2023

CISCO TALOS

REVISIÓN DEL AÑO

Introducción

El ransomware, los cargadores de productos básicos y las APT dominaron el panorama de amenazas en 2023. Como detallaremos en la segunda revisión del año de Cisco Talos, los conflictos globales influenciaron las tendencias de ciberseguridad y cambiaron varias tácticas de los actores de amenazas y enfoques en operaciones que abarcan desde el espionaje hasta el ciberdelito.

La presencia global de Cisco y la experiencia de primera clase de Talos brindaron una cantidad masiva de datos para examinar: detecciones de terminales, instancias de respuestas a incidentes, tráfico de redes, caudales de correos electrónicos, sandboxes, honeypots y mucho más. Afortunadamente, nuestros compañeros de equipo incluyen expertos en la materia de todos los extremos del espacio de la ciberseguridad para ayudarnos a convertir esta inteligencia en información procesable para defensores y usuarios. Al aprovechar estas fuentes de información completas y complejas, analizamos las tendencias principales que modelaron el panorama de la ciberseguridad en 2023.

El ransomware continuó amenazando empresas globalmente en 2023, con LockBit como la amenaza principal en este espacio por segundo año consecutivo. Los servicios de salud fueron la principal industria objetivo este año, mientras que los adversarios mantuvieron su enfoque en entidades que tienen restricciones de financiación en seguridad y baja tolerancia de tiempo de inactividad. Sin embargo, no todo fue igual ya que vimos actores como Clop implementar una colección de ataques de día cero, comportamiento que se suele asociar con actividad de amenazas persistentes avanzadas (APT). Al mismo tiempo, el código fuente del ransomware filtrado les permitió a los actores no calificados ingresar a la contienda. Para complicar los problemas aún más, observamos una nueva tendencia de actores de ransomware que recurren a la extorsión pura y omiten la encriptación por completo mientras amenazan con filtrar datos sensibles.

Se siguen utilizando los cargadores de productos básicos para ofrecer estas amenazas de ransomware y varias de las mismas familias ya que el año pasado siguieron estando prevalentes, como Qakbot y IcedID. Esto se refleja en nuestra telemetría, ya que la mayoría de las marcas comúnmente falsificadas eran envíos y servicios financieros, características distintivas de estos adversarios. Sin embargo, estos cargadores están esclareciendo todos los remanentes de sus troyanos bancarios más allá a medida que se posicionan a sí mismos más como mecanismos de entrega de cargas útiles. Los desarrolladores y operadores se están adaptando a las defensas mejoradas y así encuentran nuevas maneras de desviarse aumentando actualizaciones de seguridad y de comprometer a las víctimas. Y a pesar de que nuevamente observamos una reducción de una gran botnet, este año al ser Qakbot, nuestra experiencia muestra que esto no significa necesariamente que la amenaza se ha eliminado.

Una de las más nuevas tendencias interregionales que hemos observado este año es un aumento en la focalización de dispositivos de red de actores de ransomware y APT. Ambos grupos dependen de atacar vulnerabilidades recientemente divulgadas y credenciales predeterminadas/débiles, una de las razones por las que el uso de las cuentas válidas fue siempre una debilidad principal en las participaciones de Talos IR. Cualquiera sea la sofisticación e intención del adversario, la razón detrás de la focalización es la misma: los dispositivos de red son extremadamente de alto valor a la vez que poseen varias debilidades de seguridad.

La inestabilidad geopolítica se manifiesta en la actividad de la APT. Esto se refleja en nuestra telemetría, que muestra un aumento en el tráfico sospechoso durante eventos geopolíticos importantes. Para los grupos chinos, como las relaciones con Occidente y Asia-Pacífico se vuelven más tensas, vemos un envalentonamiento en las operaciones, como una mayor predisposición para causar destrucción. Además, observamos esto en su focalización de las organizaciones de telecomunicaciones, que poseen numerosos activos de infraestructura fundamentales en geografías estratégicamente importantes como Guam y Taiwán. Para las APT rusas, Gamaredon y Turla se dirigieron a Ucrania a un ritmo acelerado, pero la actividad rusa en general para 2023 no reflejó todo el alcance de las capacidades ciberdestructivas que hemos visto implementar en el pasado, potencialmente por los esfuerzos concertados de los defensores.

Un punto que resalta este año fue el esfuerzo establecido de Cisco para crear y entregar soluciones de seguridad creativas que ayudan a fortalecer a nuestros partners. El grupo de trabajo Ucrania de Talos continúa impidiendo ataques en contra de los partners ucranianos fundamentales. Este año, encabezamos un esfuerzo para estabilizar la matriz eléctrica de Ucrania frente a los efectos del sistema de posicionamiento global (GPS) que interfieren en el campo de batalla al entregar switches de Cisco modificados en zonas de guerra activas. Además, Cisco lanzó la Coalición para la resiliencia de las redes con partners que lideran la industria, que se enfocan en aumentar el reconocimiento y proporcionan recomendaciones procesables para mejorar la seguridad de las redes. Del mismo modo, el equipo de investigación y descubrimiento de vulnerabilidades de Talos hizo que las pequeñas oficinas de investigación, las oficinas en casa (SOHO) y los routers industriales sean una prioridad principal. Hasta la fecha se informaron 289 vulnerabilidades a los proveedores, publicadas en 141 asesorías de Talos.

A medida que empeora el conflicto en Oriente Medio, estamos una vez más posicionados para ayudar a proteger a nuestros clientes y partners. Por lo tanto, quizás la historia general de 2023 sea esta: a medida que crece la osadía, sofisticación y persistencia de nuestros adversarios, también lo hace la voluntad de los defensores para prohibirlos en la medida en la que pueden.

Contenido

CISCO TALOS

REVISIÓN DEL AÑO

2023

Tendencias de telemetrí a

Puntos destacados de la sección

- El tráfico de red sospechoso captado por los productos de seguridad de Cisco reveló fuertes aumentos en la actividad que con frecuencia se correspondían con eventos geopolíticos principales y ciberataques globales.
- Las vulnerabilidades más dirigidas eran fallas de seguridad anteriores en aplicaciones comunes, compatibles con los hallazgos de la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) en los últimos años. La mayoría de las principales vulnerabilidades dirigidas que observamos recibieron puntuaciones de alta o máxima gravedad por Cisco Kenna y el sistema de puntuación de vulnerabilidades comunes (CVSS) y se las incluyó en el catálogo de Vulnerabilidades Explotadas Conocidas (KEV) de CISA. La alta frecuencia de estos intentos dirigidos contra estos CVE, asociado con su gran impacto, pone de relieve la preferencia de los adversarios por dirigir sistemas sin parche que puedan causar interrupciones importantes.
- Los actores de amenazas abusaron de extensiones de archivos comunes y falsificaron marcas conocidas, técnicas comunes que ponen de relieve el uso de la ingeniería social para habilitar operaciones como la suplantación de identidad (phishing) y el riesgo de correo electrónico comercial (BEC). Es probable que los adversarios respondan a la deshabilitación de macros de Microsoft en 2022 al usar diferentes tipos de archivos para ocultar su malware, como los PDF, que fue la extensión de archivo más bloqueada este año.
- Los servicios financieros y las empresas de envío dan cuenta de las marcas que observamos que se falsificaron con más frecuencia en la telemetría de los correos electrónicos. Esto sugiere temas de suplantación de identidad (phishing) de larga data para los cargadores de productos básicos basados en correos electrónicos como Emotet, Qakbot y Trickbot están aún en juego. Del mismo modo, la suplantación de identidad (phishing) da cuenta de un cuarto de los vectores de acceso de inicio conocidos en las participaciones de Talos IR este año y resalta la continua dependencia de esta técnica de los actores.
- El uso de cuentas válidas fue una técnica MITRE ATT&CK de las más observadas, que dio cuenta de la dependencia de credenciales comprometidas de los adversarios y del uso de cuentas existentes para varias etapas de sus ataques. Esto es consistente con los datos de Talos IR, que muestra credenciales comprometidas/cuentas válidas que dan cuenta de casi un tercio de vectores de acceso de inicio conocidos en 2023.

Tendencias generales a través del tiempo

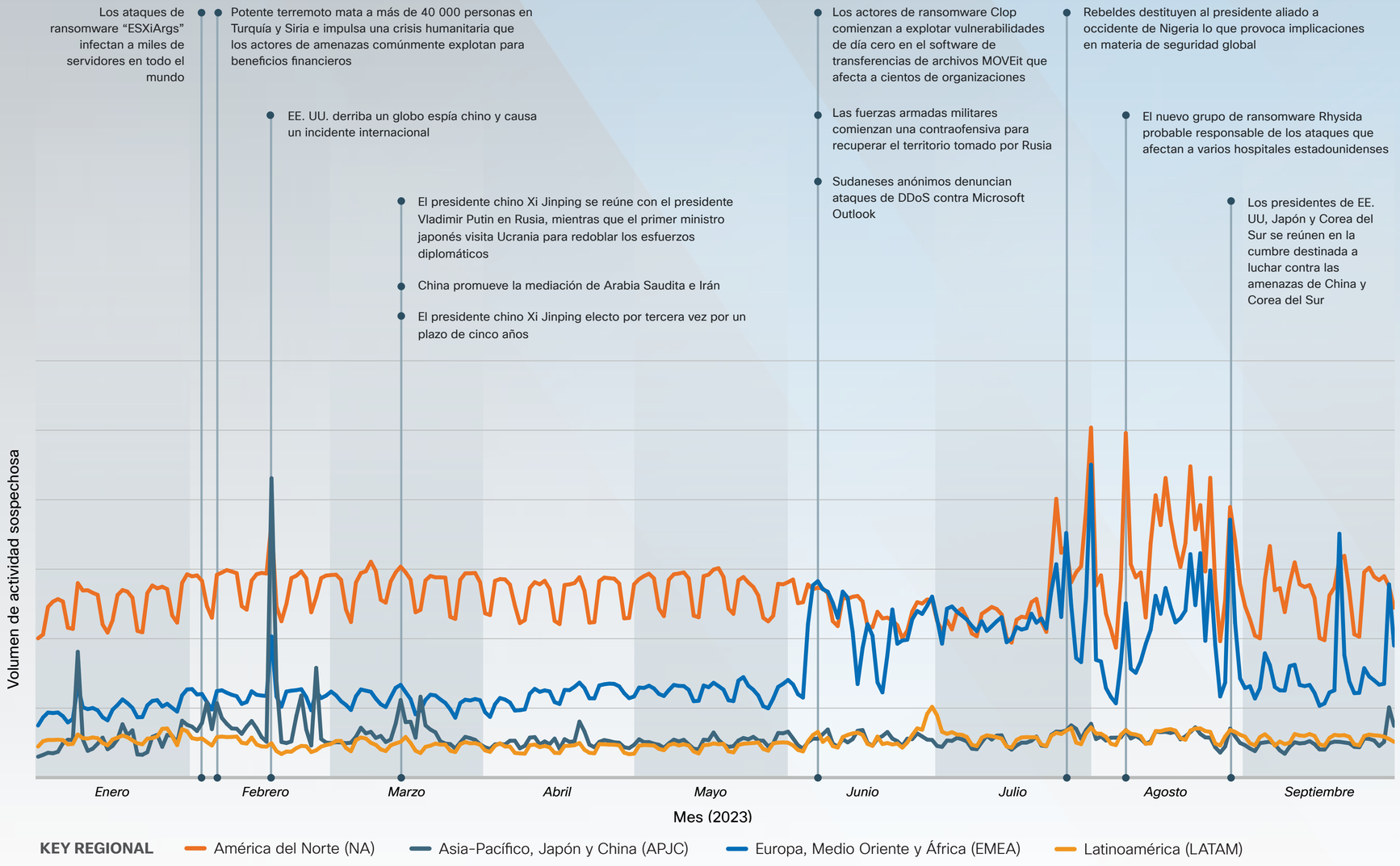
El tráfico sospechoso incluye una amplia variedad de información clasificada originada de varios productos de seguridad de Cisco, incluidos Umbrella, Secure Endpoint, Cisco® Email Security appliance, Cisco Meraki, SSE y Cisco Secure Firewall. Los ejemplos incluyen dominios maliciosos bloqueados por Umbrella, registros con disposiciones maliciosas de Secure Endpoint, correos electrónicos de suplantación de identidad (phishing) de ESA, firmas de Snort activadas de Secure Firewall y Meraki, y muchos otros.

En América del Norte, Europa, Medio Oriente, África (EMEA) y Latinoamérica, el tráfico de red sospechoso era periódico y seguía el patrón de la jornada laboral de lunes a viernes para la mayor parte del año. A mediados de año, vimos un corte de este patrón marcado por un aumento drástico en tráfico bloqueado por nuestros productos de seguridad, con frecuencia cuadruplicando la primera parte del comportamiento normal del año.

A mediados de febrero, estas regiones experimentaron varios picos en el correo electrónico no deseado web. Mientras que el volumen de correo electrónico no deseado aumentaba globalmente, afectaba de manera desproporcionada a la región Asia-Pacífico, Japón y China (APJC).

En APJC, el tráfico sospechoso era menos periódico y experimentaba grandes cambios en volumen entre enero y febrero. Estos cambios se nivelaron durante la primavera y el comienzo del verano.

Varios eventos internacionales y ciberataques principales superpuestos en el gráfico sugieren cómo dicha actividad puede afectar el panorama de amenazas. Mientras que es imposible probar la causalidad, hay varias correlaciones entre los patrones de tráfico regionales y globales sospechosos que observamos y los grandes eventos mundiales.



Principales vulnerabilidades dirigidas

En 2023, los actores de ciberamenazas atacaron vulnerabilidades de software anteriores en aplicaciones comunes. En muchos casos, las vulnerabilidades tenían más de 10 años, y eran compatibles con el hallazgo de CISA de que los adversarios han apuntado a viejas fallas de seguridad más que a aquellas divulgadas recientemente en los últimos años. De hecho, cuatro de las cinco vulnerabilidades más apuntadas que observamos CISA también las citó como frecuentemente atacadas en años anteriores, lo que destaca áun más este punto. Esto pone de relieve la necesidad de entidades para instalar regularmente actualizaciones de software, ya que es probable que muchos de estos sistemas no tengan parches dada la edad de las vulnerabilidades objetivo.

Las vulnerabilidades objetivo se encuentran en aplicaciones comunes, como Microsoft Office. Además, CISA corrobora este hallazgo, que señala que los actores en 2022 priorizaron los CVE que prevalecen más en las redes de sus dispositivos. Los adversarios probablemente priorizan dirigir vulnerabilidades masivas porque los ataques desarrollados para dichos CVE pueden tener un uso prolongado y un alto impacto.

Por último, la mayoría de las vulnerabilidades de nuestra lista causaría un impacto sustancial en caso de que fueran atacadas, con seis recibiendo una puntuación de riesgo de vulnerabilidades máxima de 100 de Cisco Kenna y siete recibiendo la puntuación "crítica" más alta del sistema de puntuación de vulnerabilidades comunes (CVSS). La mayoría de los CVE están listados en el catálogo de Vulnerabilidades Explotadas Conocidas de CISA, que pretende informar a los usuarios sobre las fallas de seguridad para las que deberían priorizar la corrección. La alta frecuencia de intentos dirigidos contra estos CVE, asociados con su gravedad, pone de relieve el riesgo de los sistemas sin parches.

Clasificación	CVE	Proveedor	producto	Hallazgos de CISA	Catálogo de KEV de CISA	Kenna/CVSS
1	CVE-2017-0199	Microsoft	Office y WordPad	Atacado de manera rutinaria en 2022	✓	100/9,3
2	CVE-2017-11882	Microsoft	Servidor de intercambio	Atacado de manera rutinaria en 2022	✓	100/9,3
3	CVE-2020-1472	Microsoft	Netlogon	Atacado de manera rutinaria en 2022	✓	100/9,3
4	CVE-2012-1461	Servicios del analizador de archivos mediante Gzip	Varios productos antivirus		✗	58/4,3
5	CVE-2012-0158	Microsoft	Empleados de oficina	Explotados comúnmente por los actores patrocinados por el estado de China, Irán, Corea del Norte, y Rusia (2016-2019)	✓	100/9,3
6	CVE-2010-1807	Apple	Safari		✗	84/9,3
7	CVE-2021-1675	Microsoft	Windows (administrador de cola de impresión)		✓	100/9,3
8	CVE-2015-1701	Microsoft	Windows (controladores de modo núcleo)		✓	72/7,2
9	CVE-2012-0507	Oracle	Java SE		✓	100/10
10	CVE-2015-2426	Microsoft	Windows (controlador de fuente)		✓	100/9,3

Fuente: Cisco Secure Endpoint

Fuentes de CISA: Principales vulnerabilidades explotadas de manera rutinaria, 2022 y 2016-2019.

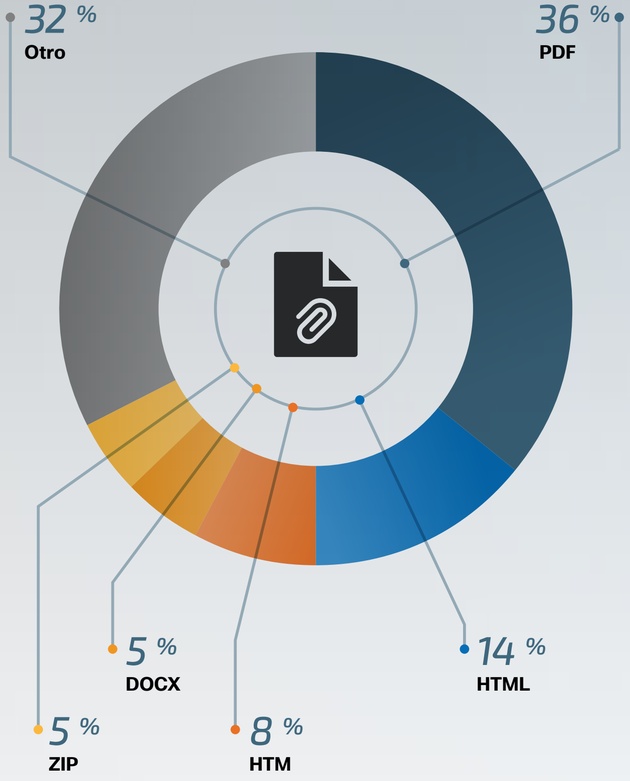
Hallazgos de correos electrónicos

PRINCIPAL ADJUNTO BLOQUEADO EXTENSIONES DE ARCHIVO

Los correos electrónicos de suplantación de identidad (phishing) son una de las formas más comunes en las que los adversarios ponen en riesgo a las víctimas y esto ha sido siempre una amenaza principal en los hallazgos de Talos IR durante años. Solo el año pasado, el 25 por ciento de los vectores de acceso de inicio identificados en las participaciones de Talos IR estaban compuestos de suplantación de identidad (phishing) (esto se puede ver en el gráfico 3b). Esta observación es compatible con los hallazgos del gobierno de EE. UU., con el FBI que menciona que la suplantación de identidad (phishing) fue el incidente principal informado a su Centro de quejas de delitos en Internet (IC3) en 2022.

Los actores de amenazas comúnmente envían correos electrónicos no solicitados en los que piden a los usuarios que descarguen o abran un adjunto para distribuir malware. Si bien la extensión de los archivos no es necesariamente indicativa del tipo de archivo, con frecuencia los actores tratan de esconder malware bajo extensiones de archivos conocidas para parecer menos sospechosos, y así es más probable que los abran. Por ejemplo, a principios de este año, el equipo de respuestas a emergencias informáticas de Japón (JP-CERT) advirtió que los adversarios estaban incorporando documentos de Word maliciosos en archivos PDF para desviar la detección, una estrategia de la que hemos visto que los actores de amenazas dependen.

Además, la decisión de 2022 de Microsoft de bloquear macros, que hasta ese momento los adversarios habían abusado en gran medida, es probable que afectara la preferencia del tipo de archivo de los actores de amenazas, Con este cambio, los actores han dejado de usar archivos de Microsoft Office como Word y Excel como lo hicieron una vez. En 2023, vimos al cargador de productos básicos Ursnif incorporar adjuntos de PDF maliciosos en sus operaciones de suplantación de identidad (phishing) por primera vez mientras este actor y otros grupos buscaban formas de evitar depender de los macros.



Fuente: *Cisco Email Security Appliance*

Nota: *Se excluyó a los tipos de archivos comunes y relacionados con imágenes, como JPG, JPEG, PNG y GIF, de la lista porque aparecen con frecuencia en una abrumadora cantidad de correos electrónicos benignos, como aquellos que contienen gráficos en las firmas de los remitentes o en el cuerpo del correo electrónico.*

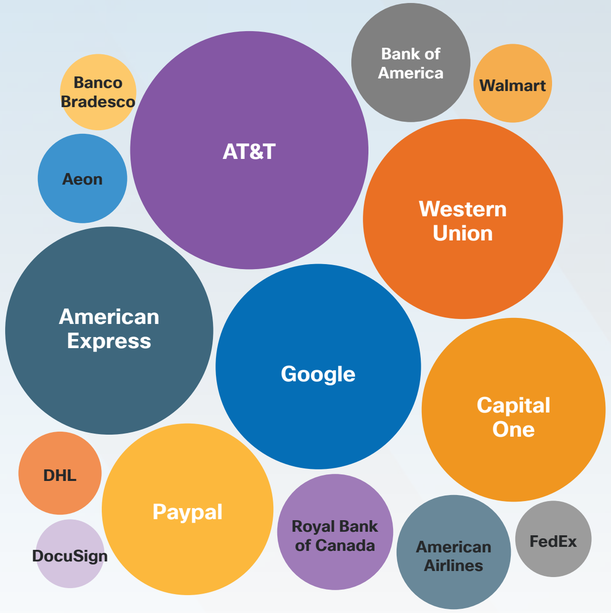
PRINCIPALES VECTORES DE ACCESO DE INICIO, SEGÚN TALOS IR

Nota: *Con frecuencia es difícil determinar el vector acceso de inicio debido a varias razones, entre ellas insuficiente registro o falta de visibilidad en el entorno afectado, lo que hace que "desconocido" sea muy representativo.*

PRINCIPALES MARCAS FALSIFICADAS EN LOS NOMBRES DE LOS EMISORES

Los cibercriminales y otros actores maliciosos dependen en gran medida de tácticas de ingeniería social para poner en riesgo a los usuarios, que es por lo cual comúnmente imitan empresas conocidas en correos electrónicos de suplantación de identidad (phishing). Por ejemplo, los cargadores de productos básicos como Emotet y Trickbot usan de manera rutinaria facturas falsas, estados bancarios o notificaciones de envío como temas para suplantación de identidad (phishing) para simular legitimidad. Esto se refleja en nuestra lista de principales marcas falsas, donde vemos que las entidades de servicios financieros y servicios de envío estaban entre aquellos que los actores falsificaban con más frecuencia.

Además, las operaciones del riesgo del correo electrónico comercial (BEC) aprovechan los nombres de empresas falsas para mejorar su legitimidad. El BEC es una estafa en la que los cibercriminales les envían correos electrónicos a destinatarios que parecen venir de una fuente conocida y hacen una solicitud legítima. El objetivo es impulsar al destinatario a hacer transferencias de dinero no autorizadas al actor de amenaza. Los actores pueden hacerse pasar por marcas confiables y conocidas, como esas representadas en nuestra lista, para engañar a los usuarios. Según el FBI, el BEC ha estado en alza en los últimos años y dio como resultado 2,7 mil millones en pérdidas en 2022.



Fuente: *Cisco Email Security Appliance*

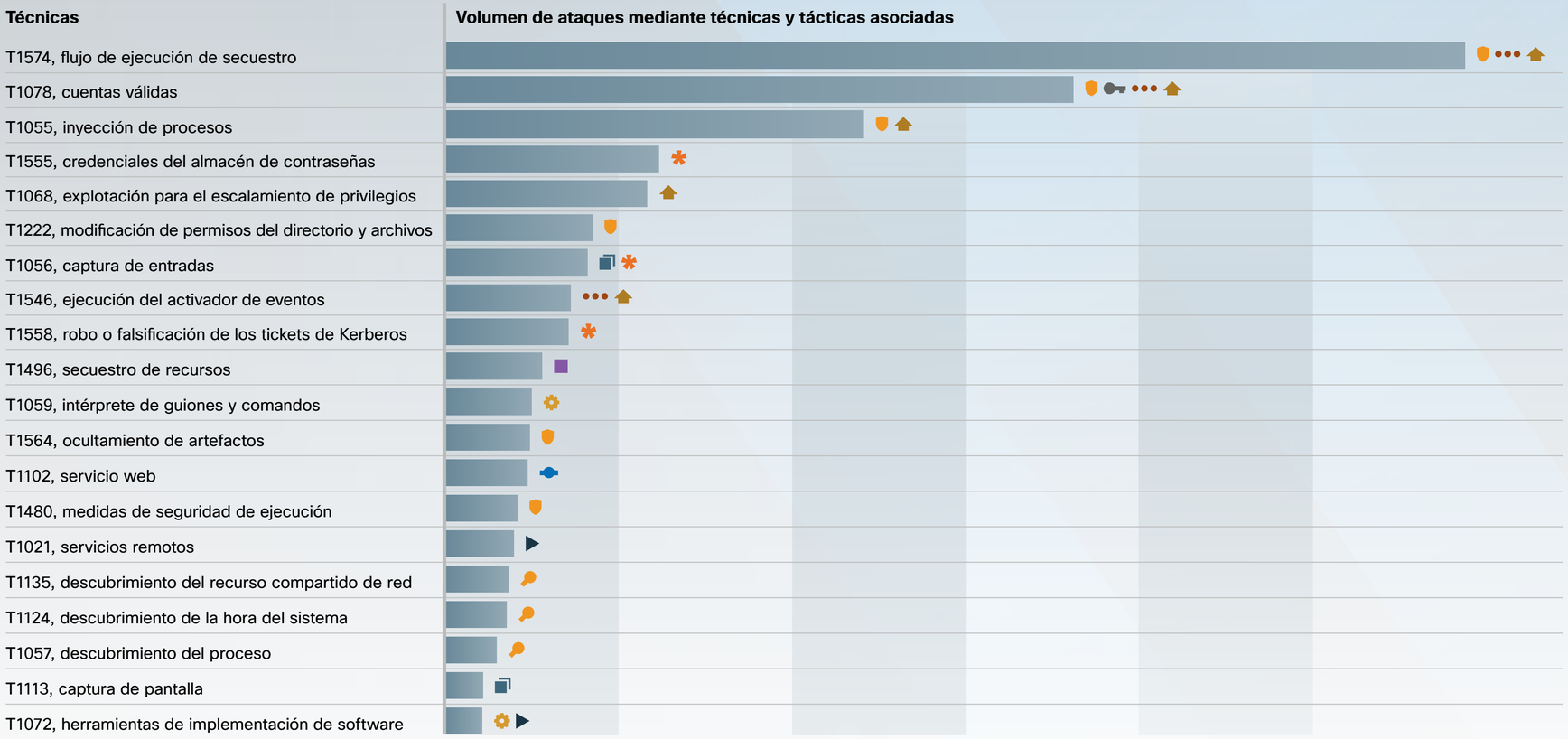
Principales técnicas de MITRE ATT&CK

Especialmente, casi un tercio de las 20 técnicas principales más comunes de MITRE ATT&CK es parte de la táctica de **evasión defensiva**, lo que sugiere que los actores están destinando recursos sustanciales en esta etapa de cadena de ataque. Las técnicas relacionadas con el **escalamiento de privilegios** y la **persistencia** también tuvieron una clasificación alta y se resaltó su importancia en ciclo de vida del ataque.

El flujo de **ejecución de secuestro** fue la técnica más común y apareció casi dos veces más que el siguiente resultado más alto. El flujo de ejecución de secuestro hace referencia a actores que se apropian de la forma en la que el sistema operativo ejecuta programas en un terminal objetivo. La carga lateral de DLL es un ejemplo común de esto, mediante la cual los actores básicamente posicionan su malware en la aplicación de la víctima. Entonces cuando el programa busca su DLL legítima, también ejecuta la carga útil maliciosa de manera involuntaria. Esta es una manera efectiva para que los actores escondan sus actividades bajo software confiable y legítimo, una técnica que comúnmente provechan los cibercriminales y las APT.

El uso de las **cuentas válidas** fue la segunda técnica más común que observamos, que pone de relieve la dependencia de los adversarios de las credenciales en riesgo y el uso de cuentas existentes. Los actores usan esta técnica para habilitar varias etapas de la cadena de ataque. Comúnmente vemos cargadores de productos básicos que implementan malware de robo de información para este mismo propósito. Del mismo modo, las **credenciales de contraseñas almacenadas** se posicionaron entre las cinco principales, y se destacó aún más el enfoque de los actores para obtener credenciales de usuario. Estos hallazgos son compatibles con los datos de Talos IR, que mostraron credenciales/cuentas válidas en riesgo que dieron cuenta de casi un cuarto de vectores de acceso de inicio conocidos en 2023.

Secuestro de recursos, posicionados entre las 10 principales, es una técnica que generalmente se asocia con la implementación de malware de minería de criptomonedas, que secuestra la potencia de procesamiento de un terminal para obtener ganancias rentables. Las amenazas de minería de criptomonedas son bastante comunes, ya que este es un tipo de ataque de bajo nivel generalmente llevado a cabo por actores sencillos. Con frecuencia vemos este tipo de malware implementado, en especial justo después de que se divulgan nuevas vulnerabilidades, antes de que las víctimas tengan tiempo de poner parches o junto con otro malware más complejo.



CISCO TALOS

REVISIÓN DEL AÑO

2023

Ransomware y extorsión

Puntos destacados de la sección

- Los incidentes de ransomware y pre-ransomware continúan afectando a los usuarios a un ritmo constante, que asciende al mismo 20 por ciento de los incidentes de Talos IR del año pasado, con los servicios de salud como la vertical más apuntada.
- Por segundo año consecutivo, LockBit fue el grupo de ransomware como servicio (RasS) más productivo, según nuestros hallazgos, compatible con la evaluación de CISA que es la variante de ransomware más implementada. LockBit fue una de las amenazas de ransomware más observadas con frecuencia en Talos IR este año, y los afiliados dieron cuenta de más del por ciento de la cantidad total de publicaciones de las víctimas sobre los sitios que filtran datos en 40 grupos de ransomware que monitoreamos.
- ALPHV, Clop y BianLian también dominaron el panorama de amenazas, y dieron cuenta de otro cuarto de toda la vulneración de extorsiones de ransomware o datos publicados en sitios de actores de la web oscura.
- Vimos a las filiales de Clop atacar siempre a las vulnerabilidades de día cero, una táctica muy inusual dada la experiencia, el personal y el acceso necesario para desarrollar dichos ataques. Esto sugiere que el grupo posee un nivel sofisticación o recursos relacionados solo por amenazas persistentes avanzadas (APT).
- Están surgiendo nuevas variantes de ramsonware que aprovechan códigos fuente filtrados de otros grupos de RaaS, que permiten actores con menos habilidades ingresar a este espacio. Al mismo tiempo, vemos operadores muy sofisticados como Clop que aprovechan las vulnerabilidades de día cero a un ritmo sin precedentes, una dicotomía interesante que demuestra la amplitud de actores en este espacio.
- Los actores están recurriendo a la extorsión de datos más que nunca, siendo esta la principal amenaza a la que Talos IR respondió en el segundo trimestre en 2023 (de abril a junio). La extorsión del robo de datos parece muy similar a la actividad de pre-ransomware, lo que crea retos para los defensores.
- Algunos actores están abandonando el uso de ransomware por completo, y en lugar de eso optan por la extorsión, una tendencia probablemente influenciada por operaciones continuas del cumplimiento de la ley, mejores detecciones de la industria y menores costos operativos.

El espacio de ransomware se mantuvo dinámico durante 2023, con grupos continuamente renovándose o fusionándose, con frecuencia actores trabajando para equipos de ransomware como servicio (RaaS) sin interrupción y nuevo grupos surgiendo continuamente. Los niveles de habilidades también variaron en gran medida, con actores experimentados que desarrollaron ataques sofisticados para las vulnerabilidades de día cero, mientras los actores más sencillos dependieron del código de ransomware reutilizado para crear sus propias amenazas. Además, vimos una tendencia emergente en este espacio, ya que los actores comenzaron a abandonar el uso de ransomware y recurrir a la extorsión del robo de datos pura sin archivos encriptados, lo que presenta una nueva línea de retos para los defensores. A pesar de estos cambios, una cosa permanece constante: el ransomware sigue siendo una amenaza principal para las entidades mundiales.

Los ataques de ransomware persisten a un ritmo constante

El ransomware y el pre-ransomware constituyeron el 20 por ciento del total de los incidentes a los que Talos IR respondió este año, una caída mínima en comparación con el año pasado. Para los defensores puede ser difícil determinar qué constituye un ataque de pre-ransomware si un binario del ransomware nunca se ejecutó y la encriptación no se lleva a cabo. Sin embargo, hay algunas indicaciones que los analistas usan para evaluar si un ransomware es el objetivo final probable, como el uso de marcos de simulación de adversarios como Cobalt Strike o herramientas para extraer credenciales como Mimikatz, el aprovechamiento de ciertos activos fundamentales como copias de respaldo o enumeración y técnicas de descubrimiento.

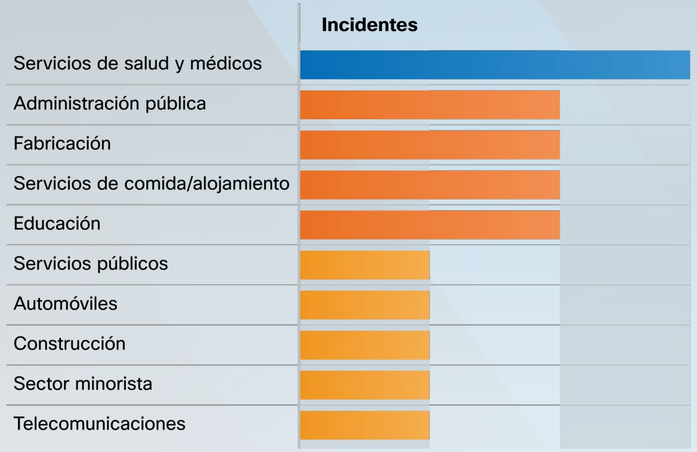
El sector de los servicios de salud y la salud pública fue la vertical más apuntada en las participaciones de ransomware y pre-ransomware de Talos IR este año, en comparación con el sector de la educación en 2022, como se informó en el reporte Revisión del año del año pasado **(consulte Figura 1)**. Las organizaciones en el sector salud son muy vulnerables a ciberataques dada su tolerancia de tiempo de inactividad baja, con frecuencia los presupuestos de ciberseguridad con fondos insuficientes y la posesión de información de salud protegida (PHI) que es valiosa para los actores de amenazas. La pandemia de COVID-19 es probable que haya exacerbado esta situación en los últimos años, con los proveedores del sector salud liberados de una perspectiva de recursos y tiempo de inactividad incluso aún menos tolerable.

Los viejos enemigos son los principales atacantes mientras que LockBit sigue siendo la amenaza principal

Por segundo año consecutivo, Lockbit fue el grupo de RaaS más activo, y dio cuenta de más de 25 por ciento de la cantidad total de publicaciones realizadas en los sitios de filtración de datos. LockBit, ALPHV, Clop and BianLian dieron cuenta de casi el 50 por ciento del total de las publicaciones realizadas en sitios de filtración este año **(Figura 2)**.

FIGURA 1

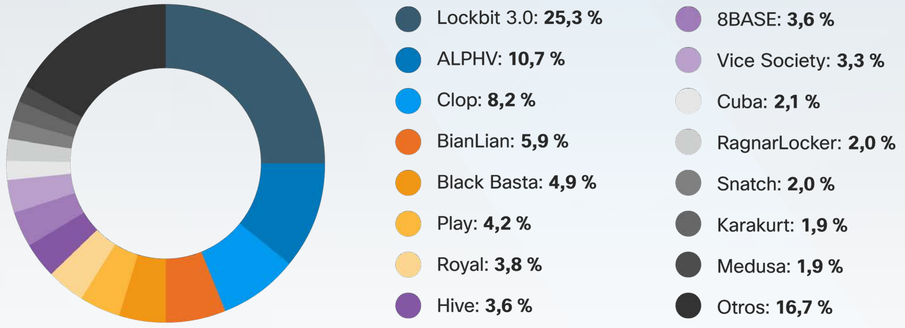
Incidentes de ransomware y pre-ransomware de Talos IR por sector



"El sector de los servicios de salud y la salud pública fue la vertical más apuntada en las participaciones de ransomware y pre-ransomware de Talos IR este año, en comparación con el sector de la educación en 2022".

FIGURA 2

Cantidad de publicaciones realizadas en sitios de filtración de datos



Talos IR responde al incidente de LockBit que afecta a la TI y redes TO

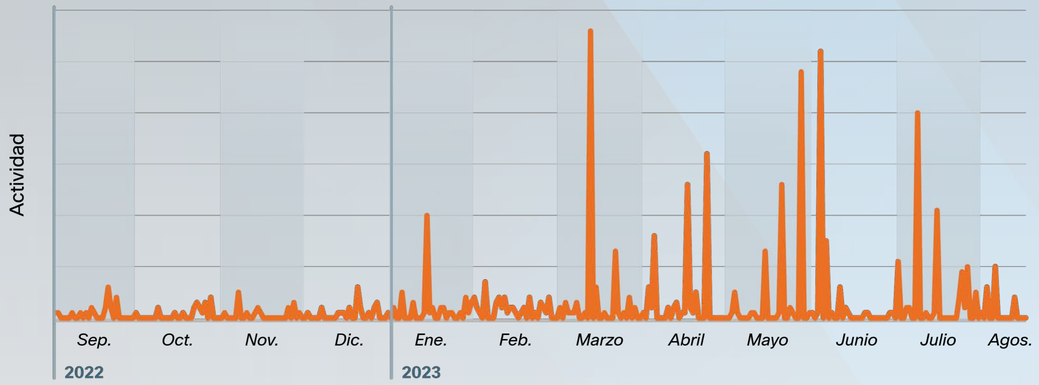
Talos IR respondió al incidente de ransomware de LockBit que afectó a una empresa de servicios públicos donde el ransomware se infiltró en la TI y las redes de TO de la organización. Esto afectó de manera significativa a la víctima y las interrupciones descendentes a los clientes. La filial de ransomware obtuvo acceso de inicio mediante las credenciales válidas de router que se autenticaron sobre la VPN donde no se implementó la autenticación multifactor (MFA). Los atacantes encriptaron servidores de producción, incluidos aquellos que monitoreaban la matriz eléctrica y tres de los cuatro controladores de dominios también estaban encriptados.

LockBit continuó llevando a cabo operaciones de ransomware prolíficas en 2023, un hallazgo que se alinea con la evaluación de CISA que es la variante de ransomware más implementada. Los ataques de Lockbit pueden ser muy impactantes y afectan a las redes de la tecnología de la información (TI) y la tecnología operativa (TO) de una empresa, el hardware y las máquinas responsables de los procesos físicos, como hemos observado en las participaciones de Talos IR. En octubre, CISA publicó una guía de orientación para asegurar entornos de TO y así poner de relieve qué tan significativo puede ser el impacto para estos sistemas. Se implementó LockBit durante el ataque de dos vulnerabilidades en el software PaperCut, una solución de administración de impresión usada ampliamente en entidades en sectores verticales de educación y gobierno, entre otras.

Las publicaciones realizadas en el sitio de filtración de datos del grupo subieron y bajaron durante el año, con detecciones de actividad de LockBit con picos en marzo. Esto coincidió de manera parcial con la implementación de LockBit contra instancias vulnerables del software de administración de impresoras PaperCut, donde siguió siendo alto de manera constante **(Figura 3)**.

FIGURA 3

Actividad de LockBit durante el año



El espacio de ransomware está repleto de grupos renombrados y nuevos

La constante renovación o rotación de los grupos de ransomware fue una tendencia destacada este año. Varias filtraciones de generadores y código fuente de ransomware, componentes esenciales para crear y modificar ransomware, han tenido un efecto significativo en el panorama de amenazas de ransomware. Estas filtraciones les permiten a los operadores de ransomware renovar u otorgar a los actores más sencillos la capacidad de generar su propio ransomware con más facilidad y menos esfuerzo o conocimiento. A medida que más actores ingresan en este espacio, Talos está viendo una cantidad de variantes de ransomware en aumento que emergen y aprovechan códigos de ransomware filtrado, y con frecuencia conducen a ataques más frecuentes y nuevos retos para los defensores y profesionales de la ciberseguridad, particularmente relacionados con la atribución de los actores.

El volumen de las nuevas variantes de ransomware en función del código fuente filtrado también pone de relieve la velocidad a la cual los actores se benefician de dichas divulgaciones públicas. Más recientemente, observamos un aumento en nuevas variedades de ransomware que emergen del generador de ransomware Yashma. Yashma, que apareció por primera vez en mayo de 2022, es una versión renombrada del generador de ransomware Chaos (v5), que se filtró en abril de 2022. Desde principios de 2023, hemos visto surgir nuevas variedades de Yashma, incluidas ANXZ y Sirattacker, probablemente implementadas por filiales más pequeñas o grupos de ellas con menos recursos dada su falta de adopción y notoriedad generalizada en el panorama. En abril, descubrimos un nuevo actor de ransomware, RA Group, que implementaba su

variante de ransomware en función de su código fuente filtrado de Babuk. Desde que un supuesto miembro del grupo Babuk filtró el código fuente completo de su ransomware en septiembre de 2021, han surgido varias nuevas variantes en función del código filtrado. Muchas aparecieron en 2023, incluidas ESXiArgs, Rorschach y RTM Locker.

Mientras que estos cambios en el panorama de amenazas han beneficiado ampliamente a las filiales, los defensores e investigadores de seguridad también tienen una ventaja con el acceso al código filtrado. Permite a los investigadores de seguridad analizar el código fuente y entender los TPP del atacante y desarrollar reglas de detección efectivas, potencialmente ayudar en la creación de descifradores y mejorar las funcionalidades de los productos de seguridad al combatir amenazas de ransomware.

Filiales que recurren a la extorsión del robo de datos durante la implementación de ransomware

Incluso con la cantidad de opciones de RaaS en aumento, algunos han alcanzado el éxito al extorsionar a cambio de fondos sin implementar ransomware. En estos casos de extorsión, un adversario roba datos de la víctima, pero no los cifra. Por esa razón, la táctica de la doble extorsión se elimina, y el actor depende solamente de la amenaza de filtrar la información en lugar de exigir un pago para desbloquear los archivos. Esta tendencia también se refleja en las participaciones de Talos IR, donde la extorsión fue la amenaza más observada en el segundo trimestre de 2023, lo que da cuenta de casi un tercio de las amenazas vistas, un 25 por ciento de aumento comparado con el trimestre anterior (de enero a abril) **(Figura 4)**.

Varios grupos conocidos de ransomware, incluidos Babuk, BianLian and Clop, han optado por la extorsión del robo de datos por sobre el ransomware, una partida de la cadena de ataque de ransomware típica de los grupos **(Figura 5)**.

Es probable que varios factores hayan contribuido a las preferencias de algunos actores de amenazas por la extorsión del robo de datos en lugar de la implementación de ransomware. EE. UU. y el cumplimiento de la ley internacional han buscado sustancialmente actores de ransomware en los últimos años, lo que condujo a interrupciones graves contra grupos conocidos. Es probable que los avances en las funcionalidades de detección y respuesta de terminal (EDR) hayan sido un obstáculo para actores de amenazas que buscan implementar ransomware y datos cifrados. Los adversarios parecen considerar la técnica como una forma viable para recibir un pago, lo que demuestra cómo los actores de ransomware están constantemente trabajando sobre los avances en EDR, operaciones de cumplimiento de la ley y otras barreras.

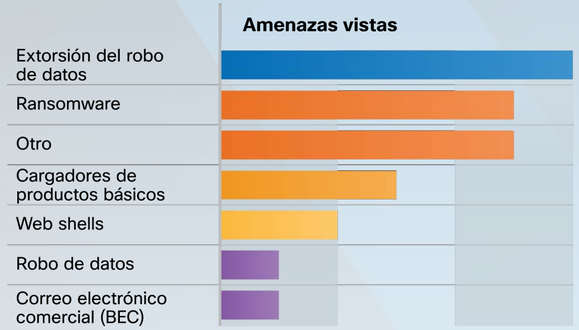
Si bien la extorsión ha demostrado ser una amenaza efectiva y grave, aún no ha superado la amenaza de ransomware que ha sido un reto para las organizaciones y los defensores durante los últimos años. Continuamos monitoreando los efectos a largo plazo de esta tendencia.

Algunos grupos de ransomware aprovechan días cero de manera uniforme y con frecuencia afectan a varias organizaciones.

Mientras que muchos adversarios inexpertos dependen de la reutilización de código este año, también continuamos viendo operadores muy sofisticados que atacan vulnerabilidades de día cero a un ritmo sin precedentes. Esto destaca la amplia diversidad técnica de actores y TTP en este espacio. Los actores de ransomware, conocidos por ser oportunistas, son rápidos para atacar las fallas cuando se hacen públicas. Cuando Clop, un grupo

FIGURA 4

Según Talos IR, la extorsión del robo de datos fue la amenaza principal en el segundo trimestre (de abril a junio de 2023),



¿Cuál es el impacto del código fuente de ransomware filtrado?

Cuando se filtra el código fuente del ransomware o los generadores, es más fácil para los cibercriminales que carecen de experiencia técnica desarrollar sus propias variantes de ransomware al hacer solo pequeñas modificaciones al código original. Además, al usar el código fuente filtrado, los actores de amenazas pueden confundir o engañar a los identificadores, ya que es probable que los profesionales de seguridad no atribuyan la actividad correctamente al actor incorrecto.

(Proviene de una investigación publicada en el blog de Talos)

FIGURA 5

Grupos destacados recurren a la extorsión del robo de datos cada vez más en los últimos años

Babuk

Un grupo de ransomware anterior que anunció públicamente su cambio a la extorsión del robo de datos en abril de 2021.

Karakurt

Un grupo de extorsión del robo de datos que apareció por primera vez en junio de 2021.

RansomHouse

Un grupo de extorsión del robo de datos que apareció por primera vez en diciembre de 2021.

Lapsus$

Un grupo de extorsión del robo de datos que apareció por primera vez en diciembre de 2021.

Clop

Un grupo de ransomware que también realizó ataques de extorsión del robo de latos lucrativos en 2023.

BianLian

Un grupo de ransomware que ha realizado extorsiones de robo de datos desde enero de 2023.

FIGURA 6

Línea de tiempo de grupos de ransomware que aprovechan vulnerabilidades destacadas

ENERO DE 2023

El grupo de ransomware Clop lanza campañas con vulnerabilidades de día cero (CVE-2023-0669) con enfoque en la plataforma GoAnywhere MFT.

ABRIL DE 2023

Los actores maliciosos comienzan a explotar vulnerabilidades en PaperCut (CVE-2023-27350) a partir de mediados de abril de 2023.

PaperCut tiene conocimiento de servidores sin parches explotados libremente y atribuidos a Clop.

Los actores maliciosos para la ejecución remota de código (RCE) explotan activamente PaperCut para implementar el ransomware Lockbit.

MAYO DE 2023

El grupo de ransomware Bl00dy explota servidores vulnerables PaperCut.

Clop comienza a explotar una vulnerabilidad conocida previamente como inyección SQL (CVE-2023-34362) en la solución de transferencia de archivos administrada (MFT) de Progress Software.

de extorsión de datos y un ransomware de alto perfil, reclama responsabilidad pública para atacar las vulnerabilidades de día cero, las filiales de ransomware adicionales rápidamente lo imitan y buscan sistemas afectados antes de que se emitan los parches **(Figura 6)**.

En abril, poco después de que la empresa de software de administración de impresiones PaperCut tenga conocimiento de los servidores sin parche atacados libremente por Clop, otros grupos de ransomware comenzaron a atacar vulnerabilidades de ejecución remota de código (RCE) (CVE-2023-27350) como parte de su cadena de ataque. Esto destaca la naturaleza generalizada de esta actividad y la estrategia de los operadores de ransomware, con frecuencia en función de las divulgaciones de otros grupos que aprovechan fallas de seguridad de alto perfil para aumentar las posibilidades de obtener pagos de las víctimas.

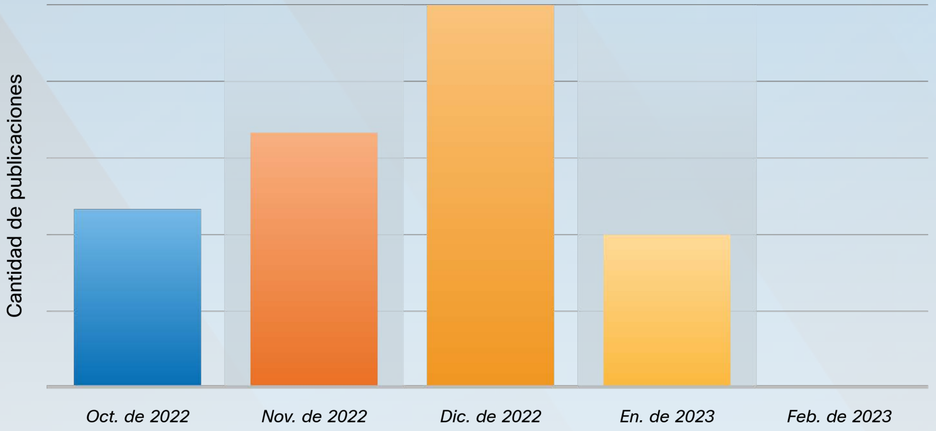
Los esfuerzos repetidos de Clop para atacar las vulnerabilidades de día cero es muy inusual para un grupo de ransomware dados los recursos necesarios para desarrollas dichas funcionalidades. Vimos muchos ejemplos de esto en 2023, a comienzos de enero, cuando el grupo de ransomware Clop lanzó una campaña que aprovecha la vulnerabilidad de día cero, (CVE-2023-0669) con enfoque en la plataforma GoAnywhere MFT. En mayo, Clop se responsabilizó por los ataques que involucraron a otra falla de día cero (CVE-2023-34362) que afectó a la solución de transferencia de archivos de Progress Software, MOVEit Transfer. Además, estos ataques demostraron el amplio kit de herramientas de Clop, ya que los operadores implementaron un web shell invisible, denominado LemurLoot, para exfiltrar los datos de las víctimas y exigir pagos en sistemas que ejecutan MOVEit.

Todas las vulnerabilidades aprovechadas por filiales/grupos de ransomware destacadas anteriormente recibieron puntuaciones del CVSS de gravedad crítica o alta, y resultaron ser atacadas fácilmente por Cisco Kenna e incluidas en el catálogo de Vulnerabilidades Explotadas Conocidas de CISA.

Dados los recursos necesarios para desarrollar o identificar dichos ataques, es posible que Clop o ciertos miembros tengan un nivel de sofisticación y fondos coincidentes solo por las APT. No hay ningún comentario en foros clandestinos sobre cómo Clop puede haber obtenido estos ataques, a pesar de que evaluamos que el grupo puede tener acceso a un desarrollador sofisticado que parece enfocarse en vulnerabilidades de identificación en sistemas de administrados de archivos de terceros y otros periféricos de red.

FIGURA 7

Publicaciones realizadas en el sitio de filtración de datos de Hive desde finales de 2022



Cambios en el panorama en el espacio de RaaS debido a interrupciones en el cumplimiento de la ley

Grupos de ransomware experimentaron interrupciones y los forzó a adaptarse o unirse a otros equipos de RaaS. En enero de 2023, el Departamento de Justicia de EE. UU. anunció que había interrumpido al grupo de ransomware Hive. Para finales de enero, vimos esto reflejado en nuestros datos, con un descenso general en las publicaciones en el sitio de filtración de datos de Hive **(Figura 7)**.

Cuando la infraestructura de ransomware se interrumpe, con frecuencia los operadores continúan su trabajo con otros grupos y crean una situación de nunca acabar para el cumplimiento de la ley y los defensores de redes. Por ejemplo, cuando se interrumpió la infraestructura de Hive, muchos miembros anteriores intentaron unirse a otros grupos de ransomware dentro de los días de la interrupción, según nuestras fuentes. Esta mayor democratización, con una afluencia de nuevos grupos que aprovechan el código de los mismos generadores, introduce complejidades para la actividad de atribuir defensores a grupos específicos ya que los TTP permanecen uniformes en los grupos.

CISCO TALOS

REVISIÓN DEL AÑO

2023

Infraestructura de red

Puntos destacados de la sección

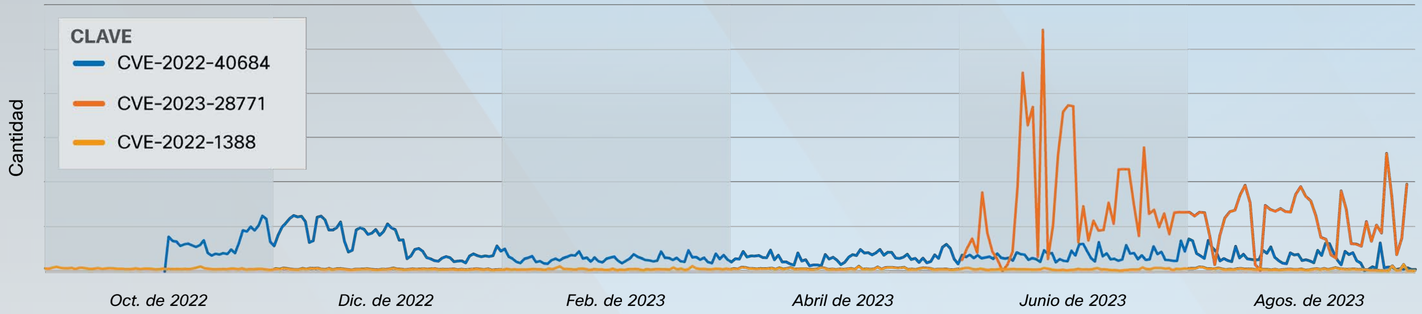
- Los actores avanzados están atacando dispositivos de red a un ritmo preocupante este año, en particular grupos con base en China y Rusia que buscan promover sus objetivos de espionaje y facilitar operaciones furtivas contra los objetivos secundarios.
- Otros cibercriminales están comenzando a imitarlos: adoptan esta técnica para vender acceso no autorizado a estos dispositivos en la web oscura o giran a redes dirigidas e implementan ransomware.
- Los actores aprovechan las debilidades de seguridad, como las credenciales predeterminadas y las vulnerabilidades sin parche, para obtener acceso inicial al dispositivo dirigido.
- Tres o cuatro de las vulnerabilidades de dispositivos más dirigidos en este espacio son críticas o severas, y el ataque puede, en algunos casos, conducir a la adquisición completa del dispositivo. Esto podría brindar a los adversarios acceso irrestricto a componentes principales de un perímetro de seguridad y a la red del objetivo.
- Por lo general, los intentos de ataque contra las vulnerabilidades en este espacio permanecieron uniformes durante el 2023 con picos ocasionales luego de la divulgación pública de las vulnerabilidades. Esto sugiere que con frecuencia las organizaciones dirigidas están fallando en poner parches a sus dispositivos oportunamente, y por lo tanto, los actores continúan viendo valor en los ataques de CVE, incluso a medida que envejecen.
- Para permanecer oculto luego de estar en riesgo y establecer métodos adicionales de acceso sin preocuparse, los actores toman medidas para debilitar defensas dentro del entorno e incluso introducirán nuevas vulnerabilidades para atacar.
- Talos está ayudando a combatir esta amenaza al apoyar la Coalición para la Resiliencia de las Redes, un grupo de líderes de la industria de proveedores de equipos de red, operadores de red y empresas de seguridad que se enfocan en asegurar las redes de datos críticos.

Talos observó un aumento en los ataques sofisticados en dispositivos de red el año pasado, en particular por actores patrocinados por el estado que intentan planificar objetivos de espionaje y facilitar operaciones furtivas. Nuestras investigaciones han involucrado en gran medida a filiales de grupos de amenazas con Rusia y la República Popular China (RPC), a pesar que de que es razonable suponer que cualquier APT suficientemente apta está, o estará, desarrollando la funcionalidad de dirigir la infraestructura de red a medida que el éxito de estos ataques consiga más atención. Recientemente, también hemos observado actividad dirigida de otros cibercriminales, incluidos los agentes de acceso de inicio y los actores de ransomware que buscan beneficiarse del acceso no autorizado a dispositivos dirigidos.

El equipo de redes es un objetivo atractivo para los actores de ciberamenazas maliciosas debido a la amplia superficie de ataque que presenta y el acceso potencial a la red de una víctima que puede ofrecer. A pesar de que estos dispositivos son componentes fundamentales de la infraestructura de TI de una organización y con frecuencia conductos de tráfico de redes confidenciales, no muy a menudo se los examina desde una perspectiva de seguridad y generalmente con parches deficientes. Además, en ocasiones no ejecutan sistemas operativos estándar, pero más bien firmware personalizado único para el proveedor, lo que significa que no se pueden proteger o monitorear con soluciones de seguridad únicas para todos. La dicotomía de alto valor y baja seguridad en estos dispositivos los hace un objetivo principal para el ataque. Debido a la gran presencia de la infraestructura de red de Cisco en todo el mundo, todos estamos bien ubicados para investigar e informar sobre los atacantes de primer nivel y sus campañas.

FIGURA 8

Intentos de ataques de CVE de dispositivos de red lanzados en 2022 o 2023



La seguridad débil con frecuencia vulnera accesos de inicio

Hemos visto actores maliciosos predominantemente obtener acceso de inicio a dispositivos de red al vulnerar vulnerabilidades sin parche, credenciales débiles o predeterminadas o configuraciones de dispositivos inseguras. Mientras que los profesionales de la seguridad no pueden implementar soluciones de EDR estándares en dispositivos de redes como se hace referencia anteriormente, esta observación demuestra que las defensas de la organización contra esta amenaza pueden mejorar en gran medida simplemente a través de rutinas de aplicación de parches, administración de credenciales y monitoreo mejorados. Una vez que se obtiene el acceso de inicio, generalmente los actores de amenaza aprovecharán más la seguridad limitada del dispositivo al destruir evidencia de una intrusión, como eliminar o deshabilitar registros.

El ataque de las vulnerabilidades alcanza un pico después de la divulgación pública

Durante el último año, la actividad de explotación contra las vulnerabilidades en dispositivos de red generalmente permaneció uniforme, a pesar de que en ocasiones alcanzó picos después de divulgaciones públicas, en función de nuestra telemetría. Un aumento repentino en los intentos de explotación podría deberse a varios factores, como una campaña única y muy extensa realizada por un actor de amenazas avanzado, o una actividad generalizada de objetivos que fue repentinamente obstaculizada por reportes ampliamente difundidos y recomendaciones para aplicar parches de seguridad. Comparativamente, los niveles dirigidos uniformes en los meses después de la divulgación sugieren que las organizaciones afectadas fracasan en parchear sus dispositivos oportunamente y, por lo tanto, los actores continúan viendo valor en la explotación de estas vulnerabilidades anteriores, incluso a medida que envejecen.

Por ejemplo, las detecciones para los ID de Snort (SID) 60726 and 60725, que alertan sobre los intentos de explotar la antes mencionada vulnerabilidad de Fortinet (CVE-2022-40684), hizo un pico justo después de que la falla de seguridad a mediados de octubre de 2022, luego disminuyó considerablemente a un nivel uniforme a principios de 2023 **(Figura 8)**. En comparación, los intentos contra los dispositivos vulnerables de Zyxel (CVE-2023-28771; SID 6185) comenzaron a mediados de mayo de 2023, poco después de que se publicara la CVE en abril, y permaneció relativamente nivelado durante los meses siguientes.

Las vulnerabilidades principales dirigidas son muy fundamentales, fácilmente explotables y generalizadas

Las vulnerabilidades que afectan a los dispositivos de red que fueron más seleccionadas en 2023 tienen puntuaciones de gravedad alta, lo que significa que se pueden explotar con facilidad y pueden causar un impacto operativo significativo. De las cinco vulnerabilidades más seleccionada en este espacio, tres tienen una puntuación de CVSS de 9,8 o 10; puntuaciones que se reservan solo para una pequeña cantidad de las más graves CVE. La explotación de las fallas de seguridad severas o críticas en los dispositivos de red pueden, en algunas ocasiones, conducir a la adquisición completa del dispositivo, y así permitirles a los adversarios acceso sin restricciones a componentes principales del perímetro de seguridad y la red del objetivo.

Además, muchos de los dispositivos afectados son ampliamente utilizados por las empresas y gobiernos globalmente y exacerban más el alcance e impacto potencial de una vulneración exitosa. Los actores de amenazas pueden descubrir miles de dispositivos vulnerables al realizar una búsqueda masiva luego de que se divulguen las fallas y también, con frecuencia, pueden encontrar ataques disponibles públicamente.

Finalmente, la variedad de proveedores representada en la siguiente lista demuestra cuán universal es este problema para los proveedores de dispositivos. Los documentos de contratación de inteligencia rusa también respaldan esto, conocidos como los Archivos Vulkan, que Talos obtuvo muestras el año pasado. Estos documentos mostraron que cualquier marca de dispositivo de red era vulnerable a ser objetivo, con un componente de búsqueda que dirige casi 20 routers diferentes y fabricantes de switch.

La mayoría de los CVE enumerados a continuación también se incluyen en la lista de vulnerabilidades de CISA que son generalmente objetivos o tienen explotación conocida. Nuestras dos vulnerabilidades principales también se incluyeron en una asesoría de CISA sobre las amenazas a la infraestructura crítica de EE. UU., lo que demuestra qué tan impactante puede ser la explotación de estas vulnerabilidades.

1. **CVE-2020-5902 (SID 54462):** Remote Code Execution Vulnerability en la interfaz de usuario de la administración de tráfico BIG-IP de F5.
2. **CVE-2019-1653 (SID 48949):** una vulnerabilidad de divulgación de la información en los routers Cisco de la serie RV.
3. **CVE-2022-40684 (SID 60725 60726):** una vulnerabilidad del desvío de autenticación en Fortinet FortiOS, FortiProxy y FortiSwitchManager.
4. **CVE-2023-28771 (SID 61865):** una vulnerabilidad de inyección de comandos no autenticados en varios firewalls de Zyxel.
5. **CVE-2020-3452 (SID 54598):** una vulnerabilidad de salto de directorio en el software de Cisco Adaptive Security Appliance (ASA) y en el software de Cisco Firepower Threat Defense (FTD).

Las descripciones de CVE originadas en el sitio web del Instituto Nacional de Normas y Tecnología (NIST) de los Estados Unidos y los ID de Snort originados en el sitio web de Snort.

Malware en ocasiones instalados después del riesgo para establecer accesos

En algunas ocasiones, observamos actores, particularmente las APT afiliadas a China, que instalaron malware en dispositivos después del riesgo para establecer accesos en la red y permitir actividad de seguimiento. Algunas de las funcionalidades permitidas por el malware que hemos visto incluyen:

- Desviar las listas de control de acceso (ACL) para que el router no pueda bloquear el tráfico.
- Permitir acceso autenticado para dispositivos fuera de los métodos normales de autenticación.
- Permitir la capacidad para dañar y deshabilitar el dispositivo.
- Redireccionar tráfico definidos por actores a infraestructura controlada por actores.

En muchas ocasiones, vemos actores usar binarios externos (LoLBins) ya sea junto con o en vez de la implementación de malware para adelantar sus operaciones y evitar la detección.

En una ocasión más reciente de malware instalado después del riesgo, los actores comenzaron a explotar una vulnerabilidad crítica previamente desconocida (CVE-2023-20198) en septiembre y octubre de 2023 para obtener acceso a ciertos dispositivos de red que ejecutan software Cisco IOS XE. Esto les permitió a los atacantes obtener el nivel de privilegio 15 para el dispositivo, que usaron para explotar un segunda vulnerabilidad de día cero (CVE-2023-20273) para implementar su malware.

En especial, la CVE-2023-20198 afecta específicamente dispositivos expuestos a la Internet y tienen la función del servidor HTTP o HTTPS habilitada, funcionalidades que el Gobierno de EE.UU. había advertido previamente.

Esta actividad pone de relieve las recomendaciones de Cisco, que son compatibles con las mejores prácticas y la orientación que el gobierno de EE. UU. ha brindado en el pasado en cuanto a la mitigación del riesgo de interfaces administradas expuestas a través de Internet. Además, esto está en acuerdo con el trabajo continuo de Cisco con los partners de la industria como parte de la Coalición para la resiliencia de las redes, que se cubre en mayor profundidad a continuación.

Recopilación de información de redes esencial para las operaciones de alta prioridad

Las APT rusas y chinas usan su visibilidad en dispositivos en riesgo para obtener información de redes confidencial, lo que facilita mayor acceso a datos más valiosos. Los actores buscan interceptar y violar datos como credenciales legítimas, detalles de relaciones de dominio confiables, diagramas de red, contratos con clientes de redes e información de configuración. Esta información puede brindar una hoja de ruta para los actores que buscan aumentar sus privilegios y girar en redes de intereses para la recopilación de inteligencia.

Además, las APT toman medidas para debilitar sus defensas dentro del entorno y escindir rutas adicionales para el acceso a largo plazo. Estos métodos incluyen el registro deshabilitado, la modificación de la memoria para reintroducir vulnerabilidades que habían tenido parches, la modificación de las configuraciones para habilitar actividad privilegiada y el reemplazo de firmware con firmware más antiguo y legítimo que se puede modificar en la memoria. Esta variedad de actividades demuestra que los adversarios tienen un alto nivel de comodidad y experiencia trabajando dentro de los confines del equipo de red en riesgo. Además, al establecer estos accesos en un entorno objetivo, los actores buscan erosionar las barreras variables en la arquitectura de seguridad de defensa en profundidad de una organización. Los organizaciones deben actualizar y mejorar sus esfuerzos de protección del sistema y las funcionalidad del monitoreo de la red para defenderse de estos grupos de amenaza

Numerosos dispositivos en riesgo desde redes de anonimización para el tráfico malicioso

Por lo tanto, mientras que las técnicas descriptas son generalmente muy especializadas para víctimas específicas, los actores también sacan provecho indiscriminado y generalizado de los dispositivos de red para facilitar operaciones furtivas contra objetivos secundarios. Hemos observado a las APT afiliadas a China poner en riesgo a varios dispositivos de red globalmente, con consideración limitada del dueño del dispositivo, para formar una red de anonimización que funciona da manera similar a Tor. Los actores usan esta red de dispositivos en riesgo para enviar tráfico malicioso desde y hasta una red dirigida, y de ese modo ofuscar el origen de su ataque. Además, estas APT pueden desviar las defensas de seguridad del objetivo que bloquean el tráfico desde ciertas regiones geográficas al tener el tráfico de C2 emanando de los proveedores de servicio de Internet (ISP) locales a la víctima.

Hemos visto a actores afiliados a China realizar campañas generalizadas para explotar las vulnerabilidades críticas asociadas con los dispositivos de red dentro de los días de la divulgación pública, lo que significa que el tipo de infraestructura dirigida con frecuencia es en gran parte oportunista.

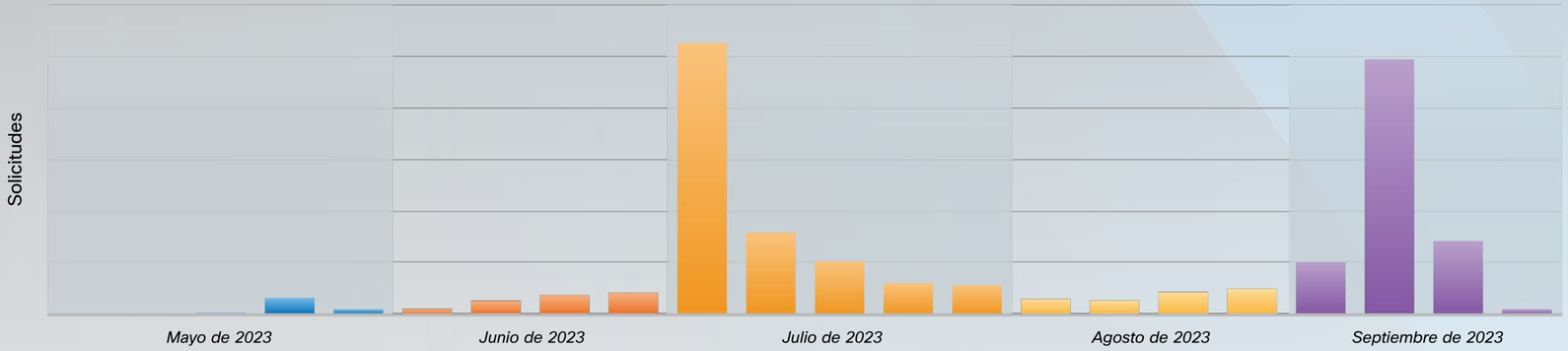
¿Cómo estamos combatiendo esta amenaza creciente?

Cisco lanzó la Coalición para la resiliencia de las redes con los principales partners de la industria en julio de 2023. Esta alianza se enfoca en aumentar el reconocimiento de este problema, comprender su alcance completo y ofrecer recomendaciones procesables para mejorar la seguridad de las redes que respaldan la seguridad nacional y económica global.

Talos ha conducido los esfuerzos para hacer frente a esta amenaza y contribuyó con una cantidad significativa de investigación e información técnica que se publicó en los boletines del gobierno de EE. UU. sobre este tema. Además, hemos aumentado la mensajería a los clientes y los defensores de red sobre cómo mejorar la resiliencia de la infraestructura de red. Participamos activamente en investigaciones y esfuerzos para compartir información con otros proveedores así como también para reforzar la seguridad total del dispositivo. Por ejemplo, el año pasado, nuestro equipo de investigación y descubrimiento de vulnerabilidades de Talos hizo que las pequeñas oficinas de investigación, las oficinas en casa (SOHO) y los routers industriales sean una prioridad principal. Como resultado directo de este esfuerzo, hemos informado 289 vulnerabilidades a los proveedores hasta la fecha, publicadas en 141 boletines de Talos. Estos reportes dieron como resultado la cobertura de detección de intrusiones en la red y varias mejoras en seguridad de cada proveedor. Estas soluciones ayudan a los clientes que implementan soluciones de seguridad de Cisco y mejoran la postura de seguridad para todo aquel que utilice estos dispositivos una vez que se parcheen las vulnerabilidades.

FIGURA 9

Picos en solicitudes relacionadas con WebVPN que coinciden con actividad dirigida a dispositivos ASA



"Los agentes de inicio de acceso y las filiales de ransomware se han vuelto más activas al identificar dispositivos de red el año pasado. Esto puso en riesgo a las credenciales débiles o predeterminadas..."

Los actores de ransomware y los agentes de acceso de inicio violan las credenciales débiles y monetizan el acceso

Los agentes de inicio de acceso y las filiales de ransomware se han vuelto más activas al identificar dispositivos de red el año pasado. Esto puso en riesgo a las credenciales débiles o predeterminadas: ya sea al vender el acceso no autorizado en los mercados de la web oscura o al usarlo para implementar ransomware en redes objetivo.

Este año, respondimos a una campaña dirigida a los dispositivos de Cisco Adaptive Security Appliance (ASA) configurados con WebVPN en la que es probable que los cibercriminales hayan tenido acceso no autorizado a los dispositivos a través de fuerza bruta y ataques de rociado de contraseñas. En julio, observamos un pico significativo en la actividad dirigida a dispositivos ASA configurados con WebVPN, que coincidió con gran parte del público que informó sobre la actividad libre dirigida a dispositivos ASA **(Figura 9)**. Además, un pico en septiembre de 2023 en solicitudes de WebVPN coincide con la asesoría en seguridad de Cisco sobre la divulgación de una vulnerabilidad para CVE-2023-20269. La explotación de esta vulnerabilidad le permite a un atacante remoto realizar ataques de fuerza bruta o a un atacante remoto y autenticado establecer una sesión VPN SSL sin cliente con un usuario autorizado. La capacidad para realizar un ataque de fuerza bruta, combinado con el uso generalizado de credenciales débiles o predeterminadas, permitió un alto impacto contra una gran cantidad de dispositivos. Además, esta actividad destaca la frecuencia en la cual los adversarios intentarán explotar las vulnerabilidades justo después de que se hagan públicas.

Se relacionó públicamente a los grupos de ransomware Akira y LockBit a esta actividad que comenzó en agosto de 2023, a pesar de que no fue claro si estos actores realizaron ataques de rociado de contraseñas o si les compraron acceso a los agentes de acceso de inicio. Se ha observado a estos dos grupos de amenazas realizar actividades similares contra otros proveedores de dispositivos, como FortiGuard. Talos considera que los agentes externos pueden ser responsables del acceso de inicio en muchos de los casos de ransomware en función del volumen y la temporización de la actividad dirigida y la naturaleza de las acciones de seguimiento luego del riesgo. La asesoría en seguridad antes mencionada incluía las recomendaciones y los indicadores de riesgo para ayudar a los defensores a protegerse contra las amenazas, y así destacar la importancia de implementar la MFA adecuada y limitar la cantidad de intentos de inicio de sesión fallidos consecutivos, que reduciría de manera significativa la exposición a esta amenaza.

CISCO TALOS

REVISIÓN DEL AÑO

2023

Amenazas persistentes avanzadas: China

Puntos destacados de la sección

- La actividad afiliada a China ocurrió a un ritmo riguroso este año, probablemente en respuesta a los eventos geopolíticos que provocaron tensión en las relaciones del país con Occidente y Asia-Pacífico.
- En función de nuestro análisis de varias campañas maliciosas, parece que Pekín puede estar dirigiendo una colección de dispositivos inteligentes más agresivos y ubicándose de antemano en caso de ataques futuros contra objetivos en estas regiones.
- Los actores han mejorado en términos de afianzarse a sí mismos profundamente en redes objetivo y evitar la detección o los esfuerzos a respuestas a incidentes, y así ubican una carga más pesada en organizaciones objetivo para mantener sus redes a salvo.
- Talos observó varias ocasiones en las que los actores de ransomware pusieron en riesgo a un objetivo siguiendo de cerca una intrusión APT cubierta y a largo plazo mediante el uso de métodos similares al acceso de inicio y la implementación de ransomware. Mientras la conexión, si la hubiera, entre la APT y los grupos de ransomware sea indeterminada, la temporización de las operaciones y la superposición en los TTP sugiere que los operadores de ransomware pueden al menos tener un conocimiento previo a las campañas de espionaje.
- Las organizaciones de telecomunicaciones fueron un objetivo principal de las ciberoperaciones chinas en 2023, en especial aquellas que ofrecían servicios en áreas de interés estratégico a China, como Guam y Taiwán. Estas entidades son objetivos particularmente atractivos para estos actores, ya que el acceso no autorizado permite una colección de dispositivos inteligentes generalizada en varios sectores críticos.
- La estructura organizativa de las organizaciones de telecomunicaciones y las ubicaciones geográficas de las víctimas con frecuencia plantean nuevos retos a los encargados de respuesta ante incidentes, incluidas la visibilidad limitada en todas las redes afectadas y las sensibilidades políticas al momento de investigar o asignar atribuciones a China.

Mientras que las APT que procedían de varias partes del mundo permanecían activas, la mayoría de nuestras investigaciones este año se centraron en China, Rusia y el Medio Oriente, que se presentan en esta sección del reporte.

Las APT asociadas a China operaron a un ritmo rápido este año, lo que condujo a intrusiones furtivas y sofisticadas en las redes de numerosos objetivos de gran valor. Según nuestra investigación, los actores responsables de estas campañas con frecuencia buscan acceso a largo plazo a redes objetivo, y se establecen varios métodos para mantener persistencia mientras se evitan mecanismos de detección de los objetivos.

TTP centrados ampliamente en evadir la detección y la atribución

Las APT afiliadas a China parecen reducir considerablemente su actividad maliciosa en una red en caso de que se detecte o un actor tenga conocimiento de los esfuerzos a respuestas a incidentes. Es probable que los operadores que mantengan accesos y que esperan hasta que el objetivo no está operando más a un nivel de conocimiento elevado para reanudar su actividad, pone de relieve la importancia de correcciones agresivas y esfuerzos de desalojo y el mantenimiento de planes de respuesta a incidentes actualizados. El éxito de mantener este acceso se evidencia en los largos tiempos de permanencia en redes en riesgo, con una intrusión investigada el año pasado en la que el tiempo de espera fue de al menos siete años. Esto demuestra el grave impacto que estos tipos de campañas pueden tener en organizaciones objetivo, ya que, con frecuencia, la corrección completa requiere un análisis integral de todos los activos de red, soporte a largo plazo de equipos de respuesta a incidentes y acciones para toda la organización como los restablecimientos de contraseñas y las actualizaciones del sistema. Si las entidades objetivo no se comprometen con estos esfuerzos de respuesta, es probable que los actores maliciosos reanuden sus actividades rápida y tranquilamente una vez que perciban que el objetivo sienta que el entorno es seguro.

Otros TTP que usaron las APT asociadas a China el año pasado incluye LoLBins para evadir la detección y el ataque de vulnerabilidades públicas, la identificación de dispositivos de red y el uso de código abierto compartido o herramientas comerciales, todas las cuales no se cambian desde el año pasado. Además, continuamos viendo estas APT conducir operaciones en las que el acceso a la entidad objetivo puede facilitar el riesgo de muchas víctimas, con actores especialmente utilizando esta metodología contra las organizaciones de telecomunicaciones.

La nueva tendencia de la implementación del ransomware después de operaciones de espionaje a largo plazo

En estas pocas ocasiones, después de una intrusión de APT orientada al espionaje, sofisticada y a largo plazo, Talos observó un grupo de amenazas secundario dirigido a la red de la víctima al usar métodos similares de obtener acceso de inicio, como el ataque de vulnerabilidades públicas y luego la implementación de cargas útiles de ransomware. Hemos observado esta tendencia en ciertas industrias, como semiconductores, y regiones, como Guam, sobra la que RPC pone un alto grado de importancia estratégica. A pesar de que aún tenemos que determinar una conexión, si la hubiera, entre dos grupos de atacantes en estas instancias, varios escenarios son posibles:

- Podrían ser ilustrativos de estas APT que participan en ataques destructivos. Hay varios ejemplos de APT chinas que incorporan ransomware en sus operaciones, como Bronze Starling o APT41.
- Podrían comprender actores afiliados con los atacantes originales, como asociados oportunistas que buscan ganancias financieras.
- Además, estos grupos no pueden estar afiliados a China en absoluto, a pesar de que esto puede ser menos probable dada la temporización de la operaciones de ransomware de seguimiento y superponerse en métodos de obtener acceso de inicio.

Ya sea que haya resultado de una colaboración estratégica, una cooperación financiera o tan solo de actores no afiliados que buscan su camino debido a algún otro elemento, como el arte más ruidoso de los adversarios originales, estos ataques representan potencialmente un elemento destructivo, nuevo y peligroso para los ataques APT afiliados a la RPC que evaluamos revela un escalamiento de años previos.

Un ritmo más riguroso de las operaciones probablemente asociadas a cambios en el entorno geopolítico

La actividad dirigida por los APT afiliados a China ocurrió a un ritmo rápido el año pasado, probablemente en parte debido a los factores geopolíticos que el liderazgo chino percibe como amenazas a la gestión del Partido Comunista de China (PCC). Cuantificamos este aumento en la actividad en función de la cantidad de acciones de la inteligencia para partners del gobierno, los proyectos de colaboración con CISA, los casos dirigidos a infraestructura relacionada y las investigaciones de alta prioridad de la actividad de las filiales de China que afecta a los clientes de Cisco.

Este cambio en el ritmo puede reflejar una diferencia en intención, un tipo de señal que no hemos observado en el pasado. Generalmente, Pekín dirige la ciberactividad con la intención de recopilar inteligencia para tratar los objetivos estratégicos, políticos y económicos del PCC. A pesar de que algunos de estos objetivos, como sus planes de cinco años, se establecen regularmente como objetivos a largo plazo para el crecimiento, otras necesidades provisionales se determinan en función de las relaciones de China con otras naciones. Por ejemplo, si una relación con una nación de la que

"La actividad dirigida por los APT afiliados a China ocurrió a un ritmo rápido el año pasado, probablemente en parte debido a los factores geopolíticos que el liderazgo chino percibe como amenazas a la gestión del Partido Comunista de China (PCC)".

Amenazas persistentes avanzadas: China

Puntos destacados de los actores de amenazas: Volt Typhoon

Volt Typhoon es un grupo de amenazas afiliado a China que fue noticia el año pasado por sus operaciones a largo plazo dirigidas a las organizaciones de infraestructura fundamental y las bases militares de EE. UU.

Talos investigó una intrusión de sostenibilidad de Volt Typhoon dirigida al sector de las telecomunicaciones en Guam, que es particularmente la sede de la base militar de EE. UU. importante para la defensa de Taiwán. Nuestra investigación reveló que los actores mantuvieron acceso constante y exfiltraron datos desde redes de un proveedor de servicio y ciertos clientes de gran valor durante al menos un año y medio. Talos continúa colaborando en gran medida con el público y los partners privados en la búsqueda de la actividad de este grupo de amenazas e investiga la infraestructura de anonimización del grupo.

China depende para las exportaciones se deteriora, los actores chinos pueden buscar datos de exfiltración patentados, enfocados en el espionaje aunque deliberadamente silenciosos. Eso puede potenciar su autosuficiencia cualquiera sea esa exportación. Si una nación se vuelve cada vez más litigiosa, China puede buscar establecer accesos en las redes de la infraestructura crítica de esa nación y se posicionan a sí mismas para futuros ataques destructivos.

Numerosos eventos geopolíticos afectaron las relaciones de China con Occidente y Asia-Pacífico este año, lo que condujo potencialmente a indicaciones de PCC para actividades dirigidas más agresivas. Talos realizó operaciones de respuesta a incidentes intensivas para objetivos estratégicos en ambas regiones.

División profunda entre China y Occidente

Uno de los factores principales que ha profundizado la división entre China y Occidente este año ha sido la alianza de la RPC con Rusia, particularmente a medida que otros líderes del mundo han denunciado enérgicamente las acciones de Moscú en la guerra entre Rusia y Ucrania. Los dos países han fortalecido su relación comercial, y las exportaciones en rápido aumento de China a Rusia han atenuado el impacto de numerosas sanciones occidentales que se han aplicado contra el país desde su invasión a Ucrania. Además, Rusia y China se han unido para expandir su presencia en Medio Oriente y los países en desarrollo: realizaron ejercicios militares juntos en el Golfo de Omán en marzo de 2023 e invitaron a numerosas naciones para unirse al grupo BRICS en agosto de 2023, y así reforzaron el bloque de comercio contra la competencia occidental.

Las posiciones y políticas de EE. UU. relacionadas con China no se han suavizado este año, con EE. UU. que continúa clasificando a China como una principal amenaza de seguridad. El director de la Inteligencia Nacional denominó a China la "amenaza más relevante" para la seguridad nacional de EE. UU. en 2023, y EE. UU. ha expandido sanciones de manera constante contra las empresas y organizaciones chinas debido a dichas preocupaciones. Estos problemas de seguridad se ejemplificaron por un accidente a principios de 2023 cuando un globo espía chino voló sobre EE. UU., reunió inteligencia de bases militares y transmitió la información a Pekín antes de ser derribado. EE. UU., Japón y Corea del Sur también reforzaron su alianza en 2023, con los líderes de los países reunidos en Camp David en agosto y comprometidos a trabajar juntos para hacer frente a los retos de seguridad de China y Corea del Sur. Pekín criticó rápidamente esta reunión y declaró públicamente que los intentos de formar bloques militares en Asia-Pacífico se alcanzarán con "vigilancia y oposición".

Conflicto creciente en Asia-Pacífico

Mientras tanto, China ya enfrenta conflictos con naciones vecinas en Asia-Pacífico. Las tensiones entre China y Taiwán han ido en aumento, exacerbadas por el apoyo de EE. UU. en la expansión de las capacidades de defensa propia de Taiwán. El Ejército Popular de Liberación de la (EPL) de la gente ha aumentado su presión militar en la isla al enviar de manera rutinaria aviones de combate, drones y barcos pasando la línea media del Estrecho de Taiwán en muestra de fuerza. Además, China se ha vuelto muy agresiva en el Mar de China Meridional por lo que redobló sus reclamos de soberanía sobre casi toda el área en disputa. Su sólida presencia militar en la región ha provocado separadores y conflicto durante el año pasado con países vecinos que tienen reclamos que compiten por el territorio, así como también las fuerzas armadas de EE. UU. que están presentes allí. Finalmente, la relación de China con Japón también ha presentado retos el año pasado, con eventos como la decisión de Japón de restringir la exportación de semiconductores y la decisión de Tokio de lanzar agua de la central nuclear de Fukushima Daiichi, que generó críticas de Pekín.

Sacar provecho del sector de las telecomunicaciones expande la recopilación y ubica de antemano a los actores para futuros ataques

Respondimos a varias intrusiones en telecomunicaciones brindado por las APT afiliadas a China este año, en particular en áreas que son de interés estratégico para Pekín.

Las organizaciones en telecomunicaciones son objetivos atractivos para estos grupos, ya que con frecuencia controlan numerosos activos de infraestructura fundamental en el país, como sistemas satelitales nacionales, servicios de Internet y redes telefónicas que son importantes para los sectores público y privado. Las APT afiliadas a China pueden usar su acceso no autorizado para establecer accesos para interrumpir servicios fundamentales, como la infraestructura en comunicación, en el caso de un conflicto con una nación objetivo. Además, pueden desplazarse en redes de objetivo de interés adicionales y de gran valor y conducir exfiltraciones generalizadas de datos sensibles.

Existen varias maneras en las cuales el uso de esta última técnica puede desafiar los esfuerzos de reparación. Un proveedor de servicio puede no darse cuenta de inmediato o tener visibilidad del alcance de una intrusión dirigida a otras empresas, suscriptores o proveedores externos, lo que les da a los actores gran cantidad de tiempo para ingresar con más profundidad en redes en riesgo. La orientación para notificar a los clientes sobre una intrusión varía según el país y posiblemente demora la respuesta a incidentes en función de la ubicación geográfica de una víctima inicial. Finalmente, dadas las delicadas relaciones diplomáticas que pueden existir entre el país objetivo y el adversario, los equipos de respuesta a incidentes basados en EE. UU. pueden enfrentar retos y sensibilidades políticas al asistir a ciertas regiones. Las víctimas en ciertos países pueden dudar al asignar atributos a un grupo de amenazas particular, podrían tener lazos organizativos fuertes con China o pueden ser cautelosos al compartir detalles fundamentales del compromiso con los equipos estadounidenses.

CISCO TALOS

REVISIÓN DEL AÑO

2023

Amenazas persistentes avanzadas: Rusia

Puntos destacados de la sección

- La APT Gamaredon patrocinada por el estado ruso ha sido una importante participante en las amenazas contra Ucrania y fue la principal amenaza a la que la Unidad de tareas de Ucrania de Cisco Talos respondió este año.
- En 2023, Gamaredon principalmente dirigió entidades a Norteamérica y Europa, con una cantidad desproporcionada de víctimas en Europa Occidental. Además, más de la mitad de las entidades objetivo se encontraban en los sectores de transporte y servicios públicos, lo que reflejó el enfoque de Rusia en infraestructura fundamental.
- Turla, otra APT afiliada al gobierno ruso, en gran parte estuvo activa entre septiembre de 2022 y febrero de 2023, pero sus operaciones disminuyeron de manera significativa cerca de mayo de 2023, que coincidió con la interrupción del Departamento de Justicia de EE. UU. gracias al malware Snake de Turla.
- La cantidad de sectores afectados y el volumen de víctimas entre estos dos grupos se diferencian ampliamente, y contrastan el objetivo más amplio de Gamaredon con la actividad más limitada de Turla contra víctimas muy selectivas.
- Más allá de la actividad de Gamaredon y Turla, también observamos un pico en la actividad de SmokeLoader, un malware usado por una variedad de diferentes grupos, a finales de abril y comienzos de mayo, que se alinea con el reporte del Equipo de Respuestas a Emergencias Informáticas de Ucrania (CERT-UA) de distribución masiva de SmokeLoader dirigido a entidades ucranianas.
- Para estabilizar la matriz eléctrica de Ucrania contra los efectos del Sistema de Posicionamiento Global (GPS) atascados en el campo de batalla, los ingenieros de hardware y software de Cisco modificaron uno de los cuatros switches de red comercial para brindar mantenimiento al equipo de la matriz eléctrica de Ucrania durante estas interrupciones de suministro.

Amenazas persistentes avanzadas: Rusia

Las amenazas de las APT alineadas con o patrocinadas por el estado ruso sigue siendo un pilar en nuestros esfuerzos de investigación y seguimiento de amenazas de este año. Desde el principio de la invasión rusa a Ucrania, se ha intensificado el compromiso de las APT rusas en ciberespionaje, ciberinfluencia y ataques destructivos. De acuerdo con la actividad mencionada en el reporte del año pasado, las APT rusas continúan adaptándose a los retos geopolíticos que provienen de la guerra y la OTAN y la asistencia militar de las naciones aliadas a Ucrania. Además, el 2023 vio un esfuerzo global para cumplir las leyes para desmantelar el malware Snake, considerado una de las herramientas de ciberespionaje más sofisticadas y prolíficas en el Servicio Federal de Seguridad (FSB) del arsenal de la Federación de Rusia comúnmente implementado contra los sistemas globalmente.

Gamaredon y Turla siguen siendo amenazas principales, los patrones objetivo varían

Los grupos APT afiliados a Rusia Gamaredon y Turla continúan persistiendo como amenazas principales en este espacio, al actualizar aspectos de sus ataques y kit de herramientas para soportar sus TTP, a pesar de los esfuerzos internacionales para combatir ciberamenazas rusas.

Cisco Talos hace un seguimiento de cerca de las actividades asociadas a Gamaredon, una APT sospechada ampliamente de ser un equipo de actores apoyado por el gobierno ruso con sede en Crimea. Mientas que el grupo en meses recientes ha concentrado sus esfuerzos en el ciberespionaje contra las entidades ucranianas, también dirigen entidades globalmente con una victimología menos centrada en comparación con otras APT rusas que operan en este espacio. Turla también realiza espionaje a largo plazo y operaciones de exfiltración de datos que son compatibles con las prioridades de inteligencia rusa que el gobierno de EE. UU. atribuye a una unidad dentro del FSB. A diferencia de Gamaredon, que observamos dirigir un rango de sectores en 2023 (Figura 10), se conoce a Turla por operaciones mucho más dirigidas contra una cantidad menor de entidad estratégicamente importantes. Turla, que públicamente se estima que opera en nombre de una unidad diferente de Gamaredon en el FSB, es probable que sea apto para llegar a un acuerdo con un espectro mucho más amplio de entidades en todo el mundo, pero limita sus operaciones a lo que perciben como objetivos de gran valor.

La cantidad de sectores y volumen de víctimas que Gamaredon y Turla dirigen se diferenciaron ampliamente, en función de nuestra telemetría **(Figuras 10 y 11)**.

FIGURA 10

Sectores verticales dirigidos por Gamaredon

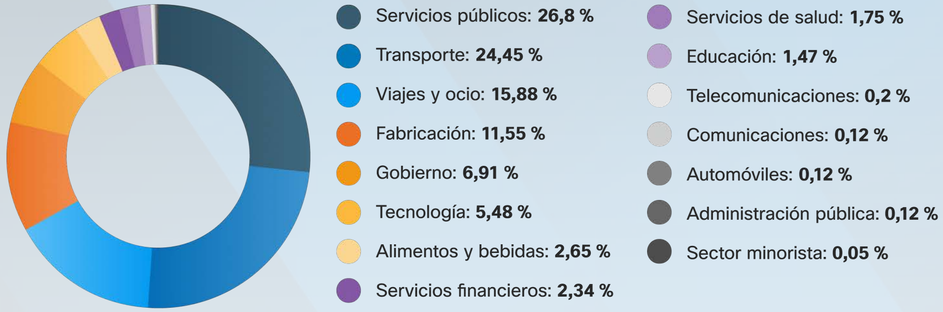
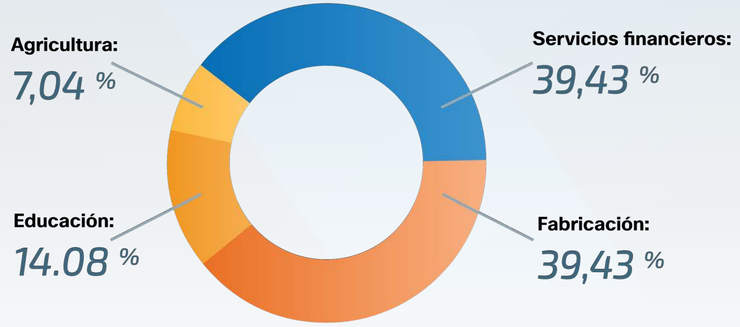


FIGURA 11

Sectores verticales dirigidos por Turla



Nota: *Los porcentajes pueden no ser iguales al 100 % debido al redondeo.*

FIGURA 12

Actividad de descarga maliciosa de Gamaredon durante el año

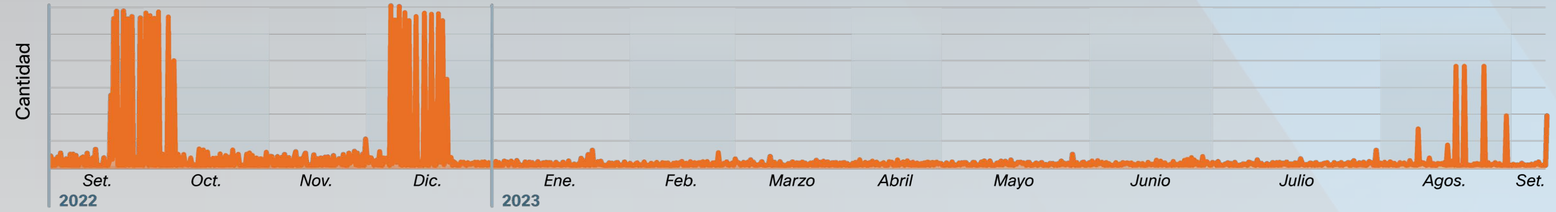
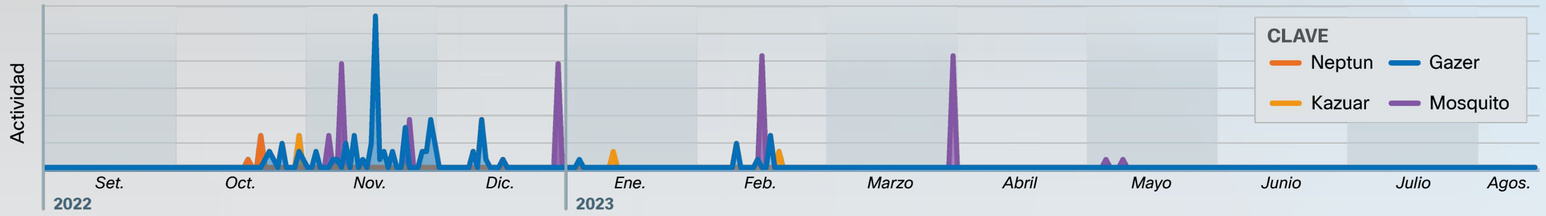


FIGURA 13

Actividad en las variantes del malware de Turla: Gazer, Kazuar, Mosquito y Neptun este año



"Más allá de destacar los sectores que Gamaredon y Turla dirigieron este año, los datos son también muy representativos del volumen de ataques que Snort ayudó a prevenir".

La más grande propagación de víctimas de Gamaredon se ubicó en Norteamérica, seguidas por Europa y Medio Oriente, con una cantidad desproporcionada de víctimas en Europa Occidental. Es probable que más de la mitad de la actividad dirigida de Gamaredon que afectó a los sectores de la industria del transporte y servicios públicos, compatible con las entidades de infraestructura crítica del objetivo de Rusia, cause la mayor interrupción a las entidades estratégicas para bloquear los efectos de guerra de Ucrania.

En septiembre y diciembre de 2022 y septiembre de 2023, vimos tres picos claros en la actividad de Gamaredon **(Figura 12)**, potencialmente representando clústeres de operaciones dirigidas específicas. El aumento de la actividad de Gamaredon como se ve en la Figura 12 en agosto de 2023 es compatible con los niveles de actividad del grupo según un reporte del Centro de Coordinación Nacional para la Ciberseguridad (NCCC) de Ucrania.

A diferencia del alcance de los sectores verticales que Gamaredon dirigió este año, Turla dirigió menos víctimas en una cantidad menor de sectores y geografías, compatible con las operaciones precisas del grupo. Se afectó a los sectores de fabricación y servicios financieros de igual manera, con educación y agricultura dirigidos a un grado menor **(Figura 11)**. Más allá de destacar los sectores que Gamaredon y Turla dirigieron este año, los datos son también muy representativos del volumen de ataques que Snort ayudó a prevenir.

El malware implementado por y personalizado para Turla, incluidos varios implantes y puertas traseras usados para accesos constantes, se ve concentrado en una serie de eventos que ocurrieron en su mayoría entre septiembre de 2022 y febrero de 2023. Mientras que la razón por mayor actividad durante este período se desconoce, creemos que es probable que haya provenido de un ritmo operativo incrementado en respuesta a la invasión rusa en Ucrania. Estas cuatro familias de malware, Gazer, Kazuar, Mosquito y Neptun, mientras que no son una lista exhaustiva del malware de Turla, son parte del gran arsenal de malware personalizado y malware de código abierto modificado de Turla, que se actualizan constantemente o se reemplazan por versiones más avanzadas.

A través del tiempo, este clúster, como se ve en la Figura 13, del malware personalizado de Turla continúa transmitiendo la narrativa del ritmo operativo de Turla, probablemente en gran medida en función de la selectividad de los objetivos. Notablemente, la representación de la actividad del malware de Turla en la Figura 13 (mientras que no es una lista exhaustiva) disminuye significativamente cerca de mayo de 2023, y coincide con la interrupción por parte del Departamento de Justicia de EE. UU. del malware Snake de Turla. Durante casi 20 años, Turla implementó Snake para robar y exfiltrar datos de sistemas dirigidos a través de numerosos nodos retransmisores desparramados en todo el mundo. Mientras que se aún se desconocen los efectos de las interrupción de Snake en las operaciones actuales y futuras de Turla, la actividad de malware disminuida puede representar cambios en el kit de herramientas de Turla como resultado de la interrupción.

FIGURA 14

Principales amenazas en investigaciones del grupo de trabajo de Ucrania

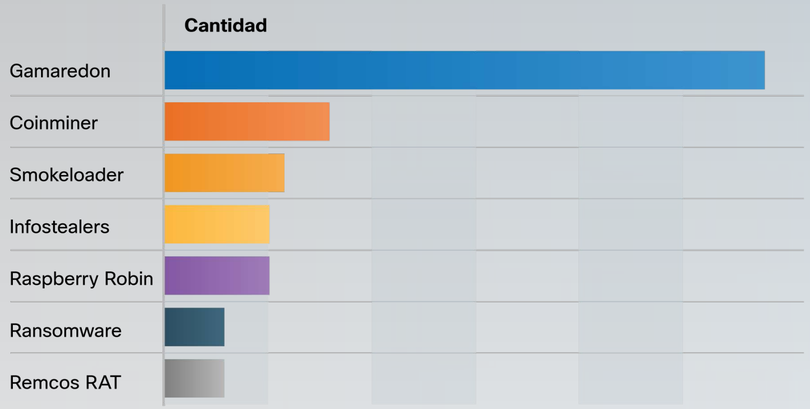
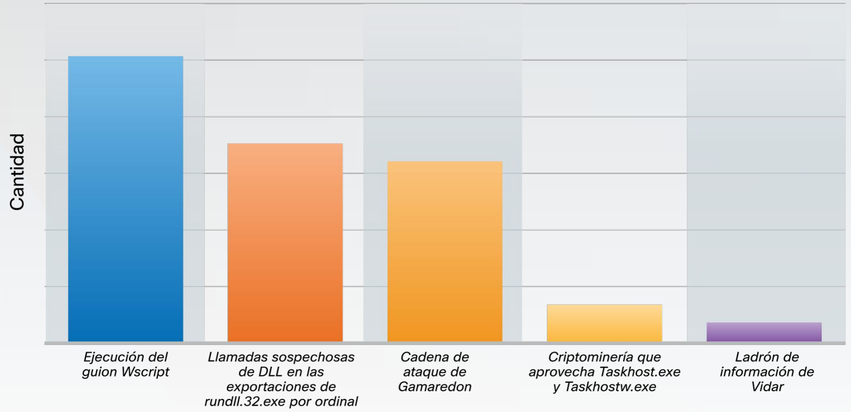


FIGURA 15

Principales cinco actividades maliciosas que afectan a los partners de Ucrania



La unidad interna de tareas continúa monitoreando amenazas a Ucrania

El soporte continuo de Talos para Ucrania continúa siendo un gran enfoque de nuestros esfuerzos operativos este año. Como parte del trabajo de la unidad de tareas, monitoreamos la actividad sospechosa en la telemetría del terminal para casi tres docenas de partners ucranianos en los sectores de infraestructura críticos, incluidos el gobierno, los servicios públicos, los servicios financieros, los servicios de salud y el transporte, entre otros.

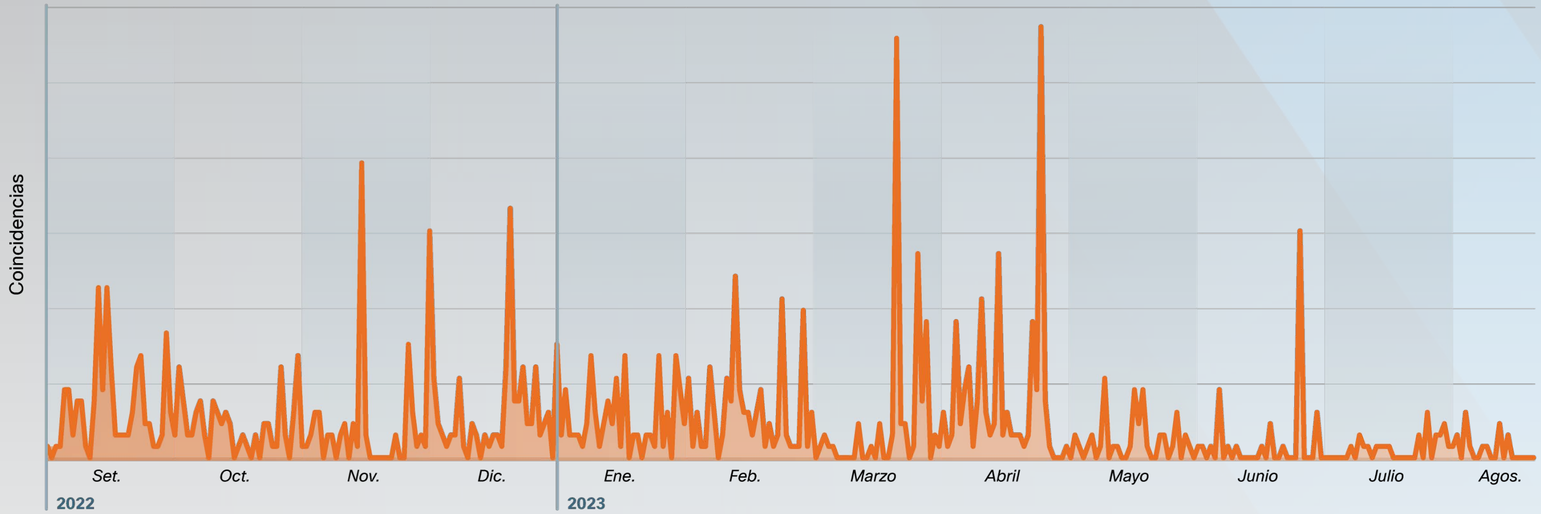
Mientras que las amenazas contra estas organizaciones pueden no estar designadas como actividad de la APT, el volumen de amenazas y el clima geopolítico volátil en los que se implementan representa un riesgo significativo para los defensores de las redes que protegen a los activos fundamentales.

Gamaredon es la principal amenaza dominante para Ucrania a la que nuestro grupo de trabajo ha respondido **(Figura 14)**. Históricamente, el grupo ha dirigido predominantemente entidades ucranianas, en particular esas responsables de la defensa, diplomacia y seguridad interna del país.

Gamaredon, y partes de su cadena de ataque, aparecen de manera uniforme entre las principales alertas de detección de amenazas de Cisco Secure Endpoint que notificaron nuestros partners ucranianos (Figura 15). Por ejemplo, estos cinco principales comportamientos demuestran el uso uniforme de LoLBins y de las técnicas asociadas a ellos, como la ejecución de Wscript, un procesador de Windows legítimo que es probable que se use para enmascarar la implementación de malware bajo la apariencia de actividad esperada, que continúa siendo aprovechada para soportar una variedad de amenazas en el ciclo de vida del ataque. La actividad generalmente asociada a cibercriminales motivados por las finanzas, como la implementación de la extracción de criptomonedas y los ladrones de información, también continúan afectando a organizaciones ucranianas en numerosas industrias, en referencia al amplio rango de amenazas Ucrania afronta.

FIGURA 16

La actividad de malware de SmokeLoader durante el año



"Los recursos de ciberdefensa significativos a los que nos dedicamos para proteger a nuestros partners ucranianos también han tenido sin duda un impacto significativo en este espacio de amenazas, que frustra interrupciones significativas al mitigar ataques en las etapas principales".

Además de destacar el ritmo uniforme de las actividades de Gamaredon como se ve muestra anteriormente, Figuras 14 y 15 también ayuda a demostrar la cantidad de amenazas a las que la Unidad de tareas ha respondido. Esto incluye actividades desde amenazas de malware como cargadores, ladrones de información, ransomware, minería de criptomonedas y Raspberry Robin, una familia de malware prolífica tratada en el reporte anual del año pasado, que sigue siendo una amenaza consistente para los entornos empresariales. Por ejemplo, SmokeLoader es un descargador aprovechado por diversos grupos a los que la Unidad de tareas ha respondido reiteradamente este año **(Figura 14)**. Generalmente entregado por correo electrónico, SmokeLoader suelta malware en máquinas infectadas y desde comienzos de mayo, el Equipo de Respuestas a Emergencias Informáticas de Ucrania (CERT-UA) lo ha reportado y resalta aún más su uso persistente en el panorama de amenazas.

Observamos un pico en la actividad de SmokeLoader a finales de abril y comienzos de mayo, que se alinea con el reporte del Equipo de Respuestas a Emergencias Informáticas de Ucrania (CERT-UA) de distribución masiva de SmokeLoader dirigido a entidades ucranianas (Figura 16).

Mientras que la Unidad de tareas ha respondido continuamente a innumerables ciberamenazas desde principios de la guerra entre Rusia y Ucrania, la actividad observada en 2023 fue mucho menos sofisticada que lo que generalmente se asocia a estos adversarios sofisticados que esperaríamos ver en este espacio. Esta actividad fue dinámica este año pero no refleja el alcance completo de las ciberfuncionalidades destructivas que Rusia ha demostrado previamente contra Ucrania y sus aliados de la OTAN. Los expertos y partners de la industria han debatido las razones detrás de esto, y es probable que sea el resultado de esfuerzos combinados de la industria de la ciberseguridad, el gobierno de EE. UU., los partners extranjeros y el propio compromiso de Ucrania para proteger a su gente. Los recursos de ciberdefensa significativos a los que nos dedicamos para proteger a nuestros partners ucranianos también han tenido sin duda un impacto significativo en este espacio de amenazas, que frustra interrupciones significativas al mitigar ataques en las etapas principales.

Encendido del sistema del proyecto: Mantener las luces encendidas en Ucrania

Al provechar las relaciones únicas de Talos con la industria, el gobierno y Ucrania, encabezamos un esfuerzo para ayudar a estabilizar la matriz eléctrica de Ucrania contra los efectos del GPS atascados en el campo de batalla.

Enfrentados con el complejo problema de cómo hacer para que las subestaciones de Ucrania sean resistentes a fallas operativas causadas por señales caídas de GPS, los ingenieros de hardware y software de Cisco modificaron uno de nuestros switches de red, el switch Ethernet industrial de Cisco, para brindar mantenimiento para el equipo de la matriz eléctrica de Ucrania durante estas interrupciones de suministro.

Después de meses de desarrollo y coordinación con varios partners, se entregaron los dispositivos a Ucrania y se instalaron en subestaciones en todo el país, una verdadera hazaña durante una zona de guerra activa. Esta historia se presentará en el Reporte anual de propósito de Cisco en el curso de este año. Este ejemplo también demuestra cómo los esfuerzos de Cisco han ayudado a proteger la infraestructura crítica de Ucrania de ciberataques severos rusos en 2023.

¿Cómo se ve afectada la matriz eléctrica de Ucrania cuando el GPS baja?

Muchas de las subestaciones eléctricas de alto voltaje de Ucrania, que desempeñan un papel fundamental en la transmisión de electricidad doméstica del país, hacen un amplio uso de la disponibilidad de la información sobre la temporización del GPS precisa para ayudar a los operaciones a anticipar, reaccionar y diagnosticar una matriz eléctrica compleja y de alto voltaje. Cuando las señales del GPS se interrumpen de manera generalizada, las subestaciones no pueden sincronizar su reporte del tiempo precisamente porque no pueden asignar marcas de hora precisas. Sin buenos datos sincronizados, los esfuerzos para administrar cargas entre diferentes partes del sistema se pueden ver afectados, y esta administración evita interrupciones de suministro y de las fallas, especialmente durante demandas máximas y momentos de sobretensiones. Esta interrupción se puede generalizar y causar que áreas amplias pierdan el servicio de GPS durante largos períodos de tiempo.

FIGURA 17

Matriz de los actores de amenazas de YoroTrooper

Alias	Desconocido
Afiliaciones	Kazajistán
Activo desde	2022
Objetivos	Espionaje, robo de datos para apoyar los objetivos estatales.
Victimología	Las entidades gubernamentales europeas con un especial enfoque en los países de la Comunidad de Estados Independientes (CEI).
TTP destacados	Malware de productos básicos y creados a medida, ingeniería social, suplantación de identidad (phising) dirigida y extracción de datos.
Malware y herramientas	YoroTrooper emplea una variedad de familias de malware de productos básicos y autodesarrollados como AveMaria/Warzone RAT, LodaRAT.

Algunos miembros de YoroTrooper provienen de Kazajistán a favor de Rusia

A principios de este año, Cisco Talos divulgó información sobre un nuevo actor de amenaza que denominamos "YoroTrooper", al que evaluamos con gran confianza se compone, al menos en parte, de personas de Kazajistán. YoroTrooper es un actor de amenaza muy motivado cuya baja sofisticación se complementa con la identificación agresiva de entidades mediante una gran cantidad de familias de malware de productos básicos. Desde 2022, el grupo ha dirigido operaciones que tienen como objetivo el robo de datos y espionaje contra las víctimas en el gobierno o sectores de energía en Azerbaiyán, Tayikistán, Kirguistán y otros miembros de la Comunidad de Estados Independientes (CEI).

Actividad de la APT de aliados rusos

Los esfuerzos de investigación y monitoreo de Talos de las amenazas regionales se han expandido a la actividad de la APT atribuida a países que anteriormente fueron parte de la Unión Soviética, cuyos objetivos de inteligencia, TTP y victimología con frecuencia se alinean con el Kremlin. Dada la unión establecida desde hace tiempo entre estos gobiernos, la colaboración es admisible. Sin embargo, no tenemos evidencia directa de la participación del gobierno ruso.

Evaluamos que YoroTrooper también dirige organizaciones de valor estratégico en gobiernos europeos y turcos **(Figura 17)**. Por ejemplo, YoroTrooper ha puesto en riesgo cuentas para al menos dos organizaciones internacionales, incluidas una agencia fundamental de servicios de salud de la Unión Europea (UE) y la Organización Mundial de la Propiedad Intelectual (OMPI). Vulneraciones exitosas también incluyen embajadas de países europeos incluidos Azerbaiyán y Turkmenistán.

Este año, Talos ha estado monitoreando las actividades operativas de GhostWriter, que es un grupo supuestamente asociado con el gobierno bielorruso, según CERT-UA. Hemos observado varias campañas de GhostWriter contra entidades gubernamentales, organizaciones militares y usuarios civiles en Ucrania y Polonia. Creemos que es probable que estas operaciones, que con frecuencia promocionan narrativas anti-OTAN que pretenden socavar la cooperación en seguridad regional, tengan como objetivo robar información y obtener acceso remoto constante. Actividades recientes, también seguidas por CERT-UA, demuestran el ataque del grupo de la vulnerabilidad que analiza a WinRAR ZIP, CVE-2023-38831. La vulnerabilidad les permite a los atacantes ocultar el código malicioso en archivos ZIP que se enmascaran como formatos de archivos populares que incluyen archivos TXT o JPG, que GhostWriter aprovechó para implementar Cobalt Strike y el descargador de malware, PicassoLoader.

No podemos descartar las contribuciones rusas a YoroTrooper o GhostWriter en este momento. Estas operaciones y partners dirigidos, que con frecuencia se alinean fuertemente con intereses estratégicos rusos, son fundamentales para entender las amenazas regionales contra el contexto de la invasión rusa a Ucrania.

CISCO TALOS

REVISIÓN DEL AÑO

2023

Amenazas persistentes avanzadas: Oriente Medio

Puntos destacados de la sección

- Los eventos a principios de octubre de 2023 entre Hamás e Israel contribuyeron a que varios grupos hacktivistas motivados políticamente lanzaran ataques no coordinados y en su mayoría no sofisticados contra ambos lados, similar a lo que observamos a principios de la guerra entre Rusia y Ucrania.
- El complicado entorno de Oriente Medio continúa siendo dinámico este año y probablemente veamos el impacto del ciberdominio avanzando. Como los adversarios regionales de toda la vida intentan normalizar los lazos, y los conflictos de décadas provocan nueva violencia, los ciberjugadores principales con intereses económicos y políticos en Medio Oriente, como China e Irán, puede que estén más motivados para influenciar los resultados a través de operaciones de proxy y directas.
- Los grupos de APT con sede en Medio Oriente dirigieron firmas de telecomunicaciones en la región, y así siguieron la tendencia que hemos visto de adversarios sofisticados dirigidos a este sector. Como parte de esta actividad, identificamos un nuevo conjunto de intrusión, ShroudedSnooper, que implementa implantes nuevos que denominamos HTTSnoop y PipeSnoop contra entidades relacionadas.
- El grupo APT MuddyWater patrocinado por el estado de Irán dependió menos que en años anteriores de la herramienta generalmente usada Syncro, esencial para el acceso remoto y la implementación de malware, probablemente en respuesta a acciones de la industria de la ciberseguridad contra conocidos TTP de MuddyWater.

Amenazas persistentes avanzadas: Oriente Medio

Grupos regionales patrocinados por el estado continúan dirigiendo ciberataques generalizados contra entidades en Norteamérica, Europa, Medio Oriente y Asia. Las empresas de telecomunicaciones resistieron la mayoría de estos ataques, una tendencia que ha trascendido varias APT, como se mencionó en otras partes de este reporte. Nuestro trabajo en este espacio dio como resultado el descubrimiento de un nuevo actor al que denominamos ShroudedSnooper que parece tener la intención de dirigir las principales entidades de telecomunicaciones en la región. El actor de APT MuddyWater patrocinado por el estado de Irán sigue siendo un jugador fundamental en espacio de amenazas y fue el foco de gran parte de nuestros esfuerzos de investigación este año. Mientras que el grupo continúa usando muchas de las mismas técnicas para promover sus objetivos principales de robo de propiedad intelectual e inteligencia colectiva, las acciones de la industria probablemente haya influenciado la capacidad del grupo de usar ciertas herramientas, incluida la plataforma del monitoreo y la administración remotos (RMM) de Syncro que el grupo usaba a fines de 2022.

Podría decirse que Medio Oriente es la región geopolítica más complicada en el mundo, y el conflicto que se llevó a cabo entre Hamás e Israel en octubre de 2023 nos recuerda que los eventos con consecuencias globales pueden iniciarse rápido y sin previo aviso. El panorama geopolítico en constante cambio aquí sin duda afectará la ciberactividad que avanza, a medida que los jugadores regionales establecidos como Irán siguen con la intención de cumplir ciertos objetivos geopolíticos y los nuevos actores como China buscan expandir su influencia.

El conflicto entre Hamás e Israel promueve la influencia de grupos hacktivistas

El ataque sorpresa de Hamás en Israel en octubre no solo tuvo implicaciones globales sino que ha afectado el ciberdominio, inmediatamente atrayendo actores de ambos lados del conflicto. Los hacktivistas con motivos públicos, incluidos los actores conocidos como Killnet y Anonymous Sudan así como también los grupos menos conocidos, lanzaron ataques no coordinados y en su mayoría no sofisticados desde el principio, mientras el espacio de amenazas se llenó rápidamente con muchos actores diferentes. Varios grupos hacktivistas anunciaron rápidamente soporte para ambos lados del conflicto entre Israel y Hamás, publicaron mensajes políticos amenazantes, llamaron a seguidores a unirse y se responsabilizaron por ataques de DDoS contra objetivos de interés, TTP hacktivistas típicos. Esto es ampliamente compatible con lo que observamos al principio de la guerra entre Rusia y Ucrania, cuando una afluencia de ciberactividad se concentró en estos países de la noche a la mañana.

Eventos geopolíticos significativos como este también invitan a la participación de adversarios mucho más sofisticados, incluidos esos que los gobiernos estatales extranjeros soportan y financian. Hemos visto esto muy recientemente en Ucrania, donde los actores avanzados patrocinados por el estado de Rusia como Gamaredon y Turla han sido implacables en su objetivo de entidades ucranianas desde el comienzo de la guerra. De mismo modo, esperamos ver un aumento de la ciberactividad iraní en Medio Oriente después del ataque de Hamás en Israel. Irán e Israel son adversarios de larga data, y su conflicto de décadas tiene una influencia importante sobre las ciberoperaciones de Irán. Irán es también un promotor fundamental de militantes antiisraelíes y grupos terroristas, incluidos Hamás, Hezbollah y el Yihad Islámica Palestina, que estaban todos involucrados en el más reciente aluvión de violencia contra Israel. El soporte de Irán para estos grupos y la hostilidad histórica de Teherán con Israel sugiere con énfasis que Irán puede usar sus ciberfuncionalidades para influenciar el resultado de la crisis, muy parecido a como otras naciones dependen de la cibernética como una herramienta esencial para promover sus objetivos de política extranjera.

"El actor de APT MuddyWater patrocinado por el estado de Irán sigue siendo un jugador fundamental en espacio de amenazas y fue el foco de gran parte de nuestros esfuerzos de investigación este año. Mientras que el grupo continúa usando muchas de las mismas técnicas para promover sus objetivos principales de robo de propiedad intelectual e inteligencia colectiva, las acciones de la industria probablemente haya influenciado la capacidad del grupo de usar ciertas herramientas".

Las ambiciones chinas en la región indican posibles ciberoperaciones

Mientras que China tradicionalmente ha tenido un rol económico destacado en Oriente Medio como uno de los inversores extranjeros más grandes, el liderazgo de la RPC también buscó expandir su presencia política en la región el año pasado al participar en la mediación del conflicto regional. En marzo, Pekín logró un acuerdo entre adversarios de larga data Irán y Arabia Saudita para restablecer lazos diplomáticos, y en septiembre, China y Siria anunciaron una colaboración estratégica, a medida que el presidente sirio Bashar Assad comienza a volver a ingresar en el orden internacional después de más de una década de una guerra civil brutal. El acuerdo entre China y Siria también puede brindar excelentes incentivos económicos para Pekín, que podría convertirse en un importante promotor financiero de los esfuerzos de reconstrucción de Siria. Estas jugadas estratégicas de China llegaron en un momento en el que EE. UU. se ha retirado de gran parte de la región después del período del 11 de septiembre, y es probable que Pekín vea esto como una oportunidad para aprovechar la participación de EE. UU. en disminución y ejercer influencia ahí.

Debido a que la presencia política en aumento de China en Medio Oriente, esperamos ver más actividad de APT china en esta región. Hemos observado a las APT chinas, entre las más activas y persistentes amenazas patrocinadas por el estado, complementar a las empresas financieras con operaciones de espionaje en regiones en las que se invierte, y se dirigen a las organizaciones del sector privado y gobiernos cuya propiedad intelectual es compatible con objetivos económicos. Es probable que las operaciones futuras estén en consonancia con los TTP de APT chinas bien establecidas, como dirigir entidades y operaciones que operan en industrias esenciales para los planes estratégicos de China, establecer un acceso furtivo y a largo plazo a redes objetivo y robar tecnología y propiedad intelectual.

FIGURA 18

URL HTTPSnoop enmascaradas como Sistema LBS de OfficeCore

```
'http://+:80/1bsadmin/valve/',0
'http://+:80/1bsadmin/salon/',0
'http://+:80/1bsadmin/disorder/',0
'http://+:80/1bsadmin/cute/',0
'http://+:80/1bs/alpha/',0
'http://+:80/lbs/special/',0
'http://+:80/1bs/blue/',0
'http://+:80/1bs/mystery/',0
'http://+:80/1bswap/army/',0
'http://+:80/1bswap/problem/',0
'http://+:80/1bswap/goose/',0
'http://+:80/1bswap/useful/',0
```

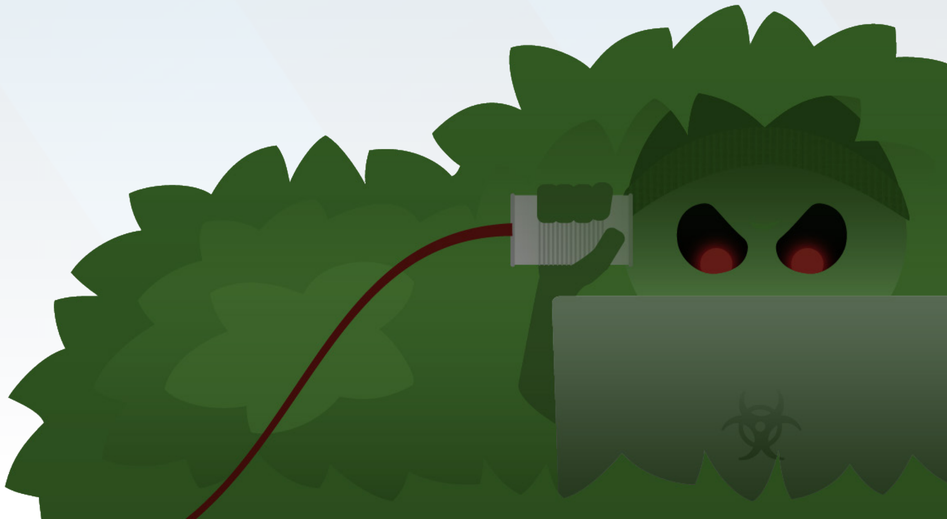
Debido a que la presencia política en aumento de China en Medio Oriente, esperamos ver más actividad de APT china en esta región.

El sector de las telecomunicaciones sigue siendo un objetivo fundamental para los actores de amenazas regionales

En 2023, descubrimos un nuevo conjunto de intrusiones, ShroudedSnooper, que implementa implantes de puerta trasera nuevos, HTTPSnoop y PipeSnoop, contra los proveedores de telecomunicaciones en Medio Oriente, a continuación de una tendencia que hemos estado monitoreando en la cual actores sofisticados con frecuencia se dirigen a este sector. En la actualidad, no hay suficiente evidencia para asociar la actividad de ShroudedSnooper a un país específico. Sin embargo, el enmascaramiento uniforme de las aplicaciones de software del grupo usadas por las firmas de telecomunicaciones en la región y el impacto sobre varios proveedores regionales es probablemente muy compatible con los actores patrocinados por el estado y adversarios sofisticados en todo el mundo.

Los implantes HTTPSnoop y PipeSnoop consisten en técnicas nuevas para escuchar las solicitudes entrantes para URL HTTP específicas y se ejecutan en un terminal infectado. Algunos de los implantes HTTPSnoop usan URL que se enmascaran como aquellas que pertenecen a OfficeTrack, que se comercializa especialmente a firmas de telecomunicaciones. OfficeTrack es una aplicación promocionada como una solución de administración de la fuerza laboral desarrollada por OfficeCore, una empresa de software que ayuda a los usuarios a gestionar las tareas administrativas. En varias ocasiones, vimos URL que terminaban en "lbs" Y "LbsAdmin", referencias al antiguo nombre de la aplicación (Sistema LBS de OfficeCore) antes de que se renovara a OfficeTrack **(Figura 18)**.

Durante todo nuestro análisis de los implantes ShroudedSnooper, el adversario usó varias URL que consisten en servicios de aprovisionamiento que imitan a los patrones de empresas de telecomunicaciones, incluido un proveedor de telecomunicaciones israelí, que es probable que se combine con un tráfico de red típico. Las variantes basadas en DLL de HTTPSnoop generalmente dependen del secuestro de DLL en servicios y aplicaciones benignas para que se activen en el sistema infectado, que se destacó como una técnica principal este año en secciones anteriores en este reporte.



Las acciones de la industria probablemente hayan afectado a operaciones de MuddyWater

A finales de 2022, se informó por primera vez que el grupo APT iraní MuddyWater estaba usando la herramienta de administración remota Syncro para tomar el control de dispositivos objetivo. Esta actividad es compatible con los datos de Talos IR desde el cuarto trimestre de 2022 (de octubre a diciembre de 2022), donde una cantidad creciente de adversarios dependían en gran medida de Syncro, observado en casi el 30 por ciento de las participaciones.

En diciembre de 2022, Syncro lanzó una declaración para tratar los asuntos sobre la implementación de Syncro por parte de MuddyWater en campañas de suplantación de identidad (phishing) focalizada dirigidas a organizaciones en Oriente Medio y Asia. La empresa implementó medidas de verificación adicionales para la creación de nuevas cuentas de prueba para limitar el uso de Syncro por parte de actores ilegítimos, y monitoreó el uso y la información irregular de las cuentas, y cerró las cuentas que violan estas nuevas políticas.

Esta acción de cambio de Cisco seguramente haya afectado a las operaciones de MuddyWater, que destacan el efecto directo que la industria puede tener en los componentes de impedimento de las operaciones de los adversarios avanzados. Mientras que se desconoce la razón por la que el uso de Syncro aumentó en el cuarto trimestre de 2022, su uso como una plataforma de acceso remoto con funcionalidades completas para los proveedores de servicio administrado (MPS) y su ubicuidad en los entornos empresariales probablemente lo hizo una opción atractiva.

"Esta acción de cambio de Cisco seguramente haya afectado a las operaciones de MuddyWater, que destacan el efecto directo que la industria puede tener en los componentes de impedimento de las operaciones de los adversarios avanzados".

Aprovechar Syncro para mantener el acceso

En un incidente que afectó a una empresa de telecomunicaciones, Talos IR identificó cuentas de correo electrónico de empresas que enviaban correctos electrónicos de suplantación de identidad (phishing) con asuntos que se traducían del árabe como "Promoción del personal". Los correos electrónicos contenían enlaces de suplantación de identidad (phishing) de OneDrive y OneHub con un archivo de Microsoft Windows Installer (MSI) que instaló Syncro. El adversario usó Syncro para seguir conectado a la estación de trabajo del usuario objetivo. Durante el análisis del archivo de MSI, varios servicios de Syncro también se instalaron, incluidos SyncroRecovery (SyncroLive) y SyncroOvermind. Las tácticas del adversario parecieron enfocarse en mantener el acceso de inicio a través de la instalación de Syncro. La falta de autenticación multifactor (MFA) para el acceso al correo electrónico permitió que el adversario realizara ataques de suplantación de identidad (phishing) y destacar la necesidad de asegurar MFA en todos los activos críticos.

CISCO TALOS

REVISIÓN DEL AÑO

2023

Cargadores de productos básicos

Puntos destacados de la sección

- Los cargadores de productos básicos como Qakbot, Ursnif, Emotet, Trickbot y IcedID representan algunas de las amenazas más generalizadas e impactantes, ya que los actores dependen de ellos de manera rutinaria para permitir partes fundamentales de sus operaciones. Su uso como descargadores para ladrones de información, ransomware y otros malware los han convertido en los pilares en el entorno de amenazas, que indiscriminadamente afectaron entidades a nivel global.
- Todos estos cargadores se desempeñaban anteriormente solo como troyanos bancarios, y los desarrolladores han diversificados sus funcionalidades en los últimos años para respaldar operaciones más avanzadas. En 2023, nuevas versiones de IcedID, Ursnif y Qakbot parecieron estar personalizadas específicamente para los actores de ransomware, según sus funciones de reconocimiento mejoradas, la eliminación de funciones que pueden activar las detecciones de virus y la rápida adopción por grupos de ransomware y agentes de acceso de inicio.
- La deshabilitación de macros de Microsoft por defecto provocó que los actores de cargadores de productos básicos inventaran nuevas formas de usar macros no detectados o evitar usarlos por completo. Los operadores de Qakbot usaron una amplia variedad de tipos de archivos, lenguajes de scripting, empaquetadores y ataques para implementar el cargador. Emotet, IcedID, and Ursnif variaron sus técnicas, pero con menos frecuencia en comparación con Qakbot, y también tendieron a aún de TTP más antiguos.
- Puede ser desafiante erradicar la amenaza de los cargadores de productos básicos incluso luego de que el botnet se desmantele, ya que los desarrolladores son conocidos por continuar operando en nombre de grupos de malware diferentes o reconstruir sus botnets. Además, otros actores de amenazas podrían aprovechar la infraestructura anteriormente en riesgo para actividad maliciosa.

Los actores han dependido de manera uniforme de los cargadores de productos básicos durante años, y 2023 no fue la excepción. Muchas de estas amenazas están ampliamente disponibles para la compra en foros clandestinos, ponen una baja barrera de entrada para los actores no sofisticados y son muy modulares, lo que permite que los actores de amenazas lleven a cabo varias etapas de un ataque. Durante 2023, Qakbot, Ursnif, Emotet, Trickbot y IcedID se destacaron como las amenazas más impactantes en este espacio.

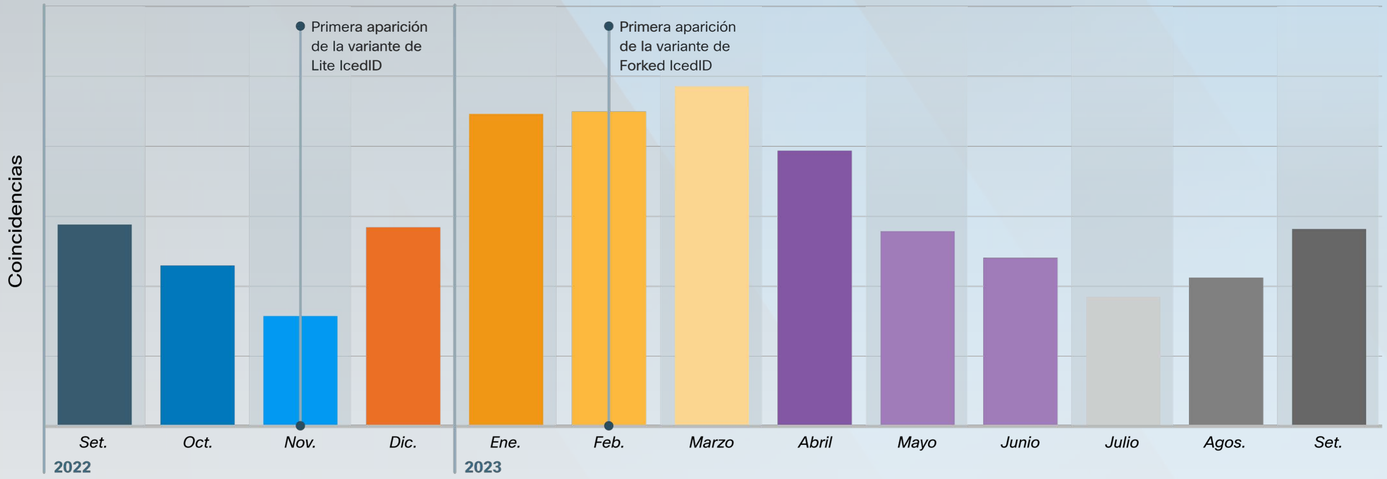
Las actualizaciones de los cargadores de productos básicos parecen personalizadas para soportar actividad de ransomware

A finales de 2023, observamos las últimas variantes de IcedID y Ursnif y una nueva característica de automatización en Qakbot, que soporta la implementación de ransomware, y sigue una tendencia de los cargadores de servicios públicos que juegan una parte integral en la cadena de infección del ransomware. Estas actualizaciones estaban adaptadas para mejorar las funcionalidades del instalador de malware, que probablemente signifique un alejamiento del uso previsto original como troyano bancario. También se conoce a Trickbot y Emotet por facilitar ataques de ransomware, sin embargo, no recibieron actualizaciones similares en 2023.

En noviembre de 2022 y febrero de 2023, los desarrolladores de IcedID lanzaron dos nuevas versiones que sacaron sus funcionalidades bancarias y diseñaron para funcionar como instaladores. En 2023, los agentes de acceso de inicio usaron estas versiones, denominadas "Forked" y "Lite". Se conoce a dicho agentes por vender accesos a redes a grupos de ransomware. Mientras que los agentes de acceso de inicio y los grupos de ransomware también usaron la versión original, es probable que las nuevas versiones sean una opción más atractiva porque se sacaron funciones que pueden activar firmas de AV, y así hace que sean furtivas. La actividad de IcedID aumentó entre noviembre de 2022 y febrero de 2023, que se corresponde con el lanzamiento de las nuevas versiones, y sugiere que los actores estaban muy interesados en probar las últimas funcionalidades de las amenazas **(Figura 19)**.

FIGURA 19

La actividad de IcedID aumentó cerca del lanzamiento de la nueva variante



La última variante de Ursnif, que se actualizó del mismo modo para excluir la funcionalidad de troyanos bancarios, también aparentemente pretendió soportar la implementación del ransomware. En 2023, el grupo de ransomware prolífico Royal adoptó esta versión actualizada (lanzada en 2022), la primer ocasión en la que un grupo de ransomware incorporó Ursnif en sus operaciones. Debido a que Royal es el único grupo que aprovechó esta nueva variante, puede haber una asociación profesional entre desarrolladores. Royal es un grupo de cibercriminales sofisticado activo por primera vez en septiembre de 2022, y sospechado por muchos profesionales de seguridad de ser una renovación del grupo de ransomware prolífico ruso Conti. Royal controla firmemente su malware y operaciones de malware, a diferencia de muchos otros grupos de ransomware que surgieron en los dos últimos años que eligieron operar como un RaaS. Por lo tanto, un partner exclusivo de la nueva variante de Ursnif y Royal el probablemente intencional y podría implicar una afiliación entre los desarrolladores.

Finalmente, a fines de 2022, Qakbot implementó varias funcionalidades de automatización, incluida una función idealmente indicada para ayudar a los grupos de ransomware a determinar objetivos valiosos antes de la implementación. Las actualizaciones incluyeron una lista de comandos de reconocimiento para planear el entorno del cliente al momento de infecciones de inicio. El resultado de estos comandos enumeró datos que serían muy útiles para los grupos de ransomware, incluidos grupos de dominio, el nombre del dominio y los nombres de los controladores de dominio. Esta información podría prestar colaboración con movimientos laterales que dan como resultado una adquisición de Active Directory, una táctica comúnmente usada por los grupos de ransomware. Las nuevas funcionalidades de reconocimiento de automatización de Qakbot también pueden haber ayudado a los grupos de ransomware a evadir la detección, ya que se podrían usar los datos recopilados para formular un plan de ataque detallado, que minimice el tiempo entre la infección inicial y la encriptación.

Cargadores de productos básicos

Los TTP evolucionados de los operadores de cargadores de productos básicos en respuesta a las actualizaciones de seguridad nuevas que bloquean macros, siguen una tendencia que comenzó a mediados de 2022.

En 2023, Microsoft bloqueó macros por defecto, un cambio notable que provocó que los actores modificaran su acceso de inicio y técnicas de entrega de malware. Previo al cambio, los macros se ejecutaban automáticamente cuando los documentos de Microsoft Office se abrían. Los actores de malware han abusado frecuentemente de macros para ejecutar malware automáticamente cuando una víctima hace clic en un adjunto malicioso en un correo electrónico de phishing. En la actualidad, el usuario recibe un aviso de seguridad si hace clic en un adjunto potencialmente malicioso, y así se reduce la probabilidad de descargar malware. La deshbilitación de los macros de Microsoft continuó teniendo un impacto durante 2023, ya que los actores de amenazas inventaron nuevas formas de usar macros no detectados o evitar usarlos por completo. Cuando Microsoft creó un nuevo parche para actualizar las funciones de seguridad, los actores de amenazas pudieron cambiar rápidamente sus TTP del juego del gato y el ratón **(Figura 20)**.

FIGURA 20

Los cargadores de productos básicos permiten que los actores de amenazas cambien rápidamente los TTP en respuesta a funcionalidades de seguridad cambiante

Las muestras de comandos de reconocimiento que observamos que las filiales de Qakbot implementaron en 2023

Los actores de amenazas dirigen reconocimiento para reunir información para operaciones adicionales. Observamos a las filiales de Qakbot abusar de servicios públicos de Windows comunes que permiten la ejecución de comandos en un intento de ocultarse entre actividad legítima. A continuación hay algunos ejemplos para demonstrar el potencial daño de estos comandos.

Netstat -nao: usado para obtener una lista de puertos abiertos que son particularmente vulnerables a ataques maliciosos y una lista de conexiones activas entre los servidores y otros sistemas, como los entornos de la nube, para determinar si la víctima puede acceder a datos que son de valor para el actor de amenaza.

Net localgroup: usado para identificar cuentas de administradores (es decir, cuentas con muchos privilegios que pueden acceder a datos sensibles y hacer cambios en el sistema): Esta información ayuda a los actores de amenazas saber qué cuentas priorizar en sus esfuerzos dirigidos.

Arp -a: usado para mostrar el caché de ARP, un registro de cada dirección IP y su correspondientes dirección MAC que realizó una conexión al servidor infectado. Con esta información, un atacante puede ubicarse así mismo entre la comunicación de dos o más dispositivos de red para robar datos adicionales o manipular datos transmitidos.

En una tendencia que comenzó en 2022 y continuó durante 2023, los adversarios que usaban cargadores de productos básicos cambiaron en reiteradas ocasiones sus TTP en respuesta a nuevas actualizaciones de seguridad de Microsoft. En noviembre de 2022, Microsoft emitió dos parches para detectar y bloquear contenido con macros habilitados con los archivos de los contenedores, como ZIP y LNK, que habían sido un particular método para subrepticiamente usar macros. Solo unas semanas después, observamos una sobrecarga de actores de amenazas, incluidos esos que usan Qakbot, Emotet y IcedID que usan archivos de adjuntos de OneNote para implementar malware. Si bien usar OneNote para entregar malware no era una técnica, facilitó la entrega de documentos con macros habilitados sin ser detectados, que es muy favorable entre las filiales que desean desviar la detección de AV **(Figura 21)**.

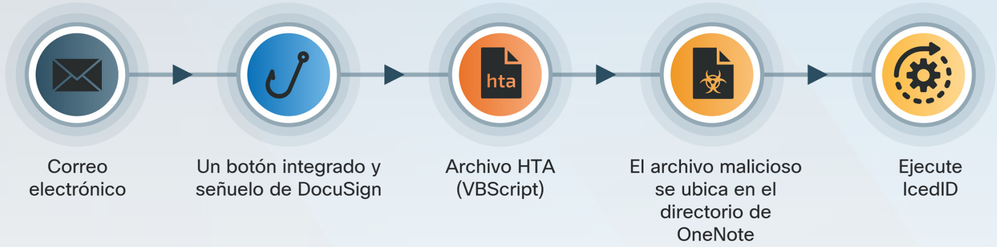
Luego en enero, Microsoft emitió una actualización silenciosamente, para que los documentos con macros habilitados integrados en los archivos de OneNote se bloquearan por defecto, lo que significa que el usuario recibiría un aviso de seguridad al abrir un adjunto de OneNote integrado con macros. Sin embargo vimos actores de amenazas usando OneNote, pero con técnicas de ingeniería social que manipulaban víctimas para que ignoren estos avisos. En una campaña observada que implementó IcedID, el actor de amenaza usó un señuelo de DocuSign para engañar a la víctima para que haga clic en un botón con un enlace integrado. El botón de "Desencriptar y ver mensaje" en efecto contenía un archivo de aplicación HTML (HTA) malicioso **(Figura 22)**. Al abrirlo, el archivo HTA se dejaba caer en el directorio de OneNote para la ejecución.

FIGURA 21

Muestra de cadena de infección que usa OneNote con un archivo de macros habilitados integrados para entregar malware

FIGURA 22

Muestra de cadena de infección que intenta manipular a las víctimas para que ignoren alertas de seguridad



Cargadores de productos básicos

FIGURA 23

Muestra de cadena de infección que no depende de macros

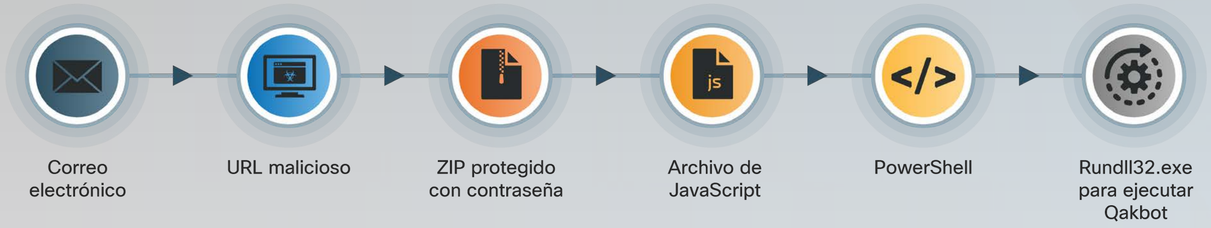


FIGURA 24

Cadena de infección de Emotet mediante relleno binario

Finalmente, en abril de 2023, Microsoft emitió otra actualización que bloqueó a los usuarios para que no abrieran archivos con una extensión potencialmente peligrosa integrada en OneNote. Para abrir un adjunto marcado como potencialmente peligroso, los usuarios de OneNote deberían guardar el archivo en su dispositivo y abrirlo desde ahí. Esto permitiría que las aplicaciones de seguridad se ejecutaran en el dispositivo para detectar cualquier código malicioso en el adjunto. Esta última actualización hizo que muchos operadores abandonaran OneNote como un método para esconder el uso de macros. En lugar de eso, observamos actores recurriendo a tipos de archivo que ejecutan malware sin depender de macros, como los archivos de JavaScript que dependen de LoLBins para la ejecución **(Figura 23)**.

Aparte de OneNote, los actores de amenazas también experimentaron con otros métodos de implementación de malware que no dependían de macros o que podrían usar macros sin ser detectados. Desde al menos diciembre de 2022, hemos observado actores de amenaza apropiarse de la plataforma de Google Ads para implementar malware como Ursnif, IcedID y Trickbot, un método que evita por completo usar macros. La cadena de ataques en estas campañas comienza con un usuario que ingresa un término de búsqueda para un software o servicio en el motor de búsqueda de Google. Una vez que se cargan los resultados de la página de Google, los anuncios maliciosos serán los primeros en aparecer en la lista de resultados, ya que se ha visto a los actores usar Search Engine Optimización (SEO) para aumentar la visibilidad. Si el usuario hace clic en el anuncio malicioso, se generará una URL de servicios de Google Ad, que luego genera una URL secundaria que guía al usuario al dominio malicioso y falso con enlaces de descarga que entregan las distintas amenazas. Talos observó los productos legítimos de software falsificados en estas campañas, como Microsoft Teams y WhatsApp, y administradores de contraseñas populares como 1Password. El uso de Google Ads y Google Search de actores de amenazas hace que su señuelo parezca muy legítimo, ya que es probable que los usuarios son menos propensos a cuestionar la autenticidad de anuncios pagos priorizados en la parte superior de sus resultados de búsqueda.

Mientras muchas filiales introdujeron nuevos TTP en 2023 en respuesta a las actualizaciones de seguridad en evolución, también observamos cargadores de productos básicos usar métodos antiguos. Por ejemplo, se observó a Emotet, IcedID y Ursnif usar documentos de Office con macros habilitados en la cadena de infección inicial. Además, observamos que se entregó Emotet en correos electrónicos de suplantación de identidad (phishing) con muestras "RedDawn" vistas por primera vez en 2020 **(Figura 24)**. Mientras que estos operadores pueden ser capaces de ataques más sofisticados, es posible que hayan alcanzado el éxito aun mediante TTP antiguos, en especial contra sistemas heredados de empresas sin parches.

Los cinco principales cargadores de productos básicos se implementan de manera similar contras sector globalmente en campañas oportunistas en masa

En 2023, observamos a todos los cinco cargadores de productos básicos que afectan a las empresas en todo el mundo, principalmente afectan a Norteamérica y Europa **(Figura 25)**. Estos objetivos geográficos no necesariamente reflejan una preferencia coordinada entre operados porque las amenazas se venden como malware como servicio (MaaS). Por lo tanto, los patrones objetivo se alinean con cualquier grupo que esté ejecutando la campaña y pueden variar.

Predominantemente observamos campañas masivas de correo electrónico no deseado que aprovechando la ocasión intentaron poner en riesgo a objetivos vulnerables, probablemente con la intención de moverse lateralmente hacia un objetivo más reforzado después de la infección inicial. Los adversarios generalmente adaptarán los señuelos de suplantación de identidad (phishing) a la geografía objetivo. Por ejemplo, en 2023, observamos a Ursnif predominantemente implementados contra empresas ubicadas en EE. UU. e Italia en campañas de correo electrónico no deseado masivas de tipo "disparar y rezar" al usar los idiomas de los países objetivo.

Hemos observado cargadores principalmente implementados contra empresas, a diferencia de datos financieros de personas objetivo, un cambio que ocurrió mientras el malware se usó con menos frecuencia que los troyanos bancarios. Esto se refleja en los señuelos de suplantación de identidad (phishing) que observamos. Por ejemplo, a fines de marzo, vimos un aumento en Emotet dirigido a empresas de EE. UU. que pagan impuestos trimestralmente. Los señuelos usaron temas relacionados con el Servicio de Impuestos Internos (IRS) con adjuntos como "Formularios de impuestos W-9 del IRS", que se vio el año pasado a fines del trimestre comercial de noviembre de 2022. Las empresas o instituciones financieras distribuyen formularios W-9 a sus empleados.

FIGURA 25

Mapa mundial de las regiones afectadas por los productos básicos, desde las más a las menos dirigidas

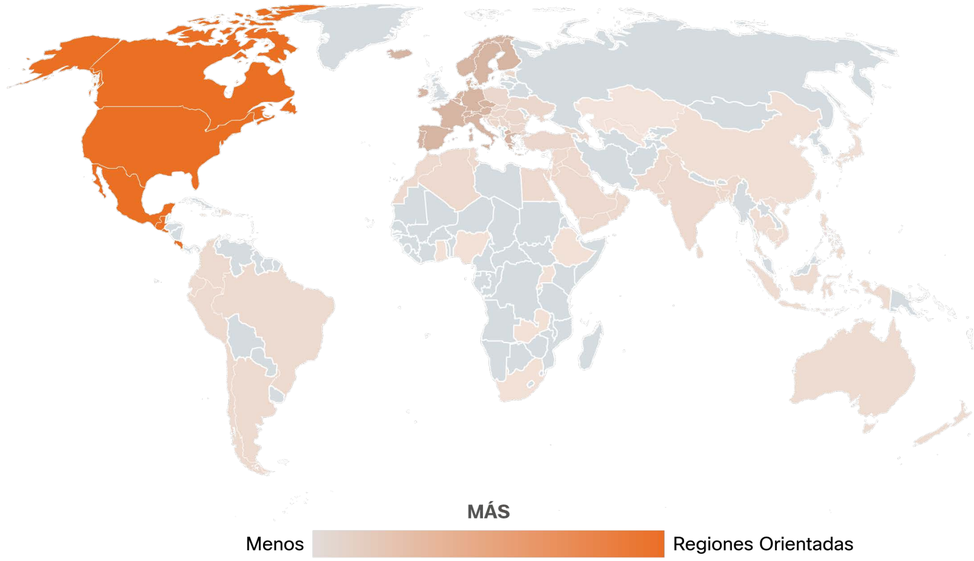
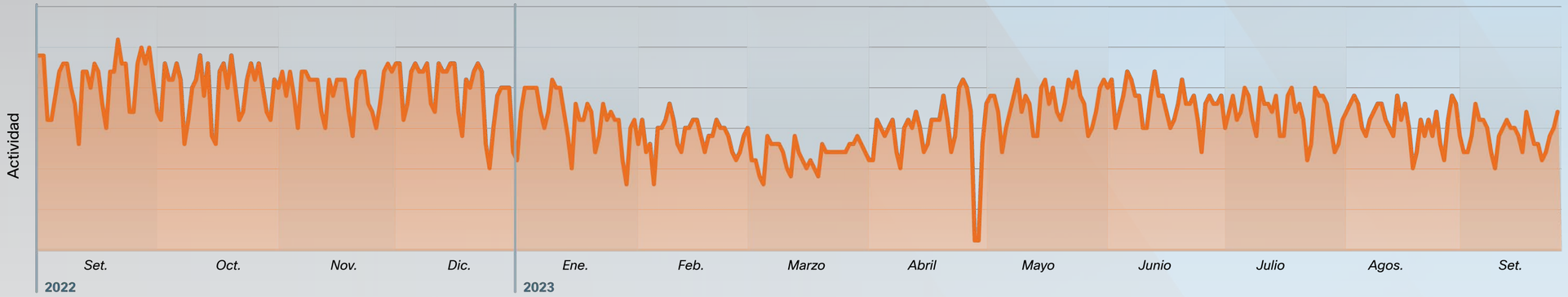


FIGURA 26

Actividad de Trickbot a través del tiempo



Las actividades de los cargadores de productos básicos pueden persistir mucho después de que sus botnets se desmantelen

En agosto de 2023, el cargador de productos básicos Qakbot se interrumpió en una gran operación de cumplimiento de la ley global, pero desmantelar la infraestructura de la botnet no siempre significa que los cibercriminales dejan de operar. Continuando, es posible que Qakbot pueda volver a emerger después de una interrupción de varios meses, ya que hemos visto escenarios similares que involucran a otros cargadores como Emotet, y además que ponga de relieve la necesidad de monitorear e informar sobre esta amenaza. Especialmente, no se detuvo a los actores de amenazas detrás de Qakbot durante la reducción global, y nuestros últimos hallazgos indican que aún están activos, aunque entregando diferentes amenazas, y. de este modo, quedó abierta la posibilidad de que puedan reconstruir la botnet Qakbot o renovarse así mismo bajo un nombre diferente.

Hemos visto otros desarrolladores de malware también continuar operando en el panorama de ciberamenazas después de que sus botnets se desmantelaran. Por ejemplo, después de que Trickbot desarmara su infraestructura en febrero de 2022, EE. UU. y el R. U. aún sancionaban a los desarrolladores en febrero y septiembre de 2023, lo que suponía que aún estaban activos en el panorama de las ciberamenazas. Los desarrolladores pueden haber elegido crear otros tipos de malware o trabajar con otros grupos con los que han tenido relaciones de larga data, como Emotet y Conti. En 2022, una serie de filtraciones revelaron relaciones profesionales cercanas entre desarrolladores de Trickbot y Conti y en 2021, Trickbot prestó partes de su infraestructura para ayudar a reconstruir la botnet Emotet.

Incluso si los actores de amenaza optan por dejar la actividad cibercriminal, aún podemos observar actividad zombi de dispositivos infectados de Qakbot. Hemos visto esto de Trickbot, donde nuestra telemetría adquirió actividad durante 2023 a pesar de que se desmantelara su infraestructura en febrero de 2022. Esto es probable debido a infecciones antiguas que aún se deben corregir o actores de amenazas que aprovechan infraestructuras previamente en riesgo. Al ver la actividad de Trickbot durante el año pasado, podemos ver que se ubicó cerca del mismo número medio, que soportaba nuestra evaluación que la botnet que aún está activa en alguna capacidad, pero los desarrolladores no están activamente involucrados en hacer crecer la botnet **(Figura 26)**.

Sería probable que se represente cualquier nueva campaña o infraestructura, como los servidores IP o C2, en los gráficos anteriores con un pico más drástico o patrones irregulares.

Mientras tanto siempre hay nuevos cargadores de productos básicos para reemplazar las botnets prolíficas anteriores como Qakbot y Trickbot. Por ejemplo, IcedID puede ser una elección lógica para llenar el vacío que Qakbot dejó. Hay una precedencia histórica, ya que IcedID atrajo filiales después de que se desmantelara Emotet en 2021. Además, es probable que muchas filiales de Qakbot ya estén familiarizadas con IcedID porque hay numerosas ocasiones de las dos que se implementan juntos como parte de la misma campaña. Finalmente, la actualización avanzada reciente de IcedID muestra que los desarrolladores son capaces de, y están motivados para, mantener un producto de alta calidad.