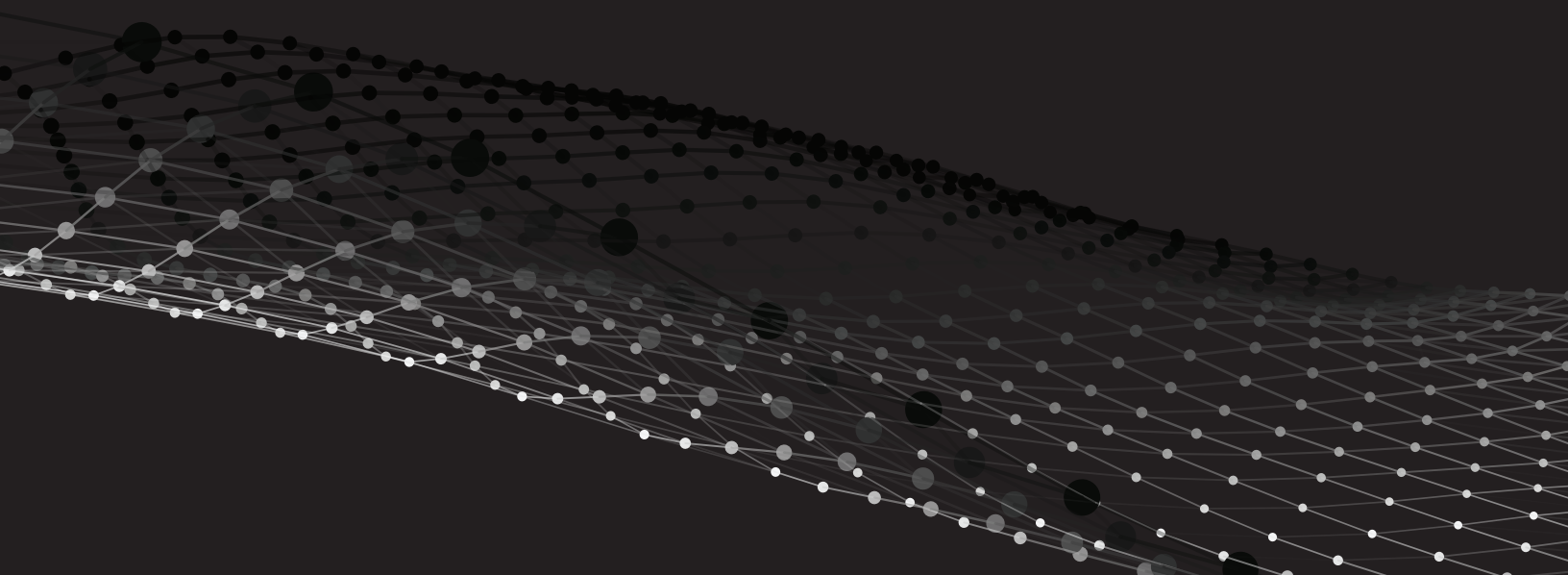
UNIT 42™
BY PALO ALTO NETWORKS

# Informe de amenazas de ransomware

2021



# Índice

# Prólogo

Antes de unirme a Palo Alto Networks, presté mis servicios durante 35 años en el Ejército de los Estados Unidos; los últimos 10 años los dediqué a asignaciones cibernéticas. Durante mi carrera, pude ver de primera mano cómo el ransomware era la principal amenaza de seguridad nacional, algo que aún seguimos viendo.

El ransomware es una de las principales amenazas en la ciberseguridad. Según el Identity Theft Resource Center (Centro de Recursos para Víctimas de Robo de Identidad), ocurrieron 878 ciberataques en 2020, el 18 % de los cuales se registró como ransomware.[1] Esta amenaza es un área de enfoque para Palo Alto Networks. Nuestros equipos de inteligencia de amenazas Unit 42 global y de respuesta a incidentes trabajaron en conjunto para crear el Informe de amenazas de ransomware de 2021 de Unit 42 a fin de proporcionar la información más reciente sobre las principales variantes de ransomware, las tendencias de pago de ransomware y las mejores prácticas de seguridad para comprender y administrar mejor la amenaza.

En pocas palabras: el ransomware es un negocio lucrativo. El pago de rescate promedio de las organizaciones en Estados Unidos, Canadá y Europa aumentó de USD 115 123 en 2019 a USD 312 493 en 2020; un aumento del 171 % interanual. Con tácticas nuevas tales como la doble extorsión, esta cifra seguirá aumentando.

Organizaciones de todo el mundo son rehenes del ransomware y muchas se ven obligadas a pagar a los ciberdelincuentes porque no están equipadas para combatir la amenaza por diferentes motivos, desde la falta de copias de respaldo recuperables hasta el costo del tiempo de inactividad, que supera el costo del pago del rescate.

Debemos reducir significativamente esta organización delictiva, por eso me enorgullece que Palo Alto Networks sea miembro del Equipo Especial de Ransomware (RTF) del Instituto de Tecnología y Seguridad, donde me desempeño como copresidente.

El RTF se centra en el desarrollo de un conjunto de recomendaciones para una estrategia integral a fin de mitigar la amenaza de ransomware. Para desarrollar un conjunto de soluciones que ataque todos los lados del flagelo del ransomware, el RTF ha reclutado un amplio y diverso grupo de expertos que actualmente investigan una gran variedad de pistas para recomendaciones y reconocen el gran trabajo que ya se ha realizado en este espacio.

Esto implica analizar preguntas tales como las siguientes:

- ¿Qué podemos hacer para preparar mejor a las organizaciones para un ataque de ransomware?
- ¿Cómo pueden las organizaciones comprender y responder mejor a un ataque de ransomware?
- ¿Cuáles son las mayores barreras para la adopción de la seguridad contra el ransomware?
- ¿Cómo podemos dificultar el ataque de los actores del ransomware?
- ¿Cómo podemos hacer que el resultado de un ataque de ransomware sea menos destructivo?
- ¿Cómo podemos crear soluciones que se adapten a las necesidades de las diferentes víctimas de los ataques de ransomware?

A medida que avanzan estos debates, el equipo especial apunta a proporcionar recomendaciones claras y procesables a nivel internacional para los responsables de tomar decisiones tanto del sector público como privado en la primavera de 2021.

Creo que los recursos, como el Informe de amenazas de ransomware de 2021 de Unit 42, nos ayudarán en este esfuerzo por aprender todo lo que podamos sobre esta amenaza, lo que nos permitirá trabajar en los sectores públicos y privados a fin de reducir de forma conjunta el problema del ransomware a un elemento más manejable que la amenaza significativa que afrontamos en la actualidad.

John Davis
General de división retirado del Ejército de los Estados Unidos
Vicepresidente del sector público de Palo Alto Networks

1. "2020 Data Breach Report" (en inglés), ITRC, 28 de enero de 2021, https://notified.idtheftcenter.org/s/2020-data-breach-report.

# Resumen ejecutivo

Para evaluar el estado actual del panorama de amenazas de ransomware, los equipos de inteligencia de amenazas Unit 42 y de respuesta a incidentes colaboraron a fin de analizar el panorama de amenazas de ransomware en 2020 con sus datos globales.

Este informe detalla las principales variantes del ransomware (con enlaces a evaluaciones de amenazas para cada variante), los pagos promedio del ransomware, las predicciones de ransomware y los pasos procesables a seguir a fin de reducir de inmediato el riesgo de ransomware.

## Los ciberdelincuentes generan y demandan más dinero que nunca

*Nota: Los siguientes datos pertenecen a Estados Unidos, Canadá y Europa.*

El pago de rescate promedio de las organizaciones aumentó de USD 115 123 en 2019 a USD 312 493 en 2020, un aumento del 171 % interanual. Además, de 2019 a 2020, el mayor rescate pagado por una organización se duplicó de USD 5 millones a USD 10 millones. Mientras tanto, los ciberdelincuentes se vuelven codiciosos. De 2015 a 2019, la mayor demanda de ransomware fue de USD 15 millones. En 2020, la mayor demanda de ransomware aumentó a USD 30 millones.

Cabe señalar que Maze demandó en 2020 un rescate promedio de USD 4,8 millones, un aumento significativo en comparación con el promedio de USD 847 344 en todas las familias de ransomware en 2020. Los ciberdelincuentes saben que pueden hacer dinero con el ransomware y cada vez son más audaces en sus demandas.

## Las organizaciones de salud están en la mira

El mundo cambió con la COVID-19 y los operadores de ransomware aprovecharon la pandemia para asediar a las organizaciones, particularmente al sector sanitario, el sector vertical más atacado por el ransomware en 2020. Los operadores de ransomware fueron descarados en sus ataques en el intento de hacer la mayor cantidad de dinero posible, a sabiendas de que las organizaciones de salud, que debían seguir operando para tratar a los pacientes con COVID-19 y ayudarlos a salvar sus vidas, no podían permitir el bloqueo de sus sistemas y, por lo tanto, estarían más dispuestas a pagar un rescate.

El ransomware Ryuk se destacó de los demás. En octubre de 2020, la Agencia de Seguridad de la Infraestructura y Ciberseguridad (CISA), la Oficina Federal de Investigación (FBI) y el Departamento de Salud y Servicios Sociales (HHS) emitieron un aviso conjunto sobre ciberseguridad, advirtiendo a las organizaciones de salud contra los ataques de Ryuk.

## El ascenso de la doble extorsión

Un ataque de ransomware común consta de un operador de ransomware que cifra los datos y fuerza a la víctima a pagar un rescate para desbloquearlos. En el caso de una doble extorsión, los operadores de ransomware cifran y roban los datos para presionar aún más a la víctima para que pague el rescate. Si la víctima no paga el rescate, los operadores de ransomware filtran los datos en un sitio de filtración o en un dominio de la web oscura; la mayoría de los sitios de filtración están alojados en la web oscura. Estas ubicaciones de alojamiento están creadas y administradas por los operadores de ransomware. Hay al menos 16 variantes de ransomware diferentes que en este momento amenazan con exponer los datos o utilizar los sitios de filtración; más variantes probablemente continuarán con esta tendencia.

La familia de ransomware que más aprovechó esta táctica fue NetWalker. Desde enero de 2020 hasta enero de 2021, NetWalker filtró datos de 113 organizaciones que fueron víctimas a nivel mundial, superando ampliamente a otras familias de ransomware. RagnarLocker quedó en segundo lugar, con una filtración de datos de 26 víctimas a nivel mundial. Cabe señalar que el Departamento de Justicia de EE. UU. anunció en enero de 2021 que había coordinado una acción de aplicación de la ley internacional para interrumpir el grupo de ransomware NetWalker. El dominio de la web oscura administrado por los operadores de NetWalker, que alojó los datos filtrados, ya no es accesible.

# 01

# Principales observaciones sobre ransomware de 2020

## Pandemia de COVID-19

Los adversarios sacaron partido a los eventos actuales para tentar a las víctimas para que abrieran correos electrónicos de suplantación de identidad, visitaran sitios web falsos o descargaran archivos maliciosos. Ejemplo concreto: con el impacto global de la pandemia de COVID-19, los atacantes del ransomware aprovecharon intensamente este tema en sus ataques de ransomware dirigidos a una variedad de industrias. Si bien el sector sanitario fue el principal objetivo en 2020 debido al coronavirus, muchas industrias sufrieron profundamente incidentes de ransomware.

Afrontando un panorama financiero más frágil durante el año y con el desafío agregado de tener los empleados trabajando desde el hogar, muchas empresas debieron arreglárselas con menos. Con menos personal y con recortes presupuestarios, la sensibilización con respecto a las ciberamenazas y las protecciones de ciberseguridad pueden ser más difíciles de implementar.

## Cambios en el enfoque

El ransomware es cada vez más fácil de apropiar y está disponible en muchos formatos dirigidos a múltiples plataformas. Hemos observado cambios de los modelos de alto volumen y esparcimiento a un modelo más centrado en la "participación", donde los operadores dedican tiempo a conocer a las víctimas y sus redes, siguiendo un enfoque de penetración de la red más tradicional.

## Plataformas abordadas

Además del ransomware que se observa en Microsoft Windows®, Apple macOS® y los sistemas operativos móviles, ahora vemos que también atacan Linux.

## Facilidad de uso y disponibilidad

Los adversarios entienden que el ransomware, específicamente el modelo de ransomware como servicio (RaaS) basado en suscripciones, es fácil de ejecutar, excepcionalmente eficaz y potencialmente rentable, tanto a través de los pagos directos como de la venta de información valiosa. El modelo de RaaS permite que los afiliados utilicen el software de ransomware existente para perpetrar los ataques; por ende, obtienen un porcentaje de cada pago de rescate exitoso.

Los operadores de ransomware siguen teniendo acceso a los entornos de las víctimas a través de métodos tradicionales, entre ellos, suplantación de identidad, credenciales de remote desktop protocol (protocolo de escritorio remoto, RDP) débiles o comprometidas y vulnerabilidades de software/aplicaciones explotadas. A pesar de las mayores fuerzas laborales remotas de 2020, estas técnicas de entrada siguen siendo las mismas. Muchos operadores además combinan productos de malware tales como Dridex, Emotet y Trickbot para el acceso inicial. Una vez dentro de la red, los adversarios usan herramientas nativas, como PSExec y PowerShell, para enumerar la red y moverse lateralmente.

## El ascenso de la doble extorsión

Varias familias de ransomware (NetWalker, RagnarLocker, DoppelPaymer y muchas otras, como se muestra en la figura 1) han mostrado su capacidad de exfiltrar datos y usar técnicas de doble extorsión. En lugar de solo cifrar los archivos de los hosts de las víctimas, los operadores primero los exfiltran para presionar aún más a las víctimas para que paguen el rescate. Los archivos exfiltrados luego se publican, o se amenaza con publicarlos, en un sitio de filtración público o de la web oscura; la mayoría de los sitios de filtración están alojados en la web oscura. Estas ubicaciones de alojamiento están creadas y administradas por los operadores de ransomware. Algunos operadores de ransomware continuarán probando su conocimiento del entorno de la red de una víctima mediante la visualización de los datos en la forma de directorios o árboles de archivos.

La figura 1 ofrece una descripción general de alto nivel de las víctimas afectadas por los sitios de filtración aún activos en enero de 2021. Esto nos permite comprender la enorme escala de daño que causan los operadores de ransomware. Más notablemente, las filtraciones del ransomware NetWalker lideraron la lista con un pasmoso 33 % y otros grupos contabilizaron un 7 % o menos cada uno. También es importante destacar que se realizó una acción coordinada de aplicación de la ley internacional para interrumpir el grupo de ransomware NetWalker el 27 de enero de 2021. El dominio de la web oscura administrado por los operadores de NetWalker ya no es accesible.

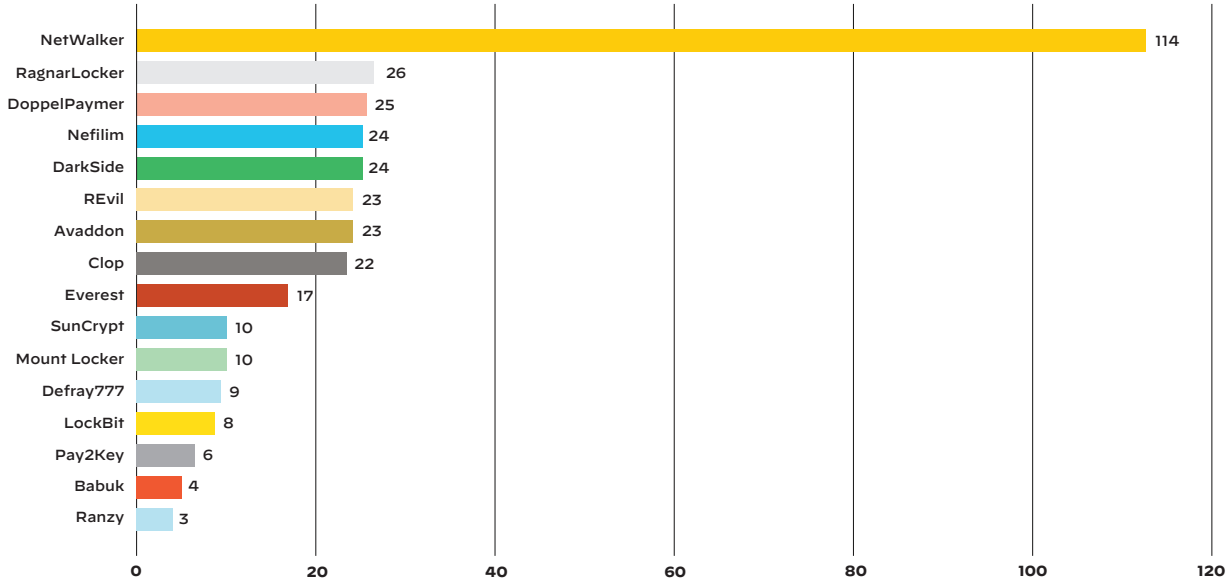



**Figura 1:** Cantidad de organizaciones que fueron víctimas a nivel mundial de una familia de ransomware que publicó datos en sitios de filtración, de enero de 2020 a enero de 2021

También examinamos la cantidad de organizaciones que fueron víctimas de publicaciones de datos en sitios de filtración por región. Como se muestra en la figura 2, la región del continente americano fue la más golpeada, seguida de EMEA (Europa, Oriente Medio y África) y JAPAC (Japón y Asia-Pacífico).

De las organizaciones que fueron víctimas de publicaciones de datos en sitios de filtración, los primeros tres países impactados a nivel global fueron Estados Unidos (47 % de las organizaciones), Canadá (12 %) y Alemania (8 %). Si estos porcentajes son paralelos a la cantidad de organizaciones que realmente pagaron el rescate, puede implicar que las organizaciones estadounidenses son más rentables para los operadores de ransomware. Además, dada la creciente aceptación de las soluciones de seguros cibernéticos en países tales como Estados Unidos, Canadá y Alemania, muchas empresas pueden decidir pagar el recate si ya están cubiertas por sus respectivos proveedores de seguro. La figura 3 proporciona un desglose de la figura 2 desde una perspectiva global.

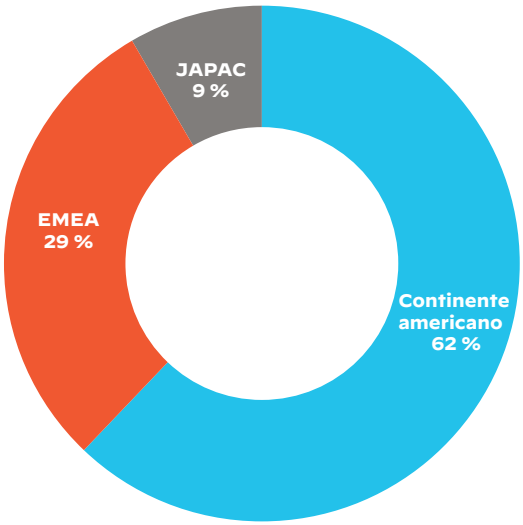
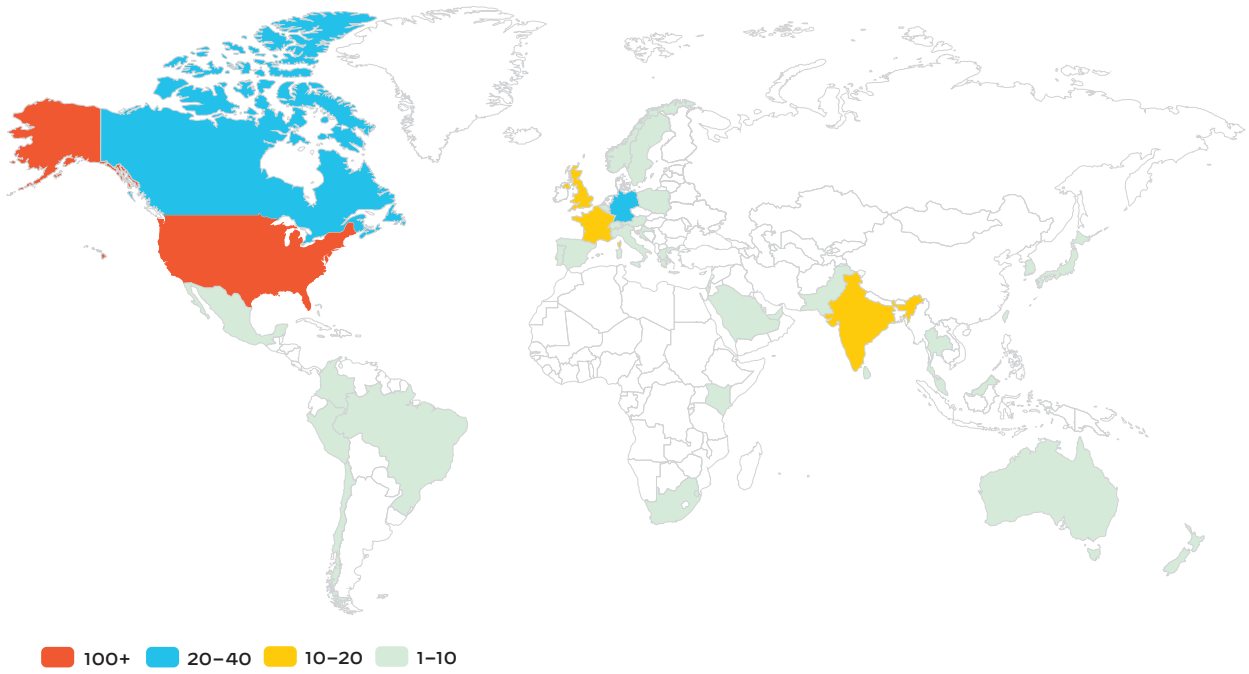



**Figura 2:** Porcentaje total de organizaciones que fueron víctimas de publicaciones de datos en sitios de filtración por región, de enero de 2020 a enero de 2021




| Cantidad de organizaciones que fueron víctimas de publicaciones de datos en sitios de filtración por país | | | | | | | |
|---|---|---|---|---|---|---|---|
| Estados Unidos | 151 | Bélgica | 4 | Chile | 1 | Pakistán | 1 |
| Canadá | 39 | Suecia | 4 | Colombia | 1 | Perú | 1 |
| Alemania | 26 | Sudáfrica | 3 | Croacia | 1 | Polonia | 1 |
| Reino Unido | 17 | España | 3 | Grecia | 1 | Portugal | 1 |
| Francia | 16 | Japón | 2 | Hong Kong | 1 | Arabia Saudita | 1 |
| India | 11 | México | 2 | Jamaica | 1 | Singapur | 1 |
| Australia | 7 | Nueva Zelanda | 2 | Kenia | 1 | Sri Lanka | 1 |
| Brasil | 5 | Corea del Sur | 2 | Luxemburgo | 1 | Taiwán | 1 |
| Israel | 5 | Suiza | 2 | Malasia | 1 | Tailandia | 1 |
| Italia | 5 | Austria | 1 | Noruega | 1 | Emiratos Árabes Unidos | 1 |

**Figura 3:** Cantidad de organizaciones que fueron víctimas de publicaciones de datos en sitios de filtración por país, de enero de 2020 a enero de 2021

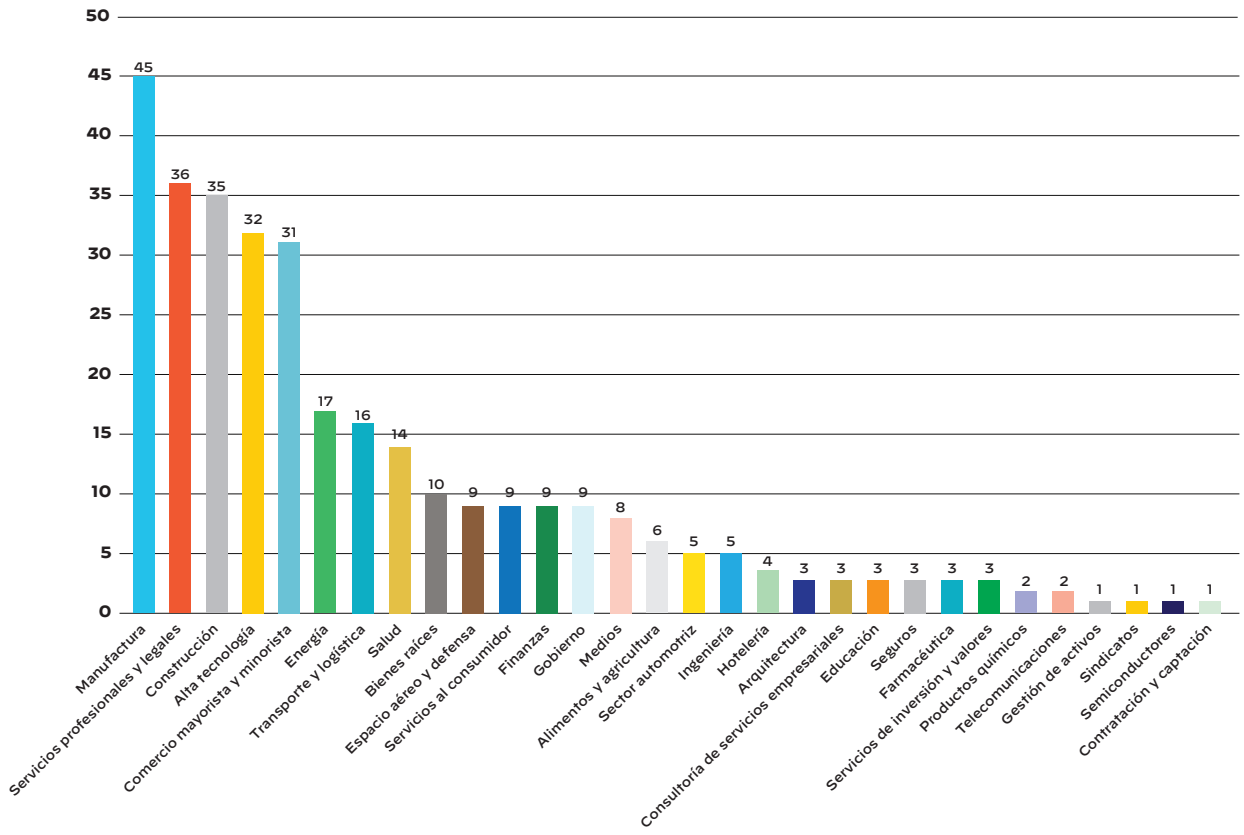



**Figura 4:** Cantidad de organizaciones que fueron víctimas de publicaciones de datos en sitios de filtración a nivel mundial por sector, de enero de 2020 a enero de 2021

La figura 4 desglosa las organizaciones que fueron víctimas por sus respectivas industrias; muestra la cantidad de organizaciones por industria donde se expusieron datos en un sitio de filtración controlado por operadores de ransomware. Muchos de los operadores han realizado filtraciones de datos de las organizaciones, probablemente en un esfuerzo por presionar a las organizaciones que son víctimas a pagar el rescate en un plazo límite, en cuyo defecto los operadores deciden filtrar la totalidad de los datos. Los datos publicados de cada organización varían entre 30 MB a más de 1000 GB.

## Reintroducción de las campañas de DDoS

Varias familias de ransomware se identificaron con la distributed denial-of-service (denegación de servicio distribuida, DDoS) contra sitios web que fueron víctimas como ventaja adicional. Por ejemplo, los operadores del ransomware Avaddon han comenzado a implementar los ataques de DDoS contra las organizaciones que son víctimas y que no cooperan con los actores durante el período de negociación. Este concepto no es nuevo. En 2016 y en 2019, los operadores enviaron amenazas de DDoS por correo electrónico a las víctimas de rescates si no pagaban. Sin embargo, en 2020, se reintrodujo esta estrategia destructiva.

## Costos de los incidentes de ransomware

Las organizaciones de todos los tamaños en muchas industrias se han visto afectadas por el ransomware. En comparación con 2019, observamos un aumento en los casos de respuesta a incidentes de ransomware en varias industrias en Estados Unidos, Canadá y Europa, como se muestra en la figura 5. Si bien esta cifra plasma un resumen de focalización general en la industria, no representa el aumento conocido de incidentes en los sectores tales como salud, manufactura y educación. La dedicación del ransomware en 2020 fue más compleja que en los años anteriores y generó tiempos de respuesta a vulneraciones más prolongados y profundos.

En particular, el sector de la tecnología de la información vio un incremento del 65 % en los casos de respuesta a incidentes de ransomware de 2019 a 2020. A medida que las organizaciones cambiaron a las fuerzas laborales remotas debido a la pandemia de COVID-19, los operadores de ransomware adaptaron sus tácticas en consecuencia, incluidos el uso de correos electrónicos maliciosos que contienen temas basados en la pandemia e incluso las aplicaciones móviles maliciosas que afirman ofrecer información sobre el virus.

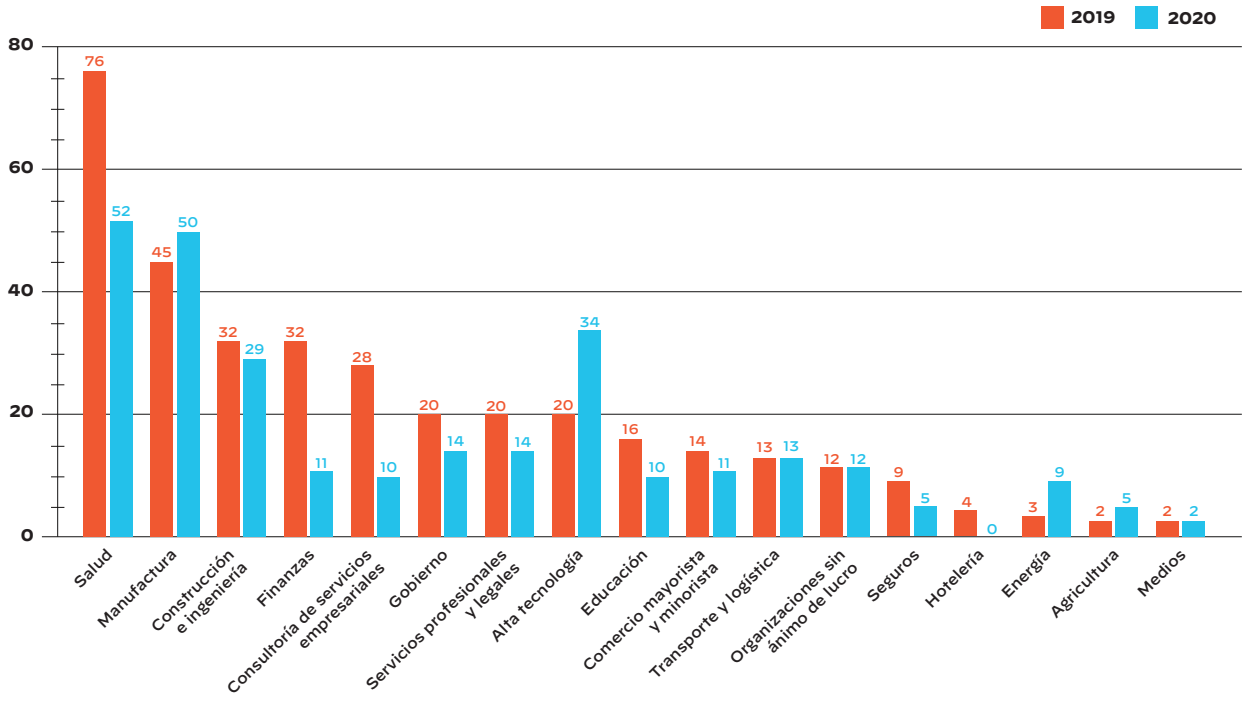



**Figura 5:** Casos de respuesta a incidentes de ransomware por industria en 2019 y 2020 en Estados Unidos, Canadá y Europa

Además, los actores del ransomware demandan más dinero cada año en Estados Unidos, Canadá y Europa. En 2020, las demandas de rescates tuvieron un promedio de USD 847 344; a menudo se solicitan en la forma de bitcoins o criptomonedas Monero. Este monto puede variar drásticamente según la familia de ransomware.

El costo total de un incidente de ransomware generalmente es mucho mayor que la demanda en sí. En 2020, el costo promedio de un proyecto forense (o investigación de la respuesta a incidentes) fue de USD 73 851, incluso cuando las copias de seguridad se consideraron una opción viable para las organizaciones. Este número no contabiliza otros costos monetarios, potencialmente acumulados, que elevan el costo promedio general total a una cifra que incapacitaría a muchas empresas.

La tabla 1 muestra un desglose de los costos de ransomware.

**Tabla 1: Costos asociados a los incidentes de ransomware en 2020 en Estados Unidos, Canadá y Europa (USD)**

| | Datos de 2020 | Datos anteriores (cuando estén disponibles) |
|---|---|---|
| Demanda promedio de rescate | USD 847 344 | – |
| Pago promedio de rescate | USD 312 493 | USD 115 123 (2019) |
| Mayor demanda de rescate | USD 30 000 000 | USD 15 000 000 (2015-2019) |
| Mayor pago de rescate | USD 10 000 000 | USD 5 000 000 (2015-2019) |
| Menor demanda de rescate | USD 1000 | – |
| Costo promedio del proyecto forense | USD 73 851 | USD 62 981 (2019) |
| Costo promedio del proyecto forense, pequeñas y medianas empresas | USD 40 719 | – |
| Demanda promedio de rescate, pequeñas y medianas empresas | USD 718 414 | – |
| Costo promedio del proyecto forense, grandes empresas | USD 207 875 | – |
| Demanda promedio de rescate, grandes empresas | USD 2 923 122 | – |

# 02

# Principales variantes de ransomware de 2020

El 2020 fue un gran año para el ransomware. Vimos cómo las familias nuevas y viejas causaron estragos en las industrias a nivel mundial. Los operadores de ransomware aprovecharon las inquietudes generalizadas respecto de la COVID-19 para perpetrar ataques de suplantación de identidad con temas relacionados con la pandemia y apuntaron intensamente a industrias ya abatidas, como la salud. Si bien la siguiente no es una lista completa, Palo Alto Networks observó estas familias durante el año calendario 2020.

## Ryuk

Desde agosto de 2018, numerosas industrias, como el gobierno, la salud, la energía y la alta tecnología, han sido abordadas por el ransomware Ryuk. Durante el 2020, vimos un aumento importante en los ataques del ransomware Ryuk a la educación, la salud y las organizaciones militares/gubernamentales, principalmente dentro de Estados Unidos, pero también en Reino Unido y Canadá. Se puso un gran enfoque en los sistemas hospitalarios, presumiblemente debido a la necesidad de disponibilidad, dado que estos sistemas se vieron abrumados por el manejo continuo de la pandemia de COVID-19. Observamos que las solicitudes de rescates iniciales de Ryuk variaron de USD 600 000 a USD 10 millones en múltiples industrias. Con mayor frecuencia, estos pagos se comunicaron mediante una cuenta de ProtonMail y se solicitaron en la forma de bitcoins.

Para obtener acceso al sistema objetivo, Ryuk ha comprometido exitosamente los hosts con macros maliciosas en documentos de suplantación de identidad, ha utilizado productos de malware tales como Trickbot, BazaLoader y Emotet, y ha aplicado técnicas de explotación que permiten que el software malicioso evada los productos de seguridad de endpoints. Se observó que, en algunos casos, Ryuk se instaló semanas o incluso meses después del malware de puerta trasera en el host de la víctima. En al menos una instancia, se implementó después del horario comercial mediante cuentas de servicio de copia de respaldo. Una vez que tienen acceso al sistema, los operadores de Ryuk aprovechan las conexiones del RDP para implementar la carga útil de Ryuk o moverse lateralmente a través de la red. Durante la infección activa, Ryuk se cierra y cifra todos los archivos, incluido su propio documento malicioso que generó la descarga inicial. Un archivo con el nombre "RyukReadMe" se coloca en el sistema y herramientas tales como PowerShell y Windows Management Instrumentation (WMI) se usan para enumerar la red mientras se evade la detección. Se cree que el ransomware Ryuk está asociado al grupo de amenazas Wizard Spider.

Visite el blog de Unit 42 para obtener más información sobre el ransomware Ryuk.

## Maze (ChaCha)

El ransomware Maze, una variante de la familia de ransomware ChaCha, se observó activo por primera vez en mayo de 2019 e incrementó su actividad exponencialmente a principios de 2020. Mediante el uso de documentos de suplantación de identidad de Microsoft Word y Excel maliciosos, Maze abordó a las organizaciones globalmente en muchas industrias, al explotar sus servicios externos vulnerables con kits de exploits tales como Spelevo para obtener acceso a los entornos de la víctima. Las industrias afectadas por Maze incluyen finanzas, salud, transporte y logística, alta tecnología, telecomunicaciones, construcción e ingeniería, medios y comunicación, y muchas otras en Estados Unidos, Reino Unido, Canadá, Francia y Suiza.

A fines de 2020, Maze comenzó a liberar su carga útil de ransomware desde dentro de la virtual machine (máquina virtual, VM) como medio para evadir la detección. Esta novedosa técnica se observó por primera vez en RagnarLocker y permite que el ransomware se implemente como VM en casi cualquier dispositivo objetivo infectado. La carga útil de encriptación de archivos de Maze se liberó en una imagen de disco virtual de VirtualBox identificada dentro del archivo MSI de Windows. Además, en el archivo MSI se incluyó un hipervisor de VirtualBox utilizado para ejecutar la VM. En algunos casos, los operadores implementaron la carga útil días después de establecer la persistencia en la red. Maze también usó varias herramientas, incluidas Cobalt Strike, Mimikatz, PowerSploit y ProcDump, durante las campañas.

Antes de cifrarlos, los operadores de Maze pueden exfiltrar los archivos para aprovechar mejor la obtención del pago del rescate deseado. Estos archivos, o las amenazas de exponerlos, se publicaron en un sitio de filtración. En 2020, las demandas de rescate de Maze tuvieron un promedio de USD 4,8 millones, un aumento significativo en comparación con la demanda de rescate promedio de USD 847 344 en todas las familias de ransomware en 2020. La comunicación directa con los operadores se llevó a cabo a través del sitio web Tor.

En noviembre de 2020, los actores de Maze anunciaron su retiro de la escena del ransomware. Sin embargo, su legado parece vivir en el ransomware Egregor, que comenzó a surgir justo antes de este anuncio. Estas acciones siguen un patrón similar al del grupo de ransomware GandCrab, que anunció su retiro en mayo de 2019, solo para regresar bajo el nombre global de REvil.

Visite el blog de Unit 42 para obtener más información sobre el ransomware Egregor o el ransomware Maze.

## Defray777

Defray777, también conocido como RansomEXX y Target777, se descubrió por primera vez en 2017. Se ejecuta por completo en la memoria y es el primer ransomware con archivos ejecutables independientes para Windows y Linux (la versión para Windows cifra todos los archivos y la variante de Linux solo cifra los directorios especificados a través de un argumento de la línea de comandos). A fines de 2020 y en 2021, los operadores de Defray777 comenzaron a mostrar su capacidad para exfiltrar datos. Los datos asociados a las víctimas de este ransomware comienzan a aparecer en la web oscura. Defray777 está relacionado con el grupo de amenazas PyXie y ha abordado a los sectores de salud, educación, manufactura, gobierno, construcción e ingeniería y alta tecnología en Estados Unidos, Canadá, Australia, Japón, Francia y Brasil.

Entre febrero y octubre de 2020, observamos a Defray777 junto con otros productos de malware, como Trickbot e IcedID. Al igual que muchas otras familias de ransomware, Defray777 se envía más comúnmente por correos electrónicos de suplantación de identidad que contienen documentos de Microsoft maliciosos o abusan de las vulnerabilidades del software. Defray777 se ejecuta con Cobalt Strike tras la instalación de malware de puerta trasera (como Vatet) y, tras el cifrado, cambia el nombre de los archivos mediante una extensión de archivo tal como .[ID exclusivo][número hexadecimal de ocho dígitos] o que contiene 777 o .txdot. Los rescates registrados para esta variante fueron de USD 16 000 a USD 42 000, demandados en bitcoins.

Visite el blog de Unit 42 para obtener más información sobre el ransomware Defray777.

## WastedLocker

Uno de los nombres más nuevos en el juego del ransomware es WastedLocker. Desde mayo de 2020, WastedLocker se ha utilizado activamente contra numerosos sectores verticales industriales, principalmente aquellos con un gran número de activos, lo que en definitiva da como resultado mayores solicitudes de rescates que rondan los USD 10 millones o más. WastedLocker está relacionado con el grupo de amenazas conocido como Evil Corp, el mismo grupo responsable de las actividades de Dridex y BitPaymer.

Entre junio y septiembre de 2020, Unit 42 observó que WastedLocker apuntaba a los sectores de tecnología de la información, servicios legales, farmacéutica, manufactura, transporte y logística en Estados Unidos y Reino Unido. Estos operadores han tenido mucho éxito con sus infecciones de ransomware gracias a algunas funciones de malware, que incluyen la capacidad de ocultarse como exploradores falsos o actualizaciones de software. WastedLocker se desarrolló con la evasión de las defensas en mente, dado que tiene la habilidad de eludir las capacidades de detección de malware en función del comportamiento en software de seguridad antimalware y cifrar de manera transparente los documentos caché en la memoria. Además, los operadores han observado el uso de herramientas disponibles estándar (como Cobalt Strike y PSExec) no solo para el acceso inicial, sino también para la enumeración del sistema, el movimiento lateral y las comunicaciones de comando y control (C2).

Visite el blog de Unit 42 para obtener más información sobre el ransomware WastedLocker.

## GandCrab + REvil

Lanzado en enero de 2018, el ransomware GandCrab perjudicó considerablemente el bolsillo de muchas organizaciones. A pesar del anuncio de retiro de mayo de 2019 y la detención de un importante distribuidor en julio de 2020, así como de un encriptador públicamente disponible para múltiples versiones de ransomware, seguimos viendo intentos de infección con GandCrab en numerosas organizaciones a lo largo del 2020. De hecho, durante noviembre de 2020, GandCrab conformó casi el 45 % de las variantes de ransomware observadas, recopiladas por la telemetría de Unit 42.

En abril de 2019, el ransomware REvil (también denominado Sodinokibi) comenzó a surgir, apuntando a los sectores de servicios legales y profesionales, manufactura, medios y comunicación, comercio mayorista y minorista, construcción e ingeniería y energía en Estados Unidos, Australia, Canadá, Finlandia y Hong Kong. Esta variante de ransomware, probablemente desarrollada por los mismos creadores de GandCrab, sigue el modelo de ransomware como servicio tradicional con una preferencia por las vulnerabilidades del RDP o la suplantación de identidad para el acceso inicial. Una vez que está en el sistema, el malware intentará iniciar solicitudes de DNS a múltiples dominios seguido de una conexión TLS 1.0 tras la resolución del DNS.

En enero de 2020, los operadores de amenazas comenzaron a utilizar métodos de doble extorsión, informando a las víctimas que expondrían públicamente los datos robados si no pagaban el rescate. Las demandas de rescates se solicitaron en bitcoins y Monero, con una fluctuación de USD 18 000 a USD 1,3 millones.

Visite el blog de Unit 42 para obtener más información sobre el ransomware GandCrab y REvil.

## NetWalker

NetWalker (a veces llamado MailTo) es otra variante de ransomware que ha expuesto datos de las víctimas comprometidas en la web oscura, con filtraciones de datos de más de 100 organizaciones en 2021. NetWalker se implementó activamente en agosto de 2019 y está dirigido a los sectores del gobierno, la salud, la manufactura, el transporte y la logística y la energía en Estados Unidos, Canadá, Arabia Saudita, Francia, Alemania, Australia, Nueva Zelanda, Suecia, Pakistán, India, Tailandia, Reino Unido, Emiratos Árabes Unidos, Colombia y Sudáfrica. Las organizaciones que fueron víctimas recibieron demandas de rescate de USD 100 000 a USD 2 millones en bitcoins.

NetWalker se basa en PowerShell y se ejecuta directamente en la memoria a través de una carga reflectante. Se ha liberado en organizaciones a través de correos electrónicos de suplantación de identidad, credenciales débiles del RDP o VPN y aplicaciones web expuestas; con frecuencia se propaga mediante la ejecución remota del Server Message Block (Bloque de mensajes del servidor, SMB) con PSExec.

En enero de 2021, se retiraron los sitios Tor que se utilizaron para comunicarse con las víctimas de NetWalker en un esfuerzo coordinado con las autoridades judiciales internacionales. NetWalker respalda el modelo de afiliado del ransomware. A pesar de que muchas de las víctimas infectadas se comunicaron con los operadores a través de Tor, en al menos un caso, las víctimas recibieron comunicaciones mediante el correo electrónico estándar. Es posible que el principal sitio de comunicación haya sido removido. Sin embargo, el malware sigue existiendo, al igual que la capacidad de poner en pie nuevas formas de comprometer a las víctimas. NetWalker está relacionado con el grupo de amenazas Circus Spider.

Visite el blog de Unit 42 para obtener más información sobre el ransomware NetWalker.

## DoppelPaymer

Otra variante de ransomware que surgió en 2019 y se mantuvo sólida en 2020 es DoppelPaymer, un conocido descendiente del ransomware BitPaymer.

Para su vector de infección inicial, se ha observado que DoppelPaymer usa actualizaciones de software falsas. Una vez que se descarga y ejecuta, la actualización falsa se descarga y ejecuta como malware de segundo grado, por ejemplo, Dridex en un sistema infectado. También se observó el uso de herramientas disponibles posteriores a la explotación, como Cobalt Strike, PowerShell Empire y Mimikatz, durante las infecciones de DoppelPaymer, al igual que PSExec (específicamente para facilitar el movimiento lateral dentro de los entornos comprometidos). Adicionalmente, se ha observado una herramienta llamada Process Hacker, que puede usarse para finalizar los procesos y servicios de seguridad en estos incidentes.

En cuanto a los enfoques para las víctimas, los operadores de DoppelPaymer se han subido a la tendencia de la doble extorsión. En febrero de 2020, lanzaron un sitio de filtración, amenazaron con vender los datos a la web oscura e incluso crearon una cuenta de Twitter para la exposición general. Además, según el FBI, los operadores de DoppelPaymer han llamado a las víctimas para presionarlas a fin de que paguen los rescates.

En términos de víctimas, los operadores de DoppelPaymer han abordado a gobiernos locales y estatales además de industrias, entre ellas, comercio mayorista y minorista, manufactura, finanzas, seguros, transporte y logística, alta tecnología, hotelería y bienes raíces dentro de Estados Unidos, Canadá, México, Sudáfrica, Bélgica, Italia, Noruega y Alemania. Las demandas de rescates de DoppelPaymer para 2020 fueron relativamente altas, desde USD 50 000 hasta USD 1,5 millones, inicialmente solicitadas en bitcoins. DoppelPaymer está posiblemente relacionado con el grupo de amenazas Indrik Spider.

Visite el blog de Unit 42 para obtener más información sobre el ransomware DoppelPaymer.

## Dharma

Una de las familias de ransomware más antiguas que aún vemos con implementación activa, Dharma (conocido también como CrySIS y Wadhrama) se identificó por primera vez de manera pública en 2016. Este ransomware generalmente se esparce a través de archivos de instalación de software falsos o correos electrónicos de suplantación de identidad y aprovecha los servidores del RDP débiles o inseguros. Dharma intenta aumentar los privilegios mediante el uso de SMB. Los archivos con frecuencia se cifran con la extensión .cezar. Sin embargo, se han observado muchas otras extensiones de archivos después del cifrado. El código fuente de Dharma se ha ofrecido a la venta en foros de ciberataques por tan solo USD 2000. Un código fuente disponible para malware como el de Dharma podría implicar una mayor personalización de otro malware, lo que generaría infecciones más dañinas y exitosas.

Dharma apuntó a los sectores de seguros, transporte y logística, alta tecnología, salud y gobierno en Estados Unidos, Italia, Japón e India con un enfoque en las pequeñas y medianas empresas. Las demandas de rescates varían muchísimo, con un mínimo de USD 1000 y un máximo de USD 150 000, solicitadas en bitcoins. Estos operadores parecen preferir comunicarse con las víctimas por correo electrónico estándar. En lugar de usar un servicio anonimizador, como Tor, al igual que muchas otras familias de ransomware, Dharma usa varios servicios gratuitos de correo electrónico, como Tutanota, Gmail, Foxmail y ProtonMail.

Visite el blog de Unit 42 para obtener más información sobre el ransomware Dharma.

## Phobos

Otro perpetrador que surgió en la escena del ransomware en diciembre de 2019 es el ransomware Phobos. Posiblemente sea una variante del ransomware Dharma que aprovecha la suplantación de identidad con URL o documentos de Word maliciosos y credenciales del RDP débiles o comprometidas para acceder al sistema. Phobos ha utilizado SMBv2 para el movimiento lateral. Los archivos a menudo se cifran con la extensión .phobos, pero se han observado otras extensiones con el tiempo que usan el formato .[ID][correo electrónico].[extensión]. Los operadores de Phobos también pueden ofrecer descifrar uno o más archivos como prueba de su capacidad de descifrado y lo harán gratuitamente como gesto de buena fe.

En 2020, Phobos abordó a las empresas pequeñas y medianas en los sectores de finanzas, educación, manufactura, servicios legales y profesionales, seguros, alta tecnología, construcción e ingeniería, salud y energía en Estados Unidos, Portugal, Brasil, Seychelles, Rumania, Indonesia, Alemania y Japón. Las demandas de rescates se solicitaron en bitcoins con una fluctuación de USD 8000 a USD 50 000.

Visite el blog de Unit 42 para obtener más información sobre el ransomware Phobos.

## Zeppelin

El ransomware Zeppelin, una posible variante de Buran/VegaLocker, se ha utilizado activamente desde al menos noviembre de 2019. Este ransomware puede implementarse en múltiples configuraciones y crea dos claves de registro distintas para almacenar la clave de cifrado. Estas claves son muy diferentes y contienen de manera visible la cadena "Zeppelin" en ellas.

En 2020, Zeppelin abordó los sectores de salud, alta tecnología, manufactura, finanzas y bienes raíces en Estados Unidos, Canadá, Bulgaria, Japón, Corea del Sur, Francia y Taiwán. Principalmente, Zeppelin se implementó mediante el uso de servidores débiles del RDP, anuncios web maliciosos y correos electrónicos de suplantación de identidad con temática de facturación con macros maliciosas. También se debe tener en cuenta que esta variante de ransomware comprueba específicamente la dirección IP de un sistema en ejecución y no se ejecutará por completo si un sistema determinado parece estar ubicado en Bielorrusia, Rusia, Ucrania o Kazajistán. Esto indica que los operadores pueden estar cerca de estas regiones o en ellas.

Al igual que otras familias de ransomware, Zeppelin ha demostrado su capacidad de doble extorsión y su interés en la exfiltración de documentos antes de vender los datos cifrados en la web oscura. Las demandas de rescate de Zeppelin tuvieron montos relativamente consistentes en cada sector industrial abordado, con variaciones de USD 13 000 a USD 35 000 solicitados en bitcoins.

Visite el blog de Unit 42 para obtener más información sobre el ransomware Zeppelin.

# Resumen del ransomware de 2020

La tabla 2 recopila los detalles clave de la sección "Principales variantes de ransomware de 2020".

**Tabla 2: Resumen del ransomware de 2020**

| Nombre (+ variantes/alias) | Modo de operación | Entrega típica (aparte de la suplantación de identidad) | Industrias comunes | Países comunes | Demanda del rescate (USD) + tipo de pago | Doble extorsión presenciada | Evaluación de la amenaza |
|---|---|---|---|---|---|---|---|
| Ryuk | Ametralla y ora | Productos de malware (p. ej. Trickbot, BazaLoader, Emotet); usa técnicas de explotación contra software de endpoints | Gobierno, salud, energía, alta tecnología | Estados Unidos, Reino Unido, Canadá | USD 600 000-10 millones, bitcoins | No | Haga clic aquí |
| Maze (ChaCha) | Ataque dirigido | RDP; servicios externos vulnerables; kits de exploits tales como Spelevo | Finanzas, salud, transporte/logística, alta tecnología, telecomunicaciones, construcción/ ingeniería, medios/ comunicación, et al. | Estados Unidos, Reino Unido, Canadá, Francia, Suiza | Promedio de USD 4,8 millones, bitcoins | Sí | Haga clic aquí |
| Defray777 (RansomEXX, Target777) | Ataque dirigido | Vulnerabilidades de software | Salud, educación, manufactura, gobierno, construcción/ ingeniería, alta tecnología | Estados Unidos, Canadá, Australia, Japón, Francia, Brasil | USD 16 000-USD 42 000, bitcoins | Sí | Haga clic aquí |
| WastedLocker | Ataque dirigido | Oculto en actualizaciones de software legítimas | Alta tecnología, servicios legales/ profesionales, farmacéutica, manufactura, transporte/logística | Estados Unidos, Reino Unido | Más de USD 10 millones, bitcoins | No | Haga clic aquí |
| GandCrab + REvil (Sodinokibi) | Ataque dirigido | RDP | Servicios legales/ profesionales, manufactura, medios, comercio mayorista/minorista, construcción/ ingeniería, energía | Estados Unidos, Australia, Canadá, Finlandia, Hong Kong | USD 18 000-USD 1,3 millones, bitcoins y Monero | Sí | Haga clic aquí |
| NetWalker (MailTo) | Ataque dirigido | RDP; VPN y aplicaciones web expuestas | Gobierno, manufactura, salud, transporte/logística, energía | Estados Unidos, Canadá, Arabia Saudita, Francia, Alemania, Australia, Nueva Zelanda, Suecia, Pakistán, India, Tailandia, Reino Unido, Emiratos Árabes Unidos, Colombia, Sudáfrica | USD 100 000-USD 2 millones, bitcoins | Sí | Haga clic aquí |
| DoppelPaymer (BitPaymer) | Ataque dirigido | Instaladores de software falsos; Dridex | Gobierno, comercio mayorista/minorista, manufactura, finanzas, seguros, transporte/logística, alta tecnología, hotelería, bienes raíces | Estados Unidos, Canadá, México, Sudáfrica, Bélgica, Italia, Noruega, Alemania | USD 50 000-USD 1,5 millones, bitcoins | Sí | Haga clic aquí |

| Tabla 2: Resumen del ransomware de 2020 (continuación) | | | | | | | |
|---|---|---|---|---|---|---|---|
| Nombre (+ variantes/alias) | Modo de operación | Entrega típica (aparte de la suplantación de identidad) | Industrias comunes | Países comunes | Demanda del rescate (USD) + tipo de pago | Doble extorsión presenciada | Evaluación de la amenaza |
| Dharma (CrySIS, Wadhrama) | Ametralla y ora | RDP; instaladores de software falsos | Seguros, transporte/ logística, salud, gobierno | Estados Unidos, Italia, Japón, India | USD 1000-USD 150 000, bitcoins | No | Haga clic aquí |
| Phobos (Dharma) | Ametralla y ora | RDP | Finanzas, educación, manufactura, servicios legales/ profesionales, seguros, alta tecnología, construcción/ ingeniería, salud, energía | Estados Unidos, Portugal, Brasil, Seychelles, Rumania, Indonesia, Alemania, Japón | USD 8000-USD 50 000, bitcoins | No | Haga clic aquí |
| Zeppelin (Buran/ VegaLocker) | Ametralla y ora | RDP | Salud, alta tecnología, manufactura, finanzas, bienes raíces | Estados Unidos, Canadá, Bulgaria, Japón, Corea del Sur, Francia, Taiwán | USD 13 000-USD 35 000, bitcoins | Sí | Haga clic aquí |

# El futuro del ransomware

Si revisamos las actividades de 2020 y miramos retrospectivamente en los últimos años, es fácil ver las tendencias actuales del ransomware y qué componentes se han detectado antes de lo esperado.

## Modelo de ransomware como servicio

La facilidad de éxito de los ataques de ransomware nos indica que seguirán apareciendo en escena más operadores motivados financieramente. Adversarios de todo tipo buscan constantemente organizaciones para abordar y saben que el ransomware no es solo eficaz, sino también sencillo, especialmente cuando se aplica el modelo de ransomware como servicio. Esperamos que más operadores sigan este modelo por muchas sumas de dinero.

## Aumento en las variantes y habilidades

Algunas de las familias de ransomware más prevalentes que observamos durante 2020 tienen menos de un año. Las variantes nuevas y actualizadas de ransomware seguirán desarrollándose e implementándose para usarse como malware independiente o con productos de malware. Adicionalmente, con Linux como uno de los objetivos más atacados, queda claro que los adversarios seguirán ampliando su capacidad para atacar todo tipo de sistemas.

## Mayor adopción de la doble extorsión

Las técnicas de evidencia de compromiso y doble extorsión también tenían menos de un año al inicio de 2020, pero ha explotado su popularidad. Hay al menos 16 variantes de ransomware diferentes que en este momento amenazan con exponer los datos o utilizar los sitios de filtración; más variantes probablemente continuarán con esta tendencia. En este sentido, el uso de Tor y otros servicios anónimos seguirá creciendo. El uso de los servicios anonimizados dificulta el seguimiento de las actividades y la identificación de los indicadores que los investigadores de seguridad y las autoridades judiciales pueden usar para defender las redes.

## Mayor demanda de rescates

La mayor demanda de rescate aumentó de USD 500 a más de USD 30 millones en tan solo unos años (se duplicó de USD 15 millones en 2019 a USD 30 millones en 2020). Siempre que los atacantes obtengan el pago, las demandas seguirán aumentando. Muy pocos operadores demandan rescates que no sean divisas virtuales; por lo general, prefieren bitcoins, aunque también solicitaron Monero en varios incidentes observados.

## Uso continuo de lo que es familiar

Gran parte del éxito de estos operadores reside en la capacidad de evadir la detección. Los adversarios seguirán infiltrando las redes mediante las credenciales débiles y la suplantación de identidad tradicional, además de las herramientas nativas dirigidas a los entornos. Estas incluyen el uso de regímenes posteriores a la explotación, como Cobalt Strike, PowerShell Empire y PowerSploit.

# 03

# Conclusión y recomendaciones

Protegerse contra los ataques de ransomware es similar a protegerse contra cualquier malware. Sin embargo, representa un riesgo mucho mayor para la organización.

## Acceso inicial

El acceso inicial es relativamente uniforme en todas las variantes de ransomware. Las organizaciones deben mantener la capacitación y sensibilización de los usuarios respecto de la seguridad del correo electrónico, además de considerar formas de identificar y corregir los correos electrónicos maliciosos ni bien entran en los buzones de correo de los empleados. Las organizaciones también deben garantizar la correcta administración de parches y la revisión de los servicios que puedan estar expuestos a Internet. Los servicios de escritorio remoto deben configurarse de manera segura y correcta, siguiendo el principio de menor privilegio siempre que sea posible, con una política vigente para detectar patrones asociados a ataques de fuerza bruta.

## Copias de respaldo y procesos de recuperación

Las organizaciones deben seguir respaldando sus datos y mantener un proceso de recuperación adecuado vigente. Los operadores de ransomware atacarán las copias de respaldo en el sitio para cifrarlas, por lo que las organizaciones deben asegurarse de que todas las copias de respaldo estén seguras fuera de línea. Deben implementarse y repasarse los procesos de recuperación con los principales interesados para minimizar el tiempo de inactividad y el costo para la organización en el caso de un ataque de ransomware.

## Controles de seguridad

Las formas más eficaces de protegerse del ransomware son la seguridad de los endpoints, el filtrado de URL o la protección web, la prevención de amenazas avanzada (amenazas desconocidas/sandboxing) y las soluciones contra la suplantación de identidad implementadas en todos los entornos y dispositivos comerciales. Si bien esto no garantiza por completo la prevención, reduce drásticamente el riesgo de infección de variantes comunes y ofrece medidas provisionales que permiten que una tecnología brinde una línea de defensa cuando otras no son eficaces.

## Capacidades de Palo Alto Networks

Los servicios de seguridad entregados en la nube permiten que miles de clientes de la red de diferentes tecnologías de seguridad coordinen la inteligencia y brinden una protección consistente en todos los vectores de ataque. Implementados en nuestra variedad de firewalls de nueva generación con ML (hardware PA-Series, software VM-Series y CN-Series, y Prisma® Access entregado en la nube), nuestros servicios eliminan las brechas de cobertura generadas por las herramientas de seguridad de redes dispares:

- El servicio de prevención de malware WildFire® detecta actividades asociadas con variantes de ransomware conocidas y desconocidas, así como otras amenazas basadas en archivos.
- El filtrado de URL puede configurarse para bloquear el acceso a las URL en categorías sospechosas, lo que evita que un host llegue a un servidor web a través de un HTTP que Palo Alto Networks considera que aloja malware/contenido sospecho.
- Threat Prevention aprovecha la visibilidad del firewall para inspeccionar todo el tráfico y prevenir de forma automática las amenazas conocidas, independientemente del puerto, el protocolo o el cifrado SSL, confrontando las amenazas en cada fase del ataque. Este servicio también puede detectar ataques de fuerza bruta cuando se habilita el perfil de protección de vulnerabilidades.
- La data loss prevention (prevención de pérdida de datos, DLP) empresarial evita la fuga de datos confidenciales de una organización de la red empresarial.

Cortex® XDR™ contiene un módulo antiransomware, prevención de exploits y un módulo antimalware para abordar las actividades basadas en el cifrado asociadas con el ransomware y otros productos de malware y para detectar el movimiento lateral. La detección de análisis local y la protección de amenazas conductual identifican las actividades anómalas y los archivos maliciosos.

Cortex XSOAR ayuda a acelerar la detección y corrección cuando el ransomware se detecta a través de la automatización de todo el proceso del usuario y el enriquecimiento de los datos del host, bloqueando los indicadores maliciosos y aislando o poniendo en cuarentena los endpoints y usuarios infectados.

Visite la Cyberpedia de Palo Alto Networks para leer más sobre la prevención del ransomware.

# Acerca de

## Respuesta a incidentes e inteligencia de amenazas Unit 42

Unit 42 reúne un grupo selecto de investigadores cibernéticos y encargados de responder a incidentes a fin de proteger nuestro modo de vida digital. Gracias a una muy buena reputación en cuanto a la entrega de inteligencia de amenazas lídel del sector, Unit 42 ha expandido su alcance para ofrecer respuesta a incidentes y servicios de gestión de riesgo cibernético de vanguardia. Nuestros consultores actuarán como socios de confianza para responder y contener rápidamente las amenazas de manera tal que usted pueda centrarse en su negocio.

## Cortex

Cortex® es un paquete de operaciones de seguridad de Palo Alto Networks que ofrece respuesta y detección extendidas mediante Cortex XDR, respuestas a vulneraciones de datos de expertos de Unit 42 y más.

Cortex XDR™ es una solución de seguridad terminal basada en el comportamiento e impulsada por la IA que fusiona datos de los endpoints, redes y nubes para un conocimiento total de la situación del host.

Cortex XSOAR es la plataforma de respuesta, automatización y organización de la seguridad (SOAR) más integral de la industria que ayuda a automatizar la investigación y la respuesta para desactivar rápidamente el ransomware y limitar su impacto en la red.

## Strata

Servicios de seguridad entregados en la nube que se integran a la perfección con la plataforma de firewall de nueva generación de Palo Alto Networks líder en la industria para coordinar la inteligencia y proporcionar protecciones en todos los vectores de ataque.

# Metodología

Los equipos de inteligencia de amenazas Unit 42 y de respuesta a incidentes colaboraron a fin de crear este informe de amenazas de ransomware. La información en este informe se derivó del análisis de datos de amenazas disponibles para el año calendario 2020 y una mirada retrospectiva a 2015-2019, cuando fue relevante.

Los investigadores de Unit 42 analizaron los datos disponibles de sitios de filtración de ransomware en la web oscura y sitios web públicos, los datos disponibles de amenazas globales a través de fuentes internas y externas, y los datos de respuesta a vulneraciones provistos por el equipo de respuesta a incidentes Unit 42 para Estados Unidos, Canadá y Europa.

### AutoFocus

El servicio de inteligencia de amenazas contextual AutoFocus™ brinda la inteligencia, el análisis y el contexto requeridos para comprender los datos de las amenazas a la red.

El siguiente conjunto de datos se utilizó para determinar las principales variantes de ransomware de 2020 como se detalla aquí conforme a Unit 42:

Sesiones de red analizadas

**19 568**

Muestras exclusivas de malware

**164**

## Respuesta a incidentes Unit 42

Los servicios de respuesta a vulneraciones de datos de Unit 42 están disponibles para cualquier incidente de ciberseguridad, incluidas infecciones de ransomware. En un ataque de ransomware, los investigadores de Unit 42 realizaron análisis forenses de expertos para contener rápidamente el ataque y proporcionar a las víctimas información sobre respuestas clave a fin de garantizar la restauración rápida y eficaz de las operaciones.

Para los años calendarios 2019 y 2020, el siguiente conjunto de datos, que incluye empresas de todos los tamaños en muchos sectores verticales industriales con datos seleccionados que datan desde 2015, se utilizó para revisar las tendencias en las actividades de ransomware en Estados Unidos, Canadá y Europa:

### Investigaciones sobre ransomware

**252**

## Sitios de filtración de ransomware

Unit 42 revisó datos entre enero de 2020 y enero de 2021 que estaban disponibles en sitios de filtración públicos y la web oscura para determinar la comprensión de las organizaciones extorsionadas por los operadores de ransomware. Los datos analizados para este informe son un resumen del siguiente conjunto de datos:

### Víctimas

**337**

### Industrias víctimas

**56**

### Regiones víctimas

**5**

### Países víctimas

**39**

UNIT 42™
BY PALO ALTO NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Teléfono principal: +1-408-753-4000
Ventas: +1-866-320-4788
Asistencia: +1-866-898-9087

www.paloaltonetworks.com