zscaler™ | ThreatLabz

ThreatLabz 2022 Estado del ransomware Informe

Índice

Introducción

Si parece que el ransomware siempre está presente en las noticias, no es solo una exageración por parte de los medios de comunicación: el equipo de investigación de Zscaler ThreatLabz descubrió que los ataques de ransomware aumentaron un 80 % más entre febrero de 2021 y marzo de 2022 en comparación con el año anterior, estableciendo nuevos récords tanto en el volumen de ataques como en el coste de los daños.

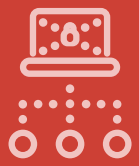
El ransomware es cada vez más atractivo para los atacantes, que pueden pagar campañas cada vez más rentables basadas en tres tendencias principales:

Ataques a la cadena de suministro

que aprovechan las relaciones de confianza con los proveedores para vulnerar las organizaciones y multiplicar el daño de los ataques al permitir a los autores de la amenaza atacar a múltiples (a veces cientos o miles) de víctimas al mismo tiempo.

Ransomware como servicio

que utiliza redes afiliadas para distribuir ransomware a gran escala, lo que permite a los hackers expertos en infringir redes compartir ganancias con los grupos de ransomware más avanzados.



Ataques de extorsión múltiple

que utilizan el robo de datos, los ataques de denegación de servicio distribuido (DDoS), las comunicaciones con los clientes y otros métodos, como tácticas de extorsión por capas, para aumentar los pagos de rescate.

Estas tácticas se unen hasta convertirse en muy perjudiciales. Los expertos del sector predicen que el ransomware será la principal táctica utilizada en las infracciones de terceros y los ataques a la cadena de suministro en 2022, y que el coste global de los daños causados por el ransomware crecerá hasta alcanzar los 42 mil millones de dólares en 2024.

Estas tendencias han hecho que el ransomware ascienda varios puestos en la lista de prioridades de ciberseguridad de las organizaciones de todos los sectores. "El Informe CISOs" de Aimpoint 2022 descubrió que el ransomware es la amenaza por la que los CISO de todo el mundo están más preocupados.

¿Cómo puede identificar y defenderse de las últimas variantes de ransomware? Este informe debería ayudarle.

ThreatLabz analiza los datos de más de 200 mil millones de transacciones diarias y 150 millones de ataques diarios bloqueados a través de Zscaler Zero Trust Exchange junto con la inteligencia de amenazas de Zscaler ThreatLabz para rastrear las familias de amenazas prevalentes, identificar las tendencias emergentes y mejorar las protecciones para los clientes de Zscaler. En este informe, ThreatLabz analizó los datos de ransomware desde el 1 de febrero de 2021 hasta el 31 de marzo de 2022 para identificar las familias de ransomware más prolíficas y sus tácticas. Compartiremos nuestros hallazgos, predicciones y orientación sobre las mejores prácticas para ayudarle a tomar decisiones informadas acerca de sus estrategias de defensa contra el ransomware.

Hallazgos clave

Los ataques de ransomware aumentaron en un 80 % con respecto al año anterior y representaron la totalidad de las cargas útiles de ransomware observadas en la nube de Zscaler.

El ransomware de doble extorsión aumentó un 117 %, lo que refleja que cada vez son más los ataques que incluyen el robo de datos en sus estrategias. Algunos sectores experimentaron un crecimiento especialmente elevado de los ataques de doble extorsión, como la sanidad (643 %), los servicios de alimentación (460 %), la minería (229 %), la educación (225 %), los medios de comunicación (200 %) y la industria manufacturera (190 %).

La industria manufacturera fue el sector que recibió más ataques por segundo año consecutivo, con casi el 20 % de los ataques de ransomware de doble extorsión.

Los ataques de ransomware a la cadena de suministro están aumentando, al igual que los ataques a la cadena de suministro en general. Explotar a proveedores de confianza permite a los atacantes infiltrarse en un gran número de organizaciones a la vez, incluidas las organizaciones que de otra manera tienen fuertes protecciones contra ataques externos. Los ataques de ransomware de la cadena de suministro del año pasado incluyeron dañinas campañas contra Kaseya y Quanta, así como una serie de ataques que aprovechan la vulnerabilidad de Log4j.

El ransomware como servicio está promoviendo más ataques. Los grupos de ransomware siguen reclutando afiliados a través de foros criminales clandestinos. Estos afiliados vulneran grandes organizaciones e implementan el ransomware del grupo, normalmente a cambio de alrededor del 80 % de los pagos de rescate recibidos de las víctimas. La mayoría (8 de 11) de las principales familias de ransomware utilizadas el año pasado han proliferado habitualmente a través de modelos de ransomware como servicio.

Las fuerzas del orden están tomando medidas. Varias de las familias de ransomware más importantes del año pasado, especialmente las que se dirigen a servicios críticos, atrajeron la atención de las fuerzas de seguridad de todo el mundo. REvil (responsable de los famosos ataques a Kaseya y JSB), DarkSide (responsable del ataque a Colonial Pipeline) y Egregor (un cambio de marca de Maze, la familia de ransomware más importante del año pasado) sufrieron la incautación de activos por parte de las fuerzas de seguridad en 2021.

Las familias de ransomware no están desapareciendo, solo están cambiando de marca. Al sentir el aumento de la presión de las fuerzas de seguridad, muchos grupos de ransomware se han disuelto y reformado bajo nuevas banderas, en las que utilizan las mismas tácticas (o muy similares). DarkSide se ha rebautizado como BlackMatter, DoppelPaymer como Grief y Avaddon como Haron y Midas. Evil Corp, sancionada por el gobierno de los Estados Unidos, ha cambiado constantemente el nombre de sus operaciones de ransomware.

El conflicto entre Rusia y Ucrania tiene al mundo en alerta máxima. Se han producido varios ataques asociados con el conflicto Rusia–Ucrania, algunos de los cuales combinan varias tácticas, como HermeticWiper y ransomware PartyTicket. Hasta ahora, la mayor parte de esta actividad se ha centrado en Ucrania. Sin embargo, los organismos gubernamentales han advertido a las organizaciones que se preparen para ataques más generalizados, ya que el conflicto persiste.

La confianza cero sigue siendo la mejor defensa. Para minimizar la posibilidad de que se produzca una brecha y el daño que puede causar un ataque exitoso, su organización debe utilizar estrategias de defensa en profundidad que incluyan la reducción de la superficie de ataque, la aplicación de un control de acceso con mínimos privilegios y la supervisión e inspección continua de los datos en todo el entorno.

La evolución del ransomware

El ransomware es un tipo de malware que los cibercriminales utilizan para interrumpir la organización de una víctima. El ransomware cifra los archivos importantes de una organización en un formulario ilegible y exige un pago de rescate para desencriptarlos. Las peticiones de rescate suelen ser proporcionales al número de sistemas infectados y al valor de los datos encriptados: cuanto más haya en juego, mayor será el pago.

A finales de 2019, los atacantes evolucionaron sus tácticas de ransomware para incluir la exfiltración de datos, comúnmente conocidas como un ataque de ransomware de "doble extorsión". En estos ataques, si las víctimas deciden no pagar el rescate para descifrar los datos y, en su lugar, intentan restaurar los datos de una copia de seguridad, los atacantes amenazan con filtrar los datos robados. A finales de 2020, algunos atacantes de ransomware añadieron otra capa de ataque con tácticas de DDoS que bombardean el sitio web o la red de la víctima, creando aún más interrupción del negocio, presionando así a la víctima para negociar.

En 2021 e inicios de 2022, la tendencia de ransomware más perjudicial implica ataques a la cadena de suministro, en los que una infracción de un proveedor (normalmente un software u otro proveedor de tecnología) abre la puerta a ataques de segunda etapa en organizaciones que dependen de sus productos. Se estima que los ataques a la cadena de suministro aumentaron el 51 % en la segunda mitad de 2021. Los autores de amenazas han llegado a los titulares de las noticias a través de vulnerabilidades de productos de software populares como SolarWinds, Kaseya y Log4j, y esperamos que esta tendencia vaya en aumento en los próximos años.

Secuencia de ataque del ransomware

Los ataques de ransomware de hoy en día suelen tener las siguientes etapas:

1. **Compromiso inicial:** los atacantes utilizan una variedad de vectores de intrusión para obtener acceso a los sistemas, incluidos correos electrónicos de phishing, explotación de vulnerabilidades en las herramientas de administrador remoto o de red privada virtual (VPN), y uso de fuerza bruta o credenciales robadas para acceder a las conexiones del protocolo de escritorio remoto (RDP). Los ataques a la cadena de suministro son otro método para infiltrarse en una organización.

2. **Movimiento lateral:** después de obtener el acceso inicial, los autores de la amenaza proceden a recopilar la información de la infraestructura de las víctimas y se mueven lateralmente a través de los sistemas de la red, escalando privilegios y estableciendo mecanismos de persistencia según sea necesario, catalogando los datos clave para robar o cifrar y depositando las cargas útiles del ransomware para su posterior ejecución.

3. **Exfiltración de datos:** en el caso de un ataque de doble extorsión, los atacantes robarán posteriormente los datos confidenciales que se usarán como táctica de extorsión secundaria para poder exigir mayores pagos de rescate. Esto reduce las opciones de las víctimas: incluso si pueden recuperar los datos cifrados de las copias de seguridad, aún deberán enfrentarse a la amenaza de que los ciberdelincuentes filtren los datos robados.

4. **Ejecución del ransomware:** a continuación, los atacantes implementan y ejecutan el ransomware, cifrando los archivos específicos en los sistemas conectados a la red. El ransomware generalmente finaliza los procesos relacionados con el software de seguridad y las bases de datos para maximizar el número de archivos que puede cifrar. Las copias de seguridad de Shadow Copy también suelen eliminarse del sistema para obstaculizar la recuperación de archivos. Algunas familias de ransomware también reiniciarán el sistema en peligro en Windows Safe Mode para omitir el software de punto final de seguridad antes del cifrado de archivos. Después del cifrado de archivos, las víctimas reciben una nota de rescate que proporciona instrucciones para pagar el rescate y descifrar sus archivos.

5. **DDoS:** si la víctima no negocia, algunos grupos de piratas informáticos lanzarán un ataque DDoS contra la red o el sitio web de la víctima, interrumpiendo sus operaciones comerciales para obtener una ventaja adicional.

La Figura 1 muestra la cadena de ataque típica de un ataque de ransomware de extorsión múltiple.

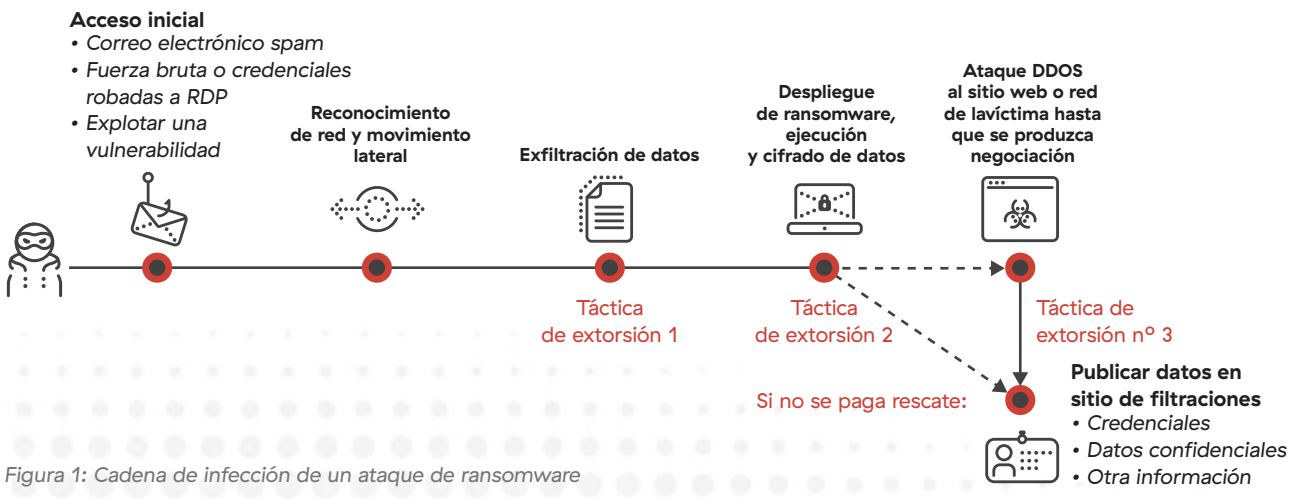


Figura 1: Cadena de infección de un ataque de ransomware

Estadísticas de ataques de ransomware 2021–2022

El gran volumen de datos de transacciones en Zero Trust Exchange proporciona una visión única de las tácticas y las víctimas de los ciberdelincuentes. Desde febrero de 2021 hasta marzo de 2022, ThreatLabz observó un aumento del 80 % en las cargas útiles de ransomware en comparación con el año anterior. Además, observamos un aumento del 117 % en las víctimas de ransomware de doble extorsión en función de los datos publicados en los sitios de filtración de datos de los autores de amenazas.

Verticales del sector afectados por el ransomware

El sector manufacturero ya fue el más atacado en 2020, constituyendo el 12,7 % de los ataques de ransomware de doble extorsión entre noviembre de 2019 y enero de 2021. Este año, el porcentaje de ataques a las organizaciones manufactureras aumentó aún más hasta alcanzar el 19,5 %, seguido de servicios (9,7 %), construcción (8,1 %), comercio minorista y mayorista (7,5 %) y alta tecnología (6,7 %).

Infecciones de ransomware por sector

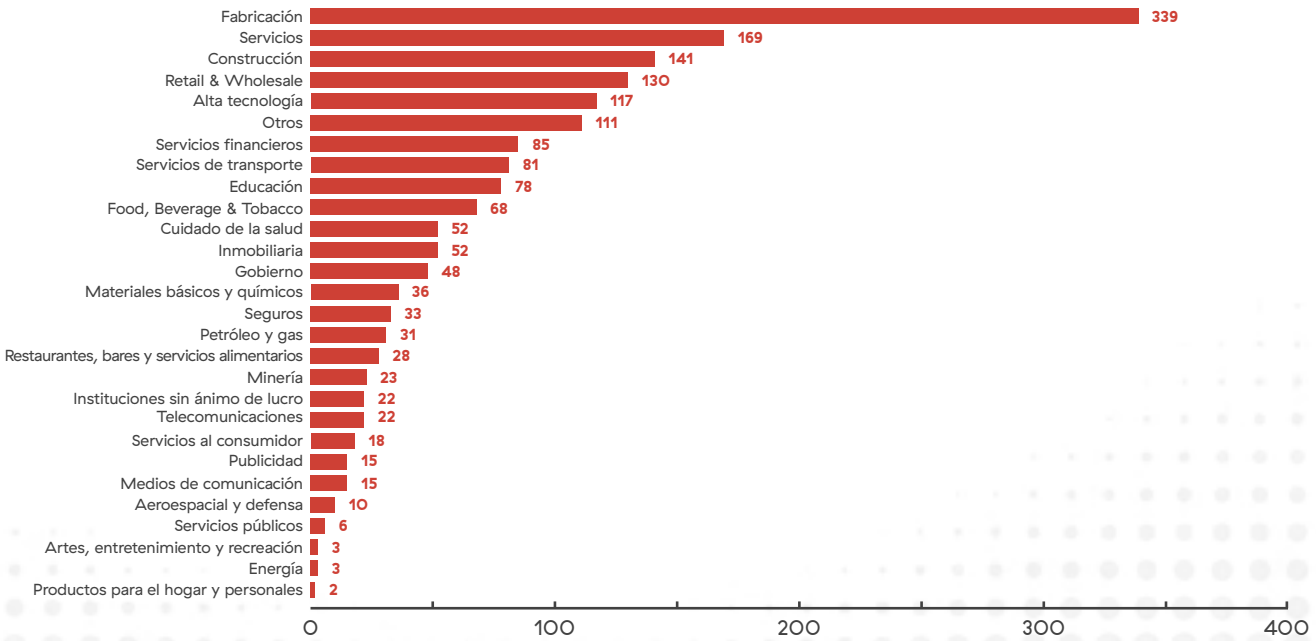


Figura 2: Infecciones por ransomware por sector

El crecimiento de los ataques de ransomware de doble extorsión varió enormemente según el sector. En el informe del año pasado, observamos un número particularmente reducido de ataques contra las organizaciones sanitarias, como consecuencia de un mayor escrutinio por parte de las fuerzas del orden público, así como la promesa de varias familias de ransomware prevalentes de que no atentarían contra la sanidad durante la pandemia de la COVID-19.

Los datos de este año cuentan una historia diferente. Los ataques de ransomware de doble extorsión contra el ámbito sanitario crecieron en un 643 % en 2021, aunque partían de una línea de base muy baja de ataques en 2020. Otros sectores verticales con puntos de partida más altos también experimentaron un crecimiento superior al 100 % en los ataques, como la educación (225 %), la industria manufacturera (190 %), la construcción (161 %), los servicios financieros (130 %) y los servicios (109 %).

Variación porcentual de los ataques de doble extorsión: 2021 frente a 2020

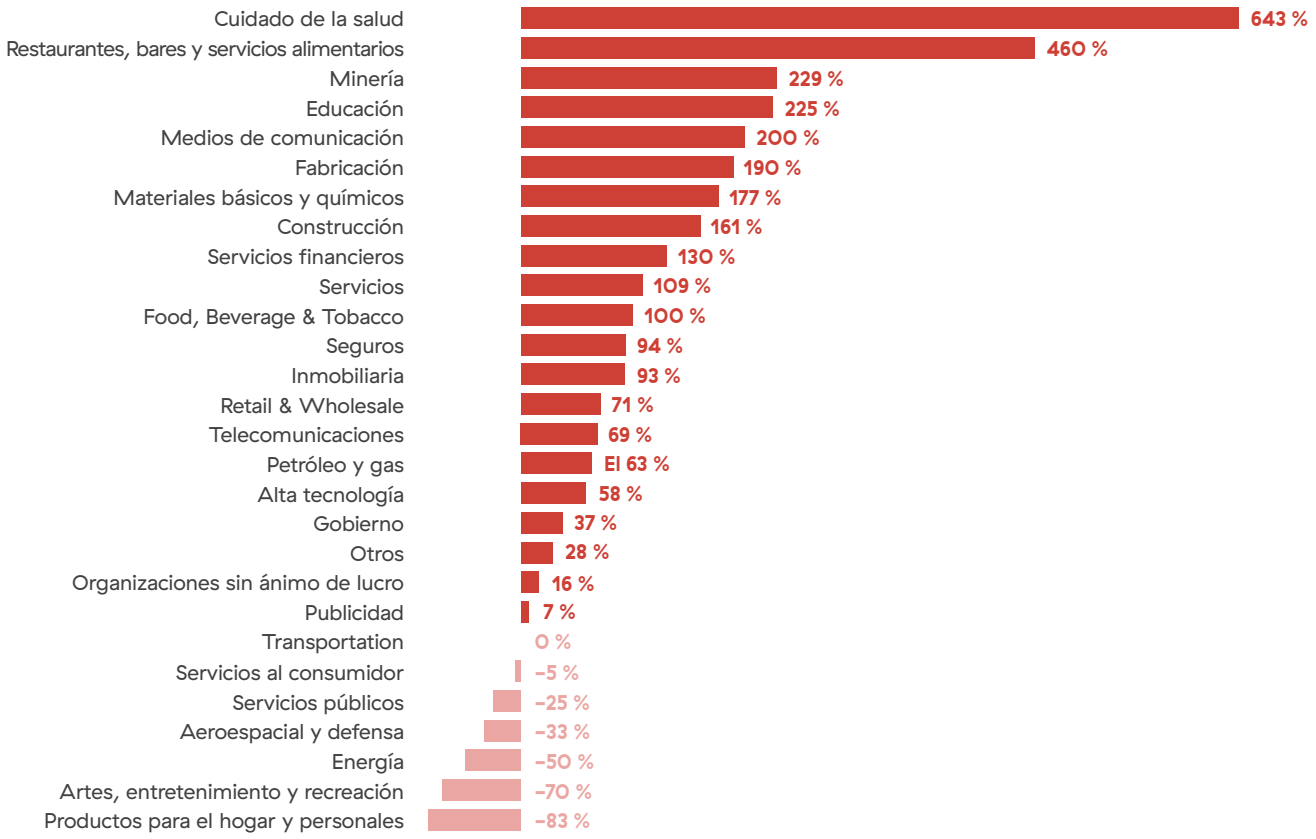


Figura 3: Porcentaje de cambio en los ataques de doble extorsión por sector

Principales familias de ransomware

Conti y LockBit fueron las familias de ransomware de doble extorsión más prevalentes en 2021, acompañadas por una serie de nuevos participantes que surgieron a lo largo del año.

La Figura 4 muestra cuándo surgieron por primera vez cada una de las familias de ransomware más activas de los últimos años y cuándo comenzaron a publicar datos en sitios con fugas o foros de piratería informática.

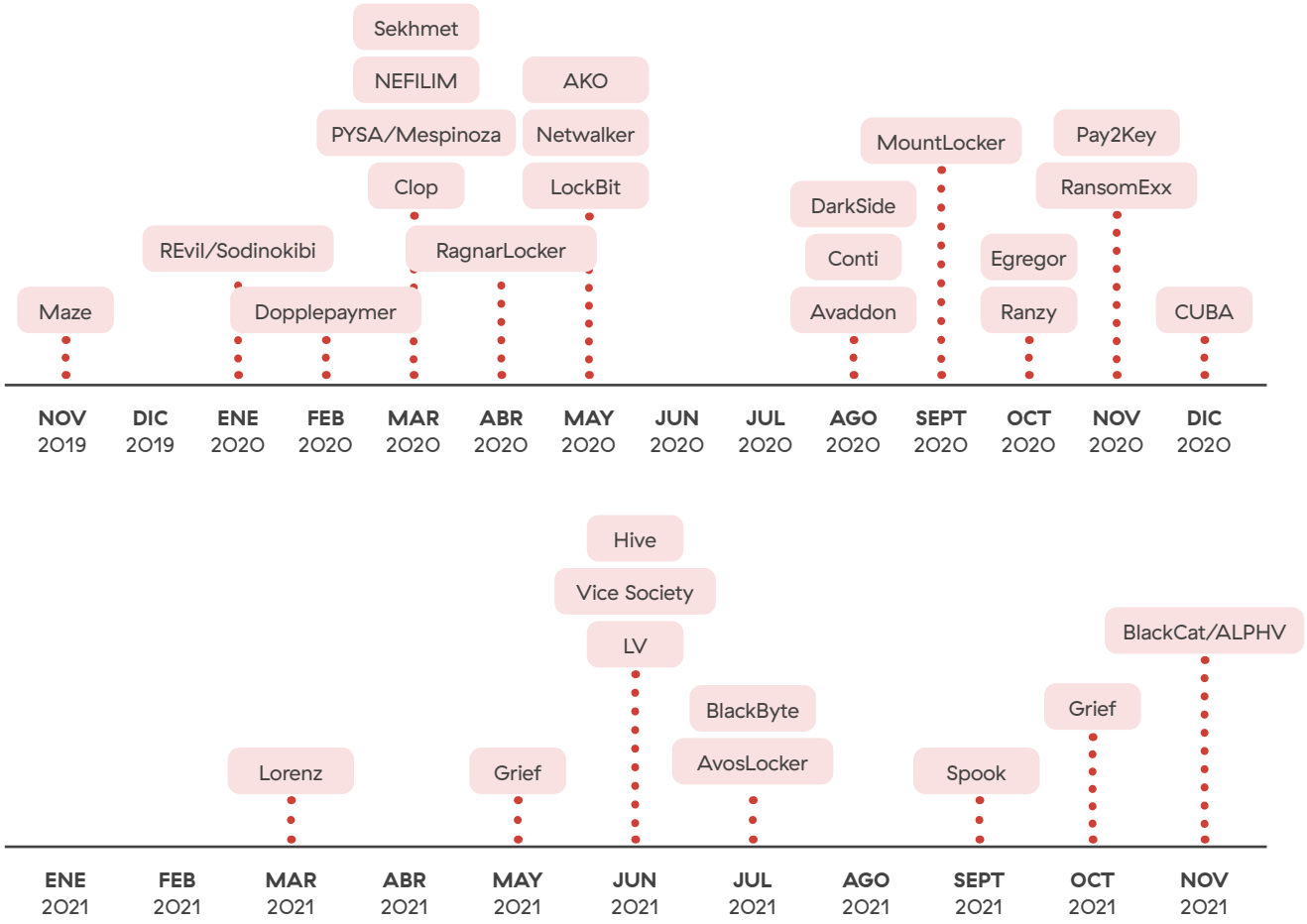


Fig. 4: Cronología de las familias de ransomware que publican datos en sitios de filtración de datos o foros de piratería informática

Muchas de las familias activas de ransomware en 2021—2022 son modelos de ransomware como servicio (RaaS), aumentando su distribución a través de redes afiliadas. En 2021, también vimos el cambio de marca de varias familias populares de ransomware, como el cambio de marca de DoppelPaymer como Grief, el cambio de marca de DarkSide como BlackMatter y el de Avaddon como Haron seguido de Midas (las dos últimas usando el creador de ransomware de Thanos).

Conti ha sido el grupo de ransomware más activo de los últimos dos años y el más costoso de todos los tiempos: el FBI estima que a partir de enero de 2022, había más de 1000 víctimas de ataques asociados con el ransomware Conti, con pagos totales que superaban los 150 millones de dólares (sin incluir daños relacionados ni costos de reparación). Entre las víctimas de Conti se encuentran diversas organizaciones de servicios críticos de los sectores financiero, informático, energético y gubernamental, como los servicios públicos de salud de Irlanda y el gobierno de Costa Rica En mayo de 2022, el Departamento de Estado de los EE. UU. ofreció una recompensa de 10 millones de dólares estadounidenses por información sobre los líderes del grupo.

LockBit, antes conocido como ransomware ABCD, tiende a atacar a pequeñas y medianas empresas, por lo que en su mayoría no llega a los titulares de noticias, con la excepción de su ataque a Accenture en agosto de 2021. LockBit es un RaaS muy utilizado que resulta atractivo para los atacantes debido a su velocidad y rendimiento.

La figura 5 muestra las familias de ransomware que afectaron al mayor número de organizaciones con ataques de doble extorsión entre febrero de 2021 y marzo de 2022, según la información de los sitios de filtración de datos.

Variación porcentual de los ataques de doble extorsión: 2021 frente a 2020

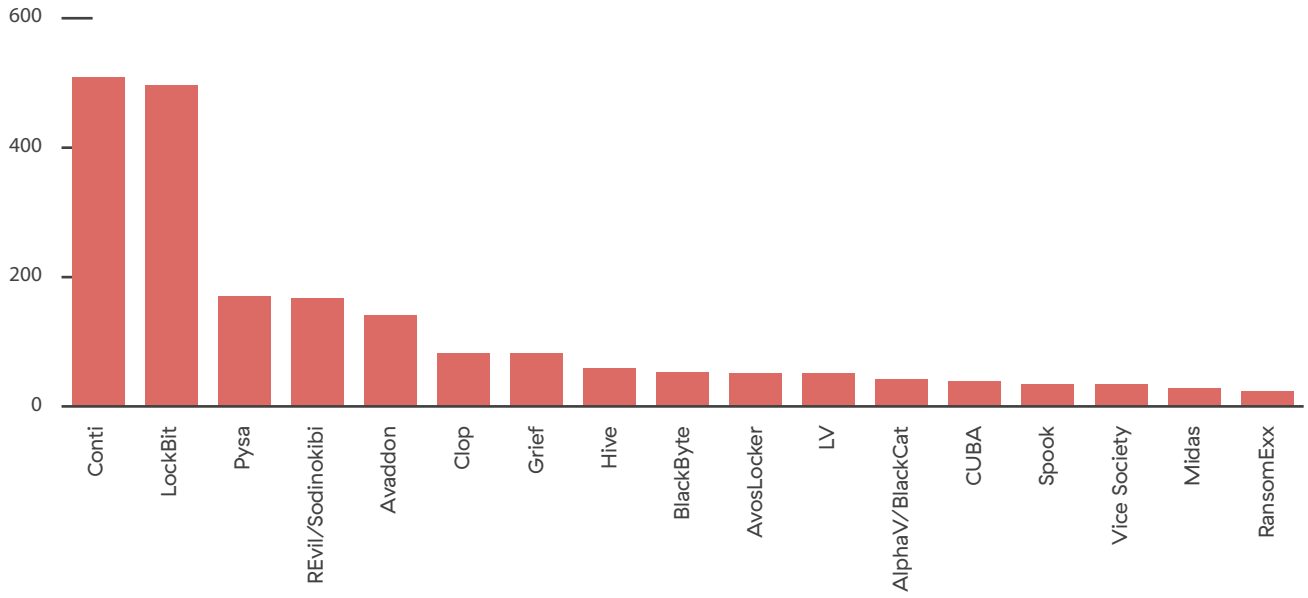


Figura 5: Ataques de ransomware por familia, febrero de 2021 – marzo de 2022

Previsiones para 2022—23

El ransomware como servicio seguirá aumentando

RaaS ha demostrado ser valioso para todas las partes implicadas. Los nuevos desarrolladores y afiliados de ransomware aumentarán el uso de este modelo para llevar a cabo ataques de rápida evolución contra organizaciones vulnerables.

Los cambios en los modelos de ransomware conducirán a cambios en los objetivos

Con creadores de ransomware e información organizativa disponibles a la venta en la web oscura, los atacantes tienen la ventaja de filtrar a través de los perfiles de las empresas para reducir sus objetivos ideales atendiendo a vulnerabilidades, ganancias y tipos de ransomware específicos. Como resultado, es de esperar que se produzca un cambio hacia objetivos más fáciles, incluidas pequeñas y medianas empresas con menos controles de seguridad y organizaciones con aplicaciones visibles en Internet que tienen vulnerabilidades conocidas junto con credenciales previamente suplantadas.

El tiempo de permanencia seguirá disminuyendo

Ahora que los autores de amenazas tienen un acceso fácil y barato a los perfiles de la empresa y a las credenciales vulneradas a la venta en la web oscura, los tiempos en los que los atacantes esperaban para atacar durante meses o incluso años, y luego se tomaban un tiempo antes de lanzar un ataque están llegando a su fin. Cada vez hay más informes públicos de atacantes de ransomware que reducen los tiempos de permanencia a solo días, indicando que los delincuentes son expertos en aumentar las técnicas de detección y son conscientes de que el tiempo es esencial para un ataque exitoso. Como resultado, los equipos de seguridad deben cerrar la brecha y acelerar la detección (a días, horas o solo minutos) para evitar las violaciones de los peores escenarios en 2022 y posteriormente.

Los ataques a la cadena de suministro aumentarán a medida que los adversarios pongan en peligro los ecosistemas de socios y proveedores

Las organizaciones más importantes del mundo suelen contar con la mejor seguridad, pero puede que no ocurra lo mismo con sus proveedores y socios, con acceso de terceros a redes, sistemas e información de apoyo. Lo vimos en el reciente ataque a Okta por parte del grupo de piratas Lapsus$, y en la amenaza de REvil a Apple a través de Quanta Computer, uno de los principales fabricantes de productos Apple. Estos grupos, y muchos otros, utilizaron ataques a la cadena de suministro para acceder a información confidencial a través del acceso de los proveedores sin tener que violar las medidas de seguridad reforzadas de sus objetivos finales.

El ransomware puede usarse como wiper o junto con él para destruir datos

A principios de 2022, los ataques publicitados a Ucrania presentaron múltiples tipos de ataques wiper, incluidos HermeticWiper junto con un ransomware señuelo conocido como PartyTicket. No es la primera vez que el ransomware se utiliza en ataques geopolíticos, ya que NotPetya y Bad Rabbit se implementaron en 2017 para atacar a organizaciones ucranianas. Las tensiones geopolíticas traen consigo la amenaza de ransomware enmascarado, wipers y otras tácticas que permiten a los autores de la amenaza un alto grado de anonimato y negación plausible.

Las vulnerabilidades anteriores (y otras nuevas) seguirán causando daños

Se descubrieron algunas vulnerabilidades importantes en el último año (por ejemplo, Log4j, PrintNightmare, ProxyShell/ProxyLogon) con las que las organizaciones tendrán que lidiar durante muchos años. Los atacantes seguirán buscando y explotando software y servidores obsoletos y no actualizados para traspasar los controles de seguridad.

Las familias de ransomware seguirán cambiando de marca

Vimos este ciclo a lo largo de 2021: un grupo de ransomware lanza un ataque importante, recibe atención y sanciones de las fuerzas del orden público, y posteriormente desaparece y se transforma más tarde bajo un nuevo nombre. Dado que el ransomware está colocado de lleno en el radar de las fuerzas del orden, este ciclo continuará a lo largo de 2022 y en el futuro

Las organizaciones necesitarán reforzar la seguridad más allá de la protección de los puntos finales

Los grupos de ransomware aumentarán el uso de tácticas para eludir los antivirus y otros controles de seguridad de los puntos finales. Las organizaciones tendrán una necesidad aún mayor de defensa en profundidad en lugar de confiar únicamente en la seguridad de los puntos finales para prevenir y detectar las intrusiones.

Los desarrolladores de ransomware le agregarán más ofuscación

Los autores de malware implementarán técnicas de ofuscación de malware para obstaculizar la ingeniería inversa y evitar la detección de firmas estáticas. La complejidad de la ofuscación de malware seguirá aumentando con técnicas avanzadas, incluyendo aplanamiento del flujo de control, ofuscación polimórfica de las cadenas y uso de paquetes virtuales basados en máquinas.

La filtración del código fuente del ransomware dará lugar a bifurcaciones

El año pasado se produjeron varias filtraciones del código fuente del ransomware, incluidas dos versiones de Conti y Babuk. Zscaler ThreatLabz ya ha observado que el código fuente de ambas familias de ransomware ha sido bifurcado por terceros y utilizado en ataques. La liberación del código fuente sin duda dará lugar a abusos por parte de otros grupos criminales que no tienen la experiencia para diseñar y construir su propio ransomware desde cero.

Orientación para la prevención

Tanto si se trata de un simple ataque de ransomware, un ataque de doble o triple extorsión, una familia de amenazas autónoma o un ataque RaaS ejecutado por una red de afiliados, la estrategia de defensa es la misma: emplear los principios de la confianzacero para limitar las vulnerabilidades, prevenir y detectar los ataques y limitar el radio de explosión de las violaciones exitosas. A continuación se presentan algunas recomendaciones de buenas prácticas para protegera su organización frente al ransomware:

1 Saque sus aplicaciones de Internet.

Los autores de ransomware comienzan sus ataques realizando un reconocimiento de su entorno, buscando vulnerabilidades que explotar y calibrando su enfoque. Cuantas más aplicaciones haya publicado en Internet, más fácil será de atacar. Utilice una arquitectura de confianza cero para asegurar las aplicaciones internas, haciéndolas invisibles a los atacantes.

2 Aplique una política de seguridad consistente para evitar la vulneración inicial.

Con un personal distribuido, es importante implementar una arquitectura de perímetro de servicio de seguridad (SSE) que pueda aplicar una política de seguridad consistente sin importar dónde trabajen sus usuarios (en la oficina o de forma remota).

3 Utilice sandboxing para detectar cargas útiles desconocidas.

La detección basada en firmas no es suficiente ante la rápida evolución de las variantes y cargas útiles del ransomware. Protéjase contra los ataques desconocidos y evasivos con un sandboxing en línea impulsado por IA, que analiza el comportamiento en lugar del empaquetadode un archivo.

4 Implemente una arquitectura de acceso a la red de confianza cero (ZTNA).

Implante una segmentación granular de usuario a aplicación y de aplicación a aplicación e intervenga en el acceso mediante controles dinámicos de acceso con privilegios mínimos para eliminar el movimiento lateral. Esto le permite minimizar los datos que se pueden cifrar o robar, lo que reduce el radio de explosión de un ataque.

5 Implemente la prevención de pérdida de datos en línea.

Evite la exfiltración de información confidencial con herramientas y políticas de prevención de pérdida de datos basadas en la confianza para frustrar las técnicas de doble extorsión

6 Mantenga actualizados los programas informáticos y haga que la capacitación sea constante.

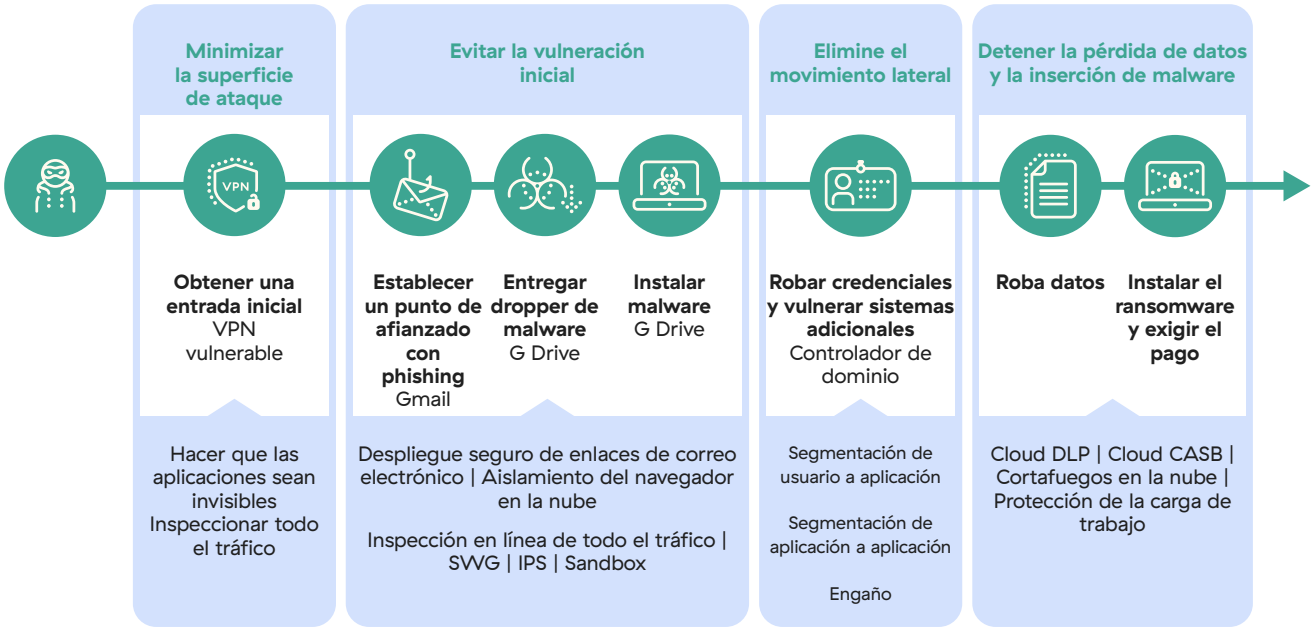
Aplique parches de seguridad en el software y lleve a cabo capacitaciones periódicas sobre concienciación sobre seguridad para reducir las vulnerabilidades que pueden explotar los ciberdelincuentes.

7 Tenga un plan de respuesta.

Prepárese para lo peor con un ciberseguro, un plan de copia de seguridad de datos y un plan de respuesta como parte de su programa general de continuidad de negocio y recuperación de desastres.

Para maximizar las posibilidades de defenderse frente al ransomware, debe adoptar defensas en capas que puedan interrumpir el ataque en cada etapa, desde el reconocimiento hasta el compromiso inicial, el movimiento lateral, el robo de datos y la ejecución del ransomware.

Detener el ransomware con confianza cero



Principales tendencias del ransomware

Ataques a la cadena de suministro

¿Qué es un ataque a la cadena de suministro?
Los ataques a la cadena de suministro (a veces denominados ataques a la cadena de valor o a terceros) son ataques contra los proveedores de una organización como medio para obtener acceso a ella. La mayoría de las grandes organizaciones cuentan con sofisticados controles de seguridad que dificultan la infiltración, por lo que los atacantes han encontrado una forma de entrar a través de los proveedores de estas organizaciones.

Los ataques a la cadena de suministro explotan la confianza que existe entre organizaciones legítimas en las operaciones comerciales normales. Los atacantes colocan una puerta trasera en un producto que saben que su objetivo utiliza, lo que permite al atacante infiltrarse en la red del objetivo sin ser detectado, normalmente entrando a través de parches automáticos o actualizaciones de software, llamadas actualizaciones "troyanizadas". Una vez dentro, los atacantes pueden espiar, robar datos, implantar otros programas maliciosos e interrumpir las operaciones.

Estos ataques implican un alto grado de planificación y sofisticación, y pueden tener un impacto devastador en las organizaciones que se encuentran dentro del radio de afectación del elemento comprometido originalmente.

Figura 6: Ataque a la cadena de suministro

Ransomware de ataque a la cadena de suministro Kaseya
El 2 de julio de 2021, la empresa de software de gestión de TI Kaseya reveló un incidente de seguridad que afectaba a su versión local del software Kaseya VSA, una plataforma que permite a los proveedores de servicios gestionados (MSP) realizar la gestión de parches, las copias de seguridad y la supervisión de clientes para sus clientes. Se cree que alrededor de 70 proveedores de servicios gestionados han sido víctimas de este ataque, llegando a afectar posteriormente a hasta 1500 pequeñas y medianas empresas.

El actor de la amenaza detrás de este ataque identificó y explotó una vulnerabilidad de día cero en el servidor VSA de Kaseya que le permitió enviar un script malicioso a todos los clientes administrados por ese servidor. El script se utilizó para entregar el ransomware REvil/Sodinokibi que cifró los archivos de los sistemas afectados.

Cadena de suministro de ordenadores Quanta
En abril de 2021, REvil atacó a Quanta Computer, el mayor fabricante de ordenadores portátiles del mundo y uno de los principales fabricantes de productos Apple. Quanta se negó a pagar un rescate de 50 millones de dólares, por lo que REvil se dirigió a Apple y a otros clientes de Quanta para pedir el rescate. REvil filtró 21 capturas de pantalla de esquemas de MacBook y amenazó con publicar más datos de Apple y otras empresas hasta que Apple o Quanta pagaran el rescate.

Ransomware de Log4j

En diciembre de 2021, Apache Software Foundation publicó un aviso de seguridad con respecto a una vulnerabilidad de ejecución de código remoto (CVE-2021-44228) en su popular biblioteca de registros Log4j. Esta vulnerabilidad permite a un atacante descargar y ejecutar una carga útil maliciosa enviando una solicitud especialmente diseñada al sistema vulnerable.

A continuación, el atacante puede controlar los mensajes de registro o los parámetros de mensajes de registro para ejecutar un código arbitrario cargado desde servidores LDAP cuando se habilita la sustitución de búsqueda de mensajes. Log4j se incorpora a muchos sitios web, aplicaciones y marcos populares, lo que hace que el impacto sea generalizado. se han producido varios ataques de ransomware explotando esta vulnerabilidad:

Ransomware NightSky
El 4 de enero de 2021, los atacantes explotaron la vulnerabilidad de Log4j en un sistema orientado a Internet que ejecuta VMware Horizon, e insertaron el ransomware NightSky.

Khonsari
Se han observado múltiples ataques que utilizan vulnerabilidades Log4j en sistemas Windows para implementar el ransomware Khonsari.

Conti
El grupo Conti también ha aprovechado la vulnerabilidad Log4j para ejecutar ataques de ransomware. AdvIntel descubrió el análisis grupal y el ataque a las versiones vulnerables de Log4j VMware vCenter, moviéndose lateralmente de las sesiones existentes de Cobalt Strike a las redes de víctimas estadounidenses y europeas.

Los atacantes de
TellYouThePass han aprovechado la vulnerabilidad de Log4j para implementar y ejecutar el ransomware TellYouThePass en sistemas Windows y Linux.

Ransomware como servicio

La web oscura se ha convertido en un lugar muy popular para que los grupos de amenazas vendan sus artículos a criminales potenciales. Hemos detallado el impacto de estos mercados para otros tipos de ataques, como el crecimiento del phishing como servicio en el informe sobre el estado del phishing de ThreatLabz de 2022.

RaaS se ha vuelto increíblemente popular y ahora promueve la mayor parte de los ataques de ransomware modernos. De hecho, 8 de las 11 principales familias de ransomware del año pasado utilizan ecosistemas RaaS.

El modelo RaaS requiere dos partes: operadores y afiliados. Los operadores son los grupos de amenazas que desarrollan el ransomware. Los afiliados seleccionan a sus víctimas, ejecutan el ransomware y establecen las demandas.

Los operadores reclutan afiliados y les proporcionan el ransomware y las herramientas necesarias para ejecutarlo, el acceso a un sitio de filtración de datos, la asistencia para negociaciones y otro soporte, a cambio de aproximadamente el 70—80 % de los beneficios de los ataques.

Este modelo es beneficioso para ambas partes. Los afiliados obtienen todo lo que necesitan para ejecutar ataques de ransomware altamente efectivos sin necesidad de realizar ningún desarrollo por sí mismos. Esto es atractivo tanto para los delincuentes calificados que ahorran tiempo y recursos de desarrollo como para los delincuentes con poca habilidad que de otra manera no podrían ejecutar tal ataque. Los operadores de ransomware pueden aumentar drásticamente la escala de sus operaciones y, en consecuencia, sus beneficios.

RaaS ha aumentado tanto el volumen como el daño de los ataques:

- **Aumento del volumen de ataques de ransomware:** más afiliados comienzan a ejecutar el ransomware, ya que ahora requiere menos tiempo y habilidad para desarrollarse.
- **Aumento del importe del rescate debido a la doble extorsión:** RaaS incluye un componente de doble extorsión en el que los autores de la amenaza roban datos y amenazan con publicarlos en un sitio de filtración de datos si no se paga el rescate. Esto aumenta el importe del rescate y la tasa de éxito del pago.

Ataques geopolíticos

Los líderes de seguridad de todo el mundo pendientes de un aumento en los ataques de ransomware como resultado del conflicto entre Rusia y Ucrania.

En marzo de 2022, el presidente estadounidense Joe Biden emitió una advertencia sobre el potencial de conducta cibernética maliciosa contra los Estados Unidos como respuesta a las sanciones económicas contra Rusia. Su declaración instó a tomar medidas inmediatas para reforzar las defensas cibernéticas tanto entre las organizaciones del sector público como privado.

8 de las 11 principales familias de ransomware de 2021 utilizan ecosistemas RaaS.

En el momento de la redacción de este informe, se han producido varios ataques de ransomware contra Ucrania y/o asociados con este conflicto:

1. **El ransomware PartyTicket:** este ransomware basado en Go ha sido utilizado junto con el malware HermeticWiper para atacar a organizaciones en Ucrania. PartyTicket es poco sofisticado y contiene un cifrado defectuoso que puede descifrarse y revertirse, lo que nos hace sospechar que fue desarrollado como señuelo para distraer de HermeticWiper.
2. **Ransomware Conti:** la Agencia de Seguridad de la Ciberseguridad e Infraestructura (CISA), la Oficina Federal de Investigación (FBI), la Agencia de Seguridad Nacional (NSA) y el Servicio Secreto de los Estados Unidos han vuelto a publicar un aviso sobre Conti, un grupo de ransomware vinculado a Rusia. Su asesor advierte que "los autores de amenazas cibernéticas Conti permanecen activos e informó que los ataques de ransomware de Conti contra organizaciones estadounidenses e internacionales han aumentado a más de 1000". A finales de febrero, Conti publicó dos declaraciones en su sitio de fugas, prometiendo el apoyo al gobierno ruso en respuesta a "el belicismo occidental y las amenazas estadounidenses de usar la guerra cibernética contra los ciudadanos de la Federación Rusa".

Medidas tomadas por las fuerzas del orden

Las fuerzas del orden de todo el mundo están prestando cada vez más atención a las familias de ransomware, especialmente a las que causan daños generalizados. Se han producido varias desmantelamientos exitosos de familias de ransomware de alto impacto en 2021 y a principios de 2022.

Desmantelamiento de REvil
REvil es una de las familias de ransomware más famosas de los últimos dos años, presente en las noticias después de importantes ataques contra Kaseya y JSB. Tras el ataque Kaseya, el FBI planificó una retirada de los servidores REvil. Sin embargo, nunca tuvieron oportunidad de llevarla a la práctica: poco después de este ataque crítico en julio de 2021, REvil cerró sus operaciones y los piratas informáticos desaparecieron. Esto resultó ser breve, ya que las operaciones de Kaseya se reiniciaron en septiembre de 2021.

En enero de 2022, el gobierno ruso aparentemente desmanteló el grupo de piratas informáticos REvil, arrestando a sus miembros a petición de los Estados Unidos. El Servicio de Seguridad Federal Rusa (FSB) buscó en 25 direcciones, deteniendo a 14 miembros del grupo de REvil, así como incautando 426 millones de rublos, 600 mil dólares estadounidenses, 500 mil euros, 20 coches de lujo y equipos informáticos. Sin embargo, REvil resurgió en abril de 2022, atacando a organizaciones con una versión actualizada de ransomware.

Desmantelamiento de DarkSide
El 6 de mayo de 2021, el grupo de ransomware DarkSide ejecutó un ataque de ransomware de alto perfil en Colonial Pipeline, el mayor oleoducto de los Estados Unidos. Las agencias federales tomaron medidas, y en las dos semanas posteriores al ataque, un actor de amenazas conocido como UNKN anunció que DarkSide había sido cerrado, ya que habían perdido el acceso a los servidores y sus criptomonedas habían sido transferidas a una cuenta desconocida. El Departamento de Justicia anunció que habían obtenido 63,7 bitcoins valorados en torno a 2,3 millones de dólares.

Desmantelamiento de Egregor
El grupo de ransomware Egregor (previamente conocido como Maze) fue desmantelado gracias a la cooperación de las fuerzas del orden el 9 de febrero de 2021. Agencias de Ucrania, Francia y Estados Unidos cerraron el sitio web de filtraciones de Egregor, detuvieron a los miembros del grupo e incautaron ordenadores relacionados con los ataques de ransomware. Egregor había extorsionado aproximadamente 80 millones de dólares a más de 150 empresas víctimas.

Cambio de marca del ransomware

Los operadores de ransomware llevan todo el año pasado redefiniendo su ransomware a ritmo acelerado. El cambio de marca se debe habitualmente a la atención no deseada de las fuerzas del orden público y de los medios de comunicación, así como a las sanciones que limitan las capacidades de los grupos para cobrar pagos por rescate.

DoppelPaymer cambió de nombre a Grief
A principios de mayo de 2021, la actividad del ransomware DoppelPaymer disminuyó considerablemente. Aunque el sitio de filtraciones de DoppelPaymer sigue en línea, no ha habido ninguna nueva publicación de víctimas desde el 6 de mayo de 2021. Además, no se ha actualizado ninguna publicación de víctimas desde finales de junio. Esta pausa es probablemente una reacción al ataque de ransomware a Colonial Pipeline que se produjo el 7 de mayo de 2021. Sin embargo, la aparente pausa se debe a que el grupo de amenazas que está detrás de DoppelPaymer cambió el nombre del ransomware por el de Grief. Ambas variantes del ransomware comparten el código del malware y los sitios de filtración son muy similares. El portal de rescate de Grief tiene algunas diferencias con el de DoppelPaymer. En particular, el método de pago de la petición de rescate se realiza en Monero (XMR) en lugar de bitcoin (BTC). Este cambio de criptodivisas puede responder a que el FBI recuperó parte del pago del rescate de Colonial Pipeline.

Darkside renombrado como BlackMatter
Tras el cierre de DarkSide en mayo de 2021, a finales de julio apareció una nueva familia de ransomware llamada BlackMatter. La rutina de cifrado utilizada en el ransomware y el texto del sitio de filtración de datos indicaban que BlackMatter era una nueva marca de DarkSide.

BlackMatter dejó de operar en noviembre de 2021. El grupo publicó un mensaje de operación cerrada en su portal de RaaS que decía: "Debido a ciertas circunstancias impredecibles asociadas con la presión de las autoridades (parte del equipo ya no está disponible, después de las últimas noticias), el proyecto está cerrado".

Cambio de marca del ransomware basado en Thanos
Anunciado en la web oscura como RaaS, el ransomware de Thanos se identificó por primera vez en febrero de 2020. Se filtró el constructor de Thanos y, en los dos años siguientes, se desarrolló una serie de nuevas variantes. La variante del ransomware de Prometheus surgió en febrero de 2021. En septiembre, se cambió el nombre de Prometheus a Spook. Ambos tienen notas de rescate y sitios de filtración de datos similares y contienen el identificador clave de firma de Thanos.

En julio de 2021, se descubrió otro ransomware derivado de Thanos denominado Haron. El ransomware de Haron tiene similitudes sorprendentes con el ransomware de Avaddon. Haron y Avaddon comparten similitudes en sus notas de rescate, sitios de negociación y sitios de filtración de datos. En octubre de 2021, se descubrió otra variante llamada Midas que es una versión con otro nombre del | ransomware Haron.

Los grupos de ransomware cambian el nombre de su marca para evitar sanciones y reducir la atención de las fuerzas del orden.

Cambio de marca de Evil Corp
La banda Evil Corp, también conocida como Indrik Spider, es conocida por una serie de actividades maliciosas. Crearon troyanos bancarios como Dridex, este último utilizado para distribuir su ransomware BitPaymer.

La Oficina de Control de Activos Extranjeros (OFAC) del Departamento del Tesoro de EE. UU. sancionó a los miembros de Evil Corp por los daños causados por su malware Dridex, alegando que infligieron más de 100 millones de dólares en daños a bancos e instituciones financieras de más de 40 países. Tras estas sanciones, las empresas de negociación de ransomware se negaron a facilitar el pago de rescates para Evil Corp por miedo a las multas o a las acciones legales del Departamento del Tesoro de Estados Unidos. Para eludir las sanciones, Evil Corp descubrió una sencilla laguna legal mediante el cambio de marca de su ransomware.

Evil Corp distribuyó el ransomware WastedLocker en junio de 2020, el ransomware Hades en diciembre de 2020 y el ransomware Phoenix en marzo de 2021. En mayo de 2021, siguieron cambiaron la marca de su ransomware a PayloadBin, haciéndose pasar por otro autor de amenazas que no estaba sujeto a las mismas sanciones.

Cambio de marca de Rook
El ransomware Rook fue detectado en noviembre de 2021, basado en el código fuente filtrado del ransomware Babuk. En diciembre de 2021, una variante de Rook recibió el nuevo nombre de Night Sky, que ha sido utilizado por el grupo de autores de amenazas con sede en China DEV-0401 para dirigirse a redes corporativas en ataques de ransomware de doble extorsión aprovechando la vulnerabilidad de Log4Shell. En enero de 2022, tanto Rook como Night Sky se cerraron, y surgió el ransomware Pandora. Basado en las similitudes de código, Pandora también es una versión con otra marca de Rook.

Principales vulnerabilidades utilizadas en ataques de ransomware

Vulnerabilidades ProxyLogon
Los ransomwares BlackKingdom y DearCry han combinado cuatro exploits de vulnerabilidad ProxyLogon diferentes para acceder a y cifrar las redes de sus víctimas. Esta táctica se ha utilizado para acceder a los servidores de Microsoft Exchange, robar correo electrónico e implementar otras puertas traseras. Las vulnerabilidades ProxyLogon incluyen CVE-2021-26855 (vulnerabilidad de falsificación de solicitud del lado del servidor [SSRF] en Exchange), CVE-2021-26857 (vulnerabilidad de deserialización insegura en el servicio de mensajería unificada), CVE-2021-26858 (vulnerabilidad de escritura arbitraria de archivos tras la autenticación en Exchange) y CVE-2021-27065 (vulnerabilidad de escritura arbitraria de archivos tras la autenticación en Exchange). Microsoft parcheó estas vulnerabilidades en marzo de 2021.

Una cadena de ataque típica que permite a un atacante ejecutar código remoto a través del puerto 443 expuesto: los atacantes utilizan la vulnerabilidad CVE-2021-26855 para eludir la autenticación de Microsoft Exchange y hacerse pasar por un usuario. El atacante envía una solicitud POST modificada para cualquier archivo en el directorio que es legible sin autenticación, donde el archivo en el directorio no es requerido. El atacante se autentifica en el panel de control de Exchange (ECP) y sobrescribe cualquier archivo en el sistema objetivo utilizando las vulnerabilidades CVE-2021-26858 o CVE-2021-27065. Después de estas vulnerabilidades, un atacante puede ejecutar código remoto mediante Web Shell en el servidor Exchange.

Vulnerabilidad de intercambio ProxyShell
El ransomware Conti explota la vulnerabilidad de Microsoft Exchange Server para entrar en la red de la víctima. Las vulnerabilidades de

intercambio de ProxyShell son una combinación de CVE-2021-34473 (vulnerabilidad de ejecución remota de código de Microsoft Exchange Server), CVE-2021-34523 (vulnerabilidad de elevación de privilegios de Microsoft Exchange Server) y CVE-2021-31207 (vulnerabilidad de elusión de funciones de seguridad de Microsoft Exchange Server). Microsoft ha parcheado estas vulnerabilidades entre abril y mayo de 2021, pero Conti sigue atacando a servidores sin parches para ejecutar código remoto. La cadena de infección de este ransomware puede verse en este informe, en el desglose de las bandas de ransomware BlackByte, AvosLocker y Hive. El ransomware LockFile también se dirige a estas vulnerabilidades para implementar el ransomware.

PrintNightmare
Los autores de ransomware aprovechan las vulnerabilidades de PrintNightmare para dirigirse a los sistemas Windows. Las vulnerabilidades de PrintNightmare son una combinación de CVE-2021-34527 y CVE-2021-34481, vulnerabilidades de ejecución de código remoto en el servicio de spooler de impresión de Windows que realiza incorrectamente operaciones de archivos privilegiados y permite a los atacantes ejecutar código remoto con privilegios SYSTEM.

La vulnerabilidad existe en la capacidad de punto e impresión en los sistemas Windows y permite a usuarios no privilegiados actualizar o instalar impresoras remotas. Microsoft publicó actualizaciones para PrintNightmare en julio y agosto de 2021 que abordan las vulnerabilidades.

En un ataque, un grupo de ransomware explotó las vulnerabilidades de PrintNightmare y lanzó el ransomware Vice Society. En otra campaña, los atacantes explotaron PrintNightmare y dejaron el ransomware Magniber.

SonicWall SMA 100
En enero de 2021, SonicWall confirmó una vulnerabilidad de inyección SQL en su producto Secure Mobile Access SMA 100 Series que permitía a los atacantes acceder a las credenciales y sesiones de inicio de sesión y vulnerar los dispositivos vulnerables mediante consultas no autenticadas y especialmente diseñadas. Fue parcheada por SonicWall en febrero de 2021.

Esto se descubrió después de que el grupo de amenazas UNC2447 usara este defecto para atacar una red objetivo e implementar el ransomware de doble extorsión FIVEHANDS en los sistemas de las víctimas. El autor de amenazas usó la vulnerabilidad de día cero para acceder y colocar la puerta trasera SOMBRAT junto con herramientas adicionales para obtener una posición, realizar un reconocimiento y exfiltrar datos, incluidas las balizas Cobalt Strike, Adfind, BloodHound, Mimikatz, PC Hunter y Rclone. Al final del ataque, UNC2447 eliminó y ejecutó el ransomware FIVEHANDS para cifrar los datos del sistema objetivo, y luego intentó extorsionar dinero bajo amenaza de publicar los datos en foros de hackers.

Dispositivo NAS de QNAP
Una nueva variante del ransomware eChOraix tenía como objetivo los dispositivos de almacenamiento en red (NAS) de Quality Network Appliance Provider (QNAP) y los dispositivos NAS de Synology. En la cadena de ataque, el atacante explotó la vulnerabilidad CVE-2021-28799 en los dispositivos NAS de QNAP. Se ha informado de una vulnerabilidad de autorización inadecuada en los dispositivos NAS de QNAP que ejecutan HBS 3 (sincronización de copia de seguridad híbrida) que permite al atacante iniciar sesión en un dispositivo de forma remota.

Las 11 familias de ransomware más importantes

A continuación se ofrece una visión general de 11 familias diferentes de ransomware y sus secuencias de ataque. Estas familias de ransomware fueron las causantes de la mayor cantidad de víctimas en 2021 y en 2022, y son la mejor representación del estado actual de ransomware frente al que su organización debe defenderse. Para cada familia, proporcionaremos un poco de historia, un resumen de sus tácticas (incluidos los mapeos de MITRE ATT&CK) y algunas estadísticas sobre sus industrias objetivo.

Conti

El ransomware Conti fue detectado por primera vez en febrero de 2020. En ocasiones, Conti se clasifica como RaaS, pero sus afiliados son esencialmente empleados, en lugar de afiliados que se registran, utilizan un portal para administrar la página y reciben una parte de los beneficios. Conti y Ryuk comparten un código similar, lo que indica que Conti es probablemente el sucesor del ransomware Ryuk. Conti ha sido el ransomware más frecuente en 2021.

Cadena de infección:
Conti ha utilizado una serie de mecanismos de acceso inicial en varias campañas:

1. Se ha distribuido a través de correos electrónicos de spam que contienen archivos adjuntos o enlaces maliciosos que descargan más TrickBot, IcedID, BazarLoader o Cobalt Strike para obtener un soporte en el sistema.
2. El acceso inicial también se realiza explotando vulnerabilidades conocidas como Log4j, ProxyShell o utilizando credenciales débiles de RDP (protocolo de escritorio remoto).

Después de vulnerar a su víctima, Conti utiliza Cobalt Strike, Mimikatz y otras herramientas posteriores a la explotación para robar credenciales y establecer una posición en la red. Se sabe que los autores de la amenaza Conti utilizan Metasploit, Netscan y otras herramientas de red team para obtener información de la red y del controlador de dominio. Después de reunir la información necesaria, los autores de la amenaza pueden utilizar AnyDesk, PsExec u otras utilidades remotas para el movimiento lateral. Los autores de la amenaza Conti exfiltran los datos utilizando Rclone u otras herramientas, y finalmente implementan y ejecutan el ransomware Conti para cifrar los datos, como se muestra en la Figura 7.

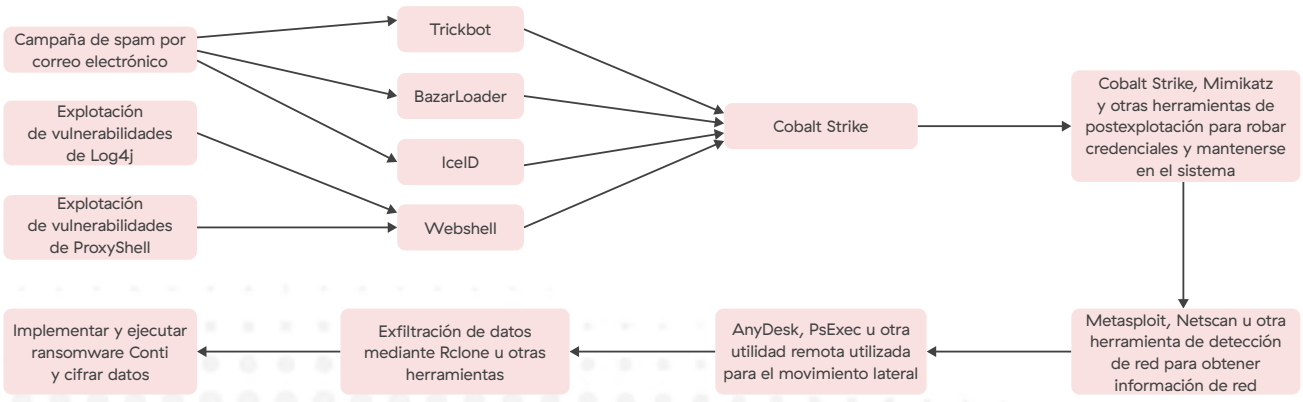


Figura 7: Anatomía de un ataque de ransomware Conti

La primera versión de Conti utilizó algoritmos RSA y AES en el proceso de cifrado. No obstante, AES fue sustituido posteriormente por el cifrado ChaCha.

A finales de enero de 2022, ThreatLabz identificó una versión actualizada del ransomware Conti como parte de nuestros esfuerzos de rastreo global de ransomware. Esta actualización se publicó antes de una filtración masiva de del código fuente y los registros de chat de Conti el 27 de febrero de 2022, publicada por un investigador ucraniano tras la invasión de Ucrania. La nueva versión de Conti añadió nuevos argumentos de línea de comandos que permiten a Conti reiniciar el sistema en el modo seguro de Windows con la red activada, y luego iniciar el cifrado. Al arrancar en modo seguro, Conti puede maximizar el número de archivos que se cifran, ya que es probable que no se estén ejecutando aplicaciones empresariales como las bases de datos. Conti también actualiza las extensiones de los archivos cifrados para incluir caracteres en mayúsculas y minúsculas y números. También resetea el fondo de escritorio de la víctima después del cifrado de los archivos.

La figura 8 muestra los sectores verticales de la industria a los que se dirigen los ataques de doble extorsión con Conti.

Infecciones de Conti por sector

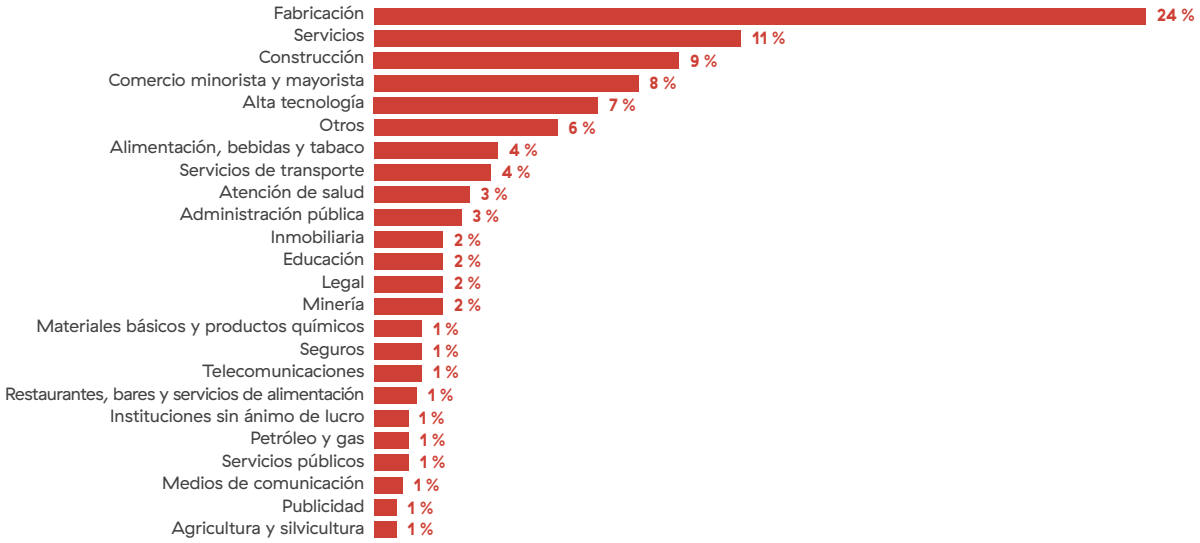


Figura 8: Infecciones de Conti por sector

Conti creó su propio sitio de filtración de datos en agosto de 2020. Si una organización no paga una demanda de rescate, Conti publicará sus datos robados.

Figura 9: Sitio de filtraciones de datos de Conti

Conti: Tácticas y técnicas de MITRE ATT&CK

Acceso inicial	Ejecución	Persistencia	Ampliación de privilegios	Evasión de defensa	Descubrimiento	Movimiento lateral	Recogida	Exfiltración	Impacto
Enlace de suplantación de identidad	Interfaz de línea de comandos	Ejecución de arranque o inicio de sesión automático	Manipulación de token de acceso	Desofuscar / descodificar archivos o información	Descubrimiento de la configuración de la red del sistema	Transferencia lateral de herramienta	Archivar datos recopilados	Exfiltración automatizada	Datos encriptados para el impacto
Ataque de phishing selectivo	Ejecución mediante carga de módulos		Explotación para ampliar privilegios	Inhabilitar las defensas	Detección remota del sistema	Servicios a distancia	Datos del sistema local	Exfiltración a través de un servicio web	Inhibir la recuperación del sistema
Explotar la aplicación orientada al público	Módulos compartidos			Inyección de procesos	Descubrimiento de archivos y directorios				Apagado/ reinicio del sistema
Cuentas válidas	Ejecución del usuario				Descubrimiento de software de seguridad				Desfiguración
Vulneración de la cadena de suministro					Registro de consultas				

LockBit

El ransomware LockBit surgió por primera vez en septiembre de 2019 como ransomware ABCD, nombre derivado de su extensión ".abcd". A principios de 2020 surgió una nueva versión que incorpora la extensión ".lockbit" a los archivos cifrados. En 2020, LockBit se unió al cartel de Maze y comenzó a publicar los datos de las víctimas en el sitio de filtración de datos de Maze. En septiembre de 2020, cuando Maze cerró sus operaciones, LockBit inició su propio sitio de filtración de datos, como se muestra en la figura 10.

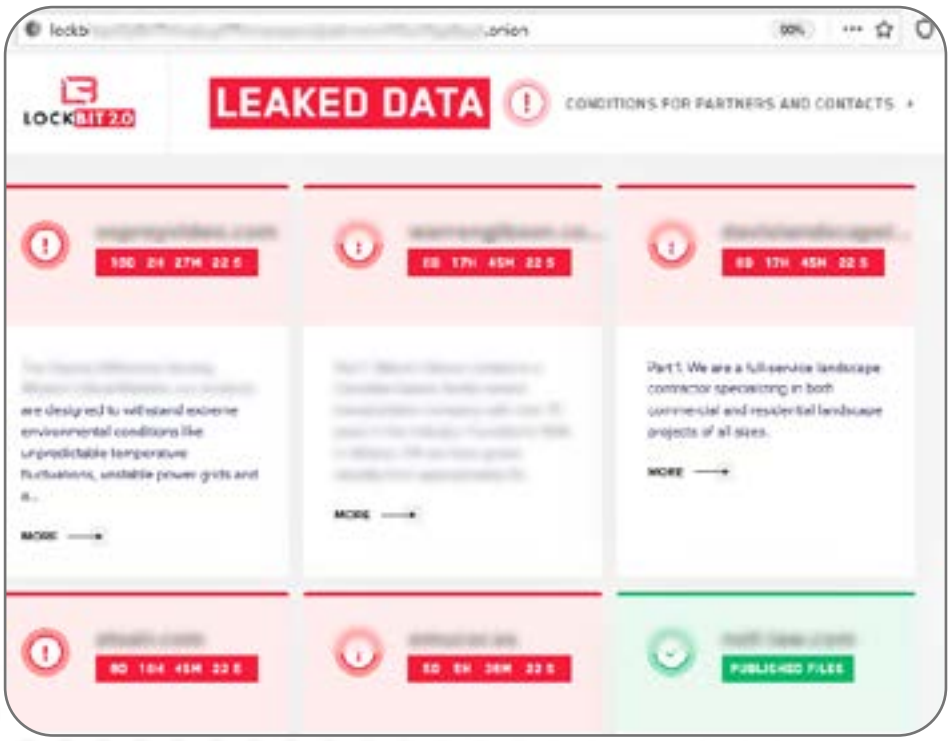


Figura 10: Sitio de filtración de datos de LockBit

En junio de 2021, LockBit lanzó una nueva versión llamada LockBit 2.0. En julio de 2021, LockBit 2.0 comenzó a publicar los datos de las empresas víctimas en su sitio de filtración de datos. Utiliza el modelo RaaS. LockBit se ha acercado a afiliados que hayan sido empleados de sus organizaciones objetivo y tengan acceso legítimo a la red. LockBit se ha distribuido a través de campañas de correo electrónico no deseado que contienen archivos adjuntos o enlaces maliciosos.

LockBit también ha obtenido acceso mediante la fuerza bruta de credenciales RDP o VPN, a través de cuentas RDP vulneradas y explotando la vulnerabilidad CVE–2018–13379 de Fortinet VPN.

Cadena de infección:
en el primer ataque LockBit 2.0 observado, el atacante utilizó una cuenta RDP pirateada para acceder al sistema objetivo. A continuación, utilizó un analizador de red para recuperar la información de red y localizar los controladores de dominio. El autor de la amenaza utilizó StealBit para exfiltrar los datos, Process Hacker y PC Hunter para terminar los procesos y servicios relacionados con la base de datos, y otras herramientas. Se utilizó un archivo por lotes para desinstalar productos de seguridad y desactivar los registros de eventos de Windows y las funciones de Windows Defender. Por último, LockBit utilizó las políticas de grupo de Windows para distribuir y ejecutar el ransomware LockBit 2.0.

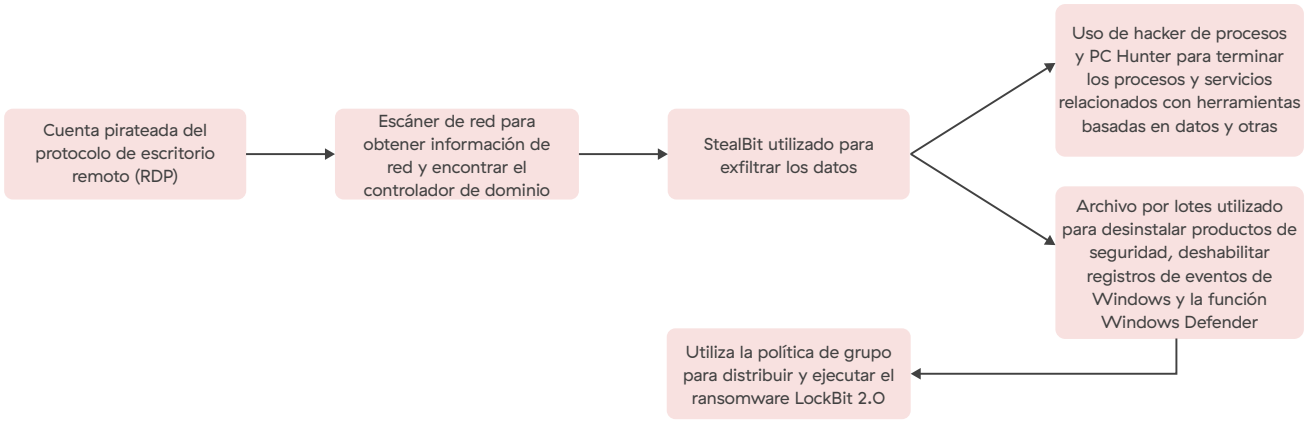


Figura 11: Anatomía de un ataque de ransomware LockBit

Parte de lo que hace que LockBit sea tan popular es su eficiencia: LockBit tiene el método de cifrado más rápido, ya que utiliza un enfoque de cifrado de múltiples hilos y cifra solo 4 KB de datos para cada archivo. Utiliza una combinación de algoritmos RSA y AES para cifrar archivos. LockBit lanzó una variante Linux y VMware ESXi en octubre de 2021. Dicha variante utiliza una combinación de los algoritmos Advanced Encryption Standard (AES) y de criptografía de curva elíptica (ECC) para el cifrado de datos.

La figura 12 muestra los sectores verticales de la industria a los que se dirigen los ataques de doble extorsión que utilizan LockBit.

Infecciones de Lockbit por sector

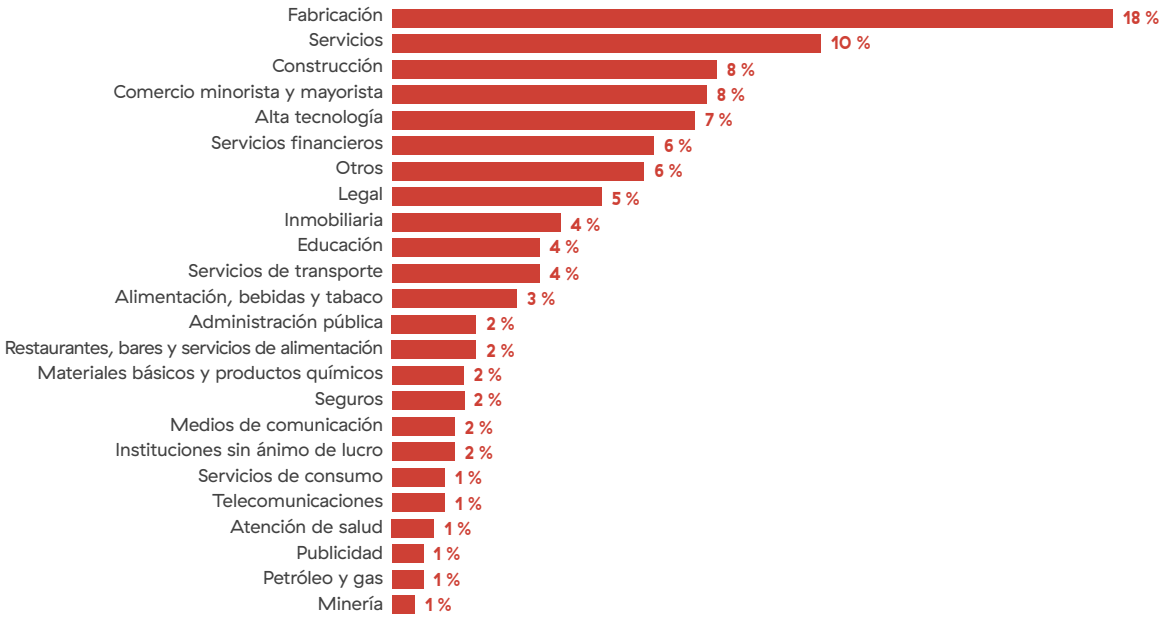


Figura 12: Infecciones de LockBit por sector

LockBit: Tácticas y técnicas de MITRE ATT&CK

Acceso inicial	Ejecución	Persistencia	Ampliación de privilegios	Evasión de defensa	Descubrimiento	Movimiento lateral	Recogida	Exfiltración	Impacto
Enlace de suplantación de identidad	Interfaz de línea de comandos	Ejecución de arranque o inicio de sesión automático	Abuso del mecanismo de control de elevación: omitir el control de la cuenta de usuario	Desofuscar / descodificar archivos o in-formación	Descubrimiento de la configuración de la red del sistema	Transferencia lateral de herramienta	Archivar datos recopilados	Exfiltración a través de un servicio web	Datos encriptados para el impacto
Ataque de phishing selectivo				Inhabilitar las defensas: desactivar o modificar herramientas	Detección remota delsistema	Servicios a distancia	Datos del sistema local		Inhibir la recuperación del sistema
Cuentas válidas				Eliminación del indicador en el host: borrar los registros de eventos de Wíndows	Descubrimiento de archivos y directorios				Desfiguración
Explotar la aplicación orientada al público				Modificación de la política de dominio: modificación de la política de grupo	Descubrimiento de software de seguridad				
Vulneración de la cadena de suministro									

PYSA/Mespinoza

El ransomware PYSA, también conocido como Mespinoza, fue detectado por primera vez en octubre de 2019. Ataca a una amplia gama de industrias en todo el mundo, pero es particularmente conocido por los ataques a "objetivos blandos", como la educación y los hospitales.

Cadena de infección
PYSA logra la vulneración inicial a través de correo electrónico de spam o credenciales RDP vulneradas. A continuación, los autores de la amenaza recopilan información de la red a través de herramientas de análisis como Port Scanner y Advanced IP Scanner desarrollado por Famatech Corp. Los atacantes utilizan herramientas de postexplotación como Mimikatz, PowerShell Empire, Koadic y PsExec para robar credenciales y moverse lateralmente. La herramienta WinSCP se ha utilizado para exfiltrar los datos de los sistemas de las víctimas. Un script de PowerShell deshabilita el software de seguridad y elimina las copias en la sombra y los puntos de restauración del sistema, impidiendo a las víctimas restaurar sus datos. Por último, el atacante implementa y ejecuta el ransomware PYSA y cifra los datos de la víctima.

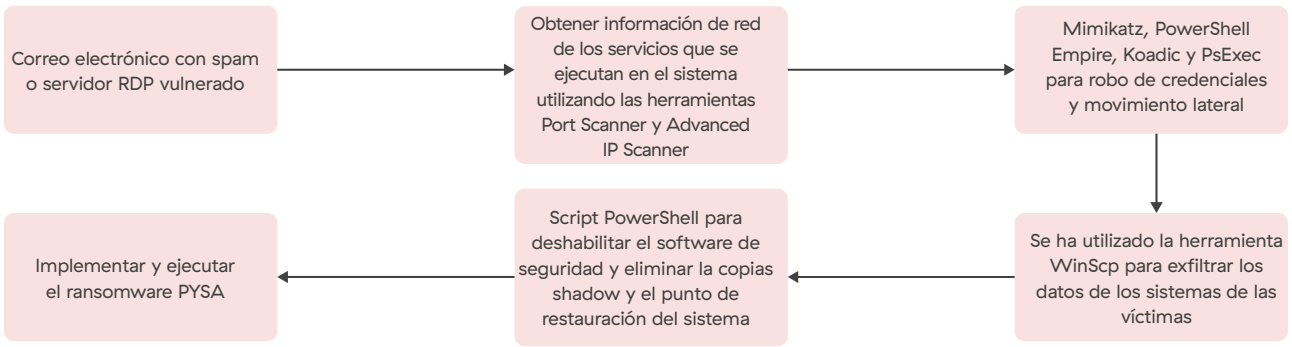


Figura 13: Anatomía de un ataque de ransomware PYSA

El 18 % de los ataques de PYSA estuvo dirigido a instituciones educativas.

PYSA utiliza una combinación de algoritmos RSA y AES-CBC para cifrar archivos.

La figura 14 muestra los sectores verticales a los que se dirigen los ataques de doble extorsión que utilizan PYSA/Mespinoza.

Infecciones de PYSA/Mespinoza por sector

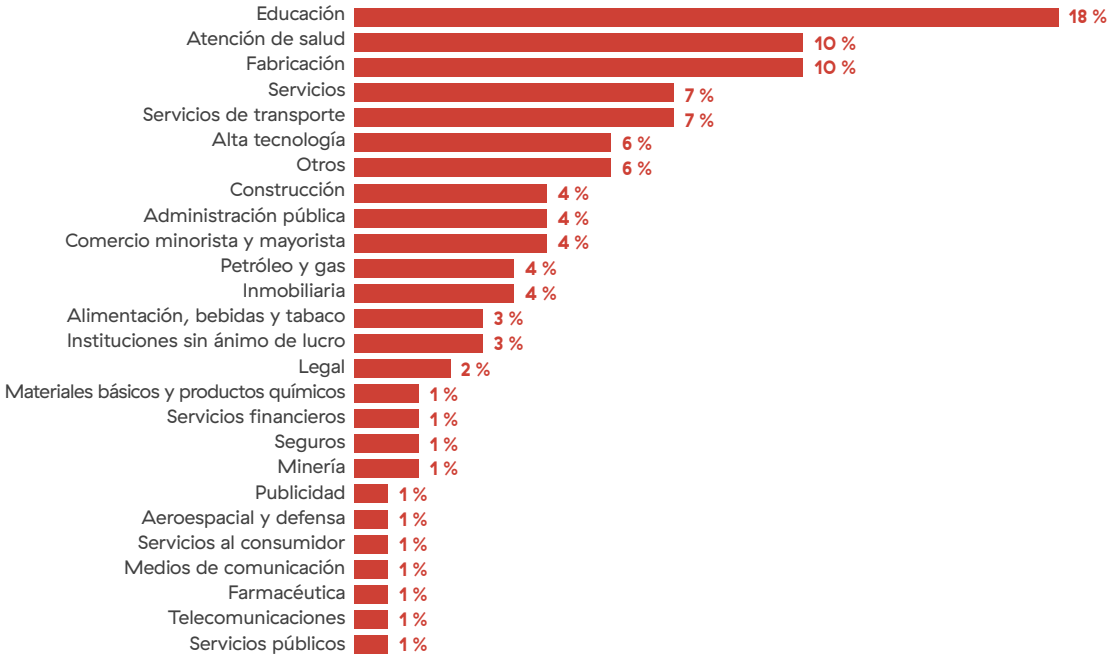


Figura 14: Ataques de PYSA/Mespinoza por sector

PYSA publica los datos robados en su sitio de filtraciones (como se muestra en la figura 15) si una víctima no paga un rescate.

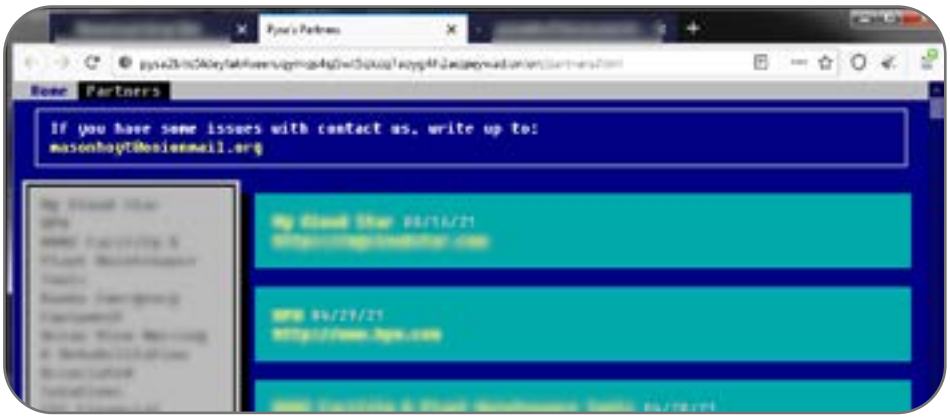


Figura 15: Sitio de filtración de datos de PYSA/Mespinoza

PYSA/Mespinoza: tácticas y técnicas de MITRE ATT&CK

Acceso inicial	Ejecución	Persistencia	Ampliación de privilegios	Evasión de defensa	Descubrimiento	Movimiento lateral	Recogida	Exfiltración	Impacto
Enlace de suplantación de identidad	Interfaz de línea de comandos	Ejecución de arranque o inicio de sesión automático	Manipulación de token de acceso	Desofuscar / descodificar archivos o información	Descubrimiento de la configuración de la red del sistema	Transferencia lateral de herramienta	Archivar datos recopilados	Exfiltración a través de un protocolo alternativo	Datos encriptados para el impacto
Ataque de phishing selectivo	Ejecución mediante carga de módulos	Tarea/trabajo programado		Inhabilitar las defensas	Detección remota del sistema		Datos del sistema local	Exfiltración a través de un servicio web	Inhibir la recuperación del sistema
Cuentas válidas	Ejecución del usuario			Modificación de la política de dominio: modificación de la política de grupo	Descubrimiento de archivos y directorios				
					Descubrimiento de software de seguridad				
					Registro de consultas				

REvil/Sodinokibi

El ransomware REvil (también conocido como Sodinokibi) apareció por primera vez en abril de 2019 y ha sido uno de los grupos de amenazas más activos en los últimos años. REvil también utiliza un ecosistema RaaS. REvil comenzó a usar la doble extorsión en enero de 2020, publicando por primera vez datos en un foro de piratería informática. En febrero de 2020, los atacantes de Sodinokibi lanzaron su propio sitio de filtración de datos como se muestra en la Figura 16.

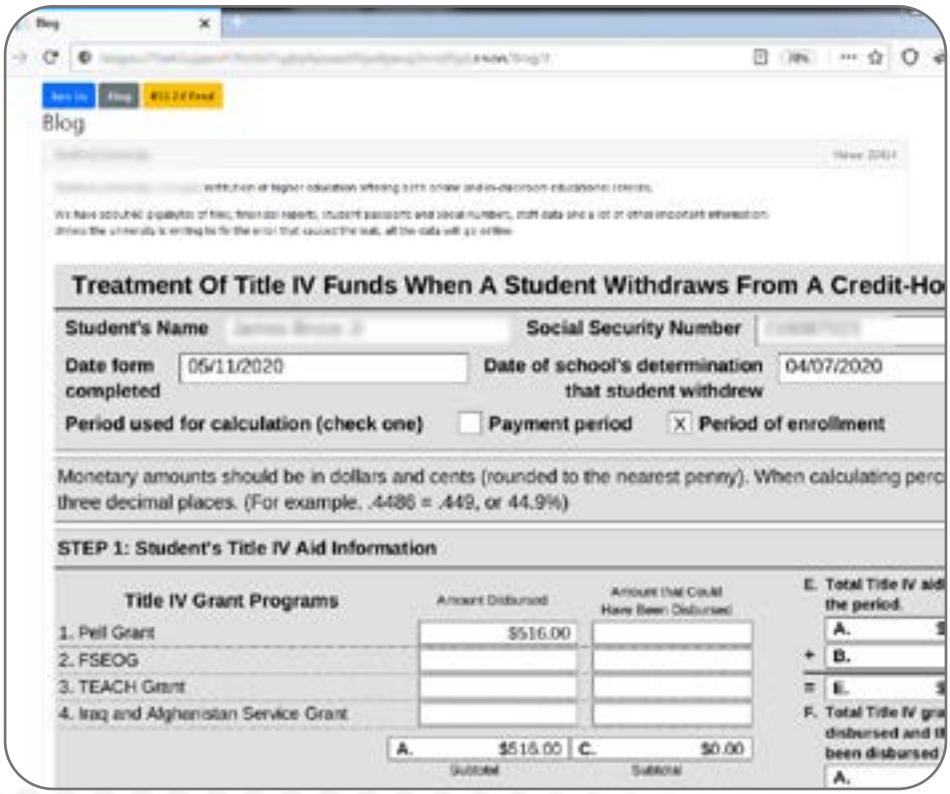


Figura 16: Sitio de filtración de datos de REvil/Sodinokibi

También experimentaron con la subasta de datos robados en su sitio de filtraciones hasta que observaron que no tenía éxito.

El grupo de amenazas REvil fue famoso por explotar una vulnerabilidad de día cero en el servidor VSA de Kaseya en julio de 2021. El servidor VSA de Kaseya vulnerado se utilizó para enviar un script malicioso a todos los clientes que eran administrados por ese servidor VSA.

Como se ha señalado anteriormente, los miembros de REvil fueron aparentemente detenidos por las fuerzas del orden rusas en enero de 2022. Sin embargo, el ransomware se actualizó y la infraestructura volvió a estar en línea en abril de 2022, momento en el que se reanudaron los ataques de REvil.

Cadena de infección

Los afiliados a REvil han utilizado una variedad de mecanismos de acceso inicial entre los que se incluyen correos electrónicos de spam, kits de explotación, cuentas RDP vulneradas y explotaciones de vulnerabilidad. Una campaña tipo comienza con un correo electrónico de spam con un archivo adjunto malicioso. Una vez abierto, el adjunto malicioso descarga un troyano como IcedID, que sirve de punto de apoyo para el movimiento lateral. Como se muestra en la figura 17, los afiliados a REvil utilizan una variedad de herramientas diferentes como Cobalt Strike, SharpSploit, Mimikatz y otras herramientas de postexplotación para robar credenciales. Además, los afiliados recopilan información de la red utilizando Netscan, BloodHound, AdFind y otras herramientas de descubrimiento de redes. Los atacantes se mueven lateralmente utilizando PsExec o acceso RDP. La exfiltración de datos se ha realizado utilizando FileZilla, Rclone, MEGAsync o FreeFileSync. Antes de implementar el ransomware, se sabe que los afiliados a REvil utilizan PC Hunter, Process Hacker, KillAV y/u otros scripts para terminar procesos y servicios relacionados con el software de seguridad. Finalmente, el autor de la amenaza implementa el ransomware REvil y cifra los datos.

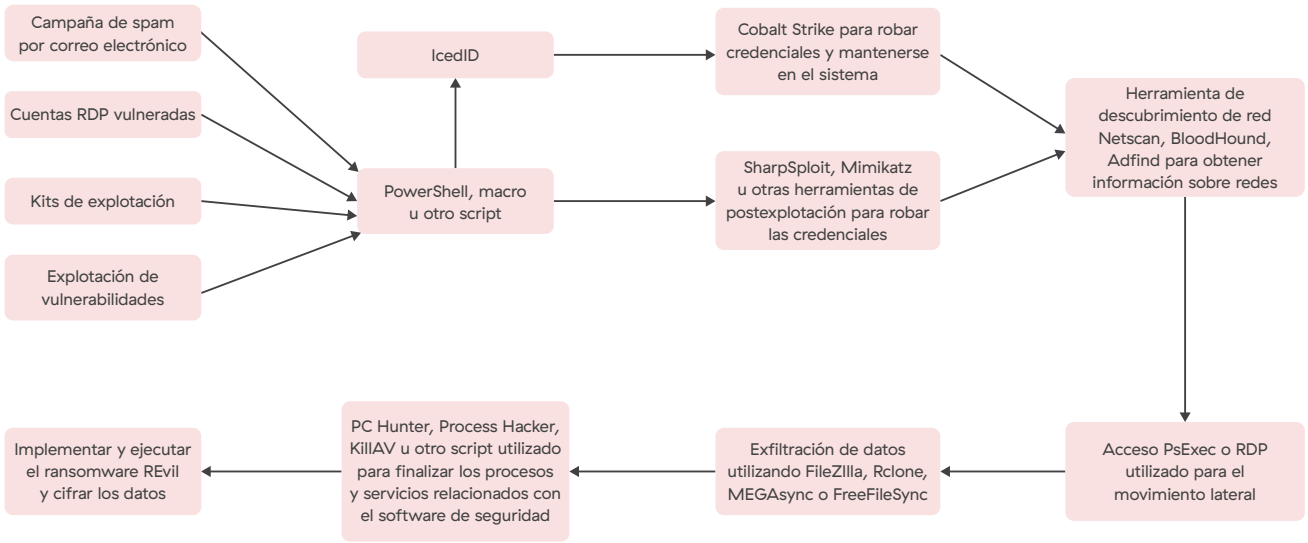


Figura 17: Cadena de ataque REvil/Sodinokibi

REvil utiliza criptografía de curva elíptica asimétrica, utilizando Curve25519 en combinación con Salsa20, para cifrar archivos.

La figura 18 muestra los sectores verticales a los que se dirigen los ataques de doble extorsión que utilizan REvil.

Infecciones de REvil/Sodinokibi por sector

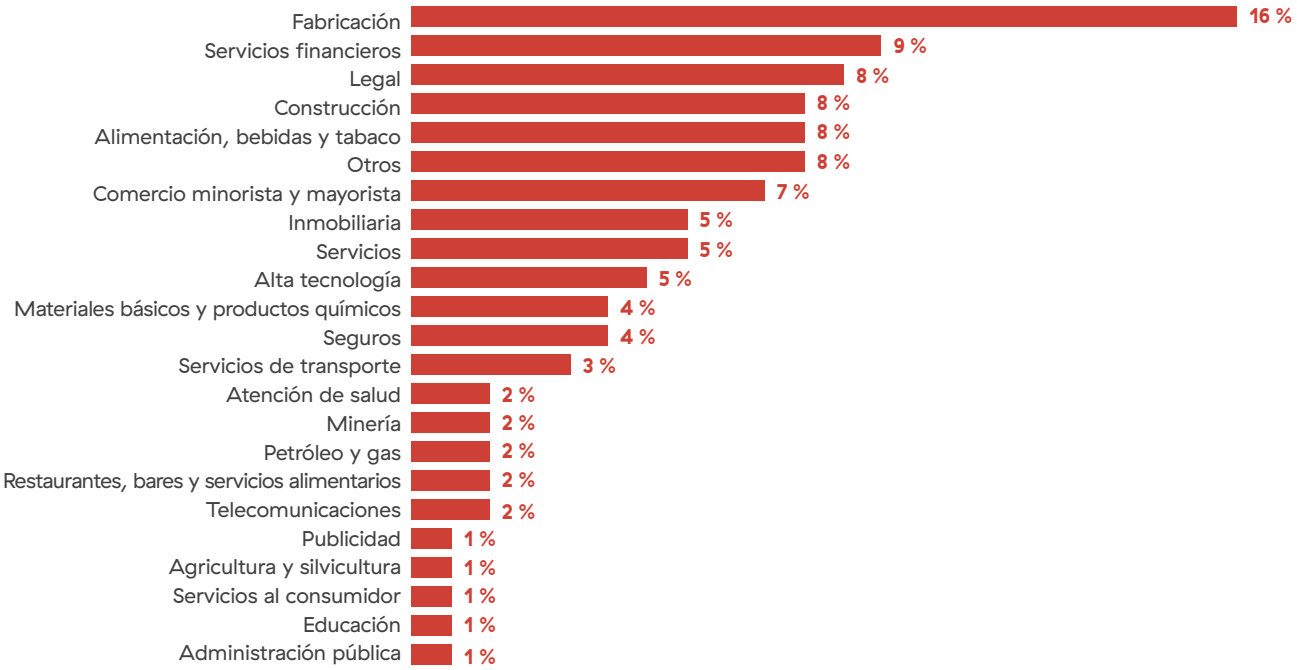


Figura 18: Infecciones por REvil/Sodinokibi por sector

REvil/Sodinokibi: tácticas y técnicas de MITRE ATT&CK

Acceso inicial	Ejecución	Persistencia	Ampliación de privilegios	Evasión de defensa	Descubrimiento	Movimiento lateral	Recogida	Exfiltración	Impacto
Enlace de suplantación de identidad	Interfaz de línea de comandos	Ejecución de arranque o inicio de sesión automático	Manipulación de token de acceso	Desofuscar / descodificar archivos o información	Descubrimiento de la configuración de la red del sistema	Transferencia lateral de herramienta	Archivar datos recopilados	Exfiltración automatizada	Datos encriptados para el impacto
Ataque de phishing selectivo	Ejecución mediante carga de módulos	Apropiación del flujo de ejecución	Apropiación del flujo de ejecución	Inhabilitar las defensas	Detección remota del sistema	Servicios a distancia	Datos del sistema local	Exfiltración a través de un servicio web	Inhibir la recuperación del sistema
Explotar la aplicación orientada al público	Módulos compartidos		Explotación para ampliar privilegios		Descubrimiento de archivos y directorios				Apagado/ reinicio del sistema
Compromiso de acom- pañamiento	Ejecución del usuario				Descubrimiento de software de seguridad				Desfiguración
Cuentas válidas					Registro de consultas				
Vulneración de la cadena de suministro									

Avaddon

El ransomware Avaddon fue detectado por primera vez en junio de 2020 y fue muy activo en ese momento. Avaddon fue otra familia de ransomware que utilizó el ecosistema RaaS. En enero de 2021, Avaddon añadió DDoS a su operación como triple táctica de extorsión. Avaddon lanza ataques DDoS tanto en el sitio web como en la red de la víctima para incentivar a la víctima a negociar con sus operadores y forzar cantidades de rescate más elevadas.

Cadena de infección
Avaddon obtuvo acceso a través de diferentes afiliados que utilizaron diferentes vectores para la vulneración inicial. Avaddon se distribuyó más ampliamente en campañas de spam y kits de explotación, pero algunos afiliados utilizaron ataques de fuerza bruta o vulneraron credenciales RDP y VPN para obtener acceso a las redes.

Como ejemplo de cadena de ataque, Avaddon obtenía acceso a un intermediador inicial que era infectado en un primer momento a través de credenciales vulneradas y utilizaba malware personalizado, como BlackCrow y DarkRaven web shells, para afianzarse en el sistema objetivo. Avaddon utilizó SystemBC para acceder a los hosts comprometidos y posteriormente Mimikatz y SharpDump para robar las credenciales. El autor de la amenaza realizó un análisis de la red después de la explotación utilizando SoftPerfect Network Scanner, PowerSploit y Empire. Para el movimiento lateral, los afiliados de Avaddon utilizaron RDP y Tareas Programadas de Windows para la persistencia. Antes de soltar la carga útil principal del ransomware, los autores de la amenaza exfiltraron datos utilizando MEGAsync y cerraron procesos y servicios relacionados con el software de seguridad. Por último, el autor de la amenaza lanzó y ejecutó la carga útil Avaddon y cifró los sistemas objetivo.

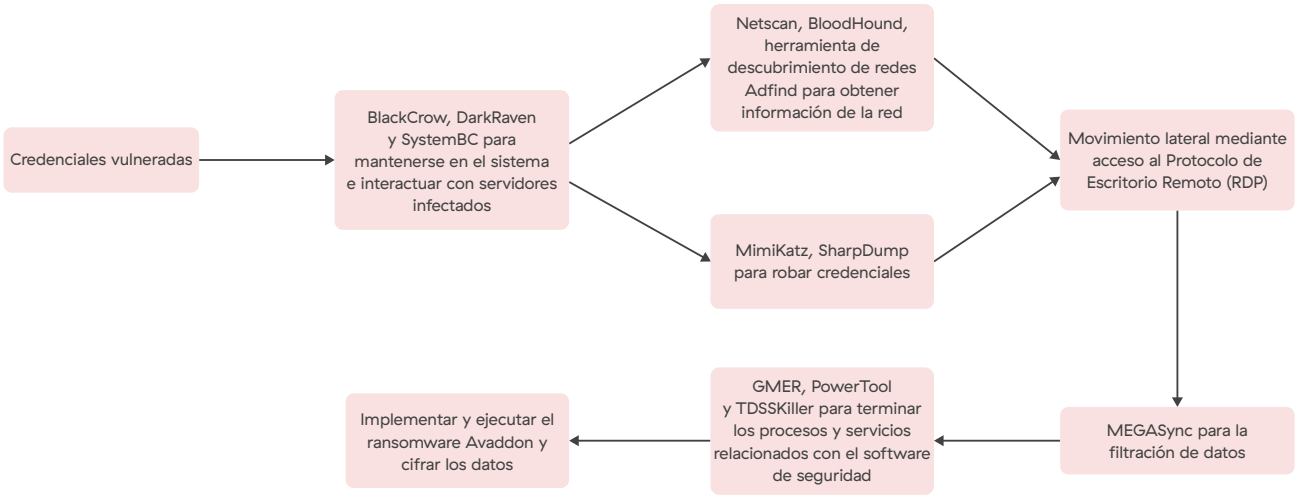


Figura 19. Anatomía de un ataque de ransomware de Avaddon

Avaddon utilizaba una combinación de algoritmos RSA y AES para cifrar los archivos. En febrero, un investigador publicó un descifrador gratuito tras descubrir un fallo, que Avaddon corrigió posteriormente. En junio de 2021, Avaddon cerró sus operaciones y liberó las claves de descifrado de las víctimas, lo que permitió a Emsisoft crear un descifrador para el ransomware Avaddon.

Al igual que las otras familias de ransomware mencionadas anteriormente, Avaddon siguió la tendencia de crear sitios web de filtración de datos, lanzando el suyo propio en agosto de 2020, como se muestra en la figura 20.

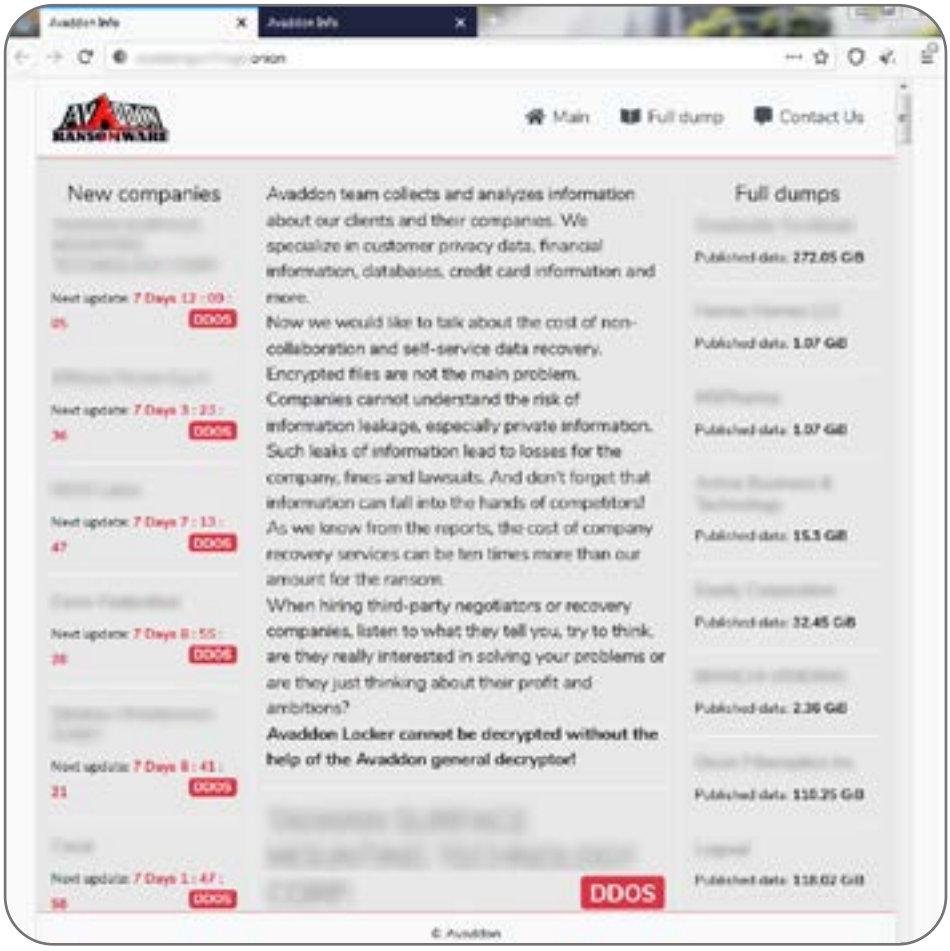


Figura 20: Sitio de filtración de datos de Avaddon

Después de que Avaddon se cerrara en junio de 2021, el grupo de amenazas relanzó los ataques utilizando el creador de ransomware de Thanos. El grupo de amenazas cambió la marca de Avaddon a Haron y, en octubre de 2021, cambió la marca del ransomware de nuevo al nombre de Midas.

La figura 21 muestra los sectores verticales a los que se dirigen los ataques de doble extorsión que utilizan Avaddon.

Infecciones de Avaddon por sector

Figura 21: Infecciones de Avaddon por sector

Avaddon: tácticas y técnicas de MITRE ATT&CK

Acceso inicial	Ejecución	Persistencia	Ampliación de privilegios	Evasión de defensa	Descubrimiento	Movimiento lateral	Recogida	Exfiltración	Impacto
Enlace de suplantación de identidad	Interfaz de línea de comandos	Ejecución de arranque o inicio de sesión automático	Cuentas válidas	Desofuscar / descodificar archivos o información	Descubrimiento de la configuración de la red del sistema	Transferencia lateral de herramienta	Archivar datos recopilados	Exfiltración a través de un protocolo alternativo	Datos encriptados para el impacto
Ataque de phishing selectivo	Tarea/ trabajo programado	Cuentas válidas		Inhabilitar las defensas	Detección remota del sistema	Servicios remotos: protocolo de escritorio remoto	Datos del sistema local		Inhibir la recuperación del sistema
Explotar la aplicación orientada al público	Ejecución del usuario			Inyección de procesos	Descubrimiento de archivos y directorios				
Compromiso de acom– pañamiento				Eliminación del indicador en el host	Descubrimiento de software de seguridad				
Cuentas válidas				Eliminación del indicador en el host	Descubrimiento de software de seguridad				

Clop

El ransomware Clop se detectó por primera vez en febrero de 2019. En marzo de 2020, Clop comenzó a utilizar la doble extorsión, filtrando datos robados de organizaciones vulneradas que no pagaban rescates a sus sitios de filtración de datos, como se muestra en la figura 22.

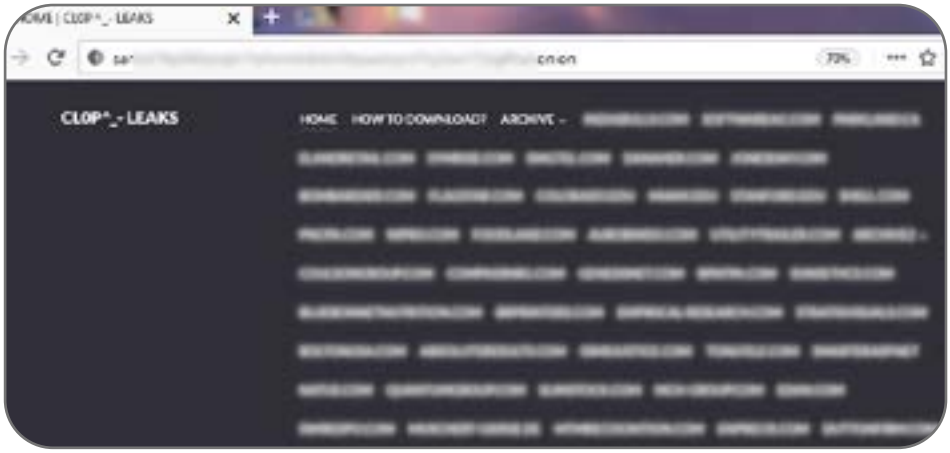


Figura 22: Cierre del sitio de filtraciones de datos

El grupo Clop centra sus esfuerzos sobre todo en las grandes organizaciones. ThreatLabz ha observado que el grupo de ransomware Clop exige rescates de decenas de millones e incluso rechaza ofertas de pago de rescate multimillonario.

El ransomware Clop fue implementado inicialmente por los grupos de amenazas TA505 y FIN11. Clop se ha distribuido ampliamente en campañas de spam llevadas a cabo por el actor de amenazas TA505. ThreatLabz ha observado varios ataques a Clop que explotan la vulnerabilidad SolarWinds Serv-U CVE-2021-35211, que permite la ejecución remota de código con privilegios elevados, para el acceso inicial. El grupo de amenazas FIN11 ha explotado múltiples vulnerabilidades en el Accellion File Transfer Appliance (FTA) rastreadas como CVE-2021-27101, CVE-2021-27102, CVE-2021-27103 y CVE-2021-27104. A continuación, FIN11 deja el shell web DEWMODE, que exfiltra los datos antes de depositar y ejecutar el ransomware Clop.

Clop causa ataques de alto perfil, con un valor estimado de 500 millones de dólares en daños a fecha de noviembre de 2021.

Cadena de infección

Un ejemplo de ataque de TA505 logró la vulneración a través de un correo electrónico de spam que contenía un archivo adjunto HTML. El adjunto redirigía a un archivo de documento XLS que además depositaba el cargador Get2. El cargador descargó otras cargas útiles como SdBot, FlawedAmmy, FlawedGrace y Cobalt Strike. Después de conseguir un punto de apoyo en la red y robar y exfiltrar datos, el grupo de amenazas implementó y ejecutó el ransomware Clop, como se ilustra en la figura 23.

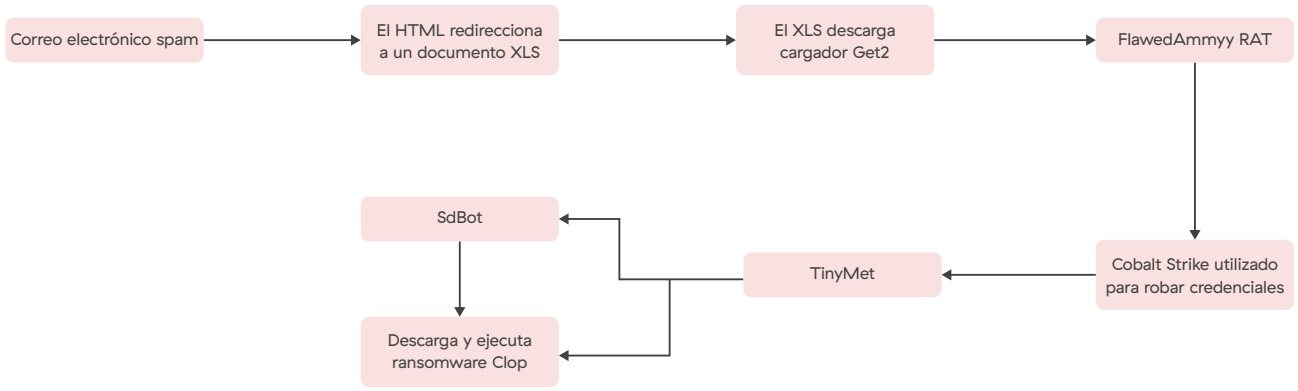


Figura 23: Anatomía de un ataque de ransomware Clop

Clop utiliza una combinación de algoritmos RSA y AES para cifrar archivos.

La figura 24 muestra los sectores verticales de la industria a los que se dirigen los ataques de doble extorsión con Clop.

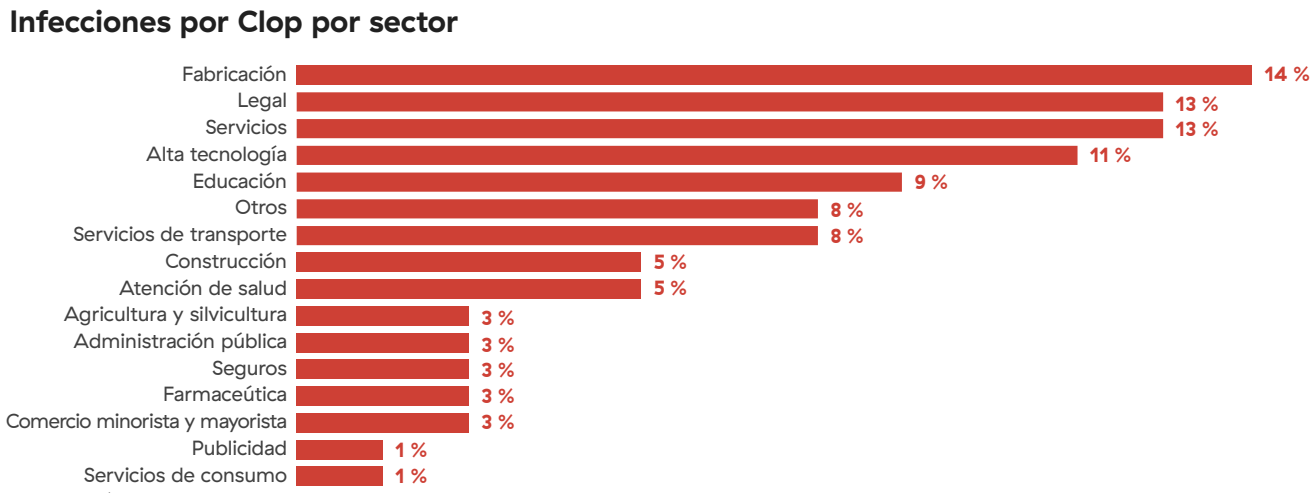


Figura 24: Infecciones por Clop por sector

Clop: tácticas y técnicas de MITRE ATT&CK

Acceso inicial	Ejecución	Persistencia	Ampliación de privilegios	Evasión de defensa	Descubrimiento	Movimiento lateral	Exfiltración	Impacto
Cuentas válidas	Interfaz de línea de comandos	Ejecución de arranque o inicio de sesión automático	Manipulación de token de acceso	Enmascaramiento: firma de código no válida	Descubrimiento de la configuración de la red del sistema	Transferencia lateral de herramienta	Exfiltración automatizada	Datos encriptados para el impacto
Ataque de phishing selectivo	Ejecución del usuario	Crear o modificar el proceso del sistema: servicio de Windows	Evitar el control de cuentas de usuario	Inhabilitar las defensas: desactivar o modificar herramientas	Detección remota del sistema	Servicios a distancia	Exfiltración a través de un servicio web	Inhibir la recuperación del sistema
Explotar la aplicación orientada al público	API nativa		Explotación para ampliar privilegios	Desofuscar / descodificar archivos o información	Descubrimiento de archivos y directorios			
Vulneración de la cadena de suministro				Inyección de proceso: inyección de DLL	Registro de consultas			
				Ejecución indirecta de comandos	Descubrimiento de software de seguridad			

Grief

El ransomware Grief es una nueva denominación de la marca DoppelPaymer, cuya actividad disminuyó significativamente en mayo de 2021 tras el ataque de Colonial Pipeline. El ransomware Grief tiene muchas similitudes con DoppelPaymer, incluido el código compartido del ransomware y los sitios web de filtración de datos. En la figura 25 se muestra una captura de pantalla de ejemplo del sitio de filtración de Grief.

Figura 25: Sitio de filtración de datos de Grief

El portal de rescate de Grief muestra algunas diferencias con respecto al portal DoppelPaymer. En particular, el método de pago de la demanda de rescate se realiza en Monero en lugar de bitcoin. Este cambio de criptomoneda puede ser en respuesta a la recuperación por parte del FBI de parte del pago del rescate de Colonial Pipeline, que se realizó en bitcoin.

Cadena de infección

El ransomware Grief se ha implementado en sistemas previamente infectados con Dridex, que el atacante utiliza antes de usar Cobalt Strike y de implementar y ejecutar la carga útil del ransomware Grief. Grief utiliza una combinación de algoritmos RSA de 2048 bits y AES de 256 bits para cifrar archivos.

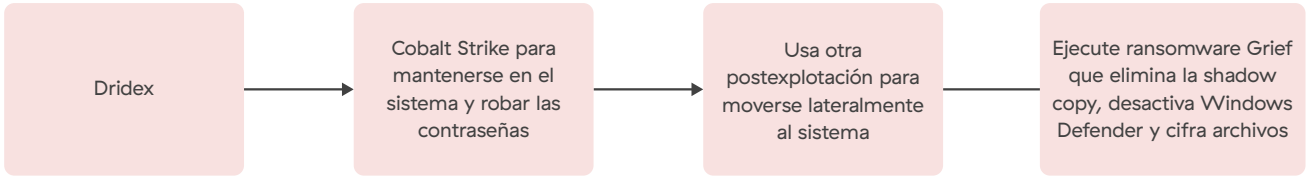


Figura 26: Anatomía de un ataque de ransomware Grief

La figura 27 muestra los sectores verticales a los que se dirigen los ataques de doble extorsión con Grief.

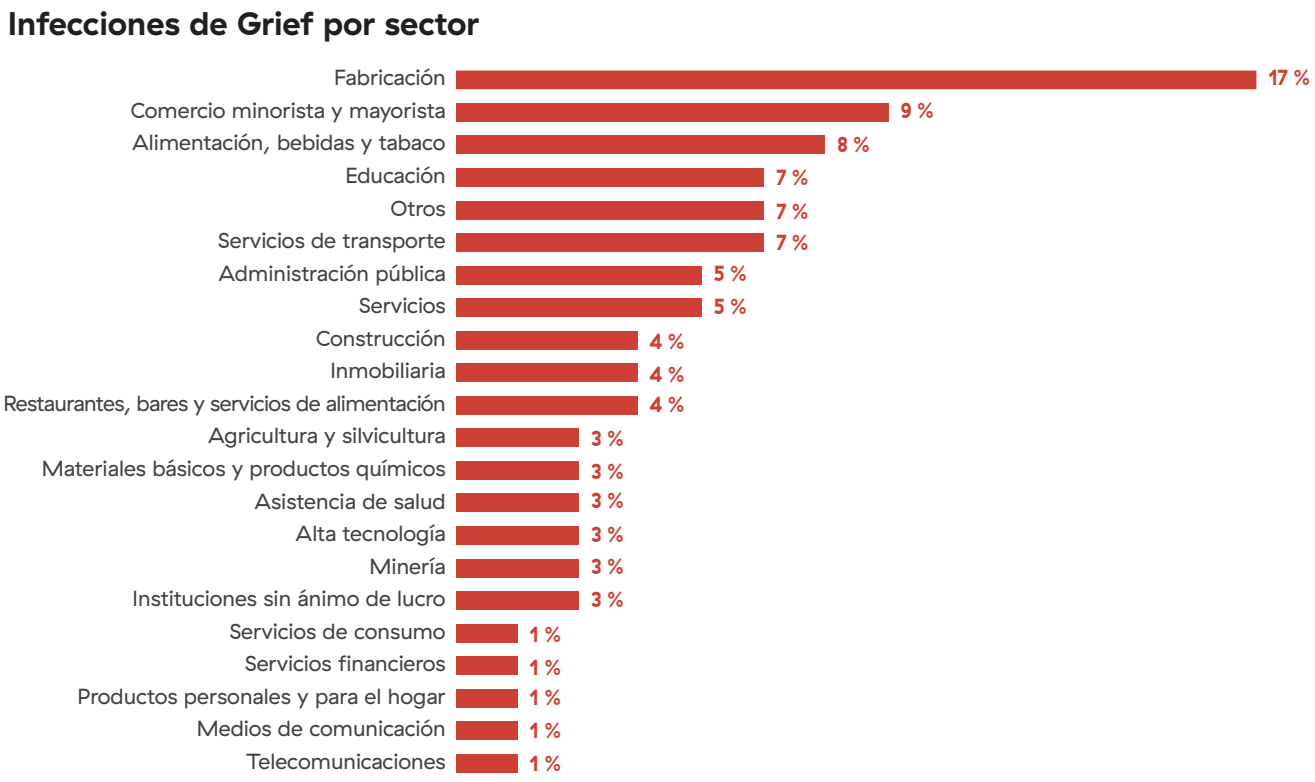


Figura 27: Infecciones de Grief por sector

Grief: tácticas y técnicas de MITRE ATT&CK

Acceso inicial	Ejecución	Persistencia	Ampliación de privilegios	Evasión de defensa	Descubrimiento	Movimiento lateral	Exfiltración	Impacto
Cuentas válidas	Interfaz de línea de comandos	Ejecución de inicio automático de inicio o inicio de sesión: claves de ejecución de registro / carpeta de inicio	Inyección de proceso	Apropiación de flujo de ejecución: apropiación de orden de búsqueda DLL	Descubrimiento de la configuración de la red del sistema	Transferencia lateral de herramienta	Transferencia programada	Datos encriptados para el impacto
Ataque de phishing selectivo	Ejecución del usuario	Tarea/trabajo programado		Desofuscar / descodificar archivos o información	Detección remota del sistema			Inhibir la recuperación del sistema
	Módulos compartidos			Inhabilitar las defensas: desactivar o modificar herramientas	Descubrimiento de archivos y directorios			Apagado/ reinicio del sistema
				Mascarada: coincidencia de nombre o ubicación legítimos	Descubrimiento de software de seguridad			

Hive

El ransomware Hive se detectó por primera vez en junio de 2021, utilizando un modelo RaaS. Utiliza múltiples mecanismos para lograr el acceso inicial, incluidos correos electrónicos de spam maliciosos, credenciales de VPN filtradas y vulnerabilidades en activos externos. La infección inicial comienza con la explotación de las vulnerabilidades de ProxyShell presentes en Microsoft Exchange Server. Las vulnerabilidades de intercambio de ProxyShell son una combinación de CVE-2021-34473 (vulnerabilidad de ejecución de código remoto de Microsoft Exchange Server), CVE-2021-34523 (elevación de vulnerabilidad de privilegios de Microsoft Exchange Server) y CVE-2021-31207 (vulnerabilidad de omisión de función de seguridad de Microsoft Exchange Server).

Cadena de infección

El atacante crea un borrador de correo electrónico dentro de un buzón, con un archivo adjunto que contiene el shell web codificado. A continuación, el atacante exporta todo el buzón (incluido el borrador de correo electrónico malicioso) al formato de archivo PST con una extensión ASPX. Esto permite a los atacantes lanzar web shells en servidores vulnerables. La shell web descarga el script PowerShell que contiene la carga útil codificada de Cobalt Strike. Además, descarga otros stagers y establece un punto de apoyo en el sistema de la víctima. A continuación, utiliza Mimikatz para robar los hashes de NTLM y aprovecha una táctica de pass-the-hash para acceder a la cuenta de control del dominio. Hive realiza un movimiento lateral adicional a través de RDP utilizando las credenciales robadas. Analiza la red y obtiene información adicional utilizando el escáner de red SoftPerfect. Al final, implementa y ejecuta el ransomware Hive y cifra los datos.

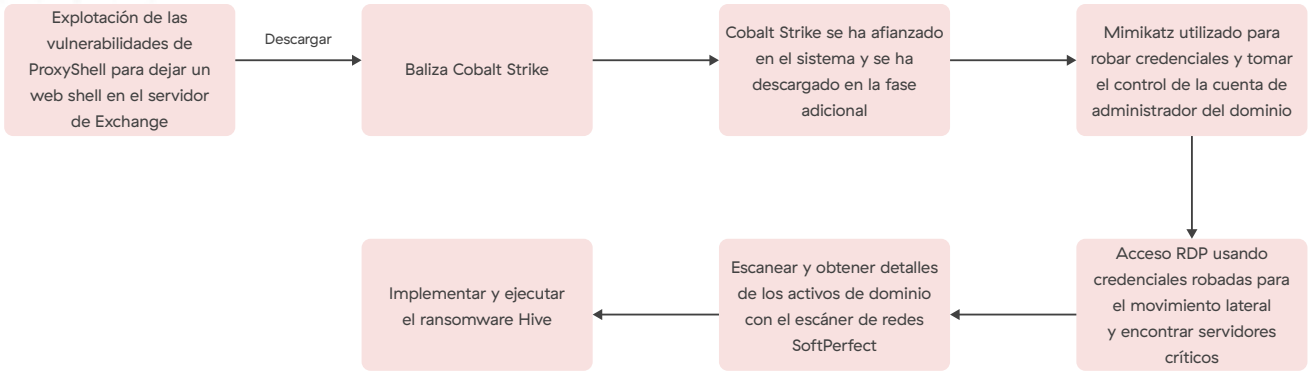


Figura 28: Cadena de ataque de Hive

Las versiones anteriores de la carga útil de ransomware Hive se escribieron en el lenguaje de programación Go y utilizaban una combinación de algoritmos RSA y AES para cifrar archivos. Las versiones más recientes de Hive se escriben en el lenguaje de programación Rust y utilizan Curve25519 y ChaCha20 para el cifrado de archivos.

Los afiliados a Hive también exfiltran datos de las víctimas antes del cifrado de los archivos. En la figura 29 se muestra una captura de pantalla del sitio de filtración de datos de Hive.

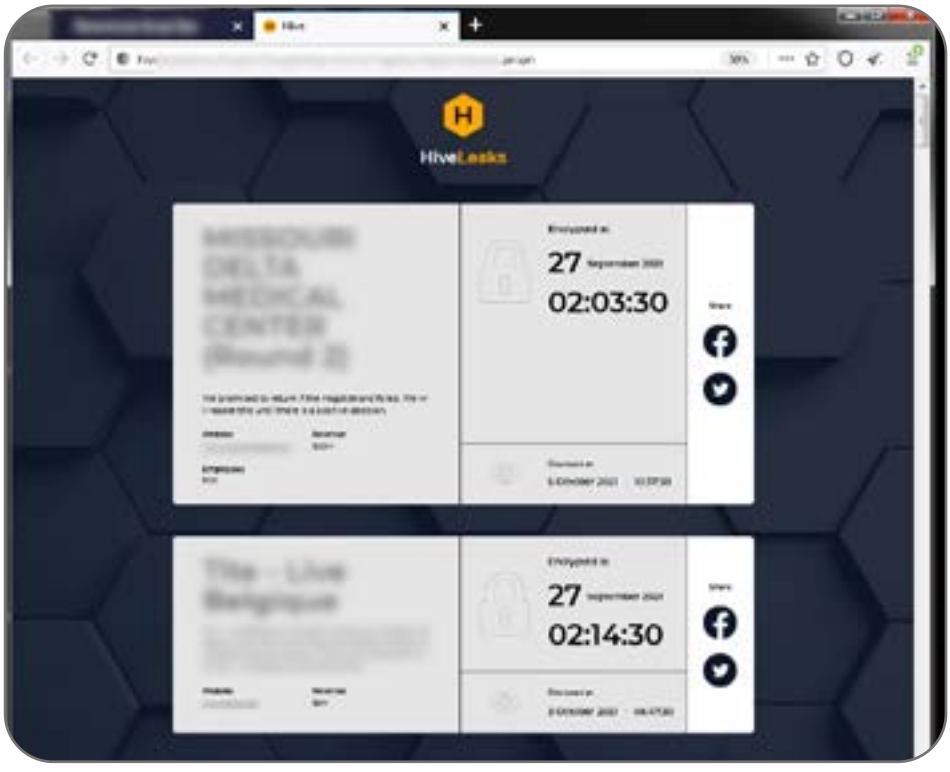


Figura 29: Sitio de filtración de datos de Hive

La figura 30 muestra los sectores verticales de la industria a los que se dirigen los ataques de doble extorsión que utilizan Hive.

Infecciones de Hive por sector

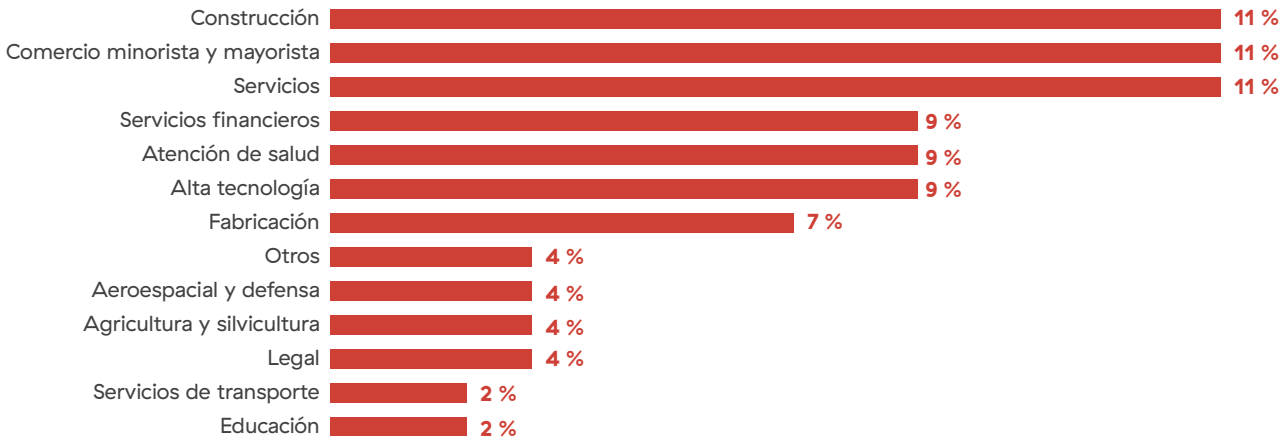


Figura 30: Infecciones de Hive por sector

Hive: tácticas y técnicas de MITRE ATT&CK

Acceso inicial	Ejecución	Persistencia	Ampliación de privilegios	Evasión de defensa	Descubrimiento	Movimiento lateral	Exfiltración	Impacto
Servicios remotos externos	Interfaz de línea de comandos	Cuentas válidas: cuentas de dominio	Cuentas válidas	Borrar los registros de eventos de Windows	Descubrimiento de la configuración de la red del sistema	Protocolo de escritorio remoto	Transferencia programada	Datos encriptados para el impacto
Ataque de phishing selectivo	Ejecución del usuario	Crear cuenta: cuenta de dominio	Cuentas de dominio	Inhabilitar las defensas: desactivar o modificar herramientas	Detección remota del sistema	Servicios a distancia		Inhibir la recuperación del sistema
Explotar la aplicación orientada al público			Explotación para ampliar privilegios	Desofuscar / descodificar archivos o información	Descubrimiento de archivos y directorios			
					Registro de consultas			
					Descubrimiento de software de seguridad			

BlackByte

BlackByte es otro grupo de RaaS que apareció de forma notoria en julio de 2021. Escrito originalmente en C#, posteriormente se volvió a desarrollar en el lenguaje de programación Go alrededor de septiembre de 2021. La versión basada en Go comparte muchas similitudes con la versión en C#, incluidos los comandos ejecutados para realizar la propagación lateral, la escalada de privilegios y el cifrado de archivos.

Las campañas de BlackByte comienzan con la explotación de las vulnerabilidades de ProxyShell presentes en Microsoft Exchange Server.

Cadena de infección
El atacante crea un borrador de correo electrónico dentro de un buzón. El correo electrónico tiene un archivo adjunto que contiene el shell web codificado. A continuación, el atacante exporta todo el buzón (incluido el borrador de correo electrónico malicioso) al formato de archivo PST con una extensión ASPX. Esto permite a los atacantes lanzar web shells en servidores vulnerables.

A continuación, el shell web se utiliza para colocar una baliza de Cobalt Strike en el servidor de intercambio de destino. Se utilizan Cobalt Strike y otras herramientas de postexplotación para robar credenciales y obtener acceso a las cuentas de servicio a fin de conseguir un punto de apoyo en el sistema. Además, BlackByte instala la herramienta AnyDesk RDP. AnyDesk se utiliza para el movimiento lateral y para colocar Cobalt Strike en el controlador de dominio infectado. Finalmente, Cobalt Strike implementa y ejecuta el ransomware BlackByte.

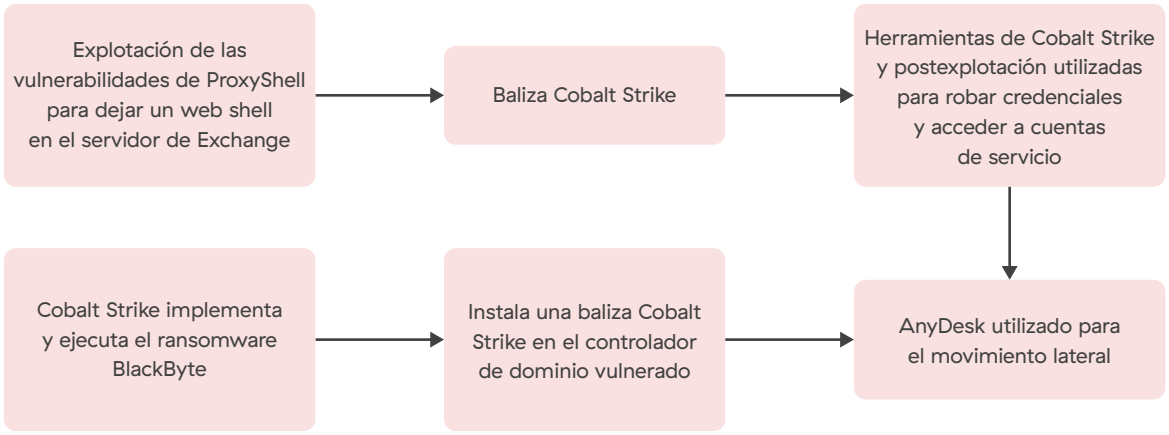


Figura 31: Anatomía de un ataque de ransomware BlackByte

Acceso inicial explotando las vulnerabilidades de ProxyShell para dejar un shell web en el servidor de intercambio. El shell web descarga la baliza Cobalt Strike. A continuación, Cobalt Strike roba las credenciales e instala la herramienta AnyDesk RDP. AnyDesk se utiliza para el movimiento lateral y para colocar Cobalt Strike en el controlador de dominio infectado. Cobalt Strike se utiliza para implementar y ejecutar el ransomware BlackByte.

BlackByte utiliza una combinación de algoritmos RSA y AES para cifrar los archivos. Las versiones más recientes de BlackByte utilizan Curve25519 ECC para el cifrado asimétrico y ChaCha20 para el cifrado simétrico de archivos.

Los autores de la amenaza BlackByte también exfiltran datos de las víctimas antes del cifrado de los archivos. En la figura 32 se muestra una captura de pantalla del sitio de filtración de datos de BlackByte.

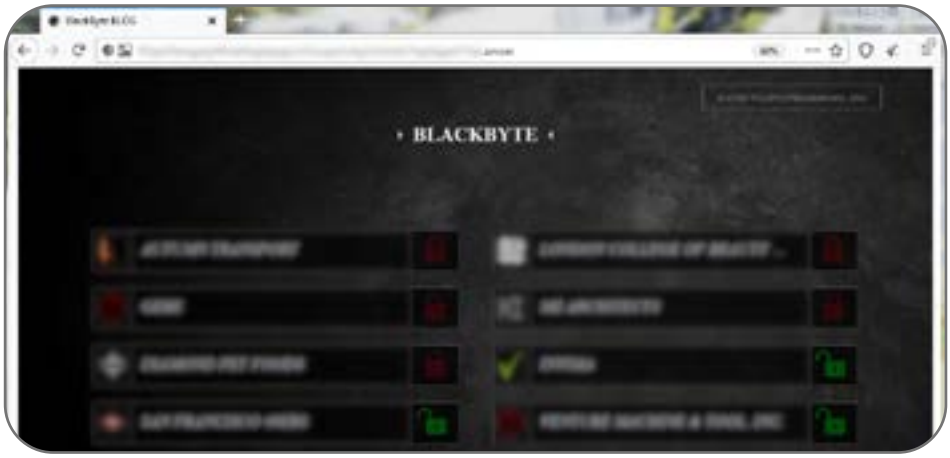


Figura 32: Sitio de filtración de datos de BlackByte

La figura 33 muestra los sectores verticales a los que se dirigen los ataques de doble extorsión que utilizan BlackByte.

Infecciones de BlackByte por sector

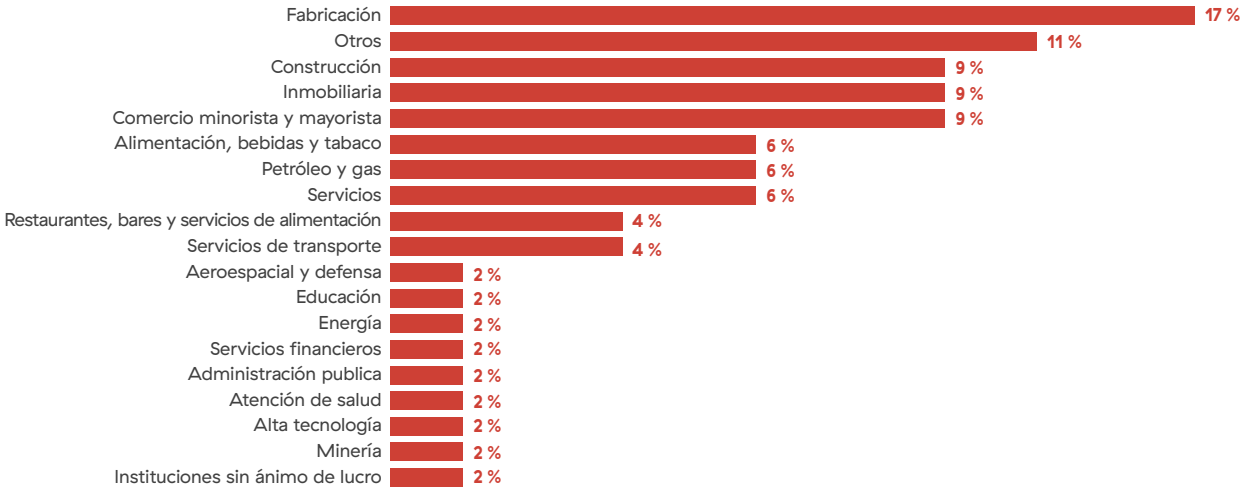


Figura 33: Infecciones de BlackBye por sector

BlackByte: tácticas y técnicas de MITRE ATT&CK

Acceso inicial	Ejecución	Persistencia	Ampliación de privilegios	Evasión de defensa	Descubrimiento	Movimiento lateral	Exfiltración	Impacto
Ataque de phishing selectivo	Intérprete de comandos y scripts	Crear o modificar el proceso del sistema: servicio de Windows	Cuentas de dominio	Inhabilitar las defensas: desactivar o modificar herramientas	Descubrimiento de la configuración de la red del sistema	Transferencia lateral de herramienta	Transferencia programada	Datos encriptados para el impacto
Explotar la aplicación orientada al público	API nativa		Explotación para ampliar privilegios	Desofuscar / descodificar archivos o información	Detección remota del sistema			Inhibir la recuperación del sistema
	Ejecución del usuario			Modificar registro	Descubrimiento de archivos y directorios			
					Registro de consultas			
					Descubrimiento de software de seguridad			

AvosLocker

El ransomware AvosLocker es un grupo RaaS que apareció de forma destacada en julio de 2021. Al igual que Hive y BlackByte, la infección inicial comienza con la explotación de las vulnerabilidades de ProxyShell CVE-2021-34473, CVE-2021-34523y CVE-2021-31207 presentes en el servidor Microsoft Exchange.

Cadena de infección

El atacante crea un borrador de correo electrónico dentro de un buzón. El correo electrónico tiene un archivo adjunto que contiene el shell web codificado. A continuación, el atacante exporta todo el buzón (incluido el borrador de correo electrónico malicioso) al formato de archivo PST con una extensión ASPX. Esto permite a los atacantes lanzar web shells en servidores vulnerables.

A continuación, se utilizan los shells web para colocar Cobalt Strike en el servidor de intercambio infectado. Cobalt Strike y Rclone se utilizan para robar credenciales y exfiltrar datos a servidores remotos.

El ataque instala AnyDesk RDP para acceder a múltiples sistemas, moviéndose lateralmente. Deposita varias secuencias de comandos por lotes para modificar y eliminar claves de registro relacionadas con el software de seguridad. También desactiva Windows Update y Windows Defender.

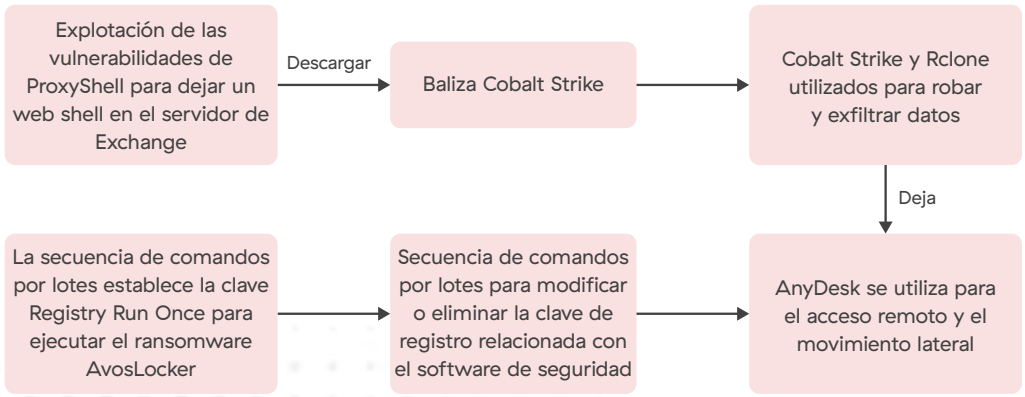


Figura 34: Anatomía de un ataque de ransomware AvosLocker

Al final, AvosLocker reinicia el sistema en modo seguro de Windows y entonces el ransomware comienza a cifrar los archivos. Al arrancar en modo seguro, AvosLocker puede maximizar el número de archivos que se cifran, ya que es probable que las aplicaciones empresariales, como las bases de datos, no se estén ejecutando. Por lo tanto, esas aplicaciones no tendrán manejadores de archivos abiertos que puedan impedir el cifrado de archivos. Además, muchas aplicaciones de software de seguridad (por ejemplo, los programas antivirus) no se cargan por defecto cuando el sistema se ejecuta en modo seguro. Esta capacidad de cifrar archivos en el modo seguro de Windows es una característica que se ha observado en otras familias de ransomware, como Conti, REvil y BlackMatter.

AvosLocker utiliza una combinación de algoritmos RSA y AES para cifrar archivos. AvosLocker creó una versión Linux de su ransomware dirigido a VMware ESXi.

Tras el ataque, el atacante amenaza con publicar los datos de la víctima en un sitio de filtración de datos y, en algunos casos, amenaza y ejecuta un ataque DDoS en la red de la víctima durante la negociación. En la figura 35 se muestra una captura de pantalla del sitio de filtración de datos de AvosLocker.

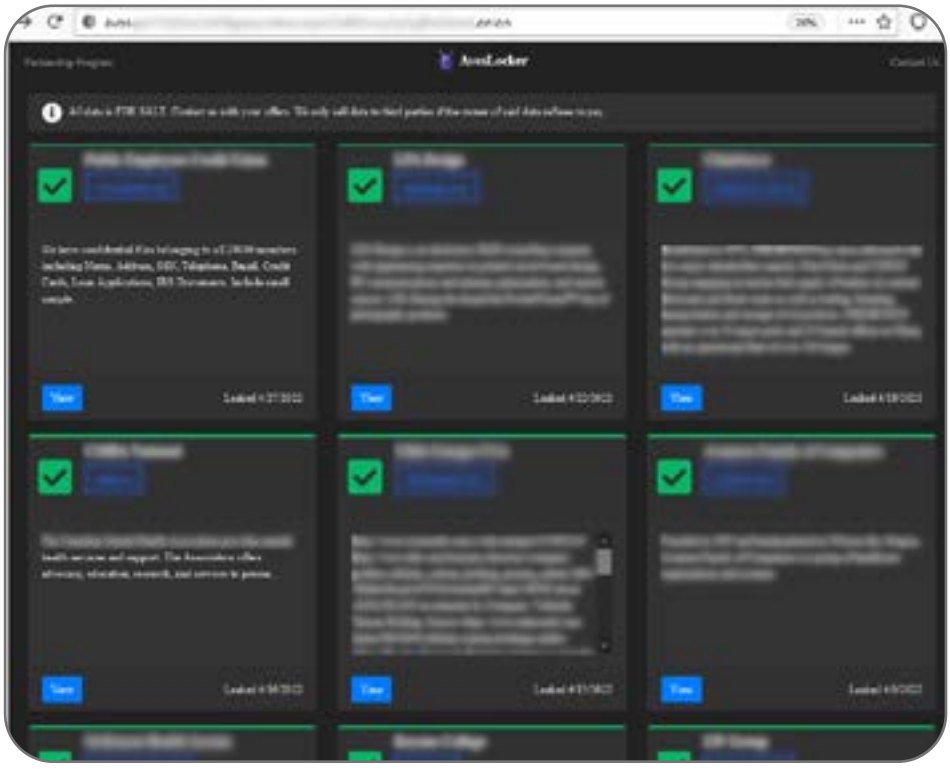


Figura 35: Sitio de filtración de datos de AvosLocker

La figura 36 muestra los sectores verticales a los que se dirigen los ataques de doble extorsión que utilizan AvosLocker.

Infecciones de AvosLocker por sector

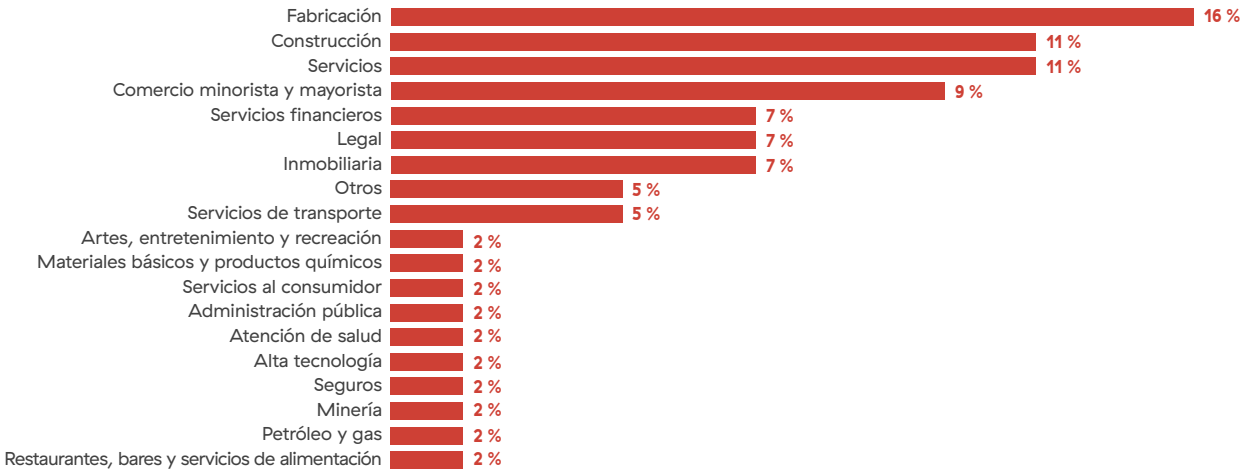


Figura 36: Infecciones de AvosLocker por sector

AvosLocker: tácticas y técnicas de MITRE ATT&CK

Acceso inicial	Ejecución	Persistencia	Ampliación de privilegios	Evasión de defensa	Descubrimiento	Movimiento lateral	Exfiltración	Impacto
Ataque de phishing selectivo	Interfaz de línea de comandos	Ejecución de inicio automático de inicio o inicio de sesión: claves de ejecución de registro / carpeta de inicio	Cuentas de dominio	Inhabilitar las defensas: desactivar o modificar herramientas	Descubrimiento de la configuración de la red del sistema	Transferencia lateral de herramienta	Transferencia programada	Datos encriptados para el impacto
Explotar la aplicación orientada al público	Ejecución del usuario	Tarea/trabajo programado	Explotación para ampliar privilegios	Desofuscar / descodificar archivos o información	Detección remota del sistema			Inhibir la recuperación del sistema
					Descubrimiento de archivos y directorios			Apagado/ reinicio del sistema
					Descubrimiento de software de seguridad			

BlackCat/ALPHV

BlackCat, también conocido como ALPHV, es una operación de RaaS que se detectó por primera vez alrededor de noviembre de 2021. BlackCat ha utilizado el lenguaje de programación RUST, que ayuda a mejorar el rendimiento y la fiabilidad del procesamiento concurrente.

Cadena de infección

La infección inicial comienza con el uso de credenciales vulneradas para obtener acceso a los sistemas de red de las víctimas. Inicialmente, utiliza scripts de Cobalt Strike, PowerShell y script por lotes para mantenerse en la red de la víctima. Una vez que obtiene acceso, vulnera las cuentas de administrador en Active Directory. Además, utiliza objetos maliciosos de políticas de grupo (GPO) para entregar y ejecutar ransomware. También utiliza Microsoft Sysinternals y otras herramientas administrativas en el ataque.

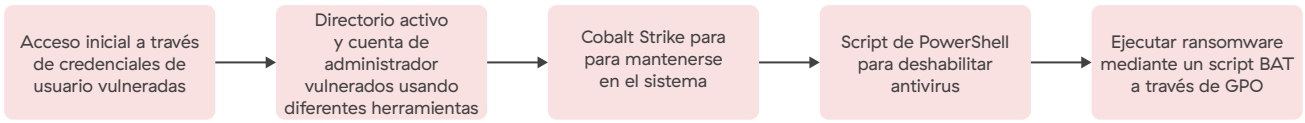


Figura 37: Anatomía de un ataque de ransomware BlackCat/ALPHV

BlackCat agregó tácticas DDoS a su operación. BlackCat lanza ataques DDoS tanto en el sitio web como en la red de la víctima para alentar a la víctima a negociar con sus operadores y forzar cantidades de rescate más elevadas. En la figura 38 se muestra una captura de pantalla de ejemplo del sitio de filtración de datos de BlackCat.

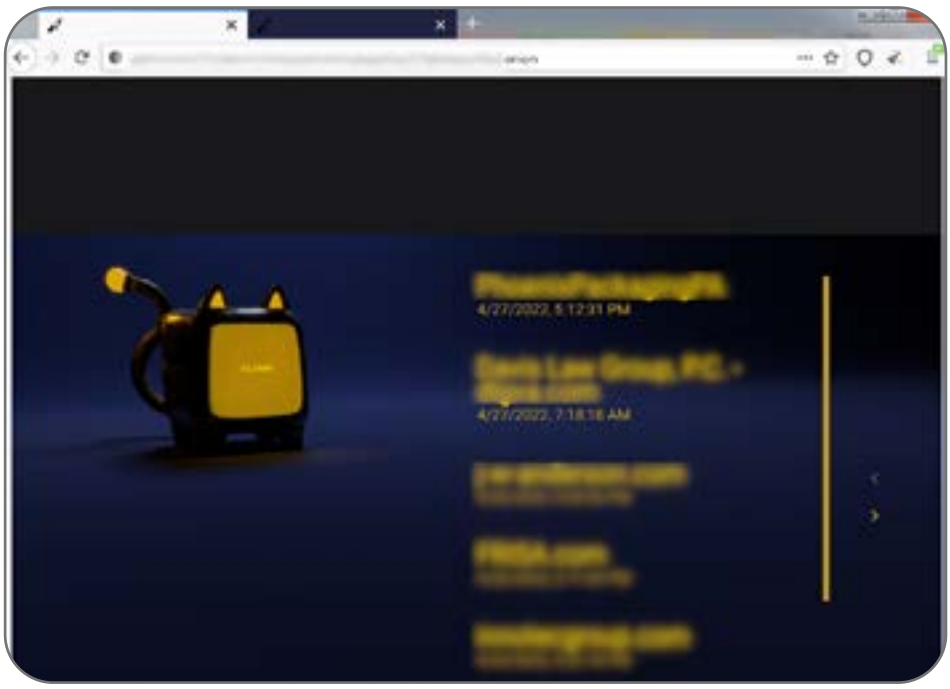


Figura 38: Sitio de filtración de datos de BlackCat/ALPHV

La figura 39 muestra los sectores verticales a los que se dirigen los ataques de doble extorsión que utilizan BlackCat/ALPHV.

Infecciones por BlackCat/ALPHV por sector

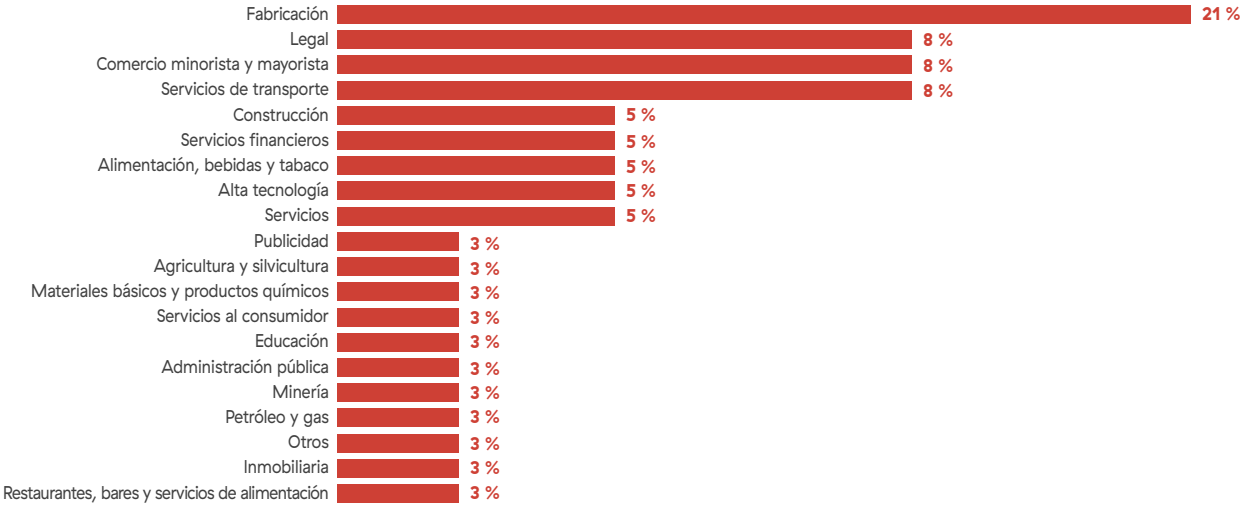


Figura 39: Infecciones de BlackCat/ALPHV por sector

BlackCat: tácticas y técnicas de MITRE ATT&CK

Acceso inicial	Ejecución	Persistencia	Ampliación de privilegios	Evasión de defensa	Descubrimiento	Movimiento lateral	Exfiltración	Impacto
Cuentas válidas	Intérprete de comandos y scripts	Ejecución de inicio automático de inicio o inicio de sesión: claves de ejecución de registro / carpeta de inicio	Cuentas de dominio	Inhabilitar las defensas: desactivar o modificar herramientas	Descubrimiento de la configuración de la red del sistema	Transferencia lateral de herramienta	Transferencia programada	Datos encriptados para el impacto
	Ejecución del usuario	Tarea/trabajo programado	Explotación para ampliar privilegios	Desofuscar / descodificar archivos o información	Detección remota del sistema			Inhibir la recuperación del sistema
				Modificación de la política de dominio: modificación de la política de grupo	Descubrimiento de archivos y directorios			
					Descubrimiento de software de seguridad			

Acerca de ThreatLabz

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

Manténgase informado sobre las investigaciones de ThreatLabz suscribiéndose a nuestro boletín Trust Issues hoy mismo.

Zscaler Zero Trust Exchange ha sido nombrado por Gartner como una plataforma de vanguardia en servicios de seguridad (SSE), que ofrece protección contra ransomware en todas las etapas de la cadena de ataque para reducir drásticamente sus posibilidades de ser atacado y mitigar posibles daños.

Zscaler integra de forma nativa capacidades líderes en el sector para:

Para saber más, visite nuestra página Zscaler Ransomware Protection.

zscaler™ | Experience your world, secured.™

Acerca de Zscaler

Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, resistentes y seguros. Zscaler Zero Trust Exchange protege a miles de clientes de los ciberataques y la pérdida de datos mediante la conexión segura de usuarios, dispositivos y aplicaciones en cualquier lugar. Distribuido en más de 150 centros de datos en todo el mundo, Zero Trust Exchange basado en SASE es la mayor plataforma de seguridad en la nube en línea del mundo. Obtenga más información en **zscaler.es** o síganos en Twitter **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.es