Estado de los ataques encriptados en 2020

El equipo de investigación de Zscaler™ ThreatLabZ comparte algunas claves acerca de cómo los atacantes están acelerando el uso de la encriptación SSL/TLS para eludir los métodos de defensa tradicionales

ENERO – SEPTIEMBRE DE 2020

Índice

INTRODUCCIÓN ____ 3

PARTE 1: Las tendencias del tráfico SSL ____ 6

PARTE 2: Los ataques son cada vez más avanzados ____ 8

PARTE 3: El análisis de la cadena de ataque ____ 11

PARTE 4: Lo que se necesita para prevenir las amenazas encriptadas ____ 19

Acerca de ThreatLabZ

ThreatLabZ es el equipo de investigación de seguridad mundial de Zscaler. Además de proteger a los clientes de Zscaler de las amenazas emergentes, el equipo analiza el tráfico empresarial que cruza la nube de Zscaler. Gracias a la experiencia del equipo en ciberseguridad, ciencia de datos y aprendizaje automático/IA, combinada con el volumen de datos analizados a partir de más de 120 mil millones de transacciones diarias en la plataforma en la nube Zero Trust Exchange™ de Zscaler, ThreatLabZ se encuentra en una posición única para proporcionar información sobre las tendencias del tráfico y seguridad empresariales.

Cuando ThreatLabZ descubre una nueva campaña de ataque o malware con técnicas o capacidades poco comunes, los investigadores detonan estos archivos y analizan su código para ver exactamente cómo están programados para evadir la detección, dejar cargas dañinas, robar información, controlar dispositivos, espiar al usuario, propagarse y dispersarse. Facilitamos los resultados de nuestros análisis libremente a la comunidad de seguridad en el **blog de investigación de Zscaler**.

En cuanto a las tendencias del SSL, los investigadores de ThreatLabZ recientemente descubrieron, analizaron e informaron sobre amenazas que aprovechaban los canales encriptados. Puede leer sobre esto en las siguientes publicaciones:

> **Sitios VPN falsos suministran infostealers**

> **Uso de la herramienta StackBlitz para alojar páginas de phishing**

> **Skimmers a través de JavaScript**

> **La amenaza persistente avanzada de Higaisa**

Para ver la nube de Zscaler en funcionamiento, vea el **Tablero de actividad de la nube**.
Este muestra el número de transacciones que se procesan y de amenazas que se bloquean cada segundo.

El tráfico SSL oculta malware. Mucho.

Para irritación de los expertos en seguridad, hay una creencia acerca del cifrado SSL que es tan persistente como equivocada: “Pensé que, siempre que un sitio web utilizase el cifrado SSL, sería seguro."

El cifrado SSL se diseñó para proteger el tráfico de los ojos curiosos, pero los adversarios también lo han aprovechado para ocultar los ataques, convirtiendo el uso del cifrado en una amenaza potencial si no tiene la inspección adecuada.

Los cibercriminales saben lo mismo que los expertos en seguridad: el cifrado SSL/TLS es la forma estándar del sector de proteger los datos en tránsito. Esos mismos ciberdelincuentes utilizan los métodos de encriptación estándar del sector e idean formas inteligentes de ocultar el malware dentro del tráfico encriptado para llevar a cabo ataques que evitan la detección. De hecho, entre enero y septiembre, la nube Zscaler bloqueó la asombrosa cantidad de 6600 millones de amenazas a la seguridad ocultas en el interior de tráfico encriptado, lo que equivale a un promedio de 733 millones bloqueados por mes. Este promedio mensual supone un aumento de casi el 260 por ciento con respecto a 2019, cuando la nube de Zscaler bloqueaba una media de 283 millones de amenazas por mes en el tráfico cifrado.

La inspección del tráfico cifrado debe ser un componente clave de las defensas de seguridad de cada organización. El problema es que las herramientas de seguridad tradicionales en las instalaciones, como los cortafuegos de última generación, tienen dificultades para proporcionar el rendimiento y la capacidad necesarios para descifrar, inspeccionar y volver a cifrar el tráfico de manera eficaz. El intento de inspeccionar todo el tráfico SSL llevaría el rendimiento (y la productividad) a un punto muerto, por lo que muchas organizaciones permiten que al menos parte de su tráfico cifrado pase sin ser inspeccionado, como el tráfico de los proveedores de servicios en la nube y otros considerados de "confianza". Esta es una deficiencia grave. El hecho de no inspeccionar todo el tráfico cifrado hace a las organizaciones vulnerables a los ataques ocultos de phishing, malware y otros, lo cual podría ser desastroso.

Entre enero y septiembre, la **nube de Zscaler identificó y detuvo 6600 millones de amenazas** ocultas en tráfico cifrado.

El equipo de ThreatLabZ analizó el tráfico cifrado en la nube de Zscaler durante los primeros nueve meses de 2020, y evaluó su uso en sectores específicos. El objetivo del análisis no es solo comprender el volumen de tráfico que utiliza cifrado, sino también las amenazas ocultas dentro de ese tráfico. Algunos de los aspectos más destacados incluyen:

- **La mayoría del tráfico de Internet está cifrado:** el 80 % de todo el tráfico utiliza el cifrado SSL/TLS de forma predeterminada.
- **El crecimiento espectacular en el volumen:** hubo un aumento del 260 % en las amenazas basadas en SSL en los últimos nueve meses, acelerado por el aumento de las aplicaciones de colaboración basadas en la nube durante la COVID-19.
- **Los ataques a la asistencia sanitaria:** la asistencia sanitaria fue el sector que sufrió más ataques, con 1600 millones de amenazas cifradas identificadas y detenidas, seguida del sector financiero y del industrial.
- **El aumento del abuso de los servicios de uso compartido de archivos basados en la nube:** más del 30 % de los ataques basados en SSL se ocultan en servicios de colaboración como Google Drive, OneDrive, AWS o Dropbox.
- **El aumento del ransomware oculto:** el ransomware introducido a través del tráfico web cifrado se ha multiplicado por más de cinco.

Los cibercriminales también utilizan SSL/TLS: ¿Por qué es importante inspeccionar el tráfico cifrado?

Cifrar el tráfico de Internet a través de SSL (Secure Sockets Layer) y de su versión más moderna, TLS (Transport Layer Security), es la norma internacional para proteger los datos en tránsito. La gran mayoría del tráfico de Internet actual está cifrado.[1] El problema es que los delincuentes también utilizan el cifrado para ocultar malware y otras vulnerabilidades. Esto significa que el tráfico que pasa a través de canales cifrados ya no puede ser de confianza simplemente por disponer de un certificado digital.

Los ciberdelincuentes han creado cadenas de ataque sofisticadas que empiezan con un correo electrónico de phishing de aspecto inocente que contiene una vulnerabilidad o malware oculto. Si un usuario desprevenido hace clic, el ataque pasa a la fase de instalación de malware y, por último, a la exfiltración de datos corporativos de valor.

Lo que hace que los ataques sean tan nefastos es que la vulnerabilidad o el malware oculto también están cifrados, lo que cambia completamente su estructura de archivos. Los sistemas de ciberseguridad dependen de la estructura (o "huella dactilar") de un archivo para identificar las amenazas entrantes; si está estructurado de cierta manera, el sistema sabe bloquearlo. Pero cada vez que se cifra un archivo, recibe una nueva huella digital que no se reconoce como una amenaza.

La inspección SSL es la única forma eficaz de bloquear los archivos maliciosos

que se entregan [usando estos servicios], ya que los motores de seguridad no pueden bloquear lo que no pueden ver.

[1] https://transparencyreport.google.com/https/overview?hl=en

Tendencias del tráfico SSL

Las empresas han aceptado en gran medida el hecho de que la encriptación es un requisito para proteger los datos en tránsito de la interceptación y la explotación. En nuestro análisis, descubrimos que el sector educativo era el que cifraba más tráfico, seguido del industrial, el financiero y el de la asistencia sanitaria. No obstante, todos los sectores, incluidos el de la venta al por menor y al por mayor, servicios, tecnología y comunicación y gobierno tienen niveles muy similares. Durante el período de análisis, entre enero y septiembre de 2020, observamos un volumen de uso del cifrado en todos los sectores de en torno al 75 por ciento y con picos de más del 80 por ciento.

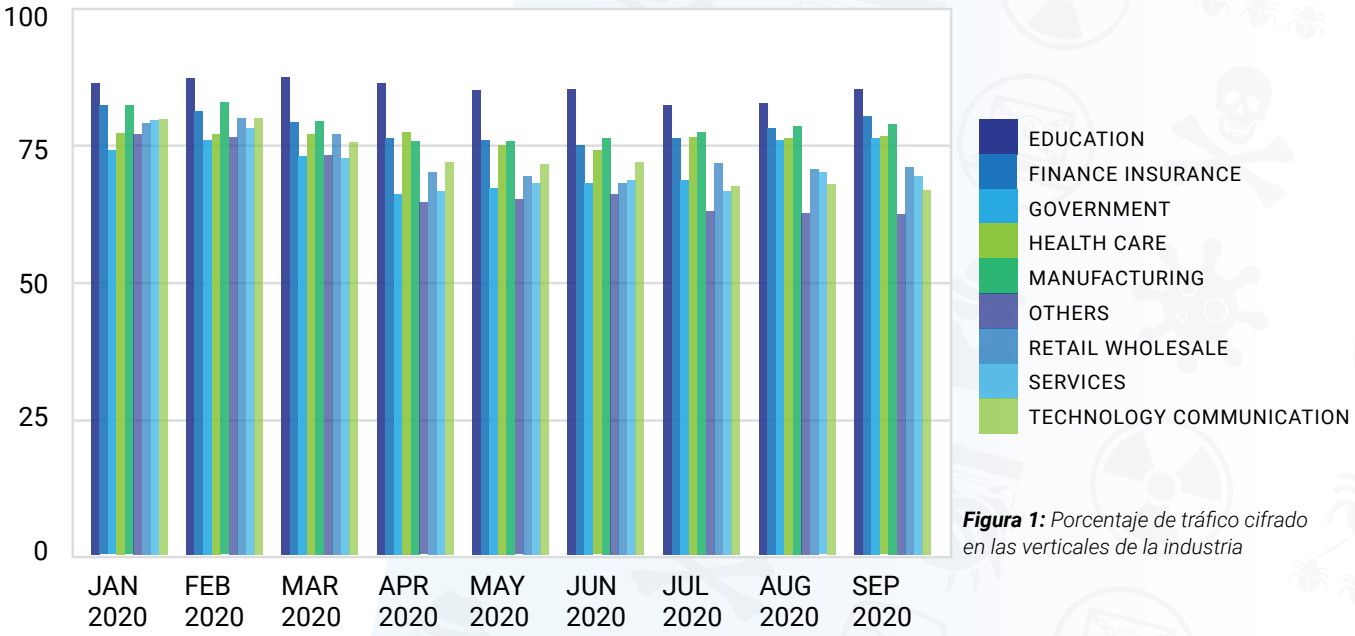


Figura 1: *Porcentaje de tráfico cifrado en las verticales de la industria*

Se observaron altas tasas de tráfico cifrado en todos los sectores verticales, lo que significa que todas las organizaciones deben considerar cómo inspeccionar el tráfico SSL/TLS en busca de amenazas.

Según nuestra investigación, los actores de la amenaza se dirigen a la asistencia sanitaria con ataques de malware cifrado más que a cualquier otro sector. Entre enero y septiembre de 2020, el sector sanitario representó el 25,5 por ciento de todas las amenazas avanzadas bloqueadas en canales cifrados en la nube de Zscaler, seguido por el de las finanzas/seguros con el 18,3 por ciento, el industrial, con el 17,4 por ciento y el gubernamental, con el 14,3 por ciento.

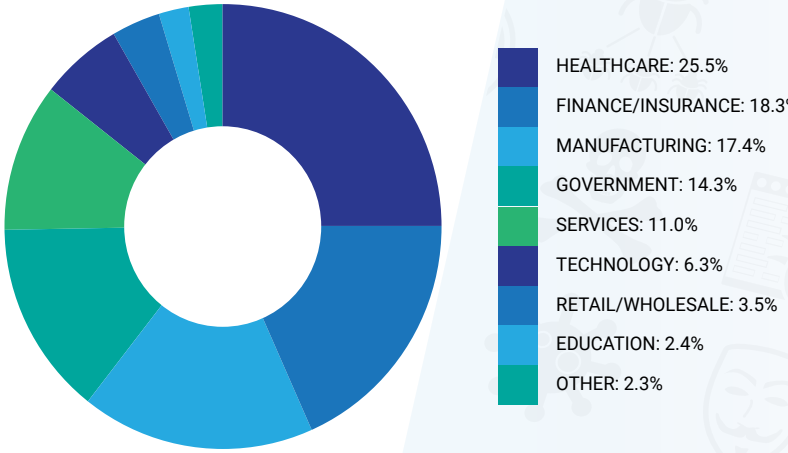


Figura 2: *Amenazas avanzadas bloqueadas en canales cifrados por sector*

Las empresas de asistencia sanitaria fueron el blanco de la mayor parte de las amenazas enviadas por canales cifrados, a pesar de que la pandemia mundial hizo que sus servicios fueran más fundamentales que nunca.

Los atacantes también han utilizado la pandemia para lanzar nuevas campañas, con sitios falsos que ofrecen noticias, productos y curas. En los primeros tres meses de 2020, ThreatLabZ informó de un aumento del **30 000 por ciento** en las amenazas relacionadas con la COVID-19.

Con más detalle: el sector de la asistencia sanitaria

El sector de la asistencia sanitaria fue el objetivo de más de 1690 mil millones de intentos de ataques en canales cifrados durante nuestro análisis, más que cualquier otro sector. La gran mayoría de los ataques en este sector se produjeron a través de URL maliciosas (84,2 por ciento). Las URL maliciosas se pueden enviar a los usuarios por correo electrónico, mensaje de texto, mensajes emergentes o anuncios en la página, lo que conduce a descargar malware, spyware o ransomware, cuentas comprometidas y mucho más.

El sector de la asistencia sanitaria suele ser el objetivo de los ciberataques debido a la presencia de sistemas heredados (que ha seguido aprobando la FDA) en el entorno. Estos sistemas heredados carecen de controles de seguridad y suelen ser vulnerables a problemas conocidos. Sin unos controles unificados y una aplicación centralizada de políticas y visibilidad, dichas organizaciones terminan teniendo brechas en sus controles de seguridad que los cibercriminales intentan aprovechar.

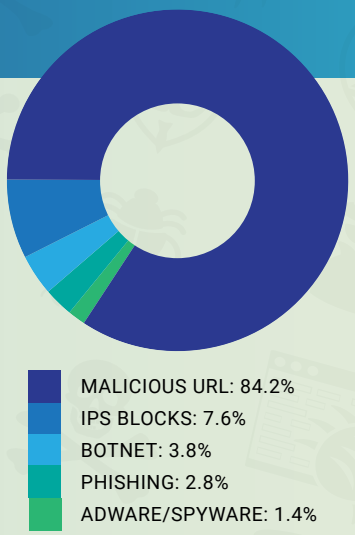


Figura 3: *Amenazas en canales encriptados dirigidas al sector de la asistencia sanitaria*

Los ataques son cada vez más avanzados

Los profesionales de la informática suelen advertir a los usuarios que busquen minuciosamente en la URL de un sitio web que sospechen que sea falso posibles errores, faltas de ortografía u otros indicadores de que quizá no sea legítimo. Pero actualmente, los ciberdelincuentes se aprovechan de técnicas como la ocupación ilegal de dominios y los ataques de IDN homógrafo para hacer que sus sitios sean prácticamente indistinguibles de los reales.

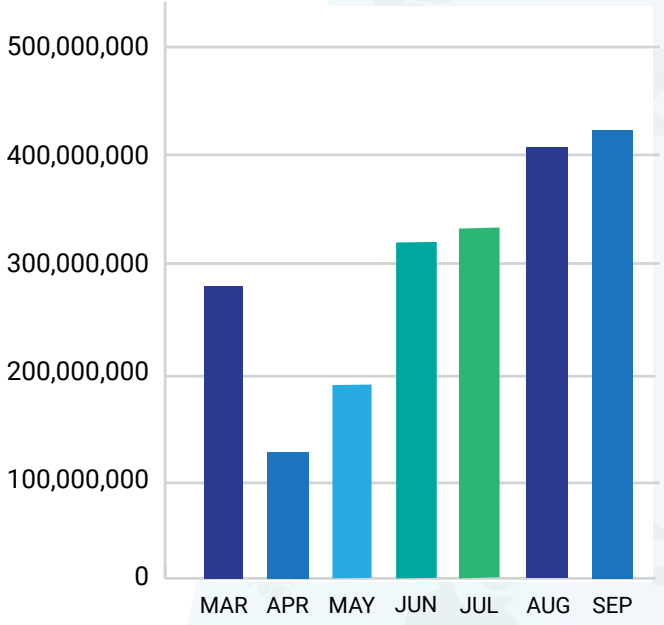
La ciberocupación de dominios consiste en registrar un dominio de nivel superior que es similar a una marca conocida (como gmali.com) para fines de phishing, robo de credenciales o entrega de malware.

Un ataque homógrafo, como una ciberocupación de dominio, se utiliza para engañar a las personas para que hagan clic en los enlaces. Para ello, se utilizan caracteres como el número "1" en lugar de una "l" en la URL de Apple (https://www.app1e.com).

Abuso de los servicios de almacenamiento en la nube

Los servicios de almacenamiento en la nube han surgido como un medio popular de ataque. Estos servicios son excelentes para compartir archivos de forma segura a través de una transmisión basada en SSL en la web. Pero dado que los ciberdelincuentes saben que la mayor parte de las empresas son incapaces de inspeccionar el tráfico SSL a escala y que los servicios en la nube son generalmente "confiables", lanzan ataques que parecen originarse en estos servicios.

Desde marzo hasta septiembre de 2020, la nube de Zscaler bloqueó **dos mil millones de amenazas** en el tráfico cifrado, la mayoría de las cuales implicaba contenido malicioso alojado en Google, AWS, Dropbox y OneDrive. Estas amenazas casi se duplicaron entre marzo y septiembre y representaron cerca del 30 por ciento de todas las amenazas cifradas SSL/TLS en esos meses.



De marzo a septiembre, la nube de Zscaler bloqueó **dos mil millones de amenazas** en el tráfico SSL originado por proveedores de servicios de almacenamiento en la nube.

Figura 4: *Amenazas avanzadas bloqueadas en TLS/SSL de los principales servicios de almacenamiento en la nube*

La Figura 5 muestra cómo se explotan los servicios en la nube para alojar y entregar malware. Los ciberdelincuentes suben la carga dañina de malware (que suele ser un archivo de descarga de fase 1) en uno o más servicios y distribuyen las URL como parte de una campaña de correo electrónico no deseado. El uso de servicios líderes, como Google, Microsoft, Amazon y Dropbox, mejora las posibilidades de que los usuarios finales hagan clic en el vínculo.

Los ciberdelincuentes también se aprovechan de los certificados SSL comodín de estos proveedores de servicios. Asumir que el tráfico de los proveedores en la nube es seguro y que no se inspecciona ayuda a los malhechores a entregar cargas dañinas de malware a través de canales cifrados y a evadir las soluciones de seguridad basadas en el filtrado de URL, como el antispam, la protección del correo electrónico o los cortafuegos, entre otros. **Un correo electrónico de phishing con un enlace a un archivo malicioso alojado en un servicio de confianza basado en la nube puede evadir las soluciones de seguridad tradicionales del correo electrónico.**

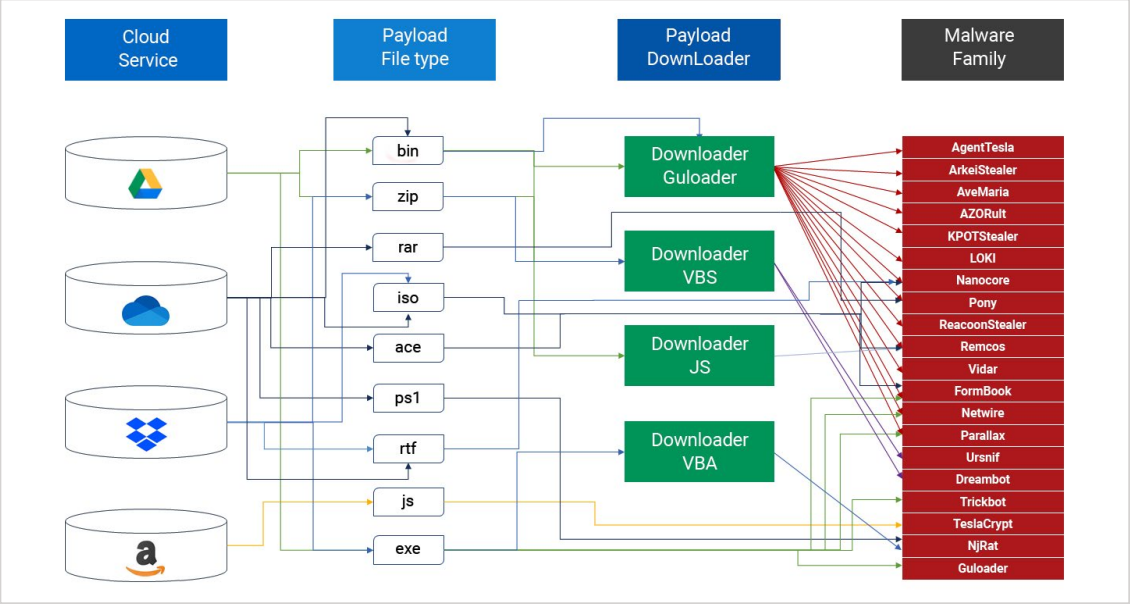


Figura 5: *Cargas de dañinas de malware entregadas a través de servicios en la nube*

El siguiente ejemplo muestra varias URL del servicio de almacenamiento en la nube OneDrive. En este ejemplo, las dos primeras URL son maliciosas y dan lugar a la descarga de malware perteneciente a las familias "Trojan EdLoader" y "Backdoor LokiBot". Sin embargo, la tercera URL es legítima y descarga el archivo real del usuario. El subdominio y el Identificador Uniforme de Recursos (URI) aparecen como patrones de cadenas aleatorias que hacen imposible distinguir los URL legítimos de los maliciosos. La inspección SSL es la única forma eficaz de bloquear los archivos maliciosos que se entregan [al usar estos servicios], ya que los motores de seguridad no pueden bloquear lo que no pueden ver.

Figura 6: *Cadenas aleatorias en los subdominios que hacen imposible distinguir las URL maliciosas de las legítimas*

Ataques móviles

Los smartphones también se han convertido en objetivos populares. De la misma manera que los ciberdelincuentes falsifican páginas web, crean aplicaciones falsas que parecen legítimas. Por ejemplo, un troyano bancario Android llamado Cerberus utiliza un nombre e icono de aplicación que imitan a una aplicación legítima de Google Play. Cuando un usuario desprevenido hace clic en la aplicación falsa, esta envía una notificación para obtener el permiso de "servicio de accesibilidad". (El servicio de accesibilidad asiste a los usuarios con discapacidades en el uso de los dispositivos Android y sus aplicaciones).

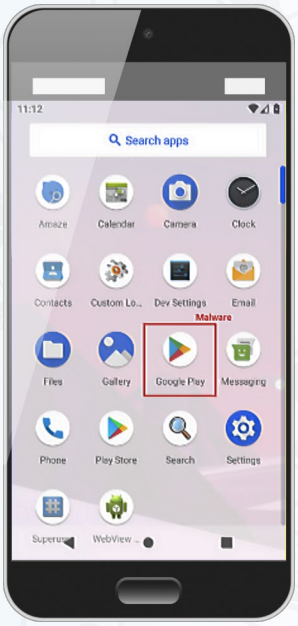


Figura 7: *Aplicación falsa de Google Play*

Esta vulnerabilidad supone que muchos usuarios "acepten" una notificación sin leerla detenidamente. En este caso, al hacer clic en "permitir", la aplicación puede ver el contenido de otras aplicaciones que se muestran en la pantalla y llevar a cabo acciones sin que lo sepa el usuario.

El malware toma las credenciales de las aplicaciones bancarias, de Gmail o de la aplicación de autenticación de dos factores Google Authenticator y, luego, las exfiltra. También puede llevar a cabo otras acciones maliciosas, como grabar el audio de forma sigilosa y robar mensajes de texto. Pero la situación puede empeorar aún más. Una vez concedido el permiso de servicio de accesibilidad al malware, puede impedir que el usuario deshabilite el permiso y puede dificultar la desinstalación de la aplicación.

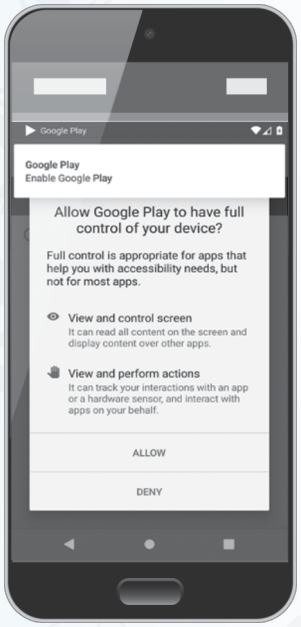
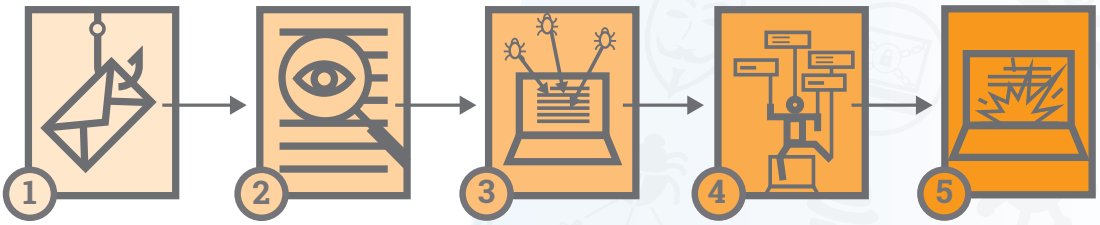


Figura 8: *Notificación sobre una aplicación falsa de Google Play*

Anatomía de un ataque



La entrega puede incluir un correo electrónico de phishing con una vulnerabilidad o malware oculto en el interior. El malware se entrega cuando un usuario lo descarga o hace clic en un enlace del correo electrónico.

La explotación es lo que ocurre cuando el programa busca vulnerabilidades en el sistema que puede explotar y ejecutar el código.

La instalación se produce cuando el malware se carga en el dispositivo de la víctima.

La llamada de comando y control (C&C) consiste en que el malware intenta comunicarse con los servidores C&C para obtener instrucciones o para enviar datos robados.

La detonación consiste en que el malware puede instalar malware adicional, exfiltrar datos o realizar otras acciones programadas por el servidor C&C.

Análisis de la cadena de ataque

Phishing

Dado que el phishing suele ser la primera etapa de los ciberataques de varias etapas que involucran el robo de credenciales, analizamos los más de **193 millones de intentos de phishing** entregados a través de canales cifrados pero identificados y bloqueados por la nube de Zscaler entre enero y septiembre de 2020. Desglosamos los intentos por verticales de la industria. El sector de la industria, que dispone de instalaciones individuales que, a menudo, utilizan diferentes infraestructuras y sistemas de TI (lo que los hace potencialmente más vulnerables), fue el objetivo más destacado, ya que tiene un 38,6 por ciento de los intentos de phishing, seguido del sector de los servicios, con un 13,8 por ciento.

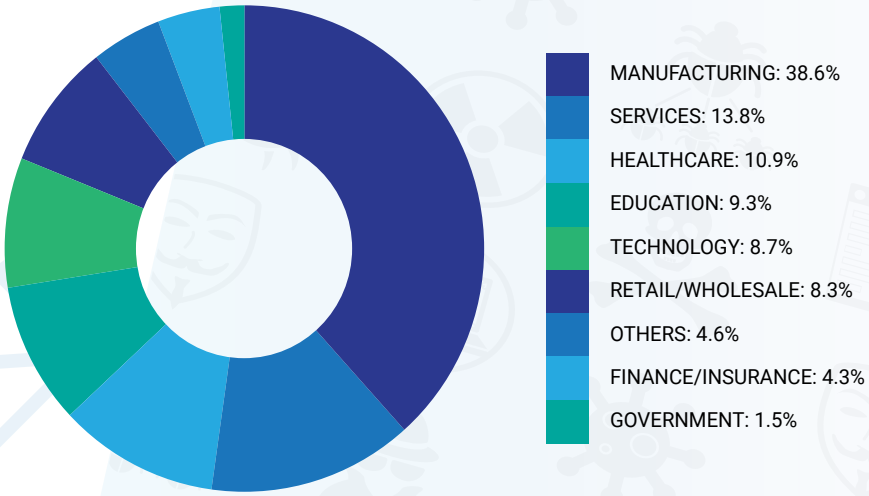


Figura 9: *Amenazas de phishing bloqueadas en canales encriptados, por sector*

Servicios corporativos y marcas que sufrían de phishing

Frecuentemente, en un intento de phishing, un sitio web fraudulento imita a una marca específica. En otras palabras, al usuario le llega un correo electrónico en el que se le indica que haga clic en un enlace que le lleva a un sitio web falso. En este sitio, al usuario se le pide que introduzca un nombre de usuario, una contraseña u otros datos importantes que puedan ser utilizados por los ciberdelincuentes para llevar a cabo los ataques.

Nuestra investigación reveló que la marca más utilizada en ataques de phishing era Microsoft. Los ataques incluyen varios productos web de Microsoft (Office 365, SharePoint, OneDrive, etc.) con los que los ciberdelincuentes intentan robar las credenciales de los servicios corporativos. Los segundos ataques de phishing más populares fueron las estafas de “Soporte Técnico", que generalmente utilizan un redireccionamiento web malicioso de sitios web comprometidos que afirman que el equipo del usuario ha sido pirateado y que “Soporte de Microsoft" lo arreglará (una vez que el usuario ha enviado la información de la tarjeta de crédito).

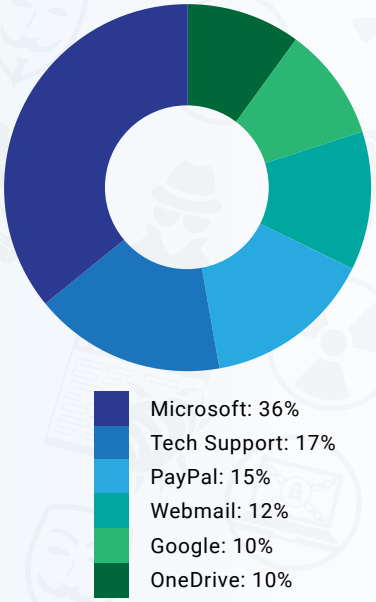


Figura 10: *Marcas y servicios corporativos con los que se hace phishing con mayor frecuencia*

PayPal y Google también se encontraban entre las principales marcas suplantadas por estos ataques de phishing.
Los sitios falsos parecen muy similares a los sitios reales, lo que dificulta la detección de la falsificación.

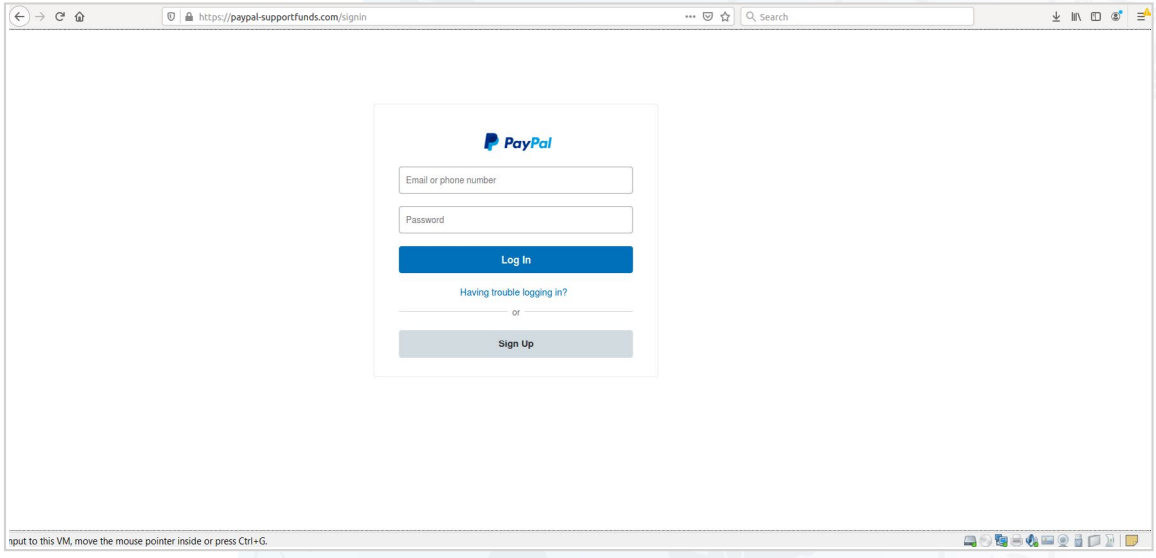


Figura 11: *Sitio de phishing de PayPal a través de HTTPS*

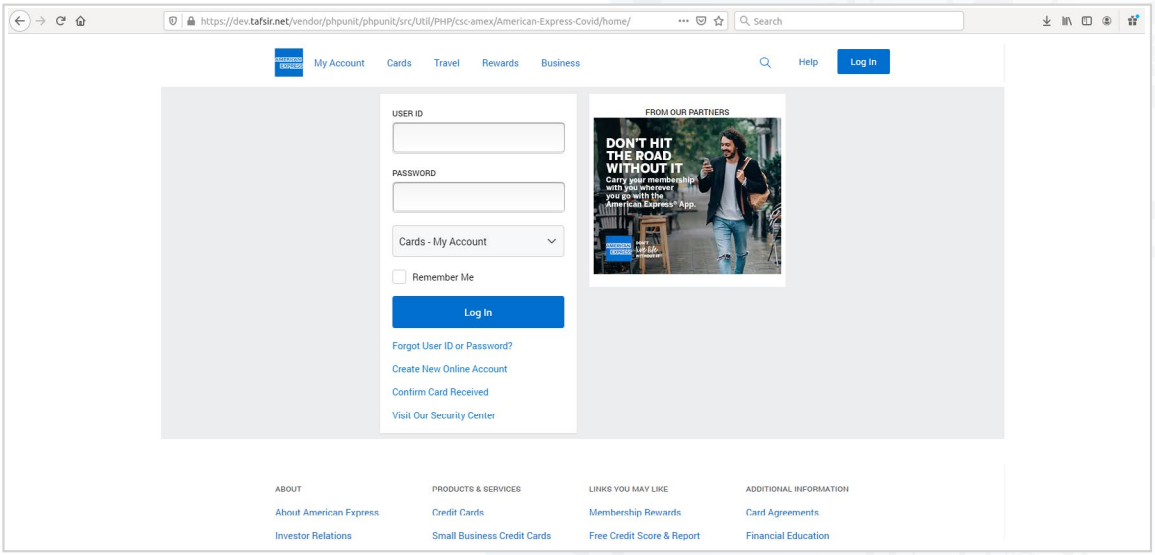


Figura 12: *Sitio de phishing de American Express a través de HTTPS*

Phishing de Netflix a través de HTTPS

El uso de los servicios de entretenimiento en línea, como Netflix, ha aumentado durante la pandemia y los ciberatacantes se han dado cuenta. Los malhechores utilizan los servicios de streaming para falsificar las credenciales de usuario. Y, tal y como se ve en la Figura 13, es difícil distinguir estas páginas falsas de las reales.

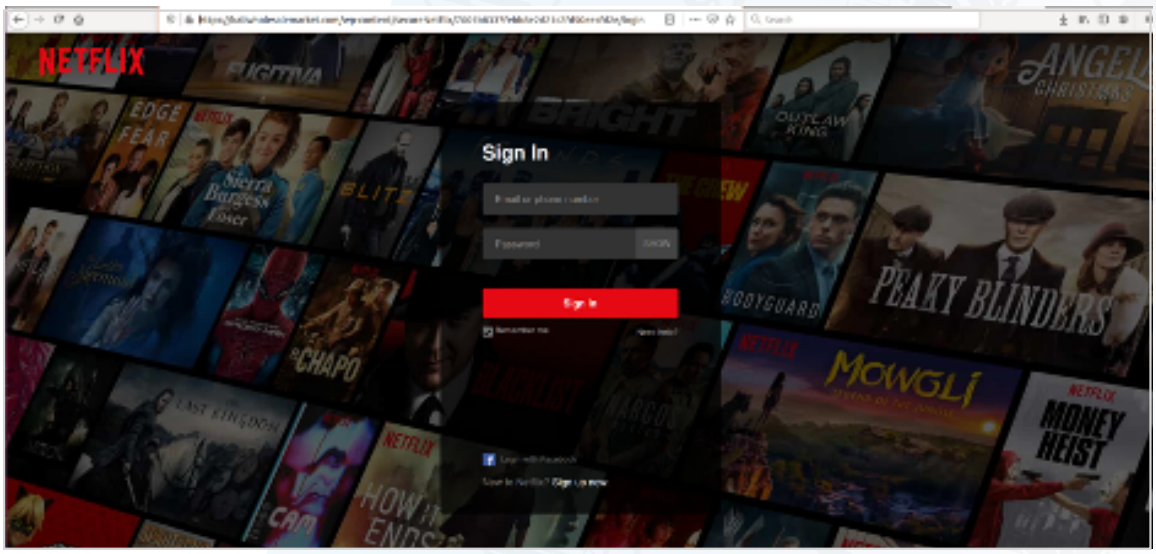


Figura 13: *Imagen de phishing de Netflix*

Estafa de soporte técnico a través de HTTPS dirigida a los usuarios de Microsoft
La figura 14 muestra una página de estafa de soporte técnico de Microsoft. Al hacer clic en la URL se muestra el certificado HTTPS como verificado por Microsoft. El uso de este certificado indica que los atacantes se aprovechan de Azure (otra marca conocida) para intentar dar la apariencia de que es una página legítima enviada por Microsoft.

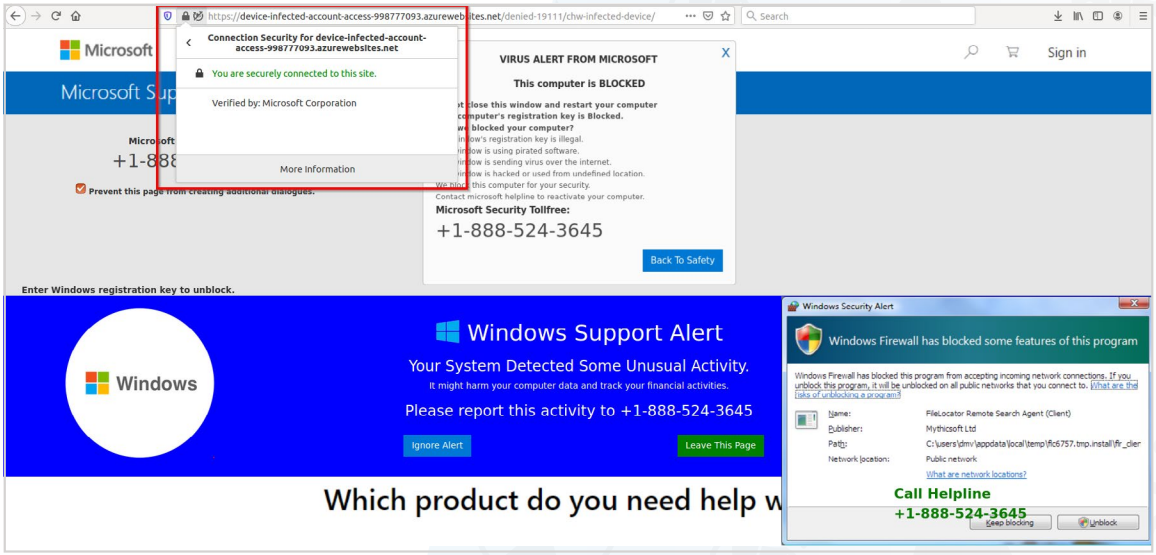


Figura 14: *Estafa de soporte técnico a través de HTTPS dirigida a usuarios de Microsoft*

Vulnerabilidades del navegador

Las vulnerabilidades del navegador permiten a los atacantes aprovechar una vulnerabilidad de un sistema operativo y cambiar la configuración del navegador de un usuario sin el conocimiento de este. La nube de Zscaler bloqueó más de 658,000 amenazas de explotación de navegadores con los siguientes sectores como principales objetivos: el de la industria (26,5 por ciento) y las finanzas/seguros (19,9 por ciento).

El sector de la industria suele ser objeto de ciberataques porque (al menos tradicionalmente) este sector estaba muy fragmentado y tenía instalaciones individuales que utilizaban infraestructuras informáticas diferentes y múltiples sistemas desarticulados. Al igual que en otros sectores, sin controles unificados y sin una aplicación centralizada de políticas y visibilidad, la seguridad está incompleta y los ciberdelincuentes siguen explotando estos agujeros.

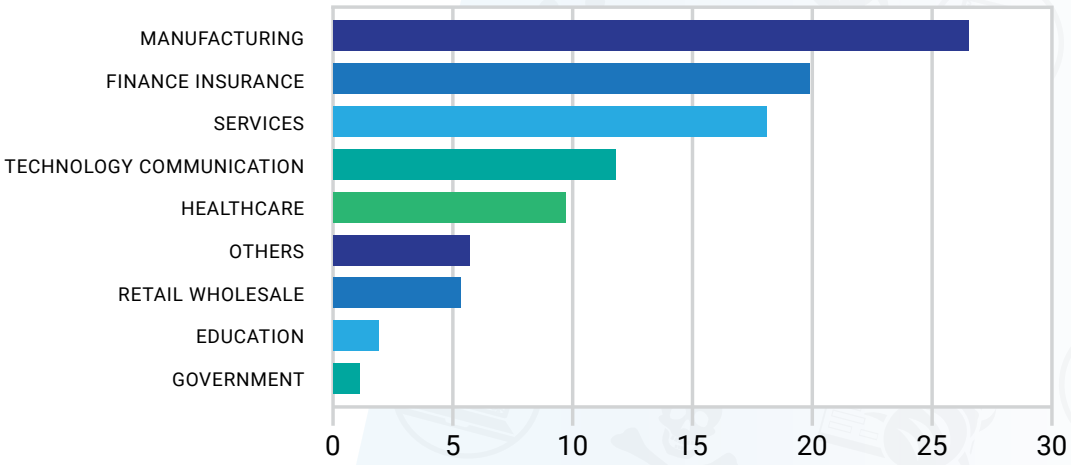


Figura 15: *Vulnerabilidades del navegador bloqueadas en canales encriptados, por sector*

Ransomware

Zscaler ThreatLabZ ha observado que los ataques de ransomware a través de los canales SSL/TLS han aumentado un 500 por ciento desde marzo de 2020. Debido a que la mayoría de los empleados trabajan de forma remota y acceden a las aplicaciones internas, se ha producido un aumento en la actividad de ransomware dirigida a las verticales de la industria que son más susceptibles y es probable que paguen rescates.

La tecnología/comunicación (40,5) y la asistencia sanitaria (26,5) fueron algunas de las verticales de la industria más azotadas por los ataques de ransomware a través de canales cifrados.

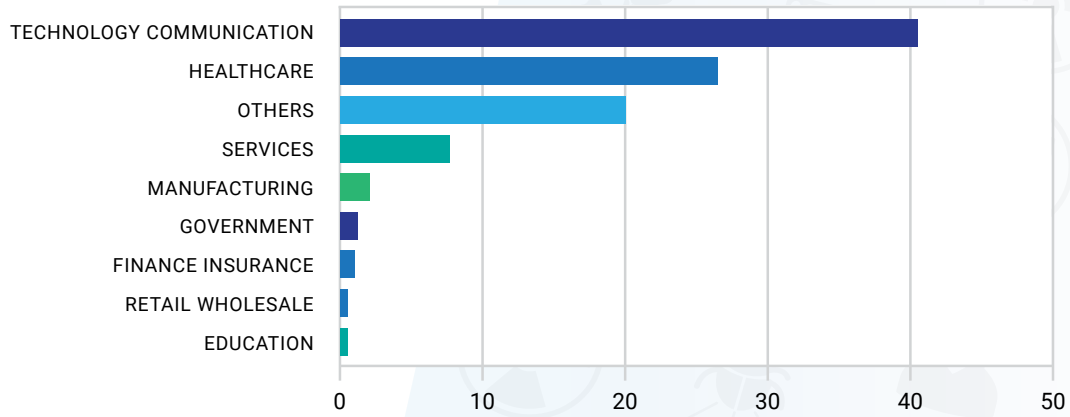


Figura 16: *Ransomware bloqueado en los canales cifrados por sector*

Entre las principales familias de ransomware que se han visto en estos ataques se incluyen variantes de FileCrypt/FileCoder, seguidas por las variantes de Sodinokibi, Maze y Ryuk. Durante el último año, ha habido un cambio destacado en muchas de estas variantes de las familias de ransomware: la incorporación de una función de exfiltración de datos. Esta nueva función permite a las bandas de ransomware exfiltrar datos confidenciales de las víctimas antes de cifrar los datos. Estos datos exfiltrados son como una póliza de seguro para los atacantes: incluso si la organización víctima del ataque tiene buenas copias de seguridad, pagará el rescate para evitar que sus datos queden expuestos.

Malware

El malware permite a un ciberdelincuente ser persistente, ya que le proporciona un acceso continuo al dispositivo de la víctima. El malware suele instalarse al explotar con éxito las vulnerabilidades o mediante ataques de ingeniería social. Según han identificado los investigadores de Zscaler, este tipo de ataque es, con diferencia, el que se da con mayor frecuencia, con más de **2600 millones de amenazas de malware** bloqueadas durante nuestro análisis.

Los sectores que manejan información de identificación personal (PII) son objetivos frecuentes de malware. En nuestro análisis, la asistencia sanitaria y las finanzas/seguros sufrieron la mayor cantidad de ataques de malware bloqueados a través de canales cifrados, con un 27,4 y 19,6 por ciento, respectivamente.

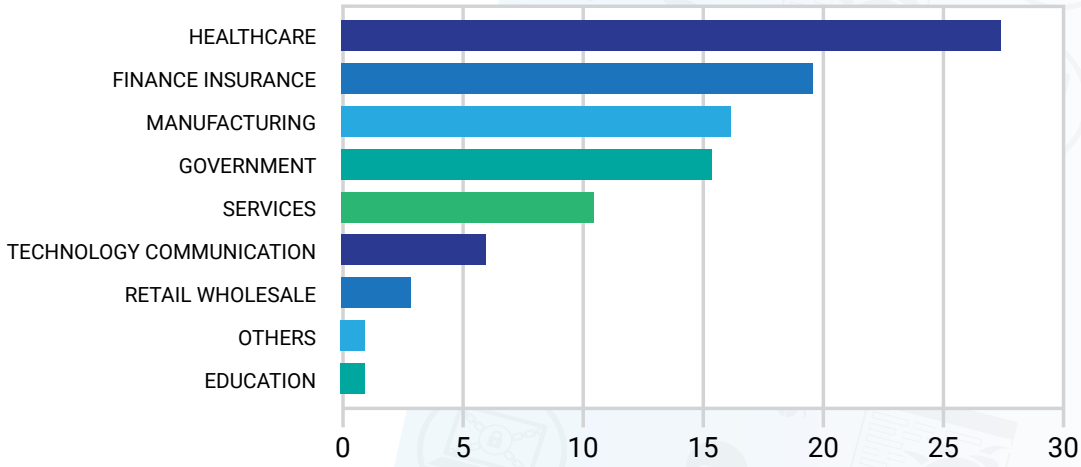


Figura 17: *Malware bloqueado en canales encriptados por sector*

Actividad de comando y control (C&C) de malware a través de canales cifrados

La comunicación C&C es otra parte clave de la cadena de ataque. Si el malware no ha sido detectado y se ha instalado con éxito en el dispositivo de un usuario final, llama de nuevo al servidor C&C para comenzar a exfiltrar datos y lanzar nuevos ataques. A menudo, las cargas de malware se programan para permanecer inactivas y esperar a que el servidor las ordene antes de iniciar cualquier actividad maliciosa. Emotet y TrickBot fueron las dos familias de malware más frecuentes en nuestro análisis.

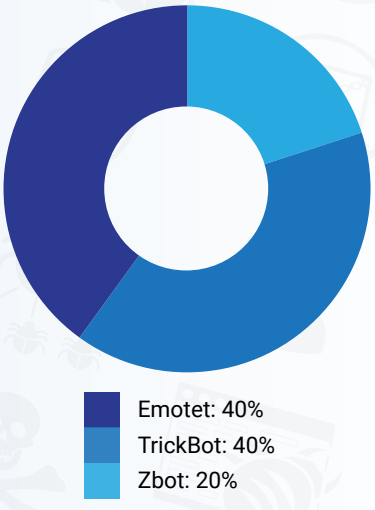


Figura 18: *Actividad de C&C más común bloqueada a través de canales cifrados*

Además de Emotet y TrickBot, vimos actividad de Ursnif y Unruy. Emotet fue el más utilizado en todos los sectores, mientras que TrickBot fue el segundo tipo de malware más utilizado en el sector de las finanzas/seguros y del gobierno. Ursnif fue popular en los ataques a la asistencia sanitaria y la industria, mientras que Unruy fue el segundo tipo de malware más utilizado en los ataques a las instituciones educativas.

Conozca el malware

Emotet: comenzó siendo un troyano bancario en 2014. Sin embargo, se ha transformado en una amenaza muy importante que se utiliza, sobre todo, para el spam y la descarga de malware en los sistemas de destino. La Agencia de Seguridad de Infraestructura Cibernética de los Estados Unidos (CISA) incluyó a Emotet entre las cepas de malware **más costosas y destructivas** que afectan tanto al sector público como al privado. Emotet ha demostrado ser resistente y modular, con mejoras regulares que dificultan su detección por parte de las organizaciones.

TrickBot: TrickBot es un sucesor del troyano bancario Dyre y se ha convertido en una de las cepas de malware más prevalentes y peligrosas en el panorama de amenazas actual. TrickBot, que suele actuar junto con otros tipos de malware, en ocasiones se utiliza como vector de infección inicial para encontrar su camino hacia el host objetivo o para descargar otras familias de malware y aprovechar así al máximo una infección.

Ursnif: el troyano Ursnif es una de las variantes más activas y prevalentes de la familia de malware Gozi, también conocida como Dreambot. El troyano se suele distribuir por kits de vulnerabilidades, archivos adjuntos de correo electrónico y enlaces maliciosos.

Unruy: es un troyano que muestra anuncios fuera de contexto y hace clic en los anuncios para conseguir ingresos para sus controladores. Se comunica con hosts remotos y también puede descargar y ejecutar archivos arbitrarios para llevar a cabo sus actividades.

Lo que se necesita para prevenir las amenazas cifradas

Es cada vez más importante reconocer que el tráfico SSL no es necesariamente tráfico seguro. Así como el uso de la encriptación ha aumentado, también lo ha hecho su uso entre los adversarios para ocultar sus ataques. La necesidad de inspeccionar el tráfico cifrado es mayor que nunca. Muchas empresas siguen las mejores prácticas de seguridad y cifran su tráfico de Internet. Sin embargo, las herramientas heredadas, como los cortafuegos de última generación, carecen del rendimiento y la capacidad para inspeccionar el tráfico SSL a escala. Nadie puede permitirse el lujo de detener las operaciones y los flujos de trabajo, por lo que muchos equipos de TI permiten que la mayoría del tráfico cifrado pase sin ser inspeccionado.

Además, existen regulaciones estrictas con respecto a cómo las empresas deben tratar los datos que contienen información personal sobre clientes, pacientes, etc. Crear políticas diferentes para saber cómo se deben inspeccionar y replicar los tipos específicos de datos en diferentes ubicaciones es una tarea ardua, por lo que las empresas se suelen saltar el proceso por completo.

¿Cómo puede proteger a su empresa de los peligros ocultos en el tráfico cifrado sin que el rendimiento se vea afectado? En la actualidad, la mayoría del tráfico empresarial está cifrado. ¿Cómo puede asegurarse de descifrar e inspeccionar todo ese tráfico, al tiempo que mantiene el cumplimiento para todos los usuarios dentro y fuera de la red?

- **Descifre, detecte y prevenga amenazas en todo el tráfico SSL** con una arquitectura de nube basada en proxy que puede inspeccionar todo el tráfico de cada usuario.
- **Ponga los ataques desconocidos en cuarentena y detenga el malware del paciente cero** estableciendo una cuarentena con la IA, que retiene el contenido sospechoso para su análisis, a diferencia de los enfoques de paso basados en cortafuegos.
- **Proporcione una seguridad coherente para todos los usuarios y todos los lugares** a fin de garantizar que todos tengan el mismo nivel de seguridad en todo momento, tanto si se encuentran en casa, en la oficina o de viaje.
- **Reduzca inmediatamente la superficie de ataque** empezando por una posición de confianza cero, donde no se puede dar el movimiento lateral. Las aplicaciones son invisibles para los atacantes y los usuarios autorizados acceden directamente a los recursos que necesitan, no a toda la red.

La solución requiere una escalabilidad y rendimiento que solo puede proporcionar una arquitectura basada en proxy nativa de la nube, como Zscaler Zero Trust Exchange. Una plataforma de seguridad basada en la nube satisface las demandas de desencriptación e inspección, ya que escala elásticamente los recursos informáticos y proporciona una aplicación coherente de las políticas en múltiples lugares. Zscaler realiza la inspección SSL a escala como parte de su plataforma de servicios y a medida que su tráfico aumenta, la capacidad se agrega instantáneamente y a demanda; no hay dispositivos que dimensionar, pedir o enviar.

Ningún sector es inmune a las amenazas a la seguridad. Y, a medida que se encripta más tráfico, inspeccionar ese tráfico se ha convertido en una misión crucial. Una estrategia de defensa profunda, de varias capas, que sea compatible con la inspección de SSL es esencial para asegurar que las empresas estén protegidas de las crecientes amenazas que se ocultan en su tráfico cifrado.

Infórmese de cómo **Zscaler** puede inspeccionar todo su tráfico SSL sin afectar al rendimiento o crear problemas de cumplimiento. También puede comprobar su capacidad para inspeccionar el tráfico SSL/TLS usando nuestra herramienta de **Análisis de la exposición a las amenazas de Internet** .

Acerca de ThreatLabZ

ThreatLabZ es la división de investigación de seguridad de Zscaler. Este equipo de primera clase es responsable de buscar nuevas amenazas y garantizar que las miles de organizaciones que usan la plataforma global Zscaler están siempre protegidas. Además de analizar el malware y de analizar el comportamiento, los miembros del equipo participan en la investigación y el desarrollo de nuevos módulos prototipo para la protección avanzada contra las amenazas en la plataforma Zscaler y realizan habitualmente auditorías de seguridad internas para garantizar que los productos y la infraestructura de Zscaler cumplen con los estándares de cumplimiento de seguridad. ThreatLabZ publica regularmente análisis detallados de amenazas nuevas y emergentes en su sitio web, **research.zscaler.com**.

Sobre Zscaler

Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, resilientes y seguros. Zscaler Zero Trust Exchange™ protege a miles de clientes de ataques cibernéticos y de la pérdida de datos conectando de forma segura a los usuarios, dispositivos y aplicaciones en cualquier ubicación. Distribuida en más de 150 centros de datos a nivel mundial, Zero Trust Exchange, basada en SASE, es la mayor plataforma de seguridad en la nube en línea del mundo. Obtenga más información en zscaler.com o síganos en Twitter **@zscaler**.

zscaler™