El ransomware en 2021: datos, principales ataques y grupos más activos

ESET analiza por qué el ransomware se convirtió en la amenaza informática que más preocupación genera a nivel global, tanto a empresas de todas las industrias como a organismos públicos. El dinero recaudado por estas bandas criminales sigue en ascenso y los montos demandados por los rescates también, lo que demuestra que continúa siendo un negocio rentable y atractivo para los cibercriminales.

Según datos revelados por la oficina de Control de Crímenes Financieros (FinCEN) de los Estados Unidos, solo en este país, entre enero y junio de este año el promedio mensual de transacciones en Bitcoin que se sospecha están relacionadas con el ransomware es de 66.4 millones de dólares. Como ejemplo, en el ataque a Kaseya, los operadores detrás del ransomware REvil demandaron un pago de 70 millones de dólares por la herramienta de descifrado para que las víctimas pudieran recuperar los archivos secuestrados.

La cantidad de ataques de ransomware casi se duplicó en 2021. Hasta el mes de noviembre se habían registrado más de 2300 organizaciones víctimas cuyos nombres fueron publicados en sitios de la Dark web controlados por los atacantes, mientras que en 2020 se registraron cerca de 1300 organizaciones víctimas, informó DarkTracer.

"Algunas de las bandas detrás de estos códigos maliciosos concentran la mayor cantidad de víctimas y generalmente son las que gozan de una mayor reputación, lo cual les permite demandar elevadas sumas de dinero. Sin embargo, la realidad indica también que existen muchos otros grupos de ransomware que también operan bajo el modelo de ransomware-as a-service (RaaS), que tienen menor actividad y reputación, pero que también conforman la escena bastante saturada del ransomware en la actualidad", comenta Camilo Gutiérrez Amaya, Jefe del Laboratorio de Investigación de ESET Latinoamérica. Teniendo en cuenta la heterogeneidad de estos grupos en cuanto a cantidad de víctimas, número de afiliados, reputación y demás, según datos de Coveware correspondientes al tercer trimestre de 2021, el monto promedio que las víctimas pagan por un ataque de ransomware es de 139.739 dólares.

Ataques de ransomware qué más repercusión tuvieron en 2021:

- El ataque a Colonial Pipeline, la compañía de oleoducto más importante de Estados Unidos, sufrió por parte del ransomware DarkSide en mayo y provocó el corte de suministro de combustible en gran parte de los Estados Unidos.
- El sufrido por Kaseya, donde el grupo REvil aprovechó una vulnerabilidad zero-day en el software de gestión de TI Kaseya VSA (utilizado comúnmente por proveedores de servicios administrados) y mediante un ataque de cadena de suministro utilizando un instalador de una actualización automática del software, comprometieron a más de 1500 compañías en varios países. Luego, demandaron la millonaria cifra de 70 millones de dólares por un descifrador para todas las víctimas.

- Más allá de estos casos, han sido varios los ataques de ransomware que en 2021 tuvieron un gran impacto por la magnitud de sus víctimas y las consecuencias. Por ejemplo, el que sufrió la empaquetadora de carne norteamericana, JBS, por parte de REvil, el ataque de Conti al sistema de salud de Irlanda, o los ataques a las compañías de seguro CNA de Estados Unidos y AXA de Francia por parte de los ransomware Phoenix y Avaddon respectivamente. En el caso de AXA, casualmente la compañía ofrecía seguros contra ataques de ransomware y una semana antes de sufrir el incidente había dejado de ofrecer este servicio.

Según información publicada por DarkTracer, compañía que se dedica a monitorear la actividad de los grupos de ransomware en la Dark web, desde el 1 de enero de 2019 al 9 de noviembre de 2021 un total de 53 bandas de ransomware afectaron a 3.767 organizaciones.

Para comprender mejor estas cifras, entre 2019 y 2020 un total de 22 grupos de ransomware afectaron afectado a 1.315 organizaciones. Solamente en 2021 se registraron más de 2.452 organizaciones afectadas en ataques de ransomware; una cifra bastante superior a las 1315 que se registraron sumando los dos años previos y que muestra el crecimiento en la cantidad de víctimas.

Vectores de ataque más utilizados por los grupos de ransomware:

Aparte de algunos ataques en particular, como el ataque a Kaseya utilizando una zero-day en el software Kaseya VSA que demuestra la evolución del ransomware en cuanto a capacidad de estas bandas, en general los vectores para obtener acceso inicial más utilizados siguen siendo los mismos que en años anteriores es decir, ataques de phishing, explotación de vulnerabilidades o ataques al protocolo de escritorio remoto (RDP).

En el caso de la explotación de vulnerabilidades, en septiembre un grupo de investigadores publicaron una lista que recopila 42 vulnerabilidades explotadas por diferentes grupos de ransomware para lograr acceso inicial a sus sistemas, donde se incluyen 17 tecnologías diferentes.

Además, los ataques de phishing siguen siendo un recurso utilizado por los criminales y también los ataques al escritorio remoto (RDP). En este sentido, si bien en 2020 los ataques de fuerza bruta a RDP crecieron 768% entre el primer y último trimestre de 2020, en 2021 el panorama se mantuvo igual. En América Latina, por ejemplo, las detecciones de ataques de fuerza bruta a clientes RDP crecieron un 32%.

Grupos de ransomware con mayor actividad en 2021:

Las bandas más activas durante 2020 fueron Ruyk, Maze, Doppelpaymer, Netwalker, Conti y REvil. En 2021 grupos como Maze o Netwalker dejaron de operar y los grupos destacados fueron Avaddon y Conti, que en noviembre registraba un total de 599 víctimas acumuladas y se convertía en el grupo de mayor actividad en 2021. Las otras familias más activas fueron Lockbit 2.0, Pysa y REvil. Todas estas bandas cobraron muchas víctimas a nivel global, incluyendo la región de América Latina.

- Ransomware REvil (Sodinokibi): En el caso de REVil, también conocido como Sodinokibi, si bien hace poco dejó de operar, esta familia que venía en actividad desde 2019 fue responsable del ataque de Kaseya, pero también de otros ataques muy importantes. Por ejemplo, el que impactó a la compañía de alimentos JBS que decidió pagar a los atacantes 11 millones de dólares. Otro ataque de REvil que tuvo gran repercusión fue el ataque a Quanta Computer, un proveedor de Apple, así como el ataque a Sol Oriens, una empresa contratada para trabajar con la Administración Nacional de Seguridad Nuclear de los Estados Unidos (NNSA, por sus siglas en inglés), además de otras agencias federales.

Varias industrias fueron afectadas por REvil, como la industria manufacturera (19%), servicios legales (15.5%) y la industria de servicios (11,9%). En América Latina, las víctimas de REvil están en Argentina, Brasil, Colombia y México. Entre los principales vectores de acceso inicial que utiliza esta

familia aparecen los correos de phishing, servicios RDP expuestos a Internet, exploit kits y explotación de vulnerabilidades.

- Ransomware Conti: Fue detectada por primera vez en 2019 y una de las más activas en 2021. En noviembre, el número de víctimas acumuladas desde sus inicios daba cuenta que es el grupo qué más organizaciones afectó con 599. Entre los ataques qué más trascendieron en 2021 se destaca el que impactó al sistema de salud de Irlanda y que provocó la interrupción en el funcionamiento de sus sistemas, además atacó a otras 16 instituciones de salud de Estados Unidos. Sin embargo, las industrias qué más padecieron a esta banda fueron la industria manufacturera, seguida por la industria de la alimentación y en tercer lugar sectores como el financiero, servicios TI y la construcción.

Entre los principales vectores de acceso inicial que utiliza esta familia aparecen los correos de phishing, servicios RDP expuestos a Internet y explotación de vulnerabilidades. Entre los países de América Latina que sufrieron este malware figuran Argentina, Brasil, Colombia, Nicaragua, República Dominicana.

- Ransomware Lockbit 2.0: Detectada entre septiembre de 2019 y enero de 2020 bajo el nombre Lockbit y desde junio de 2021 cambió a Lockbit 2.0. Según publicaron los criminales en su sitio, esta nueva versión incluye una función para el robo de información conocida como “StealBit” que permite descargar automáticamente y de manera veloz todos los archivos de los sistemas de la víctima. Asimismo, el grupo asegura contar con el software de cifrado más rápido (373MB/s) en comparación con el que utilizan otros grupos de ransomware.

En noviembre de 2021 acumulaba un total de 348 organizaciones afectadas. Uno de los ataques más recordados fue el que impactó a Accenture y en el cual solicitaron un rescate de 50 millones de dólares. En cuanto a la forma de distribuirse, esta familia utiliza correos de phishing, servicios RDP expuestos a Internet y explotación de vulnerabilidades en software, como soluciones VPN. Entre los países de América Latina que sufrieron Lockbit 2.0 figuran Brasil, México, Perú, Venezuela, Panamá.

- Ransomware Pysa: Esta familia surgió a fines de 2019 pero tomó notoriedad a fines de 2020 con ataques a instituciones educativas, agencias gubernamentales, instituciones de salud, entre otras. En noviembre de 2021 el número de organizaciones víctimas era 307 desde sus inicios.

Los métodos de distribución más utilizados por Pysa son los correos de spearphishing y ataques al servicio de escritorio remoto (RDP).

Entre los países de América Latina que sufrieron el ransomware Pysa aparecen Argentina, Brasil, Colombia y México.

- Ransomware Avaddon: Si bien las primeras apariciones de Avaddon son de fines de 2019, no fue hasta la primera mitad de 2021 que tuvo gran actividad a nivel global, y sobre todo en América Latina, registrando víctimas en Brasil, Chile, Colombia, Costa Rica, México y

Perú. Sin embargo, dejó de operar en junio de 2021 y compartió las claves de descifrado para que las víctimas puedan recuperar los archivos.

Según el Centro de Ciberseguridad de Australia, país en el que Avaddon tuvo mucha actividad y afectó a varias organizaciones públicas y privadas, el monto promedio que solicitaban los atacantes en los rescates es de aproximadamente 40.000 dólares. En cuanto a los mecanismos de distribución más utilizados, el más común eran los correos de phishing que incluían adjuntos maliciosos, como archivos ZIP o JPG. Al igual que los otros grupos que mencionamos, también utilizó como vector de acceso la explotación de vulnerabilidades y los servicios RDP.

“Hace poco más de 30 países acordaron trabajar de forma conjunta para dar lucha contra este tipo de amenaza, lo que implica compartir información entre las fuerzas de seguridad y los centros de emergencia y respuesta ante incidentes de seguridad (CERT) de cada país, y también trabajar en mejorar los mecanismos para responder a este tipo de amenazas y promover buenas prácticas que tienen un rol clave en la actividad del ransomware. Si bien hemos visto noticias de arrestos a miembros afiliados de algunos de estos grupos como parte de operaciones internacionales, así como programas que ofrecen importantes recompensas a cambio de información sobre los actores de amenazas detrás de estos grupos, los datos de 2021 muestran un crecimiento en todos los números, por lo que probablemente la tendencia se mantenga similar en 2022”, agrega Camilo Gutiérrez Amaya, Jefe del Laboratorio de Investigación de ESET Latinoamérica.