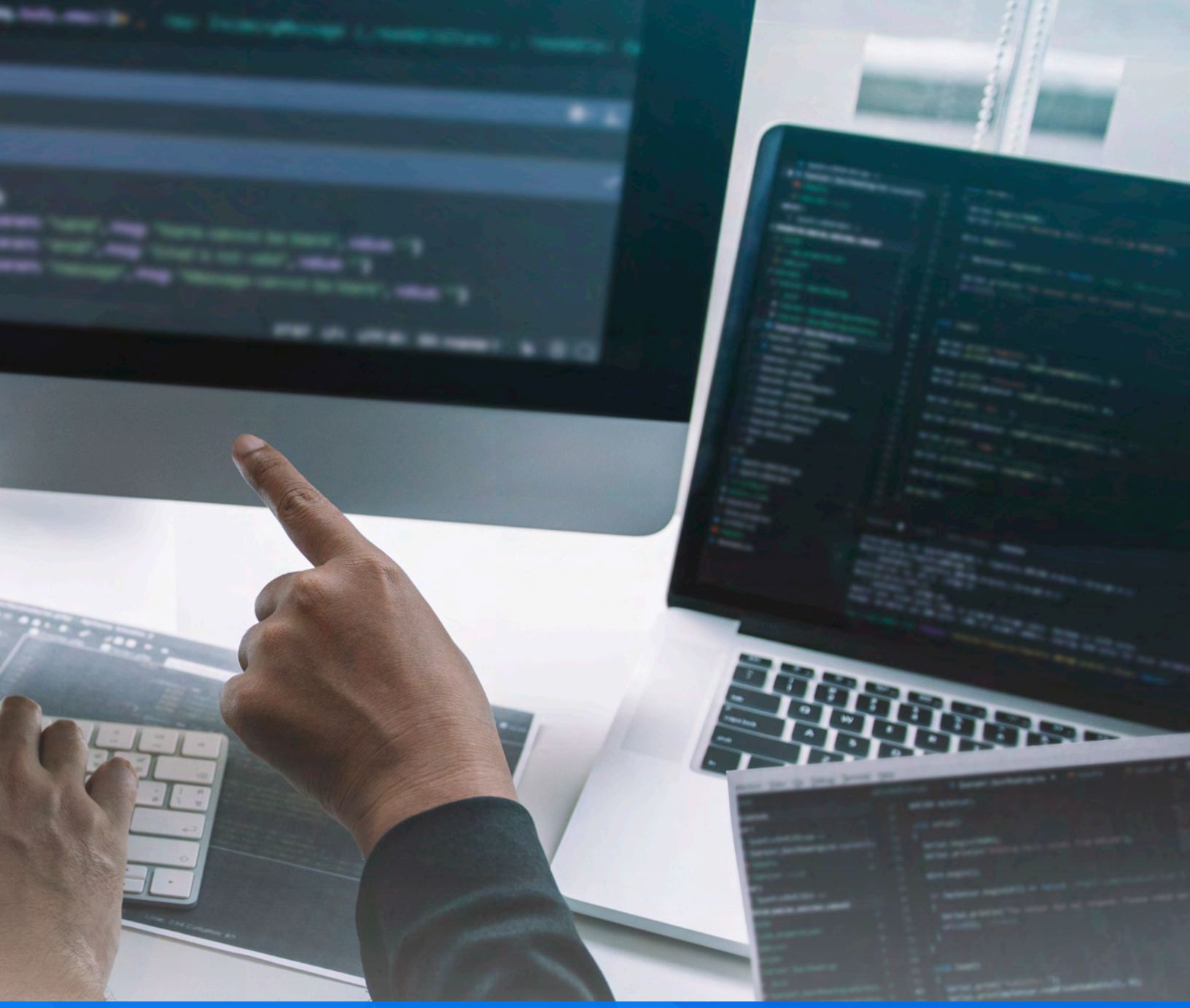

SITUACIÓN

de los ataques cifrados

INFORME 2021

zscaler™

ÍNDICE

¿Es seguro el tráfico HTTPS?

Parece haber un malentendido generalizado en lo referente a la seguridad de los datos empresariales. HTTPS (es decir, TLS, antes SSL) es el estándar de la industria para el cifrado y protege los datos en tránsito. Su tarea es la de proteger el contenido privado frente a cualquier persona que quiera espiarlo. Pero este protocolo es únicamente un vehículo; el cifrado no significa que el contenido en sí mismo sea seguro. El malware puede cifrarse y transmitirse con la misma facilidad que los archivos legítimos y, de hecho, más del ochenta por ciento del malware viaja por estos canales.

Si esta idea le parece básica, considere lo siguiente: la mayoría de las organizaciones no inspeccionan todo el tráfico cifrado. Muchas de ellas, de hecho, no inspeccionan ningún tráfico cifrado. Dado que la mayor parte del tráfico se mueve por canales cifrados, ¿por qué no iban a inspeccionarlo las empresas? Y una pregunta aún mejor: ¿qué se están perdiendo por no hacerlo?

Resulta que se están perdiendo mucho. Entre enero y septiembre de 2021, Zscaler bloqueó 20 700 millones de amenazas en HTTPS. Esto representa un aumento de más del 314 por ciento respecto a los 6600 millones de amenazas bloqueadas en 2020, que a su vez supuso un aumento de casi el 260 por ciento respecto al año anterior.

Los ciberdelincuentes son cada vez más astutos en sus tácticas de ataque, y se han beneficiado de redes de afiliación y de herramientas "como servicio" disponibles en la web oscura. Esta disponibilidad ha conducido a un estallido de ataques sofisticados que quitan el sueño a los equipos de seguridad. El ransomware, en particular, ha afectado a empresas de todo el mundo con ataques de alto perfil que causan daños por importes de decenas de millones de dólares. El cifrado del malware es un paso trivial en la secuencia de ataques.

Con el aumento del ransomware (junto con otras categorías de amenazas) y el mantenimiento de los modelos híbridos y de trabajo desde cualquier lugar, las organizaciones deben inspeccionar todo el tráfico dentro y fuera de sus instalaciones para maximizar sus posibilidades de proteger la organización. Desafortunadamente, dicha inspección requiere una cantidad increíble de recursos. Intentar hacerlo a escala con herramientas de seguridad heredadas basadas en hardware, como cortafuegos de última generación, es casi imposible y puede requerir el uso de cinco a siete veces más dispositivos para que resulte eficaz y el rendimiento no disminuya. Como resultado, muchas organizaciones dejan que al menos parte de su tráfico cifrado circule sin inspeccionar. Se trata de un enorme problema y vamos a explicar hasta qué punto exactamente.

Los ataques a través de canales cifrados aumentaron un **314 %** de 2020 a 2021.

Hallazgos clave

Zscaler Zero Trust Exchange alberga el mayor conjunto de datos de seguridad del mundo, recopilados a partir de más de 300 mil billones de señales y 160 000 millones de transacciones diarias, más de 15 veces el volumen de las búsquedas de Google cada día. El equipo de investigación de amenazas ThreatLabz de Zscaler analizó estos datos de los primeros nueve meses de 2021, evaluando las amenazas en el tráfico cifrado durante ese período. El siguiente análisis arroja información estratégica fundamental sobre el panorama de los ataques cifrados. Los hallazgos clave incluyen:

- **Las amenazas a través de HTTPS han aumentado:** Zscaler ha observado un aumento de más del 314 por ciento interanual en las amenazas dentro del tráfico cifrado por segundo año consecutivo.
- **La tecnología es un objetivo enorme:** los ataques a empresas tecnológicas aumentaron un 2344 por ciento de un año a otro; los ataques a empresas de venta minorista y mayorista aumentaron un 841 por ciento.
- **Los servicios esenciales se toman un respiro:** la sanidad fue el mayor objetivo en 2020, pero las amenazas han disminuido drásticamente, junto con los ataques a organizaciones gubernamentales. Tras los grandes ataques, como el perpetrado contra Colonial Pipeline, aumentó la atención de las fuerzas de seguridad, restando con ello atractivo a esos sectores como objetivos.
- **El Reino Unido y Estados Unidos son los principales objetivos de los ataques cifrados:** India, Australia y Francia completan los cinco primeros.
- **Las tácticas están cambiando:** el malware ha aumentado en un 212 por ciento y el phishing en un 90 por ciento, mientras que el malware de criptominería ha disminuido en un 20 por ciento, lo que refleja un cambio más amplio en las tendencias de ataque y que el ransomware va ganando popularidad.
- **Proteja su organización con confianza cero:** la mejor manera de defenderse contra las amenazas cifradas es usar una arquitectura de confianza cero basada en proxy en la nube que reduce su superficie de ataque y con la cual se puede inspeccionar todo el tráfico entrante y saliente en línea y a escala.

Los ataques a las empresas tecnológicas aumentaron **20 veces**

El cifrado moderno, incluidos SSL (Secure Sockets Layer) y su sucesor, TLS (Transport Layer Security), se utiliza en todo el mundo para proteger la mayor parte del tráfico de Internet. A medida que aumentan las tasas de cifrado del tráfico legítimo, también lo hacen las del tráfico malicioso. Zscaler bloqueó más de 20 700 millones de amenazas en un periodo de nueve meses en 2021.

En realidad, el cifrado ofrece múltiples beneficios a los atacantes: no solo es menos probable que los equipos de seguridad inspeccionen el tráfico cifrado, sino que los archivos cifrados son mucho más difíciles de leer, lo que deja que el malware se cuele sin ser detectado.

Hay varios tipos de ataques que los delincuentes pueden ocultar en el tráfico cifrado. El malware es, con diferencia, la categoría principal, ya que representa casi el 91 por ciento de los ataques.

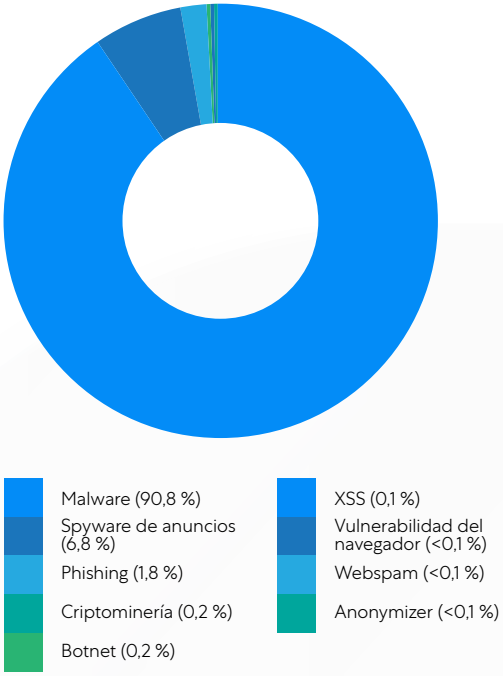

Figura 1: *Frecuencia de ataques a través de canales cifrados*

El malware representa el **91 %** de los ataques

Sin embargo, otros tipos de ataques van en aumento. El spyware de anuncios, las vulnerabilidades de los navegadores, el malware, el phishing y los ataques de botnet aumentaron en 2021 con respecto a 2020. Los únicos tipos de ataque que disminuyeron fueron la criptominería (en la que se toman los ordenadores para minar criptomonedas), el cross-site scripting o XSS (en el que se inyecta código malicioso en sitios web legítimos) y los ataques de anonimato (que utilizan proxies para dificultar el rastreo del atacante). La popularidad de los ataques de criptominería está disminuyendo, ya que el ransomware se ha convertido en una opción más lucrativa en los últimos años. El ransomware se incluye en la categoría de malware en este informe.

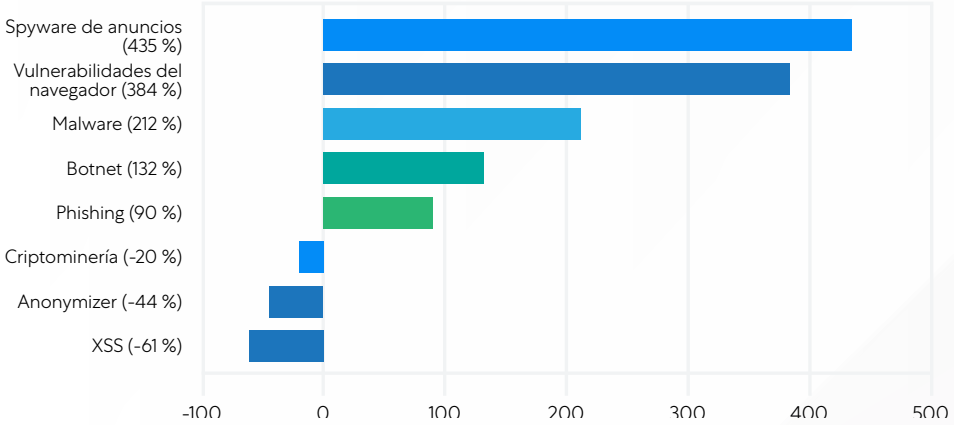

Figura 2: *Cambio anual en los ataques a través de canales cifrados*

Ataques web

La web está llena de sitios maliciosos, incluidos algunos con el prefijo HTTPS. La escasa higiene de Internet permite que las amenazas persistan durante mucho tiempo: Zscaler ha observado más de 13 000 ataques desde sitios infectados por Coinhive, a pesar de que este lleva más de dos años cerrado. Una de las categorías de ataques web más comunes que aprovechan HTTPS son los skimmers basados en JavaScript, como **Magecart**, que se utilizan para robar datos de pago en la web.

Familia	Impacto	Acción de Política
Nicehash	5 644 273	Criptominería
Magecart	2 573 304	Skimming de pagos
Adload	1 626 905	Spam de web
Covid19	972 223	Malware
Webshell	934 873	Malware
Coinhive	13 670	Criptominería

Los sitios web infectados pueden permanecer en activo durante **años** después de su lanzamiento.

Phishing

El phishing sigue siendo una de las principales tácticas, con la que se engaña a los usuarios para que hagan clic en enlaces de correos electrónicos que contienen malware oculto. Todos los servicios de correo electrónico y de intercambio de archivos son vulnerables a los ataques, pero la popularidad de Microsoft 365 lo convirtió, con diferencia, en el principal objetivo en 2021, con más de 15 millones de intentos de ataque bloqueados por la plataforma Zscaler durante un periodo de observación de nueve meses.

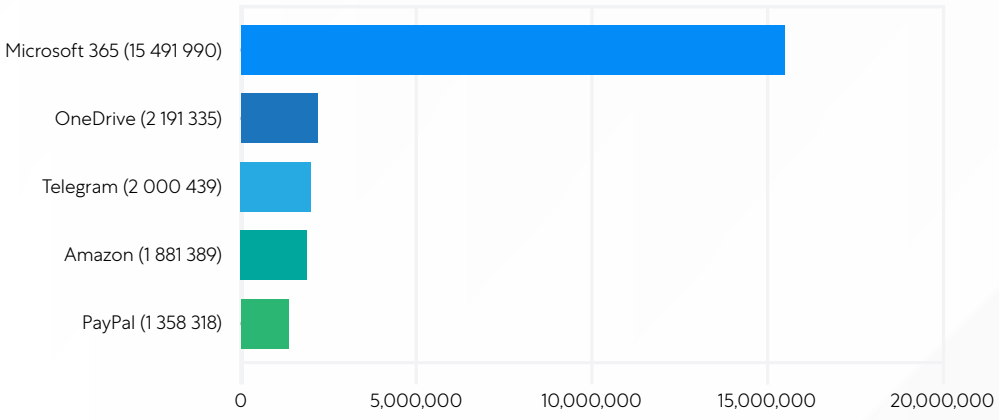

Figura 3: *Ataques de phishing cifrado*

Malware

El malware fue la principal categoría de ataques en 2021. El malware suele descargarse desde un enlace infectado de un correo electrónico o de un sitio web, por ejemplo. Aunque la mayoría de las organizaciones tienen alguna forma de protección contra el malware, los atacantes mejoran sus técnicas y crean nuevas variantes de malware que pueden eludir las tecnologías de huellas digitales. Por supuesto, para las organizaciones que no inspeccionan su tráfico cifrado, ni siquiera el software malicioso conocido tendrá visibilidad hasta después de que haya entrado en sus sistemas. A continuación se muestran algunas de las familias de malware más frecuentes en 2021. Más adelante en este informe, hay casos prácticos técnicos de cuatro de estas familias que demuestran sus secuencias de ataque.

Familia	Casos de malware
njRAT	355 753
Ursnif	336 540
Azorult	199 334
Hancitor	137 421
Emotet	58 867
Qakbot	30 199
Smokeloader	4269

La información personal identificable (PII) es el **principal objetivo** de los intentos de robo de datos.

Robo de datos

Los atacantes no solo utilizan canales encriptados para infiltrarse en los sistemas, sino que también los utilizan para exfiltrar datos. Los tipos de datos más comúnmente exfiltrados son los identificadores nacionales y fiscales, como los números Aadhar (la India), TFN (Australia), Seguridad Social (Estados Unidos) y BSN (Países Bajos). La información financiera y de tarjetas de crédito es el siguiente objetivo más popular, seguido de la propiedad intelectual y los datos médicos. El siguiente gráfico muestra solo tres meses de intentos de robo de datos.

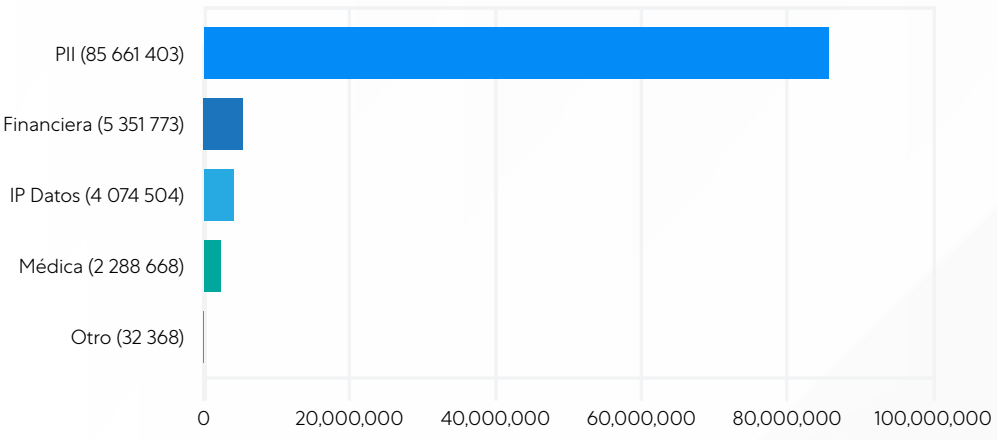

Figura 4: *Intentos de robo de datos*

Actividad de mando y control

Los servidores de mando y control se utilizan por varias razones, entre ellas la ejecución de cargas útiles de segunda etapa en ataques dirigidos, la exfiltración de datos y el control de máquinas para su uso en botnets. Los botnets son redes de dispositivos que están bajo el control de un atacante y que permiten ataques coordinados a gran escala. Se han utilizado botnets para ataques distribuidos de denegación de servicio (DDoS), infracciones financieras, minería de criptomonedas e intrusiones dirigidas.

Los atacantes utilizan una serie de herramientas para llamar a sus servidores de mando y control. Algunas de estas, incluidas Smoke Loader y Gumblar, son bots diseñados específicamente para tal fin. Otras, como Cobaltstrike y Poshc2, son herramientas de pruebas de penetración que han sido reutilizadas por los atacantes. A continuación se muestra la tasa de intentos de devoluciones de llamada con esas herramientas:

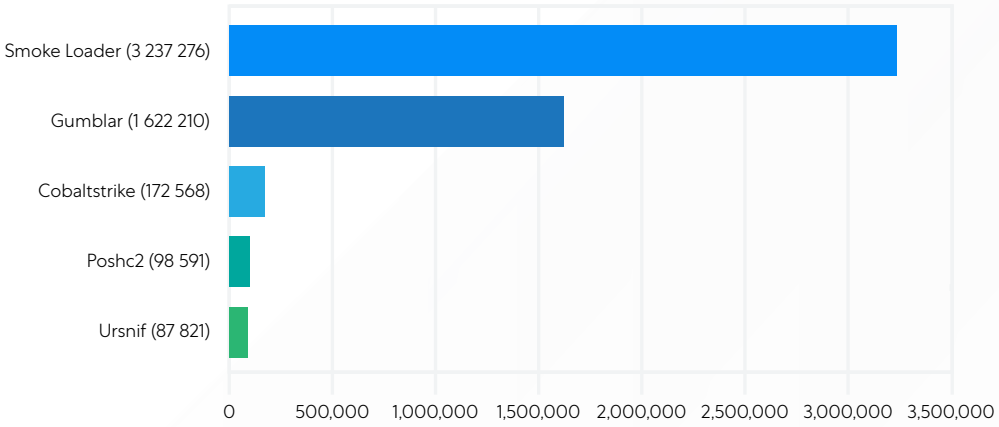

Figura 5: *Actividad de mando y control*

Los atacantes interactúan con casi el **70 %** de las aplicaciones web cifradas.

Relleno de credenciales y actividad de intrusión

No se propaga únicamente malware a través del tráfico cifrado. Los atacantes también utilizan estos canales para intentar ataques dirigidos a personas forzando aplicaciones cifradas.

El equipo de ThreatLabz también recopila información a través de una red de señuelos desplegada a nivel mundial, con la tecnología Zscaler Deception, para estudiar las tácticas, técnicas y procedimientos de los atacantes. Los activos señuelo se utilizan como cebo para los atacantes y los usuarios legítimos no interactúan con ellos, por lo que cualquier interacción con ellos es una señal de actividad maliciosa. ThreatLabz descubrió lo siguiente:

1. Casi el 70 % de todas las aplicaciones señuelo habilitadas para SSL tenían interacción, lo que indicaría que el 70 % de las aplicaciones habilitadas para SSL probablemente sufran intentos de ataque.
2. En el contexto de las aplicaciones web señuelo orientadas a Internet, casi el 48 % de los ataques de credenciales se dirigieron a señuelos de correo electrónico y VPN.
    - Las direcciones de correo electrónico señuelo fueron objetivos populares para llenar las credenciales robadas.
    - Las VPN señuelo estaban sujetas a la explotación de los CVE recientemente revelados en los productos VPN.
3. La técnica más observada fue la búsqueda de archivos ".git", probablemente con vistas a buscar servidores web mal configurados que revelaran el código fuente. Aunque esta técnica lleva tiempo existiendo, todavía es tremendamente popular durante el reconocimiento previo al ataque.

Ataques móviles

Los teléfonos inteligentes y tabletas siguen siendo objetivos populares para los atacantes, que los fuerzan con el uso de aplicaciones falsas. Tras la infección inicial, muchas de las variantes de malware móvil nuevas y más frecuentes utilizan la comunicación de red SSL para actividades de mando y control, incluida la obtención de cargas útiles o la recepción de comandos para realizar actividades maliciosas y exfiltrar datos. Familias de malware como Hydra, Joker y la recientemente descubierta GriftHorse, están recurriendo a SSL para actividades posteriores a la infección.

Malware GriftHorse

La reciente campaña de malware GriftHorse para Android alcanzó a más de 10 millones de víctimas en todo el mundo, robando un importe estimado en cientos de millones de euros. Tras la infección, se anima a las víctimas a enviar un número de teléfono para recibir un premio. Sin que la víctima lo sepa, el número de teléfono se suscribe a un servicio de SMS prémium que cobra en la factura telefónica de la víctima más de 30 euros al mes. El troyano se comunica con los servidores de mando y control en tres etapas y se ha descubierto que aprovecha SSL para las actividades posteriores a la infección.

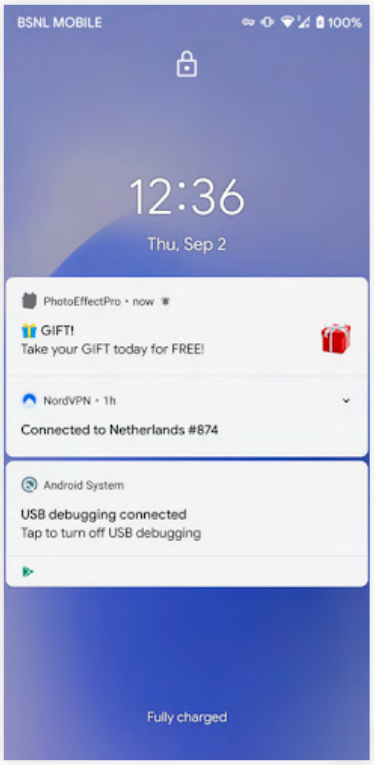

Figura 6: *Ataque de malware GriftHorse*

Malware Joker

Joker es una de las familias de malware más destacadas que se dirige a los dispositivos Android a través de Google Play Store. Zscaler bloqueó casi 22 000 intentos de devolución de llamada del malware Joker a través de TLS, que utiliza para actividades de mando y control. A pesar del conocimiento público de este malware, sigue abriéndose camino en el mercado oficial de aplicaciones de Google mediante el empleo de cambios en su código, métodos de ejecución o técnicas de recuperación de la carga útil. Joker es un tipo de spyware y está diseñado para robar mensajes SMS, listas de contactos e información del dispositivo, así como para inscribir a la víctima en servicios prémium de protocolo de aplicaciones inalámbricas (WAP).

Malware Hydra

Hydra es uno de los ejemplos más frecuentes y competentes del malware bancario. Sus capacidades incluyen la grabación de las actividades que tienen lugar en la pantalla del usuario, conocida en inglés como screencasting. Hydra también es capaz de instalar aplicaciones remotas con las que los atacantes observan y controlan los dispositivos infectados, lo que lo convierte en una grave amenaza. Hydra aprovecha los certificados SSL para realizar actividades de mando y control.

SECTOR

Si se compara 2021 con 2020 ha habido amplias variaciones por sectores. Siete de los sectores de nuestro estudio han experimentado un aumento de las tasas de ataque a través de canales cifrados, mientras que en dos de disminuyeron, entre ellos el objetivo principal del año pasado, la asistencia sanitaria.

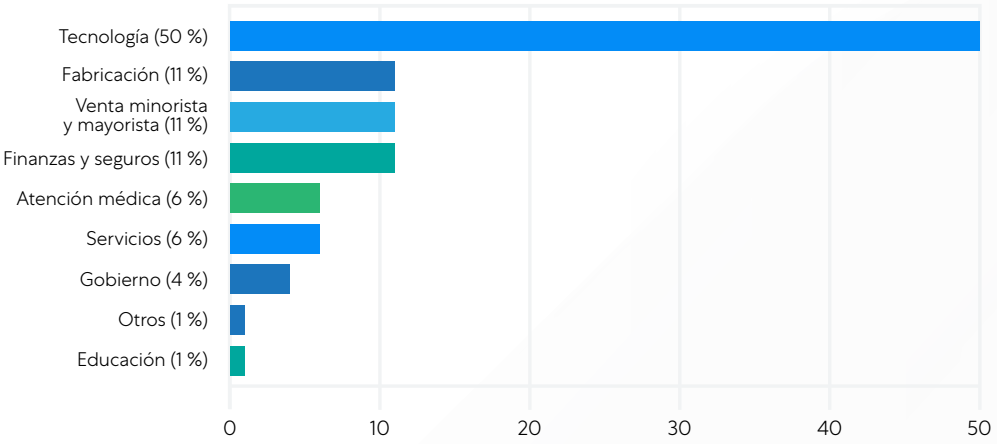

Figura 7: *Volumen de ataques por sector*

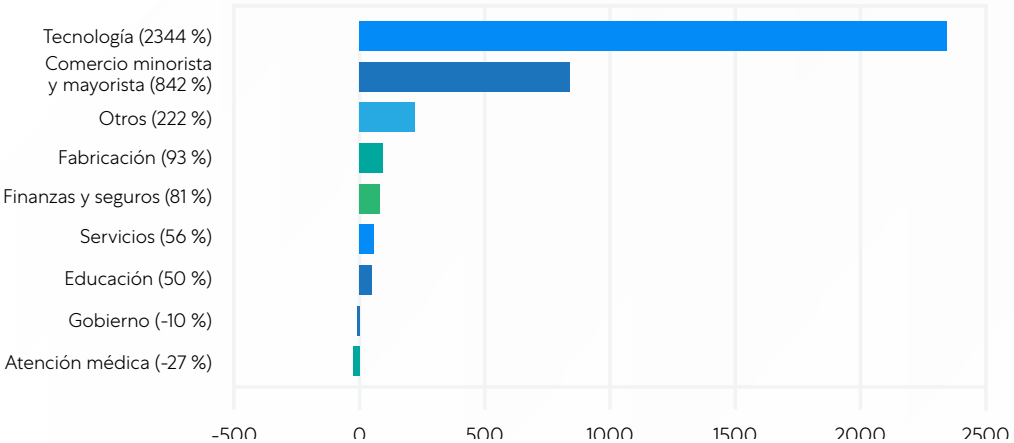

Figura 8: *2021 frente a 2020: ataques por sector*

La tecnología y el comercio minorista han experimentado un enorme aumento de ataques

Los ataques a las empresas tecnológicas se han incrementado de manera asombrosa en 23 veces y ahora representan más de la mitad de los ataques observados. El sector de la tecnología recibe ataques de malware a un ritmo mucho más alto que otros sectores. Su gran dependencia de la tecnología para casi todas las funciones empresariales ofrece a los atacantes una gran superficie de ataque que explotar. Algo que se ha visto potenciado por la repentina necesidad de dar soporte a los trabajadores remotos con todo tipo de servicios, desde conectividad remota hasta teleconferencias, aplicaciones basadas en SaaS y cargas de trabajo en la nube pública.

Las empresas tecnológicas también son objetivos atractivos debido a su papel en la cadena de suministro de otras empresas. Un ataque exitoso a la cadena de suministro puede dar a los atacantes acceso a cientos o incluso miles de víctimas posteriores, como ocurrió en los casos de Kaseya, SolarWinds y otros.

Los sectores de venta minorista y mayorista también han tenido un año extremadamente malo, con un aumento de más de 8 veces en las tasas de ataque. Solo supusieron el 3,5 % de los ataques en 2020, frente al 11 % en 2021. Hubo un repunte significativo de contenidos maliciosos que incluye skimmers, JavaScripts maliciosos y cargas útiles de malware dirigidas a vendedores minoristas y de comercio electrónico a través de canales TLS.

Mientras el mundo comienza a recuperar la normalidad y las empresas y los actos públicos empiezan a abrirse en todo el mundo, muchos empleados siguen trabajando en entornos relativamente inseguros. Obtener acceso a los sistemas de puntos de venta críticos es tremendamente atractivo para los ciberdelincuentes, ya que les abre la puerta a enormes beneficios.

Disminuyen los ataques a la sanidad y al gobierno

Después de ser el principal objetivo en 2020, los ataques a organizaciones sanitarias disminuyeron un 27 % en 2021. Del mismo modo, los ataques a organizaciones gubernamentales disminuyeron en un 10 %. Los grandes ataques de ransomware que han afectado a los servicios críticos, como el ataque a SolarWinds, el ataque a Colonial Pipeline y el ataque de ransomware al Health Service Executive de Irlanda, han atraído mucha atención de los niveles más altos de las fuerzas de seguridad, lo que hace que tocar estos sectores críticos sea demasiado arriesgado en este momento. Por otro lado, varias familias de ransomware se comprometieron a no atacar la sanidad y otros servicios críticos durante la pandemia, aunque no han cumplido del todo estas promesas.

Ámbito geográfico

Los cinco países más afectados por los ataques cifrados son el Reino Unido, Estados Unidos, la India, Australia y Francia:

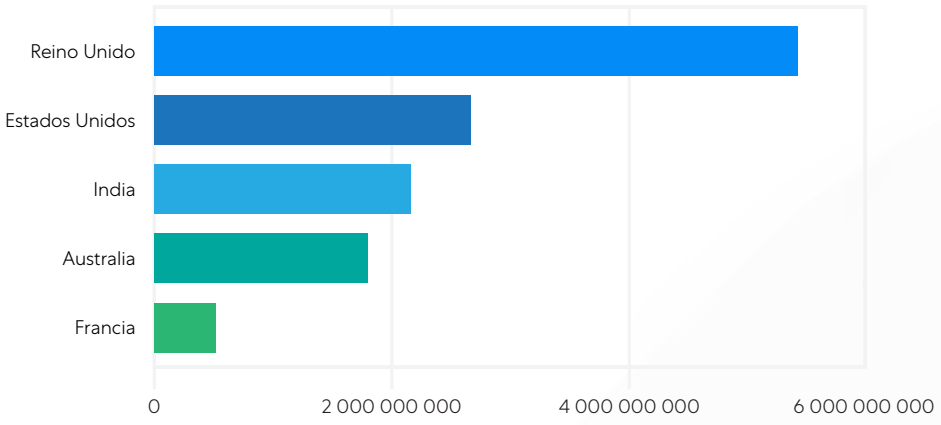

Figura 9: *Países más atacados*

Cada uno de estos países es un gran centro tecnológico y sus tasas de ataque han aumentado con el incremento general de los ataques dirigidos a ese sector. ThreatLabz ha registrado ataques en 255 países diferentes de todo el mundo, incluidos países pequeños que no son objetivos comunes. Se incluyen más de 7,5 millones de ataques en islas del Caribe, además de lugares como las Islas Feroe, San Bartolomé y las Islas Malvinas. Es resultado del crecimiento de los programas de "trabaja donde quieras", que llevan a que la plantilla trabaje a distancia.

Con el Reino Unido en cabeza, que sufrió ataques masivos, Europa en su conjunto fue el objetivo de la mayor cantidad de intentos de ataque a través de canales cifrados:

Región	**Cuenta**
Europa	7 234 747 361
APAC	4 925 542 601
Norteamérica	2 778 360 051
Sudamérica	226 320 069
África	146 865 982
Oriente Medio	137 494 862
América Central	127 354 294
Caribe	7 543 056
Antártida	16 144

Trabajar desde cualquier lugar ha ampliado el alcance geográfico de los ciberataques.

LO QUE SE NECESITA PARA PREVENIR LAS AMENAZAS CIFRADAS

A medida que las organizaciones cambian para dar soporte a nuevos modelos de trabajo habilitados digitalmente, se hace cada vez más importante garantizar que sus activos y el tráfico a dichos activos sean seguros. Además, es fundamental reconocer que el cifrado por sí solo no proporciona esa seguridad: los adversarios utilizan los canales cifrados con la misma frecuencia que los canales no cifrados.

En resumen: **debe inspeccionar su tráfico. ¡Todo el tráfico!**

Las herramientas heredadas hacen que la inspección completa sea una propuesta costosa y que degrada el rendimiento. Además, las regulaciones que requieren diferentes políticas para diferentes tipos de datos también pueden hacer que esto sea una ardua tarea. Afortunadamente, existen estrategias probadas que permiten a las organizaciones inspeccionar su tráfico cifrado a escala, sin afectar negativamente al rendimiento de sus sistemas ni hacer que el cumplimiento sea una pesadilla. Le recomendamos lo siguiente:

- Descifre, detecte y prevenga amenazas en todo el tráfico HTTPS con una arquitectura nativa 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 un sandbox con IA, que retiene el contenido sospechoso para su análisis, a diferencia de los enfoques de paso basados en cortafuegos.
- Proporcione una seguridad consistente para todos los usuarios y 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 de manera inmediata su superficie de ataque partiendo de una posición de confianza cero, en la que el movimiento lateral no puede existir. Las aplicaciones son invisibles a los atacantes y los usuarios autorizados acceden directamente a los recursos necesarios, 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. A fin de garantizar la protección de las empresas, es esencial una estrategia de defensa en profundidad de varias capas que reduzca la superficie de ataque y sea totalmente compatible con la inspección HTTPS para detectar amenazas ocultas.

La mejor manera de detener las amenazas cifradas es inspeccionar el tráfico cifrado como parte de una estrategia holística de seguridad de confianza cero.

CÓMO DETIENE ZSCALER ZERO TRUST EXCHANGE LAS AMENAZAS CIFRADAS

Las estrategias y arquitecturas de confianza cero son el medio más eficaz para proteger a su organización de las ciberamenazas de rápida evolución. La confianza cero tiene que ver con asumir que está activamente bajo ataque en un momento dado y que se ha producido una violación en su infraestructura. Se ponen en marcha controles de seguridad con esta suposición como base para evitar que el presunto ataque se desarrolle con éxito.

La mayoría de los ataques avanzados implican tres etapas distintas. Los ataques comienzan con un compromiso inicial de un punto final o activo expuesto a Internet. Una vez dentro, el atacante se propaga lateralmente, realiza un reconocimiento y establece una posición en la red. Por último, los ataques se ejecutan para lograr sus objetivos, que normalmente implican la exfiltración de datos. Zscaler Zero Trust Exchange reduce enormemente el riesgo en cada una de estas tres etapas del ataque al proporcionar diversos controles de seguridad en cada etapa:

Evitar verse comprometido
Proteja a los usuarios, servidores, cargas de trabajo e IoT/OT minimizando la superficie de ataque e inspeccionando todo el tráfico.

Evitar el movimiento lateral
Impida que los atacantes se muevan por su red para encontrar objetivos de gran valor.

Evite el robo de datos
Inspeccione todos los datos vinculados a Internet para evitar la pérdida de datos en Internet y la explotación de dispositivos no administrados.

Compromiso inicial: para detener el acceso inicial, el primer paso a dar es reducir el número de puntos de entrada a su ecosistema. Audite su superficie de ataque, manténgase al día con los parches de seguridad y solucione cualquier configuración incorrecta que pueda existir. También debería eliminar cualquier aplicación que se dirija a Internet, y puede hacerlo colocándola detrás de un proxy en la nube que intermedie la conexión. Esto proporciona a los atacantes una única puerta de entrada y otra de salida que usted puede controlar. A continuación, tal y como hemos recomendado reiteradamente, inspeccione todo su tráfico. No asuma que cualquier cosa es de confianza. Zscaler realiza la inspección HTTPS a escala como parte de su plataforma de servicios y, a medida que su tráfico aumenta, se va añadiendo capacidad al instante y bajo demanda. No hay dispositivos que dimensionar, pedir o enviar.

Movimiento lateral: con la confianza cero, no existe una "red de confianza". Debe asumir que cualquiera que tenga acceso a cualquier aplicación es hostil y por lo tanto, debe limitar el daño que puede causar. Utilice la microsegmentación para reducir el acceso, incluso para los usuarios autenticados. La solución de acceso de confianza cero de Zscaler, Zscaler Private Access™, conecta a los usuarios directamente con la aplicación necesaria sin exponer nunca la red, creando un segmento uno a uno que es intermediado y autenticado por Zero Trust Exchange. Esta es la segmentación de confianza cero en su forma más pura, y es mucho menos compleja que la segmentación de red basada en reglas que se utiliza con las tecnologías heredadas. Zscaler también utiliza la tecnología de engaño para atraer a los atacantes con señuelos estratégicamente colocados que alertan a los equipos de seguridad de un atacante que intenta moverse lateralmente o realizar un reconocimiento.

Devolución de llamada de mando y control: una vez instalado el malware, generalmente intentará ponerse en contacto con un servidor de mando y control. Este contacto permite a los atacantes tomar el control de las máquinas, emitir comandos adicionales, descargar malware adicional o robar datos. La inspección del tráfico hacia el norte (saliente) es tan importante como la del tráfico hacia el sur (entrante) para interrumpir estas comunicaciones y proteger sus datos confidenciales. Zscaler puede inspeccionar los datos cifrados de ambas maneras, implementando habilidosas capacidades de protección contra la pérdida de datos para identificar y detener cualquier tráfico saliente malicioso.

Zscaler Zero Trust Exchange detiene toda la secuencia de ataques y ofrece inspección HTTPS a escala mediante un enfoque de varias capas que cuenta con inspección de amenazas en línea, sandboxing y prevención contra la pérdida de datos, junto con una amplia gama de capacidades de defensa adicionales. Además de todo eso, el efecto de la nube de Zscaler hace que todas las amenazas identificadas en la plataforma global actualizan automáticamente las protecciones para todos los clientes de Zscaler, por lo que su postura de seguridad mejora constantemente gracias a las aportaciones de todos los clientes de Zscaler en todo el mundo. Zscaler Zero Trust Exchange, impulsado por la mayor nube de seguridad del mundo, acelera la transformación empresarial al proteger a los usuarios y las aplicaciones independientemente de su ubicación mediante la aplicación de políticas e identidad basadas en contexto.

A continuación se muestran familias de malware nuevas y frecuentes que aprovechan TLS que ThreatLabz observó en 2021.

njRAT

Se han observado 355 753 bloqueos de descarga a través de TLS.

Resumen

njRAT, también conocido como Bladabindi, es un troyano de acceso remoto (RAT) escrito en el marco .Net que puede proporcionar un control completo del sistema infectado y brinda diversas características al atacante remoto. Puede registrar las actividades del teclado del usuario, robar datos de las máquinas comprometidas y exfiltrar datos a un servidor remoto. Se observó por primera vez en junio de 2013.

Para evadir la detección, el malware puede utilizar alguna o todas las siguientes técnicas:

1. Ofuscación mediante compresores conocidos, como ConfuserX, etc.
2. Antivirtualización: comprobación de la presencia de "vboxservice.exe", “vboxtray.exe", “vmtoosd.exe”, “SDBIE.DLL”, etc.
3. Comprobación de herramientas de análisis: comprobación del proceso como processviewer.exe, processhacker.exe, etc.

Estrategia de distribución

Los atacantes distribuyen njRAT de forma descontrolada mediante diversas estrategias, como el correo electrónico y los vectores de ataque web. Algunos de los vectores de ataque populares son:

- Uso de kits de explotación como el Lord EK y el Rig EK.
- Archivos MS Office basados en macros enviados como adjuntos de correo electrónico o alojados en una URL.

Persistencia

Para una mayor persistencia, el malware puede utilizar cualquiera de los siguientes mecanismos o ambos:

1. Hacer una entrada en el registro de ejecución automática en HKCU\Software\Microsoft\Windows\CurrentVersion\Run o HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
2. Copiarse a sí mismo en la carpeta de inicio

Red

njRAT utiliza DNS dinámico para servidores de mando y control y se comunica mediante un protocolo TCP personalizado a través de un puerto configurable. Recientemente se ha visto a njRAT v2.0 utilizar cdn.discordapp.com para lanzar su carga útil, que funciona a través del protocolo HTTPS. Filebin.net, que también utiliza HTTPS, se ha utilizado asimismo para hacerse pasar por un juego crackeado.

Smoke Loader

ThreatLabz registró 4269 bloqueos de descarga y 3 237 276 bloqueos de devolución de llamada a través de TLS.

Resumen

Smoke Loader surgió por primera vez de la ciberdelincuencia rusa clandestina en 2011. Este año, Smoke Loader ha cumplido 10 años y sigue activo y sin control. Smoke Loader se utiliza principalmente como un descargador para descargar y ejecutar malware adicional. Smoke Loader es un kit delictivo que incorpora un bot y un panel de mando y control basado en PHP junto con un manual del usuario. Este malware se vende a menudo en la web oscura y el paquete completo de malware cuesta unos 1650 dólares.

Técnicas de evasión

Smoke Loader suele replicarse a través de listas de procesos para encontrar un proceso que inyectar y utiliza el método de inyección de propagación para inyectarse en explorer.exe. También está armado con múltiples trucos anti-VM. Por ejemplo, comprueba si la ruta del ejecutable contiene la cadena [A-F0-9]{4}. vmt y también verifica todos los procesos en ejecución para buscar las cadenas "qemu-ga.exe", “qga.exe”, “windanr.exe”, “vboxservice.exe”, “vboxtray.exe", “vmtoosd.exe”, “pr_toos.exe”, “vbox” y “vmmemc”, y en caso de que encuentre alguna, las salidas binarias. También busca nombres de procesos en ejecución como “procmon.exe", “ProcessHacker.exe”, "Wireshark.exe" y muchos otros y, cuando encuentra uno de estos procesos, las salidas binarias.

Mecanismo de persistencia

Genera un ID único para cada máquina atacada, que se basa en la concatenación del nombre del ordenador, un número estático codificado (que difiere entre campañas) y el número de serie del volumen de la unidad del sistema. El ID se genera entonces como un hash MD5 de la cadena concatenada y se añade de nuevo el MD5 del número de serie del volumen. El malware utiliza este ID único con varios fines, a saber, la creación de nombres de archivo aleatorios para dos archivos allí colocados: el primero es una copia del ejecutable de Smoke Loader y el segundo es un archivo lnk creado en la carpeta de inicio que se invoca como una tarea programada.

Comunicación en red

Los dominios de mando y control se cifran mediante simples operaciones XOR. A continuación, Smoke Loader envía una solicitud POST al servidor de mando y control. La carga útil se cifra mediante RC4 antes de enviarla. La solicitud POST devuelve una respuesta “404 Not Found", pero contiene una carga útil en el cuerpo de la respuesta. Smoke Loader se ha convertido en un descargador popular para varias familias de malware diferentes y se han constatado descargas de malware como Avemaría alojado en pastebin.com, que funciona a través de HTTPS. Se puede hallar comunicación similar de otros troyanos llamados dropper que utilizan HTTPS.

QakBot

30 199 bloqueos de descarga observados a través de TLS.

Resumen

QakBot es un troyano bancario, también conocido como Qbot o Pinkslipbot, que lleva activo desde 2007. Su objetivo principal es robar credenciales bancarias. Se distribuye por correo electrónico no deseado y pretende atraer a los usuarios para que descarguen archivos adjuntos maliciosos o hagan clic en enlaces maliciosos. Un documento descargado o un archivo de script descargan además la carga útil principal de Qakbot en el sistema infectado. En algunos casos, se ha distribuido a través de kits de explotación y ha sido descargado por otros programas maliciosos como TrickBot. Con el tiempo se ha ido desarrollando y ha ido añadiendo funcionalidades, como técnicas de inyección web para robar credenciales, además de números de tarjetas de crédito, números de la seguridad social, direcciones de correo electrónico y pulsaciones de teclas, y tiene funcionalidades de puerta trasera.

Mecanismo de persistencia

QakBot establece la persistencia mediante la creación de una clave RUN en la ubicación de inicio automático y la ejecución del malware en cada inicio de sesión. También crea tareas programadas para ejecutar la carga útil una vez a las 5:33 a. m. y borrar la tarea programada después de la ejecución.

> *HKEY_USERS\Software\Microsoft\Windows\CurrentVersion\Run\{Random}*
> *C:\Windows\SysWOW64\schtasks.exe 'C:\Windows\system32\schtasks.exe' /Create /RU 'NT AUTHORITY\SYSTEM' /tn {Random}/tr '\"% AppData%\Roaming\Microsoft\{Random}\{Random.exe}\" /I {Random}' /SC ONCE /Z /ST 05:33 /ET 05:45*

Comunicación en red

En una de las campañas, JavaScript descarga el formulario actualizado de QakBot *ebook[.]w3wvg.com/datacollectionservice.php3* y lo ejecuta. La carga útil que se descarga está cifrada y el script la descifra antes de introducirla en el sistema y robar la siguiente información de la máquina de la víctima:

- Dirección IP
- Nombre de Host
- Usuario
- Versión del sistema operativo
- Credenciales bancarias

Mediante WebInject consigue alterar la comunicación entre la máquina de la víctima y los sitios web bancarios y roba las credenciales. Para comunicarse con el servidor de mando y control a través de Transport Layer Security, como se muestra en la siguiente captura de pantalla, QakBot utiliza un handshake TLS en lugar de Secure Sockets Layer.

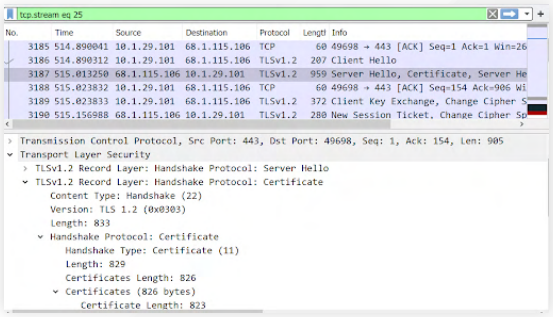

Figura 10: *QakBot recurre al handshake TLS*

Solarmarker

Resumen

El malware conocido como Solarmarker / Jupyter Infostealer / Yellow Cockatoo / Polazert es un ladrón de información y keylogger altamente modular. El malware suele empaquetarse con aplicaciones potencialmente no deseadas conocidas, como PDFSam, y generalmente utiliza Innopack para empaquetarse como un archivo de programa legítimo. La infección de Solarmarker normalmente se produce mediante el envenenamiento SEO, antigua técnica utilizada como señuelo para hacer que las víctimas descarguen archivos de Internet. La descarga del paquete de malware se realiza a través de HTTPS.

Técnicas de evasión

Este malware se distribuye mediante instaladores como MSI e Innopack. Así consiguen aumentar el tamaño del vector inicial hasta situarlo por encima de los 50 MB, que es superior al tamaño de envío de algunos repositorios de malware y sandboxes. MSI también se utiliza para evadir la detección de puntos finales y soluciones antivirus, ya que la ejecución de PowerShell por parte de MSI es menos sospechosa que un EXE que ejecuta un script PowerShell.

Mecanismo de persistencia

En campañas recientes, el malware deja un archivo .lnk en el directorio Start Menu\Programs\Startup del usuario. Con el archivo .lnk ubicado dentro de este directorio, se ejecutará en el inicio y abrirá la puerta trasera.

Comunicación en red

Solarmarker se sirve mediante el protocolo TLS y se distribuye a través del envenenamiento SEO. Debido a que este malware generalmente se empaqueta con otros instaladores, su comunicación de red queda en parte ofuscada por las comunicaciones de los compresores legítimos. La mayoría de los programas utilizan TLS y HTTPS, mientras que la comunicación maliciosa se produce a través de HTTP mediante solicitudes POST. La dirección IP está presente en el binario. Los datos de usuario se envían por medio de un JSON, como se muestra a continuación.

```
"{\"action\":\"ping\",\"",
Deimos.a.a(new char[]
{
    'h',
    'w',
    'i',
    'd'
}),
"\":\"",
A_0.g,
"\",\"pc_name\":\"",
Deimos.a.h(),
Deimos.a.b(),
"\",\"os_name\":\"",
Deimos.a.e(),
Deimos.a.b(),
"\",\"arch\":\"",
Deimos.a.f() ? "x64" : "x86",
Deimos.a.b(),
"\",\"rights\":\"",
Deimos.a.d() ? "Admin" : "User",
Deimos.a.b(),
"\",\"version\":\"",
A_0.a,
"\",\"",
```

Figura 11: *Datos de usuario enviados por medio de JSON*

BlackMatter

Resumen

BlackMatter comenzó a distribuirse en julio de 2021. Los operadores de ransomware BlackMatter utilizan técnicas de doble extorsión y se sabe que publican datos confidenciales robados de las víctimas en su sitio web si no se paga el rescate. Proporciona RaaS (ransomware como servicio) y se ha descubierto en un foro un anuncio suyo y que preguntaban por agentes que puedan dar acceso inicial a grandes redes comprometidas: los operadores de BlackMatter pagan a los agentes por el acceso a la red. El ransomware BlackMatter utiliza combinaciones de RSA+ Salsa20 en el proceso de cifrado. Este ransomware añade extensiones acabadas en ".{caracteres alfanuméricos aleatorios}" a los archivos después del cifrado. Deja una nota de rescate que solicita su lectura: "{caracteres alfanuméricos aleatorios}.README.txt".

Evasión y ofuscación

El ransomware BlackMatter elimina las copias de seguridad del dispositivo de la víctima para evitar la restauración del sistema. Termina los procesos relacionados con la productividad, como Outlook, Oracle y Notepad, para que el ransomware pueda cifrar más archivos. Tras su ejecución, también eleva los privilegios a través de una interfaz COM. Utiliza la ofuscación de cadenas y una técnica dinámica de resolución de API Win32.

Comunicación en red

BlackMatter recopila información como la versión del bot, el ID del bot, el nombre de host, el nombre de usuario, la información del disco, el sistema operativo, la arquitectura del sistema y la información de los archivos cifrados. Se comunica a través de HTTPS y utiliza TLS para el cifrado, como se muestra en la siguiente captura de pantalla. Si la carga útil no se comunica con HTTPS, recurre a HTTP para comunicarse con el servidor de mando y control.

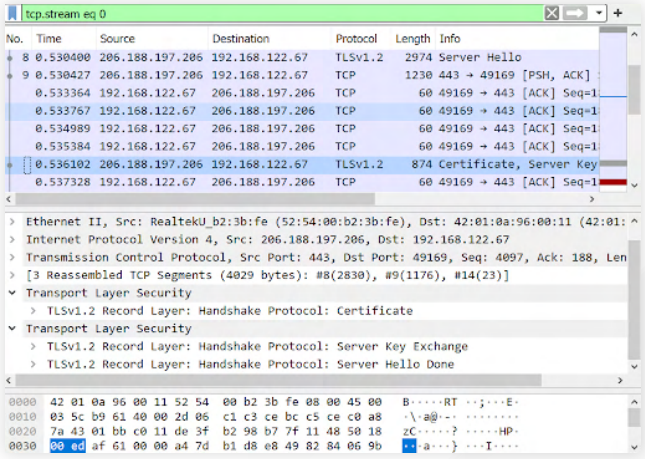

Figura 12: *BlackMatter utiliza TLS para el cifrado*

REvil/Sodinokibi

Resumen

El ransomware REvil, también conocido como Sodinokibi, se detectó por primera vez en abril de 2019 distribuido a través de correos electrónicos de spam, kits de explotación y cuentas RDP comprometidas; Sodinokibi también aprovecha con frecuencia las vulnerabilidades de Oracle WebLogic. Sodinokibi cifra cada archivo y añade la extensión {.caracteres alfanuméricos aleatorios}. Utiliza una combinación de algoritmos de intercambio de claves basados en Salsa20 y ECDH en el proceso de cifrado. Deja una nota de rescate llamada "{caracteres alfanuméricos aleatorios}-readme.txt" y cambia el fondo de escritorio del sistema infectado.

Evasión y ofuscación

REvil tiene la capacidad de utilizar técnicas de desvío UAC para realizar funciones con privilegios elevados en el contexto del proceso actual. REvil también utiliza varias API de Windows para determinar el idioma del sistema por defecto instalado en la máquina y procede a realizar las actividades maliciosas únicamente si el idioma del sistema no se encuentra en la lista blanca preconfigurada. Las cepas de ransomware suelen realizar estas comprobaciones de idioma para evitar infectar a las víctimas en regiones geográficas específicas.

Comunicación en red

REvil recopila el nombre de usuario, el nombre de host, el nombre de dominio, el diseño del teclado, el sistema operativo, la información de la unidad, la arquitectura de la CPU y los detalles de la clave de cifrado del sistema de una víctima y envía esta información a su servidor de mando y control mediante HTTPS. La lista de dominios está presente en la configuración integrada en la carga útil.

Microsoft Office 365

Hemos observado un abuso de sitios de alojamiento legítimos y editores de código en línea, como glitch.me, codesandbox y workers cloudflare, entre otros, para alojar contenido de phishing. Estos sitios sirven a las páginas de phishing a través de HTTPS y ayudan en un rápido desarrollo web. A continuación se muestran algunos ejemplos de estos sitios de phishing.

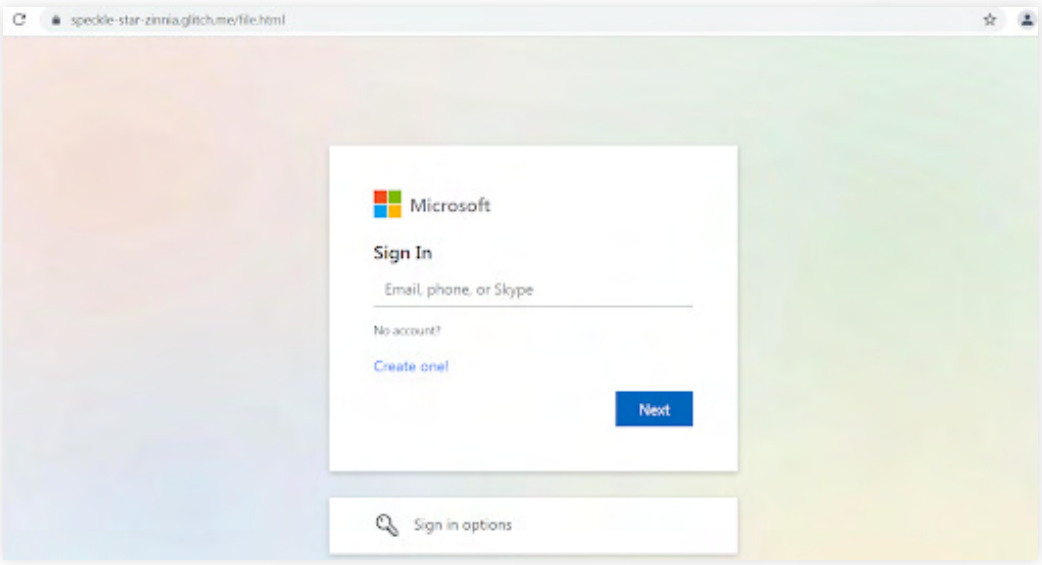

Figura 13: *Ejemplo de sitio de phishing*

Estas páginas de phishing utilizan una ofuscación multicapa, y algunas partes del código fuente se han ofuscado con una mezcla de ofuscadores de JavaScript y codificación Base64.

Figura 14: *Ejemplo de ofuscación multicapa*

A continuación se muestra otro ejemplo de ofuscación multicapa.

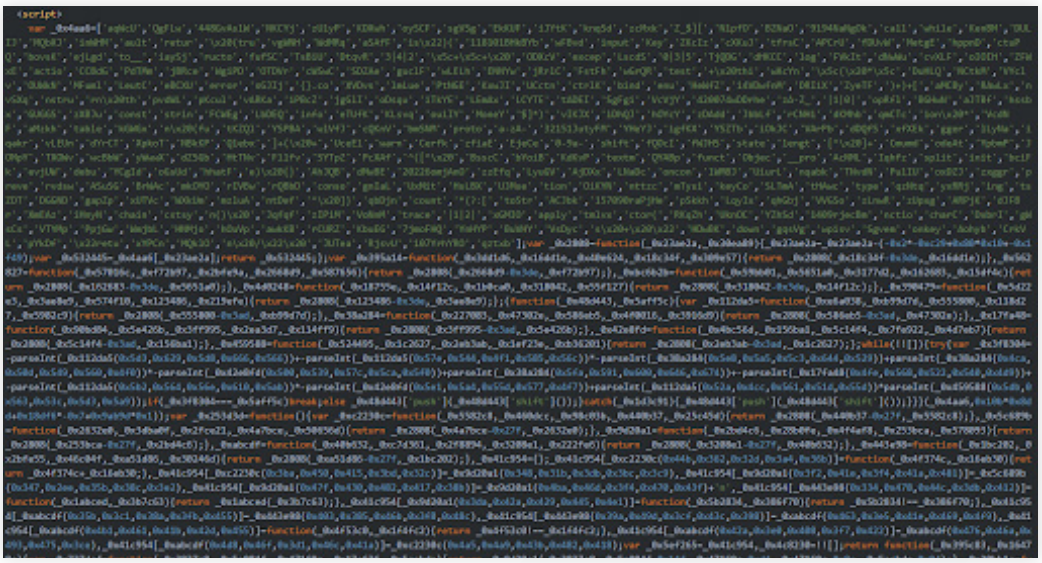

Figura 15: *Ejemplo de ofuscación multicapa*

Estos sitios de phishing también toman huellas digitales de las direcciones IP y redirigen a un sitio legítimo de Microsoft si la IP pertenece a una lista de empresas que aparece en la siguiente captura de pantalla.

```
$.ajax({
        type: "GET",
        url:'https://pro.ip-api.com/json/?key=tPiZVEq18Ne6eQ1&fields=66846719',
        dataType: "json",
        success: function (res) {
        var e833200 = res.as + " " + res.asname + " " + res.isp;
          if (
          e833200.toLowerCase().indexOf("phish".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("Paypal".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("namecheap".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("Google".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("Amazon".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("M247".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("AVAST".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("Kaspersky".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("BullGuard".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("Wintek Corporation".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("McAfee".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("commodo".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("bitdefender".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("Contina".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("Symantec".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("fireeye".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("NetCraft".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("YandexBot".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("barracuda".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("mimecast".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("appriver".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("proofpoint".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("urlscan".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("urlredirectresolver".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("urlresolver".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("bingbot".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("bot".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("trendmicro".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("spam".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("crawler".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("mozilla".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("msnbot".toLowerCase()) >= 0
```

Figura 16: *Lista de empresas*

Amazon

Hemos observado casos de phishing de Amazon a través de HTTPS. Uno de estos casos se muestra en la siguiente captura de pantalla. Podemos ver que la región de entrega ha sido predefinida a los Estados Unidos, lo que proporciona información sobre el objetivo de esta campaña de phishing.

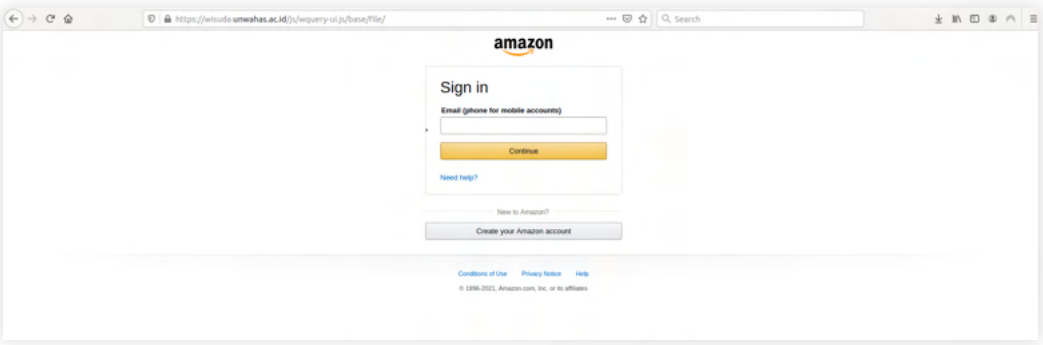

Figura 17: *Caso de phishing de Amazon a través de HTTPS*

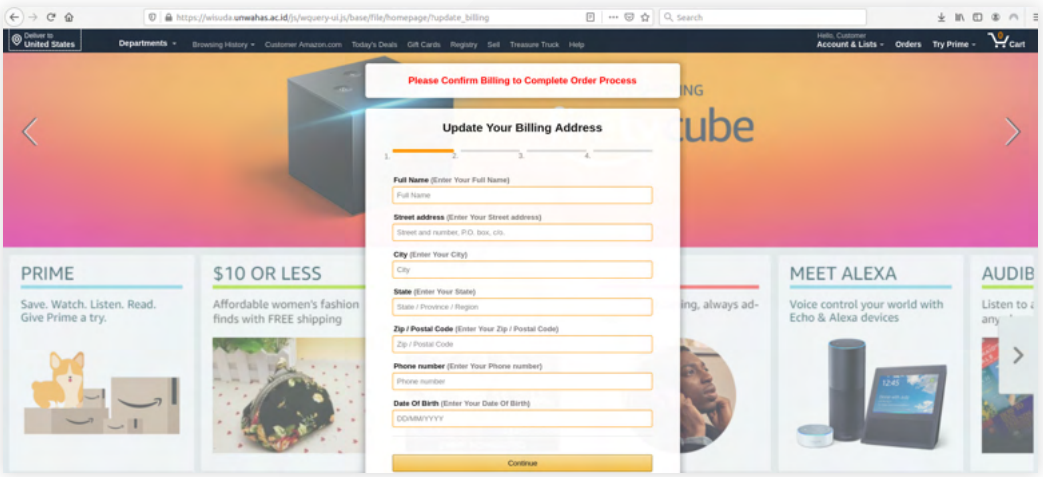

Figura 18: *Caso de phishing de Amazon a través de HTTPS*

A continuación se puede ver la página desfigurada por el atacante en la ubicación del sitio web de alojamiento de phishing de Amazon.

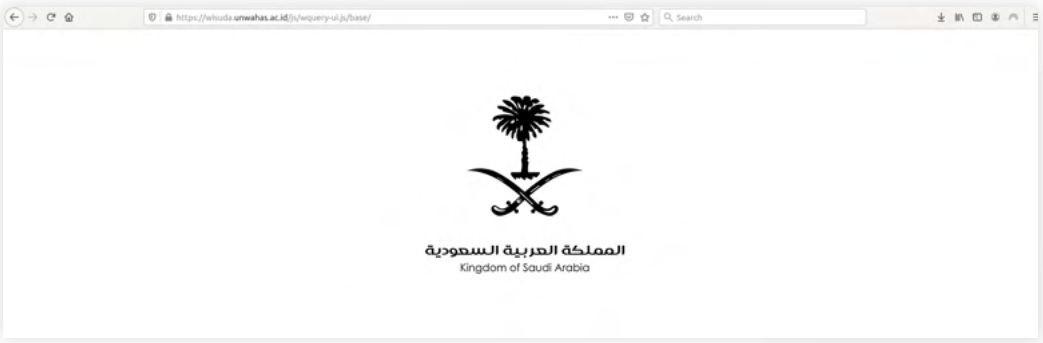

Figura 19: *Página desfigurada por el atacante*

OneDrive

Hemos observado que los atacantes sirven páginas de phishing de OneDrive a través de HTTPS. Estas se sirvieron desde sitios web comprometidos que alojaban el contenido de phishing. El código fuente está cifrado con la codificación hexadecimal básica para evadir la detección de los escáneres de contenido de phishing.

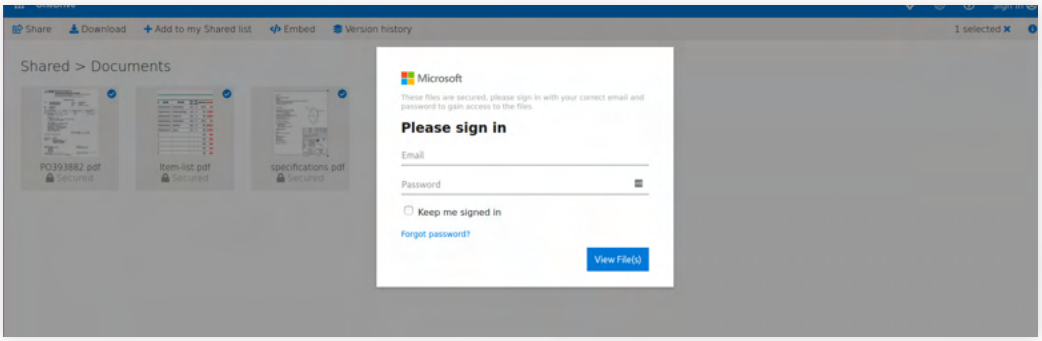

Figura 20: *Caso de phishing de OneDrive a través de HTTPS*

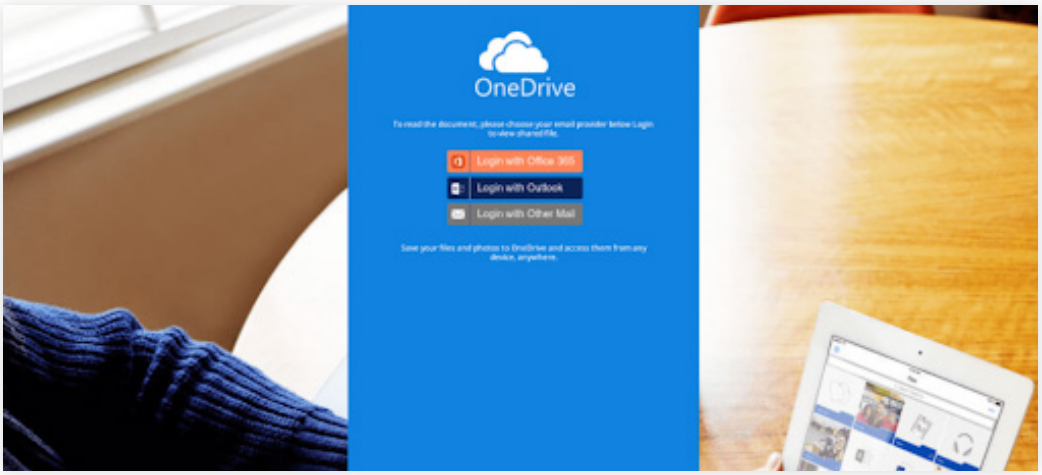

Figura 21: *Caso de phishing de OneDrive a través de HTTPS*

Figura 22: *Parte codificada del código fuente*

Telegram

Hemos sido testigos de casos de clientes web no oficiales de Telegram que utilizan HTTPS. Estos clientes web no pueden garantizar la seguridad. Estas páginas de phishing solicitan el número de teléfono del usuario y envían un OTP al número de teléfono del usuario. Una vez que el usuario introduce el OTP en el sitio web no oficial, el cliente web utiliza la API de Telegram para recuperar el contenido del usuario y lo envía al usuario. Al hacerlo, no hay garantías sobre cómo serán utilizados los mensajes del usuario, la lista de contactos y otros detalles por parte de los clientes web maliciosos. A continuación se muestra un ejemplo de tal sitio web.

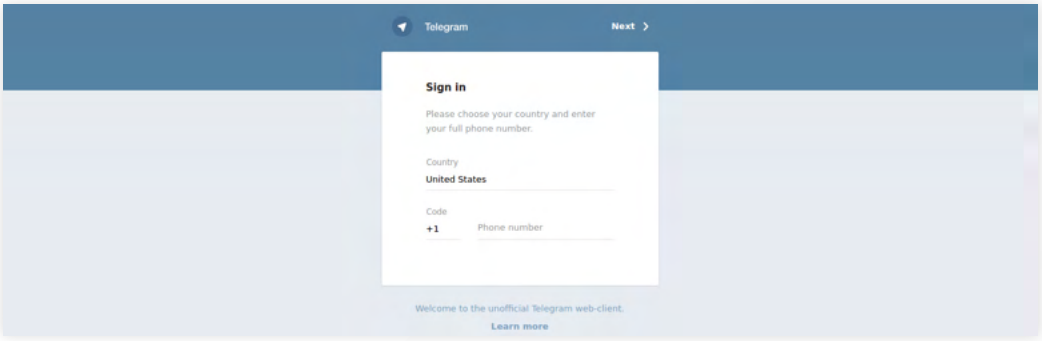

Figura 23: *Caso de cliente web no oficial de Telegram mediante HTTPS*

El fundador de Telegram recomendó usar la app oficial de Telegram para garantizar la seguridad.

Figura 24: *Caso de phishing de OneDrive a través de HTTPS*

PayPal

Hemos observado actividad de phishing de PayPal a través de HTTPS. En el siguiente caso, un sitio web de compras tiene una opción de pago de PayPal comprometida.

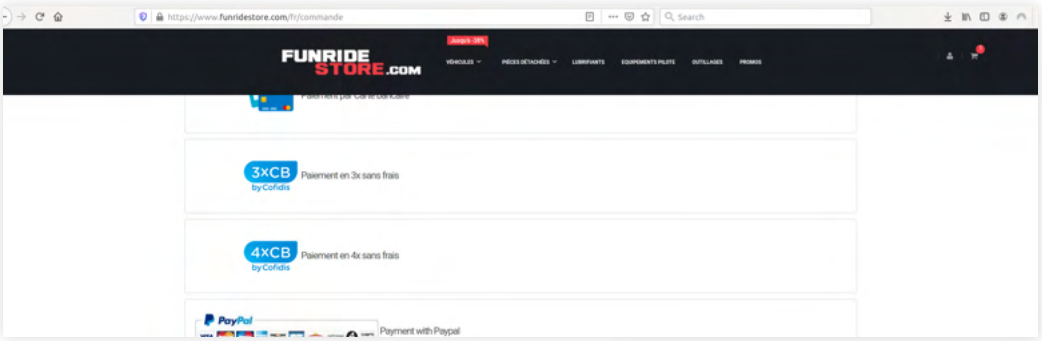

Figura 25: *Caso de actividad de phishing de PayPal a través de HTTPS*

Si el usuario añade artículos a la cesta de la compra, se le pedirá información de envío y de contacto. Tras introducir los datos, el usuario dispondrá de diferentes opciones de pago. El enlace de pago de PayPal que se muestra aquí está comprometido. Si el usuario elige la opción de PayPal, se le llevará a la página de phishing que aparece a continuación.

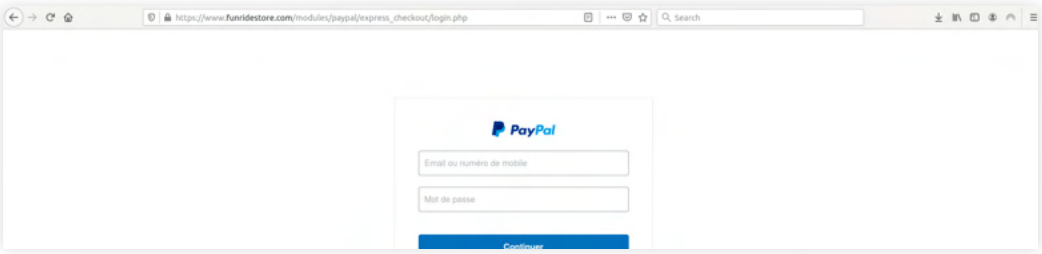

Figura 26: *Página de phishing de PayPal*

Si se introducen las credenciales de PayPal, el usuario será redirigido a la URL legítima de PayPal, donde podrá iniciar sesión y completar la compra.

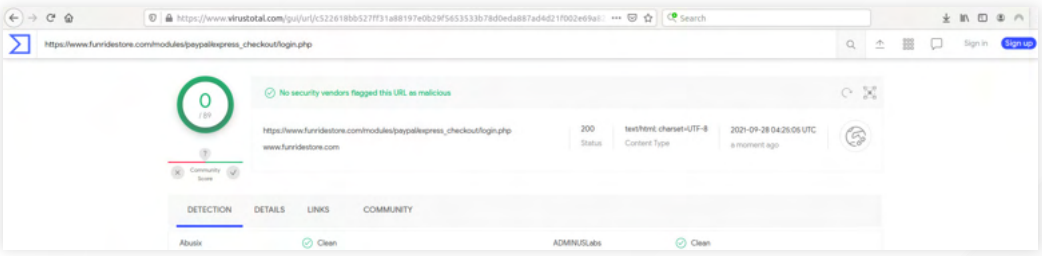

Figura 27: *Página de phishing de PayPal*

Este es un interesante ejemplo de ingeniería social. Muestra una página de compras legítima y la ubicación del vínculo de phishing de PayPal en una ubicación donde los compradores esperarían un vínculo legítimo. Los enlaces de pago con tarjeta de crédito dirigen a URL legítimas, mientras que solo el enlace de PayPal se ha visto comprometido.

Normalmente vemos que los adversarios utilizan herramientas como Cobalt Strike, Mimikatz, LaZagne, entre otras, en ataques dirigidos para propagarse lateralmente, exfiltrar datos y realizar otras actividad de mando y control. Cobalt Strike sigue siendo una de las herramientas más utilizadas en muchos de estos ataques dirigidos.

Cobalt Strike

Se han observado 24 410 bloqueos de descarga y 172 568 bloqueos de devolución de llamada a través de TLS.

Resumen

Cobalt Strike es una herramienta comercial para simulaciones de ataques de adversarios y operaciones del equipo rojo. Se trata de un software con funciones completas y perfiles de mando y control predefinidos y configurables que le permiten cambiar su comportamiento e indicadores de red para simular las tácticas, técnicas y procedimientos de diferentes familias de malware utilizadas en ataques del mundo real. Aunque es una herramienta comercial legítima, los adversarios la han utilizado repetidamente en ataques reales. Se sabe que varios grupos APT, como los siguientes, utilizan el marco Cobalt Strike:

- APT19
- DarkHydrus
- CopyKittens
- APT32
- Cobalt Group
- APT29
- Leviathan
- FIN6

Cobalt Strike es un software malicioso sin archivos compatible con shellcode multietapa que se puede utilizar para múltiples propósitos

Comunicación en red

Cobalt Strike puede configurarse para comunicarse a través de uno o varios protocolos mediante una función denominada perfiles de mando y control maleables:

- DNS (registros TXT, A y AAAA)
- HTTP/HTTPS
- SMB (tuberías nombradas)
- TCP

Técnicas de evasión

Cobalt Strike suele ser la carga útil que se deposita en la etapa final y que también utiliza tuberías nombradas, que son sockets que permiten la comunicación entre procesos o incluso hosts. Las funciones posteriores a la intrusión control de Cobalt Strike incluyen keyloggers, Mimikatz y módulos de captura de pantalla.

Movimiento lateral con credenciales robadas

Cobalt Strike usó credenciales robadas para interactuar con un recurso compartido de red remoto mediante Server Message Block (SMB), iniciar sesión en un ordenador mediante el protocolo de escritorio remoto (RDP) e iniciar sesión en un servicio específicamente diseñado para aceptar conexiones remotas, como Telnet, SSH y VNC.

PoshC2

Se han observado 98 591 bloqueos de devolución de llamada a través de TLS.

PoshC2 es un marco de mando y control compatible con el proxy que se utiliza para ayudar a los probadores de penetración con equipos rojos, posintrusión y movimiento lateral.

PoshC2 está escrito principalmente en Python3. PoshC2 viene preconfigurado con implantes PowerShell/C# y Python2/Python3 con cargas útiles escritas en código fuente PowerShell v2 y v4, C++ y C#. Esto permite la funcionalidad de mando y control en una amplia gama de dispositivos y sistemas operativos, incluidos Windows, *nix y OSX.

PoshC2 se puede utilizar con SharpSocks, que permite el proxy Socks de túnel HTTPS inverso de C#, permitiendo así que el tráfico de mando y control se ejecute sobre HTTPS.

Ursnif

Se han observado 336 540 bloqueos de descarga y 87 821 bloqueos de devolución de llamada a través de TLS.

Resumen

Ursnif (también conocido como Gozi) es un troyano bancario, pero tiene variantes que incluyen componentes como puertas traseras, spyware, inyectores de archivos y más. Se identificó por primera vez en 2006 y ha estado en funcionamiento desde entonces de manera ininterrumpida. El malware se distribuye mediante campañas de phishing específicas para cada país.

Mecanismo de persistencia

Ursnif utiliza dos mecanismos para persistir:

1. Crear una nueva tarea programada (con el nombre “Power<cualquier_palabra>" (por ejemplo, PowerSgs).
2. Si por alguna razón no se consigue, utiliza la clave de registro "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run" para poder persistir durante el reinicio del sistema.

Actividad en la red

Una vez que se ha asentado en la máquina, inicia su secuencia de trabajo principal, que continuamente sondea el servidor de mando y control para los comandos. Este malware recoge información del usuario, por ejemplo el propio "usuario", el "servidor" y la "ID" como valores hash, y mediante el valor "uptime" indica cuánto tiempo ha estado funcionando el dispositivo. "DNS" es el nombre del ordenador y "whoami" es el nombre completo del usuario. En ocasiones se ve al malware contactando y transmitiendo información a su mando y control mediante HTTPS.

Dridex

Se han observado 50 088 bloqueos de descarga y 11 167 bloqueos de devolución de llamada a través de TLS.

Resumen

Dridex, también conocido como Bugat y Cridex, es un troyano especializado en el robo de credenciales bancarias. Hizo su primera aparición en 2011, evolucionando a lo largo de los años, y apareció en varias campañas de phishing que utilizaban documentos de Microsoft Word y Excel como cargas útiles.

Técnicas de evasión

Dridex se distribuye por la red de bots Cutwail o el kit de intrusión RIG. Dridex también es conocido por utilizar campañas de phishing basadas en temas de actualidad, como el lanzamiento de SpaceX, por ejemplo.

Comunicación en red

La carga útil del documento Dridex contiene mando y control para la siguiente etapa. Se contacta con mando y control mediante HTTPS para descargar un archivo de biblioteca de enlaces dinámicos (DLL), que es la carga útil final que infecta al usuario y contacta más mando y control. Una variante de Dridex, también conocido como DoppelDridex en sus recientes campañas, ha comenzado a utilizar cdn.discordapp.com y Slack como su mando y control que contiene el archivo DLL.

Descubra cómo **Zscaler** puede inspeccionar todo su tráfico SSL sin afectar al rendimiento o crear problemas de cumplimiento. También puede comprobar su propia capacidad para inspeccionar el tráfico SSL/TLS por medio de 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 investigar 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. Asimismo 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 portal, **research.zscaler.com**.

Acerca de 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. Presente en más de 150 centros de datos de todo el mundo, Zero Trust Exchange se basa en un perímetro de servicio de acceso seguro (SASE, en su sigla inglesa) y es la mayor plataforma de seguridad en la nube en línea del mundo.
Descubra más en zscaler.com Puede seguirnos en Twitter **@zscaler.**

zscaler™