SOPHOS

Informe de Sophos sobre amenazas 2024: ciberdelincuencia contra pymes

El ransomware sigue siendo la mayor ciberamenaza existencial para las pequeñas empresas, pero hay otras que están creciendo.

Sophos X-Ops

Contenido

Contexto

La ciberdelincuencia afecta a personas de todos los ámbitos de la vida, pero se ensaña especialmente con las pequeñas empresas. Aunque los ciberataques contra grandes empresas y agencias gubernamentales son los que más salen en las noticias, las pequeñas empresas (en un sentido amplio, organizaciones con menos de 500 empleados) suelen ser más vulnerables frente a los ciberdelincuentes y sufrir peores consecuencias, proporcionalmente, como resultado de los ciberataques. En términos generales, los factores que más contribuyen a este nivel de vulnerabilidad son la falta de personal de operaciones de seguridad con experiencia, una inversión en ciberseguridad insuficiente y unos presupuestos de TI más ajustados. Y cuando una pequeña empresa es víctima de un ciberataque, los gastos de recuperación pueden incluso obligarla a cerrar.

Las pequeñas empresas no son una cuestión menor. Según el Banco Mundial, más del 90 % de los negocios del mundo son pequeñas y medianas empresas, y suman más del 50 % del empleo en todo el planeta. En los Estados Unidos, las pymes representan más del 40 % de la actividad económica total. (En este informe, utilizaremos indistintamente los términos pequeñas y medianas empresas u organizaciones, ya que nuestros datos al respecto son muy similares).

En 2023, más del 75 % de los casos de respuesta a incidentes de los clientes gestionados por el servicio Sophos X-Ops Incident Response correspondieron a pequeñas empresas. Los datos recopilados a partir de estos casos, junto con la telemetría recabada de los clientes de nuestro software de protección para pequeñas y medianas empresas, nos brinda una visibilidad única de las amenazas a las que se enfrentan estas organizaciones todos los días.

Resumen ejecutivo

Basándonos en estos datos y en las investigaciones de Sophos sobre las amenazas, constatamos que el ransomware sigue teniendo un mayor impacto en las organizaciones más pequeñas. Pero existen otras amenazas que también suponen un riesgo existencial para las pequeñas empresas:

- El robo de datos es el objetivo de la mayor parte del malware que ataca a las pymes: los ladrones de contraseñas, los registradores de pulsaciones de teclas y otro spyware sumaron casi la mitad de las detecciones de malware. El robo de credenciales mediante phishing y malware puede dejar expuestos los datos de las pequeñas empresas en las plataformas en la nube y los proveedores de servicios y, a través de filtraciones de red, también se puede atacar a sus clientes.
- Ahora los atacantes utilizan más la distribución de malware basado en web —a través de la publicidad maliciosa y la optimización maliciosa para motores de búsqueda ("envenenamiento de SEO") —para esquivar las dificultades que plantea el bloqueo de macros maliciosas en documentos, además de utilizar imágenes de disco para combatir las herramientas de detección de malware.
- Los dispositivos desprotegidos conectados a las redes de las organizaciones, como ordenadores no administrados sin software de seguridad instalado, ordenadores con errores de configuración y sistemas que ejecutan software sin soporte por parte de los fabricantes, son el principal punto de entrada para todo tipo de ciberataques contra pequeñas empresas.
- Los atacantes recurren cada vez más al abuso de controladores, ya sean controladores vulnerables de empresas legítimas o controladores maliciosos que se han firmado con certificados robados u obtenidos de forma fraudulenta, para evadir e inutilizar las defensas antimalware de los sistemas administrados.
- Los ataques por correo electrónico han empezado a dejar atrás la ingeniería social más sencilla para interactuar de manera más activa con sus objetivos a través del correo electrónico, utilizando un hilo de mensajes y respuestas para que sus señuelos resulten más convincentes.
- Los ataques contra los usuarios de dispositivos móviles, incluidas las estafas basadas en ingeniería social ligadas al abuso de servicios de terceros y plataformas de redes sociales, han crecido de manera exponencial y afectan tanto a particulares como a pequeñas empresas. Estas estafas van desde la vulneración del correo electrónico corporativo y los servicios en la nube hasta la denominada "matanza de cerdos"(shā zhū pán (殺豬盤)).

Acerca de nuestros datos

Los datos utilizados en nuestro análisis proceden de varias fuentes:

- Informes de clientes: telemetría de detección del software de protección de Sophos que se ejecuta en las redes de los clientes, que ofrece una visión amplia de las amenazas detectadas, y analizada en SophosLabs (en este informe, "conjunto de datos de Labs").
- Datos de Managed Detection and Response (MDR), recopilados durante el transcurso de los traslados de incidencias ocasionados por la detección de actividad maliciosa en las redes de los clientes de MDR (en este informe, "conjunto de datos de MDR").
- Datos del equipo de Incident Response, extraídos de los incidentes en las redes de los clientes de empresas de 500 empleados o menos en que se había implementado una protección de detección y respuesta gestionadas mínima o nula (en este informe, "conjunto de datos de IR").

Si desea un análisis más exhaustivo de los datos extraídos exclusivamente de los casos gestionados por nuestro equipo de IR externo (incluidos casos que implican a clientes con más de 500 empleados), consulte nuestra publicación hermana Informe sobre adversarios activos. Las conclusiones del presente informe se basan, a menos que se indique lo contrario, en los conjuntos de datos combinados con la correspondiente normalización.

Los datos son el principal objetivo

El mayor reto de ciberseguridad al que se enfrentan las pequeñas empresas (y las organizaciones de todos los tamaños) es la protección de los datos. Más del 90 % de los ataques registrados por nuestros clientes implican el robo de datos o credenciales de una forma u otra, independientemente de si el método es un ataque de ransomware, la extorsión con datos, el acceso remoto no autorizado o simplemente el robo de datos.

Las estafas por correo electrónico corporativo comprometido (BEC), en que un ciberdelincuente secuestra las cuentas de correo electrónico con el propósito de cometer un fraude o con otros fines maliciosos, suponen un gran problema dentro del ámbito de las pymes. Actualmente no cubrimos las estafas BEC en nuestra publicación hermana, el Informe sobre adversarios activos, pero sus autores estiman que, en 2023, nuestro equipo de Incident Response identificó estafas por correo electrónico corporativo comprometido más a menudo que cualquier otro tipo de incidente, salvo el ransomware.

El robo de credenciales, incluidas las cookies del navegador, puede utilizarse para vulnerar el correo electrónico corporativo, acceder a servicios de terceros como sistemas financieros basados en la nube y acceder a recursos internos que pueden explotarse para cometer fraudes u otras artimañas para obtener ganancias económicas. Las credenciales también pueden ser vendidas por "brókeres de acceso" a quien quiera que desee explotarlas. En este sentido, Sophos ha seguido ofertas en foros clandestinos que prometían conceder acceso a varias redes de pymes.

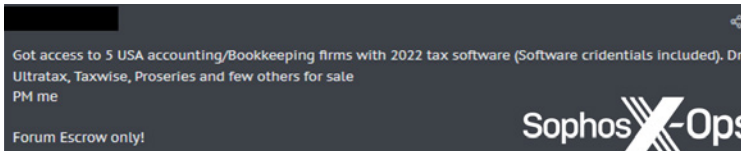


Figura 1: Una publicación en un foro anunciando el acceso a una pequeña empresa de contabilidad de EE. UU.

Figura 2: Una publicación en un foro anunciando el acceso a una pequeña empresa de Bélgica.

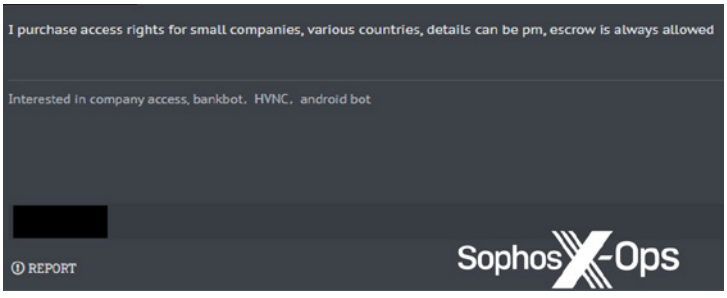


Figura 3: Un ciberdelincuente ofreciéndose para comprar el acceso a pequeñas empresas.

Figura 4: Oferta de venta del acceso a una pequeña empresa de Italia en un foro de delincuentes.

Por categoría, casi la mitad del malware detectado en 2023 perseguía los datos de sus víctimas. La mayoría de este es malware que hemos clasificado específicamente como "ladrones", es decir, malware que se apropia de credenciales, cookies del navegador, pulsaciones de teclas y otros datos, que pueden venderse por dinero o utilizarse para seguir con la explotación.

Sin embargo, dada la naturaleza modular del malware, resulta difícil clasificarlo por funcionalidad, ya que casi todo el malware tiene la capacidad de robar algún tipo de dato de los sistemas vulnerados. Estas detecciones tampoco incluyen otros métodos de robo de credenciales, como el phishing por correo electrónico o mensajes de texto u otros ataques de ingeniería social. Y luego también hay otros blancos, como los dispositivos macOS o móviles, en que el malware, las aplicaciones no deseadas y los ataques de ingeniería social buscan los datos de los usuarios, en particular los de tipo financiero.

Categorías de malware por número de actualizaciones de firmas en 2023

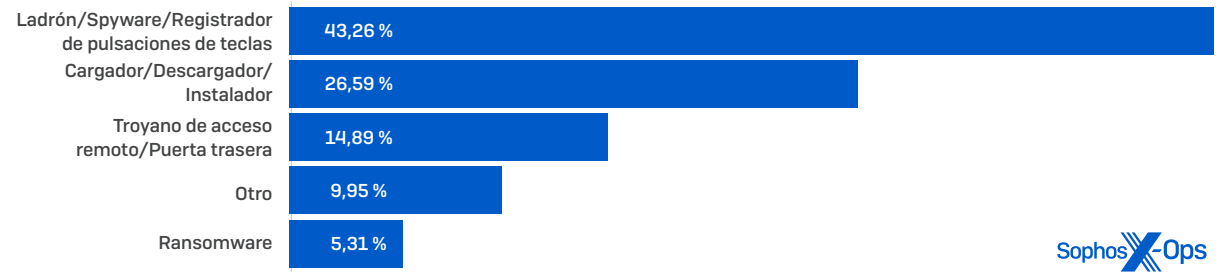


Figura 5: Detecciones de malware por tipo en 2023, según lo observado en los conjuntos de datos de Labs y MDR.

Casi el 10 % del malware detectado no entra en ninguna de las cuatro principales categorías de arriba. Esta categoría denominada "Otro" incluye el malware que ataca a los navegadores para inyectar anuncios o redirigir resultados de búsqueda para ganar dinero por clics, o que modifica o recopila datos para beneficio del desarrollador del malware, entre otras cosas.

Algunos ladrones persiguen información muy específica. Los ladrones de tókenes de Discord, que roban credenciales del servicio de mensajería Discord, suelen utilizarse para distribuir otro malware a través de los servidores de chat o de la red de distribución de contenido de Discord. Pero otros ladrones importantes (Strela, Raccoon Stealer y la venerable familia de ladrones RedLine) son mucho más agresivos en sus ataques y sustraen almacenes de contraseñas del sistema operativo y de las aplicaciones, además de cookies del navegador y otros datos de credenciales. Raccoon Stealer también ha desplegado "clippers" de criptomonedas que cambian las direcciones de las criptocarteras copiadas en el portapapeles por la dirección de una cartera controlada por el operador de malware.

Principales ladrones de información por número de denuncias de clientes en 2023

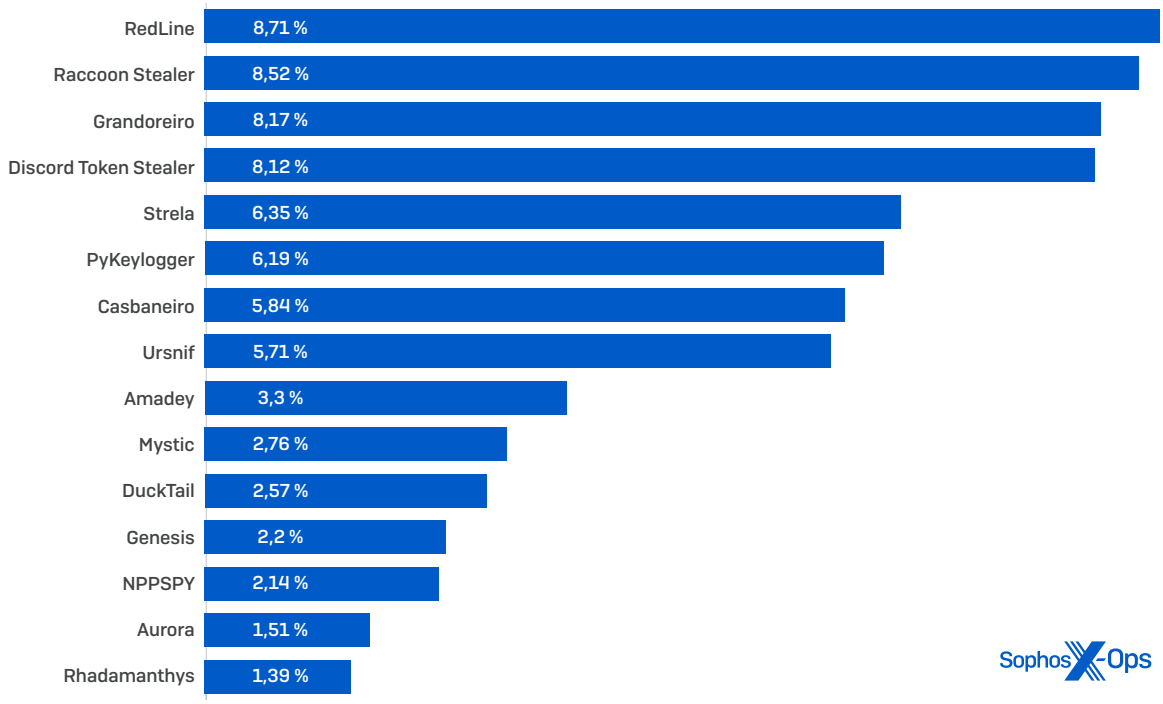


Figura 6: Detecciones de malware de ladrones de información en 2023, extraídas de la telemetría de clientes de Sophos en el conjunto de datos de SophosLabs.

Sophos ha observado un incremento del número de programas de malware que roban información de sistemas macOS, y creemos que esa tendencia continuará. Estos ladrones, algunos de los cuales se venden en foros clandestinos y en canales de Telegram por importes de hasta 3000 USD, pueden recopilar datos del sistema, datos del navegador y criptocarteras.

El ransomware sigue siendo una de las principales amenazas para las pequeñas empresas

Aunque el ransomware representa un porcentaje relativamente pequeño de todas las detecciones de malware, sigue teniendo el mayor efecto en términos de impacto. El ransomware afecta a empresas de todos los tamaños y en todos los sectores pero, según nuestras observaciones, es a las pymes a las que ataca con más frecuencia. En 2021, el Grupo de Trabajo sobre Ransomware del Instituto de Seguridad y Tecnología descubrió que el 70 % de los ataques de ransomware arremetían contra pequeñas empresas. Aunque el número total de ataques de ransomware ha variado de un año a otro, este porcentaje corrobora nuestras propias métricas.

El ransomware LockBit fue la primera amenaza en los casos de seguridad de pequeñas empresas gestionados por el equipo de Sophos Incident Response en 2023. LockBit es un ransomware como servicio distribuido por diversos afiliados, y fue el ransomware más desplegado en 2023 como se puede ver en la Figura 7.

Incidentes de ransomware en pequeñas empresas gestionados por Sophos Incident Response en 2023

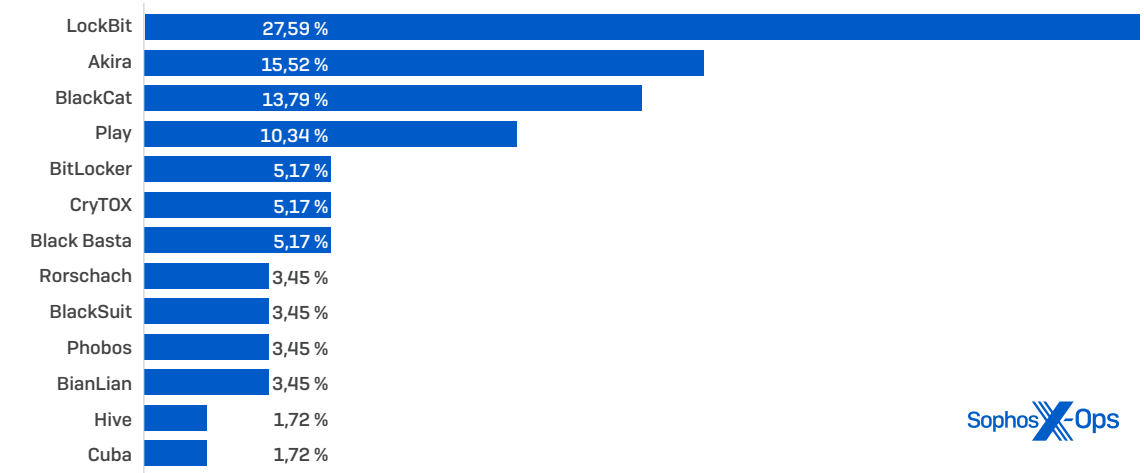


Figura 7: Desglose de los programas de ransomware tras los incidentes en pequeñas empresas investigados en 2023 por Sophos Incident Response; estas cifras reflejan el conjunto de datos de las intervenciones del equipo de IR en clientes que, por lo general, no tenían ninguna protección de Sophos previa.

Los 20 principales programas de ransomware por número de denuncias de clientes en 2023

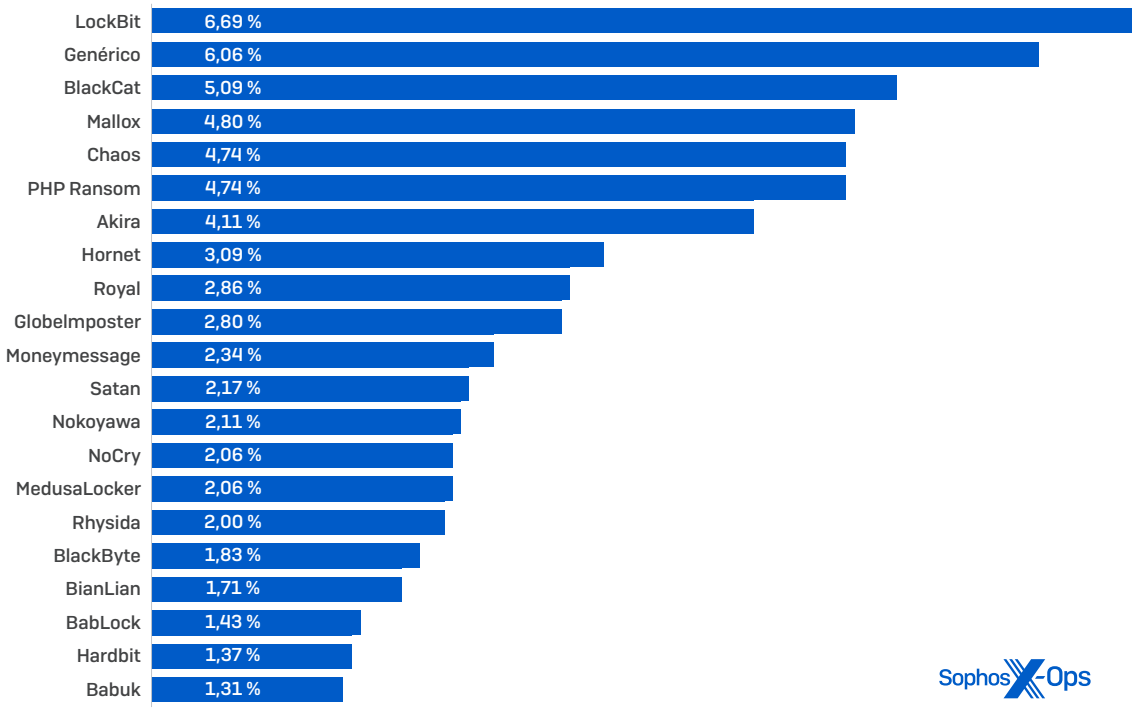


Figura 8: Los tipos de ransomware que más se intentaron distribuir, detectados por el software de protección de endpoints de Sophos y presentes en el conjunto de datos de Labs para todos los clientes en 2023, como porcentaje de todo el ransomware detectado; "Genérico" representa varios tipos de ransomware detectados con una firma general que no se detectaron bajo otra definición.

LockBit fue el malware más observado por el grupo Sophos Managed Detection and Response (MDR), que incluye al equipo de Incident Response y sus datos, con casi el triple de incidentes en que se intentó el despliegue de ransomware que su competidor más cercano, Akira.

Principales variedades de ransomware gestionadas por MDR observadas en 2023, por n.º de incidentes

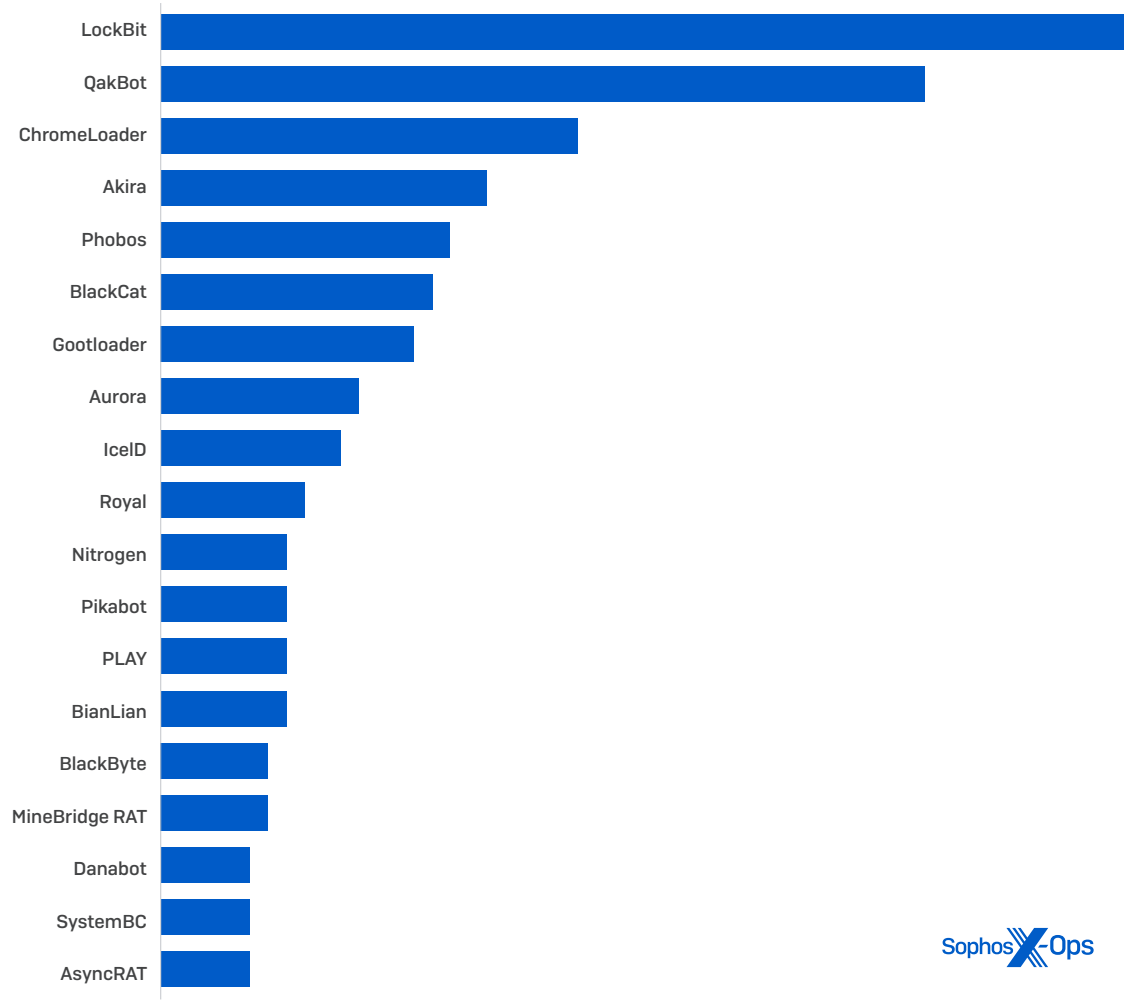


Figura 9: Malware observado con mayor frecuencia en incidentes gestionados por Sophos Managed Detection and Response en 2023, como se puede ver en el conjunto de datos de MDR. Fíjese en las diferencias entre este gráfico y el de la Figura 8: aparte de la prevalencia de LockBit en 2023, vemos que existe una amplia variedad de familias de ransomware que intentan infectar sistemas. Solo un subconjunto de ellas evolucionan hasta una fase que requiere la intervención de MDR. Tenga en cuenta que no son excluyentes; es decir, puede darse más de una detección en un único incidente.

A medida que el 2023 fue avanzando, vimos cómo se intensificaba el uso de la ejecución remota de ransomware, es decir, usar un dispositivo no gestionado en las redes de una organización para intentar cifrar archivos en otros sistemas mediante el acceso a archivos de red.

Incidentes de ransomware remoto, 2022-2023

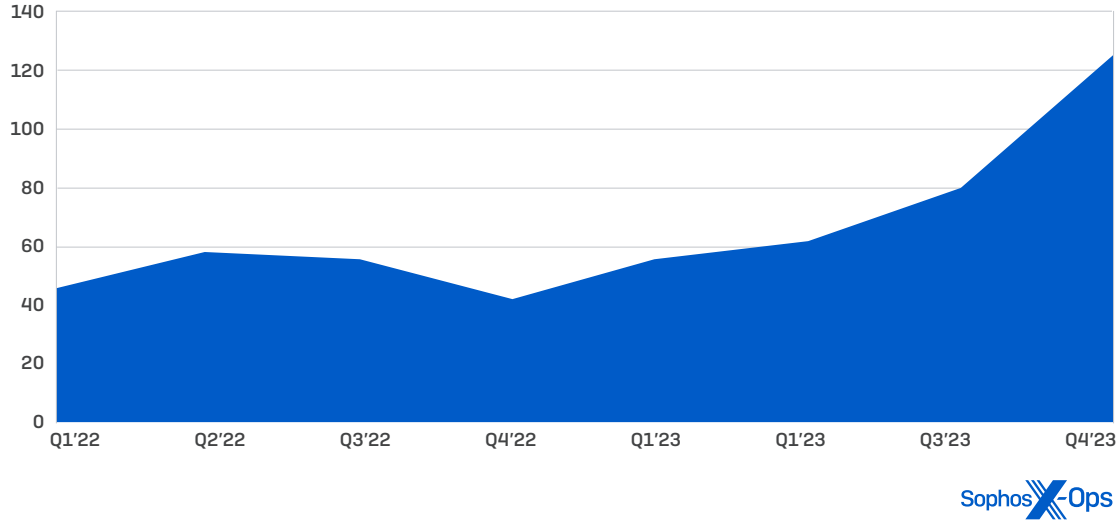


Figura 10: Los datos de los dos últimos años de la telemetría de los clientes recopilada por Sophos indican un aumento general de la proporción de intentos de ataques de ransomware que implican ransomware remoto, un problema recurrente que ha resurgido con fuerza, sobre todo en la segunda mitad de 2023.

Este tipo de ataques consiguen afianzarse explotando servidores, dispositivos personales y dispositivos de red desprotegidos que se conectan a las redes basadas en Windows de las organizaciones. Una defensa exhaustiva puede impedir que estos ataques aíslen a organizaciones enteras, pero pueden seguir dejándolas expuestas a la pérdida y al robo de datos.

Los sistemas Windows no son los únicos que ataca el ransomware. Cada vez más, los desarrolladores de ransomware y otro malware utilizan lenguajes multiplataforma para crear versiones para los sistemas operativos macOS y Linux y plataformas de hardware compatibles. En febrero de 2023, se descubrió que se había utilizado una variante para Linux del ransomware ClOp en un ataque en diciembre de 2022; desde entonces, Sophos ha observado versiones filtradas del ransomware LockBit que atacan a macOs en el propio procesador de Apple y a Linux en distintas plataformas de hardware.

Ciberdelincuencia como servicio

En el mundo del malware sigue predominando lo que denominamos "malware como servicio" (MaaS), que es el uso de marcos de distribución de malware proporcionados por ciberdelincuentes para otros ciberdelincuentes a través de mercados clandestinos. Sin embargo, tanto las mejoras en la seguridad de las plataformas como las operaciones de desmantelamiento por parte del sector y las fuerzas del orden han tenido cierta repercusión en el panorama del MaaS.

Tras una década de predominio en el negocio de la distribución de malware, Emotet ha remitido desde su desmantelamiento por parte de la Europol y la Eurojust en enero de 2021. Lo mismo ha ocurrido, en menor grado, con Qakbot y Trickbot tras la operación policialde agosto de 2023. Aunque Qakbot ha regresado de forma limitada, ha sido sustituido en gran parte por sus sucesores en potencia, Pikabot y DarkGate.

Nada de esto ha afectado al venerable troyano de acceso remoto AgentTesla, que ha pasado a ocupar el primer puesto en el mercado del MaaS. El año pasado, según nuestros datos de telemetría, fue el malware detectado con mayor frecuencia por los sistemas de protección de endpoints en 2023 (aparte de archivos .LNK genéricos maliciosos y malware ofuscado) y representó hasta el 51 % de las detecciones en el marco de distribución de malware.

Principales marcos de distribución de malware por número de denuncias de clientes en 2023

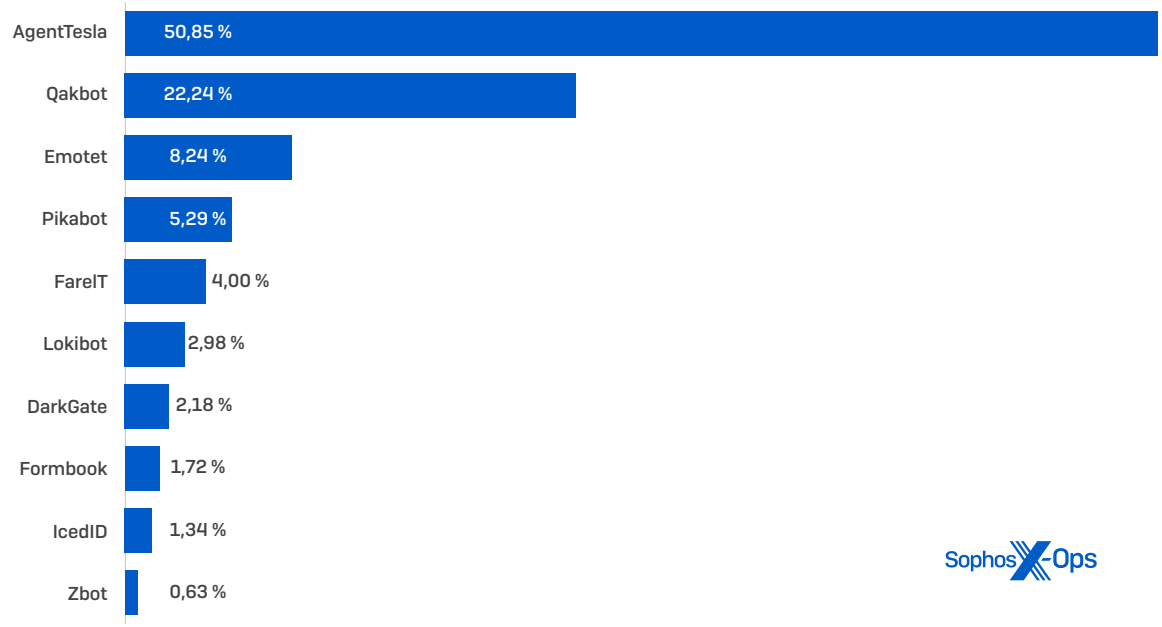


Figura 11: Desglose de los marcos más comunes utilizados por los atacantes para distribuir malware, basado en el número de detecciones en endpoints de las redes de clientes protegidas por Sophos; las cifras de Qakbot representan las detecciones anteriores a la operación policial internacional de agosto de 2023 contra su infraestructura.

En busca de una vía de distribución distinta

Los ataques de malware requieren algún tipo de acceso inicial. Esto suele implicar alguno de los siguientes elementos:

- Correos electrónicos de phishing
- Archivos adjuntos de correo electrónico malicioso
- Exploits de vulnerabilidades en sistemas operativos y aplicaciones
- Actualizaciones de software falsas
- Explotación y abuso del protocolo de escritorio remoto
- Robo de credenciales

En el pasado, los operadores del MaaS han dependido mucho de los archivos adjuntos de correo electrónico malicioso para conseguir ese afianzamiento inicial. Sin embargo, ha habido cambios en la seguridad predeterminada de la plataforma Microsoft Office que han tenido un impacto en el mercado del MaaS. Microsoft ha ido desplegando modificaciones en las aplicaciones de Office que bloquean las macros predeterminadas de Visual Basic para Aplicaciones (VBA) de los documentos descargados de Internet, de modo que los operadores del MaaS lo tienen más difícil para utilizar su método favorito para propagar el malware.

Esto ha provocado algunos cambios en los tipos de archivos adjuntos que utilizan los atacantes, que se han pasado casi exclusivamente a los archivos PDF adjuntos. Sin embargo, ha habido varias excepciones importantes. A principios de 2023, los operadores de Qakbot empezaron a utilizar documentos de OneNote maliciosos para sortear los cambios que se estaban implementando en Excel y Word, ocultando en los documentos enlaces a archivos de script que se activaban cuando la víctima hacía clic en un botón dentro del archivo de bloc de notas de OneNote.

En 2021, observamos que productos de malware como servicio como la puerta trasera RaccoonStealer habían empezado a depender en gran medida de la distribución web, utilizando a menudo trucos de optimización para motores de búsqueda (SEO) para engañar a sus víctimas para que descargaran su malware. En 2022, vimos cómo se utilizaba el "envenenamiento de SEO" como parte de una campaña de robo de información de SolarMarker. Estos métodos vuelven a estar en auge, y los ciberdelincuentes que los utilizan se han vuelto más sofisticados.

Hemos visto varias campañas destacables que utilizaban publicidad web maliciosa y envenenamiento de SEO para confundir a sus víctimas. En una de ellas, un grupo de actividad utilizaba un malware que denominamos "Nitrogen"; el grupo empleaba anuncios de Google y Bing vinculados a palabras clave concretas a fin de engañar a sus objetivos para que descargaran un instalador de software de un sitio web falso, utilizando la identidad de marca de un desarrollador de software legítimo. Esta misma técnica de publicidad maliciosa se ha usado en relación con varios programas de malware de acceso inicial, entre ellos, el agente de redes de bots Pikabot, el ladrón de información IcedID y las familias de malware de puerta trasera Gozi.

En el caso de Nitrogen, los anuncios se dirigían a técnicos informáticos y ofrecían descargas, como software de escritorio remoto muy conocido para el soporte a usuarios finales y utilidades de transferencia segura de archivos. Los instaladores incluían lo que se publicitaba, pero también distribuían una carga Python maliciosa que, al iniciarse junto con el instalador, desplegaba un shell remoto Meterpreter y cargas Beacon de Cobalt Strike. Según las conclusiones de otros investigadores, es probable que este fuera el primer paso de un ataque de ransomware BlackCat.

Herramientas de "doble uso"

Cobalt Strike, el conocido kit de software para simulaciones de adversarios y operaciones de equipos rojos, sigue siendo utilizado tanto por adversarios como por organizaciones legítimas de pruebas de seguridad. Pero no es ni de lejos el único software desarrollado comercialmente que utilizan los atacantes, como tampoco es ya el más común.

Herramientas de escritorio remoto, herramientas de compresión de archivos, software para la transferencia de archivos y otras utilidades, además de herramientas de pruebas de seguridad de código abierto, son empleadas habitualmente por los atacantes por el mismo motivo por el que lo hacen las pymes: para que les faciliten el trabajo.

Sophos MDR ha observado que los atacantes se sirven ilícitamente de las siguientes utilidades, a las que nos referimos como "herramientas de doble uso", como parte del proceso posterior a la explotación:

- **Descubrimiento:** Advanced IP Scanner, NetScan, PCHunter, HRSword
- **Persistencia:** Anydesk, ScreenConnect, DWAgent
- **Acceso a credenciales:** Mimikatz, Veeam Credential Dumper, LaZagne
- **Propagación lateral:** PsExec, Impacket, PuTTy
- **Recopilación y exfiltración de datos:** FileZilla, WinSCP, megasync, Rclone, WinRar, 7zip

Sophos MDR detectó la presencia de AnyDesk y PsExec en más incidentes que Cobalt Strike, tal como se ilustra a continuación:

Principales herramientas de "doble uso" observadas en los incidentes gestionados por MDR en 2023, por n.º de incidentes

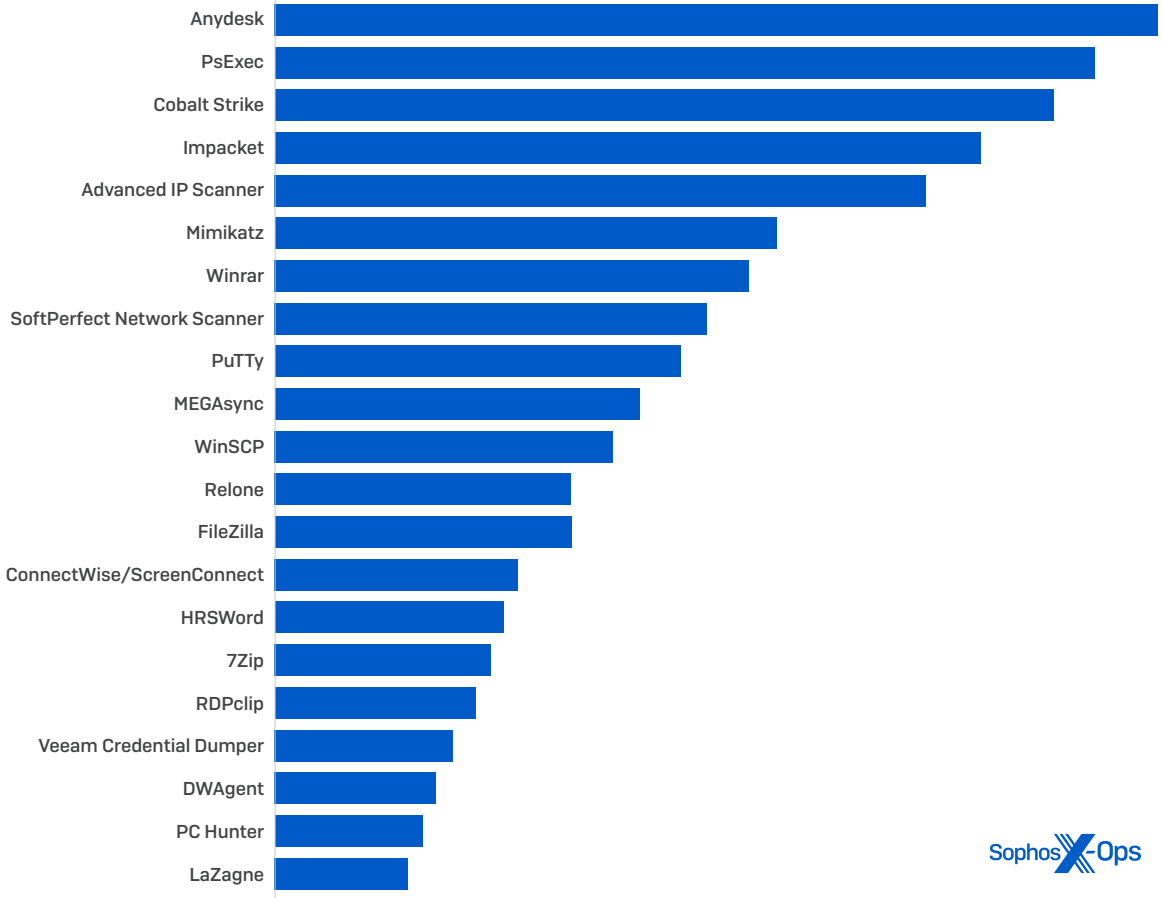


Figura 12: Las herramientas de "doble uso" detectadas con mayor frecuencia en incidentes de ciberseguridad, basado en el número de casos en los que se observó cada una en el conjunto de datos de Sophos MDR.

Ataques de día cero y otros ataques

En mayo de 2023, Progress Software detectó vulnerabilidades en su plataforma de transferencia segura de archivos gestionada MOVEit, ampliamente utilizada en la empresa, entre ellas una que había explotado por lo menos un grupo de ciberdelincuentes. Posteriormente, la empresa descubrió varias vulnerabilidades más y publicó parches para corregirlas.

Los ataques se atribuyeron a ciberdelincuentes asociados con el grupo de ransomware Cl0p. Los atacantes aprovecharon la vulnerabilidad para desplegar shells web en las interfaces web públicas de los servidores de transferencia de MOVEit, shells web que, en algunos casos, persistían incluso después de que los clientes de Progress parchearan las vulnerabilidades.

MOVEit fue solo una de las diversas vulnerabilidades "de día cero" a las que se enfrentaron los responsables de la seguridad en 2023. GoAnywhere, otro sistema de transferencia de archivos gestionado, divulgó una vulnerabilidad en febrero que otro grupo afiliado a Cl0p había intentado explotar. Por otra parte, la banda de ransomware Bl00dy explotó una vulnerabilidad de ejecución de código remoto en los productos de software de servidor de impresión PaperCut MF y NG en marzo y abril, después de que los desarrolladores la notificaran en enero.

En determinados casos, estas vulnerabilidades simplemente no pueden parchearse. Por ejemplo, una vulnerabilidad detectada en junio en los dispositivos Barracuda Email Security Gateway era tan grave que no pudo parchearse y obligó a sustituir por completo los dispositivos físicos y virtuales. Un grupo de ciberdelincuentes chino siguió explotando los dispositivos vulnerables durante el resto de 2023.

Las vulnerabilidades en el software y los dispositivos no tienen por qué ser nuevas para que puedan aprovecharlas los atacantes, quienes muchas veces buscan software que se ha quedado sin soporte, como firewalls de red y software de servidor de red antiguos, para atacar sabiendo que no hay ningún parche por llegar.

Ataques a la cadena de suministro y malware con firma digital

Las pequeñas empresas también deben preocuparse por la seguridad de los servicios de los que dependen para gestionar su negocio, así como su infraestructura de TI. Los ataques a la cadena de suministro no son solo cosa de los estados nacionales; hemos observado que los ataques contra proveedores de servicios gestionados se han convertido en una constante en el arsenal de estrategias del ransomware.

En 2023, Sophos MDR respondió a cinco casos en que los clientes de pequeñas empresas fueron atacados mediante un exploit del software de monitorización y gestión remota (RMM) de un proveedor de servicios. Los atacantes utilizaron el agente RMM de NetSolutions que se ejecutaba en los ordenadores de las organizaciones afectadas para crear nuevas cuentas administrativas en las redes atacadas y, después, distribuyeron herramientas comerciales de escritorio remoto, exploración de red y despliegue de software. En dos de los casos, los atacantes consiguieron desplegar el ransomware LockBit.

Es difícil defenderse de los ataques que se aprovechan de software de confianza, sobre todo cuando ese software da a los atacantes la capacidad de desactivar la protección de los endpoints. Las pequeñas empresas y los proveedores de servicios que les prestan servicio deben estar atentos a cualquier alerta de desactivación de la protección para endpoints en los sistemas de sus redes, porque podrían indicar que un atacante ha obtenido acceso con privilegios a través de una vulnerabilidad de la cadena de suministro o de otro software que de entrada podría parecer legítimo.

Por ejemplo, en 2023 vimos una serie de casos en que los atacantes utilizaron controladores de kernel vulnerables de software antiguo que aún disponía de firmas digitales válidas y casos en que se había creado intencionadamente software malicioso que utilizaba firmas digitales obtenidas de forma fraudulenta —incluidos controladores de kernel maliciosos firmados digitalmente a través del programa Windows Hardware Compatibility Publisher (WHCP) de Microsoft— para eludir la detección por parte de las herramientas de seguridad y ejecutar código que inhabilita la protección antimalware.

Los controladores de kernel funcionan a un nivel muy básico del sistema operativo y suelen cargarse antes que otro software al iniciarse el sistema operativo, lo que significa que, en muchos casos, se ejecutan antes de que el software de seguridad pueda arrancar. Las firmas digitales actúan como un permiso de conducción, por así decirlo: en todas las versiones de Windows desde la versión 1607 de Windows 10, los controladores de kernel necesitan una firma digital válida; de lo contrario, los sistemas operativos Windows con el arranque seguro activado no los cargarán.

En diciembre de 2022, Sophos notificó a Microsoft la detección de controladores de kernel maliciosos que tenían certificados firmados por Microsoft. Dado que esos controladores contaban con certificados firmados por Microsoft, se aceptaban por defecto como software benigno, lo que permitía su instalación, y después desactivaban las protecciones para endpoints en los sistemas en los que se habían instalado. Microsoft publicó un aviso de seguridad y después, en julio de 2023, revocó un gran número de certificados de controladores maliciosos que se habían obtenido a través de WHCP.

Los controladores no tienen por qué ser maliciosos para poder explotarse. Hemos observado muchos casos en que los atacantes utilizan controladores y otras bibliotecas de versiones antiguas e incluso actuales de productos de software para la carga lateral de malware en la memoria del sistema.

También hemos detectado la utilización de controladores propios de Microsoft en algunos ataques. En varias ocasiones, los operadores de ransomware han utilizado una versión vulnerable de un controlador para la utilidad Explorador de procesos de Microsoft a fin de desactivar productos de protección para endpoints; en abril de 2023, informamos sobre una herramienta llamada "AuKill" que utilizó este controlador en distintos ataques cuyo objetivo era distribuir el ransomware Medusa Locker y LockBit.

Algunas veces tenemos suerte y detectamos los controladores vulnerables antes de que puedan explotarse. En julio, la actividad de un controlador de un producto de seguridad de otra compañía activó las reglas de comportamiento de Sophos. La alerta saltó por una prueba de simulación de ataque de un cliente, pero nuestra investigación del evento sacó a la luz tres vulnerabilidades que notificamos al proveedor de software, quien posteriormente las parcheó.

Los spammers rompen las barreras de la ingeniería social

Puede que el correo electrónico parezca un método de comunicación algo anticuado en la era de los chats móviles cifrados de extremo a extremo, pero es como si los spammers no se hubieran dado cuenta de ello o no les importase. Aunque todavía persiste el método BEC tradicional, que consiste simplemente en hacerse pasar por un empleado y pedir a otro empleado que envíe tarjetas regalo, los spammers se han vuelto mucho más creativos.

En el último año, el equipo de seguridad de mensajería de Sophos se ha encontrado con un montón de nuevos trucos y técnicas de ingeniería social diseñados para eludir los controles convencionales del correo electrónico. Los mensajes en que el atacante envía de improviso un archivo adjunto o un enlace por correo electrónico ya no se llevan. Ahora, los spammers más eficientes suelen iniciar una conversación primero, y solo pasan al ataque en correos posteriores.

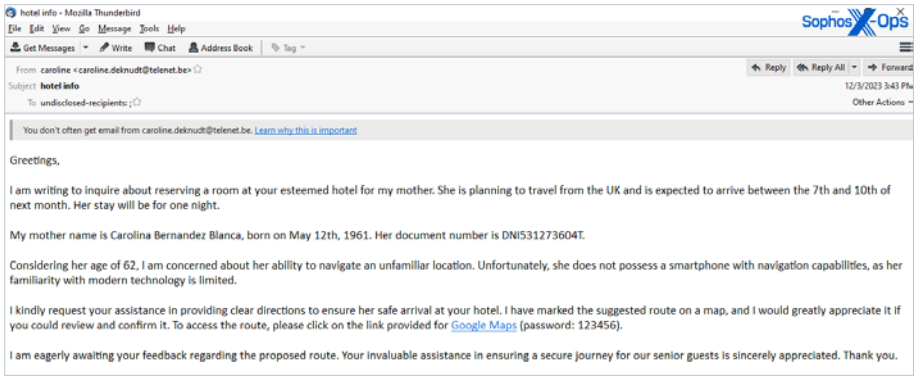


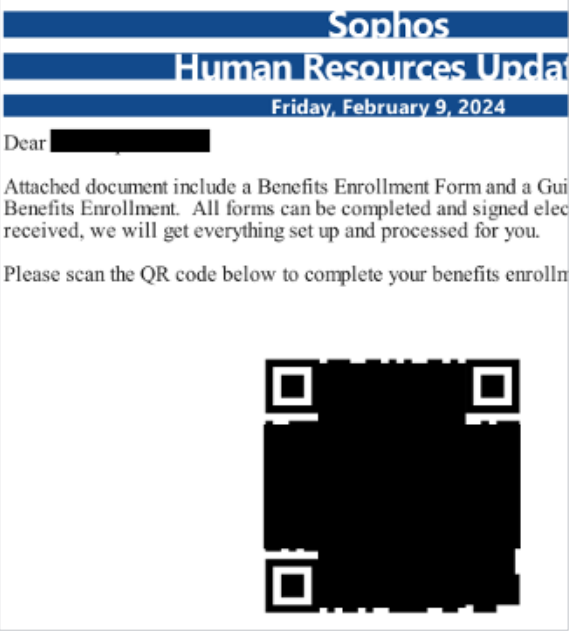
Figura 13: El spammer siempre espera a recibir respuesta de la víctima antes de enviarle un correo electrónico con un enlace a un archivo malicioso dentro de un archivo comprimido protegido con contraseña.

Hemos observado esta metodología en ataques en que los spammers se hacen pasar por trabajadores de servicios de entrega y llaman por teléfono a clientes de empresas para pedirles que abran un correo electrónico armado con malware. En ataques dirigidos contra distintos sectores durante 2023, también vimos a spammers que inicialmente enviaban una solicitud de negocio o una queja, seguida de un enlace para descargar un archivo con malware camuflado una vez que la empresa había respondido al primer mensaje.

La prevención de spam convencional implica procesos que inspeccionan el contenido de los mensajes y toman decisiones en función de ese contenido. Los spammers experimentaron con distintos métodos para reemplazar cualquier contenido de texto de sus mensajes por imágenes incrustadas. A veces las imágenes simulaban un mensaje escrito, mientras que otras veces experimentaban con el uso de códigos QR o imágenes que parecían facturas (con números de teléfono a los que los atacantes pedían que llamaran las víctimas) como forma de esquivar la detección.

Figura 14: Un archivo PDF adjunto a un mensaje de spam incrusta una miniatura borrosa e ilegible de una factura y un enlace a un sitio web que aloja una carga maliciosa.

Los archivos adjuntos maliciosos incluso rompieron barreras con la vuelta a escena de los PDF dañinos que incluían enlaces a scripts o sitios maliciosos, a veces por medio de códigos QR incrustados. La familia de malware Qakbot abusó en numerosas ocasiones del formato de documento OneNote de Microsoft, el bloc de notas (o archivo .one), para distribuir cargas, antes de que fuera desactivada más adelante ese mismo año en una operación de desmantelamiento coordinada. Los atacantes también se aferraron al formato de archivo MSIX (un tipo de formato de archivo de almacenamiento utilizado por Microsoft para distribuir aplicaciones a través de la Tienda de aplicaciones de Windows) como forma de eludir la detección.


Sophos

Human Resources Updat

Friday, February 9, 2024

Dear [redacted]

Attached document include a Benefits Enrollment Form and a Gui
Benefits Enrollment. All forms can be completed and signed elec
received, we will get everything set up and processed for you.

Please scan the QR code below to complete your benefits enrolln

Figura 15: Un archivo PDF adjunto malicioso, enviado por correo electrónico a empleados de Sophos, incrusta una imagen con un código QR que dirige a una página de phishing.

Y los atacantes también abusaron de los servicios de Microsoft: al finalizar el año, cerca de un 15 % del total del spam bloqueado por Sophos había sido enviado mediante cuentas de correo electrónico creadas en onmicrosoft.com, el sistema de mensajería orientado a empresas de Microsoft.

Malware para móviles y amenazas de ingeniería social

Las pequeñas empresas dependen enormemente de los dispositivos móviles como parte de sus sistemas de información aprobados o de uso puntual. Los mensajes de texto, las aplicaciones de mensajería y comunicaciones y las apps que se conectan a los servicios en la nube, incluidas las aplicaciones móviles para puntos de venta, son sistemas de vital importancia para las pequeñas empresas distribuidas. Los ciberdelincuentes lo saben y continúan buscando formas de atacar a los usuarios de dispositivos móviles para obtener acceso a datos o para cometer fraudes.

El spyware y los bankers constituyen un grupo de malware para Android especialmente preocupante, y que creemos que seguirá siendo una amenaza. El spyware se utiliza para recopilar datos del teléfono y, en ocasiones, incluso suscribe al usuario del dispositivo a servicios con tarifas especiales para obtener beneficios económicos directos. Recaba datos personales, incluidos mensajes SMS y registros de llamadas del dispositivo afectado, que luego se venden a estafadores o se utilizan para hacer chantaje,
o ambas cosas. Ha habido varios casos de víctimas que han llegado a quitarse la vida a consecuencia de las amenazas recibidas por parte operadores de spyware.

Estas aplicaciones móviles maliciosas se distribuyen de varias maneras. Puede que se hagan pasar por aplicaciones legítimas en Google Play o en tiendas de aplicaciones de terceros, a menudo haciéndose pasar por apps de préstamos. También se propagan a través de enlaces enviados por mensaje de texto.

Los bankers son un tipo de malware que vulnera aplicaciones financieras, como los monederos de criptomonedas, a fin de recopilar los datos de las cuentas de los usuarios para obtener acceso a sus fondos, utilizando permisos de accesibilidad para llegar a los datos confidenciales del teléfono.

Luego está la estafa "matanza de cerdos" o "shā zhū pán". Empezamos a rastrear aplicaciones falsas tanto en la plataforma iOS como en Android vinculadas a una forma de fraude que inicialmente denominamos "CryptoRom" a principios de 2021; desde entonces, estas estafas se han vuelto cada vez más sofisticadas.

Las redes delictivas que cometen estos fraudes —con frecuencia perpetrados desde instalaciones clandestinas con operarios que básicamente han sido secuestrados por el crimen organizado— han robado miles de millones de dólares a víctimas de todo el mundo, y a menudo se centran en personas relacionadas con pequeñas empresas. En 2023, un pequeño banco de Kansas quebró y fue incautado por la FDIC después de que el director general del banco enviara 12 millones USD procedentes de depósitos a estafadores para intentar recuperar fondos que supuestamente había perdido en uno de estos fraudes. Este trágico ejemplo demuestra cómo una estafa normalmente asociada a la vida personal de un individuo puede tener ramificaciones y repercusiones para las pequeñas empresas.

Los delincuentes del "shā zhū pán" engañan a sus víctimas a través de las redes sociales, apps de citas y de otro tipo y plataformas de comunidades, e incluso mensajes SMS "accidentales". Acostumbran a ir tras personas que buscan relaciones de amistad o románticas. Una vez que consiguen trasladar a su objetivo a una app de mensajería segura como WhatsApp o Telegram, se ganan su confianza e introducen una idea para ganar dinero de la que afirman tener información privilegiada y que suele implicar criptomonedas.

En el último año, hemos visto cómo las aplicaciones falsas que se utilizan en estos engaños llegaban a la tiendas de aplicaciones Google Play y App Store de iOS. Para superar la revisión de seguridad de la tienda, se presentan como una app benigna y, una vez finalizada la evaluación, cambian el contenido remoto por una app de compraventa de criptomonedas falsa. Los estafadores se embolsan de inmediato cualquier criptomoneda depositada a través de estas apps.

Recientemente, también hemos constatado que estas estafas adoptan una táctica de otro tipo de fraude con criptomonedas que no requiere ninguna app falsa; en su lugar, utilizan la funcionalidad "Web3" de las apps móviles de criptocarteras para meter mano directamente en las carteras creadas por las víctimas. Hemos identificado cientos de dominios asociados a estas variantes de minería de finanzas descentralizadas (DeFi) del "shā zhū pán" y, al igual que con las apps falsas que identificamos, seguimos denunciándolas y trabajando para que se retiren.

Conclusiones

Las pequeñas empresas se enfrentan a numerosas amenazas, y la sofisticación de estas suele estar a la par de las que se ciernen sobre grandes empresas y gobiernos. Aunque la cantidad de dinero que se puede sustraer es inferior a la disponible en una organización de mayor tamaño, los ciberdelincuentes se conforman con robar lo que pueden y compensarlo en volumen.

Los grupos delictivos cuentan con que las empresas más pequeñas no tendrán tan buenas defensas y que no habrán desplegado herramientas sofisticadas y modernas para proteger a sus usuarios y recursos. La clave para defenderse de manera efectiva frente a estas amenazas es demostrar que sus suposiciones son erróneas: forme a su personal, implemente la autenticación multifactor en todos los recursos abiertos a Internet, parchee sus servidores y dispositivos de red con la máxima prioridad y plantéese migrar recursos difíciles de gestionar como servidores de Microsoft Exchange y plataformas de correo electrónico SaaS.

La principal diferencia en nuestra experiencia entre las empresas más afectadas por los ciberataques y las que menos los sufrieron es el tiempo de respuesta. Contar con expertos en seguridad que supervisen y respondan 24/7 es fundamental para construir una defensa efectiva en 2024. Mantenerse a salvo no es imposible; solo requiere una planificación exhaustiva y unas defensas por capas que le permitan ganar tiempo para responder y minimizar los daños.

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

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

24-04-11 ES (NP)

SOPHOS