-the-lockbit-arsenal-the-stealbit-exfiltration-tool
55 https://chuongdong.com/reverse%20engineering/2022/09/03/PLAYRansomware/#anti-analysis

6 PROTECCIÓN FRENTE AL RANSOMWARE

Considerando la evolución de los actores del RaaS y la operativa observada en las diferentes campañas, en esta sección se sintetizan las recomendaciones y acciones que pueden llevarse a cabo para mejorar la protección de los sistemas frente al ransomware.

6.1 RECOMENDACIONES FRENTE AL RANSOMWARE

Los mecanismos de protección frente al ransomware deben contemplar toda la cadena de infección, y por ello podrían resumirse en los siguientes puntos:

- **Campañas de información y concienciación, dirigidas a público específico dentro de la organización.** Estas campañas no pueden ser generales, dado que se conocen diferentes vectores de entrada que deben atajarse. En particular, aunque no de forma excluyente, **motivar e informar al equipo técnico responsable de la adaptación de las reglas de detección y monitorización es básico.** Entidades nacionales como CCN-CERT o INCIBE tienen un claro carácter difusor sobre nuevas formas de amenazas y vulnerabilidades que podrían ser aprovechadas por los grupos de Ransomware. Además, plataformas como StopRansomware[56] pueden informar sobre recursos específicos que puede emplear la comunidada para informarse y protegerse.
- **Mejorar la gestión de activos y el seguimiento de vulnerabilidades.** Todos los activos deben seguir un flujo de control, y sus vulnerabilidades conocidas y mitigadas cuanto antes, estableciendo medidas de seguridad adaptadas a los diferentes escenarios. Idealmente el equipo técnico deben entender en qué se basan las correcciones de vulnerabilidades que aplican. Este es un problema que no concierne únicamente al ransomware, pero del que se beneficia indudablemente.
- **Mantener el software de seguridad actualizado con las últimas firmas de detección.** Los grupos de RaaS invierten en el desarrollo y mejora de su software como activo valioso que es. Sus mejoras consisten en evadir mejor los sistemas de detección y monitorización. Es por ello que cada vez es más importante nutrir a los sitemas de detección más allá de las firmas antivirus.

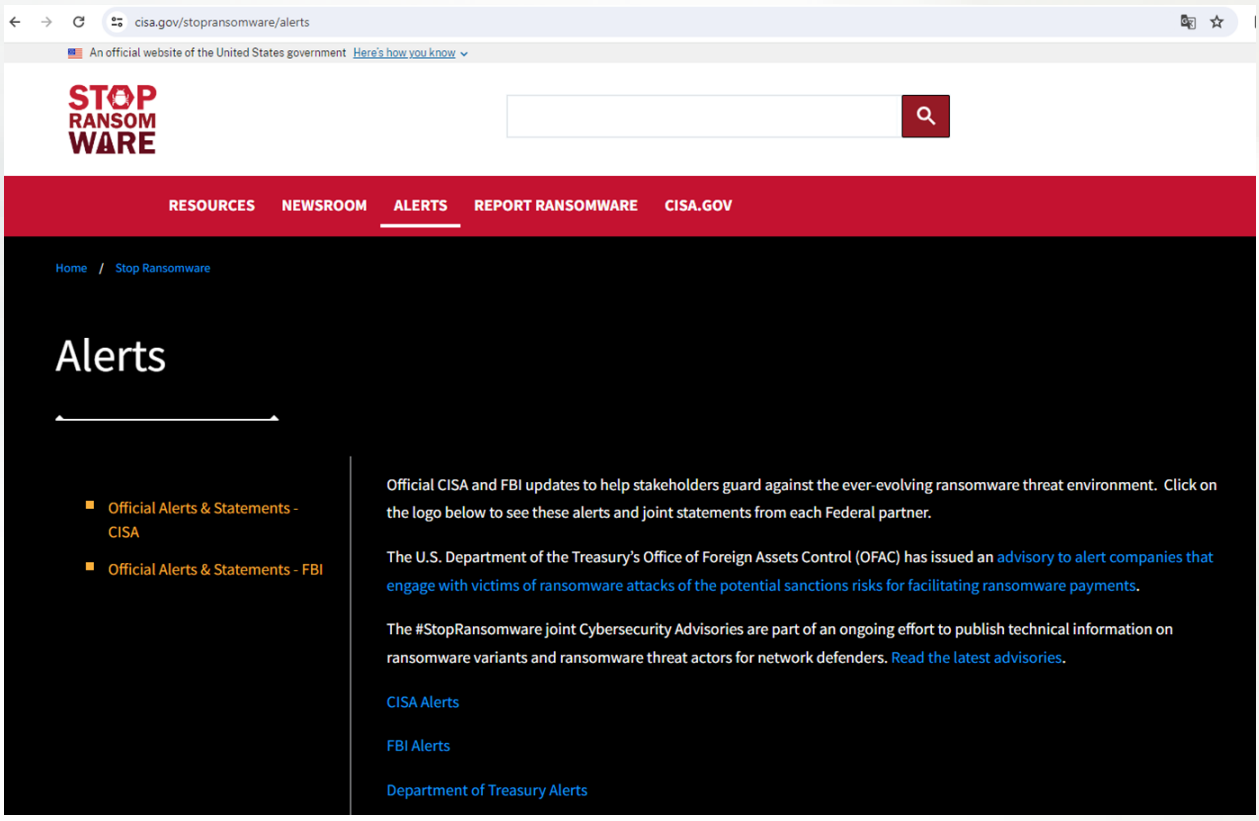


Ilustración 31. StopRansomware (CISA)[57]

56 https://www.cisa.gov/stopransomware/alerts
57 https://www.cisa.gov/stopransomware/alerts

- **Disponer de profesionales capaces de operar con las herramientas de seguridad y adaptarlas al contexto de la organización.** A medida que los grupos RaaS se profesionalizan su operativa tiende más a asemejarse a un APT. Emplean herramientas cada vez más sofisticadas. Es por ello que cada vez los sistemas tradicionales sin mantenimiento por parte de profesionales cualificados se vuelven más ineficientes. Las herramientas de seguridad no sirven de nada sin el mantenimiento adecuado.
- **Disponer de un plan de ciberseguridad que complemente los puntos anteriores y permita mejorar la gestión de recursos humanos y materiales.** Como parte de dicho plan de ciberseguridad deben contemplarse las medidas de preparación frente a los ataques de ransomware como casos específicos de ataque, y planificar las medidas de protección aplicables: copias de backup, sistemas de redundancia, etc.
- Además, es importante estar al corriente del ransomware para el cual se dispone de descifradores. **La publicación de descifradores permite que las víctimas eviten el pago del ransomware, impactando directamente en el negocio del RaaS.** Esto ocurre cuando la motivación para el pago se basa precisamente en la recuperación de dichos datos.

6.2 SOLUCIONES ESPECÍFICAS PARA CUBRIR TODO EL CICLO

Como ya se anticipó, el despliegue del ransomware se hace considerando el software malicioso como un activo de la organización cibercriminal, en este caso del grupo RaaS.

Herramientas específicas para frenar el ransomware, como microClaudia, permitirían detener infecciones en las primeras fases del despliegue del ransomware. Esto se visualiza en la Ilustración 32. **MicroClaudia es una herramienta ideada para confundir al ransomware y evitar el cifrado, emulando el concepto de vacunación en el cuerpo humano.** Es por ello que esta utilidad de vacunación contra el ransomware **actuaría en las primeras fases, antes del cifrado**. Las vacunas se definen por parte de un equipo de analistas de malware dedicado, y permiten frenar infecciones de ransomware considerando además otro malware como RAT, o bien utilidades que pueden usar los grupos de ransomware para el despliegue de muestras en las diferentes fases.

Sin embargo, como ya se ha mencionado, la operativa cada vez más especializada de los grupos de ransomware hace que la actualmente no base con soluciones específicas si no son alimentadas, aprovechando por ejemplo las fuentes de ciberinteligencia.

La Ilustración 33 ofrece una visión simplificada de las herramientas y recursos humanos necesarios para cubrir la monitorización de todo el ciclo de infección. Por una parte, como se ha adelantado, **MicroClaudia es alimentada con vacunas que proceden del análisis de malware.** Para esto es necesario contar con un equipo dedicado que conozca de primera mano las nuevas variantes de ransomware y sea capaz de generar dichas vacunas. No sólo eso, sino conocer qué variantes pueden afectar a los organismos por sectores contribuye notablemente a la hora de priorizar la generación de vacunas.

Sin embargo, no basta con la vacunación. **Soluciones SIEM como Gloria deben ser aplicadas para obtener evidencias sobre la actividad registrada en una organización y, por medio de la aplicación de reglas de detección, identificar de forma temprana cualquier actividad susceptible de análisis.** Nuevamente, el equipo humano detrás de las herramientas ayuda a la interpretación, pero también a mejorar las reglas de detección, también aprendiendo de los casos identificados para la organización. **La ciberinteligencia es fundamental para prepararse ante posibles ataques, y también para nutrir otras utilidades con analizadores, es el caso de CARMEN.** Carmen es la utilidad que permite a un equipo de Threat Hunting buscar patrones de intrusión en las organizaciones, y operar a través de Claudia. Nuevamente, se emplean analizadores que parten de análisis de malware considerando las diferentes fases de

la intrusión. **Ante cualquier indicio, CARMEN puede solicitar a CLAUDIA triajes que un equipo de especialistas DFIR puede interpretar para confirmar o descartar la amenaza.**

Las herramientas, por lo tanto, contribuyen a la efectividad del equipo humano, que es fundamental en **el proceso de respuesta, orquestado a través de un conjunto de SOCs.**

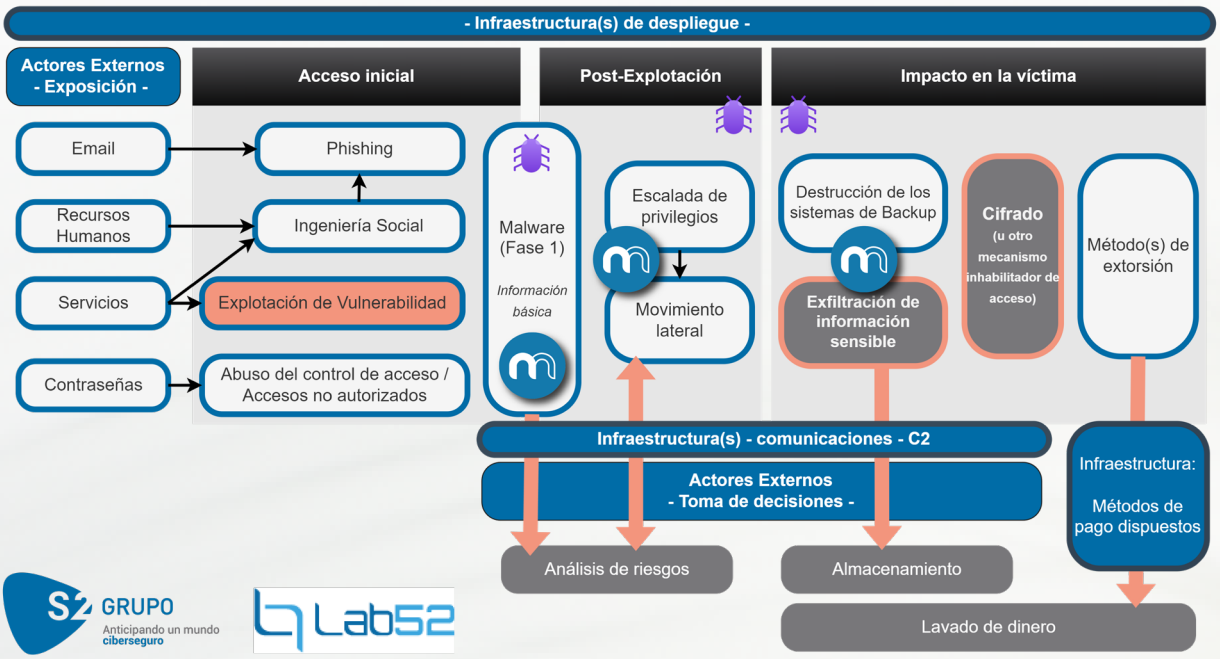


Ilustración 32. MicroClaudia en el ciclo de despliegue de ransomware

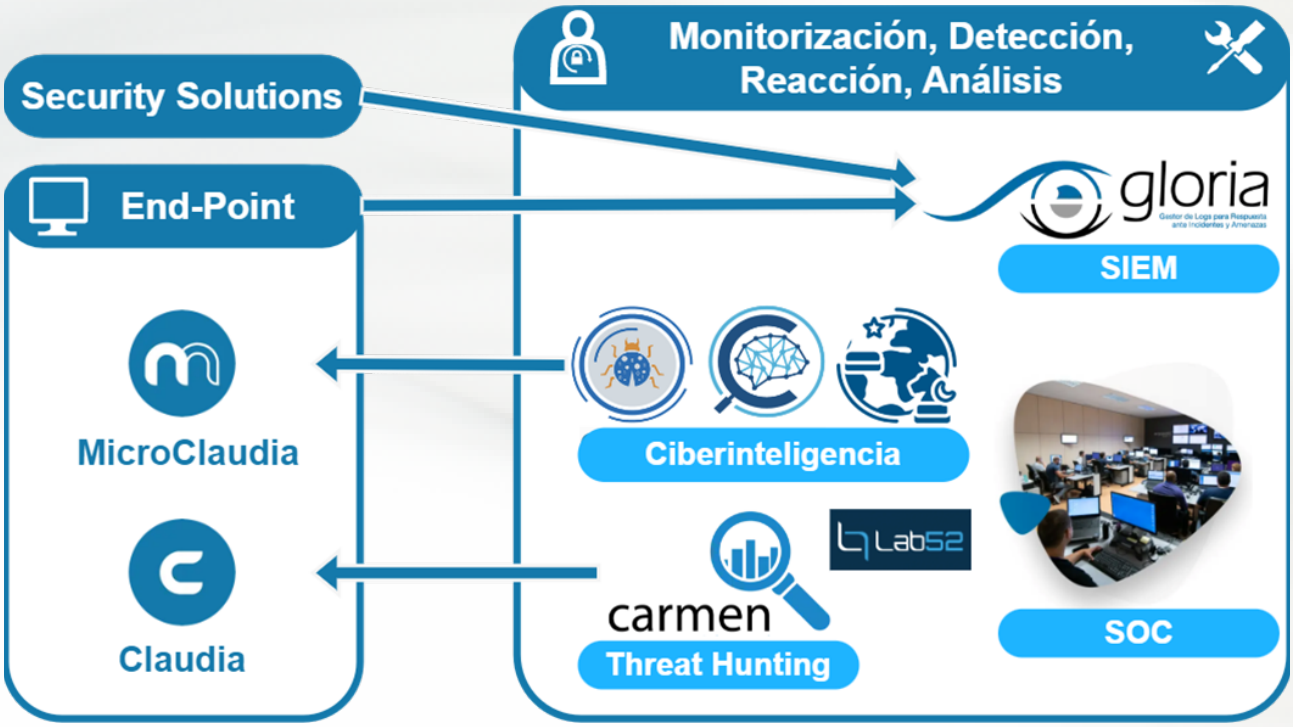


Ilustración 33. Monitorización, detección, reacción y análisis

CONCLUSIONES

El ransomware es una amenaza que sólo se detiene por medio de la colaboración entre entidades y afectadas, y trasciende al plano internacional. Comprender la evolución de los grupos RaaS resulta también fundamental para anticiparse a sus cambios de operativa y preparar mejor nuestras defensas.

En este informe se han analizado los últimos datos recopilados por el equipo de ciberinteligencia de S2 Grupo, que forma parte de Lab52. Durante el análisis se ha puesto de manifiesto la importancia que tiene el contexto geopolítico para comprender la evolución del ransomware, ya no únicamente como herramienta del cibercrimen, sino también su vinculación cada vez más cercana a grupos APT. No únicamente porque los grupos de ranomware usen herramientas que a su vez usan los grupos APT, sino porque haya registros de grupos APT que están haciendo uso de ransomware.

Un ejemplo destacado de profesionalización en RaaS es LockBit, que aún sufriendo una intervención durante este trimestre ha continuado su actividad. LockBit ha realizado fuertes inversiones para mejorar su operativa y su software, lanzando además un programa de recompensas a la comunidad. Tanto este grupo como otros invierten en la inversión y protección de su propio software, y algunos grupos destacan incluso la necesidad de contratar a profesionales. El impacto de LockBit hace que su repercusión se muestre en las distintas métricas observadas como el ransomware en el puesto número uno actualmente. Sin embargo, sí se percibe variabilidad entre grupos objetivos si cambiamos el contexto y centramos la atención en Latinoamérica.

Latinoamérica tiene su propia cultura que es importante destacar para comprender adecuadamente el contexto del cibercrimen y priorizar correctamente el análisis de ransomware que más impacta actualmente a los países que conforman la región. Existen, además, diferencias palpables en cuanto a los sectores afectados por ransomware, a nivel global y en Latinoamérica. El sector manufacturas a nivel global está siendo fuertemente afectado por las familias de ransomware más destacadas.

También se incluye en el informe un análisis de las vulnerabilidades que se conoce han estado explotando familias de ransomware. A este respecto, a día de hoy aún se publican artículos que destacan la explotación de vulnerabilidades numeradas hace varios años y que siguen siendo rentables para los grupos. Atendiendo a la cadena de despliegue del ransomware, el factor humano y la corrección de vulnerabilidades son puntos clave para detener esta amenaza.

Sin embargo, como se ha demostrado, el comportamiento cada vez más cercano a APT de los grupos de ransomware, así como sus cambios de operativa y su impacto divergente en diferentes regiones provoca que **la ciberinteligencia sea crucial para hacer frente a esta amenaza.** No sólo por comprender mejor la amenaza desde el punto de vista contextual, sino para **nutrir adecuadamente y de forma continua los sistemas de detección de intrusiones y las herramientas de vacunación.** En el panorama actual del ransomware queda más claro que nunca que la inversión en herramientas debe ir acompañada de **la inversión en recursos humanos cualificados y preparados**, y esto es algo de lo que los ciberdelincuentes ya han tomado nota.

S2 GRUPO
Anticipando un mundo
ciberseguro

MADRID
BARCELONA
VALENCIA CERT
VALENCIA HQ
SEVILLA
SAN SEBASTIÁN

SANTIAGO DE CHILE
C.D. MÉXICO
BOGOTÁ
BRUSELAS
LISBOA
RÓTERDAM

Síguenos en: • @s2grupo • s2grupo.es