Superautopista de ataques

Profundizamos en el tráfico de DNS malicioso

Akamai

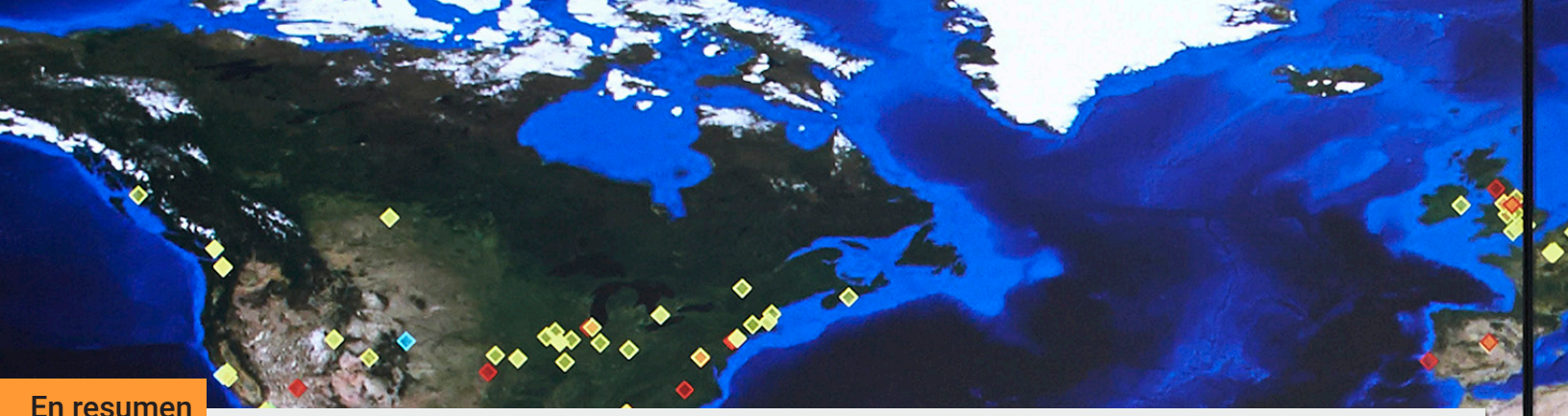
Tabla de contenido

Servidores de nombres de dominio: una vía libre para el tráfico de ataque

El sistema de nombres de dominio (DNS) ha sido una parte fundamental de la infraestructura de Internet desde sus orígenes. Gran parte de nuestro uso de Internet, ya sea en casa o en el trabajo, debe facilitarse a través del DNS para que podamos llegar correctamente a nuestro destino en la World Wide Web. Como era de esperar, los atacantes suelen aprovechar esta infraestructura para introducir sus ataques, ya sea una amenaza que accede a los servidores de mando y control (C2) a la espera de comandos o una ejecución remota de código que llega a un dominio para descargar archivos maliciosos en un equipo. Debido a su omnipresencia, el DNS se ha convertido en una parte importante de la infraestructura de ataques.

Como empresa de seguridad, Akamai ocupa una posición única que nos permite examinar y proteger tanto a empresas como a particulares contra el tráfico de DNS malicioso que podría poner en peligro el sistema y robar información. En este informe, proporcionaremos un análisis del tráfico malicioso dirigido a particulares y empresas de todo el mundo. Un análisis exhaustivo del tráfico de DNS malicioso, que incluye la correlación con grupos o herramientas de atacantes, podría proporcionar a las organizaciones información importante sobre las amenazas más frecuentes para su organización. Como tal, esta información podría ayudar a los profesionales de la seguridad a evaluar su estrategia de defensa e identificar las lagunas para hacer frente a las técnicas y metodologías utilizadas en su contra. De lo contrario, podrían producirse infracciones que provocarían pérdidas de datos confidenciales, pérdidas financieras o sanciones debido a infracciones de cumplimiento. Con el aumento anual del coste de la ciberdelincuencia, que se prevé que llegue hasta los 10,5 billones de USD al año para 2025, las organizaciones deben estar preparadas incluso antes de que se produzcan los ataques.

Al analizar el tráfico de DNS malicioso de particulares y empresas, pudimos detectar varios ataques y campañas en el proceso, como la propagación de FluBot, un malware basado en Android que se mueve de un país a otro por todo el mundo, así como la prevalencia de varios grupos ciberdelincuentes dirigidos a empresas. Tal vez el mejor ejemplo sea la presencia significativa de tráfico de C2 relacionado con los agentes de acceso inicial (IAB) que vulneran las redes corporativas y rentabilizan el acceso al venderlo a otros, como los grupos de ransomware como servicio (RaaS). Esas actividades son visibles para nosotros en la autopista de la información que es el DNS, y las estamos compartiendo por el bien de nuestros lectores.



En resumen

Según nuestros datos, entre el 10 % y el 16 % de las organizaciones han detectado tráfico de C2 en su red en un trimestre determinado. La presencia de tráfico de C2 indica la posibilidad de un ataque o una filtración en curso, y las amenazas van desde botnets de robo de información hasta IAB.

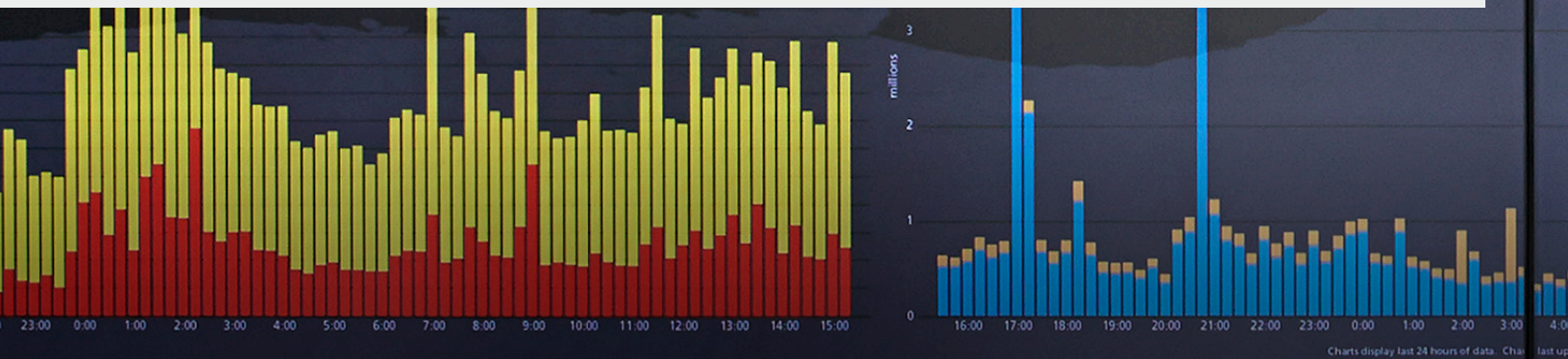
El 26 % de los dispositivos afectados ha llegado a dominios de C2 de IAB conocidos, como los relacionados con Emotet y Qakbot. Los IAB presentan un grave riesgo para las organizaciones, ya que su función principal es llevar a cabo la filtración inicial y vender el acceso a grupos de ransomware y otros grupos ciberdelincuentes.

Los dispositivos de almacenamiento conectado a la red (NAS) resultan perfectos para los atacantes, ya que es menos probable que se les apliquen parches y pueden contener muchísimos datos valiosos. Nuestros datos muestran que los atacantes se aprovechan de estos dispositivos a través de QSnatch y que el 36 % de los dispositivos afectados de las redes corporativas acceden a dominios de C2 relacionados con esta amenaza.

El 30 % de las organizaciones afectadas pertenecen al sector de la fabricación, el doble que el segundo sector más afectado, lo que pone de relieve las implicaciones reales de los ciberataques, como los problemas en la cadena de suministro y las interrupciones en la vida cotidiana. Normativas como la Directiva sobre Seguridad de las Redes y los Sistemas Informáticos 2 (SRI 2) podrían ayudar a frenar los ataques contra sectores esenciales o infraestructuras críticas como la fabricación.

Los ataques a las redes domésticas tratan de abusar no solo de los dispositivos tradicionales, como los ordenadores, sino también de los teléfonos móviles y el Internet de las cosas (IoT). Una cantidad significativa de tráfico de ataque puede estar correlacionada con el malware móvil y las botnets del IoT.

A través de nuestro análisis de datos de DNS, detectamos un ataque creciente de malware FluBot en Europa, Oriente Medio y África (EMEA), Latinoamérica (LATAM) y Asia-Pacífico y Japón (APJ). Las tácticas de ingeniería social del malware y su uso de múltiples idiomas de la Unión Europea (UE) podrían ser algunos de los factores que contribuyen al aumento de la infección.



Terminología del análisis del tráfico de DNS de Akamai

Akamai Edge DNS y la infraestructura de DNS monitorizan hasta 7 billones de solicitudes de DNS al día. Con el fin de proteger a los usuarios y empresas, Akamai bloquea las solicitudes que conducen a dominios que distribuyen malware o sitios que podrían robar información. El análisis de estas transacciones de DNS maliciosas también nos permite clasificar estos dominios en tres categorías (malware, sitios de phishing y C2) y realizar una investigación exhaustiva para determinar las mayores amenazas actuales para las empresas y los usuarios.

A partir de una exhaustiva muestra de datos del tráfico de DNS malicioso, podemos extraer conclusiones significativas sobre las amenazas más frecuentes. Nuestra protección cubre dos grupos demográficos: Un grupo demográfico es el de las empresas cuyas redes corporativas están protegidas por Akamai, y el otro grupo demográfico es el de los usuarios que acceden a Internet en sus redes personales y que están expuestos a amenazas como botnets que pretenden introducirse en sus dispositivos con fines nefastos, como la obtención de beneficios económicos a través de la criptominería.

En primer lugar, vamos a definir los términos *sitios de phishing*, *malware* y *C2* y explicaremos cómo los utilizamos en este informe.

 Los **sitios de phishing** son dominios vinculados a kits de phishing que imitan y clonan el aspecto de las empresas minoristas, los bancos, las empresas de alta tecnología y otros, con el fin de engañar a los usuarios para que divulguen información como credenciales e información de identificación personal (PII). Akamai monitoriza este tráfico a través de DNS para proteger tanto a los usuarios como a las empresas frente al robo de identidad y la pérdida de información.

 El **malware** es un dominio (o dominios) malicioso que sirve o contiene archivos maliciosos. Esta categoría también contiene sitios que alojan JavaScript malicioso y sitios web comprometidos que sirven anuncios no deseados o que redirigen a los usuarios a una página que contiene estos anuncios. Muchos ataques modernos requieren la descarga de un archivo malicioso a un dispositivo desde una fuente externa para su carga inicial o para descargar la siguiente fase de un ataque en curso. La monitorización y el bloqueo de este tráfico pueden ayudar a proteger a una organización de una infección inicial o un ataque en curso.

 **C2**, en el contexto de nuestro análisis de tráfico de DNS, es un dominio utilizado para comunicarse con los dispositivos infectados para enviar comandos y controlar el dispositivo. Tras el ataque inicial, los atacantes establecen comunicaciones de C2 entre el sistema infectado y un servidor que controlan para enviar otros comandos, como la descarga y propagación de otro malware, la exfiltración de datos, y el apagado y reinicio del sistema, entre otros, y comprometer ulteriormente la seguridad del sistema o la red. La detección del tráfico de C2 es crucial, ya que indica un ataque en curso que aún podría mitigarse. Además, el bloqueo de los dominios asociados a los servidores de C2 impide que se establezcan comunicaciones de C2 y evita que el malware descargue más instrucciones o comandos, lo que reduce las posibilidades de que los atacantes realicen actividades maliciosas en la red.

Peligro inminente: la omnipresencia del tráfico malicioso en las organizaciones

Según el análisis de Akamai sobre el tráfico de DNS, podemos ver que el 13 % de los dispositivos intentaron conectarse al menos una vez a dominios asociados con malware en el cuarto trimestre de 2022 (Figura 1). Además, el 6 % se comunicó con dominios relacionados con el phishing. En el ámbito de C2, en el que nos centraremos en gran medida en este informe, observamos una tendencia creciente a lo largo del año, con un descenso muy leve en dicho trimestre.

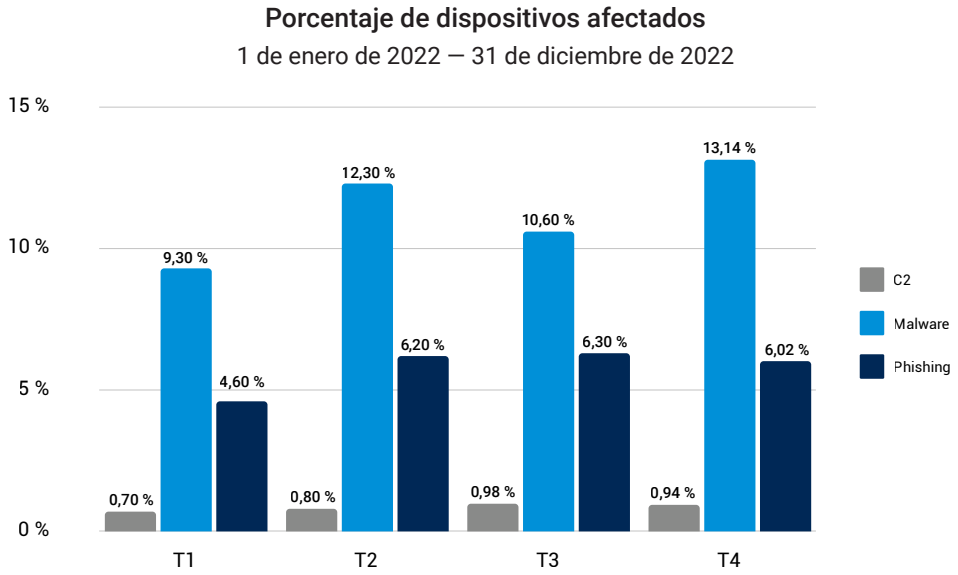


Fig. 1: Vemos una tendencia creciente en la llegada de dispositivos protegidos a destinos maliciosos

Tenga en cuenta que la Figura 1 solo hace referencia a dispositivos individuales que intentaron comunicarse con dominios maliciosos. Es importante señalar la disparidad entre los dispositivos que llegan a destinos de malware (que los atacantes pueden utilizar para descargar malware) y los dispositivos que llegan a dominios de C2 (que se suelen utilizar durante un ataque en curso para facilitar la comunicación entre el atacante y el malware, y se pueden utilizar para descargar malware adicional para continuar con un ciclo de ataque). Esta disparidad puede ser indicativa de las diferencias entre los intentos de infiltración en la red, que pueden bloquearse en el primer intento de descargar malware en un equipo, y la infiltración exitosa (que, según nuestros datos, puede no haber atravesado el DNS) o los ataques en curso, que pueden conducir a un dominio de C2 para llevar a cabo el ataque.

Este informe se centrará principalmente en el tráfico de C2 como indicador potencial de una instancia en la que un atacante ha logrado infiltrarse en a un dispositivo. Para que podamos entender la prevalencia de estos ataques, debemos examinar los datos mediante una perspectiva diferente. En lugar de analizar los dispositivos individuales, podemos agregar los datos por organización para examinar la frecuencia con la que aparece un ataque en curso (indicado por la existencia de tráfico de C2) dentro del conjunto de datos.

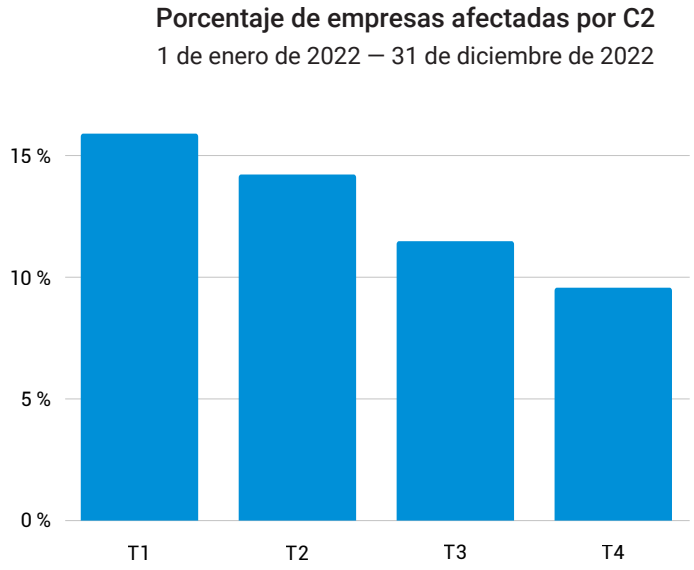


Fig. 2: Un análisis del tráfico de C2 malicioso muestra el porcentaje de organizaciones que han tenido al menos un dispositivo en un dominio de C2 a lo largo del año

> **Según nuestros datos de DNS, entre el 10 % y el 16 % de las organizaciones ha experimentado al menos un caso en el que se observó que el tráfico de C2 se desplazaba fuera de su red en un trimestre determinado.**

Según nuestros datos de DNS, entre el 10 % y el 16 % de las organizaciones ha experimentado al menos un caso en el que el tráfico de C2 intentaba desplazarse fuera de su red en un trimestre determinado (Figura 2). Esto puede indicar que el malware intenta comunicarse con un operador y es un signo de una posible infracción. Nuestra solución bloqueó este tráfico de C2 para que no llegara a su destino, pero los ataques exitosos podrían haber provocado la exfiltración de datos, ataques de ransomware y mucho más. En el primer semestre de 2022, se detectaron 2300 millones de cepas de malware, con un promedio de 1501 al día. Nuestra investigación destaca la eficacia de aprovechar el DNS para evitar que el malware progrese en una red o cause daños.

Los agentes de acceso inicial suponen una amenaza frecuente para las organizaciones

Los ataques multifase se han convertido en un elemento básico del panorama de ataques actual (Figura 3). Los atacantes consiguen un mayor éxito cuando pueden trabajar juntos (o contratarse entre sí) o cuando pueden combinar varias herramientas en un solo ataque. El C2 es fundamental para que estos ataques tengan éxito. Se pueden utilizar no solo para comunicarse, sino también para facilitar la descarga de una carga útil y el malware de la siguiente etapa para llevar a cabo el ataque. Esto se ejemplifica mejor con la cadena de ataques de ransomware Emotet/TrickBot/Ryuk observada en los últimos años. Emotet primero se infiltra en la red de la víctima y, una vez que se establece el acceso inicial, se dirige a un dominio para descargar la carga de TrickBot y obtener datos personales, credenciales y mucho más. Si la víctima se considera un objetivo de gran valor para los atacantes, el malware llega a sus servidores de C2 y descarga la carga final: Ransomware Ryuk.

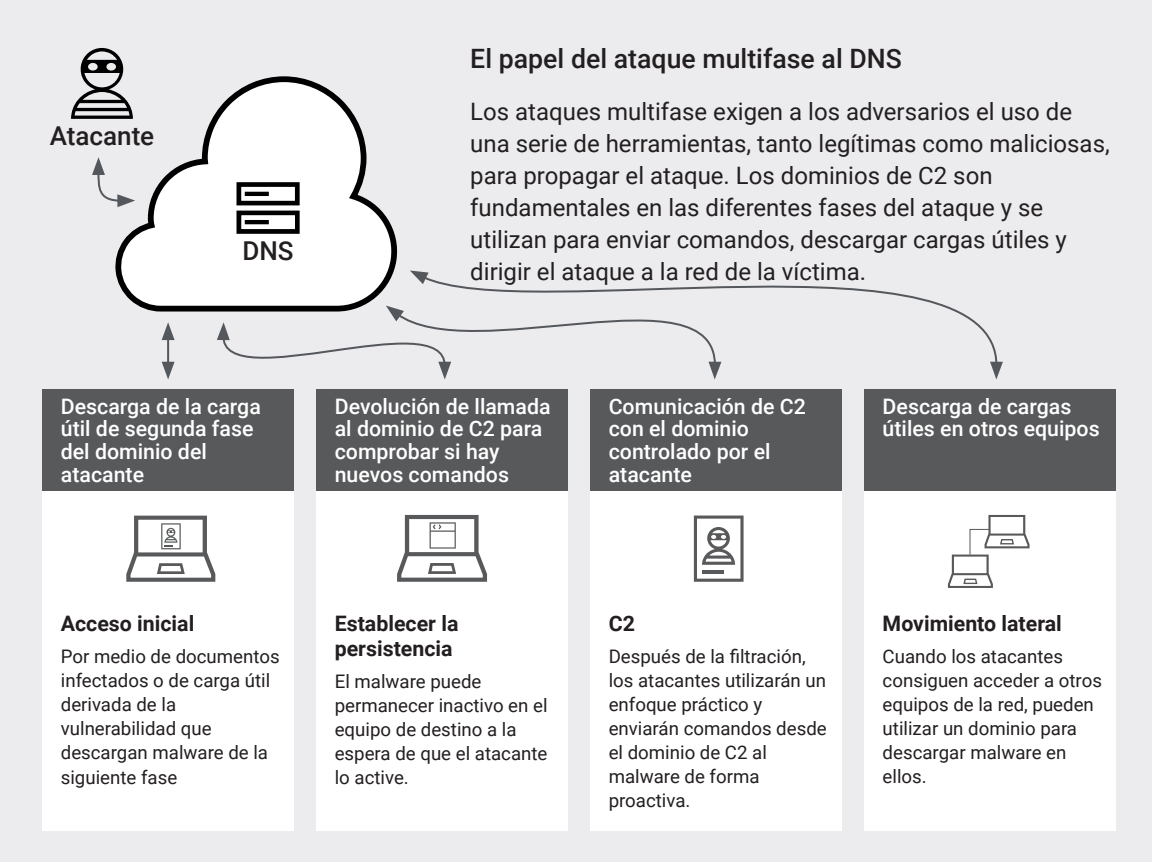


Fig. 3: El papel de C2 en cada etapa del ataque

Es importante tener en cuenta esta cadena de acontecimientos al evaluar la información contenida en este informe. La comunicación de C2 puede producirse en varias etapas del ataque. Nuestro reciente análisis de la metodología de los grupos de ransomware modernos, como el grupo Conti, demostró que los atacantes sofisticados suelen asignar operadores para que trabajen con "manos en el teclado" para avanzar de forma rápida y eficaz en un ataque. La capacidad de ver y bloquear el tráfico de C2 puede ser fundamental para detener un ataque en curso.

Los dominios de C2 que hemos observado podrían clasificarse en dominios con y sin atribución a una familia de amenazas o grupo de atacantes específicos. En esta sección, profundizaremos en los dominios de C2 asociados a un tipo de amenaza y ayudaremos a los lectores a evaluar el nivel de riesgo según las capacidades y metodologías de cada grupo. Tenga en cuenta que algunas de estas familias de malware pueden adaptarse a varios casos de uso, en función de cómo las utilicen los atacantes durante un ataque.

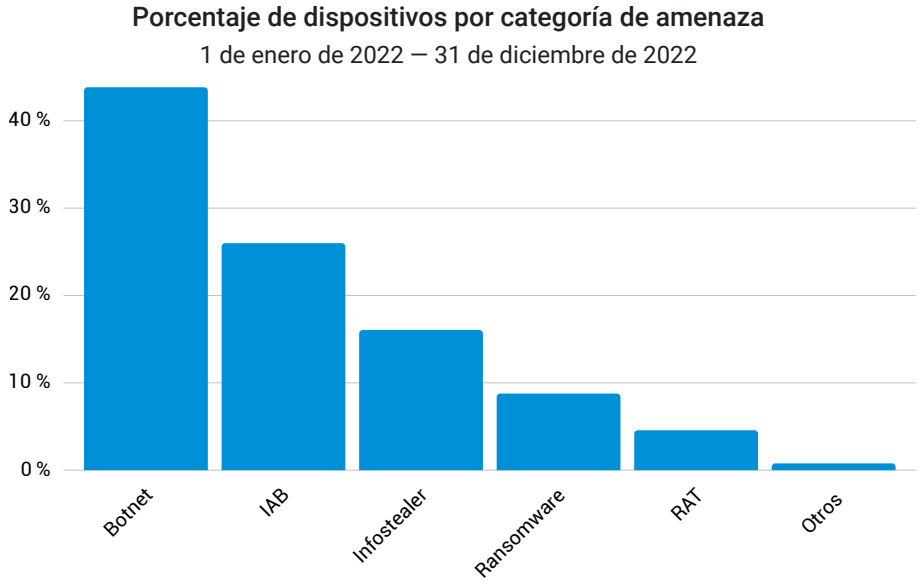


Fig. 4: Las empresas son el objetivo principal de las botnets, seguidas por los IAB y los infostealers.

En la figura 4, los grupos de atacantes se clasifican en IAB, botnets y grupos RaaS. Nuestros datos revelan que los IAB suponen una de las mayores amenazas para las redes corporativas, al igual que las botnets destinadas a la exfiltración de datos.

Agentes de acceso inicial
Los IAB se centran principalmente en proporcionar un punto de entrada inicial para que otros ciberdelincuentes, incluidos los grupos de ransomware, se introduzcan en las redes de las organizaciones. persistencia, ejecución remota de la carga útil después de la intrusión y exfiltración de datos.

Grupos de ransomware como servicio
Se trata de grupos que permiten que otros atacantes (incluso aquellos sin experiencia técnica) se conviertan en afiliados y utilicen su software de ransomware por una tarifa.

Botnets
Los atacantes pueden utilizar botnets para innumerables propósitos, desde criptominería y ataques DDoS hasta exfiltración de datos, implementación de malware y movimiento lateral.

Ladrones de información
Los infostealers recopilan varios tipos de datos, como nombres de usuario, contraseñas, información del sistema, credenciales bancarias, cookies, y así sucesivamente.

También observamos el ransomware, las herramientas de acceso remoto (RAT) y los infostealers en la combinación. Todos ellos tienen un papel fundamental que desempeñar en las varias etapas del ataque. Además, con herramientas disponibles en la clandestinidad tanto para los atacantes novatos como para los ciberdelincuentes experimentados que les permiten acceder inicialmente, permanecer ocultos en la red y, más adelante, perpretar el ataque, las organizaciones son más susceptibles que nunca a la ciberdelincuencia. A medida que avancemos por estas agrupaciones, también estableceremos las intersecciones en las que operan y las posibles implicaciones e impactos que pueden tener en las organizaciones.

Grupos de agentes de acceso inicial

Esta clase específica de ciberdelincuentes, denominada "agentes de acceso inicial" (IAB), se centra principalmente en proporcionar un punto de entrada inicial para que otros ciberdelincuentes y atacantes se infiltren en las redes de las organizaciones. Si bien varios grupos ciberdelincuentes tienen metodologías de vulneración similares (como la explotación de vulnerabilidades relacionadas con RDP y VPN, el uso de ataques de fuerza bruta, la recopilación de volcados de credenciales y el lanzamiento de correos electrónicos de phishing con malware), los IAB se especializan en obtener acceso a estos sistemas infectados y venderlos a otros grupos de atacantes, en lugar de llevar a cabo el ataque completo. Los grupos de ransomware detrás de LockBit, DarkSide, Conti y BlackByte, entre otros, habrían recurrido a los IAB en parte de sus operaciones. Un estudio de investigación de 2023 señaló que el precio promedio de venta para el acceso inicial es de aproximadamente 2800 USD.

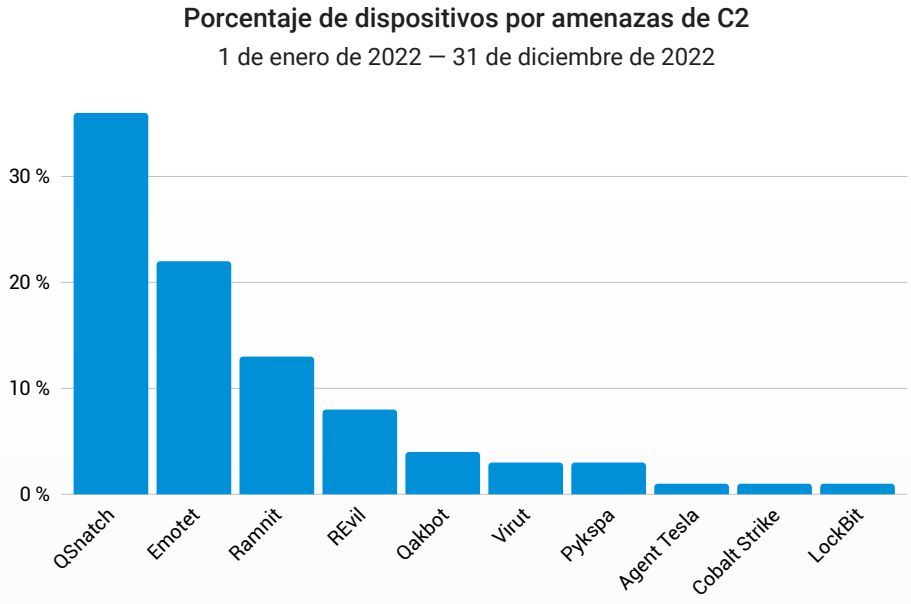
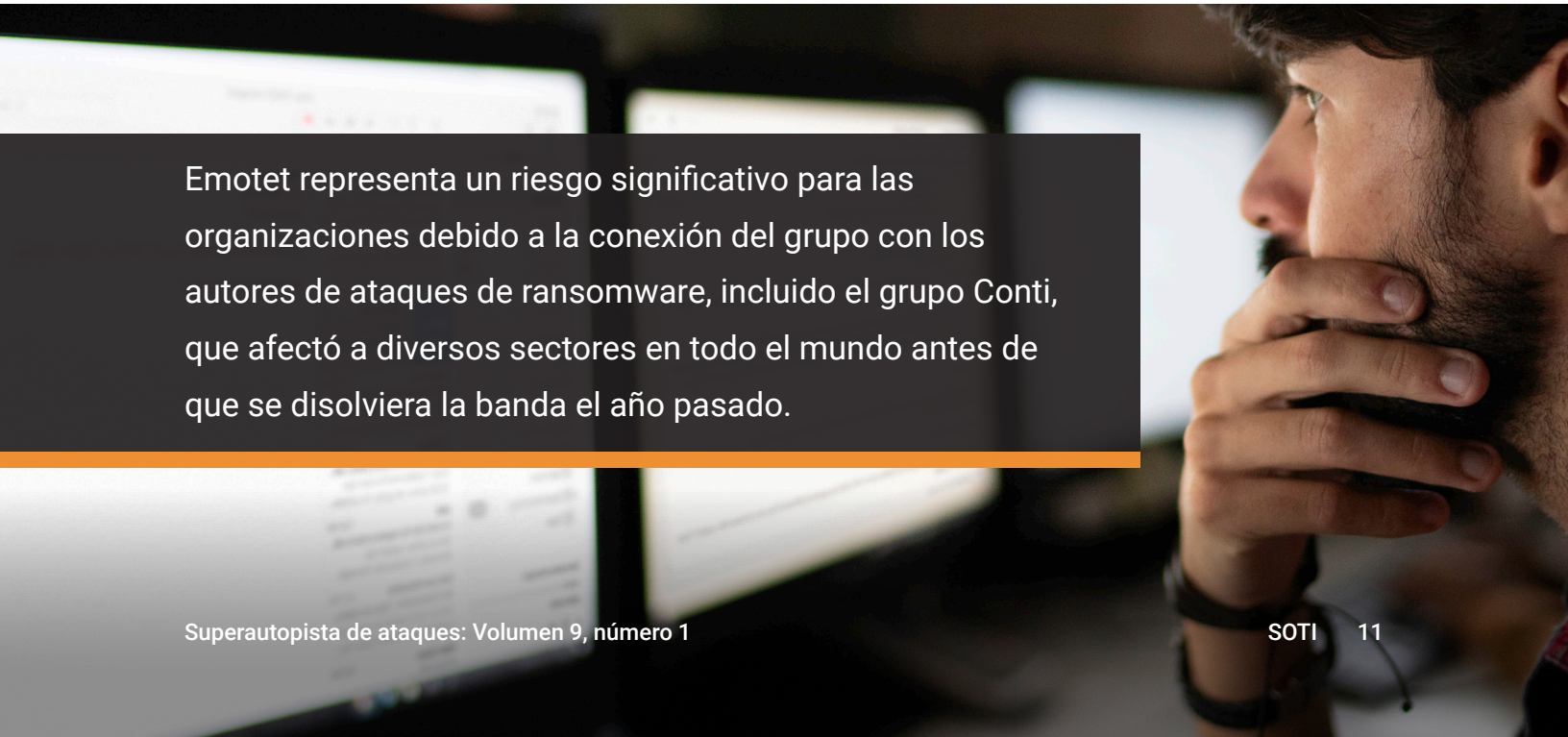


Fig. 5: QSnatch, Emotet y Ramnit son las principales familias de C2 detectadas en el tráfico de red corporativa

Según nuestros datos de DNS (Figura 5), el 26 % de los dispositivos infectados llegaba a dominios relacionados con IAB, como Qakbot (4 % de los dispositivos infectados) y Emotet (22 % de los dispositivos infectados). Los IAB desempeñan un papel importante en el modelo de negocio del RaaS y en el panorama de la ciberdelincuencia. Los autores de ataques de ransomware y otros ciberdelincuentes necesitan acceso remoto y credenciales no solo para infiltrarse en las redes de sus víctimas, sino también para moverse lateralmente, establecer la persistencia y obtener privilegios de acceso, entre otras actividades. Los atacantes aprovechan los IAB para realizar tareas laboriosas de reconocimiento, análisis de posibles objetivos e infección inicial. El acceso fácil de forma clandestina elimina ese paso y reduce el nivel de experiencia y el tiempo que necesitan los atacantes para lanzar un ataque. Como tal, introduce una gran cantidad de posibles ataques contra las organizaciones previstas, lo que da lugar a programas de chantaje, robo de información confidencial y sensible, espionaje y filtraciones de datos.

Emotet emerge como uno de los IAB más prominentes en nuestros datos. Emotet representa un riesgo significativo para las organizaciones debido a la conexión del grupo con cibercriminales que perpetran ataques de ransomware, incluido el grupo Conti, que afectó a diferentes sectores de todo el mundo antes de que se disolviera el año pasado. A lo largo de los años, Emotet ha añadido más módulos, como los que posibilitan los ataques distribuidos de denegación de servicio (DDoS) y de robo de correo electrónico, y ha expandido sus objetivos. De ser un troyano/botnet bancario con una gran cantidad de funcionalidades, Emotet se convirtió en un malware como servicio (MaaS), que distribuye amenazas como el troyano bancario IcedID, TrickBot y el ransomware UmbreCrypt. También se observó que el grupo TrickBot utilizaba Emotet para distribuir varias cepas de ransomware, como Ryuk, ProLock y Conti, entre otras. Puede encontrar una visión más detallada de las técnicas utilizadas por Emotet en el marco de MITRE ATT&CK sobre el tema.



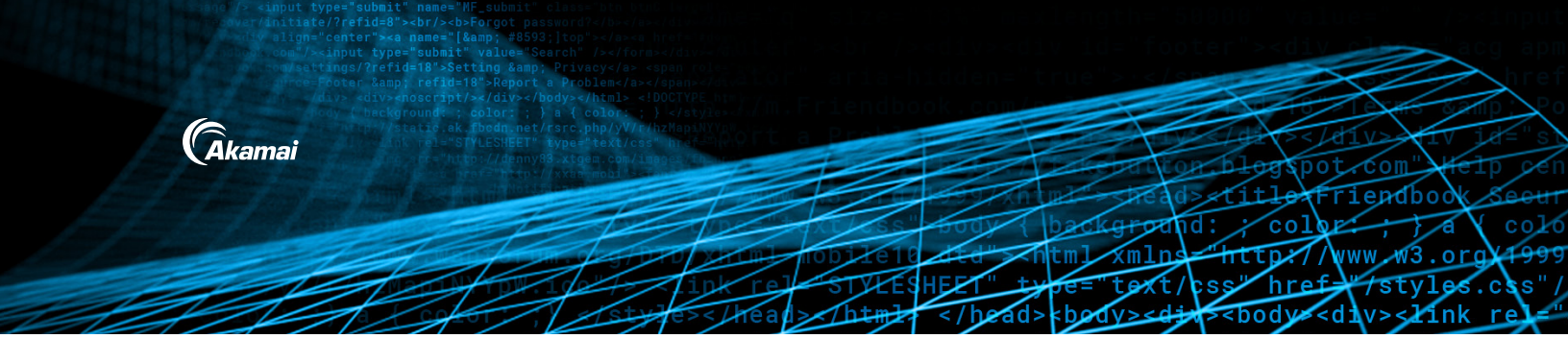
Emotet representa un riesgo significativo para las organizaciones debido a la conexión del grupo con los autores de ataques de ransomware, incluido el grupo Conti, que afectó a diversos sectores en todo el mundo antes de que se disolviera la banda el año pasado.

El segundo IAB más destacado en los datos es Qakbot. Se sabe que este grupo ha colaborado con el grupo de ransomware Black Basta que, según los datos, ha afectado al menos a 50 organizaciones de distintas partes del mundo. El equipo Qakbot es conocido por su capacidad para robar información y por difundir malware de segunda fase para comprometer ulteriormente la seguridad del sistema. Según la investigación, Qakbot aprovecha Cobalt Strike, una herramienta legítima para hacer pruebas de penetración utilizada por los equipos rojos y explotada por los adversarios, para realizar una serie de actividades maliciosas después de la intrusión y abrir una puerta trasera en el entorno de la víctima. Se trata de una técnica que cada vez utilizan más los IAB en los últimos años. El marco MITRE ATT&CK puede proporcionar inteligencia adicional relacionada con las técnicas utilizadas por Qakbot durante su ataque.

Grupos de botnets

En nuestro análisis, las botnets constituyen el mayor grupo de tipos de amenazas, con un 44 % del tráfico de C2 analizado. En este grupo hay una amplia gama de atacantes, y es esencial recordar que no todas las botnets se crean de la misma manera. Las variantes más benignas podrían introducir programas de criptominería o aprovechar el equipo de la víctima para llevar a cabo ataques DDoS. Aunque representan un coste de por sí, las botnets que hemos observado en las empresas se pueden utilizar para la exfiltración de datos y los ataques multifase, lo que puede representar un riesgo más importante. Las botnets pueden propagarse lateralmente en la red y utilizarse para implementar programas de ransomware, como en el caso de TrickBot, o pueden centrarse específicamente en el robo de información y la recopilación de credenciales.

Hemos observado que QSnatch, la botnet más grande encontrada en entornos empresariales, hace exactamente eso: exfiltración de datos de dispositivos conectados a la red. Según nuestros datos, QSnatch afectó al 36 % de los dispositivos infectados. Este malware se dirige específicamente a QNAP, un tipo de dispositivo NAS utilizado para copias de seguridad o almacenamiento de archivos por parte de las empresas. Aunque el método de infección aún se desconoce, los investigadores suponen que QSnatch podría infectar mediante la explotación de vulnerabilidades de firmware o ataques de fuerza bruta en dispositivos con nombre de usuario y contraseña predeterminados. Se recomienda encarecidamente que las empresas que utilicen QNAP mantengan su firmware actualizado (una vez infectado, QSnatch impediría la instalación de parches y desactivaría los productos de seguridad) y que cambien las contraseñas predeterminadas inmediatamente. Los atacantes utilizan QSnatch para extraer credenciales, registrar contraseñas, acceder de forma remota y exfiltrar datos, por poner algunos ejemplos. Es posible que los atacantes se dirijan a los dispositivos de almacenamiento, ya que contienen mucha información valiosa, y la infección de estos dispositivos deja a las empresas sin copias de seguridad en caso de ataques de ransomware. En esta alerta de CISA se detallan las tácticas y medidas defensivas.



Grupo de ransomware como servicio

En nuestro análisis del tráfico de DNS, el 9 % de los dispositivos infectados que llegaron a familias de C2 accedió a los dominios asociados a los grupos RaaS. Este tipo de grupo de ciberdelincuentes permite que otros atacantes (incluso sin experiencia técnica) se conviertan en afiliados y utilicen su software de ransomware por una tarifa. Las organizaciones afectadas por ransomware se enfrentan a innumerables consecuencias que no se limitan a la pérdida de datos confidenciales. Las empresas podrían enfrentarse potencialmente a costes de reparación y recuperación, honorarios legales, multas, tiempo de inactividad, lo que daría lugar a una pérdida de productividad y daños a la marca y la reputación. Cybersecurity Ventures estimó que el coste de los ataques de ransomware podría ascender hasta alcanzar aproximadamente los 265 000 millones de dólares al año en 2031. El informe global de ransomware de Akamai también subraya los efectos devastadores del ransomware, que van más allá de las pérdidas financieras, como la interrupción de la cadena de suministro, y, en algunos casos, podría representar una cuestión de vida o muerte.

Un prolífico grupo RaaS es el grupo REvil, que se dio a conocer por atacar a un proveedor de gestión de TI en un ataque a la cadena de suministro que afectó a más de 1500 proveedores de servicios gestionados. Sus operaciones cesaron con la detención de varios miembros por parte del gobierno ruso. Sin embargo, pocos meses después de la disolución, los investigadores de seguridad observaron que el sitio de filtración de REvil estaba nuevamente activo con información de sus últimas víctimas, incluyendo algunas universidades de los Estados Unidos. Los investigadores han especulado que puede que no sea el mismo grupo REvil quien dirige esta campaña y han advertido sobre gobiernos que afirman ser el grupo REvil para ocultar sus huellas. En términos de tácticas, REvil es conocido por personalizar su flujo de ataque en función de las víctimas a las que va dirigido, lo que demuestra el nivel de conocimiento que el grupo tiene de sus objetivos. Para aprender más sobre las tácticas, técnicas y procedimientos relacionados con REvil, consulte la publicación de MITRE.

> **Es posible que los atacantes se dirijan a los dispositivos de almacenamiento, ya que contienen mucha información valiosa, y la infección de estos dispositivos deja a las empresas sin copias de seguridad en caso de ataques de ransomware.**

Otro grupo RaaS que hemos detectado en nuestro análisis del tráfico de DNS es LockBit. Tras la "desaparición" de Conti, el grupo LockBit se convirtió en uno de los proveedores de RaaS más activos. Antes de eso (de noviembre de 2019 a marzo de 2022), fue el operador de RaaS con el mayor número de organizaciones afectadas después de Conti, según este informe.

El grupo LockBit se enorgullece de tener un mecanismo de cifrado más rápido que otros grupos RaaS, y afirmó haber afectado a más de 12 000 empresas con su LockBit 2.0. En junio de 2022, el grupo lanzó LockBit 3.0, con funcionalidades adicionales, incluyendo un programa de recompensa por hallar vulnerabilidades. También aprovecha la vulnerabilidad Log4j para obtener acceso inicial a sus objetivos, lo que subraya la importancia de la aplicación de parches. Las organizaciones que no han abordado estos fallos de seguridad pueden correr un mayor riesgo de infectarse con LockBit. LockBit sigue reinventándose; una de las últimas incorporaciones es la táctica de triple extorsión mediante la que cifran archivos, los publican en sitios de filtración y lanzan ataques DDoS si las víctimas se niegan a pagar el rescate.

Herramientas de trabajo

Las herramientas identificadas en esta sección pueden desempeñar un papel específico en un ataque, ya sea por violar el sistema, obtener información o escalar privilegios. El arsenal que observamos en varios grupos de atacantes a menudo requiere comunicación para funcionar como infostealers y RAT. Comprender estas herramientas, junto con las tácticas utilizadas por los grupos de atacantes, puede ayudar a los profesionales de la seguridad a comprender cómo se producen los ataques y a planificar en consecuencia.

Infostealers

Diseñados para obtener diversos tipos de datos (como nombres de usuario, contraseñas, información del sistema, credenciales bancarias y cookies, entre otros), los infostealers siguen siendo una de las ofertas de MaaS utilizadas con más frecuencia en los ataques. Los atacantes que no tengan conocimientos o habilidades técnicas suficientes podrían simplemente adquirir infostealers a un coste relativamente bajo y lanzar sus propios ataques.

En la lista de familias de malware de C2, observamos que el 16 % de los dispositivos han accedido a la atribución conocida de C2 valiéndose de infostealers. Ramnit (el 13 % de los dispositivos infectados) no es simplemente otro infostealer común. Su punto fuerte reside en su gran modularidad, que permite a los atacantes aprovechar sus diversas funcionalidades, como robar otros datos confidenciales y descargar o implementar malware para alcanzar su objetivo final o continuar el ataque. En 2021, Ramnit fue considerado el principal troyano bancario, con noticias recientes que destacan cómo otro malware compartía un código similar con Ramnit.

La presencia de infostealers en su red es una señal reveladora de que sus credenciales de usuario pueden estar en riesgo. La información robada recopilada podría venderse en los mercados clandestinos y ser utilizada por otros atacantes para obtener acceso inicial. Los grupos de ransomware podrían implementar un infostealer mediante phishing o botnets para obtener credenciales válidas, alquilar una licencia de acceso a un infostealer en un foro clandestino que ofrezca MaaS o adquirir acceso a la red a través de IAB. En algunos casos, los operadores de infostealer podrían convertirse en IAB y vender credenciales recopiladas de alto valor (como accesos VPN o RDP) al mejor postor u otros atacantes que podrían lanzar un ataque mucho más sofisticado.

Herramientas de acceso remoto

Varios grupos de atacantes han explotado Cobalt Strike en el curso de sus operaciones. Los atacantes utilizan esta potente RAT de diversas formas, entre las que se incluyen el reconocimiento, la escalada de privilegios, el movimiento lateral a través de la red, el establecimiento de persistencia, la ejecución remota de la carga útil tras la intrusión (como el ransomware) y la exfiltración de datos. Aunque la herramienta se utiliza principalmente después de la filtración para el movimiento lateral y la exfiltración, también puede ser el vector de acceso inicial, ya que tiene un módulo de spear-phishing. Los grupos que han utilizado esta herramienta son Conti, Qakbot, TrickBot y Emotet, entre otros. Para ayudar a detectar Cobalt Strike en un entorno, se ha creado este conjunto de reglas de YARA para determinar el uso malicioso de la herramienta.

Nuestros datos también muestran la presencia de tráfico de C2 de Agent Tesla. Esta RAT se vende en el mercado clandestino y su precio asequible y facilidad de uso hacen que esta herramienta resulte atractiva para los ciberdelincuentes. Los atacantes podrían utilizar esta herramienta para recopilar credenciales de varios navegadores y registrar las teclas pulsadas y capturas de pantalla. Una de sus tácticas más notables es la apropiación de formularios, que permite a los atacantes recopilar información de identificación personal (PII) y otra información confidencial. Dicha información robada podría utilizarse para el robo de identidad o el fraude. PCrisk ha publicado más detalles sobre las técnicas de Agent Tesla y sobre cómo afecta a los usuarios.

El panorama de actividad muestra campañas esporádicas de malware a lo largo del año

En el transcurso de un año, observamos fluctuaciones en las actividades de malware C2 (Figura 6). Pongamos como ejemplo este caso: Emotet se muestra particularmente activo durante enero y febrero de 2022, tras su resurgimiento en noviembre de 2021. Este aumento de la actividad demuestra una formidable campaña para ayudarle a recuperar su estatus después de meses de inactividad. En los meses siguientes a su regreso, Emotet mejoró sus tácticas incluyendo formas de eludir la decisión de Microsoft de deshabilitar las macros de Visual Basic for Applications. Ciertos informes indican que Emotet volvió a estar inactivo entre julio y noviembre de 2022; nuestros análisis de datos demuestran una disminución del tráfico de C2 en julio, como se observó en el menor porcentaje de dispositivos infectados que llegan a los dominios de Emotet. Esto puede indicar que el grupo ha permanecido activo durante todo el año, o podría tratarse de un caso de malware instalado que sigue comunicándose con una infraestructura obsoleta. Las detecciones de 2023 podrían ayudarnos a determinar si el grupo Emotet ha quedado realmente inactivo.

Porcentaje mensual de dispositivos por amenazas principales de C2

Enero de 2022 — Diciembre de 2022

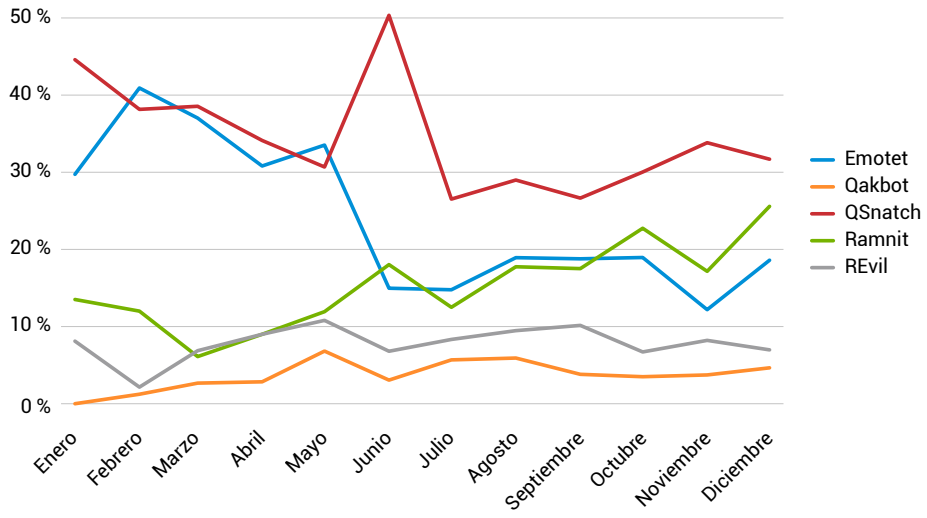


Fig. 6: El gráfico de tendencia mensual muestra que QSnatch estuvo constantemente activo durante 2022

> **Emotet se muestra particularmente activo en enero y febrero de 2022, tras su resurgimiento en noviembre de 2021. Este aumento de la actividad demuestra una formidable campaña para ayudarle a recuperar su estatus después de meses de inactividad.**

QSnatch permanece activo durante todo el año, alcanzando su máximo en junio, lo que demuestra la prevalencia de esta amenaza. Los servidores NAS son objetivos viables para los atacantes por varias razones: En primer lugar, contienen datos confidenciales; en segundo lugar, hay menos probabilidades de que se apliquen parches a los servidores NAS; y, en tercer lugar, estos dispositivos son potencialmente más accesibles en la red de la organización y podrían servir de centro de movimiento lateral. Aunque se han producido cambios en los últimos años, como la incorporación de soluciones de seguridad integradas, los ciberdelincuentes las eludieron desactivando los productos de seguridad instalados o impidiendo que los dispositivos se actualicen con nuevas correcciones. Por lo tanto, estos dispositivos siguen siendo vulnerables frente a nuevas cepas de este malware.

También observamos el aumento de las cifras de Ramnit en las redes corporativas de agosto a diciembre. Esto es preocupante, ya que este malware podría robar una amplia variedad de información confidencial que los atacantes podrían vender posteriormente a otros atacantes para futuros ataques.

QSnatch y Emotet: amenazas comunes en todas las regiones

Para determinar las amenazas más frecuentes por región, examinamos el porcentaje de dispositivos de cada región que llegan a dominios de C2 (Figura 7). Cada porcentaje está relacionado con el número de dispositivos afectados por región, que también varía de una a otra. Curiosamente, detectamos tendencias de ataque similares en todas las regiones, aunque con muy pocos valores atípicos. Por lo tanto, recomendamos que cada región siga las recomendaciones proporcionadas en la sección “Conclusión y recomendaciones” o en cada grupo de malware de las secciones anteriores.

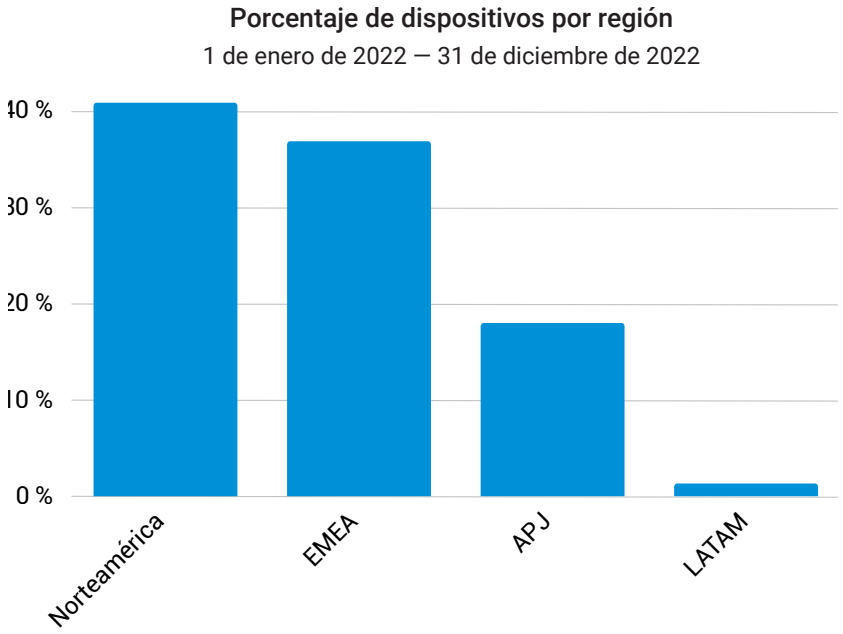


Fig. 7: Norteamérica se pone a la cabeza con un 41 %, seguida de EMEA (37 %) y APJ (18 %), en lo que respecta al número de dispositivos afectados por región

Norteamérica

La mayoría de las organizaciones de todo el mundo sufrieron estas dos amenazas principales: QSnatch y Emotet. En Norteamérica, aproximadamente el 29 % de los dispositivos afectados de la región han sido víctimas de Emotet, mientras que el 33 % lo han sido de QSnatch (Figura 8). Según un informe de Dark Reading, una búsqueda de Shodan mostró que hay 300 000 dispositivos QNAP conectados a Internet, lo que lo convierte en un objetivo atractivo. Además, los dispositivos NAS como QNAP se pueden utilizar como copia de seguridad y actuar como servidores de archivos o medios.

Otras amenazas notables en Norteamérica son Ramnit, Qakbot y REvil. Resulta interesante dado que los IAB como Emotet allanaron el camino para otras infecciones, incluyendo (entre otros) el ransomware.

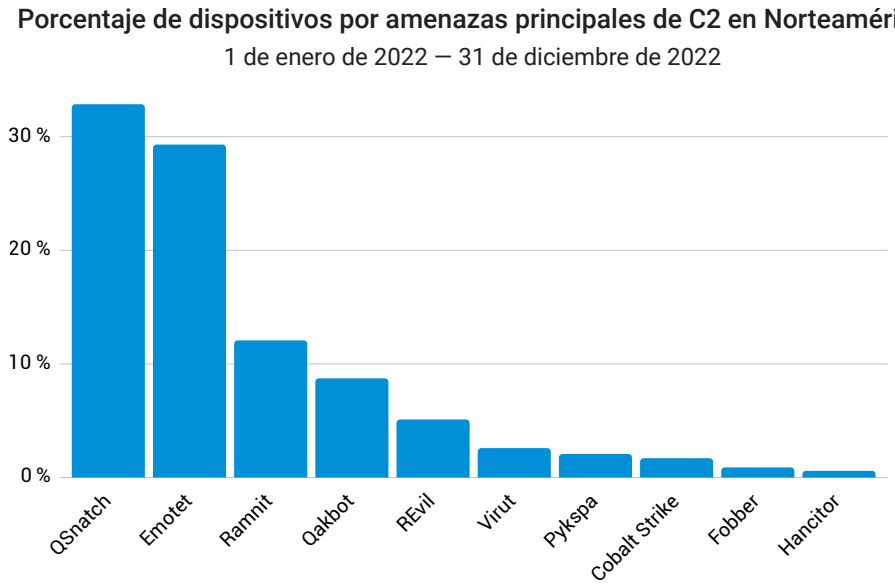


Fig. 8: La mayoría de los dispositivos afectados de las organizaciones norteamericanas accedió a dominios relacionados con QSnatch, Emotet y Ramnit al menos una vez

Europa, Oriente Medio y África

EMEA tiene el mayor porcentaje de dispositivos afectados junto a Norteamérica. Las principales amenazas que observamos en la región (Figura 9) fueron QSnatch (28 %) y Ramnit (21 %). No es sorprendente ver el ascenso de Ramnit en la región, ya que sus operadores habían atacado a instituciones bancarias y financieras en Italia, el Reino Unido y Francia en el pasado. En una de sus iteraciones, la configuración de Ramnit incluyó a países de la UE como objetivos principales. De hecho, si se compara el número de dispositivos afectados por Ramnit en todo el mundo, EMEA sigue registrando el mayor número de infecciones. Además, los dispositivos con infección por Emotet también fueron altos en la región, con un 19 %.

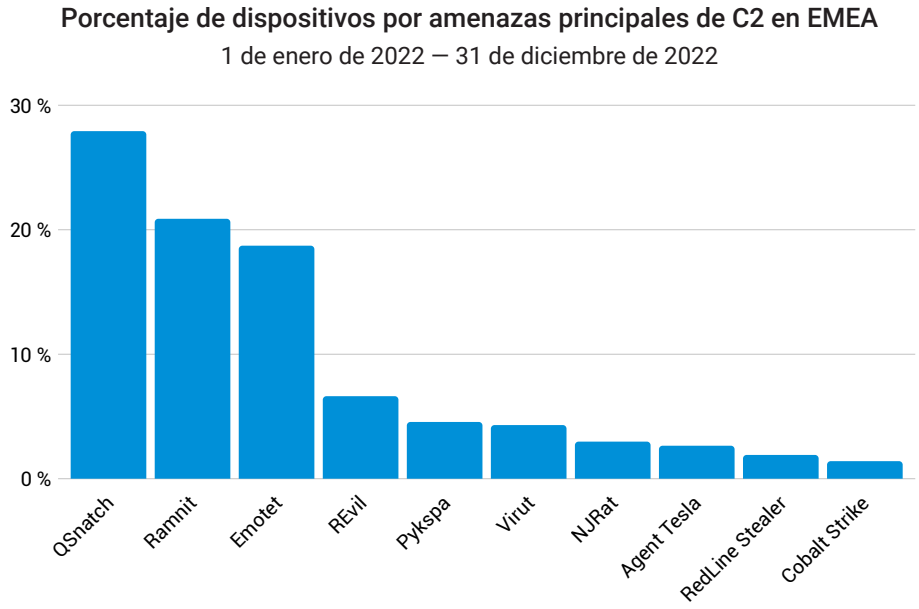
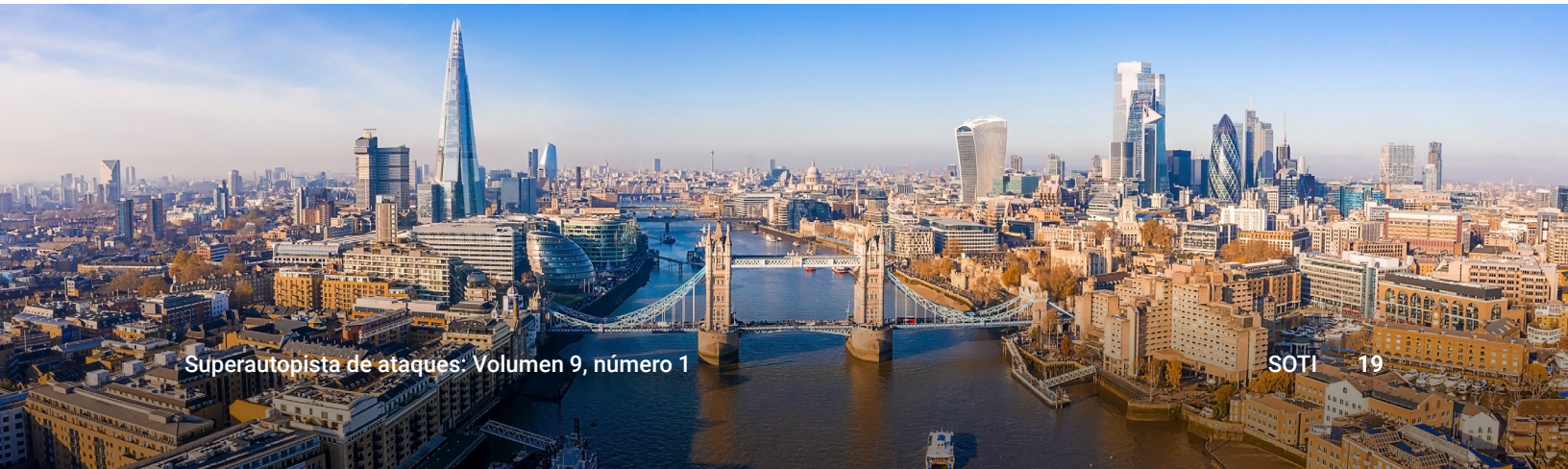


Fig. 9: Hemos observado que más dispositivos llegan a Ramnit C2 en EMEA que en otras regiones, lo que aumenta significativamente el riesgo de sus organizaciones



Asia-Pacífico y Japón

En la región APJ, constatamos una alta tasa de incidencia de QSnatch (Figura 10). Cuando comparamos las cifras de cada región, APJ ocupa el segundo lugar junto a Norteamérica en términos de dispositivos con infecciones por QSnatch. Por otro lado, APJ también debería protegerse de las cepas de ransomware REvil y LockBit, ya que se encuentran entre las cinco principales amenazas observadas en los dispositivos afectados de la región. Aunque los miembros de la banda REvil fueron detenidos el año pasado, este malware se ha detectado de nuevo varios meses después. Es posible que antiguos miembros que tienen acceso al código intentaran reactivar REvil. No es sorprendente ver amenazas de ransomware (que están motivadas en gran medida por objetivos financieros) como LockBit y REvil. Además, puesto que los operadores de RaaS siguen utilizando IAB como Emotet, el ransomware sigue siendo un problema de seguridad crítico para las empresas de todos los sectores y regiones.

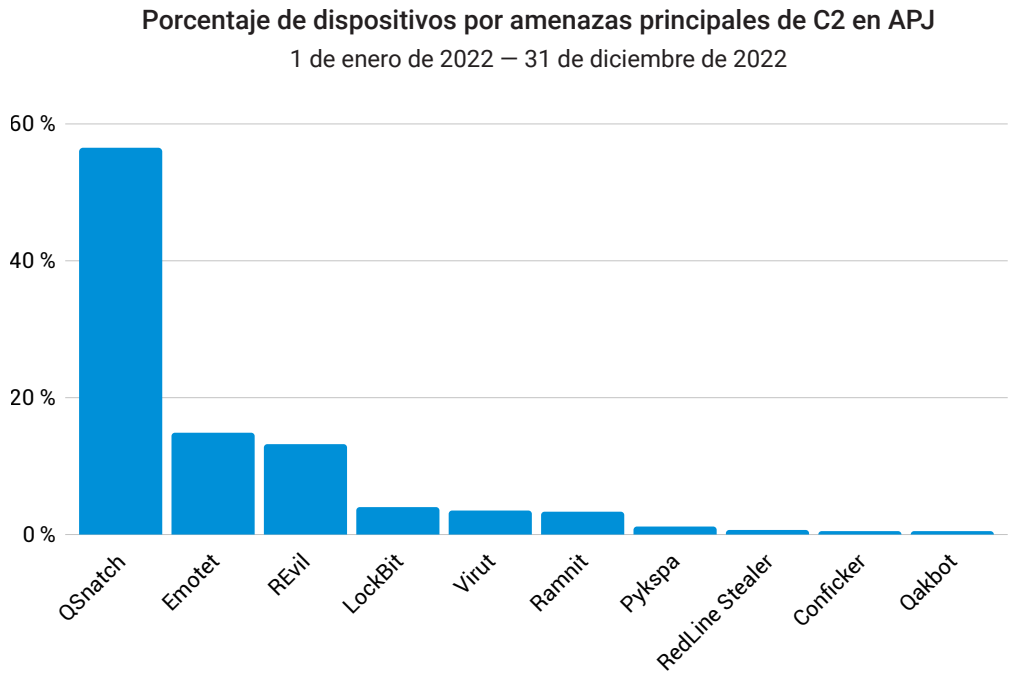
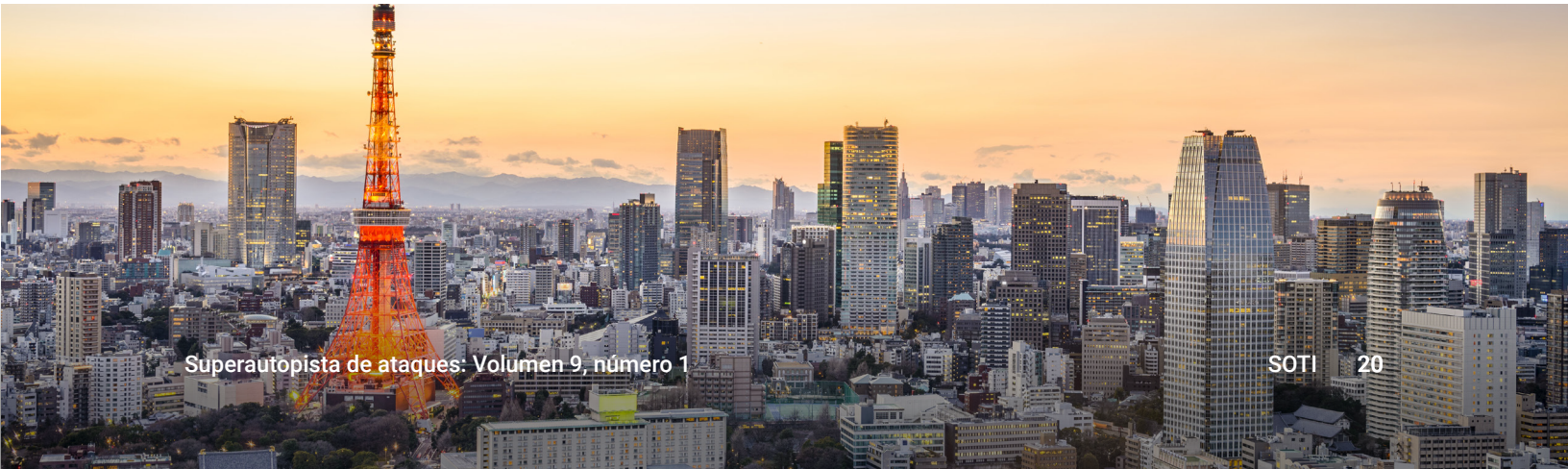


Fig. 10: Akamai observó un número significativo de infecciones de QSnatch en la región



Latinoamérica

Examinemos ahora las tendencias en Latinoamérica. Aunque esta región tiene el menor número de dispositivos afectados, eso no significa necesariamente que sufra un menor impacto. Al igual que en las tendencias mundiales, esta región se ha visto afectada por QSnatch y Emotet (Figura 11). Al examinar esta región individual por sí sola, se revela que Agent Tesla, Virut, y Ramnit son prominentes.

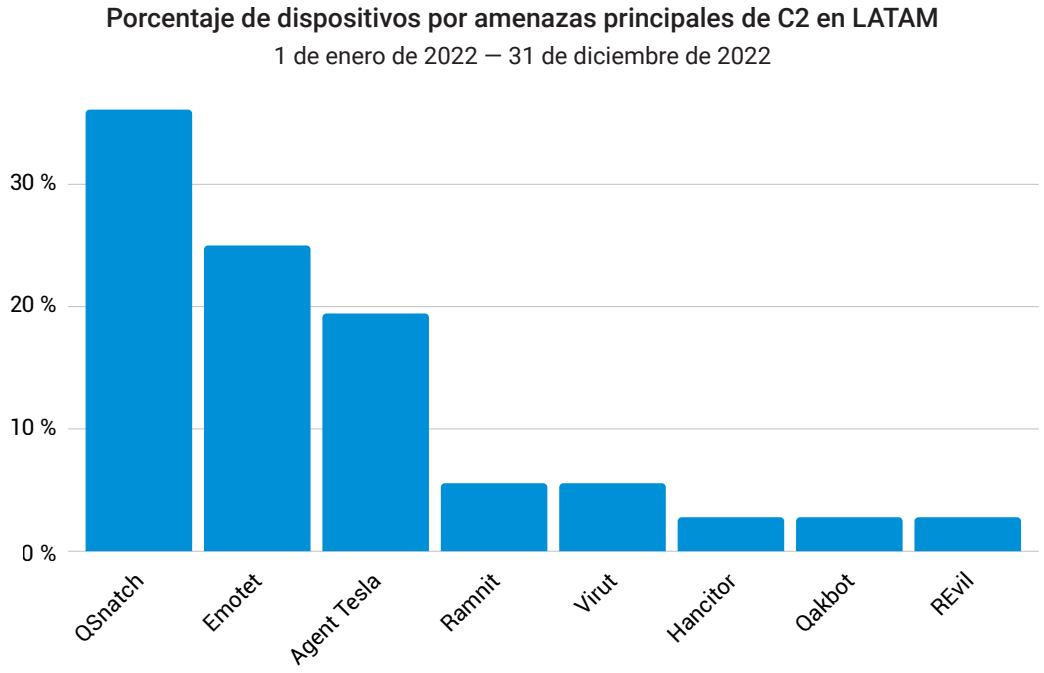


Fig. 11: Las tendencias globales también se reflejan en el panorama de amenazas de LATAM

Los desgloses regionales son importantes para ver no solo las similitudes, sino también para identificar qué amenazas específicas son únicas en cada región. Aunque QSnatch es siempre la principal familia de amenazas, las siguientes cuatro principales amenazas cambian en todas las regiones con una combinación de Emotet, REvil, Ramnit y Agent Tesla. Las amenazas regionales marcan la diferencia a medida que decide en qué deben centrarse sus equipos de gestión de vulnerabilidades y pruebas de penetración (pentest).

Tendencias en la industria y en sectores verticales: la fabricación se vio gravemente afectada por los agentes de acceso inicial, botnets

El análisis de las tendencias de la industria nos permite ver el nivel de riesgo de cada sector vertical individual y su situación en comparación con otros sectores. En lugar de examinar el número de dispositivos afectados, hemos agregado los dispositivos por clientes para determinar cuántas empresas se ven afectadas por cada vertical (Figura 12). Según nuestros datos de DNS, más del 30 % de las organizaciones analizadas con tráfico de C2 malicioso se encuentran en el sector de la fabricación. Además, las empresas de los sectores verticales de servicios empresariales (15 %), alta tecnología (14 %) y comercio (12 %) también se han visto afectadas. Los dos sectores verticales principales de nuestros datos de DNS (fabricación y servicios empresariales) también se encuentran entre los más afectados por el ransomware Conti, que abordamos en nuestro informe global de ransomware. En ese informe, profundizamos en las víctimas del ransomware Conti y las perfilamos según el sector, los ingresos y la región, ilustrando las tendencias de ataque de esta prolífica amenaza.

> **Según nuestros datos de DNS, más del 30 % de las organizaciones analizadas con tráfico de C2 malicioso se encuentra en el sector de la fabricación. Además, las empresas de los sectores verticales de servicios empresariales (15 %), alta tecnología (14 %) y comercio (12 %) se han visto afectadas de forma similar.**

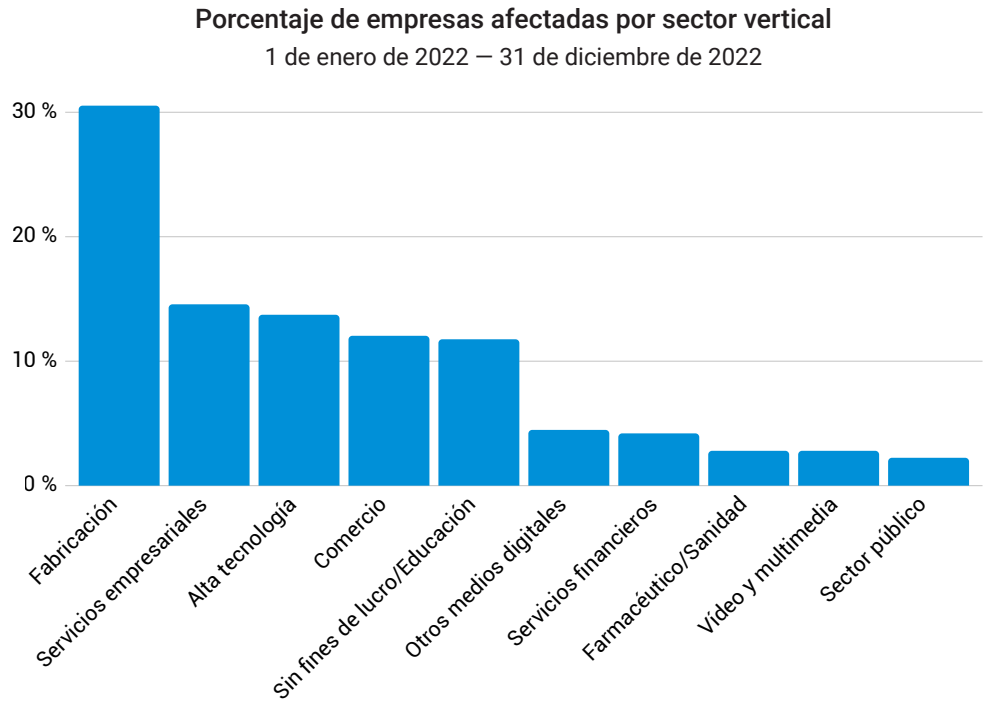


Fig. 12: Los sectores de la fabricación, los servicios empresariales y la alta tecnología son los más afectados por las infecciones de C2

El hecho de que estemos viendo que la fabricación se ve gravemente afectada por diversos ataques de C2 es preocupante, ya que se considera una infraestructura crítica, y los ataques consumados en este sector podrían tener repercusiones concretas, como interrupciones en la cadena de suministro. Los datos no muestran razones específicas de por qué la fabricación es el sector vertical más afectado, pero una investigación más exhaustiva sobre los tipos de amenazas en este sector podría arrojar algo de luz.

Estamos observando cómo algunos países utilizan las normativas para reforzar la seguridad en sectores críticos como el de la fabricación. La directiva NIS2 de la UE ha reforzado los estándares de ciberseguridad y los requisitos de seguridad, como los análisis de riesgos y las políticas de seguridad de los sistemas de información, la protección de la cadena de suministro y la gestión de incidentes para entidades esenciales (por ejemplo, energía, transporte, banca, salud, etc.). También ha ampliado el alcance de los sectores verticales afectados.

Porcentaje de dispositivos por amenazas principales de C2 en el sector de la fabricación

1 de enero de 2022 — 31 de diciembre de 2022

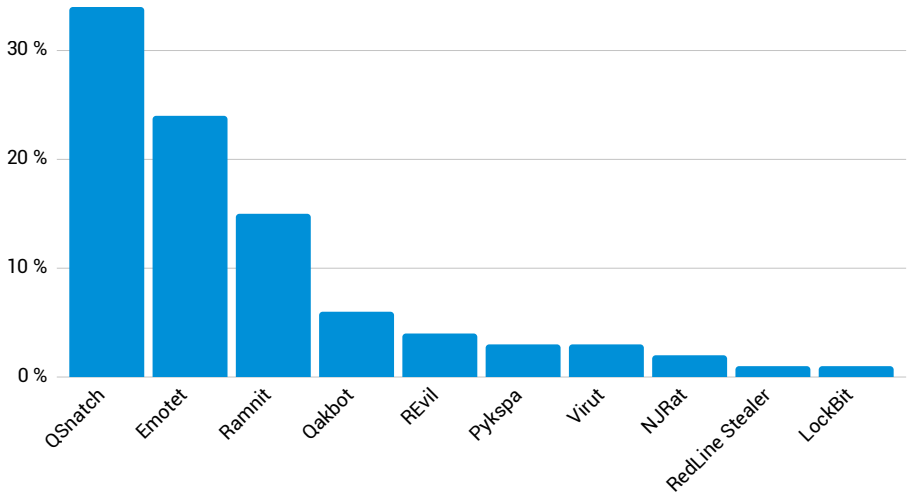


Fig. 13: Las principales familias de amenazas de C2 identificadas en el sector de la fabricación son QSnatch, Emotet y Ramnit

Un análisis detallado del sector de la fabricación revela que QSnatch, IAB y Ramnit son algunos de los principales dominios relacionados con C2 a los que accedieron las organizaciones en este sector vertical (Figura 13). La presencia de IAB en su red podría ser indicativa de que los atacantes están recopilando información sobre sus posibles objetivos y, una vez que tienen acceso a los equipos comprometidos, pueden vender esos datos a otros ciberdelincuentes, como los grupos RaaS. Además, también detectamos infostealers en la lista de malware C2 que está amenazando a este sector. Una amenaza a tener en cuenta es RedLine Stealer, que tiene la capacidad de recopilar información del navegador, como credenciales y detalles de tarjetas de crédito, y actualmente se vende como MaaS por una suscripción mensual de 100–150 USD. Según las investigaciones del Group-IB, este infostealer recopiló unos 35 585 412 registros, que pueden contener cuentas de registro único, entre el segundo semestre de 2021 y el primer semestre de 2022. Además, los dominios de C2 relacionados con este infostealer aumentaron en un 409 % solo en el T3 2022.

Siempre es interesante observar las tendencias de los sectores. Lo que ocurre en un sector vertical suele ser solo un peldaño, ya que los ciberdelincuentes se abren paso por todos los sectores de la industria. A veces, observamos que los atacantes se centran en una tecnología que es prominente en un sector. Otras veces, atacarán a los que tienen más probabilidades de pagar o a quienes pueden pagar más. También los hemos visto atacar a sectores que tradicionalmente no invierten tanto en ciberseguridad. La conclusión es que, si se ve humo en la casa del vecino, conviene comprobar el propio sistema de prevención de incendios.

Usuarios particulares objeto de ataque

Los atacantes centran su atención en las empresas porque presentan una mayor rentabilidad cuando se vulneran sus redes. Utilizan una amplia gama de herramientas y tácticas para infiltrarse en el perímetro de una empresa, mantener la persistencia y, en algunos casos, exfiltrar información confidencial. Como tal, vemos amenazas como los infostealers y los IAB en las redes corporativas, como se explicó en la sección anterior. Sin embargo, es una situación diferente en las redes domésticas, en cuanto a qué tipo de amenazas se está empleando y con qué fin.

Los usuarios domésticos representan a un grupo demográfico que a menudo no es tan seguro como un entorno corporativo. Además, este grupo no ofrece el mismo rendimiento monetario. Los atacantes lo saben, por lo que buscan formas de rentabilizar su capacidad para infectar los dispositivos domésticos con mayor facilidad. Por ejemplo, lanzan campañas a gran escala con la esperanza de poner en peligro tantos dispositivos como sea posible en las tácticas “spray and pray”, mientras que los ataques contra las empresas son muy focalizados. Una vez que estos dispositivos domésticos pasan a formar parte de una botnet masiva, los atacantes pueden movilizar estos dispositivos zombis para realizar innumerables actividades de ciberdelincuencia sin el conocimiento del usuario, como spam y lanzamiento de ataques DDoS contra organizaciones. Y para que las botnets tengan éxito o para que los ciberdelincuentes alquilen sus botnets, deben infectar tantos dispositivos como sea posible. Otra forma en que los atacantes pueden beneficiarse económicamente del impacto en los usuarios domésticos es utilizando los recursos informáticos de los dispositivos infectados con fines de criptominería.

> **Una vez que estos dispositivos pasan a formar parte de una botnet masiva, los atacantes pueden movilizar estos dispositivos zombis para realizar innumerables actividades de ciberdelincuencia sin el conocimiento del usuario, como spam y lanzamiento de ataques DDoS contra organizaciones.**

Las redes domésticas muestran un tráfico intenso de botnets

A medida que nos centremos en los usuarios domésticos, examinaremos el tráfico de DNS malicioso de las redes domésticas mediante el análisis de una muestra anónima de los millones de consultas con indicadores maliciosos de los últimos seis meses, para demostrar qué amenazas deberían preocupar a los usuarios. De un vistazo, las principales amenazas se relacionan con las botnets, lo que podría explicar cómo los atacantes utilizan los dispositivos del IoT para diferentes fines, algo que trataremos en las siguientes secciones.

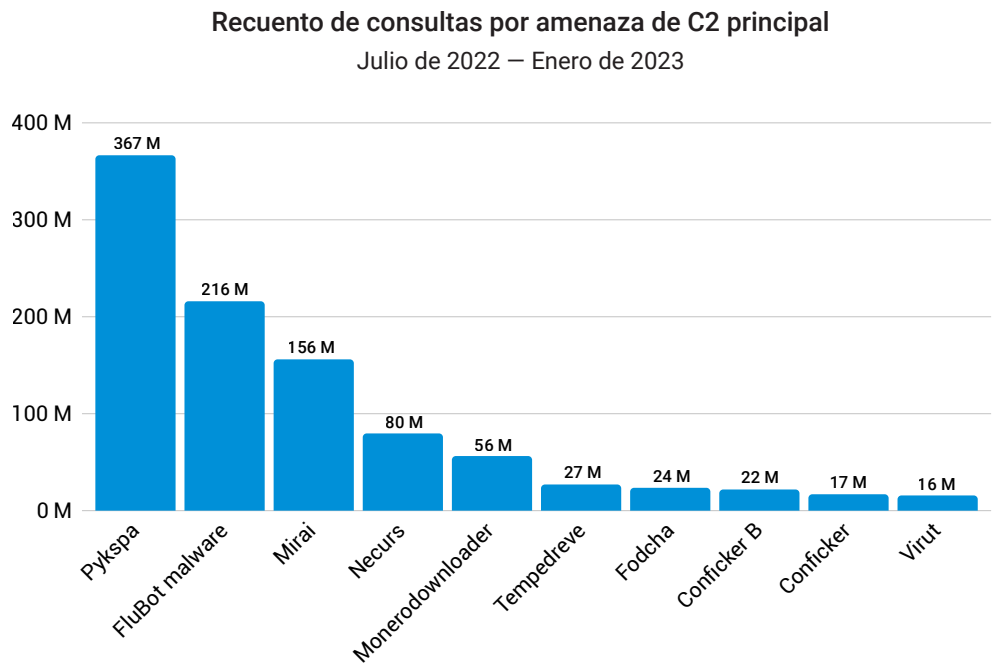


Fig. 14: Pykspa, el malware FluBot y Mirai son las tres botnets principales observadas en el tráfico de DNS de las redes domésticas

Pykspa: propagación a través de las redes sociales

Según nuestros datos, Pykspa fue responsable de 367 millones de consultas de DNS registradas a nivel global (Figura 14). Esta amenaza se propaga a través de Skype mediante el envío de enlaces maliciosos a los contactos de los usuarios afectados. En algunos casos, cuando Twitter se abre en la pestaña del navegador, también se crea un twit con un enlace de descarga al malware. Además, utiliza un algoritmo de generación de dominios (DGA) para establecer la comunicación de C2. En el pasado, su v2 utilizaba un subconjunto de su DGA para evitar que se detectara y permanecer dentro de la red durante más tiempo.

Sus capacidades de puerta trasera permiten a un atacante conectarse a un sistema remoto y ejecutar comandos arbitrarios como descargar archivos, terminar procesos y propagarse por diversos medios (por ejemplo, unidades asignadas, recursos compartidos de red), entre otros. Pykspa también consulta la configuración de Skype para recopilar información personal sobre los usuarios afectados. También impide que los usuarios accedan a determinados sitios web, especialmente si contienen ciertas cadenas relacionadas con soluciones antimalware. Curiosamente, comprueba la interfaz de idioma de Skype del usuario afectado y, si es uno de los muchos idiomas que están supervisando (incluidos inglés, alemán, francés, español e italiano) el malware modifica el mensaje de spam de Skype en consecuencia.

FluBot: botnet de malware de Android

El malware FluBot es la principal familia de malware C2 después de Pykspa. Infecta principalmente teléfonos Android a través de mensajes de texto, los cuales invitan a los usuarios a hacer clic en un enlace malicioso que conduce a la descarga del malware. Como parte de su táctica de propagación, el malware FluBot carga las listas de contactos de los usuarios afectados en el servidor de C2 y también envía a los contactos de las víctimas el mismo cebo de ingeniería social. Para los usuarios, tener FluBot en su dispositivo pone en riesgo su información bancaria y financiera, ya que este malware tiene la capacidad de superponer una página falsa cuando los usuarios acceden a aplicaciones bancarias legítimas. Por lo tanto, estas credenciales podrían utilizarse para el robo de identidad o para realizar transacciones fraudulentas.

Este malware utiliza varios cebos de ingeniería social. Por ejemplo, puede sugerir que los usuarios hagan clic en un enlace para comprobar el estado de la entrega de un paquete; en otras situaciones, puede engañar a los usuarios para que descarguen una aplicación de correo de voz falsa diciéndoles que hay un mensaje de voz. También puede pretender ser una actualización de seguridad e instar a los usuarios a hacer clic en el enlace. Una vez que los usuarios hacen clic en él, se les indica que descarguen una aplicación. Esta aplicación, a su vez, solicita permiso para acceder a las listas de contactos y realizar llamadas de teléfono, etc. Lo que hace que esta amenaza sea tan peligrosa es que también solicita permiso a los servicios de accesibilidad, lo que permite a los atacantes controlar los toques en la pantalla y podría llevar a la instalación de más aplicaciones. Se recomienda a los usuarios que restablezcan sus dispositivos a los ajustes de fábrica para eliminar este malware.

Mirai: aprovechar el poder del Internet de las cosas para provocar una interrupción a gran escala

En nuestra investigación, Mirai sigue de cerca los pasos del malware FluBot, con 156 millones de consultas de DNS procesadas. Conocido por atacar dispositivos de IoT con puertos telnet abiertos, Mirai se hizo famoso por el ataque DDoS contra uno de los mayores proveedores de DNS. Este gusano de autopropagación busca dispositivos vulnerables que utilicen las combinaciones predeterminadas de nombre de usuario y contraseña. En un momento dado, acumuló una tanda de más de 100 000 dispositivos zombis que los atacantes utilizaron en ataques DDoS contra objetivos de alto perfil. En uno de sus ataques anteriores, Mirai utilizó 145 000 dispositivos para atacar a una empresa tecnológica. Este es un ejemplo de cómo los dispositivos no seguros podrían utilizarse como armas para cometer ciberataques y provocar interrupciones a gran escala en las empresas.

En 2016, el grupo detrás de Mirai publicó el código fuente, posiblemente para evitar que las autoridades policiales lo rastrearan hasta dar con los autores originales (y, por lo tanto, evitar la detención). Con esto, otros grupos comenzaron a utilizar el código de Mirai, modificándolo y mejorándolo con más funcionalidades, como la de poder infectar sistemas. Uno de los efectos de publicar el código es que hemos detectado nuevas variantes, como Okiru, Satori, Masuta y PureMasuta, con el fin de lanzar ataques DDoS. Aunque reiniciar el dispositivo infectado ayuda, dado que el malware está constantemente buscando dispositivos, existe una alta probabilidad de que se vuelva a infectar a menos que el usuario cambie sus contraseñas.

Necurs: distribuidor de malware y vendedor de accesos

La botnet Necurs, que se detectó por primera vez en 2012, representó 80 millones de consultas procesadas en los últimos seis meses. Supone un grave riesgo tanto para los particulares como para las organizaciones, gracias a su capacidad para distribuir otras cargas de malware como Dridex, TrickBot y Locky, entre otros. Un factor notable que vale la pena destacar es que esta botnet también vende el acceso a ordenadores infectados a otros grupos como parte de sus ofertas de botnets de alquiler. Al igual que la mayoría de botnets, utiliza un DGA para generar numerosos dominios para sus servidores de C2 y continuar sus operaciones aunque los dominios se bloqueen.

Además de distribuir ransomware y troyanos bancarios, Necurs también se utiliza para distribuir varios ataques de spam, como estafas a través de sitios de citas rusos, estafas farmacéuticas, etc. Durante una investigación, Microsoft supervisó las actividades de esta botnet y descubrió que, en tan solo 58 días, envió aproximadamente 3,8 millones de mensajes de correo electrónico spam. En 2020, las operaciones de la botnet Necurs se vieron interrumpidas por la colaboración de las fuerzas del orden público y la comunidad de la seguridad.

Monerodownloader: botnet de minería

Una de las muchas formas en las que los atacantes obtienen beneficios es utilizando los equipos comprometidos para la criptominería. La creciente popularidad de la criptomoneda Monero entre los ciberdelincuentes es una de las razones por las que estamos detectando botnets creados específicamente para minarla. Los atacantes prefieren esta criptomoneda, ya que la cadena no está tan expuesta y ofrece anonimato; por lo tanto, no se rastrea hasta ellos. Aunque se sabe muy poco acerca de Monerodownloader, algunas de las tácticas que realiza incluyen la recopilación de información y la conexión a servidores de C2 para la carga útil real.

No actualizar los sistemas allana el camino para amenazas como los programas de criptominería de Monero. Otros mineros similares de Monero aprovechan las vulnerabilidades, se presentan como software gratuito para atraer a los usuarios y conseguir que descarguen el minero, y tienen la capacidad de moverse lateralmente a través de la red e infectar otros dispositivos para obtener tantos ingresos como puedan. Aunque la descripción del movimiento lateral es más aplicable a las empresas que a los particulares, esto nos da una idea de cómo funcionan los programas de criptominería para maximizar la infección.

Principales amenazas por región: las botnets siguen prevalenciendo en las redes domésticas

Examinemos más de cerca nuestros datos regionales para dilucidar qué botnets específicas prevalecen por región en función del tráfico de DNS de las redes domésticas, y para analizar algunos factores potenciales que contribuyen a tal tendencia.

Norteamérica

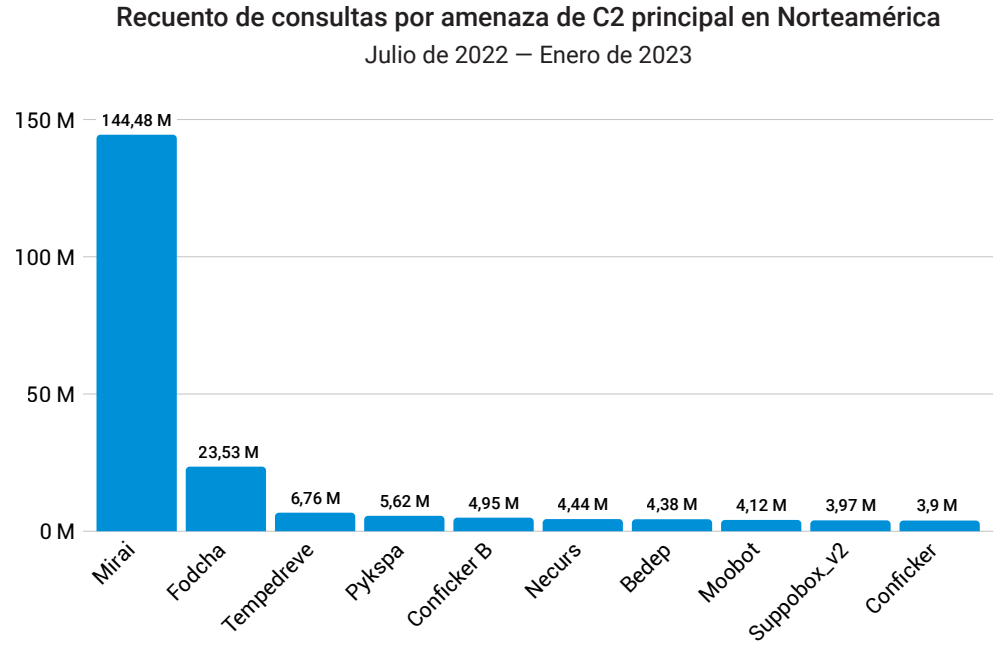


Fig. 15: Mirai sigue causando estragos en Norteamérica, posiblemente debido a la falta de seguridad de los dispositivos IoT

En Norteamérica, se observaron más de 144 millones de consultas asociadas a la botnet Mirai en las redes domésticas (Figura 15). Esta botnet se dirige a los dispositivos vulnerables del IoT que siguen utilizando nombres de usuario y contraseñas predeterminados. El gran volumen de consultas procedentes de esta región podría deberse a la popularidad o al elevado uso de los dispositivos IoT en los hogares. Solo en 2022, según los datos, los hogares estadounidenses tenían un promedio de 22 dispositivos conectados, lo que disminuyó ligeramente con respecto a los 25 del año anterior. Además, con las previsiones de aumento de las conexiones de IoT en Norteamérica (5400 millones de dólares en 2025), existe una alta probabilidad de que se produzcan más amenazas como Mirai o variantes similares que abusen de los dispositivos de IoT no seguros.

Para los usuarios domésticos, el impacto de una amenaza de este tipo es que los ciberdelincuentes pueden explotar sus dispositivos sin su conocimiento para cometer delitos. Sin embargo, las empresas también sufren los efectos de los ataques DDoS, o incluso de las campañas de spam maliciosas, lanzadas por botnets como Mirai. Como práctica recomendada, conviene siempre cambiar el nombre de usuario y la contraseña predeterminados de los dispositivos para protegerlos de Mirai y otros ataques similares.

Europa, Oriente Medio y África

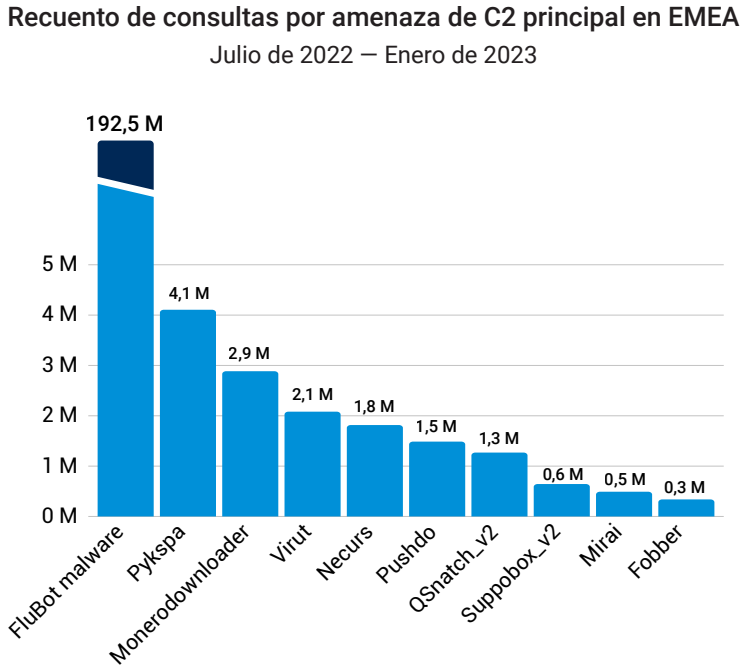


Fig. 16: Detectamos un brote de malware FluBot en la región EMEA debido posiblemente a su táctica de propagación y al uso de varios idiomas europeos como parte de su cebo de ingeniería social

Decir que el malware FluBot se está propagando como un incendio en EMEA sería quedarse corto. El enorme volumen de consultas de DNS registradas en esta región (aproximadamente 193 millones) es notable. Gracias a nuestro análisis del tráfico de DNS, Akamai pudo ver cómo se producían estas infecciones en EMEA (Figura 16). Un factor que contribuye es su táctica de propagación del smishing, una forma de phishing en la que el atacante envía SMS a la lista de contactos de la víctima. Además, engaña a los usuarios para que descarguen una aplicación relacionada con una entrega de paquetes o una aplicación de mensajería de voz que en realidad es el malware. Aparte de esto, FluBot pide permisos adicionales y registra de forma secreta las credenciales bancarias/financieras de los usuarios sin su conocimiento. Según los datos, atacaba a usuarios de España, Alemania, Finlandia y el Reino Unido, entre otros. El SMS también está escrito en varios otros idiomas de la UE, como alemán y húngaro, lo que podría ser uno de los muchos factores que indica que este malware surgió en Europa.

Latinoamérica

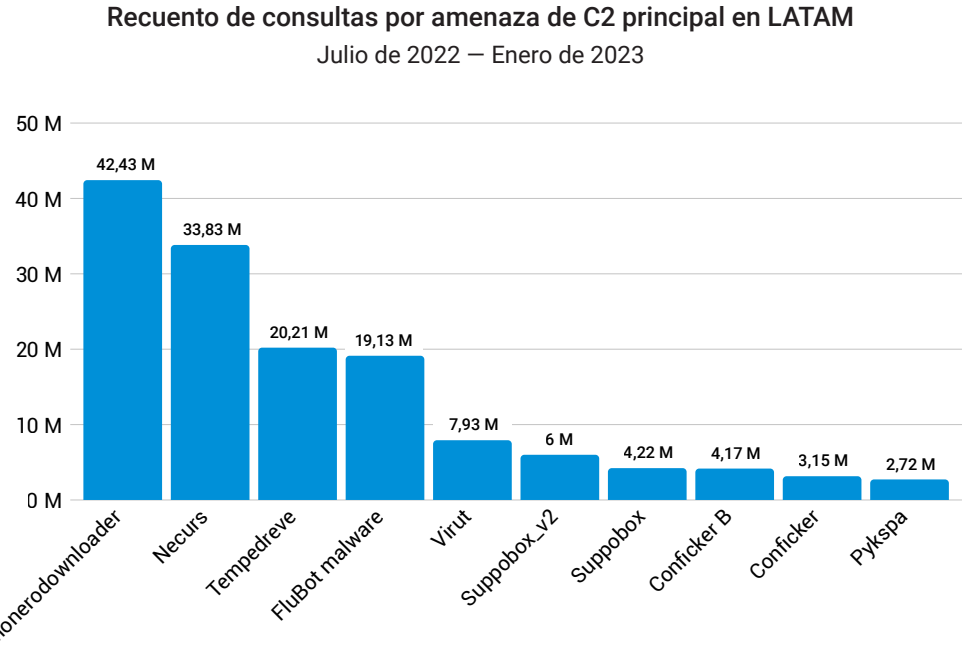


Fig. 17: La botnet de criptominería Monerodownloader se convirtió en la principal amenaza en Latinoamérica, posiblemente debido al elevado uso de criptomonedas en la región

A diferencia de Norteamérica y EMEA, la región de Latinoamérica mostró una distribución más diversa de botnets (Figura 17). Monerodownloader, una botnet de criptominería, lidera la lista de grupos de botnets activos con 42 millones de consultas procesadas, seguido por Necurs (34 millones) y Tempedreve (20 millones). La elevada tasa de adopción de criptomonedas en la región, impulsada por la alta inflación y las remesas, podría explicar por qué botnets como Monerodownloader encabezaron la lista. Sin el conocimiento del usuario, los ciberdelincuentes podrían estar utilizando los recursos de los dispositivos de los usuarios para fines de minería y para su propio beneficio financiero. También cabe destacar que FluBot es una de las principales amenazas detectadas en el tráfico de DNS, lo que muestra la prevalencia de la botnet incluso fuera de la región EMEA, donde observamos un gran volumen de tráfico.

Asia-Pacífico y Japón

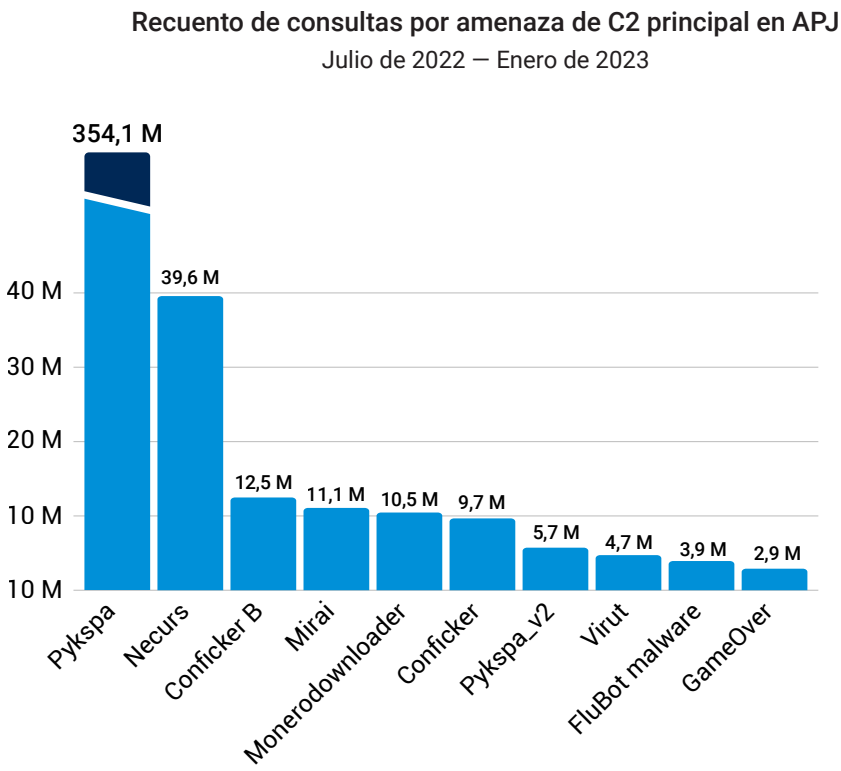


Fig. 18: Las amenazas predominantes en APJ son Pykspa y Necurs

En APJ se observaron más de 350 millones de consultas relacionadas con PykSPA (Figura 18). En una entrada de blog de 2019, señalamos que Pykspa utilizaba un mecanismo selectivo de DGA para permanecer oculto durante un largo período de tiempo. Los dominios destacados en ese informe se encontraban principalmente en Asia oriental. También hemos observado consultas relacionadas con botnets como Necurs, lo que es un claro indicador de que los sistemas están infectados con otros malware.

Descripción general del panorama de phishing

En la última parte de nuestro análisis del tráfico de DNS, examinamos los kits de phishing y su papel crucial en el éxito de las campañas de esta forma de engaño. El phishing sigue siendo relevante, más que nunca, debido a las tácticas en constante evolución que utilizan los adversarios y a la creciente cantidad de información personal disponible en línea. Los adversarios utilizan la ingeniería social para hacer que sus intentos de phishing parezcan legítimos, y las pruebas indican que el índice de éxito de estos ataques sigue siendo alto. La investigación de Akamai sobre las estafas de phishing navideñas reveló nuevas técnicas y tácticas utilizadas por los adversarios para seguir permaneciendo ocultos. Estas tácticas novedosas incluyen el uso de testimonios de usuarios falsos como parte de la estafa y la técnica recién descubierta de utilizar el anclaje HTML para asegurarse de que solo los usuarios válidos lleguen a los sitios web de la estafa.

El aumento del teletrabajo debido a la pandemia de la COVID-19 también ha dificultado la detección y prevención de ataques de phishing, lo que ha recalcado la importancia de que los usuarios y las organizaciones permanezcan atentos y tomen medidas para protegerse. Además, el aumento del uso de las redes sociales y el creciente número de dispositivos conectados a Internet han creado más oportunidades para los adversarios.

Las campañas de phishing afectan a los servicios financieros

Al investigar las marcas por las que se hacen pasar los estafadores que usan métodos de phishing, hay varias maneras posibles de recopilar los datos. Comparamos el número total de campañas con el número de víctimas. Esto nos permite evaluar la tasa de éxito de una campaña determinada, y también nos permite ver qué porcentaje de cada sector está siendo el objetivo de ataques.

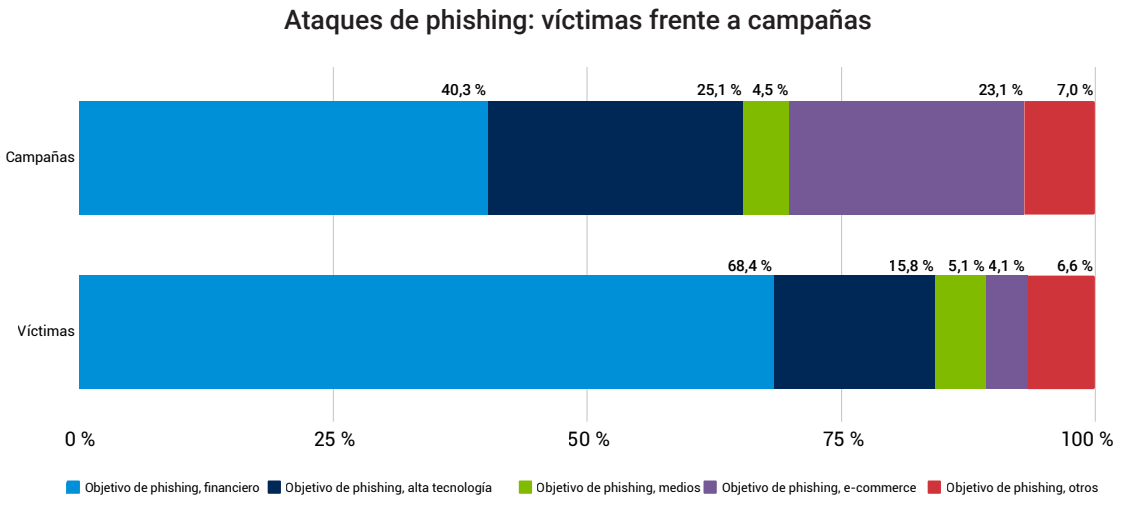


Fig. 19: La mayoría de las campañas de phishing se dirigió al sector de los servicios financieros (T4 2022)

En nuestra investigación se descubrió que las marcas financieras y de alta tecnología lideraron tanto en el número de campañas como de víctimas (Figura 19). Observamos que el 40,3 % de las campañas iban destinadas a clientes de servicios financieros, y en ellas se alcanzó a un 68,4 % de las víctimas; esto indica que los ataques contra los servicios financieros fueron muy eficaces en el cuatro trimestre de 2022. En nuestro informe de servicios financieros, Enemigo a las puertas: Análisis de los ataques a las empresas de servicios financieros, destacamos cómo los ataques de phishing tienen motivaciones económicas y se dirigen principalmente a los servicios financieros y a sus clientes. Los posibles efectos de dichos ataques incluyen daños a la marca y a la reputación, así como la pérdida de confianza de los clientes. El phishing también podría requerir el uso de recursos de la organización para solucionar el problema.

El comercio electrónico atrajo el 23 % de las campañas de phishing en el cuarto trimestre de 2022. Aunque hemos detectado más campañas que víctimas reales, también vale la pena señalar que los atacantes se dirigen a este sector y que los usuarios deben permanecer atentos, ya que los ciberdelincuentes pueden perseguir su información personal o bancaria.

Kits de herramientas de phishing: facilitadores de estafas de phishing

La sorprendente magnitud y escala del panorama del phishing están motivadas, en gran parte, por la existencia de kits de herramientas que posibilitan la implementación y el mantenimiento de sitios web de phishing y que permiten, incluso a los estafadores sin conocimientos técnicos, unirse a este ecosistema de de adversarios y cometer estafas.

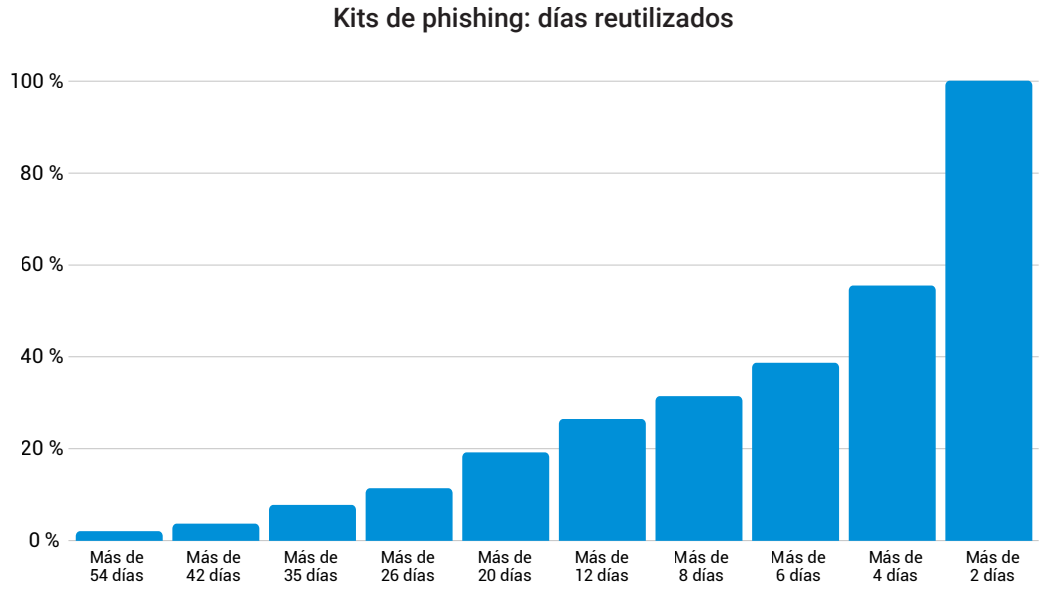


Fig. 20: Kits de herramientas de phishing por número de días reutilizados (T4 2022)

Según nuestra investigación, en la que se realizó un seguimiento de más de 300 kits de herramientas de phishing diferentes que estaban en circulación para lanzar nuevas campañas de ataque, el 2,04 % de los kits rastreados se reutilizaron en al menos 54 días distintos en el cuarto trimestre de 2022 (Figura 20). Además, el 55,5 % de los kits se reutilizaron para lanzar una nueva campaña de ataque durante al menos cuatro días, y el 100 % de los kits rastreados se reutilizaron en no menos de dos días distintos durante el cuarto trimestre de 2022.

Conclusión y recomendaciones: combatir los ataques modernos con medidas proactivas

Ahora que hemos tratado los grupos de amenazas y las metodologías de los atacantes, hablemos sobre cómo aprovechar toda esa información. Comenzaremos con cómo gestionar el DNS, internamente o mediante la externalización a un tercero. Para las organizaciones más grandes o complejas, tiene sentido que un proveedor especializado en la gestión de DNS se encargue de este asunto. En cualquier caso, asegúrese de supervisar el rendimiento y las protecciones de su DNS. A continuación, considere los diferentes controles que necesitará. La protección contra DDoS, ataques de malware y scraping, el movimiento lateral y la exfiltración son las áreas clave en que se debe centrar. Siguiendo este proceso de datos y buscando todas las vulnerabilidades críticas que pueden frenarse en cada paso, se encuentra un modelo de ciberseguridad que a menudo se conoce como "cadena de exterminio de la ciberseguridad".

Considere la posibilidad de crear guías de las técnicas de ataque tratadas en este informe. Consulte a su equipo de pentest o a su equipo de red para determinar si utilizan las mismas herramientas y técnicas que los IAB, como Qakbot y Emotet, los bots, como QSnatch, el ransomware, como LockBit (en un entorno de laboratorio), y herramientas como Cobalt Strike. Es importante asegurarse de que los controles de seguridad alertan y detienen estos tipos de ataques de forma eficaz, y de que sus equipos están capacitados para hacerles frente.

Si se detecta Cobalt Strike en la red, es recomendable crear inmediatamente un informe de incidentes e investigarlo. Aunque su equipo rojo podría utilizar la herramienta (en cuyo caso, debe investigarse y notificarse de todos modos), la presencia de dicho tráfico debería hacer saltar las alarmas, ya que esto podría indicar una intrusión por parte de otros grupos RaaS o atacantes, y señalar un ataque en curso que aún podría mitigarse.

Piense en cómo funciona su centro de operaciones de seguridad y determine cómo está realizando el seguimiento de procesos (como bits, Wget, or cURL) que podrían indicar la probabilidad de que una amenaza relacionada con IAB está en la red llevando a cabo un reconocimiento. Lo más importante es averiguar qué se ha descargado e interrumpir la descarga si aún está en curso. A continuación, investigue qué desencadenó el IAB: ¿se trataba de un archivo LNK, una macro o un VScript? y descubra a partir de ahí cómo comenzó la filtración.

Manténgase conectado a nuestra investigación más reciente visitando nuestro Centro de investigación sobre seguridad.

Metodologías

Tráfico de ataque de comando y control

Los datos de este informe los genera nuestro producto Secure Internet Access (SIA) y describe el tráfico de ataque de comando y control (C2). SIA es una puerta de enlace web basada en la nube diseñada para ayudar a los usuarios a conectar fácilmente sus dispositivos a Internet de forma segura. Los dos conjuntos diferentes de datos utilizados en este informe reflejan por separado los datos de alertas de seguridad de organizaciones empresariales con grandes cantidades de usuarios o proveedores de Internet con usuarios particulares. Estos datos se midieron por el número de dispositivos afectados y el número de consultas, respectivamente. Un dispositivo afectado se definió como un dispositivo que llegó a un dominio de C2 conocido e identificado al menos una vez. De forma similar, una consulta de C2 se definió como una consulta que llegó a un dominio de C2 conocido e identificado. Nuestros equipos de seguridad utilizan estos datos de forma interna para investigar ataques, detectar comportamientos maliciosos para notificar a los clientes y proporcionar información adicional a las soluciones de seguridad de Akamai.

Créditos

Editorial y redacción

Or Katz

Eliad Kimhy

Badette Tribbey

Revisión y expertos en la materia

Tanya Belousov

Shiran Guez

Ophir Harpaz

Stiv Kupchik

Grace Wang

Steve Winterfeld

Análisis de datos

Ronan Ballantine

Gal Kochner

Chelsea Tuttle

Marketing y publicación

Georgina Morales Hampe

Shivangi Sahu

Más información acerca de Estado de Internet / Seguridad

Lea números anteriores del aclamado informe sobre el estado de Internet en materia de seguridad de Akamai e infórmese de cuándo se publican los siguientes números. akamai.com/soti

Más información acerca de la investigación de Akamai sobre amenazas

Conozca los últimos análisis de inteligencia frente a amenazas, informes de seguridad e investigación sobre ciberseguridad. akamai.com/security-research

Acceda a los datos de este informe

Vea versiones de alta calidad de los gráficos a los que se hace referencia en este informe. Puede usar estas imágenes y hacer referencia a ellas libremente, siempre que se cite debidamente a Akamai como fuente y que se conserve el logotipo de Akamai. akamai.com/sotidata

Más información sobre las soluciones de Akamai

Para obtener más información sobre las soluciones de Akamai para las amenazas dirigidas a empresas, visite nuestra página de Secure Internet Access Enterprise. Los proveedores de servicios que se centran en los mercados de consumidores y pymes pueden visitar Servicios Secure Internet Access para ISP.

Akamai potencia y protege la vida online. Las empresas líderes de todo el mundo eligen Akamai para crear, proteger y ofrecer sus experiencias digitales, ayudando así a millones de personas a vivir, trabajar y jugar cada día. Akamai Connected Cloud, plataforma de nube distribuida de forma masiva en el Edge, acerca las aplicaciones y las experiencias a los usuarios mientras mantiene las amenazas a raya. Para obtener más información acerca de las soluciones de cloud computing, seguridad y distribución de contenido de Akamai, visite akamai.com y akamai.com/blog, o siga a Akamai Technologies en Twitter y LinkedIn. Publicado en 03/23