SOPHOS
Cybersecurity delivered.

Manual de estrategias del adversario activo 2022

Los comportamientos, las tácticas y las herramientas de los ciberdelincuentes observados en 2021 por los expertos en respuesta a incidentes que trabajan en primera línea

Por **John Shier**, asesor sénior de seguridad, departamento de CTO

Monográficos de Sophos *Junio de 2022*

Introducción

El reto de defender una organización contra las ciberamenazas, que evolucionan rápidamente y cada vez son más complejas, puede ser considerable. Los adversarios continuamente adaptan y perfeccionan su comportamiento y sus herramientas, aprovechan nuevas vulnerabilidades y usan herramientas de TI cotidianas de forma indebida para evadir la detección y mantenerse un paso por delante de los equipos de seguridad.

Para los profesionales de TI y de operaciones de seguridad de una organización puede ser difícil mantenerse al día con los métodos más recientes utilizados por los adversarios. Lo es aún más cuando se trata de ataques dirigidos y activos, perpetrados por más de un autor, como cuando un agente de acceso inicial (IAB) se infiltra en los sistemas de una víctima y vende posteriormente ese acceso a una banda de ransomware que lo usará en su propio ataque.

El Manual de estrategias del adversario activo 2022 detalla los principales adversarios, herramientas y comportamientos de ataque observados en casos reales en 2021 por los gestores de respuesta a incidentes de Sophos que trabajan en primera línea. Es una continuación del Manual de estrategias del adversario activo 2021 y muestra cómo el panorama de los ataques sigue evolucionando.

El objetivo es ayudar a los equipos de seguridad a comprender qué es lo que hacen los adversarios durante sus ataques y cómo detectar y defenderse de esa actividad cuando consiguen infiltrarse en la red.

Los resultados se basan en los datos de los incidentes investigados por el equipo de Sophos Rapid Response durante 2021. En la medida de lo posible, los datos se comparan con los hallazgos de la respuesta a incidentes descritos en el Manual de estrategias del adversario activo 2021.

Datos demográficos de la respuesta a incidentes en 2021

El informe está basado en 144 incidentes que afectaron a organizaciones de todos los tamaños y de diversos sectores, situadas en EE. UU., Canadá, Reino Unido, Alemania, Italia, España, Francia, Suiza, Bélgica, Holanda, Austria, Emiratos Árabes Unidos, Arabia Saudita, Filipinas, Bahamas, Angola y Japón.

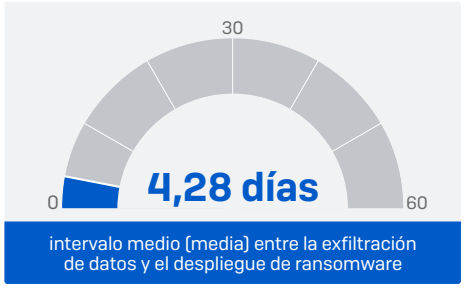
Los sectores con más representación fueron los de fabricación (17 % de los casos de respuesta a incidentes) seguido del comercio minorista (14 %), la sanidad (13 %), TI (9 %), la construcción (8 %) y la educación (6 %). En las tablas de datos al final de este informe se encuentra información adicional sobre el perfil de las víctimas.

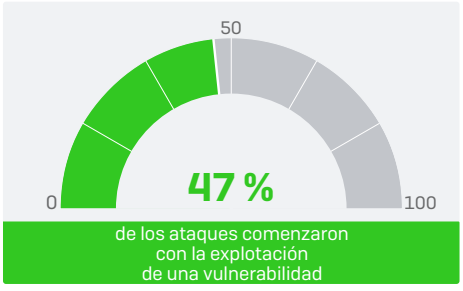
Panel de datos: anatomía de los ataques activos en 2021

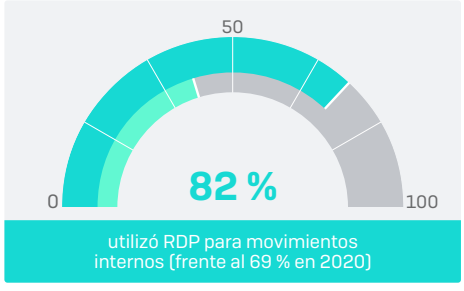
Dos de los acontecimientos en materia de ciberamenazas más influyentes del año se produjeron en marzo y agosto de 2021, con la divulgación de las vulnerabilidades ProxyLogon y ProxyShell en los servidores de Microsoft Exchange. Tal y como han indicado recientemente la CISA y otras agencias de seguridad gubernamentales, los exploits ProxyLogon/ProxyShell han sido ampliamente utilizados por los ciberdelincuentes. Por tanto, no es de extrañar que aparezcan en un número significativo de los incidentes investigados por Sophos en 2021.

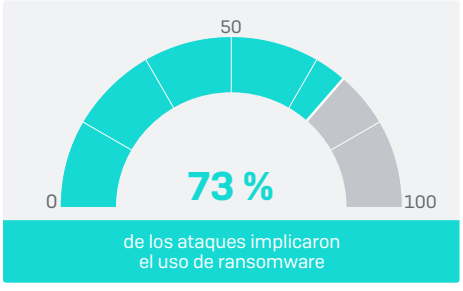
Panel de datos: anatomía de los ataques activos en 2021

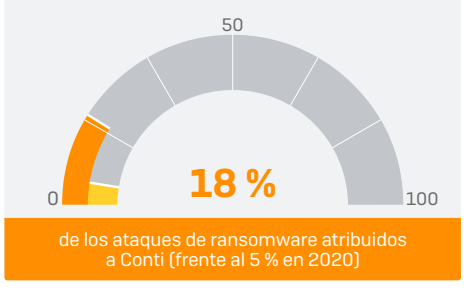
Resultados más destacados de las investigaciones de respuesta a incidentes











Probablemente haya muchas más brechas de ProxyLogon/ProxyShell que aún se desconocen, en las que se hayan implantado shells web y puertas traseras en los sistemas de las víctimas para proporcionar un acceso persistente y que ahora mismo esperan pacientemente a que ese acceso se use o venda.

Esto conduce a otra tendencia importante que ha conformado el panorama de las ciberamenazas en 2021: la influencia y el poder crecientes de los agentes de acceso inicial (IAB).

El éxito de los IAB depende de ser los primeros en infiltrarse en un objetivo y lograr un acceso que puedan vender posteriormente. En consecuencia, los IAB son también los primeros en aparecer en cuanto surgen nuevos errores, con la esperanza de comprometer los sistemas de las víctimas antes de que se apliquen los parches de forma generalizada. Su objetivo es afianzar su posición en la red de la víctima y posiblemente realizar algunos movimientos de exploración iniciales para hacerse una idea del valor de los activos antes de vender el acceso a otros adversarios, como los operadores de ransomware, que lo usarán para lanzar ataques, a veces meses después de la intrusión inicial.

Como se destacó en el Informe de amenazas 2022 de Sophos, el aumento de los IAB refleja la creciente "profesionalización" de los ataques en un mercado de ciberamenazas con un número cada vez mayor de proveedores de servicios especializados. El auge de la industria del ransomware como servicio (RaaS) es otro ejemplo de esta tendencia.

Por último, pero no por ello menos importante, las evidencias forenses halladas durante las investigaciones de respuesta a incidentes en 2021 han relevado casos en que la misma organización sufrió ataques a manos de múltiples adversarios de forma simultánea, incluyendo IAB, bandas de ransomware, criptomineros y, ocasionalmente, incluso varios operadores de ransomware. Esta es una tendencia que continuará conformando el panorama de las ciberamenazas en 2022 y años sucesivos.

El tiempo que los intrusos pasan en las redes de sus víctimas está aumentando, probablemente debido a este tipo de actividad. Otros adversarios que adoptan estrategias a largo plazo y que pueden estar (a veces simultáneamente) en las redes de las víctimas durante un periodo prolongado son los desarrolladores de botnets y los hackers que usan plataformas de distribución de malware o droppers.

A continuación desarrollamos todas estas tendencias en profundidad.

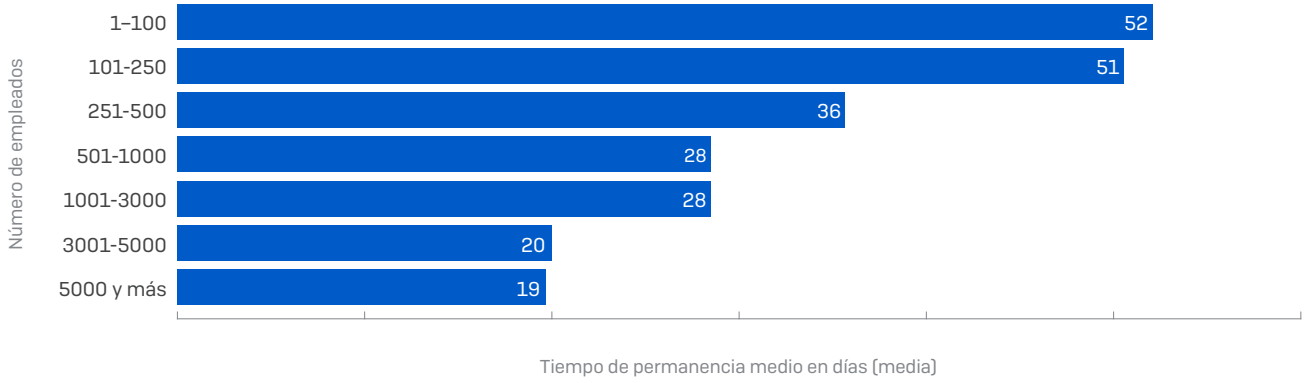
Los intrusos invisibles

Los datos de los incidentes muestran que la mediana del tiempo de permanencia aumentó aproximadamente un tercio entre 2020 y 2021, de 11 días a 15. Sí hay variaciones considerables: los ataques que culminaron en ransomware tuvieron tiempos de permanencia más cortos, aproximadamente 11 días de promedio (dato menor con respecto a los 18 días en 2020), y aquellos que implicaban otras intrusiones duraron significativamente más, con una mediana del intervalo de 34 días.

Variaciones en el tiempo medio de permanencia de los intrusos (mediana)

Como se ha sugerido más arriba, los tiempos de permanencia más largos pueden reflejar la involucración de un IAB. En el caso de negocios o sectores industriales más pequeños, como por ejemplo la educación (promedio de permanencia de los intrusos: 34 días), estos tiempos de permanencia más largos también reflejan lo difícil que puede ser para el personal de seguridad de TI interno buscar, investigar y responder de forma proactiva a las alertas y amenazas potenciales.

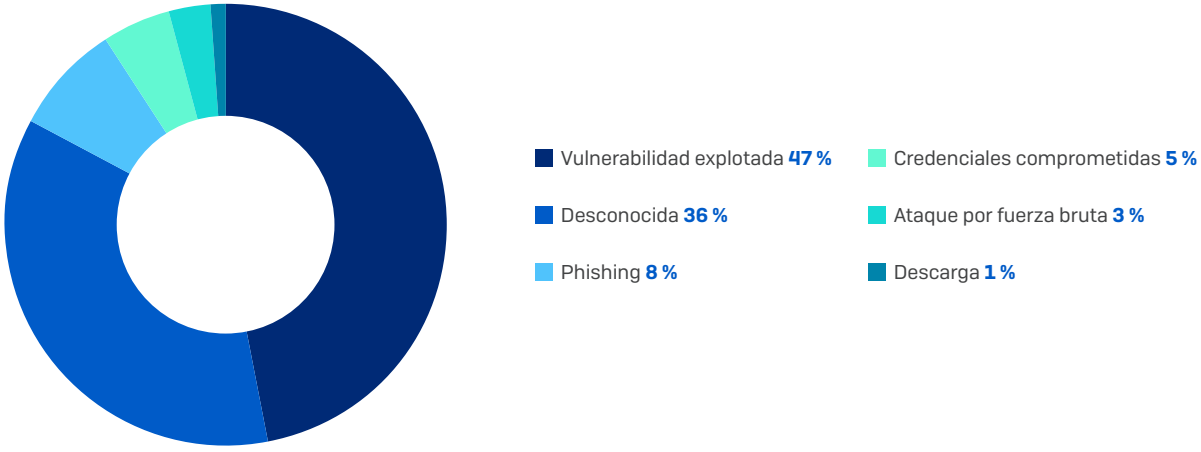
Tiempo de permanencia de los intrusos por tamaño de la empresa (media)



Las causas raíz de los ataques

No siempre es posible ni fácil identificar la causa raíz de un ataque. A veces, cuando llegan los expertos en respuesta, los atacantes ya han eliminado todo rastro de su actividad; en otros casos, los equipos de seguridad TI ya han formateado o recreado la imagen de los equipos comprometidos. A pesar de esto, las pruebas muestran que entre los incidentes investigados por Sophos, la explotación de vulnerabilidades sin parchear, como ProxyLogon o ProxyShell, fue la causa de prácticamente la mitad (47 %) de los ciberincidentes investigados en 2021.

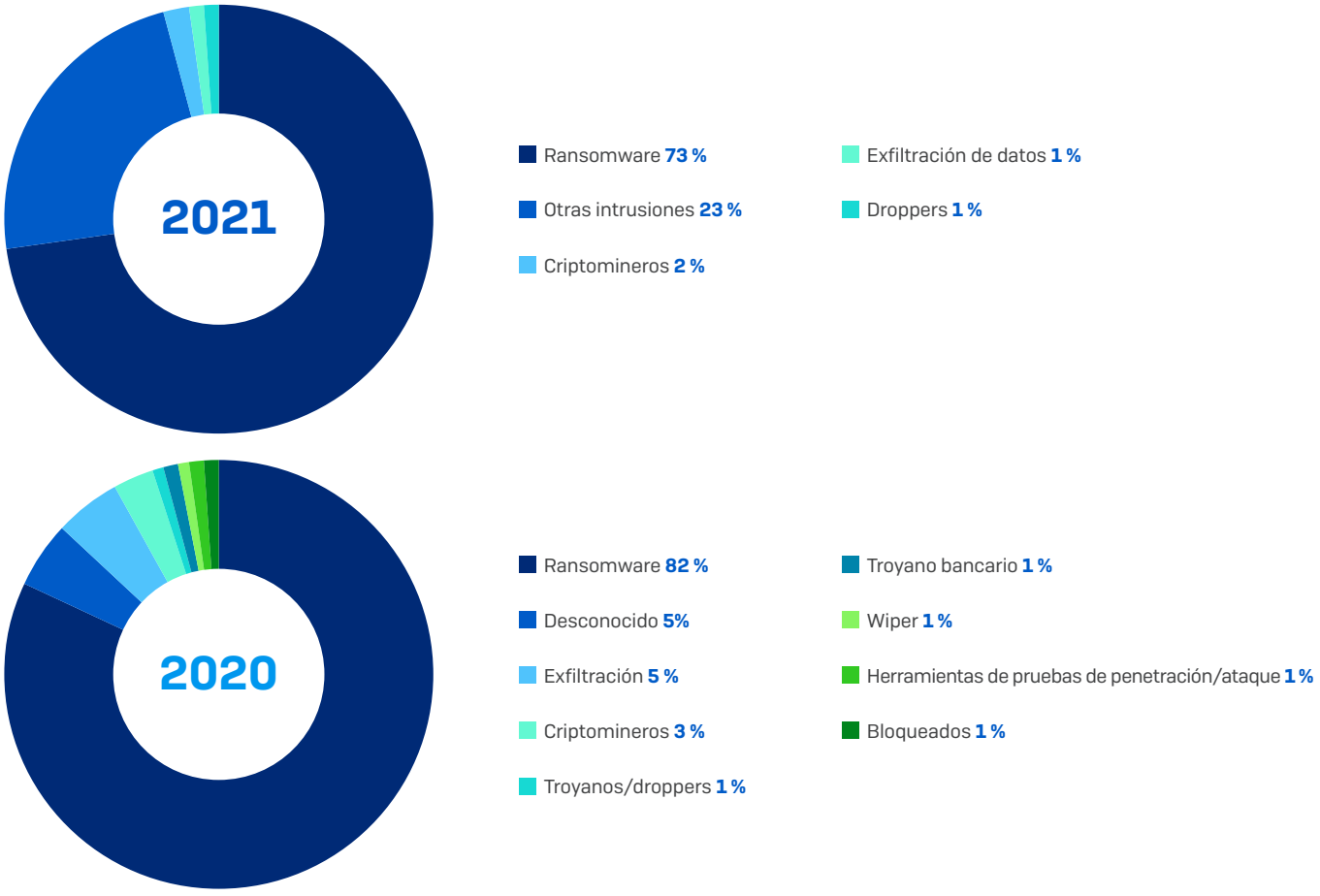
Causas raíz de los ataques



Los principales tipos de ataques

El despliegue del ransomware es frecuentemente el momento en el que los ataques se vuelven visibles a los equipos de seguridad TI. Por lo tanto, no es de extrañar que el 73 % de los incidentes a los que Sophos respondió en 2021 estuvieran relacionados con el ransomware. El ransomware también fue el tipo de ataque más predominante en 2020, con un 82 % (el porcentaje más alto probablemente refleje la menor cantidad de datos del estudio). En lo que respecta a los casos de exfiltración de datos, que representan el 1 % de los incidentes, los gestores de incidentes piensan que probablemente estos se habrían convertido en ataques de ransomware, pero que se detectaron y neutralizaron a tiempo.

Tipos de ataques



El segundo tipo de ataque más predominante detectado por las investigaciones de respuesta a incidentes fue la amplia categoría de "otras intrusiones", que representó un 23 % de los incidentes. A efectos de este informe, "otras intrusiones" son las que no han derivado en un ataque de ransomware ni ningún otro tipo de ataque con seguimiento.

Una intrusión suele ser el resultado de explotar una vulnerabilidad sin parchear, como ProxyLogon y ProxyShell, pero también incluye el uso indebido de servicios de acceso remoto o VPN no seguras, credenciales de cuenta robadas o descuidos de seguridad (como, p. ej., dejar puntos de entrada abiertos a Internet).

La cuestión importante es que las intrusiones fueron detectadas y neutralizadas antes de que pudiera desplegarse una carga maliciosa devastadora en los sistemas de la víctima. Es razonable suponer que algunas de estas intrusiones, si no la mayoría, eran inventario sobrante perteneciente a IAB: accesos "apartados" a la espera de ser vendidos a otro ciberdelincuente. Si las intrusiones no se hubiesen detectado, es probable que un número significativo de ellas se hubiese convertido en un ataque de ransomware.

Los criptomineros fueron el principal tipo de ataque en el 2 % de los incidentes investigados. La presencia de criptomineros maliciosos suele detectarse debido a su impacto en el rendimiento del sistema, ya que las actividades ilícitas de minería de criptomonedas consumen capacidad de procesamiento de los equipos. Puede resultar tentador desestimar a los criptomineros como una amenaza molesta de importancia menor, pero el hecho de su presencia en la red es prueba de que en alguna parte hay un punto de entrada vulnerable, y pueden ser precursores de amenazas más serias en el futuro.

Lo mismo ocurre con los sistemas de entrega e instaladores de malware en general, que están diseñados para distribuir, cargar o instalar otras cargas maliciosas en el sistema de la víctima. Son elementos que allanan el camino para un ataque, proporcionando una plataforma para módulos maliciosos adicionales, como puertas traseras y ransomware. Por lo tanto, los responsables de la seguridad deben tratar la presencia de droppers y sistemas de distribución de malware, como Trickbot, Emotet y otros, con la misma seriedad que un grupo de ransomware importante, ya que frecuentemente son los precursores de ataques más graves.

Un escenario concurrido

Los distintos tipos de ataque no son excluyentes entre sí. Como se ha mencionado ya antes, es posible encontrar a la vez distintos adversarios, incluyendo IAB, bandas de ransomware y criptomineros, en la red de una única víctima.

Por ejemplo, aunque los criptomineros fueron el tipo de ataque principal solo en el 2 % de los casos de respuesta a incidentes, también estuvieron presentes en el 7 % de los incidentes de ransomware. Los criptomineros suelen escanear las redes infectadas en búsqueda de otros mineros para eliminarlos, pero pueden coexistir cómodamente con otras amenazas, como el ransomware.

Entre los incidentes de ataques simultáneos detectados por Sophos en 2021 se incluyen uno relacionado con el ransomware Atom Silo y dos criptomineros, y un ataque doble de ransomware relacionado con Netwalker y REvil. Esta tendencia se mantendrá en 2022.

La caja de herramientas del adversario

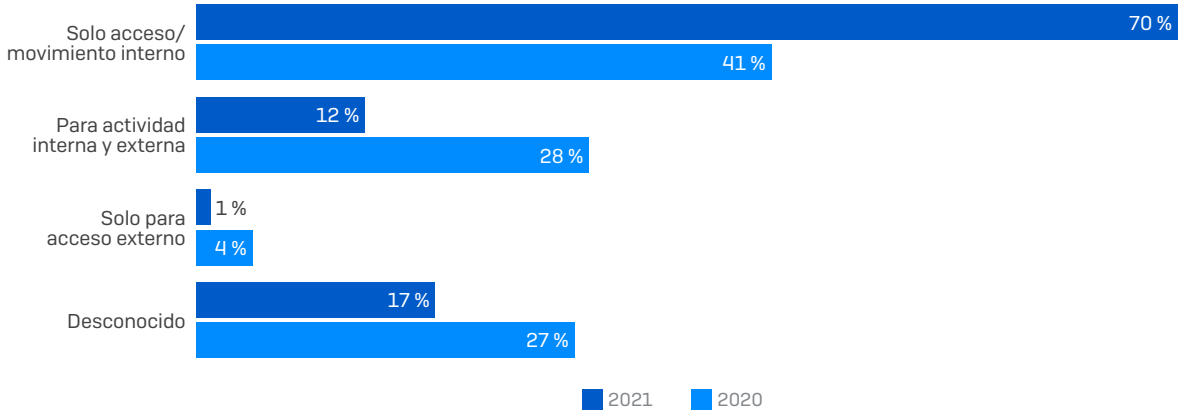
Los servicios de escritorio remoto son una de las principales amenazas internas

El protocolo RDP tuvo un papel importante en por lo menos el 83 % de los ataques, un aumento con respecto a 2020 (con una presencia del 73 % en los ataques). El uso interno se observó en el 82 % de los casos, mientras que el uso externo se detectó en el 13 % de los incidentes. En el 2020, las cifras fueron del 69 % y del 32 % respectivamente.

Sin embargo, merece la pena reseñar la forma en que los atacantes utilizan el RDP. En menos de tres cuartos (70 %) de los incidentes relacionados con el protocolo RDP, la herramienta se utilizó *solo* para el acceso interno y el movimiento lateral, un aumento significativo con respecto al 41 % en 2020.

El RDP se usó para el acceso externo en *solo* el 1 % de los casos, un descenso con respecto al 4 % en 2020; y solo el 12 % de los ataques evidenciaron que los atacantes usaban el protocolo tanto para el acceso externo como para los movimientos internos, un porcentaje que se redujo a más de la mitad en comparación con 2020 (cuando fue el 28 %).

Uso del protocolo de acceso remoto (RDP) por los atacantes



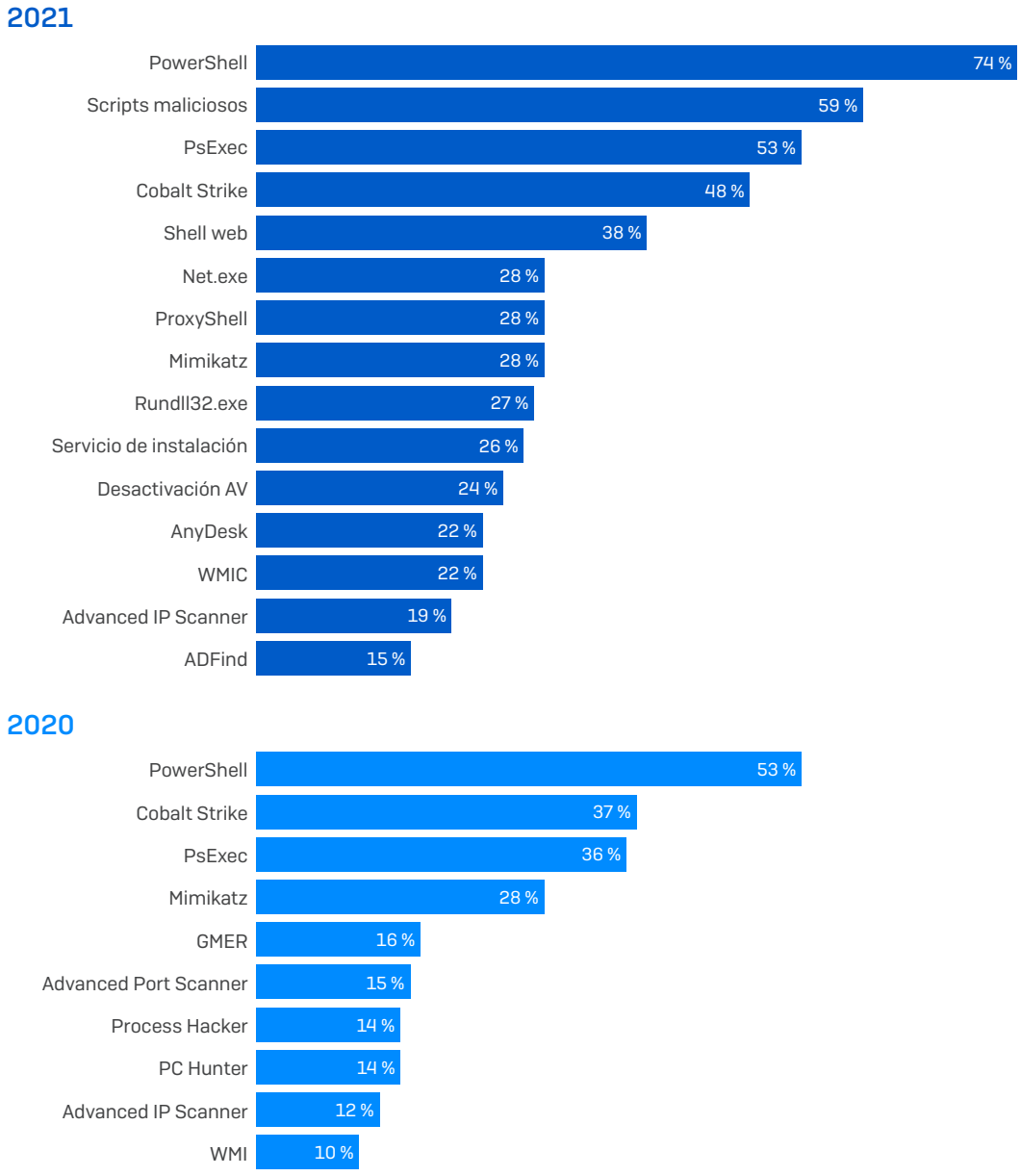
La disminución del uso del protocolo RDP para el acceso externo probablemente refleje la mejora de la seguridad, incluida la deshabilitación del servicio. Sin embargo, el RDP sigue siendo accesible dentro del perímetro de la red, y reforzar este acceso debe ser un objetivo clave para los equipos de seguridad.

El juego de herramientas de ataque en 2021

En el siguiente gráfico se muestran los "artefactos" (incluyendo herramientas, técnicas y servicios) más frecuentemente identificados en los conjuntos de herramientas de los ciberdelincuentes en 2021. Muchos de estos también pueden ser usados por los profesionales de TI para fines benignos. Gozan de popularidad entre los adversarios porque les permiten camuflar sus acciones entre las operaciones informáticas habituales de la víctima y conducir actividades como el robo de credenciales, la localización de recursos, el movimiento lateral y la ejecución de malware, entre otras.

El número y la naturaleza de los artefactos ponen de manifiesto el reto que supone para los responsables de la seguridad diferenciar entre la actividad maliciosa y la legítima en la red.

Principales artefactos utilizados en los ataques



Un análisis más profundo a los elementos más populares utilizados en los ataques revela las estrategias típicas de los ciberataques en 2021.

Los artefactos que componen los juegos de herramientas

Los artefactos identificados durante las investigaciones de respuesta a incidentes pueden dividirse en tres categorías: herramientas legítimas y de hacking, binarios de Microsoft y artefactos adicionales (scripts, técnicas, servicios, etc.).

Las investigaciones de respuesta a incidentes detectaron 525 artefactos en general, dato superior a los 132 de 2020 (aunque el tamaño de la base del estudio también ha sido más grande), incluyendo 209 herramientas legítimas y de hacking, 107 binarios de Microsoft y 209 artefactos adicionales.

Herramientas legítimas y de hacking

Aquí se incluye el software usado para asistir a los ataques. Cobalt Strike (48 %) y Mimikatz (28 %) mantienen los dos primeros puestos, como en 2020, seguidos por AnyDesk (22 %), Advanced IP Scanner (19 %) y ADFind (15 %). En comparación con 2020, Cobalt Strike ha registrado un aumento (37 % en 2021), Mimikatz se ha mantenido estable (28 %) y tres nuevas herramientas han logrado irrumpir en los cinco primeros puestos.

Cobalt Strike es una suite de herramientas de explotación producida comercialmente y diseñada para ayudar a los equipos de seguridad a recrear un amplio abanico de escenarios de ataque. Los atacantes intentan establecer una puerta trasera con la función "Beacon" de Cobalt Strike en un equipo infectado. Las funciones Beacon pueden configurarse para ejecutar comandos, descargar y ejecutar software adicional, reenviar comandos a otras cargas Beacon instaladas en la red de la víctima y comunicarse con el servidor de Cobalt Strike. Cualquier detección de Cobalt Strike en la red debe investigarse inmediatamente.

La segunda herramienta más vista, **Mimikatz**, también fue diseñada originalmente como una herramienta de seguridad ofensiva, y tiene capacidad para robar contraseñas y otras credenciales de cuentas para utilizarlas en un ataque.

Los escáneres de red legítimos como **IP Scanner** y **Advanced Port Scanner** se utilizan para generar una lista de direcciones IP y nombres de dispositivos, que permite a los atacantes centrarse en los equipos y la infraestructura más crítica de la víctima.

El uso malintencionado de la herramienta legítima de administración de TI **AnyDesk** es cada vez más popular, ya que ofrece a los atacantes un control directo sobre un equipo, incluyendo el control sobre el ratón/teclado y la posibilidad de ver la pantalla. Servicios de acceso remoto legítimos como **TeamViewer**, **Screen Connect**, **Atera RMM** y **Splashtop** también han entrado en la lista de favoritos de 2021.

Process Hacker, **PCHunter** y **GMER** son herramientas legítimas que incluyen controladores de kernel. Si un atacante logra instalar el controlador de kernel correcto, a menudo puede deshabilitar los productos de seguridad.

Binarios de Microsoft

La separación entre las herramientas de Microsoft y las herramientas genéricas muestra cómo los atacantes han desarrollado tácticas para "vivir de la tierra". Todas estas herramientas están digitalmente firmadas por Microsoft. Como es de esperar, **PowerShell** (74 %) ocupa el primer puesto en la lista, seguido por **PsExec** (53 %), "**net.ex**e" (28 %), "**rundll32.exe**" (27 %) y la herramienta de **línea de comandos WMI** (WMIC) (22 %). El uso de PowerShell, PsExec y WMIC, en comparación con 2020, ha aumentado en 2021.

La herramienta "net.exe" fue usada en muchas fases de un ataque, principalmente como herramienta de detección, mientras que "rundll32.exe" fue usada generalmente para ejecutar ataques y evadir las defensas.

Otras herramientas de Microsoft que pueden indicar que hay un atacante acechando en la red son "**whoami.exe**," el **Programador de tareas** (para mantener la persistencia) y "**schtasks.exe**" (para ejecutar código malicioso). El uso de cualquiera de estas herramientas debería supervisarse de cerca.

Artefactos adicionales

Esta categoría incluye tanto herramientas como técnicas, p. ej., intentos de deshabilitar la protección, vulnerabilidades como ProxyShell, el uso de servicios en la nube como **Mega.io**, malware adicional, infecciones secundarias y el uso de protocolos de transporte.

En el 59 % de los incidentes investigados se detectaron **scripts maliciosos** (excluyendo PowerShell). Un script malicioso es un código de software que posibilita actividad maliciosa. Entre los ejemplos de scripts usados malintencionadamente por los atacantes se incluyen scripts de ejecución por lotes y de línea de comandos de DOS/CMD, scripts de Python (un conjunto de comandos en un archivo que se ejecutan como un programa) y VBScripts (scripts de Visual Basic que se pueden ejecutar en Windows o Windows Explorer).

Las shells web fueron el segundo tipo de amenaza más común detectado (en el 38 % de los incidentes), ocupando un lugar destacado ProxyShell (28 %) y ProxyLogon (11 %). La instalación de servicios, la desactivación de la protección, el volcado de LSASS, la creación de cuentas fraudulentas, la modificación del registro y el borrado de archivos de registro completan la lista de los 10 artefactos más populares.

Exfiltración de datos

En 2021, **Rclone** entró en la lista de los artefactos más populares para la exfiltración. Rclone es una herramienta de línea de comandos que se conecta a una gran variedad de proveedores de almacenamiento en la nube, como Mega, y en 2021 fue la herramienta más usada para la exfiltración de datos. Otros proveedores de almacenamiento en la nube que aparecen en los datos de este año son **Dropbox**, **DropMeFiles**, **M247**, **pCloud** y **Sendspace**.

Además de Rclone, otras herramientas que han aparecido en las investigaciones de incidentes como medios auxiliares para la exfiltración de datos fueron **Megasync**, **FileZilla**, **Handy Backup**, **StealBit**, **WinSCP** y **Ngrok**.

La entrada de herramientas de exfiltración en la lista de favoritos de 2021 no es ninguna sorpresa si se tiene en cuenta que en el 38 % de todos los incidentes investigados hubo exfiltración de datos (27 % en 2020). Otros incidentes (8 % en general) mostraron indicios de recopilación de datos y su preparación para un posible robo. En los casos en los que hubo exfiltración, la evidencia sugiere que la información robada fue filtrada posteriormente en el 46 % de los incidentes.

Los atacantes generalmente eliminan la información en la última fase de un ataque antes de desplegar el ransomware. El análisis de incidentes de Sophos muestra que en 2021 la mediana del intervalo entre la exfiltración de datos y la distribución del ransomware fue de unas 44 horas. La media fue de algo más de 4 días (4,28 días) y la mediana estuvo algo por debajo de los dos días (1,84 días).

Independientemente del promedio que se aplique, el mensaje importante es que después de una exfiltración los responsables de la seguridad cuentan con una ventana de oportunidad potencial para prevenir que se despliegue la fase final y más dañina del ataque. Por lo que cualquier detección de herramientas conocidas por ser usadas para la exfiltración de datos debe ser investigada de forma prioritaria.

Combinaciones de herramientas

Las investigaciones de incidentes revelaron un patrón de combinaciones de herramientas en las redes de las víctimas que proporciona una valiosa señal de alerta para los equipos de seguridad TI (datos comparativos con 2020 disponibles en algunos casos):

- En 2021, PowerShell y scripts maliciosos que no son PowerShell aparecieron juntos en el 64 % de los casos
- La combinación de PowerShell y Cobalt Strike se observó en el 56 % de los casos, con respecto al 58 % en 2020
- Se detectaron PowerShell y PsExec en el 51 % de los casos, con respecto al 49 % en 2020
- Se vieron PowerShell, scripts maliciosos y Cobalt Strike en el 42 % de los casos
- Se observaron PowerShell, scripts maliciosos y PsExec en el 38 % de los casos
- PowerShell, Cobalt Strike y PsExec presentes en el 33 % de los casos, dato superior con respecto al 12 % en 2020
- Cobalt Strike y Mimikatz se vieron juntos en el 16 % de los casos

Estas correlaciones mantienen la misma importancia este año que el año pasado, porque su detección puede servir como un aviso anticipado de un ataque inminente o una confirmación de la presencia de un ataque activo.

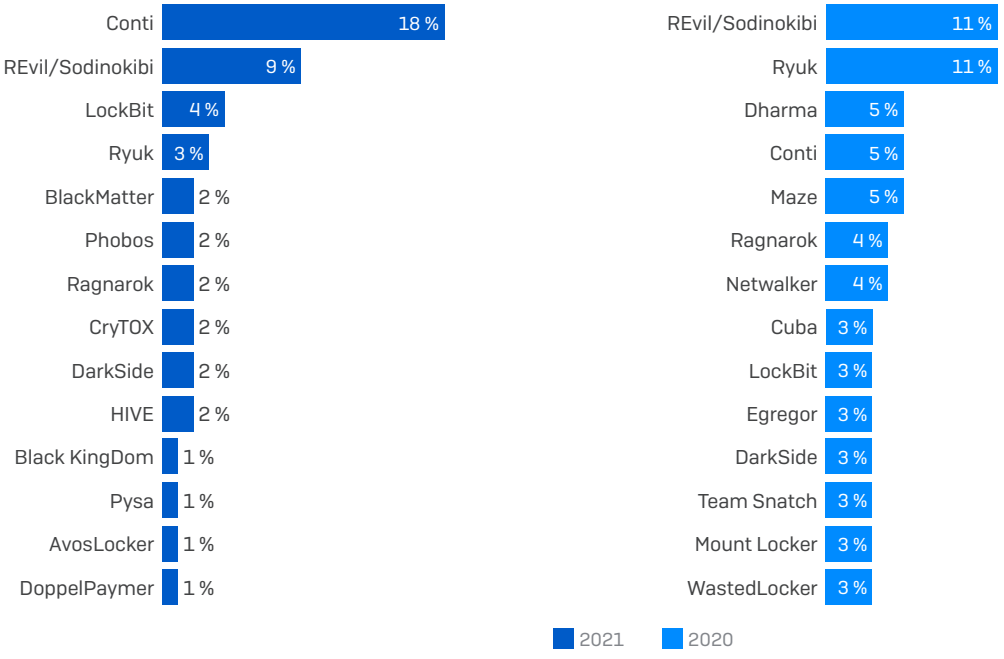
Los principales adversarios de ransomware en el 2021

En los 144 incidentes analizados, se identificaron 41 adversarios de ransomware distintos. De estos, aproximadamente dos tercios (28) fueron nuevos grupos detectados por primera vez en 2021. Dieciocho grupos de ransomware vistos en 2020 han desaparecido de la lista en 2021, una indicación clara de cómo de concurrido, dinámico y complejo se ha vuelto el panorama de las ciberamenazas, y cómo esta circunstancia puede dificultar las cosas a los encargados de la seguridad.

En muchos sentidos, 2021 "perteneció" a Conti, un prolífico operador de RaaS detrás de casi uno de cada cinco (18 %) incidentes investigados por Sophos. No obstante, cabe destacar que el ransomware REvil estuvo implicado en uno de cada 10 incidentes en general, a pesar de que aparentemente dejó de actuar en julio de 2021 (reapareciendo brevemente en septiembre de 2021 y de nuevo en 2022).

Otras familias de ransomware predominantes durante 2021 fueron DarkSide, el RaaS detrás del famoso ataque a Colonial Pipeline en los EE. UU., y Black KingDom, una de las "nuevas" familias que aparecieron en marzo de 2021 como consecuencia de la vulnerabilidad ProxyLogon.

Distribución de los principales adversarios de ransomware



Cerca de un cuarto (24 %) de los incidentes en 2021, y un 25 % en 2022, se atribuyeron a otros grupos de ransomware, mientras que los incidentes restantes no se pudieron atribuir con certeza a ningún grupo conocido.

Sophos ha informado ampliamente sobre el ransomware Conti. Una lista completa de artículos sobre Conti y otras familias prevalentes de ransomware, incluyendo LockBit, Ryuk y otras más, puede consultarse en el Centro de información sobre amenazas de ransomware de Sophos.

Conclusión

Cualquier organización puede ser la víctima elegida por un ciberdelincuente situado en algún lugar del mundo y, cada vez más, nos enfrentamos a más de un hacker. Desde phishing y fraude financiero a desarrolladores de botnets, plataformas de distribución de malware, criptomineros, IAB, robo de datos, espionaje corporativo, ransomware, etc.: si hay un punto de entrada vulnerable en una red, existe la posibilidad de que los atacantes lo busquen y acaben por encontrarlo y explotarlo.

Y hasta que ese punto de entrada no se cierre y todo lo que hayan hecho los atacantes para establecer y retener el acceso se haya erradicado completamente, cualquiera podrá entrar detrás de ellos. Y probablemente lo haga.

Los equipos de seguridad pueden defender su organización monitorizando e investigando la actividad sospechosa. La diferencia entre lo que es benigno y malicioso no es siempre fácil de establecer. La tecnología en cualquier entorno, tanto cibernético como físico, puede hacer mucho, pero no es suficiente por sí sola. La experiencia y el conocimiento humanos y la habilidad para responder son una parte vital de cualquier solución de seguridad.

Las lecciones más importantes de la respuesta a incidentes de 2021 son cómo de rápido y en qué medida los adversarios aprovechan las vulnerabilidades extendidas y fáciles de explotar, contribuyendo a intrusiones más duraderas y adversarios múltiples. Para los responsables de la seguridad, estas lecciones significan que detectar, investigar y responder a las señales de alarma de los conjuntos de herramientas y técnicas conocidas de los adversarios es más importante que nunca.

Sophos Rapid Response

Los hallazgos de este informe están basados en los datos de incidentes investigados por el equipo de Sophos Rapid Response, un equipo dedicado de gestores de respuesta a incidentes y especialistas de neutralización de amenazas. El servicio Sophos Rapid Response está disponible tanto para los actuales clientes de Sophos como para los que no lo son.

Si está sufriendo un incidente activo y desea hablar con el equipo de Rapid Response, llame a los números a continuación en cualquier momento:

EE. UU.: +1 4087461064

Australia: +61 272084454

Canadá: +1 7785897255

Francia: +33 186539880

Alemania: +49 61171186766

Reino Unido: +44 1235635329

Suecia: +46 858400610

Tablas de datos adicionales

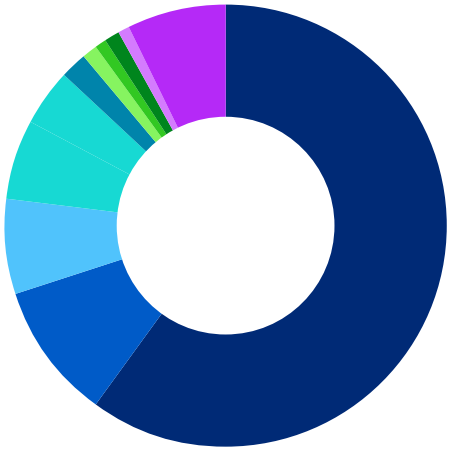
Artefactos detectados en las investigaciones de incidentes correlacionados con la cadena de ataque MITRE

Las herramientas, las técnicas y otros artefactos observados durante las investigaciones de incidentes se han correlacionado con el marco de MITRE ATT&CK. Se publicarán más detalles en un artículo relacionado en Sophos News.

Fases de ataque MITRE											
Acceso inicial	Ejecución	Persistencia	Aumento de privilegios	Evasión de defensa	Acceso a credenciales	Descubri-miento	Propagación lateral	Recopilación	Comando y control	Exfiltración	Impacto
Artefactos											
Servicios remotos	PowerShell	Cobalt Strike	Mimikatz	PowerShell	Mimikatz	Advanced IP Scanner	RDP	Exploración de la red	Cobalt Strike	Rclone	Cifrado de datos
Exploits	PsExec	AnyDesk	ProcDump	Rundll32.exe	ProcDump	Netscan	Cobalt Strike	Rclone	PowerShell	WinRAR	Infiltración en la red

Datos demográficos de la respuesta a incidentes en 2021

Casos de respuesta a incidentes por país

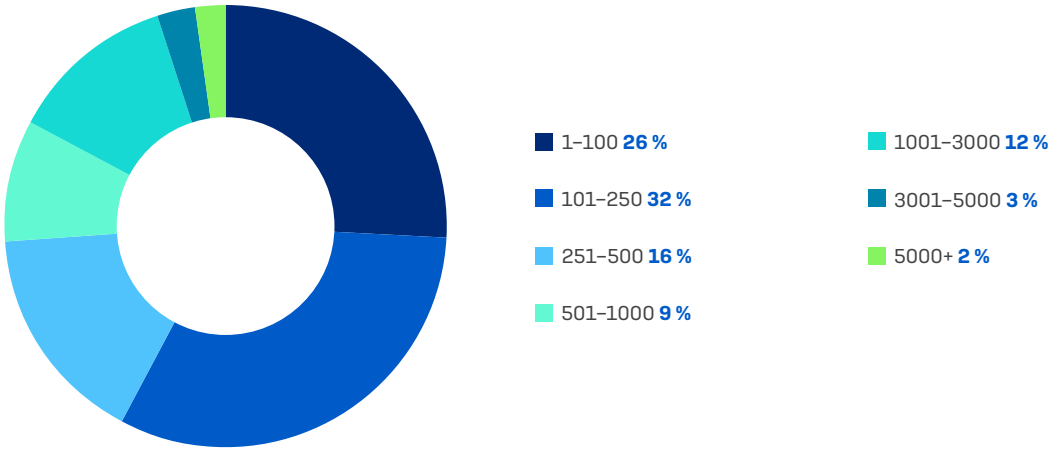


- EE. UU. **60 %**
- Alemania **10 %**
- Reino Unido **7 %**
- Canadá **6 %**
- Italia **4 %**
- España **2 %**
- Francia **1 %**
- Suiza **1 %**
- Bélgica **1 %**
- Filipinas **1 %**
- Otros **7 %** (Holanda, Austria, Emiratos Árabes Unidos, Arabia Saudita, Bahamas, Angola, Japón)

Casos de respuesta a incidentes por sector

- Fabricación **17 %**
- Comercio minorista **14 %**
- Sanidad **12 %**
- Tecnología de la información **9 %**
- Construcción **8 %**
- Educación **6 %**
- Alimentación **4 %**
- Logística **4 %**
- Finanzas **4 %**
- Entretenimiento **3 %**
- Servicios **3 %**
- Medios informativos **3 %**
- Otros **13 %** (transporte, farmacéutico, MSP/ alojamiento, sin ánimo de lucro, gobierno, hostelería, legal, agricultura, energía, inmobiliaria)

Casos de respuesta a incidentes por tamaño de la organización (número de empleados)



Ventas en España
Teléfono: (+34) 913 756 756
Correo electrónico: comercialES@sophos.com

Ventas en América Latina
Correo electrónico: Latamsales@sophos.com

25-05-2022 ES (DD)