THREAT REPORT

PRIMER CUATRIMESTRE DE 2022

WeLiveSecurity.com
@ESETresearch
ESET GitHub

Digital Security
Progress. Protected.

CONTENIDO

PRÓLOGO

¡Bienvenido a la edición del ESET Threat Report para el primer cuatrimestre de 2022!

Luego de haber pasado más de dos años protegiéndonos de una pandemia mundial, recibimos una recompensa: ¡la guerra! Se han desencadenado varios conflictos en distintas partes del mundo, pero para nosotros, éste es diferente. Justo al otro lado de las fronteras orientales de Eslovaquia, donde ESET tiene su Casa Matriz y varias oficinas, los ucranianos luchan por sus vidas y su soberanía en esta guerra no provocada, enfrentándose a un adversario que posee armas nucleares. Como leerá en las siguientes páginas, Ucrania no solo debe resistir los ataques en el mundo físico, sino también en el espacio cibernético.

Nuestra historia destacada relata varios ciberataques relacionados con la guerra en curso que los investigadores de ESET analizaron o ayudaron a mitigar. Entre ellos se encuentra la resurrección del infame malware Industroyer, cuyo objetivo son las subestaciones eléctricas de alto voltaje.

Poco antes de la invasión rusa, la telemetría de ESET registró la primera de dos caídas pronunciadas de los ataques al protocolo RDP. El descenso de estos ataques se produjo tras dos años de crecimiento constante y, como explicamos en la sección Exploits, este giro en los acontecimientos podría estar relacionado con la guerra en Ucrania. Incluso con esta caída, casi el 60% de los ataques al RDP vistos en el primer cuatrimestre de 2022 se originaron en Rusia. Otro efecto secundario de la guerra: mientras que en el pasado las amenazas de ransomware tendían a evitar los objetivos situados en Rusia, en este período, según nuestra telemetría, Rusia fue el país más atacado. Incluso detectamos variantes de malware de bloqueo de pantalla que utilizan el saludo nacional ucraniano "Slava Ukraini" ("Gloria a Ucrania").

No es de extrañar que la guerra también haya sido notablemente aprovechada por el spam y las amenazas de phishing. Inmediatamente después de la invasión del 24 de febrero, los estafadores empezaron a aprovecharse de las personas que intentaban apoyar a Ucrania, utilizando como señuelos organizaciones benéficas y recaudadores de fondos ficticios. Ese mismo día, notamos un gran pico en las detecciones de spam. También podemos confirmar que Emotet (el infame malware, que se propaga principalmente a través de correos electrónicos de spam) regresó tras los intentos de desmantelamiento del año pasado, y se ha disparado de nuevo en nuestra telemetría. Sus operadores lanzaron una campaña tras otra de spam, por lo que las detecciones de Emotet se multiplicaron más de cien veces.

Nuestra telemetría ha observado, desde luego, muchas otras amenazas no relacionadas con la guerra entre Rusia y Ucrania; lo invito a leer la sección Estadísticas y Tendencias para conocer el panorama completo. Los últimos meses también han estado repletos de interesantes hallazgos de nuestro Equipo de Investigación. Los expertos de ESET descubrieron, entre otras cosas, malware que aprovecha vulnerabilidades en los controladores del kernel; vulnerabilidades de alto impacto en la UEFI; malware para criptomonedas dirigido a dispositivos Android e iOS; y las campañas de Mustang Panda, Donot Team, Winnti Group y el grupo de APT TA410.

Los investigadores de ESET estuvieron presentes en las conferencias S4x22, CARO Workshop, Botconf y NorthSec, donde presentaron sus análisis detallados de Industroyer2, las filtraciones en las redes aisladas por barreras de aire y las campañas desplegadas por los grupos de APT InvisiMole, OilRig, MuddyWater, FreshFeline y TA410. En lo que respecta a los meses venideros, nos gustaría invitarlo a las charlas de ESET en RSA, REcon, Virus Bulletin y muchas otras conferencias.

Le deseo una lectura esclarecedora.

Roman Kováč
ESET Chief Research Officer

RESUMEN EJECUTIVO

HISTORIA DESTACADA

Ciberataques en Ucrania
El Equipo de Investigación de ESET descubrió varios nuevos ataques wiper desplegados en Ucrania y analizó el regreso del infame Industroyer, todos ellos relacionados con la guerra en curso.

ACTIVIDAD DE GRUPOS DE APT

Donot Team
El Equipo de Investigación de ESET analizó las recientes campañas de Donot Team (también conocido como APT-C-35 y SectorE02), que se centra en el espionaje cibernético y tiene como principal objetivo de ataque Asia del Sur.

Mustang Panda
El Equipo de Investigación de ESET descubrió una campaña de ciberespionaje aún en curso llevada a cabo por el grupo de APT Mustang Panda, en la que utilizan Hodur, una variante de Korplug anteriormente no documentada.

Winnti Group
El Equipo de Investigación de ESET detectó nuevas variantes de PipeMon utilizadas por el grupo Winnti.

TA410
El Equipo de Investigación de ESET reveló un perfil detallado de TA410, un grupo paraguas de ciberespionaje vagamente vinculado con APT10.

ESTADÍSTICAS Y TENDENCIAS

Categoría	3º cuatrimestre de 2021 / 1º cuatrimestre de 2022	Qué se destacó en el 1º cuatrimestre de 2022
Amenazas totales	+20,1% ↑	Las campañas de Emotet incrementan la actividad general de las amenazas
Infostealers	+12,0% ↑	JS/Spy.Banker alias Magecart se vuelve más prevalente
Ransomware	-4,3% ↓	Rusia es objetivo cada vez más frecuente del ransomware
Downloaders	+121,5% ↑	Emotet lanza campañas masivas de spam
Amenazas para criptomonedas	-29,3% ↓	Disminución general de la actividad de las amenazas para criptomonedas
Amenazas web	-1,8% →	La cantidad de detecciones de URL de phishing se dispara en marzo
Amenazas por correo electrónico	+36,8% ↑	Emotet satura las bandejas de entrada con documentos maliciosos
Amenazas para Android	+8,0% ↑	El spyware para Android se extiende cada vez más
Amenazas para macOS	-14,9% ↓	Descenso en todas las categorías de amenazas monitoreadas
Ataques al RDP	-40,8% ↓	Los ataques al RDP experimentan el primer descenso desde 2020

HISTORIA DESTACADA

Ciberataques en Ucrania

Equipo de Investigación de ESET

Los investigadores de ESET descubrieron varios nuevos ataques de wipers desplegados en Ucrania y analizaron el regreso del infame Industroyer, todos ellos relacionados con la guerra en curso.

En la víspera de la invasión rusa de Ucrania, los investigadores de ESET hallaron un nuevo wiper (malware de borrado de datos) desplegado ese mismo día, que se instaló en cientos de máquinas de al menos cinco organizaciones de dicho país. El incidente comenzó pocas horas después de que una serie de ataques de denegación de servicio distribuido (DDoS) dejara fuera de servicio a varios sitios web importantes ucranianos. El wiper fue visto por primera vez justo antes de las 17:00 hora local (15:00 UTC) del 23 de febrero. Los investigadores de ESET se quedaron hasta tarde analizando el malware y publicaron el descubrimiento en *Twitter* [1], sin saber lo que los medios de comunicación mundiales anunciarían a la mañana siguiente como noticia de último momento.

Los investigadores de ESET están seguros de que las organizaciones afectadas fueron comprometidas mucho antes del despliegue del wiper. Se basan en estos tres hallazgos:

- Los atacantes utilizaron un certificado de firma de código genuino a nombre de una empresa llamada Hermetica Digital Ltd., emitido el 13 de abril de 2021. Esa es también la razón por la que ESET decidió llamar al malware *HermeticWiper* [2], como se sugirió en una respuesta al *tweet del Equipo de Investigación de ESET* [3].
- Aunque los vectores de acceso iniciales variaron de una organización a otra, el despliegue de HermeticWiper a través de un objeto de directiva de grupo (GPO) en al menos una instancia sugiere que los atacantes tenían acceso previo a uno de los servidores de Active Directory de esa víctima.
- Su marca de fecha y hora de compilación muestra que el wiper fue creado el 28 de diciembre de 2021.

Cronología de los ataques detectados por los investigadores de ESET durante el comienzo de la invasión rusa a Ucrania

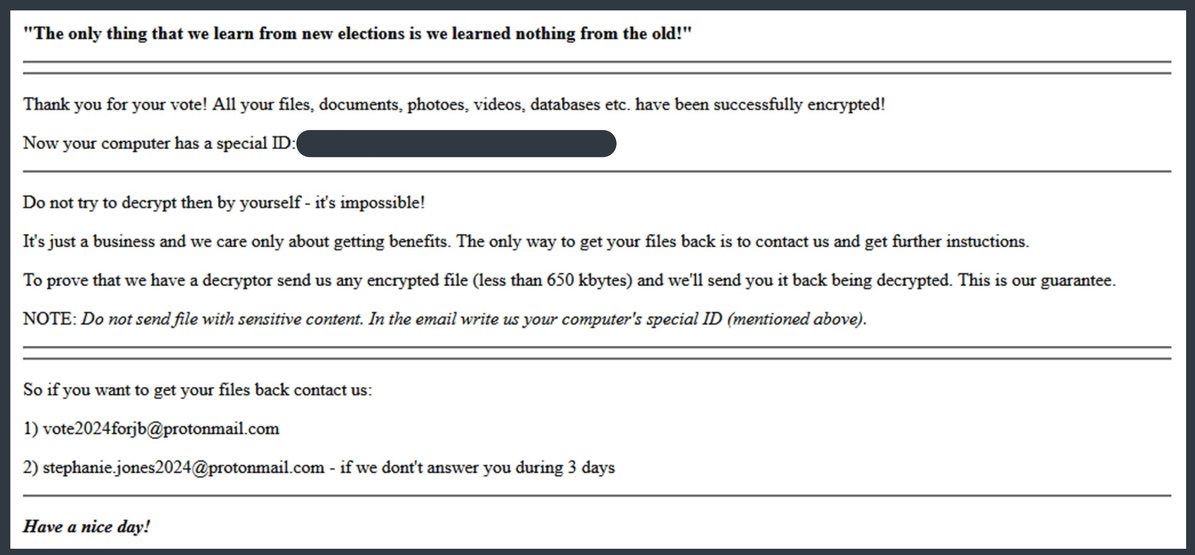
HermeticWiper sobrescribe varias ubicaciones (como el registro de arranque maestro y la tabla maestra de archivos) en los sistemas comprometidos con bytes aleatorios; hace lo mismo con los vínculos simbólicos y los archivos grandes de las carpetas Mis Documentos y Escritorio. Borra recursivamente las carpetas y los archivos de las carpetas Windows, Archivos de Programa, Archivos de Programa(x86), PerfLogs, Boot, System Volume Information y AppData. El wiper incluso se borra a sí mismo del disco sobrescribiendo su propio archivo con bytes aleatorios. Esta medida antiforense tiene probablemente la finalidad de impedir el análisis posterior al incidente. Aunque la máquina se reinicia; no podrá arrancar porque la mayoría de los archivos fueron borrados. Los investigadores de ESET creen que no es posible recuperar las máquinas afectadas a menos que se hayan hecho copias de seguridad.

Campaña de Hermetic con falso ransomware

Mientras buscaban otras muestras firmadas por el mismo certificado de firma de código, los investigadores de ESET encontraron una nueva familia de malware que denominaron *HermeticWizard* [4]. Se trata de un gusano que se desplegó en un sistema ucraniano a las 14:52:49 UTC del 23 de febrero de 2022. Primero, HermeticWizard intenta encontrar otras máquinas en la red local. Recopila las direcciones IP locales y luego intenta conectarse a ellas (solo si son locales) para ver si aún tiene acceso. Cuando accede a una máquina, instala sus módulos de propagación. Por último, descarga HermeticWiper y lo ejecuta. Todo el mecanismo de propagación es muy rudimentario, lo que implica que el despliegue de este ataque fue apresurado.

Los investigadores de ESET también observaron que en Ucrania se estaba utilizando HermeticRansom (un "ransomware" escrito en Go) al mismo tiempo que la campaña de HermeticWiper. HermeticRansom fue reportado por primera vez en las primeras horas de la mañana UTC del 24 de febrero de 2022, en un *tweet* [5] de AVAST. La telemetría de ESET muestra un despliegue mucho menor en comparación con HermeticWiper. El ransomware se desplegó al mismo tiempo que HermeticWiper, posiblemente para ocultar las acciones del wiper. Dado que las motivaciones de HermeticRansom no eran financieras, como es habitual en el ransomware, los investigadores de ESET lo denominaron "falso ransomware".

En una ocasión, los investigadores de ESET observaron que HermeticRansom se desplegaba a través de un objeto de directiva de grupo (GPO), al igual que HermeticWiper. Los atacantes dejaron unas cuantas cadenas en el binario de HermeticRansom, donde hacen referencia al presidente estadounidense Biden y a la Casa Blanca. El mensaje de rescate que se muestra a la víctima una vez cifrados los archivos menciona el dicho "¡Lo único que aprendemos de las nuevas elecciones es que no aprendimos nada de las anteriores!".



"The only thing that we learn from new elections is we learned nothing from the old!"

Thank you for your vote! All your files, documents, photoes, videos, databases etc. have been successfully encrypted!

Now your computer has a special ID: [redacted]

Do not try to decrypt then by yourself - it's impossible!

It's just a business and we care only about getting benefits. The only way to get your files back is to contact us and get further instuctions.

To prove that we have a decryptor send us any encrypted file (less than 650 kbytes) and we'll send you it back being decrypted. This is our guarantee.

NOTE: *Do not send file with sensitive content. In the email write us your computer's special ID (mentioned above).*

So if you want to get your files back contact us:

1) vote2024forjb@protonmail.com

2) stephanie.jones2024@protonmail.com - if we dont't answer you during 3 days

Have a nice day!

La nota de rescate, en la que se menciona un dicho

IsaacWiper

El 24 de febrero de 2022, los investigadores de ESET detectaron otro nuevo wiper en una red gubernamental ucraniana y lo llamaron IsaacWiper. Se observó en una organización que no había sido comprometida por HermeticWiper. No tiene ninguna similitud de código con HermeticWiper y es mucho menos sofisticado. Considerando la cronología, es posible que ambos estén relacionados, pero los investigadores de ESET aún no han encontrado ninguna conexión sólida. Si su marca de tiempo de compilación ejecutable portátil (PE), que es del 19 de octubre de 2021, no fue manipulada, IsaacWiper podría haber sido utilizado en otras operaciones meses atrás.

IsaacWiper comienza enumerando las unidades físicas; luego borra los primeros 0x10000 bytes de cada disco usando el generador de números pseudoaleatorios (PRNG) Mersenne Twister. A continuación, enumera las unidades lógicas y borra recursivamente todos los archivos de cada disco con bytes aleatorios también generados por el PRNG Mersenne Twister. Es interesante notar que borra recursivamente los archivos en un solo hilo, lo que significa que le llevaría mucho tiempo borrar un disco grande. El 25 de febrero de 2022, los atacantes lanzaron una nueva versión de IsaacWiper con registros de depuración. Esto puede indicar que los atacantes no lograron borrar algunas de las máquinas objetivo y añadieron mensajes de registro para entender lo que estaba sucediendo.

CaddyWiper

El 14 de marzo de 2021, los investigadores de ESET descubrieron otro wiper destructivo de borrado de datos utilizado en ataques contra organizaciones ucranianas y que se detectó en varias docenas de sistemas pertenecientes a un número limitado de organizaciones. *CaddyWiper* [6], tal y como lo denomina ESET, no tiene grandes similitudes de código con HermeticWiper o IsaacWiper. Sin embargo, al igual que con HermeticWiper, las pruebas sugieren que los actores responsables de CaddyWiper se habían infiltrado en las redes de los objetivos antes de desplegar el

malware.

A diferencia de *NotPetya* [7], otro falso ransomware, estos wipers se desplegaron en un número limitado de organizaciones de manera selectiva. Los investigadores de ESET creen que, a diferencia del brote anterior, los atacantes dirigieron estas campañas de wipers a organizaciones específicas, tal vez con el objetivo de perjudicar su capacidad de responder adecuadamente a la invasión. El Equipo de Investigación de ESET detectó víctimas de los sectores financiero, de medios de comunicación y gubernamental; y según sus conclusiones, atribuimos CaddyWiper y HermeticWiper al infame grupo Sandworm.

Incluso poco antes de la guerra, Ucrania había sido objeto de otros ataques. El ataque de *DDoS* [8] mencionado precedió a un *ataque contra Viasat* [9] que tuvo como objetivo la red de Internet por satélite de la empresa y afectó los módems residenciales en Ucrania. Según las autoridades ucranianas, este ataque obstaculizó seriamente su comunicación al principio de la guerra. En enero, varios sitios web de diversas entidades gubernamentales ucranianas sufrieron alteraciones con un mensaje que advertía "tengan miedo y esperen lo peor". Poco después, el Centro de Inteligencia de Amenazas de Microsoft publicó una *entrada de blog* [10] sobre un malware destructivo llamado *WhisperGate* [11] dirigido a organizaciones ucranianas. Luego de inspeccionar la información relevante, los investigadores de ESET creen que las alteraciones de los sitios y el ataque de WhisperGate están conectados.

El regreso de Industroyer

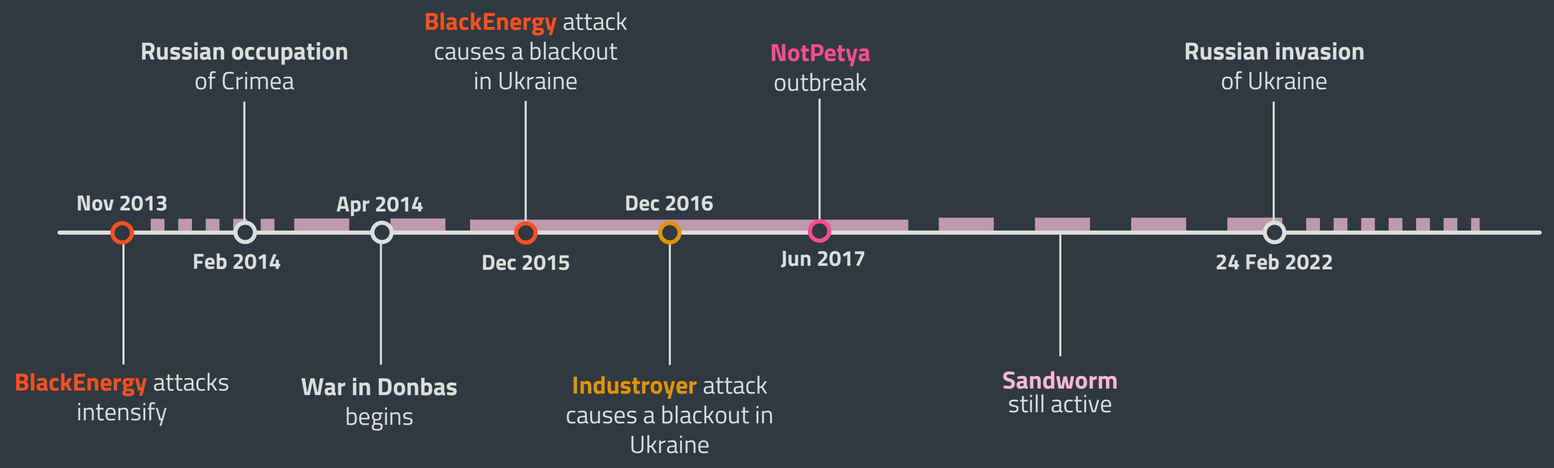
Si nos remontamos al pasado, Ucrania es el país que sufrió el primer ataque de malware de la historia diseñado específicamente para atacar las redes eléctricas, el 23 de diciembre de 2016. Los investigadores de ESET descubrieron este malware desplegado por Sandworm y lo denominaron *Industroyer* [12]. Su nivel de sofisticación solo era superado por Stuxnet y su objetivo de ataque era la subestación de transmisión eléctrica del norte de Kiev. Durante más de cinco años, los investigadores de ESET se han preguntado por qué Industroyer, con lo sofisticado que era, no volvió a desplegarse.

En abril de este año, la espera terminó cuando colaboramos con *CERT-UA* [13] para responder a un incidente cibernético que afectó a un proveedor de energía en Ucrania, ayudando a remediar y proteger esta infraestructura crítica. Esta colaboración no solo permitió desarticular el ataque, sino también descubrir una nueva variante de Industroyer que, junto con CERT-UA, denominamos *Industroyer2* [14].

En este caso, los atacantes de Sandworm intentaron desplegar Industroyer2 en subestaciones eléctricas de alta tensión en Ucrania. Además de Industroyer2, Sandworm utilizaba varias familias de malware destructivo, entre las que se encontraban CaddyWiper, ORCSHRED, SOLOSHRED y AWFULSHRED. Los investigadores de ESET no saben de qué forma los atacantes comprometieron a la víctima inicial, ni cómo pasaron de la red informática a la red del Sistema de Control Industrial (ICS). De haber tenido éxito, este ataque podría haber dejado sin electricidad a dos millones de personas, *afirmó Farid Safarov* [15], viceministro de Energía de Ucrania.

Malware destructivo para Linux y Solaris

Industroyer2 se compiló el 23 de marzo de 2022, según su marca de tiempo PE, y se configuró para desplegarse mediante una tarea programada a las 16:10:00 UTC del 8 de abril de 2022, lo que sugiere que los agresores habían planeado el ataque previsto durante más de dos semanas. En coordinación con Industroyer2, los atacantes desplegaron una nueva versión del malware destructivo CaddyWiper en la red del ICS.



Ataques de alto perfil, detectados y analizados por los investigadores de ESET, que tenían como objetivo Ucrania mucho antes de la guerra

Además del malware para Windows, los atacantes también desplegaron malware destructivo en sistemas Linux y Solaris. Cabe notar que los wipers para estos sistemas operativos son muy poco frecuentes. Los investigadores de ESET creen que su finalidad era ralentizar el proceso de recuperación y evitar que los operadores de la compañía energética recuperaran el control de las consolas del ICS a tiempo. También se desplegó un wiper en la máquina donde se ejecutó Industroyer2, probablemente para cubrir huellas.

Cómo ayudamos

Además del *apoyo humanitario* [16], ESET comparte sus investigaciones y proporciona conocimientos de seguridad a los numerosos organismos europeos y mundiales que se esfuerzan por abordar, resolver y mitigar las ciberamenazas derivadas de la guerra entre Rusia y Ucrania. En el presente artículo solo se incluye una pequeña parte de dichos hallazgos.

Sin embargo, es importante señalar que los ciberataques relacionados con esta guerra no están dirigidos únicamente a los organismos gubernamentales, sino también a las empresas y a la población general de Ucrania, como se vio en *muchos ejemplos* [17] de *señuelos de phishing* [18x] que aprovecharon la situación en Ucrania, y que fueron detectados por ESET.

Los ciberataques más destacados del pasado

Ucrania ha estado en la mira de los ataques cibernéticos desde hace años. Estos son los ejemplos más notables de grupos de APT de estados-nación enfocados en Ucrania que fueron *rastreados por los investigadores de ESET* [19] exhaustivamente *con el paso de los años* [4]:

Sandworm

Desde finales de 2013 y principios de 2014, la telemetría de ESET observó cómo Sandworm *intensificaba sus ataques* [20] en Ucrania utilizando el malware BlackEnergy. Esto sucedió poco antes de la ocupación rusa de Crimea y la posterior guerra en Donbás. En diciembre de 2015, el grupo *atacó la red eléctrica de Ucrania* [21], lo que se convirtió en el primer apagón de la historia causado por un ciberataque, dejando los hogares de unos 230.000 ucranianos a oscuras. Un año después, el grupo *desplegó Industroyer* [12]. En los años siguientes, Sandworm dividió sus actividades: el *clúster GreyEnergy* [22] continuó con los ataques al sector energético, mientras que el *clúster TeleBots* [23] llevó a cabo ataques principalmente contra el sector financiero en Ucrania; por ejemplo, el desestabilizador *brote de NotPetya* [7] en 2017. Hasta el día de hoy, NotPetya es financieramente el ciberataque más devastador de la historia.

Sednit

Además de acosar a Ucrania, este grupo también es conocido por atacar a los países de la OTAN. La sofisticación técnica de Sednit se reveló en 2018 en un análisis de investigación de ESET donde se detalló cómo el grupo conseguía establecer una persistencia tan resistente en los sistemas comprometidos mediante el *uso de LoJax* [24], el primer rootkit para la UEFI encontrado activo en el mundo real.

Gamaredon

Este grupo, que opera desde 2013, ha sido el más activo de Ucrania en los últimos años. *Gamaredon despliega* [25] ataques de gran volumen y de fuerza bruta, y mantiene su malware en constante desarrollo. Su objetivo es penetrar en las organizaciones seleccionadas, normalmente utilizando campañas de phishing dirigido, para llevar a cabo acciones de ciberespionaje. A lo largo de los años y en algunas ocasiones, los investigadores de ESET han observado que este grupo pasaba algunos de sus objetivos al grupo InvisiMole.

InvisiMole

InvisiMole también está activo desde 2013, pero en marcado contraste con Gamaredon, *su modus operandi* [26] es altamente encubierto, y se centra en el espionaje en Ucrania y Europa del Este. Sus operadores realizan ataques de ciberespionaje muy selectivos contra instituciones gubernamentales, entidades militares y misiones diplomáticas.

Turla

Este grupo de espionaje es conocido por su *complejo malware* [27]. Se cree que ha estado operando desde al menos 2008, cuando logró infiltrarse en el ejército estadounidense. También ha participado en importantes ataques contra muchas entidades gubernamentales en Europa y el Medio Oriente; sus principales objetivos son organizaciones gubernamentales y militares.

Buhtrap

Este grupo es conocido por sus ataques a instituciones financieras y empresas en Rusia y Ucrania. Desde finales de 2015, los investigadores de ESET *han observado* [28] un cambio en el perfil de los objetivos tradicionales del grupo: de ser un grupo puramente criminal que perpetraba ciberdelitos para obtener beneficios económicos, su conjunto de herramientas se ha ampliado con malware utilizado para realizar ciberespionaje.

NOTICIAS DEL LABORATORIO

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

Exploits

Controladores del kernel firmados: una puerta desprotegida para acceder al núcleo de Windows

Los investigadores de ESET publicaron un estudio sobre el abuso de las vulnerabilidades en los controladores del kernel. Estas vulnerabilidades son las más aprovechadas por los desarrolladores de trampas para juegos con el objetivo de burlar los mecanismos de protección, pero también han sido utilizadas por varios grupos de APT y los malware commodity (vendidos en forma masiva como productos básicos).

El kernel es el componente central del sistema operativo Windows y los controladores del kernel constituyen la capa de software que proporciona funciones específicas de hardware y otras no relacionadas con el hardware. Aunque en las nuevas versiones de Windows ya no se puede cargar directamente un controlador malicioso sin firmar, es posible cargar código malicioso en el kernel manipulando controladores legítimos y vulnerables. Esta técnica también se conoce como "Traiga su propio controlador vulnerable" (BYOVD).

La técnica BYOVD ha sido empleada por varios grupos de APT, como el grupo Slingshot y el grupo InvisiMole. Además, *LoJax* [29], el primer rootkit para la UEFI encontrado activo en el mundo real y descubierto por ESET, usaba indebidamente el controlador RWEverything para obtener acceso a los módulos de la UEFI de las víctimas.

Nuestros investigadores también buscaron nuevas vulnerabilidades en los controladores del kernel y notificaron a los proveedores afectados, que se apresuraron a solucionar los problemas descubiertos. La lista completa de vulnerabilidades halladas y las técnicas útiles de mitigación se detallan en nuestro blog.

Entrada del blog WeLiveSecurity [30]

Android

Falsas tiendas electrónicas buscan extraer credenciales bancarias mediante un malware para Android

Los investigadores de ESET analizaron tres aplicaciones maliciosas para Android dirigidas a clientes de ocho bancos malayos. A medida que aumenta la cantidad de personas que utilizan sus teléfonos inteligentes para comprar, también aumentan las oportunidades para que los

ciberdelincuentes obtengan beneficios. En esta campaña en curso, los actores de la amenaza intentan robar credenciales bancarias utilizando sitios web falsos que se hacen pasar por servicios legítimos. Estos sitios web usan nombres de dominio similares a los de los servicios que suplantan.

Con el fin de engañar a las víctimas para que descarguen sus aplicaciones maliciosas, los sitios web de imitación no ofrecen la opción de comprar directamente a través de ellos. En cambio, contienen botones que simulan descargar las aplicaciones desde Google Play, aunque en realidad conducen a servidores bajo el control de los actores de la amenaza.

Una vez que las víctimas hacen sus pedidos a través de estas aplicaciones, se les presentan varias opciones de pago, de las cuales solo es posible seleccionar la transferencia directa. Al seleccionarla, las víctimas son conducidas a una página de pago FPX falsa en la que se les pide que seleccionen uno de los ocho bancos malayos. Cuando ingresan sus credenciales bancarias, éstas son enviadas a los atacantes. Las aplicaciones falsas de las tiendas electrónicas también reenvían a los operadores todos los mensajes SMS recibidos por las víctimas en caso de que contengan códigos de autenticación en dos fases.

Aunque la campaña está dirigida exclusivamente a Malasia, más adelante podría ampliarse para atacar otros países y bancos. En este momento, los atacantes van tras las credenciales bancarias, pero en el futuro también podrían robar información de las tarjetas de crédito.

Entrada del blog WeLiveSecurity [31]

Android e iOS

Malware en billeteras de criptomonedas alteradas dirigido a dispositivos Android e iOS

El Equipo de Investigación de ESET descubrió un sofisticado esquema que distribuye aplicaciones Android e iOS troyanizadas simulando ser billeteras populares de criptomonedas. Estas aplicaciones maliciosas son capaces de robar las frases secretas de las víctimas haciéndose pasar por Coinbase, imToken, MetaMask, Trust Wallet, Bitpie, TokenPocket o OneKey.

Los atacantes se aseguraron de que las aplicaciones tuvieran la misma funcionalidad que las originales e insertaron su propio código malicioso en lugares difíciles de detectar. Esto requiere un análisis en profundidad de las aplicaciones legítimas, ya que los actores de la amenaza tienen que encontrar puntos en el código donde la frase semilla es generada o importada por el usuario.

Encontramos docenas de grupos en Telegram que promocionan estas aplicaciones, probablemente creados por los mismos autores de la amenaza en busca de más socios comerciales para su distribución. A partir de octubre de 2021, descubrimos que estos grupos de Telegram fueron compartidos y promocionados en al menos 56 grupos de Facebook. También encontramos dos sitios web chinos legítimos en noviembre de 2021 que distribuían estas billeteras maliciosas. Cabe notar que el código fuente de las aplicaciones se filtró y compartió en Internet, lo que facilitará su propagación.

Las aplicaciones maliciosas se comportan de forma diferente según el sistema operativo en el que se instalen. Si la versión legítima de la aplicación existe en Android, no puede ser sobrescrita por la aplicación falsificada, porque está firmada por un certificado diferente. Por lo tanto, las únicas víctimas son los nuevos usuarios de criptomonedas sin una aplicación de billetera legítima. Sin embargo, en iOS, la víctima puede tener instalada tanto la aplicación legítima como la maliciosa, ya que no comparten el mismo ID de paquete.

Estas aplicaciones troyanizadas no están disponibles directamente en la App Store, pero algunas estaban disponibles en Google Play. A raíz de nuestra solicitud como *partners de Google App Defense Alliance* [32], Google eliminó 13 aplicaciones maliciosas encontradas en la tienda oficial en enero de 2022.

Entrada del blog WeLiveSecurity [33]

Downloaders

ESET participa en una operación global para desmantelar las botnets de Zloader

El Equipo de Investigación de ESET colaboró con sus partners de la Unidad de Crímenes Digitales de Microsoft, los Laboratorios Black Lotus de Lumen, la Unidad 42 de Palo Alto Networks y otros en un intento de desmantelar las conocidas botnets de Zloader. Contribuimos proporcionando análisis técnicos, información estadística, así como nombres de dominio y direcciones IP de los servidores de Comando y Control conocidos.

Zloader, una de las muchas familias de troyanos bancarios fuertemente inspirada en el famoso troyano bancario Zeus, evolucionó hasta convertirse en distribuidor de otros programas maliciosos, incluyendo el ransomware.

La operación de interrupción coordinada tuvo como objetivo tres botnets específicas, cada una de las cuales utilizaba una versión diferente de Zloader. Ayudamos a identificar 65 dominios que habían sido utilizados últimamente por estos operadores.

Al igual que otros programas maliciosos, Zloader se promociona y vende en foros clandestinos.

Cuando un afiliado lo adquiere, recibe todo lo que necesita para configurar sus propios servidores con paneles de administración y empezar a construir sus bots. Los afiliados son entonces responsables de la distribución de los bots y del mantenimiento de sus botnets.

Dado que este malware aún se puede conseguir con relativa facilidad, lo seguiremos vigilando para detectar cualquier nueva actividad tras esta operación de interrupción de sus botnets existentes.

Entrada del blog WeLiveSecurity [34]

Funcionamiento de la máquina virtual multicapa de Wslink

Los investigadores de ESET analizaron Wslink, un loader previamente no documentado que se ejecuta como un servidor y cuenta con un ofuscador basado en una máquina virtual. No existían similitudes de código, funcionalidad u operación que nos permitieran, en ese momento, atribuir Wslink a algún actor de amenazas conocido.

Aunque las muestras virtualizadas de Wslink no contienen ningún artefacto claro que lo vinculen fácilmente con un ofuscador de virtualización conocido, desarrollamos una solución semiautomatizada para ayudarnos a analizar el código del programa.

Esta máquina virtual introdujo un arsenal diverso de técnicas de ofuscación, que pudimos sortear para revelar una parte del código malicioso desofuscado. El white paper publicado sobre el tema describe la estructura interna general de las máquinas virtuales y contiene información detallada sobre varios pasos necesarios para ver a través de las técnicas de ofuscación utilizadas por Wslink. En las últimas secciones del paper, también presentamos partes del código que desarrollamos para facilitar nuestra investigación.

Entrada del blog WeLiveSecurity [36]

White paper [35]

Amenazas para la UEFI

Cuando lo "seguro" no es para nada seguro: se descubren vulnerabilidades de alto impacto en la UEFI de portátiles Lenovo

Los investigadores de ESET descubrieron y analizaron tres vulnerabilidades que afectan a varios modelos de computadoras portátiles Lenovo. Dos de estas vulnerabilidades, *CVE-2021-3971* [37] y *CVE-2021-3972* [38], corresponden a controladores de firmware de la interfaz UEFI originalmente destinados a utilizarse solo durante el proceso de fabricación, pero que se incluyeron por error en las imágenes del firmware de producción sin desactivarse correctamente. El aprovechamiento de estas vulnerabilidades permitiría a los atacantes desplegar y ejecutar con éxito en los dispositivos afectados implantes flash SPI o ESP, como LoJax o *ESPecter* [39], nuestro último descubrimiento de malware para la UEFI.

Mientras investigábamos esos dos controladores, descubrimos la tercera vulnerabilidad: la corrupción de la memoria SMM dentro de la función del controlador SW SMI (*CVE-2021-3970* [40]). Esta vulnerabilidad permite la lectura y escritura arbitrarias desde o hacia SMRAM, lo que puede conducir a la ejecución de código malicioso con privilegios de SMM y, potencialmente, al despliegue de un implante flash SPI.

Le informamos a Lenovo sobre las vulnerabilidades el 11 de octubre de 2021. La lista completa de dispositivos afectados, que contiene más de cien modelos diferentes de portátiles para consumidores, se publicó en un *comunicado de Lenovo* [41].

Dado que las amenazas para la UEFI se ejecutan al principio del proceso de arranque, lo que les permite eludir casi todas las medidas de seguridad, pueden ser extremadamente sigilosas y peligrosas. En el último año, se divulgaron numerosas vulnerabilidades de alto impacto en el firmware, lo que, junto con nuestros descubrimientos, demuestra que el despliegue de las amenazas para la UEFI podría ser más fácil de lo que se esperaba.

Entrada del blog WeLiveSecurity [42]

ACTIVIDAD DE GRUPOS DE APT

Aspectos destacados de las investigaciones de ESET sobre los grupos de Amenazas Persistentes Avanzadas y sus campañas

Donot Team

Ataques de ciberespionaje persistentes

El Equipo de Investigación de ESET analizó las recientes campañas realizadas por el grupo Donot Team (también conocido como APT-C-35 y SectorE02). Estuvimos supervisando a Donot Team desde septiembre de 2020 hasta octubre de 2021 y descubrimos que el grupo lleva a cabo actividades de ciberespionaje, centrándose en un pequeño número de objetivos ubicados principalmente en el sur de Asia. Un informe reciente de Amnistía Internacional vincula el software malicioso del grupo con una empresa india de ciberseguridad. Estos actores de amenazas son muy persistentes en sus ataques, reiterándolos con oleadas de correos electrónicos de phishing dirigido a las mismas entidades una y otra vez cada dos o cuatro meses.

Varias de las campañas de Donot Team que identificamos usan el malware para Windows derivado del marco de malware yty característico del grupo, cuyo objetivo principal es recopilar y extraer datos. Consiste en una cadena de downloaders que, en última instancia, termina descargando un backdoor con una funcionalidad mínima, utilizado para descargar y ejecutar otros componentes del conjunto de herramientas de este grupo de APT. Nuestros investigadores analizaron dos variantes del marco del malware: Gedit y DarkMusical.

DarkMusical se distribuyó a través de correos electrónicos de phishing dirigido con documentos de PowerPoint. Estos contienen una macro que despliega el primer componente de una cadena de downloaders y persiste usando una tarea programada. Gedit también se propagó a través del correo electrónico de phishing dirigido, pero en cambio contiene un documento RTF malicioso que aprovecha la vulnerabilidad *CVE-2017-11882* [43] para soltar dos archivos DLL desde el documento y ejecutar uno de ellos. Otros componentes se van descargando en la computadora comprometida en distintas etapas.

Entrada del blog WeLiveSecurity [44]

Campaña sin atribuir

Ataque de watering hole despliega un nuevo malware para macOS en Asia: DazzleSpy

Los investigadores de ESET descubrieron que el sitio web de la emisora de radio prodemocracia de Hong Kong D100 había sido infectado para distribuir un exploit dirigido a Safari que instalaba malware de ciberespionaje en los equipos Mac de los visitantes. El sitio web entregaba un nuevo malware para macOS que denominamos DazzleSpy.

Para conseguir la ejecución de código en el navegador, los atacantes usaron un exploit que tenía más de 1.000 líneas de código. Algunas partes del código sugieren que la vulnerabilidad también podría haber sido aprovechada en iOS, incluso en dispositivos como el iPhone XS y más recientes.

DazzleSpy se emplea para llevar a cabo actividades de ciberespionaje, y es probable que sus objetivos sean personas políticamente activas y partidarias de la democracia en Hong Kong. Este malware es capaz de: recopilar información sobre el equipo comprometido; buscar archivos concretos y escanear archivos en las carpetas Escritorio, Descargas y Documentos; ejecutar los comandos del shell suministrados; iniciar o finalizar una sesión de pantalla remota; y escribir en el disco un archivo suministrado.

Debido a la complejidad de los exploits utilizados en esta campaña, concluimos que el grupo responsable de esta operación tiene una gran competencia técnica. Esta campaña es similar a *otra de 2020* [45] en la que el malware LightSpy para iOS se distribuyó de la misma forma, utilizando la inyección de iframes en sitios web para ciudadanos de Hong Kong y conduciéndolos luego hasta un exploit de WebKit. No podemos confirmar en este momento si ambas campañas fueron realizadas por el mismo grupo.

Entrada del blog WeLiveSecurity [46]

Mustang Panda

Hodur de Mustang Panda: viejos trucos; nueva variante de Korplug

Los investigadores de ESET descubrieron una campaña de ciberespionaje aún en curso llevada a cabo por el grupo de APT Mustang Panda, en la que utilizan una variante de Korplug anteriormente no documentada. La llamamos Hodur por su parecido con la variante THOR documentada previamente por *Unit 42* [47] en 2020. En la mitología nórdica, Hodur es el hermanastro ciego de Thor, engañado por Loki para matar a su hermanastro Baldr. Atribuimos esta campaña a Mustang Panda con gran confianza. Se trata de un grupo de ciberespionaje cuyo objetivo son principalmente las entidades gubernamentales y las ONG, y sus víctimas se encuentran sobre todo en el este y el sudeste de Asia.

La campaña actual recurre a los últimos acontecimientos en Europa como señuelo de phishing, incluyendo la invasión rusa de Ucrania. Otros señuelos de phishing mencionan las actualizaciones de las restricciones de viaje por el COVID-19, un mapa de ayuda regional aprobado para Grecia y un Reglamento del Parlamento y del Consejo Europeos, lo que demuestra que este grupo de APT es capaz de reaccionar rápidamente a los temas de actualidad.

Mustang Panda es conocido por sus elaborados loaders personalizados y sus variantes de Korplug, que pueden verse claramente en las muestras de esta campaña. Lo que la distingue en particular de otras campañas es que utiliza intensivamente técnicas de ofuscación de control de flujo y antianálisis en cada etapa del proceso de despliegue.

Entrada en el blog WeLiveSecurity [17]

Winnti Group

Se descubren nuevas variantes de PipeMon

Los investigadores de ESET descubrieron nuevas variantes de PipeMon del grupo Winnti. Las virtualizaron usando el Code Virtualizer de Oreans y las hicieron pasar por un procesador de impresión ubicado fuera del directorio dedicado al procesador de impresión del sistema, para hacerlas persistentes. La primera vez que documentamos el backdoor PipeMon fue en *2020* [48], cuando se utilizó contra varias empresas de videojuegos con sede en Corea del Sur y Taiwán.

Aunque la documentación de Microsoft menciona específicamente que las DLL del procesador de impresión deben estar ubicadas en el directorio del procesador de impresión del sistema, es posible colocar dichas DLL en cualquier lugar de la unidad del sistema y utilizar una ruta relativa en el registro que apunte a la DLL, en lugar de utilizar solo un nombre de archivo. De esta manera, una DLL maliciosa persistente puede pasar desapercibida si el atacante la hace pasar por un procesador de impresión y la guarda en una ubicación diferente.

Hilo de Twitter [49]

TA410

Una mirada atrás bajo el paraguas del TA410: sus tácticas, técnicas, procedimientos y actividades de ciberespionaje

El Equipo de Investigación de ESET reveló un perfil detallado de TA410, un grupo paraguas de ciberespionaje vagamente vinculado con APT10, conocido sobre todo por atacar organizaciones de servicios públicos con sede en Estados Unidos, y organizaciones diplomáticas en Oriente Medio y África.

Creemos que el grupo está formado por tres equipos diferentes que utilizan distintos conjuntos de herramientas, incluyendo una nueva versión del backdoor de espionaje FlowCloud descubierto por ESET. Estos equipos, denominados FlowingFrog, LookingFrog y JollyFrog, tienen coincidencias en sus tácticas, técnicas y procedimientos (TTP), victimología e infraestructura de red. Suponemos que estos subgrupos operan de forma relativamente independiente, pero que pueden compartir los requisitos de inteligencia, el equipo de acceso que ejecuta sus campañas de phishing dirigido y también el equipo que despliega la infraestructura de la red.

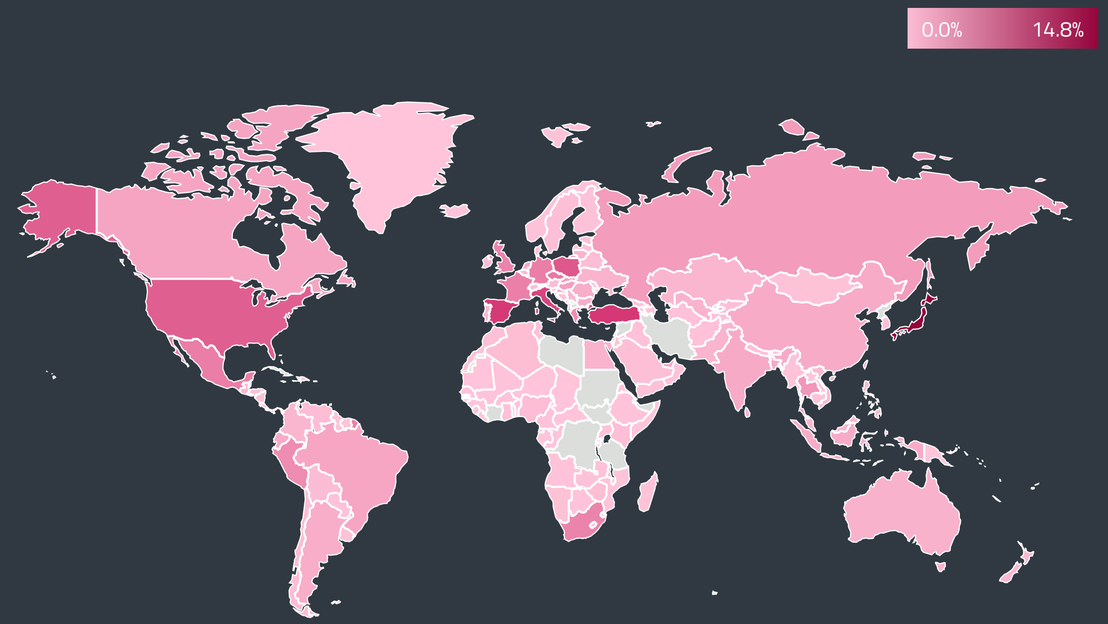
Aunque la mayoría de los objetivos del grupo TA410 son organizaciones de alto perfil en los sectores de la diplomacia y la educación, ESET también ha identificado víctimas en el sector militar, una fábrica en Japón, una empresa minera en la India y una organización benéfica en Israel.

La nueva versión de FlowCloud, un troyano complejo y modular de acceso remoto (RAT) en C++ utilizado por el equipo de FlowingFrog, tiene varias capacidades interesantes. Entre ellas se encuentran: el monitoreo de los eventos del portapapeles para robar su contenido, el monitoreo de los eventos del sistema de archivos para recopilar los archivos nuevos y modificados, el control de los dispositivos de cámara conectados para tomar fotografías del entorno del equipo comprometido, e incluso el control de los micrófonos conectados y la activación de la grabación cuando se detectan niveles de sonido por encima de un umbral de volumen especificado. La última función se activa con cualquier sonido que supere los 65 decibelios, es decir, por sobre el volumen normal de una conversación.

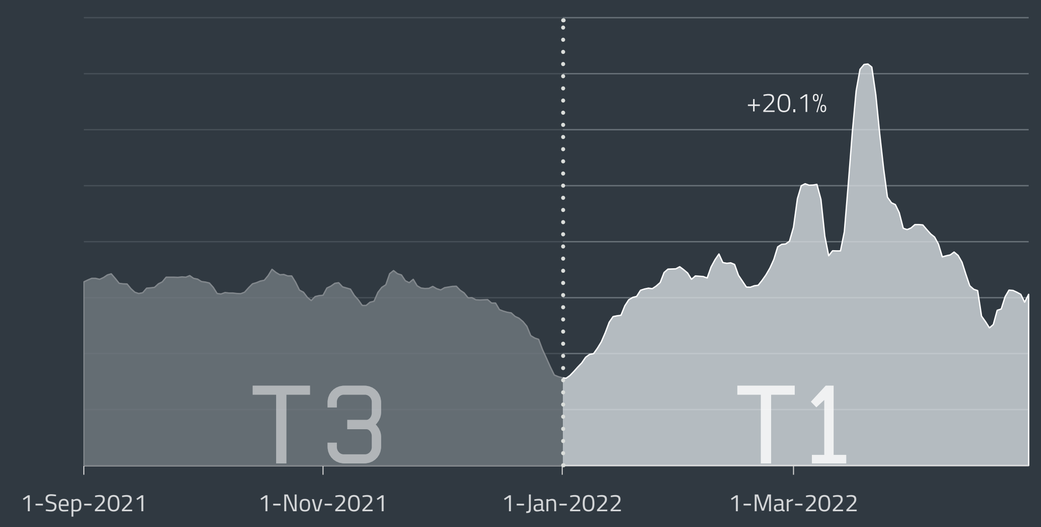
Entrada del blog WeLiveSecurity [50]

ESTADÍSTICAS Y TENDENCIAS

El panorama de amenazas en el primer cuatrimestre de 2022 según la telemetría de ESET



Distribución global de las detecciones de malware en el primer cuatrimestre de 2022



Tendencia general de detección de amenazas en el tercer cuatrimestre de 2021 y primero de 2022, promedio móvil de siete días

INFORMACIÓN GENERAL SOBRE EL PANORAMA DE AMENAZAS

Un resumen de la evolución del panorama de amenazas durante el primer cuatrimestre de 2022.

Tras haberse mantenido relativamente estable por algún tiempo, el número de detecciones de amenazas aumentó un 20,1% en el primer cuatrimestre de 2022. Hubo dos picos notables, el 2 y el 15 de marzo, causados por el troyano DOC/TrojanDownloader.Agent. Tanto el aumento en las tasas totales de detección de amenazas como los picos fueron causados por el dramático regreso de Emotet.

Por lo tanto, no es de extrañar que la categoría ***Downloaders*** esté dominada por la reciente campaña de Emotet. Cuando se compara con los valores relativamente bajos del malware en el tercer cuatrimestre de 2021, su aumento astronómico, de más de cien veces, sigue asombrando. ¡A eso sí que se le llama volver buscando venganza!

La campaña de Emotet también influyó en la categoría ***Amenazas por correo electrónico,*** que creció un 37% gracias a ella. Por otra parte, la campaña provocó un aumento del 829% en la incidencia de DOC/TrojanDownloader.Agent, que subió al segundo puesto en la lista de las 10 principales amenazas por correo electrónico.

En la sección ***Exploits***, el número de ataques al protocolo RDP (la causa habitual de las grandes cifras atemorizantes en el Threat Report) descendió un 43% tras haber experimentado un crecimiento ininterrumpido desde principios de 2020.

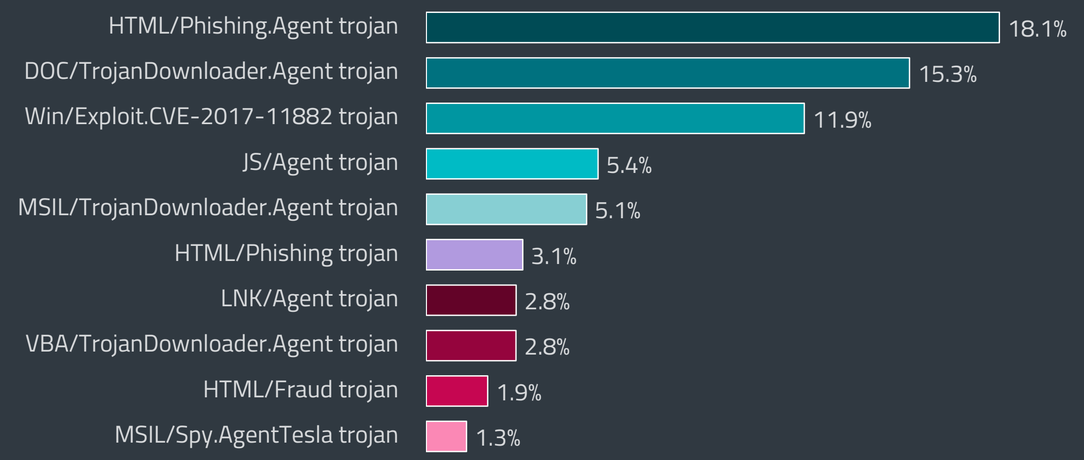
Como siempre, el panorama de las amenazas de ***Ransomware*** no fue para nada aburrido, con el arresto de los miembros principales de Sodinokibi, las importantes filtraciones de información interna de la banda Conti y el hecho de que Rusia se convirtiera en el objetivo número uno de los ataques de ransomware en el primer cuatrimestre, según nuestra telemetría.

Las ***amenazas para macOS*** experimentaron descensos en todas sus subcategorías, con una disminución global del 14,9%. Casi la mitad de las amenazas monitoreadas se clasificaron como aplicaciones potencialmente no deseadas (PUA). La categoría ***Android*** registró un ligero aumento en las detecciones, con una suba del 8%. Sin embargo, dos de sus subcategorías, los troyanos SMS para Android y el spyware para Android, crecieron de un modo espectacular, la primera un 145% y la segunda un 170%.

En lo que respecta a las ***Amenazas para criptomonedas,*** el primer cuatrimestre de 2022 se caracterizó por varios hackeos de plataformas de criptomonedas de gran repercusión, que les permitieron a los ciberdelincuentes ganar mucho dinero, si bien el número global de detecciones en esta categoría disminuyó un 29,3%.

Los datos de la categoría ***IoT*** muestran que, años después de la publicación online del código fuente de Mirai, las botnets que utilizan el código siguen siendo muy comunes, atacando cientos de miles de dispositivos. Mientras que el ritmo de propagación de la famosa botnet Mozi se redujo un 11%, ZHTrap consiguió aumentar el número de sus ataques un 9%.

En cuanto a las ***Amenazas web***, nuestra telemetría registró un aumento del 29% en las URL de phishing, causado por un pico de nuevas URL en marzo. Como los ciberdelincuentes siempre están dispuestos a sacar provecho de la desgracia humana, también se produjo un aumento de los sitios web de phishing y estafas que aprovechaban el interés y la preocupación por la guerra entre Rusia y Ucrania.



Las 10 principales detecciones de malware en el primer cuatrimestre de 2022 (porcentaje de detecciones de malware)

Finalmente, tras una pausa en el tercer cuatrimestre de 2021, los ***Infostealers*** empezaron a crecer otra vez. Experimentaron un aumento del 12%, y la subcategoría que más creció (74,5%) fue la de malware bancario. La mayor parte de este crecimiento se debió a JS/Spy.Banker, que creció un 177,7% y representó el 77,6% del malware bancario.

El aumento de Emotet también afectó al conjunto de las diez principales detecciones de malware: aunque no consiguió destronar al troyano HTML/Phishing.Agent, que constituyó el 18,1% de todas las detecciones, DOC/TrojanDownloader.Agent pasó de ser la novena familia de malware más detectado a la segunda, con un 15,2%. En comparación con el tercer cuatrimestre de 2021, sus cifras aumentaron un 758,4%.

MSIL/TrojanDownloader.Agent, que descarga malware como Agent Tesla y Fareit, también creció significativamente durante el primer cuatrimestre, y este crecimiento del 117,9% lo situó en el quinto lugar (en vez del octavo que tenía en el tercer cuatrimestre de 2021). El resto de las diez primeras detecciones de malware bajaron en su mayoría una o dos posiciones, pero la lista en sí no perdió a ninguna de las 10 familias anteriores, ni apareció ningún nuevo integrante.

LAS 10 PRINCIPALES DETECCIONES DE MALWARE

→ Troyano HTML/Phishing.Agent

HTML/Phishing.Agent es el nombre de detección de un código HTML malicioso que muchas veces se distribuye junto a un archivo adjunto de correo electrónico de phishing. Los atacantes suelen usarlo en lugar de otros tipos de archivos porque los archivos adjuntos ejecutables suelen bloquearse automáticamente o es más probable que generen sospechas. Cuando se accede al archivo adjunto malicioso, se abre un sitio de phishing en el navegador web que intenta pasar, por ejemplo, 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, para luego enviar los datos al atacante.

↗ Troyano DOC/TrojanDownloader.Agent

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

↘ Troyano Win/Exploit.CVE-2017-11882

Este nombre de detección abarca documentos especialmente diseñados que aprovechan la vulnerabilidad ***CVE-2017-11882*** [51] del editor de ecuaciones de Microsoft, un componente de Microsoft Office. El exploit está disponible al público y por lo general se usa en la primera etapa de la infección. Cuando el usuario abre el documento malicioso, se activa el exploit y se ejecuta su shellcode. Luego se descarga malware adicional en la computadora para realizar acciones maliciosas arbitrarias.

↘ Troyano JS/Agent

Este nombre de detección abarca varios archivos de 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 MSIL/TrojanDownloader.Agent

MSIL/TrojanDownloader.Agent es el nombre de detección de un software malicioso escrito para la plataforma Windows que utiliza el Framework .NET; este malware intenta descargar otro malware utilizando diversos métodos. Suele contener una URL o una lista de direcciones URL que conducen al payload final. Este malware suele actuar como la primera capa de un paquete mucho más complejo, encargándose de la tarea de instalación en el sistema de la víctima.

↘ Troyano HTML/Phishing

El troyano HTML/Phishing representa las detecciones de malware genérico recopiladas al analizar direcciones URL maliciosas en correos electrónicos y archivos adjuntos. Si un correo electrónico o su adjunto contiene una URL de la lista negra, se activa una detección de HTML/Phishing.Gen.

↘ Troyano LNK/Agent

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 son populares 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 suelen formar parte de otro malware más complejo. A menudo se usan para lograr la persistencia de los principales archivos maliciosos en el sistema o como parte del vector de infección.

↘ Troyano VBA/TrojanDownloader.Agent

VBA/TrojanDownloader.Agent es una detección que normalmente abarca archivos de Microsoft Office creados con fines maliciosos que intentan manipular a los usuarios para que habiliten macros. 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 HTML/Fraud

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 que promete cobrar una fortuna pero solicita el pago de una ***pequeña suma por adelantado*** [52], como la famosa estafa del "príncipe nigeriano", también conocida como "estafa 419".

→ Troyano MSIL/Spy.AgentTesla

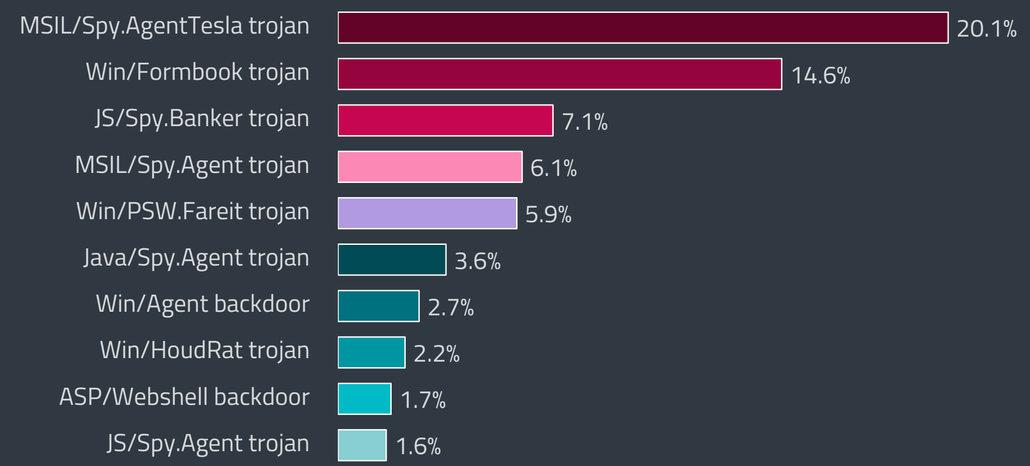
MSIL/Spy.AgentTesla es un troyano de tipo spyware como servicio basado en .NET y disponible en foros clandestinos. Obtiene datos y comandos de hosts remotos y sirve para adquirir información confidencial, registrar las pulsaciones del teclado y controlar la cámara o el micrófono de la víctima.

INFOSTEALERS

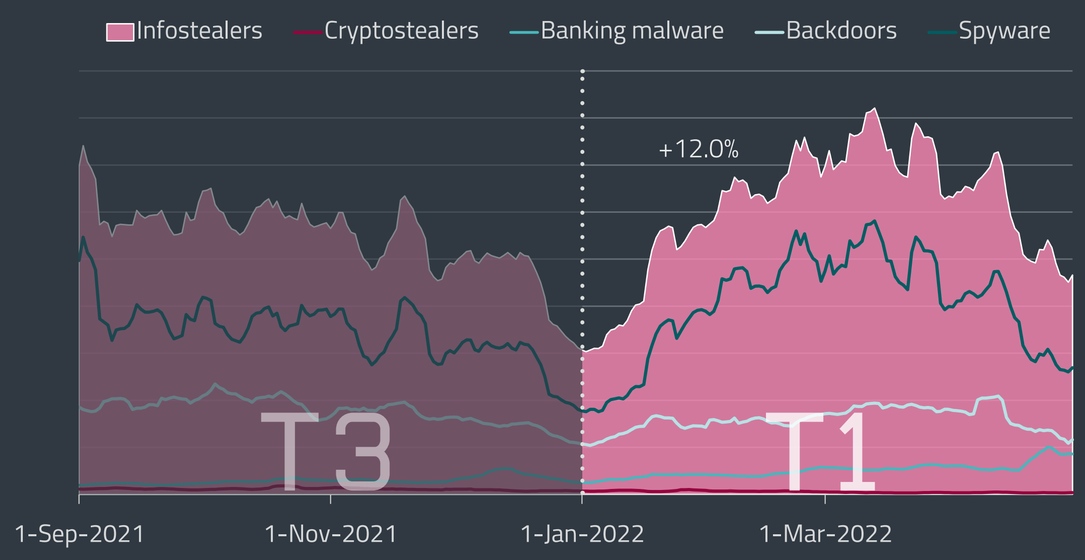
TrickBot se retira, mientras que JS/Spy.Banker domina el panorama de las amenazas de malware bancario.

Tras una breve pausa en el tercer cuatrimestre de 2021, la categoría Infostealers reanudó su crecimiento en el primer cuatrimestre de 2022, subiendo casi un 12%. Como de costumbre, lo que ocasiona la mayoría de las detecciones es el spyware, que también fue el responsable del pico más significativo el 22 de marzo de 2022, por cortesía de MSIL/Spy.AgentTesla. El spyware y el malware bancario aumentaron en cantidad de detecciones, los backdoors disminuyeron y los cryptostealers se redujeron considerablemente tanto en tendencia como en número.

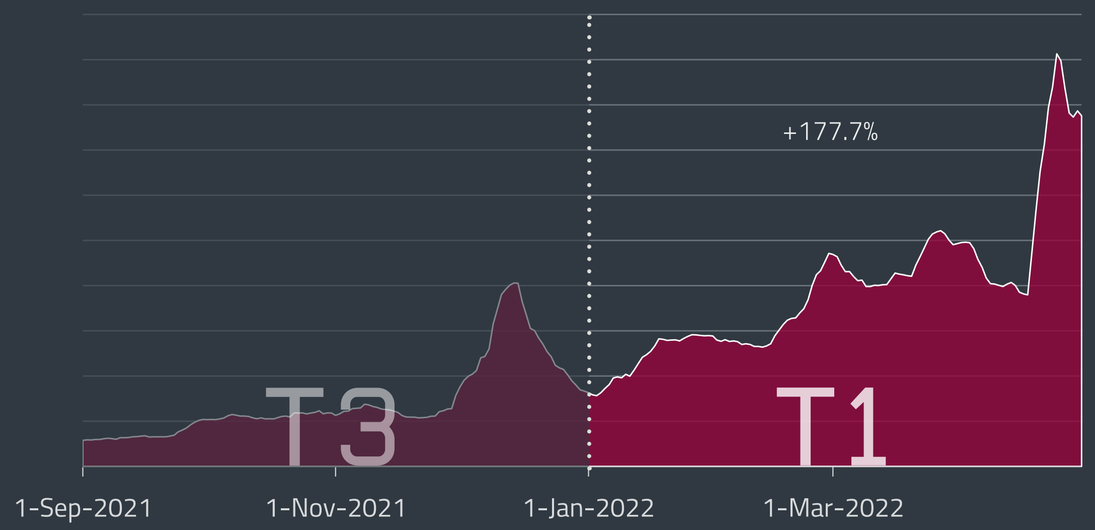
En el primer cuatrimestre de 2022, el spyware creció un 18,2% y representó el 64,4% de todas las detecciones de infostealers, consolidando aún más su posición como la mayor subcategoría de infostealers. A ello contribuyó la relativa accesibilidad del malware de tipo spyware como servicio en los foros clandestinos. Un ejemplo típico de este modelo de negocio, el troyano MSIL/Spy.AgentTesla, o simplemente Agent Tesla, fue una vez más el spyware más destacado según los datos de telemetría de ESET, con un crecimiento del 243,6% entre el tercer cuatrimestre de 2021 y el primero de 2022. En el primer cuatrimestre, se propagó mediante *documentos maliciosos de PowerPoint* [53] en campañas de phishing. Además, ESET registró su distribución en otra campaña de phishing junto con el backdoor Win/Agent a finales de abril.



Las 10 principales familias de infostealers en el primer cuatrimestre de 2022 (porcentaje de detecciones de infostealers)



Tendencia de detección de infostealers en el tercer cuatrimestre de 2021 y primero de 2022, promedio móvil de siete días



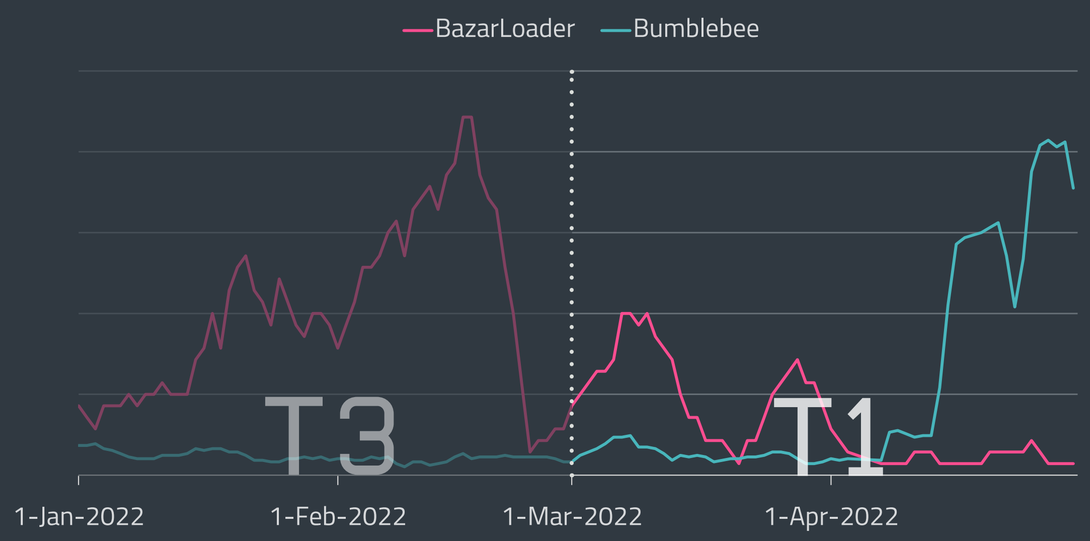
Tendencia de detección de JS/Spy.Banker en el tercer cuatrimestre de 2021 y primero de 2022, promedio móvil de siete días

Las 10 principales detecciones de infostealers también estuvieron encabezadas por el spyware, que ocupó los dos primeros puestos de la lista. Agent Tesla tuvo las cifras más altas, con el 19,3% de todas las detecciones de infostealers y el 29% de las detecciones de spyware. Le sigue el troyano Win/Formbook, que representa el 14% de los infostealers y el 21,1% de los spyware. El troyano MSIL/Spy.Agent se situó en cuarto lugar en la clasificación general con un 5,8% y fue el tercer spyware más detectado con un 8,8%.

Mientras que los primeros puestos de la lista tradicionalmente han sido ocupados por spyware y backdoors, en esta ocasión una familia de malware bancario ascendió al tercer puesto. El troyano JS/Spy.Banker representó el 6,8% de los infostealers. Esta familia de malware, también conocida como Magecart, inyecta código de JavaScript que actúa como un skimmer en los sitios web para extraer la información de las tarjetas de crédito. Entre el tercer cuatrimestre de 2021 y el primero de 2022, creció un 177,7% y se convirtió prácticamente en sinónimo de la subcategoría de malware bancario, representando el 77,6% de sus detecciones. El siguiente malware más detectado en la subcategoría, el troyano MSIL/ClipBanker, se quedó con los restos en comparación con JS/Spy. Banker, ya que disminuyó un 59,4%, constituyendo tan solo el 4,5% del malware bancario.

Esta subcategoría creció un 75% en el primer cuatrimestre de 2022 y representó el 8,5% de todas las detecciones de infostealers. El 19 de abril experimentó un importante pico causado por el mencionado JS/Spy.Banker, donde Tailandia fue el país más afectado.

TrickBot, el malware bancario convertido en herramienta de ataque multipropósito dirigida a las empresas, y uno de los pilares del panorama de amenazas, ***finalizó sus operaciones*** [54] en febrero. Se especula que la banda detrás de TrickBot, que tiene estrechos vínculos con el grupo de ransomware Conti, decidió cambiar su enfoque a



Tendencias de detección de BazarLoader y Bumblebee en el tercer cuatrimestre de 2021 y primero de 2022, promedio móvil de siete días

BazarLoader. Aunque TrickBot fue muy exitoso e incluso logró reponerse tras los esfuerzos de desmantelamiento en 2020, después no hubo actualizaciones significativas en su núcleo.

BazarLoader, otra herramienta del arsenal de los creadores de TrickBot, utiliza técnicas más avanzadas y es más difícil de rastrear y analizar. Cabe destacar la posibilidad de que BazarLoader esté siendo reemplazado, ya que empezaron a aparecer ***reportes*** [55] de un nuevo loader llamado Bumblebee que se ha estado propagando desde marzo. Los actores de amenazas que están usando Bumblebee son los mismos que antes utilizaban BazarLoader. Queda por ver cuál de estos loaders gana al final, o si ambos se mantienen en circulación.

COMENTARIO DE EXPERTOS

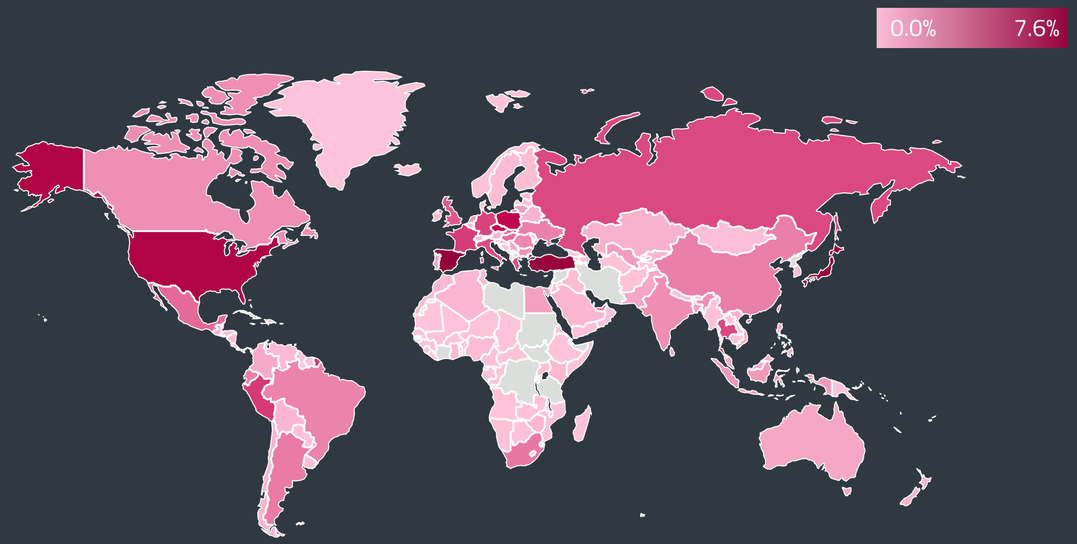
Desde principios del año 2021, BazarLoader ha estado en continuo desarrollo. Su ritmo se ha acelerado considerablemente en los tres primeros meses de 2022, cuando observamos avances en sus técnicas de antianálisis. El malware cuenta ahora con una técnica mejorada de ofuscación de las llamadas a la API, que combina tres hashes en lugar de uno, y además añadió ofuscación del flujo del código.

Me sorprende que nuestras últimas investigaciones apunten a que Bumblebee sustituirá a BazarLoader. Desde el punto de vista de los analistas, los ciberdelincuentes están trabajando activamente en BazarLoader, que se ha convertido en un sofisticado malware difícil de rastrear y analizar. Claramente, no es una herramienta que un atacante quiera descartar, por lo que creo que volveremos a encontrarnos con ella.

En comparación, Bumblebee, en su estado actual, no tiene ningún tipo de ofuscación en su núcleo y utiliza parcialmente código abierto. Es probable que Bumblebee siga desarrollándose en un futuro próximo.

Jakub Tomanek, ESET Malware Analyst

La mayoría de los troyanos bancarios latinoamericanos no se desviaron de sus patrones habituales: siguieron robando credenciales bancarias principalmente en México y Brasil, con alguna incursión ocasional en España. Sin embargo, parece que uno de los miembros de este grupo de malware está tratando de ampliar sus horizontes de manera considerable: ***Grandoreiro*** [56] añadió ***más de 900 nuevos objetivos*** [57] a su lista, entre ellos el cambio de criptomonedas y los juegos NFT. Este troyano bancario latinoamericano puede considerarse actualmente el más activo del grupo.



Distribución global de las detecciones de infostealers en el primer cuatrimestre de 2022

Parece que mientras Grandoreiro empezaba a invadir el terreno de los cryptostealers, los propios cryptostealers no se mostraban demasiado activos. Sus números de detección se redujeron un 51,6% durante el primer cuatrimestre de 2022, continuando su tendencia a la baja, lo que debería alegrar a todos los propietarios de criptomonedas. Esta subcategoría experimentó un pico notable el 25 de enero causado por el troyano Win/PSW. Delf, cuyos intentos de ataque se registraron principalmente en Japón y Hong Kong en ese momento.

La subcategoría Backdoors, habitualmente fuerte, disminuyó en cantidad de detecciones, ahora por segundo período consecutivo. A pesar de su disminución del 11,1%, siguen ocupando el segundo lugar en las detecciones de infostealers, el 25,5% de las cuales fueron clasificadas como backdoors.

También aparecieron en la lista de las 10 principales detecciones de infostealers, en los puestos sexto, octavo y décimo. El primero de ellos fue el backdoor PHP/Webshell (15,6% de los backdoors, 4,1% de los infostealers), seguido del backdoor Win/Agent (9,7% de los backdoors, 2,6% de los infostealers) y el backdoor ASP/Webshell (6,4% de los backdoors, 1,7% de los infostealers). El 7 de abril se observó un pico significativo de backdoors, causado por el backdoor Win/Agent y su variante TJS, con más de tres cuartas partes de sus intentos de ataque registrados en España. Win/Agent.TJS es la misma variante que los productos de ESET detectaron propagándose a través de correos electrónicos junto con Agent Tesla a finales de abril.

Otra variante de este backdoor, más concretamente Win/Agent.NE, alias el RAT G3ll3rt Grind3lwald, se estaba distribuyendo en una *nueva campaña* [58] descubierta por los investigadores de ESET a principios de año. Aunque nuestra telemetría no mostró tantas visitas en ese momento, algunas bandas criminales como Zloader se interesaron activamente por el malware. Luego de los aumentos de actividad en enero y febrero, las cifras de G3ll3rt Grind3lwald fueron disminuyendo en forma gradual.

En el primer cuatrimestre, los infostealers fueron más frecuentes en España, donde se registró el 7,6% de todos los intentos de ataque, luego en Turquía, con el 7,1%, y en Japón, con el 6,9%.

RANSOMWARE

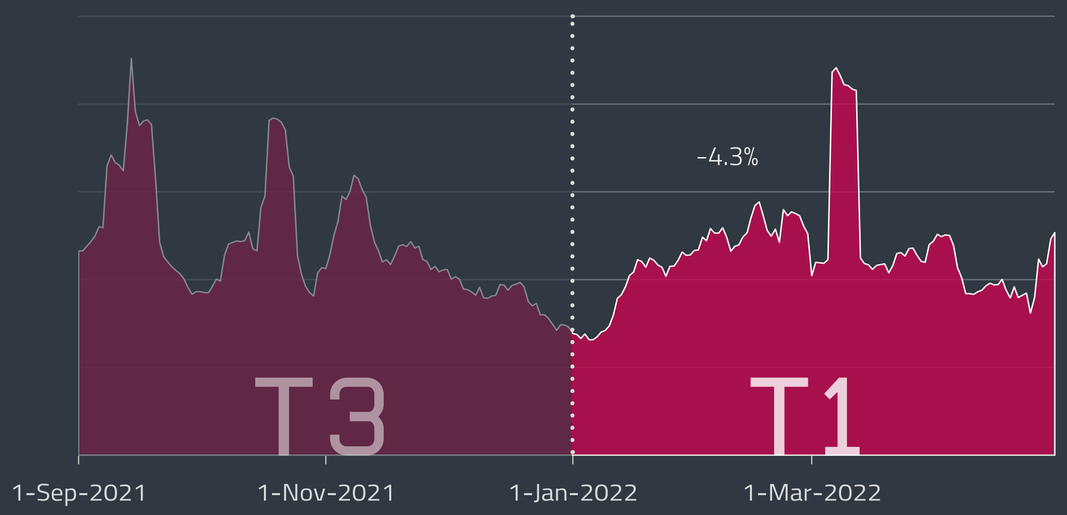
La guerra en Ucrania provocó un aumento de los ataques de ransomware motivados por la ideología, donde Rusia es el objetivo cada vez más frecuente de los ataques.

El primer cuatrimestre de 2022 comenzó con una gran noticia. En enero, el Servicio Federal de Seguridad ruso (FSB) allanó 25 direcciones y detuvo a 14 presuntos miembros principales de la infame banda de ransomware *Sodinokibi/REvil* [59]. La operación fue impulsada por las autoridades estadounidenses, que informaron sobre el líder del grupo. Durante las redadas, los agentes incautaron criptomonedas y monedas fiduciarias por un valor de más de 6 millones de dólares, 20 coches de lujo y el hardware utilizado para llevar a cabo la operación maliciosa.

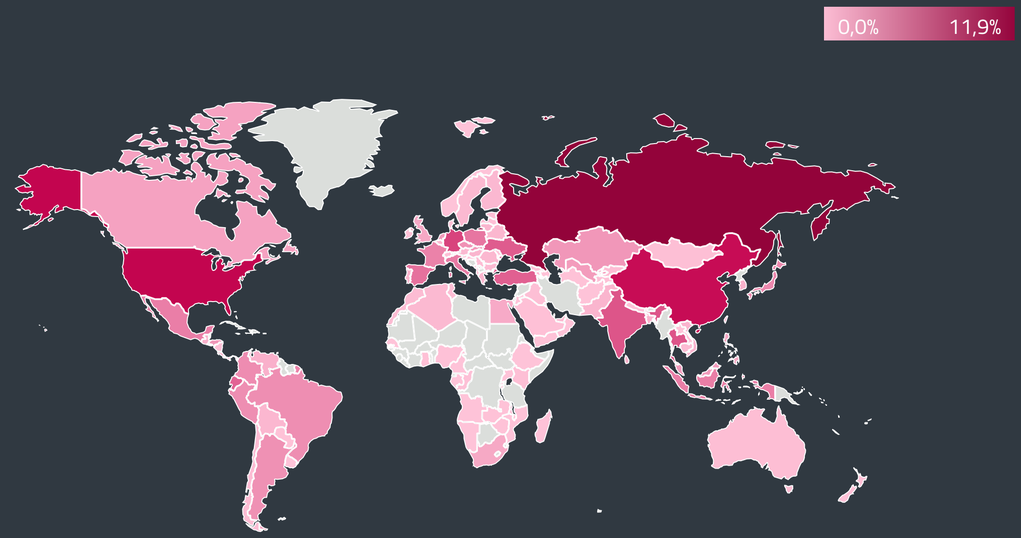
Sin embargo, las detenciones no tuvieron un efecto duradero, ya que el *sitio de filtraciones TOR utilizado por Sodinokibi* [60] cobró vida tan solo unas semanas después y comenzó a recopilar nuevas víctimas. Tras analizar las muestras de los ataques, los investigadores confirmaron que se trataba de *nuevas instancias de Sodinokibi* [61], compiladas a partir del código fuente original. Esto sugiere que uno de los antiguos miembros principales (con acceso a los recursos de la banda) sigue libre y está dirigiendo la operación.

No obstante, la actividad de las fuerzas policiales contra Sodinokibi pronto se vio eclipsada por acontecimientos mucho más sombríos. La invasión rusa de Ucrania tuvo numerosas influencias en la categoría Ransomware. Aparte de los ataques de *HermeticRansom* [4] a varias organizaciones ucranianas de alto perfil, la tendencia de detección de ransomware continuó su lento ritmo descendente, cayendo un 4% en comparación con el tercer cuatrimestre de 2021.

Si se observan las alzas en el gráfico, la primera fue causada por la banda Conti, que atacó los sistemas de



Tendencia de detección de ransomware en el tercer cuatrimestre de 2021 y primero de 2022, promedio móvil de siete días



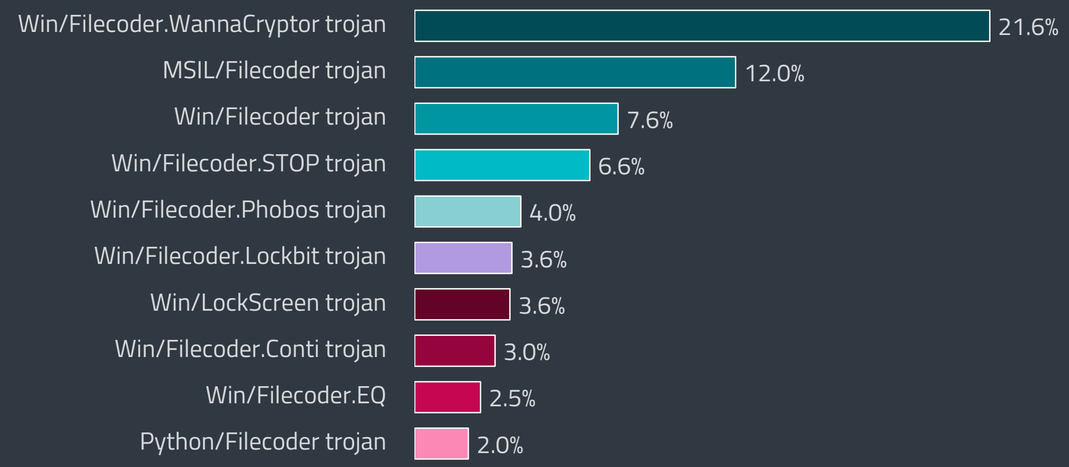
Distribución global de las detecciones de ransomware en el primer cuatrimestre de 2022

Honduras y representó el 53% de las detecciones diarias. El segundo pico del 6 de marzo, aún mayor, fue provocado por MSIL/Filecoder.ACB, que atacó la red de una gran organización en Rusia, intentando cifrar sus datos desde dentro del entorno.

Este incidente indica un posible cambio en el panorama del ransomware. Antes de la invasión, Rusia y algunos países de la Comunidad de Estados Independientes (CEI) estaban excluidos de muchas listas de objetivos de ransomware. Probablemente esto se debía a que los delincuentes residían en esos países o temían las represalias de Rusia. El primer cuatrimestre de 2022 revela un posible cambio, ya que Rusia se enfrentó a la mayor proporción de detecciones (12%) en la categoría Ransomware. Aunque no es inusual, hasta ahora Rusia no había tenido que probar tanto de su propia medicina.

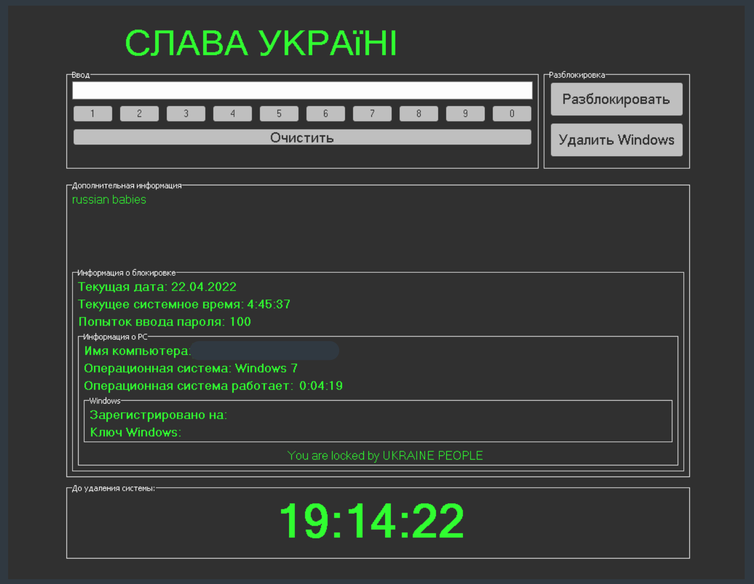
La serie de incidentes que hubo contra objetivos rusos de alto nivel parece corroborar esta interpretación. El grupo *NB65* [62] comenzó a atacar a víctimas rusas, entre ellas, la agencia espacial Roscosmos y la emisora estatal de televisión y radio. Como reacción a la masacre de Bucha (Ucrania), NB65 utilizó el código fuente filtrado del ransomware Conti para vulnerar sus objetivos y filtrar su información confidencial en Internet.

Un segundo actor que recurrió al tema de la guerra fue *OldGremlin* [63]. Al parecer, este grupo utilizó correos electrónicos de phishing dirigido y backdoors personalizados para penetrar en bancos rusos, empresas industriales, organizaciones médicas y desarrolladores de software.



Las 10 principales familias de ransomware en el primer cuatrimestre de 2022 (porcentaje de detecciones de ransomware)

Un dato interesante que se destacó en el primer cuatrimestre de 2022 fue el aumento del número de incidentes de ransomware de bloqueo de pantalla, que saltó a la séptima detección de ransomware más frecuente. Cerca del 40% de estos ataques estaban dirigidos a Rusia y el 11% a Ucrania. La variante de Win/LockScreen.AWI dirigida a Rusia incluso mostraba el título "Slava Ukraini" (en letra mayúscula cirílica ucraniana), es decir, "Gloria a Ucrania", un saludo nacional utilizado por los ucranianos.



Variante de Win/LockScreen.AWI dirigida a víctimas rusas con el título "Gloria a Ucrania"

Otra noticia importante sobre el ransomware relacionada con la guerra en Ucrania es la ya mencionada filtración de datos de Conti. El material fue publicado por un *investigador* [64] informático ucraniano, que se molestó por la *promesa* [65] de la banda de apoyar a Rusia en sus esfuerzos bélicos agresivos. A su vez, abrió una *cuenta de Twitter* [66] que usó para filtrar los datos del grupo, incluyendo el código fuente de varias de sus familias de malware y años de *comunicaciones internas confidenciales* [67], con indicios de un posible vínculo con el gobierno ruso. Otros actores, como *LockBit* [68], trataron de evitar consecuencias similares y publicaron declaraciones en varios idiomas en las que afirmaban que se mantendrían imparciales.

Una buena noticia es que en el primer cuatrimestre de 2022 se publicó una gran cantidad de herramientas de descifrado gratuitas. La lista incluye algunos de los nombres más conocidos como *Maze, Egregor, Sekhmet* [69] y *Diavol* [70], pero también cepas menos conocidas como *TargetCompany* [71] y *Yanlouwang* [72]. En cuanto a la guerra en Ucrania, se ha publicado una herramienta de descifrado gratuita para las víctimas de *HermeticRansom* [73], el malware descrito en nuestra *Historia destacada*. Un grupo de investigadores surcoreanos también detallaron las vulnerabilidades del algoritmo de cifrado del *ransomware Hive* [74] y mostraron cómo aprovecharlas para recuperar los datos afectados.

El inicio de este año fue también el período en el que algunos de los actores del ransomware escucharon sus sentencias. Un hombre de Estonia pasará los próximos *66 meses en la cárcel* [75] y pagará 36 millones de dólares en concepto de indemnización por su vinculación con 13 ataques, que causaron pérdidas acumuladas de más de 50 millones de dólares. Un afiliado canadiense de NetWalker fue *condenado a 80 meses* [76] por su participación en los ataques que afectaron a 17 víctimas.

A pesar de que algunos de los actores terminaron arrestados, todavía parece haber bastantes criminales codiciosos que quieren una tajada de esos grandes montos y se incorporan a la escena del ransomware con sus bandas. La banda *NightSky* [77] fue una de las primeras y más visibles que aparecieron en el primer cuatrimestre de 2022. Su objetivo de ataque son las redes corporativas y aprovecha vulnerabilidades en la biblioteca *Log4J* [78]. Además de eCh0raix, los dispositivos NAS están siendo atacados por un nuevo ransomware llamado *DeadBolt* [79]. Otro recién llegado, White Rabbit, parece ser un proyecto paralelo del grupo de hackers FIN8.

Pero no todas las bandas de ransomware se centran en las empresas y en los grandes beneficios. Un nuevo RaaS llamado *ransomware Sugar* [80] parece estar bastante interesado en los usuarios normales y las pequeñas empresas, exigiendo rescates significativamente menores que la competencia. En el primer cuatrimestre de 2022, también fueron novedad los ransomware *Black Basta* [81] y *Onyx* [82], este último destruye la mayor parte de los datos en lugar de limitarse a cifrarlos.

COMENTARIO DE EXPERTOS

Desde la invasión rusa de Ucrania, hemos observado un aumento en el número de ransomware y wipers de aficionados. Sus autores a menudo prometen apoyar a uno de los bandos combatientes y convierten los ataques en un acto de venganza personal. Lo interesante es que las variantes proucranianas superan a las prorrusas por un pequeño margen. Prevemos que estos ataques continuarán en los próximos meses e incluso se intensificarán, ya que la ideología y la propaganda bélica se están convirtiendo en las principales fuerzas impulsoras de su propagación.

Igor Kabina, ESET Senior Detection Engineer

DOWNLOADERS

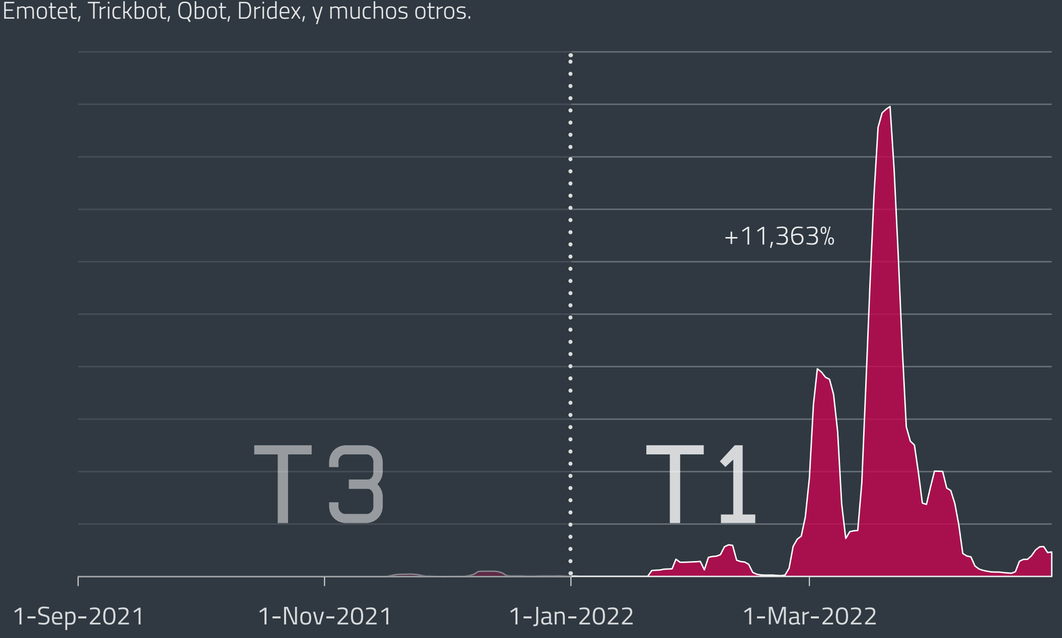
Emotet cambia de ritmo y añade un nuevo método de distribución; Zloader se enfrenta a un intento de desmantelamiento.

En el tercer cuatrimestre de 2021, detallamos la resurrección de Emotet, las mejoras en su binario y sus módulos, y los ajustes en su técnica, principalmente con el objetivo de cambiar su payload por Cobalt Strike Beacon. Aunque parecía una lista bastante extensa, el primer cuatrimestre de 2022 demuestra que tan solo era una etapa preparatoria de lo que estaba por venir.

En marzo y abril de 2022, los operadores de Emotet aumentaron el ritmo, y su botnet comenzó a lanzar una campaña de spam tras otra, utilizando documentos de Word maliciosos (DOC/TrojanDownloader.Agent) como archivos adjuntos. En comparación con las campañas iniciales relativamente pequeñas que se vieron tras su regreso en el tercer cuatrimestre de 2021, las detecciones de Emotet en el primer cuatrimestre de 2022 aumentaron más de cien veces (un crecimiento mayor al 11.000%).

El primer gran repunte se produjo el 2 de marzo, dirigido muy claramente a Japón (67% de las detecciones). El 16 de marzo se observó el mayor pico desde la resurrección de Emotet, que afectó sobre todo a víctimas de Japón (50%), Italia (16%) y México (4%). También hubo una réplica más pequeña el 21 de marzo con objetivos similares.

Como se *anunció* [83] en febrero, Microsoft deshabilitó la descarga de macros de Visual Basic para Aplicaciones (VBA) por defecto. Esto *cortó efectivamente* [84] una de las vías de distribución más populares utilizadas por Emotet, Trickbot, Qbot, Dridex, y muchos otros.



Tendencia de detección de Emotet en el tercer cuatrimestre de 2021 y primero de 2022, promedio móvil de siete días

Los operadores de Emotet trataron de adaptarse a la nueva realidad experimentando con otros vectores para comprometer grupos más pequeños de víctimas. Una de estas *campañas* [85] de prueba fue documentada por los investigadores de ESET entre el 26 de abril y el 2 de mayo, en la que los operadores de la botnet sustituyeron el típico documento adjunto de Office por archivos LNK maliciosos (LNK/TrojanDownloader.Agent.AMQ). Uno de los nombres de archivo más frecuentes fue form.lnk, que intentaba atraer a las víctimas de Japón (28%), Italia (16%) y México (11%) para que descargaran y ejecutaran el binario Emotet.

Proofpoint [86] documentó una técnica diferente en la campaña de Emotet entre el 4 y el 19 de abril. Los operadores utilizaron señuelos relacionados con los salarios y las bonificaciones, lo que conducía a un archivo ZIP almacenado en OneDrive que, al descomprimirse, contenía archivos de complementos de Microsoft Excel (XLL). Una vez ejecutados, estos archivos lanzan y activan el binario principal de Emotet.

COMENTARIO DE EXPERTOS

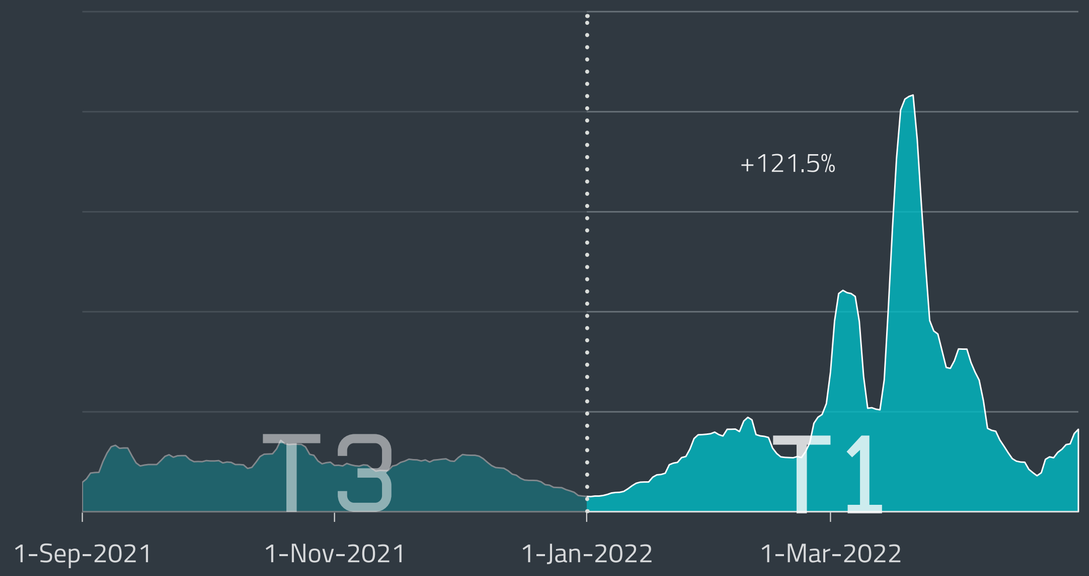
El tamaño de las últimas campañas LNK y XLL de Emotet fue significativamente menor que las distribuidas a través de los archivos DOC comprometidos vistos en marzo. Esto sugiere que los operadores solo están utilizando una fracción del potencial de la botnet mientras prueban nuevos vectores de distribución que podrían sustituir a las macros de VBA, ahora desactivadas por defecto. Tan pronto como uno de los enfoques probados dé resultados satisfactorios, podemos esperar una nueva puesta en marcha de Emotet.

Dušan Lacika, Senior Detection Engineer

Si observamos la categoría Downloaders en general, la tendencia de detección se vio influenciada sobre todo por los picos de la botnet Emotet, que contribuyó significativamente al crecimiento del 121% de toda la categoría entre el tercer cuatrimestre de 2021 y el primero de 2022.

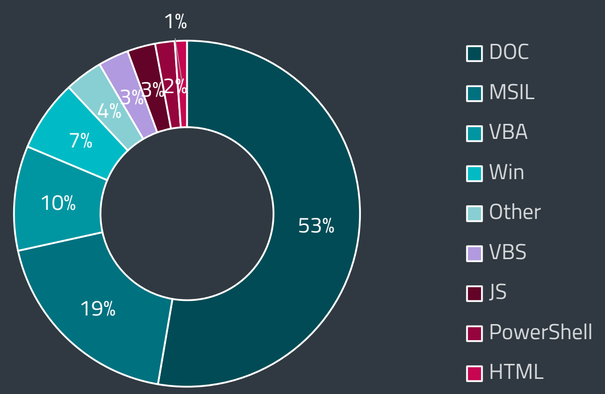
Sin embargo, también hubo otra amenaza que ayudó a sostener esas cifras: MSIL/TrojanDownloader.Agent. Esta familia de downloaders aumentó su actividad un 118% en comparación con el tercer cuatrimestre de 2021 y terminó en segundo lugar en la lista de las 10 principales detecciones, con 18%. Cuatro de sus cinco variantes principales (MSIL/TrojanDownloader.Agent.JBZ, .IYB, .IUU, .JEG) descargaban dos binarios: un payload en forma de archivo EXE, y una herramienta DLL utilizada para ejecutarlo. Los payloads finales se descargaban desde la plataforma Discord e incluían el agente Tesla, Fareit y el troyano MSIL/Agent.CFQ.

El primer cuatrimestre de 2022 es el primer período desde que ESET comenzó a publicar sus Threat Reports

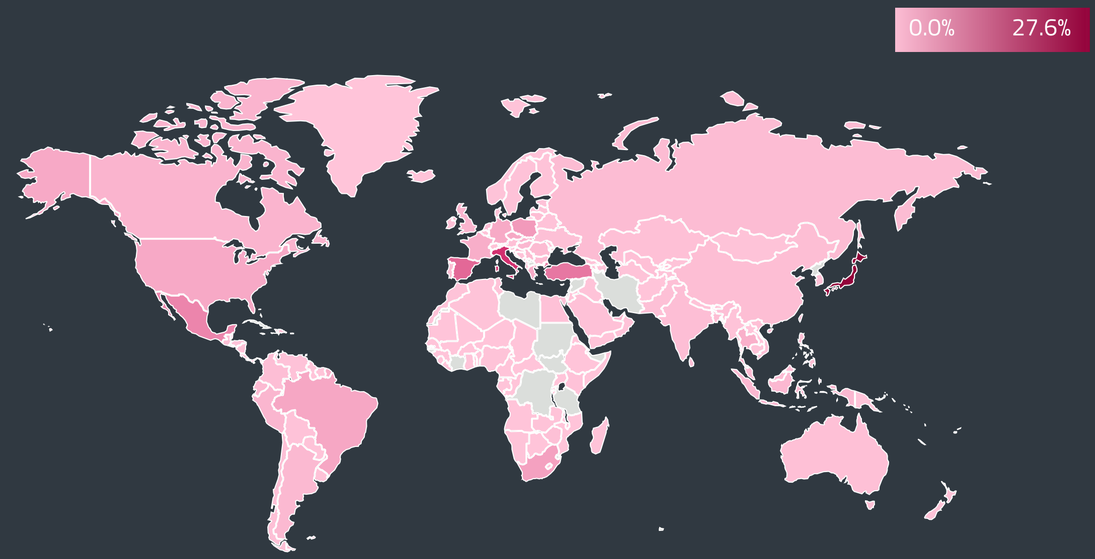


Tendencia de detección de downloaders en el tercer cuatrimestre de 2021 y primero de 2022, promedio móvil de siete días

en el que la plataforma VBA perdió su liderazgo, quedando nada más que en tercer lugar con un 10%. Dado que Microsoft ha deshabilitado las macros por defecto, esperamos ver un descenso continuo de las detecciones de malware mediante VBA en el futuro, ya que los atacantes sustituirán este vector por otros nuevos y más eficaces. La mayor cuota de la plataforma DOC se debe principalmente a las campañas masivas de Emotet en



Detecciones de downloaders por tipo de detección en el primer cuatrimestre de 2022



Distribución global de las detecciones de downloaders en el primer cuatrimestre de 2022

marzo, en las que se utilizaron documentos de Word maliciosos.

El primer cuatrimestre de 2022 también trajo un intento de desmantelamiento. Una coalición de proveedores liderada por la Unidad de Crímenes Digitales de Microsoft tomó medidas contra Zloader, un antiguo troyano bancario que se convirtió en un canal de distribución para otras cepas de malware. El operativo de desactivación se centró en tres botnets específicas vinculadas a la familia de malware. El Equipo de Investigación de ESET contribuyó a la operación proporcionando análisis técnicos e inteligencia sobre amenazas. Encontrará una explicación más detallada del desmantelamiento de Zloader en la sección ***Noticias del Laboratorio*** o en nuestra ***publicación del blog*** [34].

Por otra parte, en el primer cuatrimestre de 2022, el equipo Threat Hunter de Symantec detectó por primera vez un nuevo loader llamado ***Verblecon*** [87]. Según sus conclusiones, se trata de un malware complejo, potente y polimórfico que utiliza mecanismos antianálisis para evitar la detección por parte de las soluciones de seguridad y los investigadores. ESET detecta esta amenaza como Java/Agent.OR.

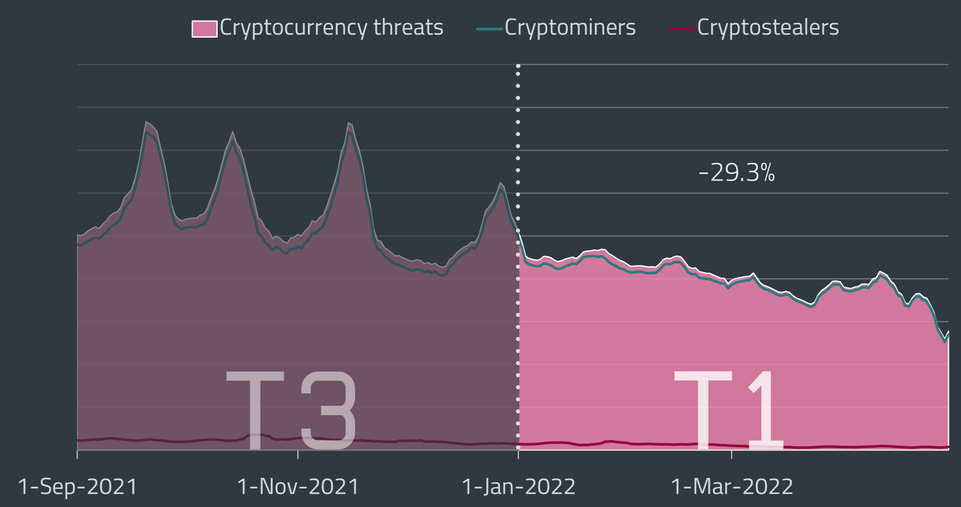
AMENAZAS PARA CRIPTOMONEDAS

Hackeo a plataformas de criptomonedas para obtener importantes beneficios, incluso cuando disminuyen las detecciones de estas amenazas.

El primer cuatrimestre de 2022 no fue el mejor período para las criptomonedas. Aunque sus tasas de cambio estuvieron lejos de colapsar, las criptomonedas más destacadas tuvieron dificultades para alcanzar sus máximos anteriores. El precio del Bitcoin rondó los 40.000 dólares a lo largo del cuatrimestre, y Ethereum solo consiguió superar los 3.500 dólares a principios de año y luego durante unos días en abril. En cambio, las amenazas sí lo pasaron peor que las criptomonedas, ya que su número de detecciones se redujo un 29,3% en el primer cuatrimestre de 2022.

Como se ha explicado en numerosas ocasiones en nuestros Threat Reports, la cantidad de amenazas para criptomonedas se correlaciona hasta cierto punto con sus tasas de cambio. Se podría decir con seguridad que el período de enero a abril no fue muy generoso con estas formas alternativas de pago e inversión. El estancamiento de los valores de las criptomonedas puede *atribuirse a* [88] la agitación general del mercado, causada principalmente por la guerra de Rusia contra Ucrania, junto con la anticipación de las regulaciones monetarias en los Estados Unidos.

Sin embargo, aunque el número de amenazas contra las criptomonedas ha disminuido, siguen siendo tan peligrosas como siempre. A principios de año se produjeron varios hackeos de plataformas de criptomonedas de gran repercusión: los usuarios de la plataforma de cambio de criptomonedas Crypto.com perdieron más de *30 millones de dólares* [89], en su mayoría en Ethereums y Bitcoins, después de que actores malintencionados eludieran la autenticación en dos fases; la plataforma de criptomonedas de cadena cruzada Wormhole fue hackeada por *326 millones de dólares* [90] cuando los ciberdelincuentes aprovecharon una vulnerabilidad en su red; y, por último, OpenSea, el mercado de intercambio de NFT, volvió a ser objetivo de los hackers, que consiguieron robar *cerca de 1,7 millones de dólares* [91] en tokens digitales durante un ataque de phishing.



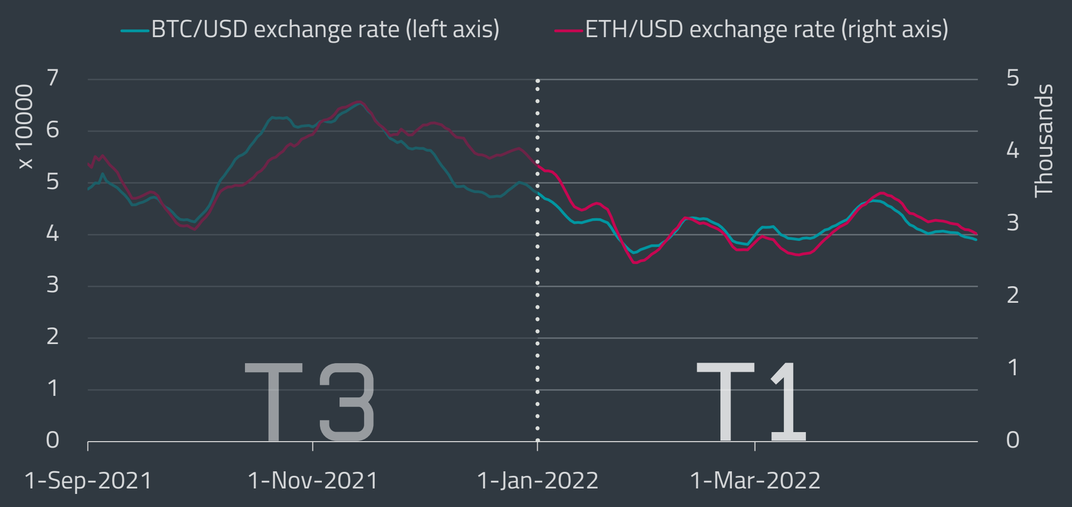
Tendencia de detección de amenazas para criptomonedas en el tercer cuatrimestre de 2021 y primero de 2022, promedio móvil de siete días

COMENTARIO DE EXPERTOS

La guerra en Ucrania, las estrictas sanciones impuestas a las empresas mineras de criptomonedas en Rusia y los crecientes ataques a las plataformas de criptomonedas por los ciberdelincuentes han disminuido la motivación de los actores maliciosos de crear y propagar malware relacionado con las criptodivisas. Por otra parte, las tasas de cambio de las criptomonedas aumentaron luego de que la República Centroafricana adoptara el bitcoin como moneda oficial. Debido a la situación actual, es bastante difícil predecir cómo evolucionará el panorama de las amenazas, pero podemos esperar un aumento a gran escala de los ataques dirigidos, similar a lo que está ocurriendo con el ransomware.

Igor Kabina, ESET Senior Detection Engineer

Los coinminers, que suelen ser la más activa de las subcategorías de amenazas para criptomonedas, disminuyeron un 28,4% entre el tercer cuatrimestre de 2021 y el primero de 2022. No hubo grandes saltos en su actividad hasta el mes de abril, en el que se produjeron dos pequeños picos en las detecciones de la aplicación potencialmente no deseada (PUA) Win/CoinMiner. La primera fue el 11 de abril, cuando se registró una oleada de la variante AGen.D en Francia, y la segunda fue el 20 de abril, encabezada por las variantes TA y SF, ambas vistas principalmente en Japón.



Tipos de cambio Bitcoin y Ethereum/dólar en el tercer cuatrimestre de 2021 y primero de 2022, promedio móvil de siete días

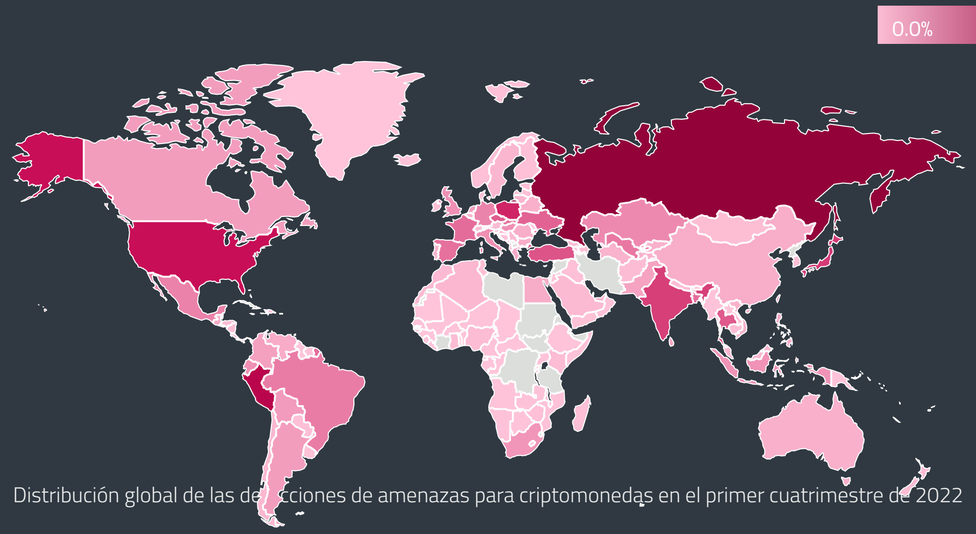
Relación entre troyanos/PUA y entre navegadores/equipos de escritorio en las detecciones de criptominers durante el primer cuatrimestre de 2022

Los tres coinminers más detectados en el primer cuatrimestre fueron la PUA Win/CoinMiner, el troyano Win/CoinMiner y la PUA JS/CoinMiner. La PUA Win/CoinMiner constituyó casi la mitad de todas las detecciones de coinminers, con un 49,2%, aunque su número se redujo un 41,5% en comparación con el período anterior. El troyano Win/CoinMiner tuvo un 12,4% de detecciones y también disminuyó su número un 16,4%. La PUA JS/CoinMiner le siguió de cerca con un 11,8% y sufrió el menor descenso de los tres primeros, que fue del 9,6%. A pesar de la caída en los números, los tres primeros actores lograron mantener las mismas posiciones que en el tercer cuatrimestre del año pasado y, de hecho, las estadísticas generales de 2021.

En el último Threat Report mencionamos que a lo largo de 2021 había surgido una tendencia interesante en cuanto a la relación entre PUA/troyanos y entre equipos de escritorio/navegadores, es decir, que las detecciones de PUA y amenazas para equipos de escritorio iban creciendo de manera constante en cada período. En esta ocasión, sin embargo, tanto las detecciones de troyanos como de malware para navegadores lograron recuperar parte del terreno perdido. En el tercer cuatrimestre de 2021, la proporción de detecciones de PUA frente a troyanos fue de 74% a 26%, mientras que en el primer cuatrimestre de 2022 fue de 69% a 31% respectivamente. En lo que respecta a la relación

	3º cuatrimestre de 2021	1º cuatrimestre de 2022
1	dl-x[.]com	webminepool[.]com
2	wypracowanie.edu[.]pl	dl-x[.]com
3	monerominer[.]rocks	wypracowanie.edu[.]pl
4	carrierecalciatori[.]it	slovolam[.]sk
5	instagrammi[.]ru	carrierecalciatori [.]it
6	newsoholic[.]com	arafifblues[.]com
7	mituus[.]com	kaizoku-ehime[.]jp
8	idaakulubu[.]com	mainevnap[.]com
9	cumpleañosdefamosos[.]com	mituus[.]com
10	slovolam[.]sk	monerominer[.]rocks

Los 10 dominios de criptojacking más visitados en el tercer cuatrimestre de 2021 y el primero de 2022



Distribución global de las detecciones de amenazas para criptomonedas en el primer cuatrimestre de 2022

de detecciones de amenazas mediante navegadores contra equipos de escritorio, fue de 90% a 10% en el tercer cuatrimestre del año pasado y de 87% a 13% en el primero de este año.

El aumento del porcentaje de coinminers a través del navegador debería servir de recordatorio para desconfiar de los sitios web de streaming gratuitos y de los sitios con contenido para adultos, ya que algunos de ellos pueden secuestrar el ordenador del usuario para minar criptomonedas. En el sector izquierdo de la página figura la lista de los 10 dominios de criptojacking más visitados en el tercer cuatrimestre de 2021 y el primero de 2022.

Los coinminers fueron observados principalmente en Rusia, donde ESET registró el 10,6% de sus detecciones, luego Perú con el 6,4%, y Estados Unidos, que presenció el 5% de todos sus intentos de ataque.

El descenso de los cryptostealers fue aún más pronunciado que el de los coinminers: la subcategoría bajó un 51,6%. Sin embargo, el 25 de enero la variante OSF del troyano Win/PSW Delf tuvo un pico en sus detecciones, con la mayor cantidad de intentos de ataque en Turquía, Japón y Hong Kong.

En comparación con el tercer cuatrimestre de 2021, los tres principales cryptostealers se mantuvieron con valores similares, aunque intercambiaron un poco sus posiciones. El troyano Win/Spy.Agent fue el cryptostealer más detectado, con un 37,4% de las detecciones. El troyano Win/PSW.Delf fue el segundo más detectado, con 24,3%, seguido de MSIL/ClipBanker, con 19,5%. Al igual que en el caso de los coinminers, los tres cryptostealers más detectados tuvieron una tendencia a la baja en el primer cuatrimestre. MSIL/ClipBanker sufrió el peor descenso de los tres y cayó casi un 70%.

Según nuestra telemetría, los ataques de los cryptostealers estuvieron bastante repartidos por todo el mundo. Aun así, el país que se enfrentó a más intentos de ataques de cryptostealers en el primer cuatrimestre de 2022 es Perú con 6,9%. Le sigue Turquía, con 4,9%, y el tercer puesto lo ocupa España, con 4,5%.

Las estadísticas por países de todas las detecciones de amenazas para criptomonedas tenían los mismos tres países a la cabeza que en la lista de coinminers: Rusia con un 10,4%, Perú con un 6,4% y Estados Unidos con un 4,9%.

AMENAZAS WEB

La cantidad de direcciones URL de phishing se dispara; los estafadores aprovechan el interés por la guerra entre Rusia y Ucrania.

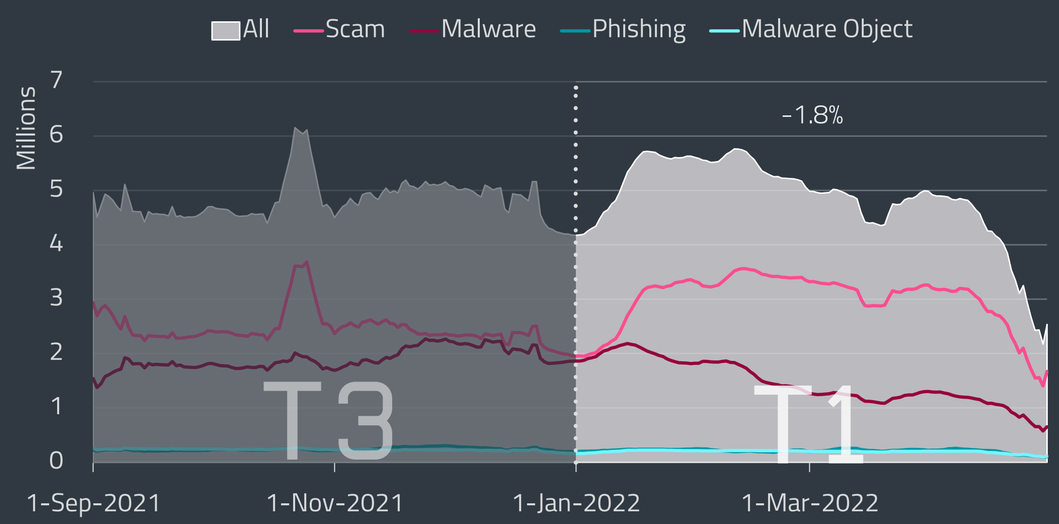
Los primeros cuatro meses de 2022 experimentaron un nivel estable de amenazas web (en su mayoría bloqueadas), con un descenso insignificante del 1,8%. En cuanto al número de direcciones URL únicas bloqueadas, se produjo un descenso del 14,9%. En promedio, la telemetría de ESET registró 4,8 millones de bloqueos diarios de amenazas web y 370 mil direcciones URL dañinas por día.

Los sitios web que distribuyen malware, representados por la categoría Malware, experimentaron el mayor descenso tanto en la cantidad global de bloqueos como en la cantidad de direcciones URL vistas, con una disminución del 26% y el 23% respectivamente. En la categoría Phishing, el número de direcciones URL bloqueadas aumentó casi un 30%. Cabe destacar que no provocó el crecimiento total de bloqueos de phishing, e incluso éstos experimentaron un descenso del 13,2%.

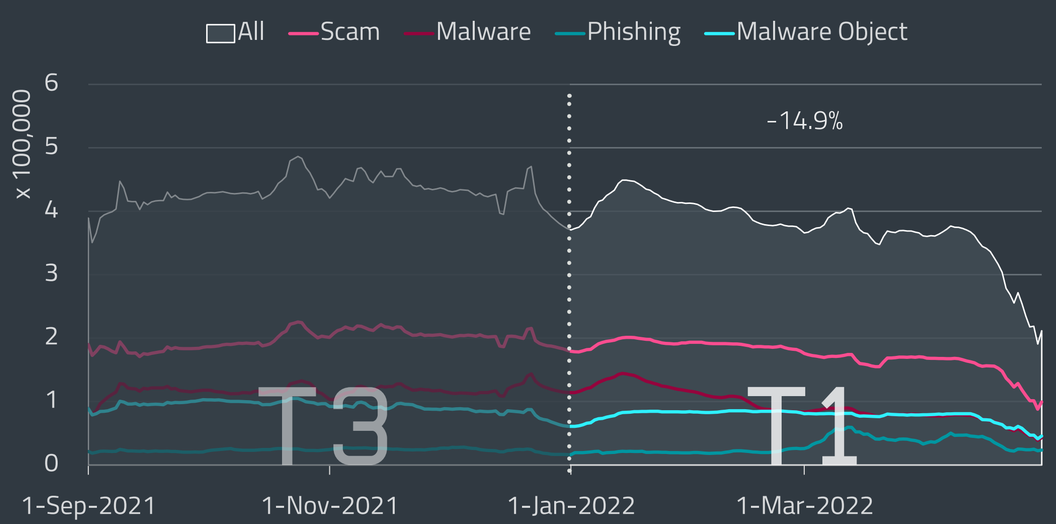
La cantidad de direcciones URL de phishing bloqueadas comenzó a aumentar bruscamente en marzo y los niveles se mantuvieron muy por encima del promedio de este cuatrimestre y del anterior durante el resto del período. El nivel máximo de detección, alcanzado el 7 de marzo, fue tres veces superior a la media diaria del primer cuatrimestre de 2022, con 82.000 direcciones URL únicas bloqueadas.

	Malware	Estafas	Phishing
1	pdloader[.]com	survey-smiles[.]com	propu[.]sh
2	iclickcdn[.]com	newrrb[.]bid	mrproddisup[.]com
3	demotzincky[.]casa	v.vfghe[.]com	tech4-you[.]com
4	aj2396[.]online	bwukxn[.]com	www--bancosantafe--com--ar.insuit[.]net
5	plehimselves[.]info	cellar.z5h64q92x9[.]net	thecred[.]info
6	jecromaha[.]info	loft.z5h64q92x9[.]net	foreign-movies.baby-supernode[.]xyz
7	vk-online[.]xyz	prirodnolijecite[.]com	watchvideoplayer[.]com
8	www.hostingcloud[.]racing	sentrynew.sdh.com[.]ua	update.updtbrwsr[.]com
9	d.ftte[.]fun*	glotorrents[.]pw	medvitro[.]info
10	buikolered[.]com	serch07[.]biz	gelturla[.]com

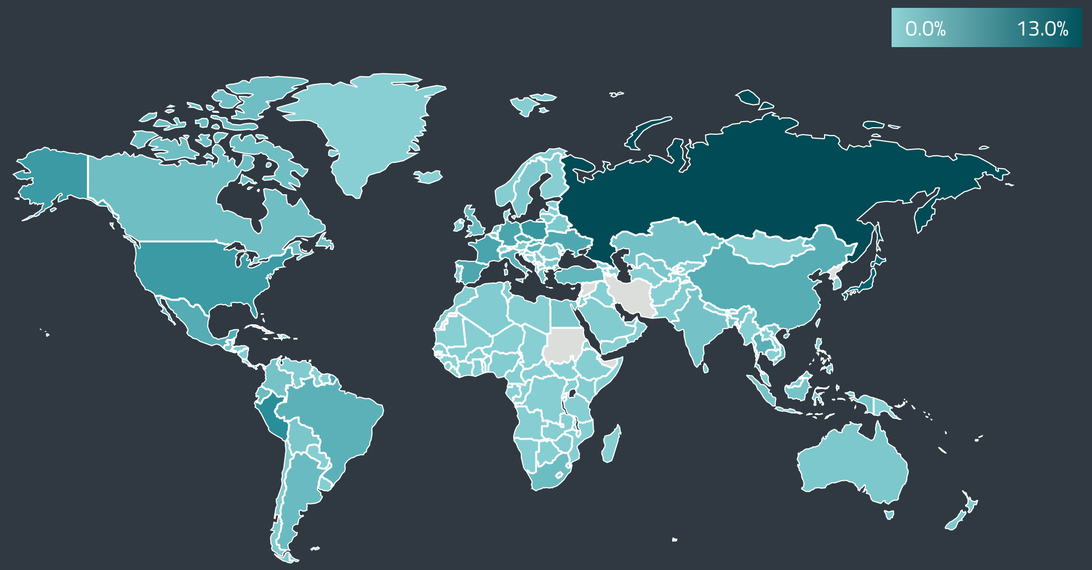
Los 10 dominios de malware, estafas y phishing más bloqueados durante el primer cuatrimestre de 2022; los dominios detectados por primera vez en este período están marcados con un *



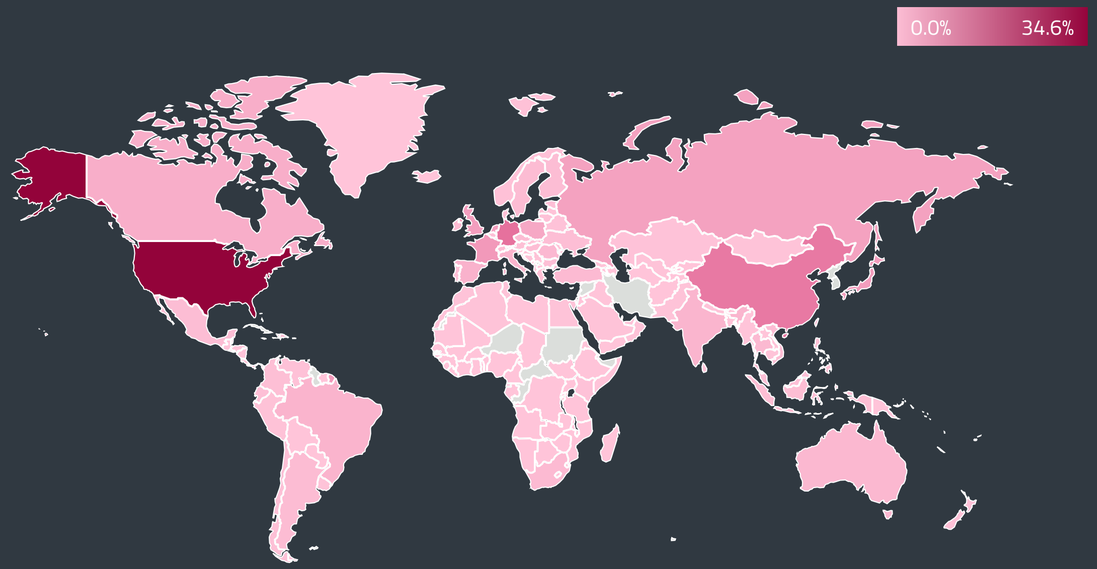
Tendencia de amenazas web bloqueadas en el tercer cuatrimestre de 2021 y primero de 2022, promedio móvil de siete días



Tendencia de direcciones URL únicas bloqueadas en el tercer cuatrimestre de 2021 y primero de 2022, promedio móvil de siete días



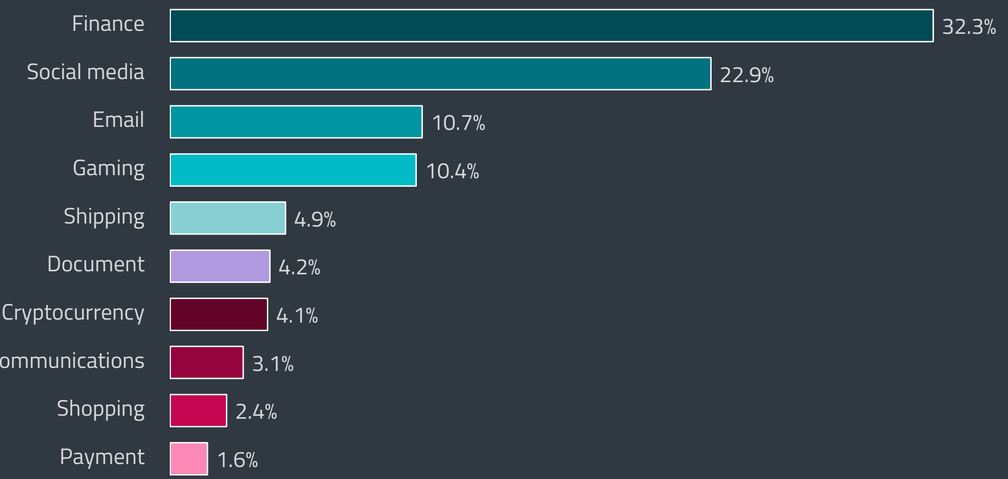
Distribución global de las amenazas web bloqueadas en el primer cuatrimestre de 2022



Distribución global de los dominios de hosting bloqueados en el primer cuatrimestre de 2022

Lo contrario ocurrió con los sitios web de estafas, que tuvieron aproximadamente un 20% más de bloqueos totales, aunque este aumento no se reflejó en el número de direcciones URL vistas. Los bloqueos de los sitios de estafas empezaron a aumentar en la segunda quincena de enero, se mantuvieron en niveles elevados hasta mediados de abril y luego bajaron al mínimo de todo el cuatrimestre.

La invasión rusa de Ucrania provocó una afluencia de campañas de phishing y estafas que se aprovechaban de las personas que intentaban apoyar a Ucrania durante la guerra. En la mayoría de los casos, las campañas utilizaban como señuelo organizaciones benéficas y recaudadores de fondos ficticios. Los primeros dominios fraudulentos que aprovecharon el tema de la guerra empezaron a aparecer casi inmediatamente tras el inicio de la invasión, tal y como documentó el Equipo de Investigación de ESET en *Twitter* [92].

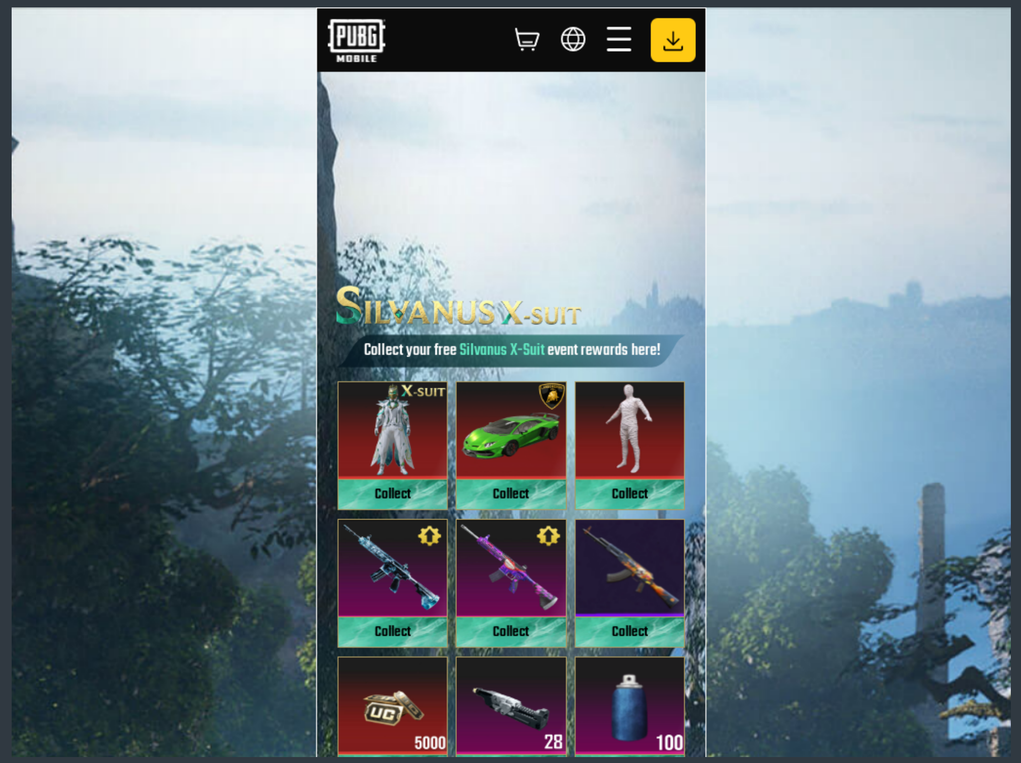


Las 10 principales categorías de sitios web de phishing en el primer cuatrimestre de 2022 por cantidad de direcciones URL únicas

En general, el número de sitios web dañinos bloqueados durante el primer cuatrimestre de 2022 fue mayor en Rusia (13,0% de todos los bloqueos de sitios web), seguido de Japón (9,1%), Perú (4,4%), Polonia (3,9%) y Estados Unidos (3,6%). En cuanto a los países de origen de las amenazas web (conocidos por la geolocalización IP de los dominios bloqueados), más de un tercio de los dominios bloqueados estaban alojados en Estados Unidos (34,2%), seguidos con un amplio margen por Alemania (7,4%), China (6,6%), Francia (3,9%) y Japón (3,5%).

Según las fuentes de phishing de ESET, aproximadamente un tercio de las URL de phishing detectadas en el primer cuatrimestre de 2022 se hicieron pasar por organizaciones financieras, al igual que en el tercer cuatrimestre de 2021. Los señuelos de phishing de redes sociales, representados principalmente por páginas falsas de inicio de sesión de Facebook y WhatsApp, ocuparon el segundo lugar con el 23% de las URL vistas.

[1] The statistic is based on phishing URLs that could be categorized.



Ejemplo de un sitio web de phishing (pubgmystical[.]com) que se hace pasar por un mercado del juego PUBG MOBILE

Tras su auge en el tercer cuatrimestre de 2021, las categorías Compras y Criptomonedas disminuyeron en el primer cuatrimestre de 2022. El phishing con temática de compras online, representado sobre todo por sitios web que suplantan a Amazon, redujo significativamente el número de direcciones URL en circulación, disminuyendo un 73,6% y cayendo del tercer al noveno puesto. Los sitios web de phishing que se hacen pasar por plataformas de criptomonedas retrocedieron del cuarto al sexto puesto, con un descenso del 45% en el número de direcciones URL únicas detectadas.

Por otro lado, los sitios web de phishing que se hacen pasar por servicios de correo electrónico y plataformas de juegos aumentaron en este período, el primero en un 54% y el segundo en un notable 291% según la cantidad de direcciones URL vistas. En la categoría Juegos específicamente, se difundieron los sitios web que simulan ser mercados de diversos juegos online.

Aunque no se encuentra entre las 10 primeras categorías, hubo un notable aumento del 126% en las URL de phishing con temática de viajes. Estas URL maliciosas estaban representadas casi exclusivamente por imitaciones de Airbnb, que a menudo tenían nombres de dominio engañosos; por ejemplo, "airbnb" utilizado como subdominio en lo que en realidad es un dominio no relacionado (como airbnb.com[.]ee).

También se observó una tendencia similar de aumento de los señuelos con temática de viajes en las *Amenazas por correo electrónico*, lo que podría deberse al levantamiento de las restricciones por la pandemia.

En el ámbito de los ataques de homoglifos, los 10 principales objetivos se han reorganizado bastante, ya que ocho de los objetivos son nuevos en la lista y aproximadamente la mitad de los dominios fraudulentos subyacentes aparecieron por primera vez en el primer cuatrimestre de 2022.

Por otra parte, varios de los dominios con homoglifos que prevalecían anteriormente desaparecieron por completo de la escena en este cuatrimestre, y el número total de bloqueos registrados se redujo casi a la mitad en comparación con el tercer cuatrimestre de 2021. Cabe notar que los sitios web falsos relacionados con las criptomonedas (que anteriormente encabezaban la lista junto con los que se hacían pasar por bancos y redes sociales) no se encuentran entre los principales dominios con homoglifos detectados durante este período.

El segundo dominio impostor más frecuente, nuevo en este cuatrimestre, " [.]online" (en lugar de u), probablemente intentaba suplantar el sitio web de Eastman Credit Union. En el momento en que se escribe este artículo, el dominio fraudulento ya no está operativo.

Otros dominios con homoglifos vistos por primera vez en el primer cuatrimestre de 2022, aunque solo con un puñado de bloqueos, intentaban suplantar a Mastercard (masterca d[.]com - en lugar de r), Suncoast Credit Union (suncoastcreditunl n[.]com - l en lugar de i y en lugar de o), LinkedIn (linkedin[.]com - ı en lugar de i) y Twitter (tw tter[.]com - en lugar de i).

Las 10 marcas y nombres de dominio que más sufrieron los ataques de homoglifos en el primer cuatrimestre de 2022

AMENAZAS POR CORREO ELECTRÓNICO

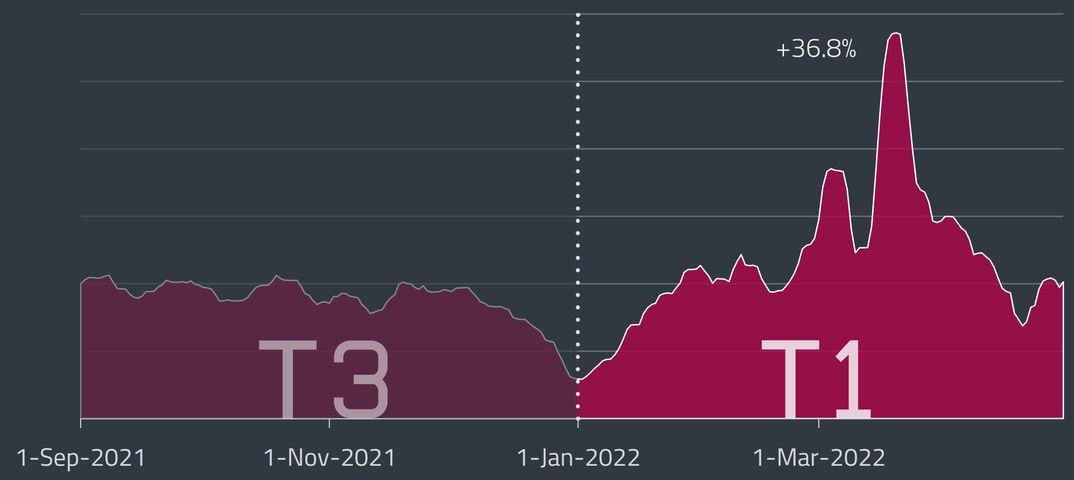
Las amenazas por correo electrónico se disparan a medida que los documentos maliciosos de Emotet desbordan las bandejas de entrada de los usuarios.

Las amenazas por correo electrónico crecieron un 37% en el primer cuatrimestre de 2022, el mayor aumento observado en esta categoría desde 2020. La actividad de las amenazas aumentó continuamente a lo largo de enero y febrero, alcanzó un pico a mediados de marzo (las detecciones diarias de amenazas por correo electrónico triplicaron con creces la media del cuatrimestre), para luego disminuir a lo largo de abril.

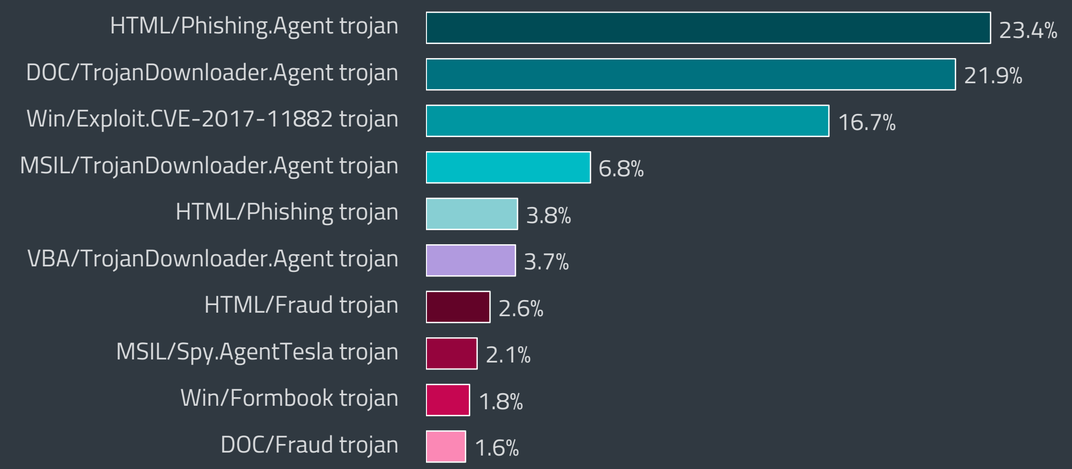
El pico de marzo fue impulsado por las campañas de correo electrónico a gran escala del conocido Emotet, que se basan en documentos maliciosos de Microsoft Word, detectados como variantes de DOC/TrojanDownloader.Agent. La incidencia de DOC/TrojanDownloader.Agent en las bandejas de entrada de los correos electrónicos aumentó nada menos que un 829% en comparación con el tercer cuatrimestre de 2021, lo que lo convierte en la segunda amenaza de correo electrónico más frecuente del período.

Las detecciones de DOC/TrojanDownloader.Agent estuvieron dominadas por sus variantes DPV y DWJ, que generaron la mayor parte del pico de mediados de marzo. Japón fue el país más afectado por estas campañas de Emotet, seguido de Italia y España. Estos tres países también encabezan la lista de detecciones de amenazas por correo electrónico.

Como se comentó en la sección ***Downloaders***, esta campaña precedió a la medida de Microsoft de bloquear las macros de Internet por defecto en los programas de Office. Hacia el final del cuatrimestre, justo cuando el cambio se iba a poner en marcha, los investigadores de ESET notaron que los operadores de Emotet estaban modificando sus tácticas y habían comenzado a utilizar archivos adjuntos maliciosos de correo electrónico LNK, aunque operaban a una escala mucho menor que con sus infames campañas basadas en documentos.



Tendencia de detección de correos electrónicos maliciosos en el tercer cuatrimestre de 2021 y primero de 2022, promedio móvil de siete días



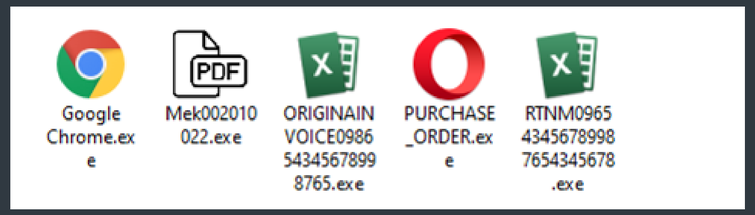
Las 10 principales amenazas por correo electrónico detectadas en el primer cuatrimestre de 2022

COMENTARIO DE EXPERTOS

Las campañas de correo electrónico de Emotet observadas en el primer cuatrimestre de 2022 evocaron un desagradable recuerdo de la prolífica época de la botnet previa a su desmantelamiento en 2020. Sin embargo, con el bloqueo de las macros por parte de Microsoft, la oleada de marzo bien podría haber sido la última avalancha de documentos maliciosos entregados por Emotet que veremos, aunque desafortunadamente, es solo cuestión de tiempo hasta que los ciberdelincuentes encuentren otra vía de distribución con un potencial similar.

Jiří Kropáč, ESET Director of Threat Detection

Otra amenaza que experimentó un crecimiento sustancial en el primer cuatrimestre fue MSIL/TrojanDownloader.Agent, con un aumento del 130% respecto al último cuatrimestre del año pasado. Lo más visto en las bandejas de entrada de los correos electrónicos fue MSIL/TrojanDownloader.Agent.KJO, un troyano utilizado para descargar

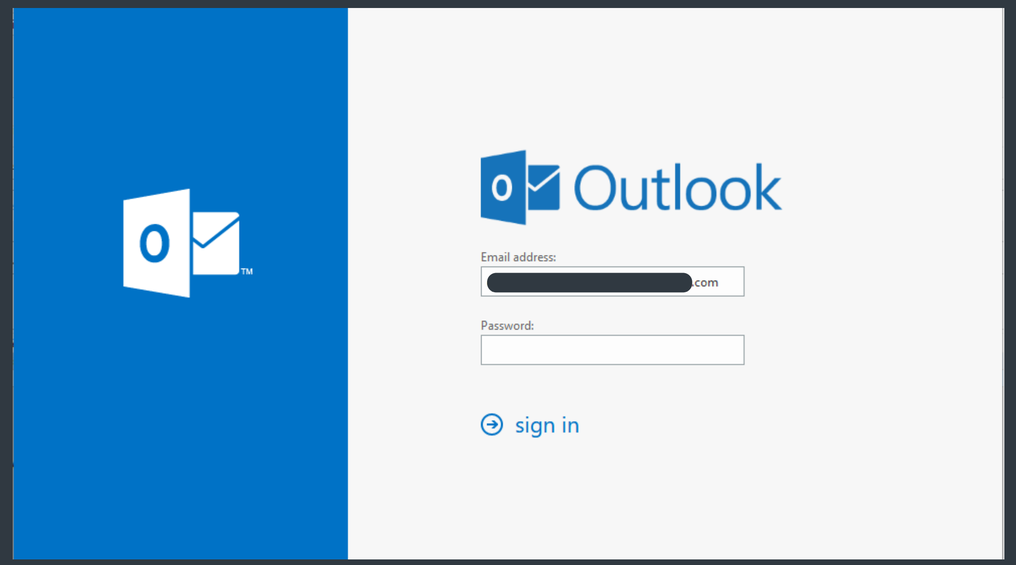


Ejemplos de adjuntos de correo electrónico con MSIL/TrojanDownloader.Agent

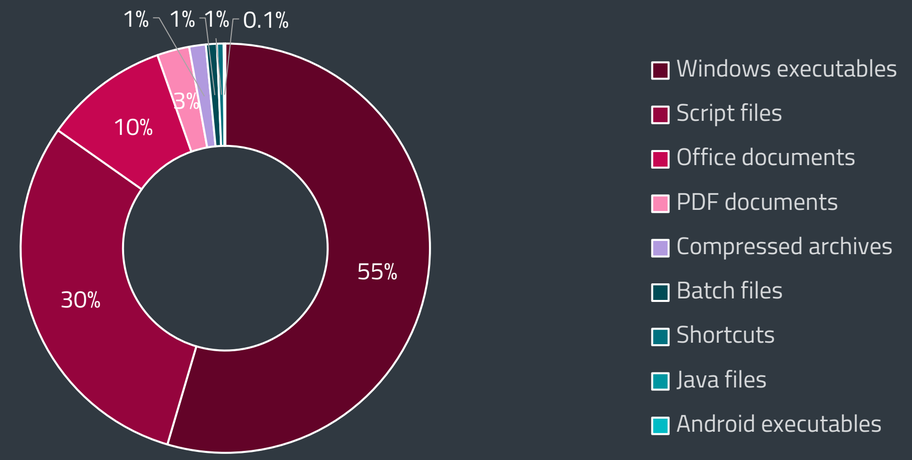
más malware desde la plataforma de comunicación Discord. Se distribuye a través de mensajes de Discord y correo electrónico, en archivos adjuntos EXE que a menudo utilizan íconos para imitar archivos Excel o HTML. El malware descargado suele ser un infostealer avanzado, como Agent Tesla o QBot. La telemetría de ESET muestra una campaña de correo electrónico de MSIL/TrojanDownloader.Agent.KJO de gran envergadura pero de corta duración en febrero, con las cifras de detección más altas en Turquía, Japón y España.

Outlook, DHL y Microsoft fueron las marcas suplantadas con más frecuencia en los correos electrónicos de phishing en el primer cuatrimestre de 2022. Los correos electrónicos que simulan incluir una página de inicio de sesión de Outlook se detectaron en grandes oleadas en febrero y abril, superando en cantidad total de detecciones a los señuelos con temática de DHL (que solían ser los primeros). De hecho, estos correos electrónicos, detectados como HTML/Phishing.Outlook, no consiguieron entrar en la lista de los 10 principales por poco, situándose en el undécimo lugar con el 1,5% de las detecciones totales de amenazas por correo electrónico del cuatrimestre.

Según la telemetría de ESET, HTML/Phishing.Outlook se detectó con mayor frecuencia en el Reino Unido, seguido



Formulario de phishing que se hace pasar por Outlook, detectado como HTML/Phishing.Outlook



Principales tipos de archivos adjuntos en correos electrónicos maliciosos[2] en el primer cuatrimestre de 2022

de Nueva Zelanda y Estados Unidos. Sin embargo, las direcciones de correo electrónico previamente completadas en los formularios de phishing sugieren que el phishing podría haber estado dirigido a las industrias mineras de Kazajistán y África.

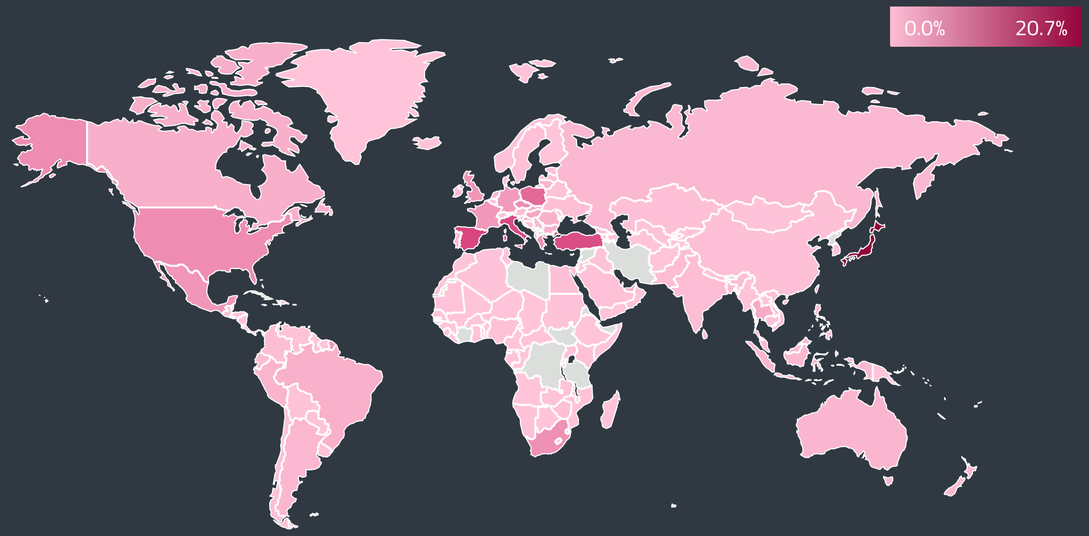
Por otra parte, las campañas de phishing anteriormente activas que se hacían pasar por el servicio de firma de documentos DocuSign disminuyeron en este cuatrimestre: sus detecciones se redujeron un 75% en comparación con el tercer cuatrimestre de 2021.

Al examinar los asuntos de los correos electrónicos maliciosos detectados en el primer cuatrimestre, el más común fue "EU Business Register 2022/2023" (Registro de empresas de la UE 2022/2023), un mensaje actualizado de una estafa generalizada que viene circulando desde hace tiempo y que se ha detectado como PDF/Fraud. A través de estos correos electrónicos, los estafadores intentan engañar a los destinatarios para que paguen una gran cantidad de dinero por su inclusión en una supuesta base de datos comercial europea.

Más allá de los temas habituales de los correos electrónicos maliciosos (como los pagos, los pedidos y las entregas), que se mantuvieron prácticamente sin cambios, en este cuatrimestre hubo un notable aumento de los correos electrónicos maliciosos con temática de viajes. Estos crecieron más de siete veces en comparación con el tercer cuatrimestre de 2021, pero aún así representan menos del 1% de todos los mensajes de correo electrónico maliciosos identificados.

En cuanto a los tipos de archivos adjuntos maliciosos detectados en los correos electrónicos, los ejecutables siguen siendo el formato principal, seguidos de los archivos de script y los documentos de Office. Mientras que la proporción de ejecutables se redujo en el cuatrimestre, los archivos de script y los documentos de Office aumentaron su prevalencia. Los archivos de Office duplicaron su cuota en este período como resultado de la

[2] La estadística se basa en una selección de extensiones conocidas.



Distribución global de las detecciones de amenazas por correo electrónico en el primer cuatrimestre de 2022

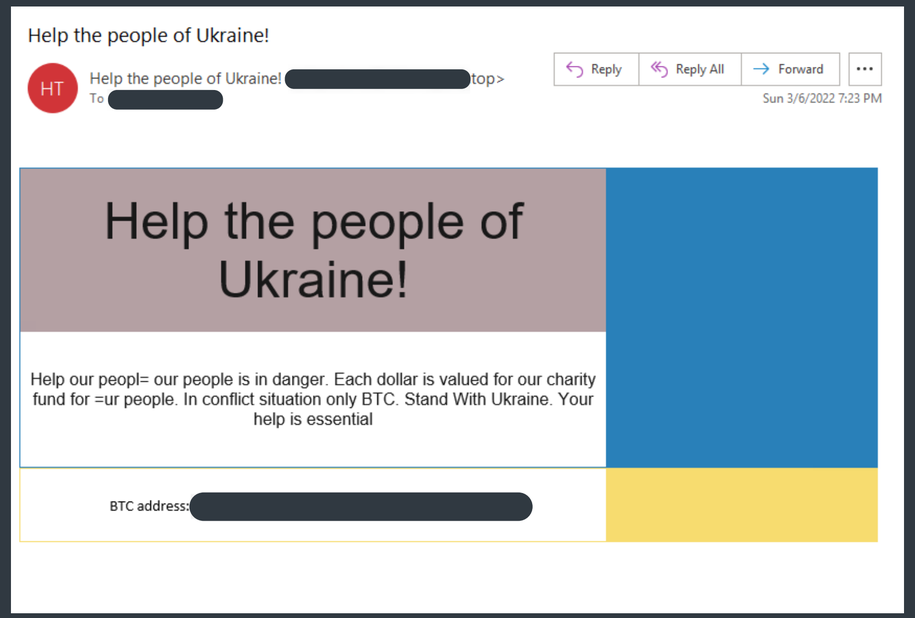
mencionada actividad de Emotet, aunque se espera que esta tendencia se invierta en los siguientes períodos.

Las detecciones de spam aumentaron un 5,8% en el primer cuatrimestre, sobre todo debido a dos grandes picos, el primero el 24 de febrero y el segundo el 12 de abril. La telemetría de ESET registró un aumento general de los mensajes de correo electrónico explorados en esas fechas, pero mientras que el número total de correos electrónicos explorados aumentó solo un 37% con respecto a la media de todo el primer cuatrimestre, los niveles de spam se duplicaron y triplicaron. A excepción de estos picos, los niveles de spam se mantuvieron bastante estables durante este período.

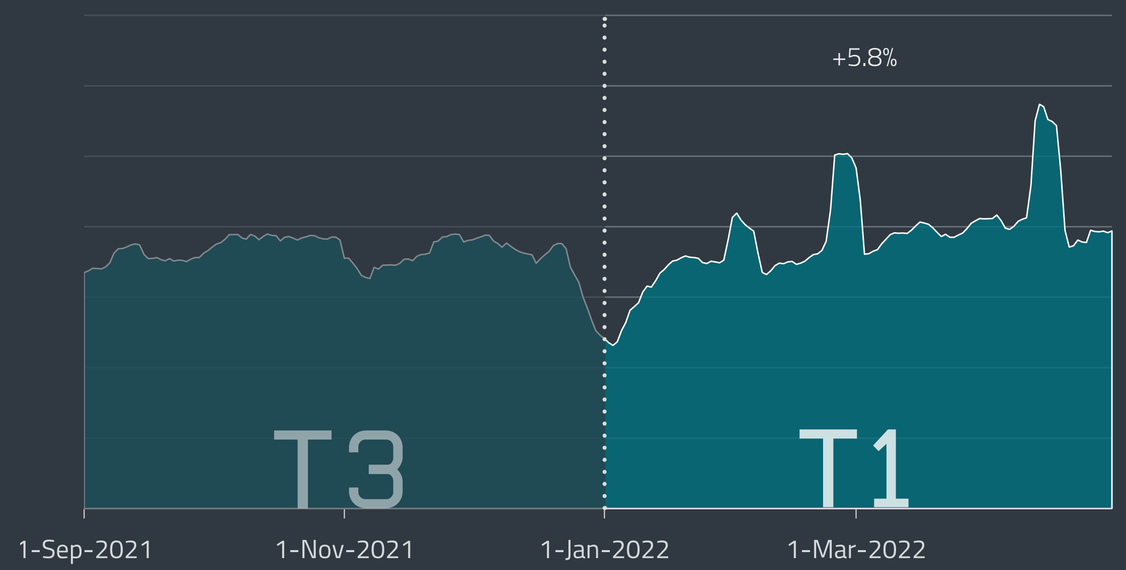
El pico del 24 de febrero coincide con el inicio de la invasión rusa a Ucrania. Como se indica en la sección *Amenazas web*, los estafadores no se privaron de explotar la guerra e inmediatamente empezaron a aprovecharse de las personas que intentaban apoyar a Ucrania, utilizando organizaciones benéficas y recaudadores de fondos ficticios como señuelo.

Si observamos la distribución geográfica de las fuentes de spam según la telemetría de ESET, el 16% de los correos electrónicos de spam detectados en el primer cuatrimestre se originaron en Estados Unidos, seguidos de China (13,2%), Japón (9,9%), Polonia (6,5%) y Francia (5,7%), los mismos cinco países principales que en el período anterior. La proporción de spam en el total de correos electrónicos enviados fue mayor en China (66%), seguida de Singapur, Corea del Sur, Rusia y Argentina, donde entre el 23% y el 34% de los correos electrónicos enviados constituían spam.

Al interpretar estos datos, hay que tener en cuenta que la visibilidad de ESET sobre el spam es limitada debido a que el tráfico de correo electrónico suele filtrarse primero a nivel del proveedor de servicios de correo electrónico en Internet y en otros puntos, antes de llegar a las endpoints protegidas por ESET.



Ejemplo de correo electrónico de spam que utiliza como tema la guerra en Ucrania



Tendencia de detección de spam en el tercer cuatrimestre de 2021 y primero de 2022, promedio móvil de siete días

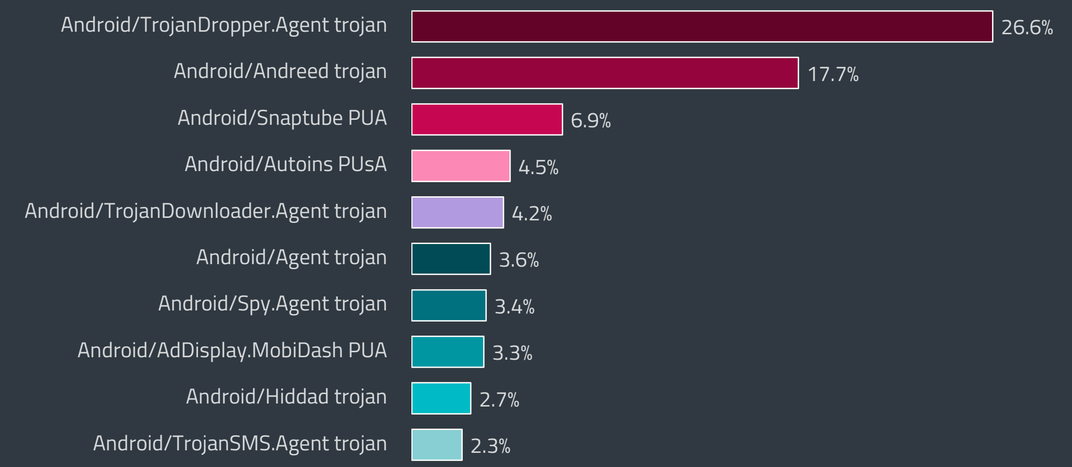
AMENAZAS PARA ANDROID

Las detecciones de amenazas para Android aumentaron ligeramente en el primer cuatrimestre de 2022. Las HiddenApps siguieron siendo el tipo de amenaza para Android más frecuente, mientras que el Spyware experimentó un crecimiento significativo.

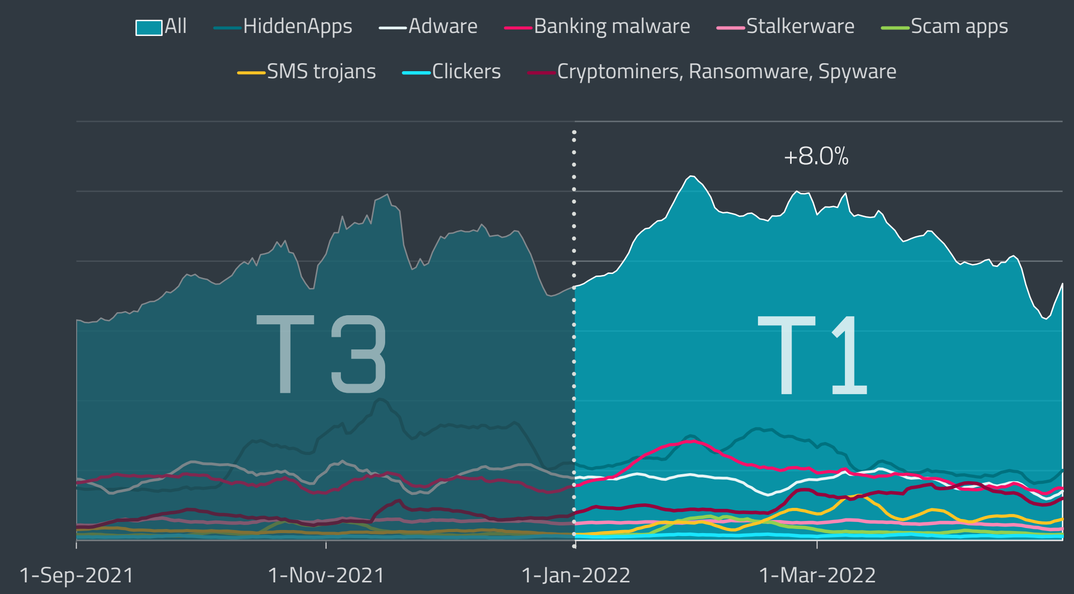
En comparación con los últimos cuatro meses de 2021, las detecciones en Android experimentaron un ligero crecimiento del 8% en el primer cuatrimestre de 2022; sin embargo, no todas las categorías de amenazas para Android experimentaron un mayor número de detecciones.

Las HiddenApps (aplicaciones engañosas que ocultan sus propios íconos) siguieron siendo el tipo de amenaza para Android más frecuente según la telemetría de ESET; aunque sus detecciones disminuyeron un 10,2% en este cuatrimestre.

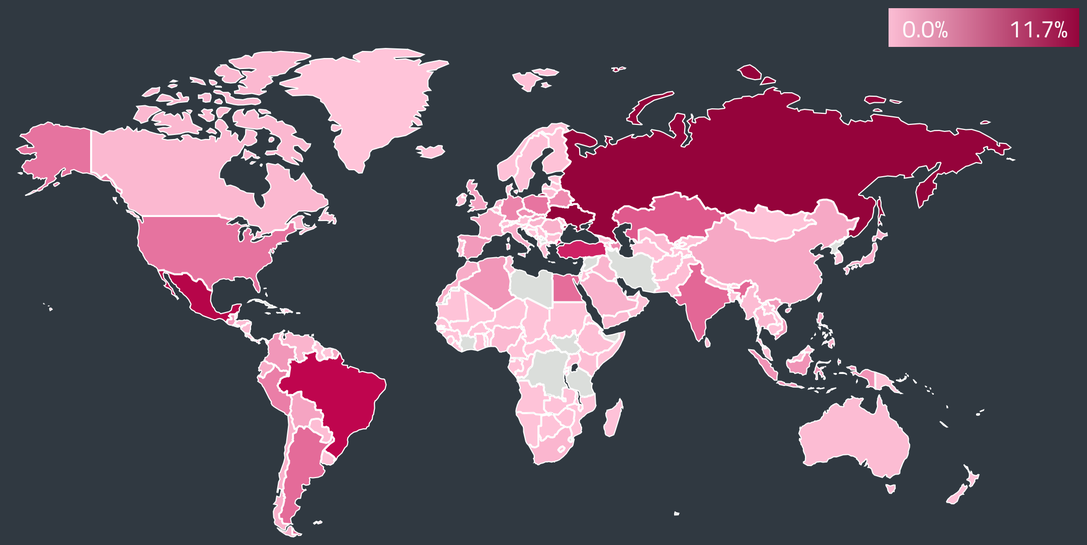
Otra categoría de Android que experimentó un descenso en las cifras de detección es el adware (-11%), continuando la tendencia iniciada en el tercer cuatrimestre de 2021. Las detecciones de stalkerware también descendieron un 11,7% en comparación con el último cuatrimestre del año pasado. ESET monitorea esta categoría de amenazas por separado y no como parte del spyware, aunque el stalkerware es un tipo de spyware para consumidores.



Las 10 principales detecciones de amenazas para Android en el primer cuatrimestre de 2022 (porcentaje de detecciones de amenazas para Android)



Tendencias de detección de categorías seleccionadas de amenazas para Android en el tercer trimestre de 2021 y primero de 2022, promedio móvil de siete días



Distribución global de las detecciones de amenazas para Android en el primer cuatrimestre de 2022

Es importante recalcar las conclusiones del *análisis exhaustivo* [93] que hizo el Equipo de Investigación de ESET sobre el stalkerware. Una investigación de TechCrunch reveló que algunas de las aplicaciones de stalkerware identificadas en el análisis anterior de ESET están de hecho controladas por un operador que es, según *afirman* [94], una empresa con sede en Vietnam llamada 1Byte. Tal y como demostró ESET, estas aplicaciones de stalkerware suelen estar repletas de vulnerabilidades, exponiendo no solo a la víctima sino también al comprador de dichas aplicaciones.

El ransomware para Android también experimentó una importante caída en sus detecciones en el primer cuatrimestre de 2022 (-49,3%). Este descenso puede explicarse por la alta volatilidad de las criptomonedas que se suelen utilizar para pagar los rescates, lo que significa que es difícil hacer predicciones sobre cualquier amenaza que utilice criptomonedas.

La categoría que experimentó el mayor crecimiento fue la de Spyware (170,2%). Este tipo de amenaza es capaz de acceder a diversas funciones del smartphone (como las grabaciones de audio y video), y el gran aumento de sus detecciones implica que los atacantes tienen muchas formas distintas de monetizar los datos personales o incluso corporativos a los que se puede acceder a través de un dispositivo Android. Los investigadores de *Lab52* [95] identificaron un spyware que toma el control total del dispositivo y su contenido cuando el usuario acepta los permisos de la aplicación maliciosa. ESET detecta esta amenaza como "una variante del troyano Android/Spy.Agent", que ocupa el séptimo lugar en la lista de las 10 principales detecciones de amenazas para Android.

Los investigadores Joel Reardon y Serge Egelman de *AppCensus* [96] descubrieron varias aplicaciones disponibles en Google Play que contenían código malicioso para recopilar números de teléfono, direcciones de correo electrónico y datos de localización. Algunas de ellas se habían descargado más de 10 millones de veces antes de que Google las retirara. No obstante, posteriormente volvieron a aparecer en la tienda, aunque sin el kit de desarrollo de software (SDK) responsable de la recopilación de datos. Los investigadores relacionaron estas aplicaciones con una empresa con sede en Panamá que, según el *Wall Street Journal* [97] (paywall), está vinculada a un contratista de defensa estadounidense que presta servicios de ciberinteligencia.

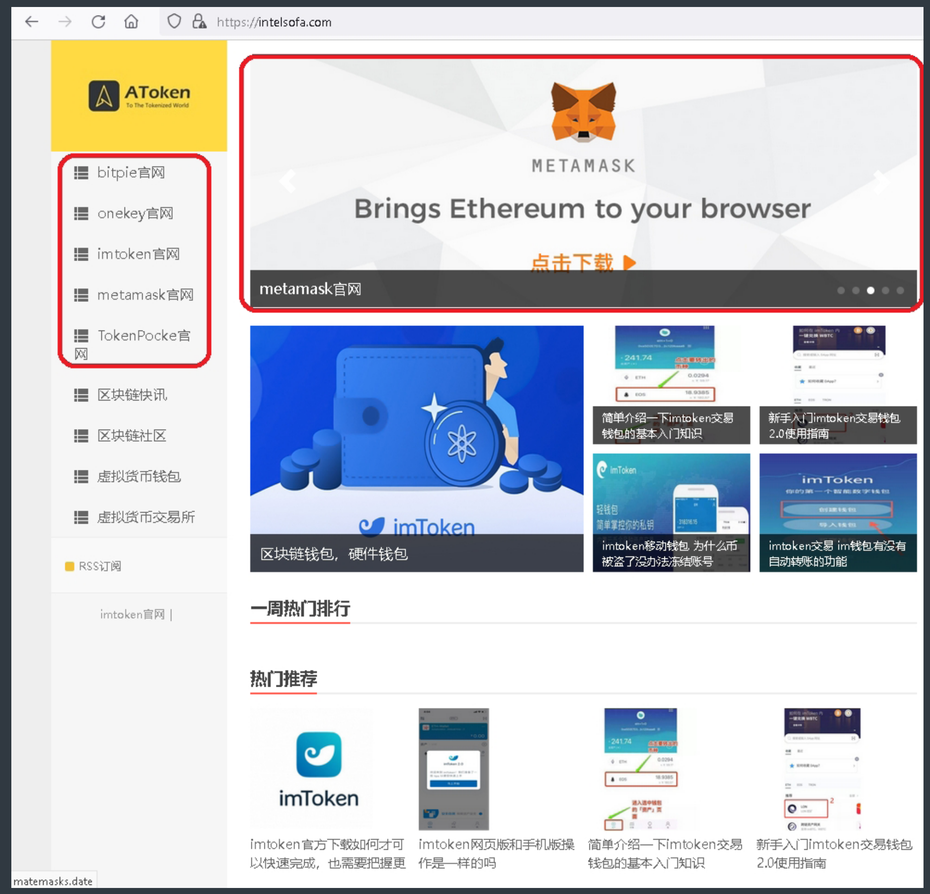
COMENTARIO DE EXPERTOS

El spyware no roba dinero directamente a sus víctimas; en cambio, roba la mayor cantidad posible de datos confidenciales del dispositivo móvil afectado. A continuación, el atacante crea un paquete con datos de una gran cantidad de víctimas y lo vende en el mercado negro al mejor postor o, básicamente, a cualquiera. Es posible que las víctimas nunca sepan cuándo se utilizarán sus datos indebidamente. En muchos casos, el robo de identidad personal los tomará por sorpresa años más tarde y no podrán conectarlo con ninguna acción que pueda haberlo ocasionado. Por lo tanto, la mayoría de las personas afectadas por este aumento reciente en las detecciones de spyware aún no saben que se han convertido en víctimas.

Lukáš Štefanko, ESET Malware Researcher

Además, *Pradeo* [98] describió otro programa espía, instalado por más de 100.000 usuarios gracias a un nuevo vector de distribución. El programa espía Facestealer estaba disponible en la tienda de Google Play como una herramienta para crear dibujos animados a partir de una fotografía y utilizaba la ingeniería social para robar las credenciales de Facebook. Más tarde, Google eliminó la aplicación maliciosa de su tienda.

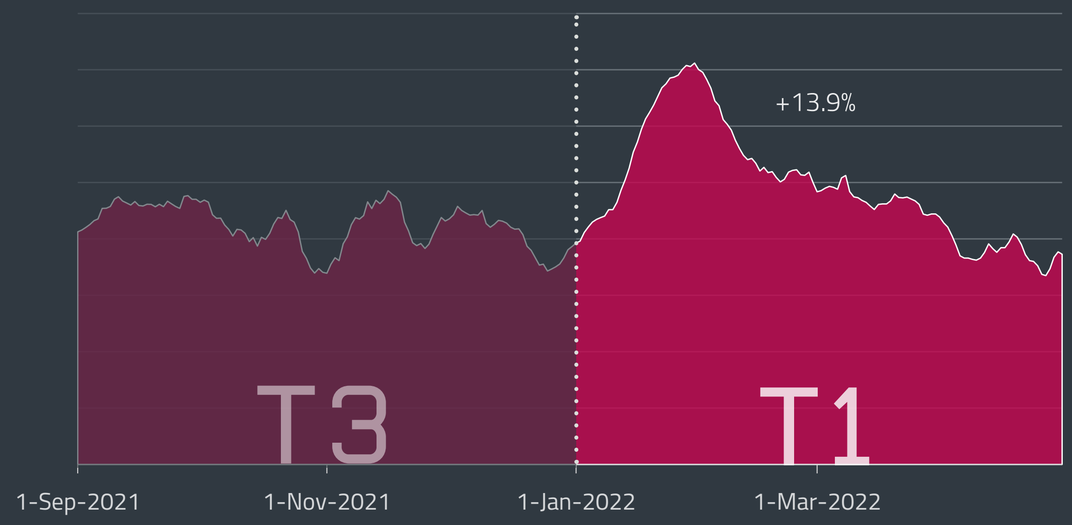
Otras categorías de malware para Android que experimentaron un aumento significativo en sus detecciones fueron las aplicaciones fraudulentas (27,7%), los clickers (31,6%) (que son una forma de fraude publicitario) y los troyanos SMS (145,20%). Esta última amenaza, que se hace visible en la factura mensual del dispositivo móvil de los usuarios afectados, figura en la lista de las 10 principales amenazas para Android como Android/TrojanSMS.Agent.



Página con publicidad de billeteras falsas

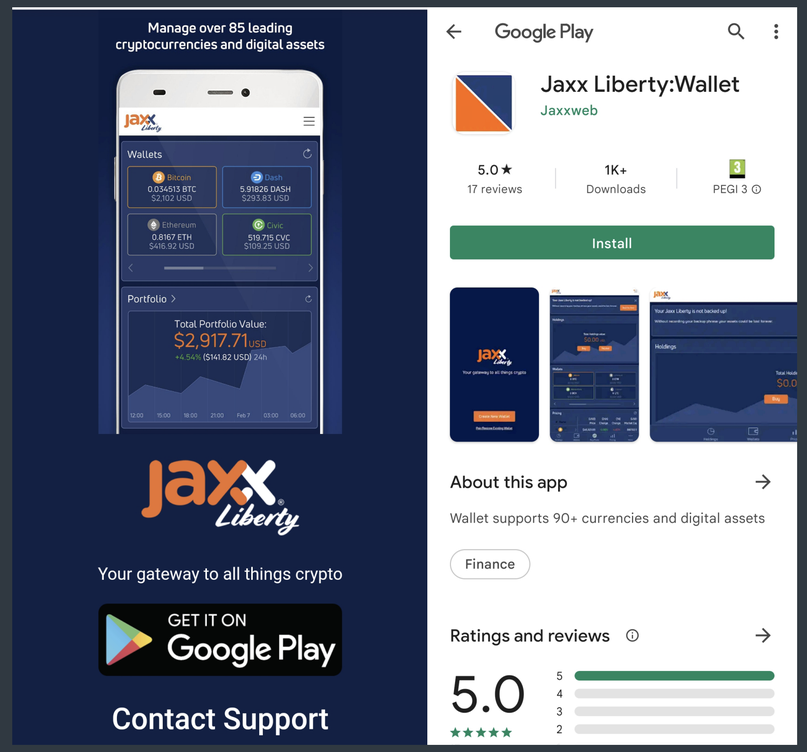
Las detecciones de criptominers para Android se duplicaron en el primer cuatrimestre de 2022, sin embargo, su número total en dicha plataforma es demasiado bajo para juzgar si este crecimiento tiene alguna relevancia. Como los investigadores de ESET ya han señalado en varias ocasiones en el pasado, las criptoamenazas dependen de monedas a veces muy volátiles; y cuando el bitcoin parecía estar recuperando lentamente su valor tras varios meses malos, los *investigadores de ESET descubrieron* [33] un sofisticado esquema que distribuye aplicaciones troyanizadas para Android e iOS haciéndose pasar por populares billeteras de criptomonedas.

Estas aplicaciones maliciosas son capaces de robar las frases secretas de las víctimas haciéndose pasar por Coinbase, imToken, MetaMask, Trust Wallet, Bitpie, TokenPocket o OneKey. Se trata de un vector de ataque sofisticado, donde el autor del malware tuvo que estudiar en profundidad las aplicaciones legítimas empleadas para poder insertar su propio código malicioso en lugares donde sería difícil de detectar, al tiempo que se aseguraba de que dichas aplicaciones manipuladas no perdieran su funcionalidad original. Todas las docenas de aplicaciones de billeteras de criptomonedas troyanizadas detectadas por ESET se distribuían a través de sitios web que imitaban servicios legítimos. Para empeorar las cosas, su código fuente se filtró online, lo que significa que podría atraer a otros atacantes.

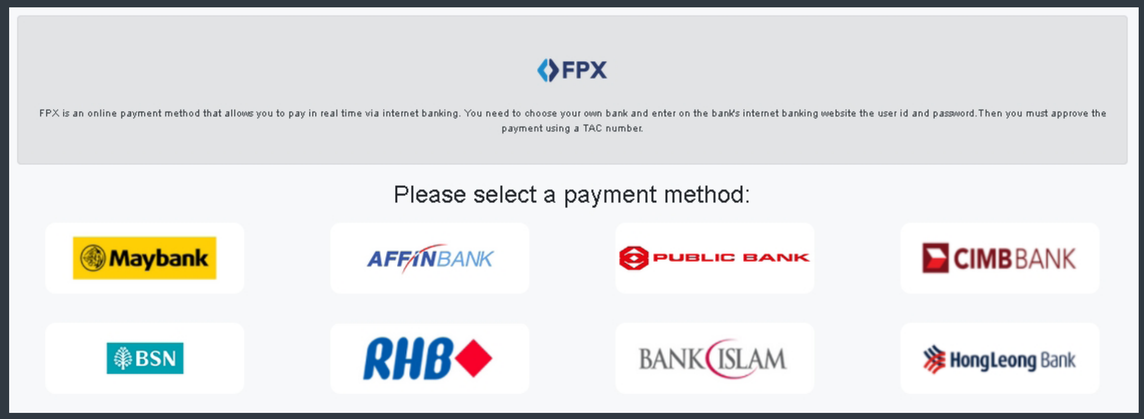


Tendencia de detección de malware bancario para Android en el tercer cuatrimestre de 2021 y primero de 2022, promedio móvil de siete días

Los investigadores de ESET también encontraron aplicaciones maliciosas que suplantaban la aplicación legítima Jaxx Liberty Wallet en la tienda Google Play. Una de las aplicaciones utilizaba un sitio web falso de imitación como vector de distribución. Como el actor de la amenaza responsable de esta aplicación maliciosa consiguió colocarla en la tienda oficial de Google Play, el sitio web falso redirigía al usuario para que descargara su versión móvil desde la tienda de Google Play y no tuviera que utilizar una tienda de aplicaciones de terceros como



Sitio web falso que redirige al usuario para instalar la aplicación falsa desde Google Play



Bancos malayos afectados por las aplicaciones maliciosas

intermediario. Google retiró 13 de estas aplicaciones de su tienda en enero de 2022.

El malware bancario para Android creció un 13,9% en el primer cuatrimestre de 2022, tras experimentar un descenso en el tercer cuatrimestre de 2021. En la lista de las 10 amenazas principales para Android, estaba representado por Android/TrojanDropper.Agent. Uno de los casos de malware bancario para Android que los investigadores de ESET analizaron durante este cuatrimestre fue una campaña dirigida a los clientes de *ocho bancos malayos* [31]. El malware se distribuye a través de sitios web que copian servicios legítimos, la mayoría de los cuales son servicios de limpieza disponibles en Malasia.

Estos sitios web de imitación incluyen botones que dicen descargar aplicaciones de Google Play. Sin embargo, estos botones no conducen realmente a la tienda de Google Play, sino a aplicaciones maliciosas controladas por los atacantes. Las aplicaciones maliciosas simulan vender bienes y servicios con una interfaz similar a la de las tiendas legítimas. A la hora de pagar, se abre una página de pago falsa donde se les pide a las víctimas que seleccionen uno de los ocho bancos malayos e introduzcan sus credenciales bancarias online.

Muchos otros investigadores también descubrieron nuevos programas maliciosos bancarios para Android o nuevos vectores de distribución. *Check Point* [99] halló Sharkbot haciéndose pasar por aplicaciones de seguridad en la tienda Google Play, *Bitdefender* [100] identificó nuevas campañas de FluBot y TeaBot que se propagan a través de mensajes SMS que preguntan "Is this you in this video?" ("¿Eres tú el de este video?"), mientras que los investigadores de *Threat Fabric* [101] analizaron otro malware bancario para Android, Medusa, que inició un esquema de distribución utilizando el mismo servicio de phishing por SMS que FluBot. *También* [102] descubrieron una nueva amenaza que denominaron Xenomorph, dirigida a usuarios de 56 bancos europeos diferentes. Todas las amenazas mencionadas son detectadas por ESET como variantes del troyano Android/TrojanDropper.Agent. Según la telemetría de ESET, los países con mayores detecciones de esta amenaza de malware bancario paraguas son Brasil, México, Turquía, Argentina y Ucrania.

Y para demostrar que Android también puede sufrir vulnerabilidades de gran impacto, los *investigadores de la Universidad de Tel-Aviv* [103] descubrieron que los teléfonos de Samsung se entregaban con defectos de diseño en los servicios de gestión de claves criptográficas respaldados por hardware de Android. La falla afectó a millones de teléfonos emblemáticos de Samsung, incluyendo Galaxy S8, S9, S10, S20 y S21.

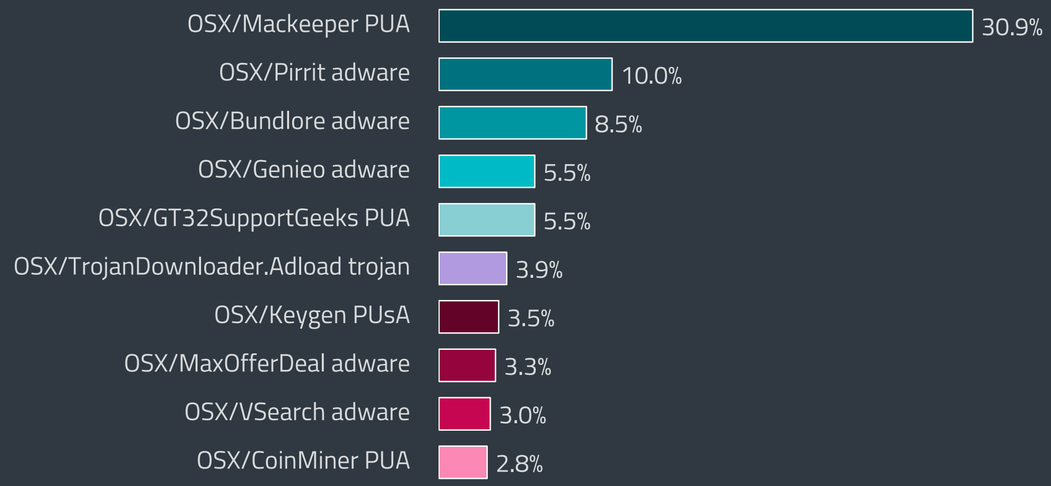
AMENAZAS PARA macOS E iOS

Las cifras de detección de amenazas para macOS experimentaron un notable descenso en el primer cuatrimestre de 2022. En comparación con el tercer cuatrimestre de 2021, el mayor descenso se produjo en la categoría Troyanos.

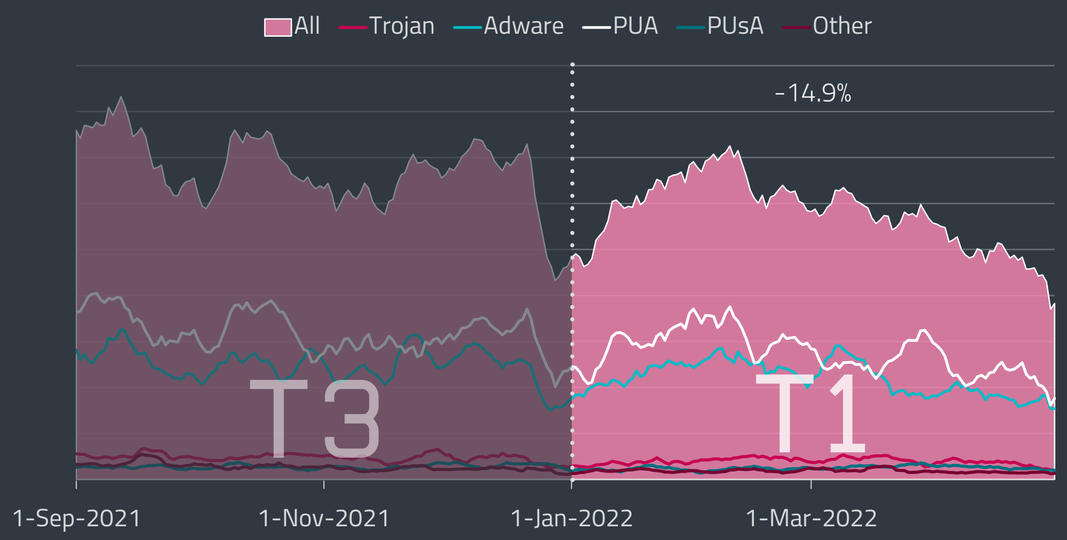
En el primer cuatrimestre de 2022, las detecciones de amenazas para macOS experimentaron un notable descenso (14,9%) y, lo que es más, se detectó una baja importante en todas las categorías de amenazas para macOS monitoreadas. Los troyanos experimentaron la mayor caída (-18,8%) en comparación con el tercer cuatrimestre de 2021 seguidos de las aplicaciones potencialmente no deseadas (PUA, -15,6%). Este tipo de amenaza es el peligro más extendido dirigido a los sistemas Mac: representó alrededor del 47% de todas las detecciones de amenazas para macOS durante los primeros cuatro meses de 2022, visible también en la lista de las 10 principales amenazas para macOS según la telemetría de ESET. La detección número uno en macOS, la PUA OSX/Mackeeper, es la misma desde nuestro Threat Report del primer trimestre de 2020, aunque ahora con una mayor prevalencia. En el primer cuatrimestre de 2022 fue responsable de más del 30% de todas las detecciones de amenazas para macOS. Esta PUA, que muestra anuncios no solicitados, estuvo más activa en Estados Unidos y Japón.

Otros ejemplos de este tipo de aplicaciones, que llevan la descripción de un programa supuestamente útil y engañan a los usuarios para que las instalen, son las PUA OSX/GT32SupportGeeks y OSX/CoinMiner, que ocupan los puestos cinco y diez de la lista de las 10 principales amenazas para macOS. La primera suele presentarse como un analizador del rendimiento que informa sobre supuestos problemas en el sistema macOS; la segunda utiliza los recursos del sistema para minar monedas digitales.

El adware (-13,8%) y las aplicaciones potencialmente no seguras (PUsA, -12,7%) también disminuyeron en el primer cuatrimestre; sin embrago, el adware fue la segunda amenaza más frecuente para macOS en el período, con un 38% de prevalencia global. En la lista de las 10 principales amenazas para macOS, el adware está representado por OSX/Pirrit, OSX/Bundlore, OSX/Genieo, OSX/MaxOfferDeal y OSX/VSearch. OXS/Bundlore es conocido por "empaquetar" aplicaciones de adware junto con las aplicaciones legítimas, mientras que OSX/Genieo, OSX/MaxOfferDeal y OSX/VSearch interceptan las búsquedas en Internet. Todas las aplicaciones de adware mencionadas anteriormente muestran anuncios intrusivos.



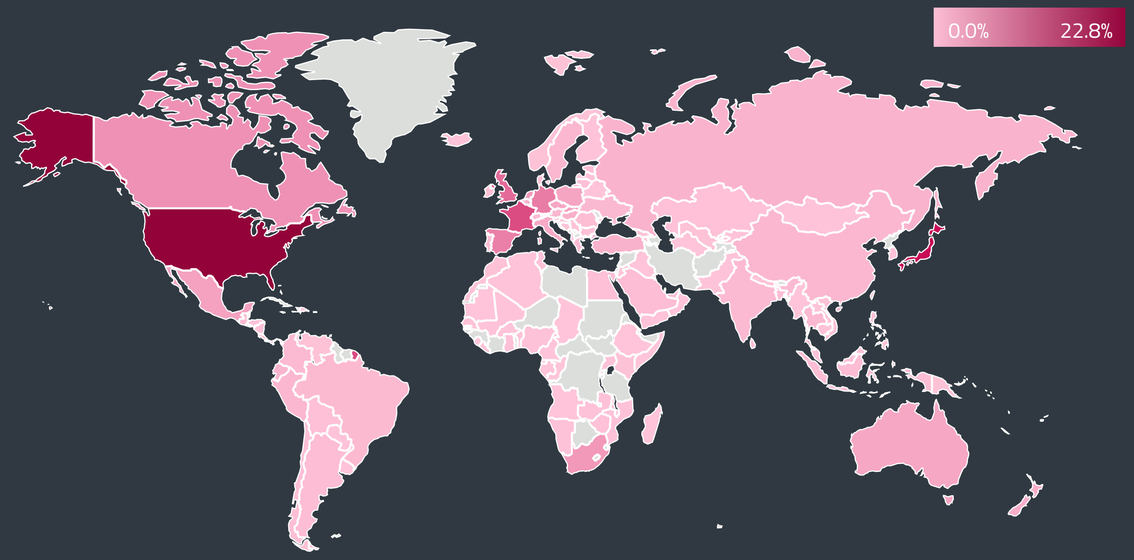
Las 10 principales detecciones de amenazas para macOS en el primer cuatrimestre de 2022



Tendencia de detección de amenazas para macOS en el tercer cuatrimestre de 2021 y primero de 2022, promedio móvil de siete días

Según la telemetría de ESET, el mayor número de detecciones de amenazas para macOS en el primer cuatrimestre de 2022 se produjo en Estados Unidos, con un 21,6%, seguido de Japón (12,8%), Reino Unido (7,2%), Sudáfrica (5,9%) y Francia (5%). El notable descenso hacia finales de 2021 y principios de 2022 es similar al detectado el año anterior, y podría atribuirse a la época específica del año en la que la gente de todo el mundo celebra diversas festividades religiosas y culturales, y simplemente no utiliza sus computadoras con tanta frecuencia.

Con el fin de redactar nuestros Threat Reports, es importante señalar que a fin de año cambiamos la metodología de análisis de la prevalencia de las amenazas para macOS con el objetivo de describirlas y monitorearlas de una manera más real. Asimismo, también se han recalculado los datos del período anterior para poder analizar datos comparables en este informe. Y aunque el número global de detecciones de amenazas para macOS está efectivamente disminuyendo, las empresas, organizaciones y personas de alto perfil deben tener en cuenta que, si un objetivo es lo suficientemente interesante, los actores de amenazas o grupos de APT también desplegarán malware dirigido a otros sistemas que no sean Windows.



Distribución global de las detecciones de amenazas para macOS en el primer cuatrimestre de 2022

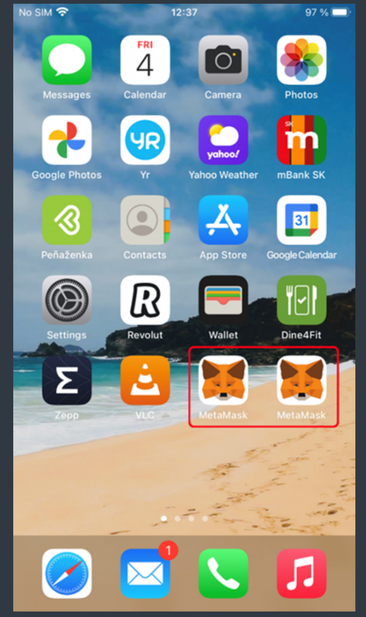
El último hallazgo del Equipo de Investigación de ESET de un caso como este es una amenaza *compilada tanto para Intel como para los nuevos procesadores de silicio de Apple* [104] utilizados en la línea de producción de equipos Mac. Este malware, detectado por ESET como OSX/NukeSped.N, es un ejecutable que se hace pasar por un documento con la descripción de un puesto de trabajo; los investigadores de ESET creen que forma parte de una campaña del infame grupo de APT Lazarus, que tiene una amplia experiencia en ocultar malware en falsos señuelos de ofertas laborales.

A principios de año, los investigadores de ESET publicaron su análisis sobre el sitio web comprometido de una emisora de radio prodemocracia de Hong Kong. El sitio distribuía un exploit para Safari que instalaba malware de ciberespionaje en los dispositivos macOS de los visitantes. *DazzleSpy* [46], como lo llamó ESET, es un malware para macOS que la telemetría de ESET no había visto hasta el momento. Sus funciones incluyen la recopilación de información sobre el sistema; la búsqueda, descarga y carga de archivos; la extracción de la cadena de claves de macOS; y el acceso del agresor a través del escritorio remoto. Los comentarios en su código sugieren que también podría atacar dispositivos iOS y otros dispositivos que tuvieran habilitado el Código de Autenticación de Puntero (PAC), como el iPhone XS y los modelos más nuevos. Dada la complejidad de los exploits utilizados en esta campaña, los investigadores de ESET consideran que el grupo responsable de esta operación tiene una gran capacidad técnica.

Otra amenaza multiplataforma, llamada *SysJoker* [105], fue descubierta por los investigadores de Intezer. *Objective-See* [106] describió con detalle la versión para macOS de este malware. SysJoker se hace pasar por una actualización del sistema y forma parte de una campaña de espionaje; Intezer evalúa que este backdoor persigue objetivos muy específicos. La telemetría de ESET sugiere lo mismo: SysJoker tiene una baja prevalencia con detecciones principalmente en Asia y Estados Unidos. *Volexity* [107] también descubrió una nueva variante para macOS de una familia de malware multiplataforma con muchas funciones, denominada Gimmick. Utiliza servicios de alojamiento en la nube pública (como Google Drive) para las funciones de Comando y Control.

A pesar de sus funciones de seguridad integradas, los dispositivos iOS también son objeto de ciberamenazas y ataques dirigidos. Como se describe en la sección *Amenazas para Android*, los investigadores de ESET descubrieron *billeteras de criptomonedas maliciosamente alteradas* [33] para robar las frases semilla de las víctimas no solo en dispositivos Android sino también iOS. Estas aplicaciones maliciosas no están disponibles en la App Store de Apple; deben descargarse e instalarse usando perfiles de configuración, que añaden un certificado de firma de código de confianza arbitrario. Utilizando estos perfiles, es posible descargar aplicaciones no verificadas por Apple, desde fuentes ajenas a la App Store.

Esto significa que el eslabón más débil de la seguridad en estos casos es el usuario. No obstante, no todas las amenazas pueden ser detectadas por el comportamiento seguro del usuario y las herramientas de seguridad, como ocurre con el malware de hackeo de teléfonos Pegasus, mencionado varias veces en los ESET Threat Reports pasados. Mientras salen a la luz nuevas revelaciones sobre las últimas víctimas de esta herramienta de espionaje del grupo NSO, como el *presidente del Gobierno de España* [108] y *diplomáticos finlandeses* [109], Reuters *descubrió* [110] que una segunda empresa de espionaje israelí (QuaDream) utilizó exploits similares. Además, el *Project Zero de Google* [111] publicó su propio análisis en profundidad del exploit ForcedEntry que puede comprometer remotamente un dispositivo iOS con el fin de instalar el spyware Pegasus. Para un usuario típico, Pegasus es imposible de detectar; sin embargo, Apple corrigió los problemas subyacentes en septiembre de 2021. Esto significa que los dispositivos con el parche instalado deberían ser seguros, aunque el descubrimiento de otras vulnerabilidades *deja en claro* [112] que la actualización debe hacerse en forma periódica, con la esperanza de no ser el objetivo de otro exploit 0-day en el ínterin.



Billetera troyanizada instalada con éxito en un iPhone

COMENTARIO DE EXPERTOS

La disminución de las amenazas para macOS debería ser una señal positiva para los usuarios. Sin embargo, como no solo lo demuestra nuestra propia investigación, las empresas y organizaciones deberían estar atentas al malware dirigido a macOS, proteger sus sistemas de manera acorde e intentar concientizar a los empleados sobre las amenazas basadas en otros sistemas operativos aparte de Windows. Las empresas sencillamente no tienen redes homogéneas y tan solo hace falta un dispositivo para poder comprometerlo, independientemente de su sistema operativo.

Marc-Etienne M.Léveillé, ESET Senior Malware Researcher

SEGURIDAD DE LA IOT

Las botnets basadas en Mirai siguen causando estragos. La guerra de Rusia en Ucrania afecta a la IoT.

Cuando en 2016 la soga alrededor del cuello de los autores de Mirai se tensaba, antes de que la policía los detuviera, publicaron el código fuente online. Seis años después, los investigadores siguen rastreando muchas botnets de la IoT que utilizan el código original o se basan en él. Gafgyt, BotenaGo o Enemybot son solo algunos de los nombres que pertenecen a esta categoría en la telemetría de ESET.

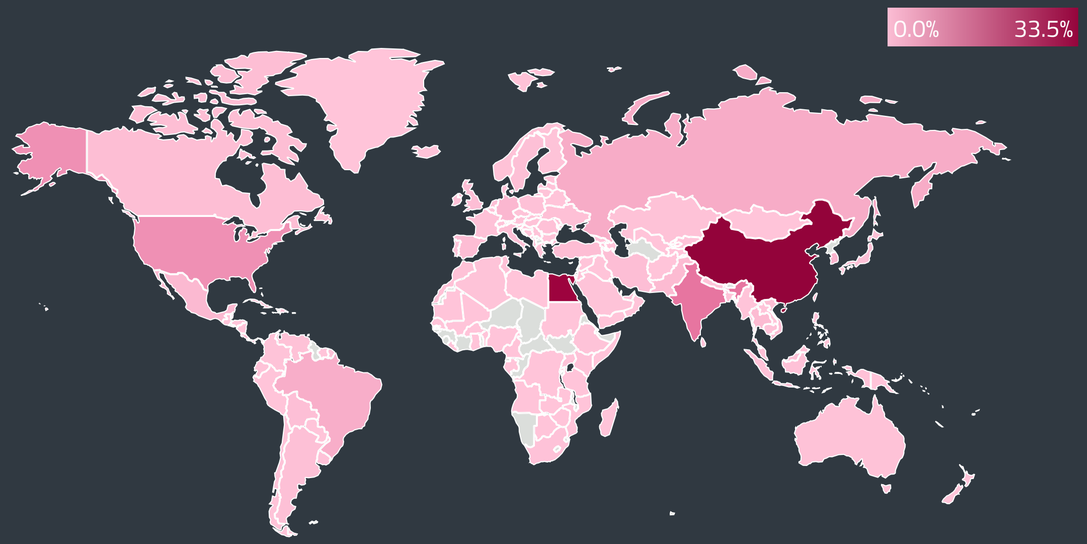
Si dejamos de lado a Mozi y ZHtrap, que se monitorean aparte, las botnets basadas en Mirai fueron responsables de cerca de 7,3 millones de ataques en el primer cuatrimestre de 2022. De todas ellas, el 26% iban dirigidas a Estados Unidos, el 7% al Reino Unido y el 6% a Alemania. Si nos centramos en las IP únicas que sufren estos ataques, la mayoría se encuentran en Alemania (14%) y Estados Unidos (12%). Japón, México y el Reino Unido representan cada uno un 5%.

¿Cuál es el origen de estos ataques? Los tres primeros países con más direcciones IP de atacantes fueron China (33%), Egipto (30%) e India (7%). En cuanto a la mayor cantidad de tráfico malicioso producido, China lidera el grupo (22%), seguida de Egipto (16%), Corea del Sur (14%) y Estados Unidos (14%). Resulta interesante que la mayoría de los más de 800 servidores de payloads (es decir, los servidores que entregan el payload final con sus direcciones IP incrustadas en las inyecciones de comandos de los exploits) estaban ubicados cerca de sus víctimas, concretamente en los Estados Unidos (37%), los Países Bajos (10%) y Alemania (9%).

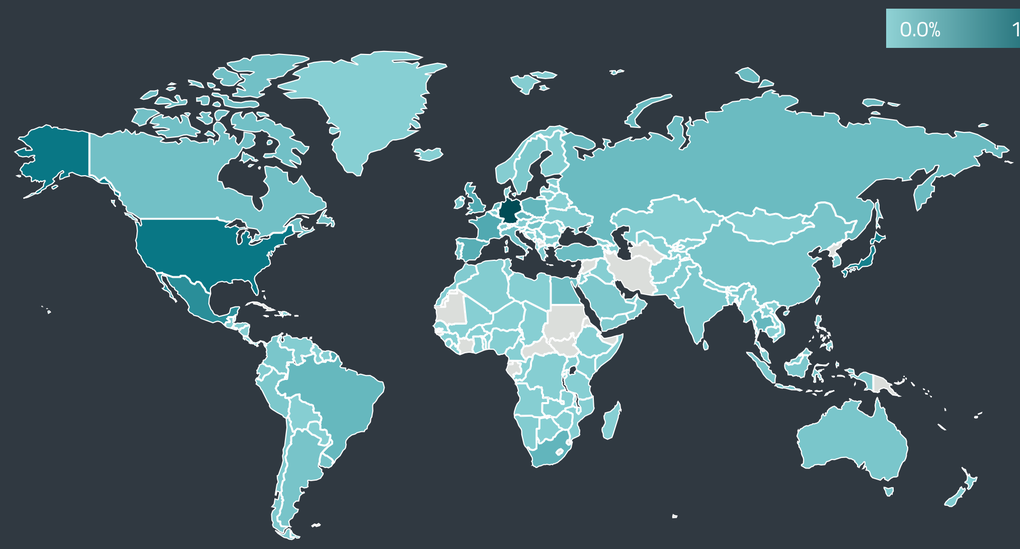
En cuanto al mecanismo de propagación de las botnets basadas en Mirai, la vulnerabilidad *ED 41471* [113] (una ejecución de comandos shell en MVPower DVR) fue la más extendida, representando el 84% de todos los intentos de ataque. Una *búsqueda en Shodan* [114] muestra casi 67.000 dispositivos de este tipo, aunque más de un tercio de ellos están etiquetados como honeypots. La segunda vulnerabilidad más aprovechada fue una inyección de comandos de 2017 en los routers ZyXEL P660HN (*CVE-2017-18368* [115]), que supuso el 8% de los intentos de ataque detectados por ESET.

Otra botnet basada en Mirai y rastreada por ESET es ZHtrap. Para ampliar el alcance, sus bots se centraron exclusivamente en la vulnerabilidad *CVE-2015-2051* [116], un fallo de ejecución remota de código en los routers D-Link DIR-645. La telemetría de ESET informó sobre 106.000 ataques en el primer cuatrimestre de 2022, un aumento del 9% de la actividad en comparación con el tercer cuatrimestre de 2021.

En el primer cuatrimestre de 2022, los servidores de payloads de ZHtrap se observaron con mayor frecuencia en los Países Bajos (41%), que es también donde se originó el mayor número (29%) de los 106.000 ataques detectados. La segunda fuente más frecuente de tráfico malicioso fue EE.UU., con un 28%, seguido de Rumania, con un 12%, Alemania, con un 11%, y Polonia, con un 9%.



Distribución global de las direcciones IP de bots basados en Mirai en el primer cuatrimestre de 2022



Distribución global de las direcciones IP objetivo de la botnet Mozi en el primer cuatrimestre de 2022

COMENTARIO DE EXPERTOS

Aunque Mirai comenzó como una botnet dirigida a la infraestructura de Minecraft, rápidamente se convirtió en una poderosa botnet de alcance mundial. La publicación de su código fuente la convirtió en la base de la mayoría de las nuevas botnets de la IoT y dio lugar a muchos mods, mejoras y funcionalidades adicionales que no estaban presentes en la versión original.

Las botnets basadas en Mirai también demuestran por qué la gente necesita instalar parches en sus dispositivos y sistemas inteligentes de acceso público. Los dispositivos que han llegado al final de su vida útil y los que todavía presentan vulnerabilidades que necesitan ser parcheadas son los principales objetivos que permiten la propagación continua de esta amenaza.

El uso de contraseñas fuertes y configuraciones adecuadas también son clave para prevenir los ataques del tipo Mirai, ya que las propias botnets suelen forzar su entrada en los servicios de línea de comandos débilmente protegidos y expuestos, como Telnet y SSH.

Milan Fránik, ESET Malware Researcher

Aunque EE.UU. (13%), Alemania (11%) y el Reino Unido (6%) lideraron la lista de direcciones IP únicas de los objetivos de ZHtrap, las mayores oleadas de ataques aterrizaron en Taiwán (16%).

La mayor botnet de la IoT rastreada por ESET es Mozi. Sus operadores fueron supuestamente ***arrestados*** [117] por las autoridades chinas en 2021, pero la botnet parece sobrevivir y propagarse por sí misma, como lo haría cualquier zombi devorador de cerebros en un mundo lleno de humanos vulnerables.

En el primer cuatrimestre de 2022, ESET detectó cerca de 500.000 direcciones IP únicas comprometidas por Mozi, un 11% menos que en el tercer cuatrimestre de 2021. La geolocalización de las IP de los atacantes era predominantemente china (59%) e india (30%). En cuanto a las IP objetivo, los alemanes fueron los más afectados con un 17%, seguidos por las víctimas de Estados Unidos (8%) y Japón (7%).

Si se tiene en cuenta la cantidad de ataques, la botnet Mozi fue detectada 5,6 millones de veces, un crecimiento del 6% en comparación con el tercer cuatrimestre de 2021. Estados Unidos tuvo que repeler cerca de un tercio de los ataques (30%).

La distribución de Mozi se basó en los mismos vectores de intrusión que en el tercer cuatrimestre de 2021, es decir, el aprovechamiento de las vulnerabilidades en los dispositivos Netgear DGN (EDB-25978), los routers DASAN (CVE-2018-10562), los routers D-Link (CVE-2015-2051) y los servidores web Jaws (EDB-41471). Los datos de ESET muestran un aumento de la actividad de Mozi, detectando sus ataques en 5,5 millones de ocasiones en el primer cuatrimestre de 2022, un crecimiento del 6% frente al tercer cuatrimestre de 2021.

En el primer cuatrimestre de 2022, el número de exploraciones de routers solicitadas por los clientes, así como la cantidad de comprobaciones de seguridad de routers únicos, se mantuvieron casi idénticos a los del tercer cuatrimestre de 2021, oscilando en torno a 270.000 y 164.000, respectivamente.

Estas exploraciones también confirmaron una tendencia positiva observada en el segundo y tercer cuatrimestre de 2021, a saber, que el uso de contraseñas débiles o predeterminadas para los routers está disminuyendo lentamente. Según las últimas comprobaciones de seguridad, su proporción descendió un 7,5% con respecto al tercer cuatrimestre de 2021. Otro dato igualmente positivo es que el índice de routers vulnerables a uno de los fallos monitoreados por ESET también ha disminuido, en este caso un 15% entre el tercer cuatrimestre de 2021 y el primero de 2022.

En abril, surgieron informes sobre una nueva botnet de Enemybot dirigida por el grupo Keksec. Los investigadores de Fortinet la ***describieron*** [118] como una posible actualización y cambio de nombre de Gafgyt, con características adicionales de Mirai. Sus operadores parecen tener dos objetivos principales: DDoS y cryptomining. A diferencia de otras botnets mencionadas en esta categoría, Enemybot parece utilizar un conjunto más amplio de vulnerabilidades (incluyendo algunas muy recientes) para "reclutar" bots entre los routers Seowon Intech, D-Link e iRZ.

Por la misma época, el laboratorio de investigación de seguridad de redes de Qihoo 360 observó otra nueva botnet de DDoS llamada ***Fodcha*** [119]. Según sus hallazgos, los principales objetivos utilizados para su propagación son varios routers, DVR y servidores, y el número de bots activos diarios supera los 50.000.

Cuando se menciona la seguridad de la IoT, la mayoría de la gente piensa en los routers con contraseñas débiles o en cámaras IP que se pueden secuestrar. Pero los dispositivos "inteligentes" más caros también están en juego. El investigador de seguridad David Colombo ***descubrió*** [120] que, si aprovechaba un fallo en una aplicación de terceros, podía tomar el control de múltiples funciones de los coches Tesla, incluyendo su seguimiento, la apertura de puertas y ventanas, y el arranque del motor.

Como demuestran las múltiples historias relacionadas con la invasión de Ucrania, la seguridad de la IoT puede ser clave en futuros conflictos. Entre ellos podemos mencionar el hackeo y sabotaje de la ***red KA-SAT de Viasat*** [9]; una nueva variante de la botnet Cyclops Blink (que sustituye a VPNFilter) dirigida a los dispositivos de firewall de red de los routers ***WatchGuard*** [121] y ***ASUS*** [122], que posteriormente fue ***desmantelada*** [123] por las autoridades estadounidenses; y (aunque la relación no es tan directa) las vulnerabilidades de los routers ***MikroTik*** [124] aprovechadas por las campañas de Glupteba y Trickbot. Para saber más sobre los atentados relacionados con la guerra de Ucrania, consulte nuestra ***Historia destacada***.

EXPLOITS

Los ataques al RDP descendieron por primera vez desde principios de 2020; le siguieron los dirigidos a SQL y al SMB.

Desde principios de 2020, los ataques de adivinación de contraseñas dirigidos a servicios del protocolo RDP expuestos no habían dejado de crecer. Después de más de dos años, esto varió por primera vez, y los intentos de adivinación por fuerza bruta disminuyeron un 41% entre el tercer cuatrimestre de 2021 y el primero de 2022.

El cambio se produjo el 10 de enero, cuando los ataques al RDP alcanzaron un máximo histórico. Desde entonces, los intentos detectados empezaron a caer bruscamente. El 15 de enero alcanzaron el primer mínimo y luego se recuperaron parcialmente para volver a descender a principios de febrero. El 20 de febrero (poco antes de la invasión rusa de Ucrania), la adivinación de contraseñas volvió a caer y osciló en ese nivel hasta fines del primer cuatrimestre de 2022.

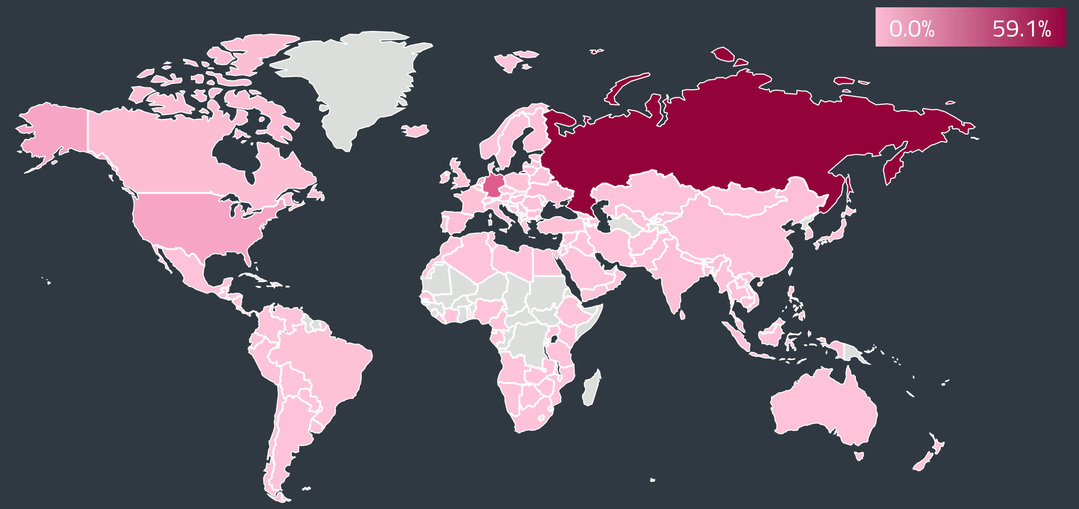
La cantidad de clientes únicos que reportaron ataques al RDP ha seguido una trayectoria similar, disminuyendo más notablemente a fin de año y, en general, con una caída de 40% entre el tercer cuatrimestre de 2021 y el primero de 2022. En consecuencia, el valor promedio de clientes únicos también disminuyó de 160.000 en el tercer cuatrimestre de 2021 a 97.000 en el primero de 2022.

De los 121 mil millones de intentos de ataque al RDP observados en el primer cuatrimestre de 2022, el país más afectado fue Francia (16%), seguido de España (14%), Alemania (8%), Estados Unidos (6%) e Italia (5%). Casi el 60% de los ataques recibidos procedían de Rusia, seguida de lejos por Alemania, con un 16%, y Estados Unidos, con un 5%.

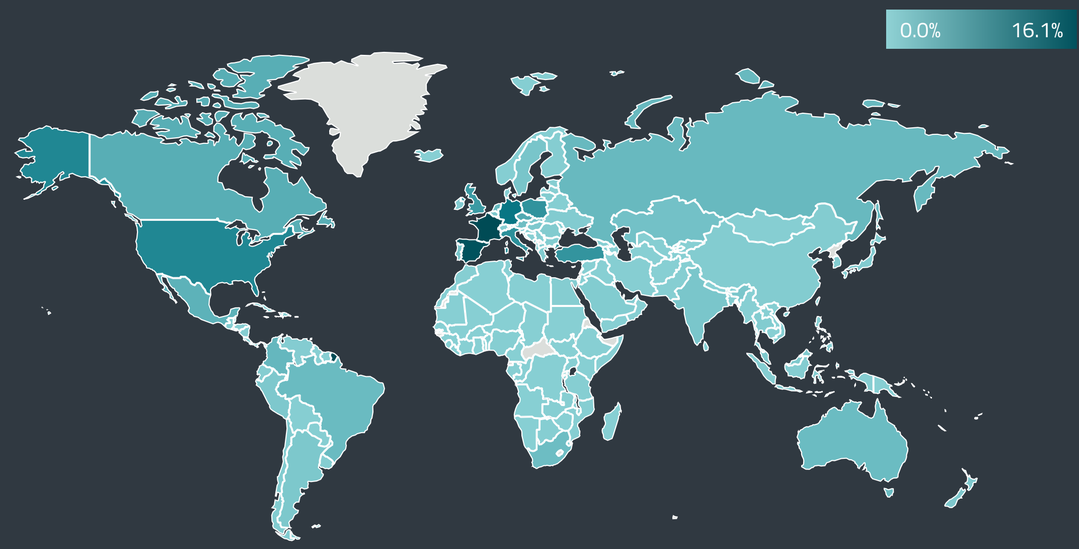
Cabe destacar que la telemetría de ESET muestra un patrón de caída en picada casi idéntico para las adivinaciones de contraseñas contra los servicios SQL expuestos. Como ocurrió con el RDP, las estadísticas de ataques a SQL alcanzaron un máximo histórico el 10 de enero, seguido de un descenso extremo en los días posteriores. A diferencia del RDP, los números de ataques a SQL aún no se han recuperado. Con 860 millones de ataques contra SQL, el primer cuatrimestre de 2022 experimentó un descenso del 64% en comparación con el tercer cuatrimestre de 2021. La cantidad de clientes únicos que informaron sobre conexiones SQL maliciosas disminuyó en el mismo período un 12%.

En el caso de los servicios expuestos del protocolo SMB, el descenso comenzó el 9 de enero y fue más lento y gradual que con RDP y SQL. Al comparar el tercer cuatrimestre de 2021 con el primero de 2022, los ataques dirigidos al SMB disminuyeron un 26%, y el número de clientes únicos se redujo un 6%.

Como se informó a finales de 2021, los atacantes también comenzaron a utilizar una nueva vía de intrusión: la ***vulnerabilidad crítica Log4J*** [125]. Según informes públicos, el inicio de 2022 no hizo más que ampliar el abanico de grupos que lo adoptaron en sus kits de herramientas, incluyendo el ransomware ***Prophet Spider*** [126] y ***NightSky*** [78] entre los delincuentes, y Magic Hound (también conocido como APT35, Charming Kitten, Phosphorus,



Distribución global de las fuentes de los intentos de ataque de adivinación de contraseñas contra el RDP en el primer cuatrimestre de 2022



Distribución global de los objetivos de los intentos de ataque de adivinación de contraseñas contra el RDP en el primer cuatrimestre de 2022

COMENTARIO DE EXPERTOS

Puede haber muchas razones tras el descenso de los ataques al RDP. En primer lugar, la pandemia de COVID-19 parece estar llegando a su fin y la gente está volviendo a las oficinas. Al haber menos trabajo a distancia, podría haber menos objetivos interesantes de alto perfil. Otro factor que podría haber contribuido a esta evolución positiva es la mayor concientización de los departamentos de TI y la mejora gradual de la seguridad de los entornos corporativos, donde se eliminaron muchos de los servicios y sistemas expuestos.

La guerra de Rusia contra Ucrania probablemente también haya desempeñado su papel. Si bien el descenso de los ataques al RDP y a SQL comenzó más de un mes antes de la invasión, los trastornos físicos y cibernéticos y las sanciones impuestas después del 24 de febrero probablemente influyeron en el acceso y la disponibilidad de la infraestructura que participó en los ataques por fuerza bruta.

Ladislav Janko, ESET Senior Malware Researcher

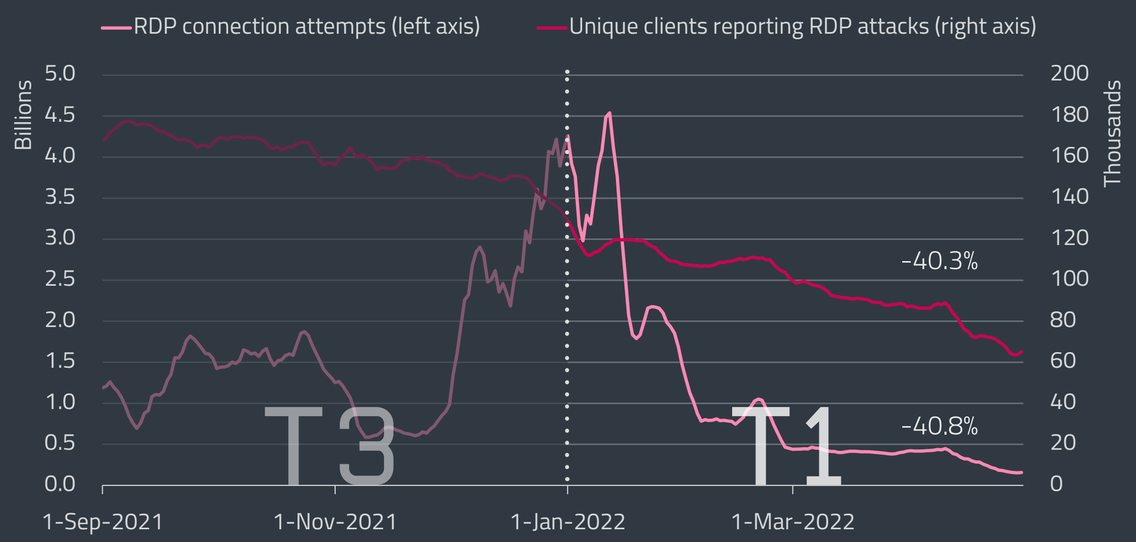
TA453), *Hafnium* [127], *Deep Panda* [128] y *TunnelVision* [129] entre los grupos de espionaje cibernético.

Según la telemetría de ESET, el número de intentos de aprovechamiento de Log4J se disparó tras la publicación de la vulnerabilidad el 10 de diciembre. Entre el 1 y el 5 de enero, las cifras bajaron de cientos de miles por día a decenas de miles por día, pero al parecer se trató de un paréntesis navideño de corta duración. Después del 6 de enero, la actividad de los atacantes (y probablemente también de las pruebas de penetración) volvió a saltar a los niveles de 2021.

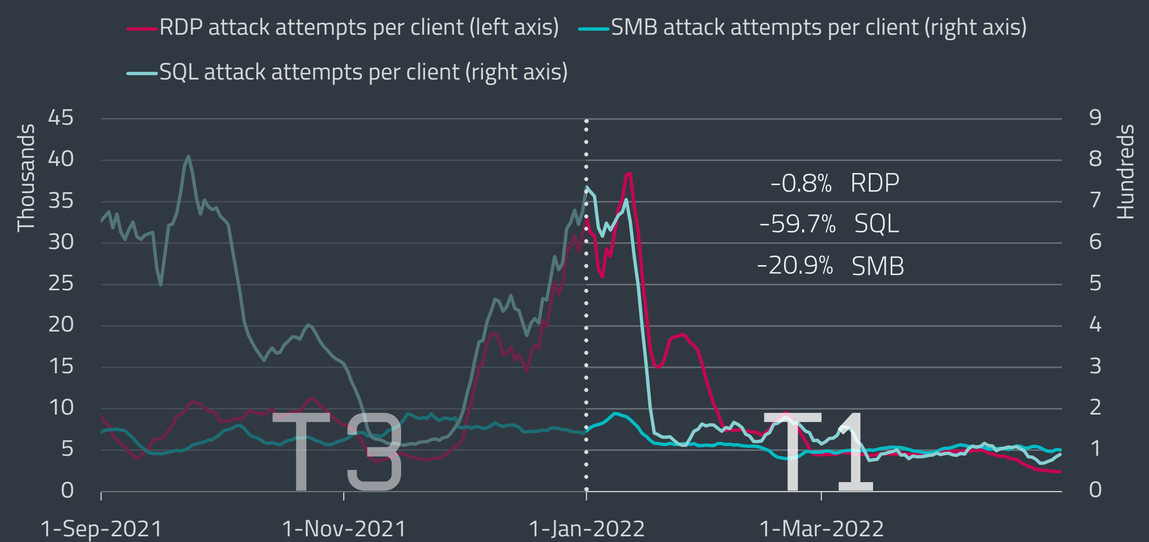
A pesar de la disminución gradual que se observa en nuestro gráfico, Log4J no va a desaparecer pronto, ya que todavía hay muchas aplicaciones vulnerables activas. Así lo confirma el *informe* [130] de Rezilion, que identificó "más de 90.000 aplicaciones potencialmente vulnerables accesibles desde Internet" y reconoce que probablemente solo sean la punta del iceberg.

En abril de 2022 apareció otra vulnerabilidad crítica, con una puntuación CVSS de 9,8. Esta vulnerabilidad, llamada Spring4Shell (*CVE-2022-22965* [131]), está presente en el popular marco de trabajo de código abierto VMWare Spring Core Java y les permite a los atacantes aprovechar la falla para ejecutar código en forma remota (RCE) en todas las aplicaciones que utilicen la versión del código sin parches.

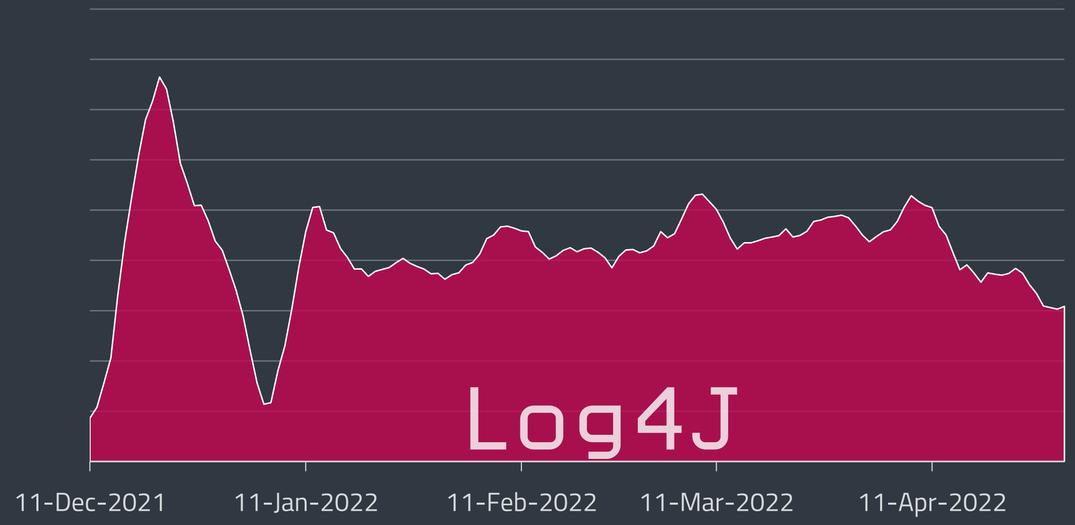
Al igual que Log4J, la vulnerabilidad Spring4Shell se puede aprovechar enviando una consulta maliciosa al servidor vulnerable, lo que les permite a los atacantes acceder a una amplia gama de datos, credenciales y recursos de las víctimas. A pesar de que esto la convierte en una vulnerabilidad bastante grave, la buena noticia es que es más fácil de identificar y luego de solucionar que Log4J.



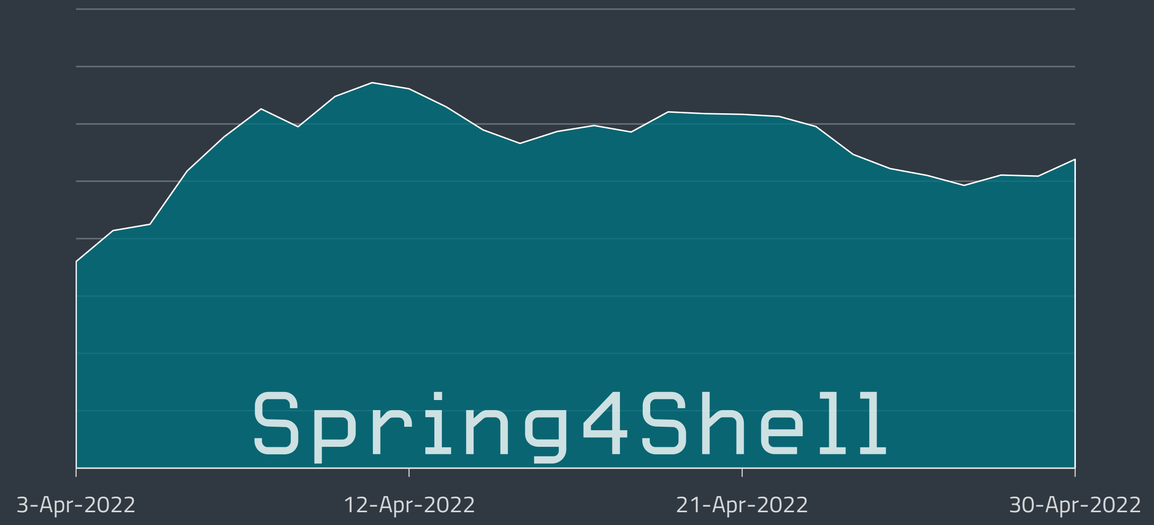
Tendencias de intentos de conexión por RDP y cantidad de clientes únicos en el tercer cuatrimestre de 2021 y primero de 2022, promedio móvil de siete días



Tendencias de intentos de ataque mediante RDP, SMB y SQL por cliente en el tercer cuatrimestre de 2021 y primero de 2022, promedio móvil de siete días



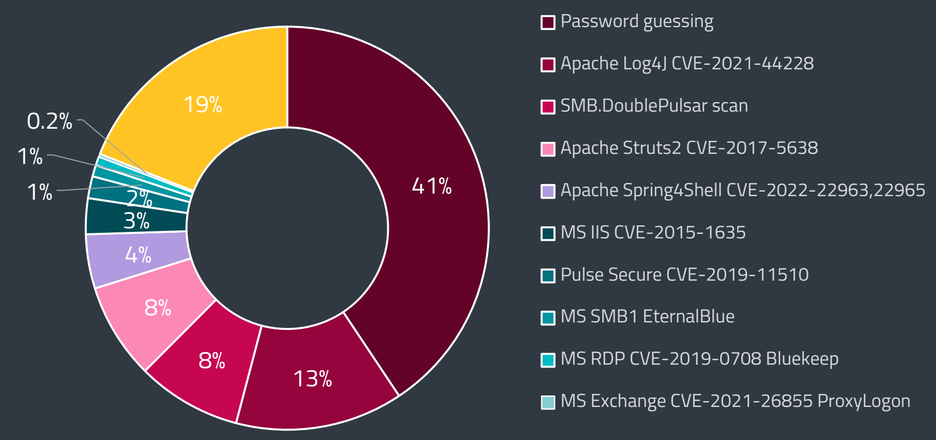
Tendencia de intentos de aprovechamiento de Log4J, promedio móvil de siete días



Tendencia de intentos de aprovechamiento de Spring4Shell en abril de 2022, promedio móvil de siete días

Un mes tras su publicación, la telemetría de ESET vio cientos de miles de intentos de aprovechamiento de Spring4Shell. Como en el caso de Log4J, observamos el mayor pico de actividad poco después de la publicación de la vulnerabilidad.

Entre los 10 vectores de intrusión principales en redes externas, la adivinación de contraseñas sigue siendo el más extendido. No obstante, con un 13%, Log4J llegó a un sólido segundo lugar en el primer cuatrimestre de 2022, robando la mayor parte de la gloria a ***ProxyLogon*** [132], una cadena de vulnerabilidades RCE en los servidores MS Exchange. Nuestros datos sugieren que ProxyLogon se ha vuelto obsoleto para los actores ofensivos, ya que los intentos de aprovechamiento dirigidos a estas fallas cayeron del 14% en el tercer cuatrimestre de 2021 a menos del 1% en el primero de 2022.



Vectores de intrusión en redes externas notificados por clientes únicos en el primer cuatrimestre de 2022

Spring4Shell parece repetir la trayectoria de Log4J en la lista de los 10 vectores principales y, a pesar de que solo se conoce desde hace un par de semanas, ocupó el quinto lugar, con el 4% de los intentos de ataque detectados.

Una nueva vulnerabilidad de Linux con una puntuación de 7,8 en la escala CVSS causó sensación en marzo. "Dirty Pipe" (***CVE-2022-0847*** [133]), que afecta la versión 5.8 del kernel de Linux y posteriores, fue revelada por el investigador de seguridad Max Kellermann. Según su ***informe público*** [134], la falla hace posible "la sobrescritura [de] datos en archivos arbitrarios de solo lectura". Esto permite a los atacantes inyectar su código en los procesos raíz y escalar sus privilegios en la máquina de la víctima.

En el primer cuatrimestre de 2022, Google Project Zero y Mandiant publicaron resúmenes de sus hallazgos de vulnerabilidades 0-day del año anterior. El ***equipo de Google*** [135] declaró haber encontrado 58 vulnerabilidades previamente desconocidas; un aumento del doble en comparación con las 25 descubiertas en 2020. Los investigadores señalan que las razones del crecimiento posiblemente sean el aumento de la capacidad de detección y divulgación. Google también destacó que solo dos de los 58 exploits 0-day se destacaron como novedosos, ambos relacionados con un exploit de iMessage de cero clics (sin interacción por parte del usuario) llamado FORCEDENTRY.

Las ***conclusiones*** [136] de Mandiant son similares, aunque su lista incluye más exploits 0-day. En 2021, sus investigadores identificaron 80 nuevas vulnerabilidades, duplicando con creces el récord anterior de 32 de 2019. Mandiant también señala que el número de actores con motivación financiera que despliegan exploits 0-day está aumentando, sobre todo debido a las bandas de ransomware que los utilizan para el acceso inicial a los entornos de las víctimas de alto perfil.

CONTRIBUCIONES DE INVESTIGACIÓN DE ESET

Últimas colaboraciones y logros de los expertos de investigación de ESET

PRÓXIMAS PRESENTACIONES

Conferencia RSA 2022

ESPecter: mostrando el futuro de las amenazas para UEFI [137]

En los últimos años, ha quedado claro que las amenazas para UEFI son reales y se han desplegado en el mundo real. Los implantes en la interfaz UEFI (como LoJax y MosaicRegressor) han utilizado el nivel más bajo de persistencia: la flash SPI. Los actores detrás del bootkit ESPecter piensan que comprometer el cargador de arranque es el mejor camino. En esta sesión, Jean-Ian Boutin, ESET Director of Threat Research, y Martin Smolár, ESET Malware Researcher, describirán el hallazgo por parte de ESET del mencionado ESPecter, un bootkit para UEFI del mundo real no documentado anteriormente que persiste en la partición del sistema EFI (ESP). El objetivo de esta sesión es concientizar sobre las amenazas para la UEFI que afectan al ESP, así como proporcionar orientación y recursos a los defensores para ayudar a proteger su entorno anterior al sistema operativo. El análisis de Boutin y Smolár de este bootkit para UEFI que persiste en la partición ESP, desconocido hasta el momento, ayudará a los asistentes a comprender en detalle las técnicas utilizadas por estas amenazas. Si bien las amenazas para UEFI son muy raras, el descubrimiento de ESPecter por parte de ESET demuestra que ciertamente no son simples "espectros".

Black Hat USA 2022

Industroyer2: la guerra cibernética de Sandworm vuelve a tener como objetivo la red eléctrica ucraniana [138]

En esta charla, Anton Cherepanov, ESET Senior Malware Researcher, y Robert Lipovský, ESET Principal Researcher, ofrecerán detalles técnicos de Industroyer2, una nueva versión del único malware que logró provocar apagones eléctricos. Su última variante se observó en Ucrania en medio de la invasión rusa en curso, con el objetivo de causar un gran corte eléctrico en una región con más de dos millones de habitantes, utilizando componentes que amplifican el impacto. En la presentación, los investigadores mostrarán datos que relacionan este ataque con el conocido grupo de APT Sandworm, y discutirán por qué y cómo el ataque resultó ser en mayor parte infructuoso. Además, se proporcionarán consejos prácticos para los defensores, incluyendo entradas de registro de comprobación, reglas EDR a tener en cuenta, opciones de configuración para dificultar la infección con Sandworm y su movimiento lateral, así como reglas Snort y YARA para la detección y la cacería de la amenaza.

Virus Bulletin 2022

Lazarus y BYOVD: amenaza al núcleo de Windows [139]

En esta sesión, Peter Kálnai, ESET Senior Malware Researcher, y Matěj Havránek, ESET Malware Analyst, realizarán una profunda inmersión técnica en un componente malicioso que fue utilizado en un ataque del grupo de APT Lazarus a finales de 2021. No documentado hasta el momento, este malware es un sofisticado módulo de modo de usuario que utiliza la técnica "Traiga su propio controlador vulnerable" (BYOVD) y aprovecha una vulnerabilidad en un controlador de Dell legítimo y firmado. Tras obtener acceso de escritura a la memoria del kernel, el objetivo global del módulo es cegar las soluciones de seguridad y las herramientas de monitoreo. Esto se consigue tácticamente a través de varios mecanismos distintos dirigidos a importantes funciones, estructuras y variables del kernel de los sistemas Windows desde la versión 7.1 hasta Windows Server 2022. Kálnai y Havránek aclararán cómo funcionan estos mecanismos y qué cambios introducen en la supervisión del sistema una vez que se ejecuta el módulo en modo usuario. Nuestros investigadores también compararán este caso de Lazarus con otros grupos de APT que se aprovechan de la técnica BYOVD, ya que posee un complejo conjunto de métodos nunca antes vistos para desactivar las interfaces de monitoreo.

REcon 2022

Funcionamiento de la máquina virtual multicapa de Wslink [140]

Wslink es un loader único, vinculado al grupo Lazarus, que los investigadores de ESET descubrieron y documentaron a finales del año pasado. La mayoría de las muestras de Wslink están empaquetadas y protegidas con un ofuscador avanzado basado en una máquina virtual (VM); las muestras no contienen artefactos claros, como nombres de sección específicos, que las relacionen fácilmente con un ofuscador ya conocido y descrito públicamente. Esta VM introduce además otras técnicas de ofuscación como la inserción de código basura, la codificación de operandos virtuales, la duplicación de códigos de operación virtuales, predicados opacos, la fusión de instrucciones virtuales y una VM anidada. En su presentación, Vladislav Hrčka, ESET Malware Researcher, analiza la estructura de la máquina virtual y describe el enfoque semiautomatizado del Equipo de Investigación de ESET para lograr ver a través de las técnicas de ofuscación en un tiempo razonable. El enfoque se demuestra en algunos fragmentos de código de bytes de una muestra protegida y los resultados se comparan con una muestra no ofuscada descubierta posteriormente para confirmar la validez del método.

PRESENTACIONES REALIZADAS

S4x22

Dentro de Industroyer2 y los últimos ciberataques de Sandworm contra Ucrania [141]

Robert Lipovsky, ESET Principal Malware Researcher, presentó el trabajo del equipo que descubrió Industroyer2, una nueva variante del malware Industroyer desplegada por el infame grupo Sandworm, que intentó atacar a una empresa energética ucraniana tras el estallido de la guerra en el país. Lipovsky contó cómo la colaboración con CERT-UA mitigó el ataque y lo comparó con el malware original Industroyer que apagó las luces en 2016. La presentación también analizó otros ciberataques recientes de Sandworm contra infraestructuras críticas ucranianas.

CARO Workshop 2022

Petróleo, agua y algo fresco: cazando a los actores de amenazas en Oriente Medio [142]

En esta presentación, Robert Lipovsky, ESET Principal Malware Researcher, habló sobre la cacería de los actores de amenazas de Oriente Medio: OilRig, MuddyWater y un nuevo grupo que el Equipo de Investigación de ESET llama FreshFeline. Basándose en la investigación de Adam Burgher, ESET Senior Threat Intelligence Analyst, Lipovsky expuso la metodología de caza de los investigadores de ESET y cómo los condujo a un backdoor de OilRig recientemente descubierto, a varias campañas nuevas de MuddyWater, y a la cadena de aprovechamiento de vulnerabilidades y los backdoors utilizados por el grupo FreshFeline.

El detrás de escena de la caza de InvisiMole [140]

Desde que ESET descubrió este grupo en 2018, nuestros investigadores han estado siguiendo de cerca sus actividades de ciberespionaje altamente dirigidas. En esta sesión, Anton Cherepanov, ESET Senior Malware Researcher, y Zuzana Hromcová, ESET Malware Researcher, compartieron información no disponible públicamente sobre la caza de InvisiMole. También hablaron de dos campañas de 2021 hasta ahora no divulgadas dirigidas a Ucrania y de cómo el momento se alinea con otros acontecimientos geopolíticos en la región.

CARO Workshop 2022 - Botconf 2022

TA410: el primo lejano de APT10 (CARO Workshop 2022) [140]

TA410: el primo lejano de APT10 (Botconf 2022) [143]

TA410 es un grupo de ciberespionaje descrito por primera vez en agosto de 2019 y que muestra interesantes capacidades técnicas con su uso de complejos implantes. La actividad de TA410 comparte algunas características con las operaciones anteriores de APT10. Por ello, algunos informes públicos han atribuido erróneamente las actividades de TA410 a APT10. En esta presentación, Alexandre Côté Cyr, ESET Malware Researcher, y Matthieu Faou, ESET Senior Malware Researcher, aclararon qué es TA410 y en qué se diferencian sus actividades de las actuales del grupo APT10. Valiéndose de la telemetría de ESET, presentaron la visión del Equipo de Investigación de ESET sobre los principales objetivos de TA410.

Botconf 2022 - NorthSec

Saltando la barrera de aire: 15 años de esfuerzos de los estados-nación (Botconf 2022) [144]

Saltando la barrera de aire: 15 años de esfuerzos de los estados-nación (NorthSec) [145]

Las barreras de aire (air-gapping) se utilizan para proteger las redes más sensibles. Solo en la primera mitad de 2020, surgieron cuatro marcos maliciosos previamente desconocidos diseñados para vulnerar las redes con barreras de aire, lo que eleva el total, según el recuento de ESET, a 17. El departamento de investigación de ESET decidió revisar cada uno de los marcos conocidos hasta la fecha y ponerlos en perspectiva, uno al lado del otro. En esta presentación, Alexis Dorais-Joncas, que lidera el Equipo de Investigación de Malware en Canadá, y Facundo Munõz, ESET Security Intelligence Analyst, describieron cómo operan los marcos de malware que tienen como objetivo las redes con barrera de aire, y compararon en detalle sus tácticas, técnicas y procedimientos (TTP) más importantes.

Botconf 2022

ProxyChaos: un año de análisis del aprovechamiento de vulnerabilidades en Microsoft Exchange [146]

Desde principios de 2021, Exchange ha sido objeto de varias vulnerabilidades críticas, incluyendo las cadenas de vulnerabilidades ProxyLogon y ProxyShell, y sus variantes. Los investigadores de ESET han seguido de cerca las actividades maliciosas relacionadas con estas vulnerabilidades desde que se hicieron públicas y descubrieron múltiples grupos de APT que las aprovechaban. En esta presentación, Mathieu Tartare, ESET Malware Researcher, repasó toda la cronología de acontecimientos y mostró cómo los atacantes aprovecharon sistemáticamente las vulnerabilidades y con qué propósito. Asimismo, brindó información general sobre los diversos grupos que se aprovecharon de cada una de las vulnerabilidades, incluyendo algunas actividades aún no divulgadas. Tartare también proporcionó a los asistentes una línea de tiempo detallada de los eventos y estadísticas de la telemetría de ESET, para mostrar el amplio alcance de estos ataques.

SeQCure

Divulgación de vulnerabilidades: un desafío incluso en 2022 [147]

Encontrar vulnerabilidades no está intrínsecamente asociado a ser un investigador de malware. Aún así, los investigadores de ESET descubren regularmente diferentes tipos de vulnerabilidades en el curso de su trabajo y participan activamente en el proceso de divulgación coordinado. En esta presentación, Alexis Dorais-Joncas, que dirige el Equipo de Inteligencia de Seguridad de ESET, y Mathieu Tartare, ESET Malware Researcher, explicaron cómo la investigación de malware puede conducir al descubrimiento de vulnerabilidades. A lo largo de la presentación de estudios de casos reales, nuestros investigadores detallaron los diferentes tipos de vulnerabilidades que se descubren con más frecuencia, cómo funciona el proceso de divulgación y las lecciones aprendidas.

ESET World

Los contratistas aeroespaciales y de defensa de todo el mundo, atacados por Lazarus [148]

Los actores de amenazas avanzadas que operan bajo el paraguas de Lazarus han estado atacando implacablemente a contratistas de defensa y empresas del sector aeroespacial de todo el mundo durante años. En esta presentación, Jean-Ian Boutin, ESET Director of Threat Research, explicó los detalles de las últimas campañas del grupo contra este sector crítico. Aunque el señuelo inicial sigue siendo el mismo (una oferta de trabajo falsa a través de redes sociales como LinkedIn), la sofisticación y diversidad de la campaña sigue aumentando.

Día Europeo de la Ciberseguridad organizado por ESET - SEMAFOR

El pasado y el presente de la guerra cibernética en Ucrania (Día Europeo de la Ciberseguridad organizado por ESET) [149]

El pasado y el presente de la guerra cibernética en Ucrania (SEMAFOR) [150]

Con la brutal intensificación de la guerra contra Ucrania, Robert Lipovsky, ESET Principal Malware Researcher, examinó más de cerca su faceta "cibernética". ¿Qué ha pasado en Ucrania? ¿La guerra cibernética podría extenderse a otros países europeos? ¿Los usuarios deberían estar preocupados? Lipovsky explicó a los asistentes de estos dos eventos los ciberataques más importantes relacionados con el conflicto armado, tanto en las últimas semanas como en los últimos ocho años.

Día Europeo de la Ciberseguridad organizado por ESET

¿El aprendizaje automático mejorará o alterará el equilibrio de la ciberseguridad? [151]

Las tecnologías basadas en el aprendizaje automático ayudan cada vez más a combatir el fraude a gran escala, a evaluar y optimizar los procesos corporativos, a mejorar los procedimientos de prueba y a desarrollar nuevas soluciones para los problemas existentes. Juraj Jánoík, líder del Equipo de Detección Automática de Amenazas y Aprendizaje Automático de ESET, habló durante su charla sobre cómo ESET reconoció el potencial del aprendizaje automático desde el principio y lo empleó para mejorar la detección de malware desde hace más de 20 años.

Un acercamiento al panorama de amenazas actual [152]

Ondrej Kubovič, ESET Security Awareness Specialist, compartió las conclusiones sobre las últimas amenazas y tendencias detectadas en la telemetría de ESET durante los últimos meses de 2021. Entre otras cosas, su presentación abarcó los cientos de miles de millones de adivinaciones de contraseñas destinadas a romper la protección del acceso remoto mediante el protocolo RDP; la resurrección de Emotet, una amenaza descrita por Europol como el "malware más peligroso del mundo"; y el incremento de más de 400 veces del malware bancario para Android de un año a otro.

WHITE PAPERS

Funcionamiento de la máquina virtual multicapa de Wslink [36]

Los investigadores de ESET recientemente analizaron Wslink, un loader malicioso único previamente no documentado que se ejecuta como un servidor y cuenta con un ofuscador basado en una máquina virtual. En este white paper, Vladislav Hrčka, ESET Malware Researcher, describe la estructura de la máquina virtual utilizada en las muestras de Wslink y sugiere un posible enfoque para ver a través de las técnicas de ofuscación utilizadas en las muestras analizadas. La máquina virtual introdujo un arsenal diverso de técnicas de ofuscación, que los investigadores de ESET lograron sortear para revelar una parte del código malicioso desofuscado descrito en este documento. El white paper también describe la estructura interna general de las máquinas virtuales y presenta algunos términos y marcos importantes utilizados en nuestro análisis detallado de la máquina virtual de Wslink.

PODCAST DE INVESTIGACIÓN DE ESET

Para ampliar el alcance de las investigaciones de ESET entre los profesionales de seguridad cibernética, administradores, investigadores y la comunidad de seguridad de la información en general, hemos decidido iniciar nuestro propio Podcast de Investigación de ESET. Hay un nuevo episodio cada vez que publicamos un artículo de investigación importante, lo que suele ocurrir cada pocos meses.

El presentador de nuestro podcast es *Aryeh Goretsky* [153], ESET Distinguished Researcher y

pionero de la seguridad informática, que habla con los investigadores, los presenta a ellos y a sus descubrimientos, y les ofrece a los oyentes una mirada detrás del telón sobre cómo surgió cada investigación.

Los últimos episodios se pueden escuchar a través de las plataformas de podcast más populares, como *Spotify* [154], *Google Podcasts* [155], *Apple Podcasts* [156] y *PodBean* [157].

CONTRIBUCIONES A MITRE ATT&CK

Los investigadores de ESET hacen contribuciones regulares a *MITRE ATT&CK®* [158] (Tácticas, Técnicas y Conocimiento Común de Adversarios) [159], una base de conocimiento de tácticas y técnicas maliciosas accesible a nivel mundial. En el primer cuatrimestre de 2022, la contribución de ESET *Process Injection: ListPlanting* [159] se añadió a la base de conocimientos de ATT&CK.

ListPlanting es un método para ejecutar código arbitrario en el espacio de direcciones de un proceso vivo separado. El código ejecutado a través de ListPlanting también puede evadir la detección de los productos de seguridad, ya que su ejecución se enmascara bajo un proceso legítimo. InvisiMole utiliza ListPlanting para inyectar código en un proceso de confianza.

InvisiMole [160] es un programa espía modular que ha sido utilizado por el grupo de APT InvisiMole desde al menos 2013. El grupo InvisiMole también tiene dos módulos backdoor llamados RC2FM y RC2CL, que se utilizan para realizar actividades posteriores a la infección. Se ha descubierto en víctimas comprometidas en Ucrania y Rusia. La infraestructura del grupo *Gamaredon* [161] ha sido utilizada para descargar y ejecutar el programa espía InvisiMole contra un pequeño número de víctimas.

ESET ha llevado a cabo una exhaustiva investigación sobre estos dos grupos de APT. Los investigadores de ESET *revelaron* [26] el modus operandi y el amplio conjunto de herramientas del escurridizo grupo InvisiMole, que tiene como objetivo entidades militares y diplomáticas. Varias de las herramientas utilizadas por Gamaredon también son *bien conocidas* [25] por los investigadores de ESET, que las monitorean y rastrean con frecuencia.

El último listado de ATT&CK *(versión 11)* [162] también incluye las detecciones ahora vinculadas con las fuentes de datos relacionadas: componentes de datos, una versión beta de subtécnicas de ATT&CK para móviles, ATT&CK para sistemas de control industriales (ICS) en *attack.mitre.org* [156], así como actualizaciones y agregados regulares en las categorías Técnicas, Software y Grupos.

EVALUACIONES MITRE ATT&CK

ESET participó en la última ronda de evaluaciones MITRE ATT&CK, que se centró en las tácticas, técnicas y procedimientos aplicados por los grupos de APT de estados-nación Wizard Spider y Sandworm: *Evaluación ATT&CK de Wizard Spider y Sandworm organizada por MITRE Engenuity* [163].

Estas evaluaciones no constituyen un análisis competitivo, como subraya *MITRE Engenuity* [164]. Algunos parámetros clave que no se tienen en cuenta en las evaluaciones son los requisitos de rendimiento y recursos, la estrategia de alerta, el ruido (fatiga de alertas: cualquier producto podría obtener una puntuación muy alta en la mayoría de estos resultados si produjera alertas en cada acción registrada en el entorno de prueba), la integración con el software de seguridad de las endpoints y la facilidad de uso. En el caso de ESET, se evaluó *ESET Inspect* [165], nuestra solución de detección y respuesta ampliada, que les proporciona visibilidad de las amenazas y del sistema a los gestores de riesgos y a los responsables de la respuesta a incidentes.

Los escenarios de detección consistieron en 19 pasos (10 para Wizard Spider y 9 para Sandworm) que abarcan un espectro de tácticas enumeradas en el marco de ATT&CK, desde el acceso inicial hasta el movimiento lateral, la recolección, la extracción, etc. Estos pasos luego se desglosan en un nivel más granular, dando un total de 109 subpasos. ESET Inspect para equipos Linux aún no había sido lanzado en el momento de la evaluación, por lo que los pasos y subpasos relacionados con Linux quedaban fuera de alcance. Esto significa que se evaluaron 15 pasos y 90 subpasos en el caso de ESET.

De los 15 pasos aplicables en la evaluación de detección, ESET Inspect *detectó todos los pasos (100%)* [166]. Al desglosar la emulación del ataque a un nivel más granular, de los 90 subpasos aplicables en la emulación, ESET Inspect detectó 75 subpasos (83%) incluso sin tener los módulos en ESET Inspect con soporte para Linux. Como indican los resultados, ESET Inspect proporciona a los defensores una excelente visibilidad de las acciones del atacante en el sistema comprometido a lo largo de todas las etapas del ataque. Como ya se ha señalado, ESET no participó en la parte de Linux de la evaluación, pero con el lanzamiento público de ESET Inspect con soporte para Linux el 30 de marzo de 2022, la cobertura de la compañía de todas las principales plataformas de endpoints, junto con Windows y macOS, está ahora completa.

Para entender los antecedentes de ESET, la empresa es pionera en la investigación de Sandworm, y ha hecho algunos de los descubrimientos más importantes sobre este grupo de amenazas. La excelente visibilidad que tiene ESET de este grupo queda demostrada por el resultado de nuestras destacadas investigaciones, como el reciente descubrimiento de *Industroyer2* [14]. El descubrimiento del ataque, dirigido a un proveedor de energía en Ucrania, y la cooperación de ESET con el CERT-UA permitieron evitarlo. Otros ejemplos de investigaciones de ESET que analizan las operaciones y herramientas de Sandworm incluyen los *ataques contra la red eléctrica ucraniana* [12], los ciberataques

contra *objetivos de alto valor en el sector financiero ucraniano* [167], los *ataques a la cadena de suministro contra Ucrania* [168], y el devastador *ransomware NotPetya* [169], por nombrar algunos.

Wizard Spider ha llevado a cabo campañas de ransomware utilizando herramientas infames como TrickBot, una botnet que ha infectado más de un millón de computadoras. En 2020 los investigadores de ESET participaron en una operación global para *desarticular esta botnet* [170]; sin embargo, no mucho después, este infostealer volvió a la carga con *nuevos módulos* [171].

OTRAS CONTRIBUCIONES

Los investigadores de ESET descubrieron múltiples vulnerabilidades en varios modelos de portátiles Lenovo para consumidores que le permiten a un atacante con privilegios de administrador exponer al usuario al malware en el nivel del firmware; también identificaron una vulnerabilidad del MSR en el controlador del kernel AMDPowerProfiler.sys.

CVE-2021-26334 [172]

Los investigadores de ESET identificaron una vulnerabilidad del MSR en el controlador del kernel AMDPowerProfiler.sys, que forma parte del software de creación de perfiles *AMD µProf* [173]. Una vez instalado el paquete de software subyacente, el controlador se ejecuta en cada arranque del sistema. El acceso MSR IOCTL no filtrado, combinado con la falta de indicadores FILE_DEVICE_SECURE_OPEN y la presencia en el arranque, da a los atacantes una buena oportunidad de aprovechar el controlador incluso como un usuario sin privilegios (esto es una ventaja en comparación con la técnica BYOVD, donde los atacantes necesitan cargar el controlador ellos mismos).

AMD *reconoció* [174] la existencia de la vulnerabilidad y lanzó una revisión en su publicación de los *Martes de Parches* [172] de noviembre de 2021. Para más información sobre el malware que se aprovecha de las vulnerabilidades en los controladores del kernel, consulte el *artículo del blog* del Equipo de Investigación de ESET titulado "Controladores del kernel firmados: una puerta desprotegida para acceder al núcleo de Windows" [30].

CVE-2021-3971 [37], *CVE-2021-3972* [38]

Estas dos vulnerabilidades afectan a los controladores de firmware de la UEFI originalmente destinados a utilizarse solo durante el proceso de fabricación de las computadoras portátiles de Lenovo para consumidores. Un atacante puede activar los controladores de firmware afectados para deshabilitar directamente las protecciones de la flash SPI (bits de registro de control del BIOS y registros de rango protegido) o la función de arranque seguro de la UEFI desde un proceso privilegiado en modo usuario durante el tiempo de ejecución del sistema operativo. Esto implica que el aprovechamiento de dichas vulnerabilidades les permitiría a los atacantes desplegar y ejecutar con éxito en los dispositivos afectados implantes flash SPI o ESP, como *LoJax* [29] o *ESPecter* [39], el último descubrimiento de malware para UEFI del Equipo de Investigación de ESET.

CVE-2021-3970 [40]

Mientras los investigadores de ESET analizaban los controladores vulnerables mencionados arriba, descubrieron una tercera vulnerabilidad: la corrupción de la memoria SMM dentro de la función del controlador SW SMI. Esta vulnerabilidad permite la lectura y escritura arbitrarias desde o hacia SMRAM, lo que puede conducir a la ejecución de código malicioso con privilegios de SMM y, potencialmente, al despliegue de un implante flash SPI.

Lenovo confirmó las vulnerabilidades el 17 de noviembre de 2021 y publicó un aviso el 18 de abril de 2022. En total, la lista de dispositivos afectados contiene más de cien modelos diferentes de portátiles para consumidores con millones de usuarios en todo el mundo, desde modelos económicos como el Ideapad-3 hasta otros más avanzados como el Legion 5 Pro-16ACH6 H o el Yoga Slim 9-14ITL05. La lista completa de los modelos afectados con soporte de desarrollo activo se publicó en un *comunicado de Lenovo* [41]. Además de los modelos enumerados en el comunicado, varios otros dispositivos que reportamos a Lenovo también están afectados, aunque no serán reparados debido a que están llegando a su Fin de Soporte de Desarrollo (EODS). Hay más información disponible en la *entrada del blog* [42] del Equipo de Investigación de ESET titulado "Cuando lo 'seguro' no es para nada seguro: se descubren vulnerabilidades de alto impacto en la UEFI de portátiles Lenovo".

Serie de consideraciones para los CISO, de Frost & Sullivan: participación en el panel sobre las implicaciones de la guerra en Ucrania [175]

La guerra en Ucrania cambió la geopolítica en Europa y la alianza de la OTAN más rápido de lo que nadie podía haber imaginado. Según la empresa de investigación y consultoría Frost & Sullivan, un aspecto de la guerra del que se habla poco es la dimensión de la seguridad cibernética y la cuestión de si las sanciones y las prohibiciones de venta de tecnología impulsarán nuevas oleadas de ataques de ransomware y espionaje cibernético.

Ejecutivos de ciberseguridad de todo el mundo se reunieron con Frost & Sullivan para discutir las potenciales implicaciones de ciberseguridad de la mayor guerra en Europa desde la Segunda Guerra Mundial. Jean-Ian Boutin, director del Equipo de Investigación de Amenazas de ESET, compartió los conocimientos de la empresa sobre diversas amenazas detectadas por ESET en Ucrania, no solo durante el estallido de la guerra, sino también las que la precedieron. Describió 2022 como el año de WhisperGate, HermeticWiper, IsaacWiper y CaddyWiper desde la perspectiva de los CISO, y esbozó cómo la comunidad de proveedores puede garantizar la mitigación de estos ataques. También habló de los diversos grupos de APT, como Mustang Panda, que aprovechan el conflicto de Ucrania como señuelo para llevar a cabo acciones adversas, y de lo que significa para los CISO y su rol cada vez más importante.

CRÉDITOS

Equipo

Peter Stančík, Team Lead
Klára Kobáková, Managing Editor

Aryeh Goretsky
Branislav Ondrášik
Bruce P. Burrell
Hana Matušková
Nick FitzGerald
Ondrej Kubovič
Zuzana Pardubská

Prólogo

Roman Kováč, Chief Research Officer

Colaboradores

Anton Cherepanov
Dušan Lacika
Igor Kabina
Jakub Souček
Jakub Tomanek
Ján Šugarek
Jean-Ian Boutin
Jiří Kropáč
Juraj Jánošík
Ladislav Janko
Lukáš Štefanko
Marc-Etienne M.Léveillé
Martin Červeň
Matthieu Faou
Michal Malík
Milan Fránik
Miroslav Legéň
Patrik Sučanský
Robert Kapp
Robert Lipovský
Vladimír Šimčák
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.

Los datos se procesaron con la sincera intención de mitigar todas las actitudes tendenciosas conocidas y se hizo un esfuerzo por maximizar el valor de la información proporcionada sobre las amenazas más importantes activas en el mundo real.

Además, los datos excluyen las detecciones de *aplicaciones potencialmente no deseadas* [176], *aplicaciones potencialmente no seguras* [177] y *adware* [178], excepto donde se indique lo contrario en las secciones más detalladas específicas para cada plataforma y en la sección Amenazas para 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.

REFERENCES

[1] https://twitter.com/ESETresearch/status/1496581903205511181

[2] https://www.welivesecurity.com/2022/02/24/hermeticwiper-new-data-wiping-malware-hits-ukraine/

[3] https://twitter.com/ESETresearch/status/1496614321442459655

[4] https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/

[5] https://twitter.com/AvastThreatLabs/status/1496663206634344449

[6] https://www.welivesecurity.com/2022/03/15/caddywiper-new-wiper-malware-discovered-ukraine/

[7] https://www.welivesecurity.com/2017/06/27/new-ransomware-attack-hits-ukraine/

[8] https://cip.gov.ua/en/news/chergova-kiberataka-na-saiti-derzhavnikh-organiv-ta-banki

[9] https://www.viasat.com/about/newsroom/blog/ka-sat-network-cyber-attack-overview/

[10] https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/

[11] https://twitter.com/ESETresearch/status/1483161464106098689

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

[13] https://cert.gov.ua/article/39518

[14] https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/

[15] https://edition.cnn.com/2022/04/12/politics/gru-russia-hackers-ukraine-power-grid/index.html

[16] https://www.eset.com/int/ua-crisis/?utm_source=facebook&utm_medium=cpc&utm_campaign=ukraine-crisis&utm_term=eset-response-center&fbclid=IwAR2pu0PR2VThhA0GpRE0-Km9NmA3oELsHzsrR9l8DzNR_33I_2Sw0urrrD4#eset-helps

[17] https://www.welivesecurity.com/2022/03/23/mustang-panda-hodur-old-tricks-new-korplug-variant/

[18] https://www.welivesecurity.com/2022/02/27/beware-charity-scams-exploiting-war-ukraine/

[19] https://www.welivesecurity.com/2022/03/11/eset-research-webinar-apt-groups-ukraine-cyber-battlefield/

[20] https://www.welivesecurity.com/2014/09/22/back-in-blackenergy-2014/

[21] https://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/

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

[23] https://www.welivesecurity.com/2017/07/04/analysis-of-telebots-cunning-backdoor/

[24] https://www.welivesecurity.com/2018/09/27/lojax-first-uefi-rootkit-found-wild-courtesy-sednit-group/

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

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

[27] https://www.welivesecurity.com/2020/12/02/turla-crutch-keeping-back-door-open/

[28] https://www.welivesecurity.com/2019/07/11/buhtrap-zero-day-espionage-campaigns/

[29] https://www.welivesecurity.com/wp-content/uploads/2018/09/ESET-LoJax.pdf

[30] https://www.welivesecurity.com/2022/01/11/signed-kernel-drivers-unguarded-gateway-windows-core/

[31] https://www.welivesecurity.com/2022/04/06/fake-eshops-prowl-banking-credentials-android-malware/

[32] https://appdefensealliance.dev/

[33] https://www.welivesecurity.com/2022/03/24/crypto-malware-patched-wallets-targeting-android-ios-devices/

[34] https://www.welivesecurity.com/2022/04/13/eset-takes-part-global-operation-disrupt-zloader-botnets/

[35] https://www.welivesecurity.com/2022/03/28/under-hood-wslink-multilayered-virtual-machine/

[36] https://www.welivesecurity.com/wp-content/uploads/2022/03/eset_wsliknkvm.pdf

[37] https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-3971

[38] https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-3972

[39] https://www.welivesecurity.com/2021/10/05/uefi-threats-moving-esp-introducing-especter-bootkit/

[40] https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-3970

[41] https://support.lenovo.com/us/en/product_security/len-73440

[42] https://www.welivesecurity.com/2022/04/19/when-secure-isnt-secure-uefi-vulnerabilities-lenovo-consumer-laptops/

[43] https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2017-11882

[44] https://www.welivesecurity.com/2022/01/18/donot-go-do-not-respawn/

[45] https://www.trendmicro.com/en_us/research/20/c/operation-poisoned-news--hong-kong-users-targeted-with-mobile-ma.html

[46] https://www.welivesecurity.com/2022/01/25/watering-hole-deploys-new-macos-malware-dazzlespy-asia/

[47] https://unit42.paloaltonetworks.com/thor-plugx-variant/

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

[49] https://twitter.com/ESETresearch/status/1506904404225630210

[50] https://www.welivesecurity.com/2022/04/27/lookback-ta410-umbrella-cyberespionage-ttps-activity/

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

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

[53] https://www.bleepingcomputer.com/news/security/malicious-powerpoint-files-used-to-push-remote-access-trojans/

[54] https://thehackernews.com/2022/02/notorious-trickbot-malware-gang-shuts.html

[55] https://www.proofpoint.com/us/blog/threat-insight/bumblebee-is-still-transforming

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

[57] https://twitter.com/ESETresearch/status/1494249522301743105

[58] https://twitter.com/ESETresearch/status/1485660697044398081

[59] https://krebsonsecurity.com/2022/01/at-request-of-u-s-russia-rounds-up-14-revil-ransomware-affiliates/

[60] https://www.bleepingcomputer.com/news/security/revils-tor-sites-come-alive-to-redirect-to-new-ransomware-operation/

[61] https://www.bleepingcomputer.com/news/security/revil-ransomware-returns-new-malware-sample-confirms-gang-is-back/

[62] https://www.bleepingcomputer.com/news/security/hackers-use-contis-leaked-ransomware-to-attack-russian-companies/

[63] https://www.bleepingcomputer.com/news/security/oldgremlin-ransomware-gang-targets-russia-with-new-malware/

[64] https://edition.cnn.com/2022/03/30/politics/ukraine-hack-russian-ransomware-gang/index.html

[65] https://twitter.com/BrettCallow/status/1497249143663652865?s=20&t=NUaoFyINtpUfN4Vj2oxBEw

[66] https://twitter.com/contileaks

[67] https://www.washingtonpost.com/politics/2022/03/18/11-big-takeaways-conti-ransomware-leaks/

[68] https://twitter.com/uuallan/status/1498048260425977856?s=20&t=IiOyo7tgumTKIUnLqiermQ

[69] https://www.emsisoft.com/ransomware-decryption-tools/maze-sekhmet-egregor

[70] https://www.bleepingcomputer.com/news/security/free-decryptor-released-for-trickbot-gangs-diavol-ransomware/

[71] https://decoded.avast.io/threatresearch/decrypted-targetcompany-ransomware/

[72] https://www.bleepingcomputer.com/news/security/free-decryptor-released-for-yanluowang-ransomware-victims/

[73] https://decoded.avast.io/threatresearch/help-for-ukraine-free-decryptor-for-hermeticransom-ransomware/

[74] https://arxiv.org/abs/2202.08477

[75] https://krebsonsecurity.com/2022/03/estonian-tied-to-13-ransomware-attacks-gets-66-months-in-prison/

[76] https://www.bleepingcomputer.com/news/security/netwalker-ransomware-affiliate-sentenced-to-80-months-in-prison/

[77] https://www.bleepingcomputer.com/news/security/night-sky-is-the-latest-ransomware-targeting-corporate-networks/

[78] https://www.bleepingcomputer.com/news/security/

night-sky-ransomware-uses-log4j-bug-to-hack-vmware-horizon-servers/

[79] https://www.bleepingcomputer.com/news/security/qnap-warns-of-new-deadbolt-ransomware-encrypting-nas-devices/

[80] https://www.bleepingcomputer.com/news/security/a-look-at-the-new-sugar-ransomware-demanding-low-ransoms/

[81] https://www.bleepingcomputer.com/news/security/new-black-basta-ransomware-springs-into-action-with-a-dozen-breaches/

[82] https://www.bleepingcomputer.com/news/security/beware-onyx-ransomware-destroys-files-instead-of-encrypting-them/

[83] https://techcommunity.microsoft.com/t5/microsoft-365-blog/helping-users-stay-safe-blocking-internet-macros-by-default-in/ba-p/3071805

[84] https://www.bleepingcomputer.com/news/microsoft/microsoft-plans-to-kill-malware-delivery-via-office-macros/

[85] https://twitter.com/ESETresearch/status/1518923380782739458

[86] https://thehackernews.com/2022/04/emotet-testing-new-delivery-ideas-after.html

[87] https://thehackernews.com/2022/03/new-malware-loader-verblecon-infects.html

[88] https://time.com/nextadvisor/investing/cryptocurrency/bitcoin-crash-continues/

[89] https://www.vice.com/en/article/g5qj9j/cryptocom-says-incident-was-actually-dollar30-million-hack

[90] https://www.bleepingcomputer.com/news/cryptocurrency/wormhole-cryptocurrency-platform-hacked-to-steal-326-million/

[91] https://thehackernews.com/2022/02/hackers-steal-17-million-worth-of-nfts.html

[92] https://twitter.com/ESETresearch/status/1497194165561659394

[93] https://www.welivesecurity.com/2021/05/17/android-stalkerware-threatens-victims-further-exposes-snoopers-themselves/

[94] https://techcrunch.com/2022/02/22/stalkerware-network-spilling-data/

[95] https://lab52.io/blog/complete-dissection-of-an-apk-with-a-suspicious-c2-server/

[96] https://blog.appcensus.io/2022/04/06/the-curious-case-of-coulus-coelib/

[97] https://www.wsj.com/articles/apps-with-hidden-data-harvesting-software-are-banned-by-google-11649261181

[98] https://blog.pradeo.com/spyware-facestealer-google-play

[99] https://blog.checkpoint.com/2022/04/07/android-banking-stealer-dubbed-sharkbot-found-disguised-as-legitimate-anti-virus-apps-on-the-google-play-store/

[100] https://www.bitdefender.com/blog/labs/new-flubot-and-teabot-global-malware-campaigns-discovered

[101] https://www.threatfabric.com/blogs/partners-in-crime-medusa-cabassous.html

[102] https://www.threatfabric.com/blogs/xenomorph-a-newly-hatched-banking-trojan.html

[103] https://eprint.iacr.org/2022/208.pdf

[104] https://twitter.com/ESETresearch/status/1521735320852643840

[105] https://www.intezer.com/blog/malware-analysis/new-backdoor-sysjoker/

[106] https://objective-see.com/blog/blog_0x6C.html

[107] https://www.volexity.com/blog/2022/03/22/storm-cloud-on-the-horizon-gimmick-malware-strikes-at-macos/

[108] https://www.politico.eu/article/pegasus-hacking-spyware-spain-government-prime-minister-pedro-sanchez-margarita-robles-digital-espionage-crisis/

[109] https://www.bleepingcomputer.com/news/security/finnish-diplomats-phones-infected-with-nso-group-pegasus-spyware/

[110] https://www.reuters.com/technology/exclusive-iphone-flaw-exploited-by-second-israeli-spy-firm-sources-2022-02-03/

[111] https://googleprojectzero.blogspot.com/2022/03/forcedentry-sandbox-escape.html

[112] https://www.cvedetails.com/vulnerability-list/vendor_id-49/product_id-15556/Apple-Iphone-Os.html

[113] https://www.exploit-db.com/exploits/41471

[114] https://www.shodan.io/search/report?query=jaws%2F1.0

[115] https://nvd.nist.gov/vuln/detail/CVE-2017-18368

[116] https://nvd.nist.gov/vuln/detail/CVE-2015-2051

[117] https://twitter.com/360Netlab/status/1420390398825058313

[118] https://thehackernews.com/2022/04/new-enemybot-ddos-botnet-borrows.html

[119] https://www.bleepingcomputer.com/news/security/new-fodcha-ddos-botnet-targets-over-100-victims-every-day/

[120] https://www.vice.com/en/article/akv7z5/how-a-hacker-controlled-dozens-of-teslas-using-a-flaw-in-third-party-app

[121] https://arstechnica.com/information-technology/2022/02/russias-most-cut-throat-hackers-infect-network-devices-with-new-botnet-malware/

[122] https://thehackernews.com/2022/03/new-variant-of-russian-cyclops-blink.html

[123] https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-disruption-botnet-controlled-russian-federation

[124] https://thehackernews.com/2022/03/over-200000-microtik-routers-worldwide.html

[125] https://www.welivesecurity.com/2021/12/13/log4shell-vulnerability-what-we-know-so-far/

[126] https://thehackernews.com/2022/01/initial-access-broker-involved-in.html

[127] https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/

[128] https://www.zdnet.com/article/chinese-hackers-deep-panda-return-with-log4shell-exploits-new-fire-chili-rootkit/

[129] https://securityaffairs.co/wordpress/128159/apt/tunnelvision-exploits-log4j-vulnerability.html

[130] https://www.rezilion.com/wp-content/uploads/2022/04/Log4Shell-4-Months-Later.pdf

[131] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22965

[132] https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/

[133] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0847

[134] https://dirtypipe.cm4all.com/

[135] https://googleprojectzero.blogspot.com/2022/04/the-more-you-know-more-you-know-you.html

[136] https://www.mandiant.com/resources/zero-days-exploited-2021

[137] https://www.rsaconference.com/usa/agenda/session/ESPecter%20First%20Real-World%20UEFI%20Bootkit%20Persisting%20on%20ESP

[138] https://www.blackhat.com/us-22/briefings/schedule/#industroyer-sandworms-cyberwarfare-targets-ukraines-power-grid-again-27832

[139] https://www.virusbulletin.com/conference/vb2022/

[140] https://recon.cx/2022/conference.html

[141] https://whova.com/embedded/session/xfYtdNgvSv-eYXY1By4aWq606%4092h9NXnd7hwTzd-z4=/2292486/?widget=primary

[142] https://caro2022.org/agenda/

[143] https://botconf2022.sched.com/event/1199o/ta410-apt10s-distant-cousin

[144] https://botconf2022.sched.com/event/119AL/jumping-the-air-gap-15-years-of-nation-state-efforts

[145] https://nsec.io/speakers/

[146] https://botconf2022.sched.com/event/119A0/proxychaos-a-year-in-review-of-microsoft-exchange-exploitation

[147] https://www.seqcure.org/en/#speakers

[148] https://www.esetworld.com/growth.protected/event-agenda/detail/157

[149] https://eecd.eset.com/agenda/detail/112

[150] https://www.computerworld.pl/event/semaforeng

[151] https://eecd.eset.com/agenda/detail/117

[152] https://eecd.eset.com/agenda/detail/120

[153] https://www.welivesecurity.com/author/goretsky/

[154] https://open.spotify.com/show/1WDjY2A3A3s5FKycrOVkhg

[155] https://podcasts.google.com/feed/aHR0cHM6Ly9mZWVkLnBvZGJlYW4uY29tL2VzZXRyZXNlYXJjaC9mZWVkLnhtbA

[156] https://podcasts.apple.com/us/podcast/eset-research-podcast/id1596306608

[157] https://esetresearch.podbean.com/

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

[159] https://attack.mitre.org/techniques/T1055/015/

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

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

[162] https://attack.mitre.org/resources/updates/updates-april-2022/

[163] https://attackevals.mitre-engenuity.org/enterprise/wizard-spider-and-sandworm/

[164] https://attackevals.mitre-engenuity.org/using-attack-evaluations/

[165] https://www.eset.com/int/business/solutions/xdr-extended-detection-and-response/

[166] https://www.eset.com/blog/awards-and-testing/hunting-down-sandworm-and-wizard-spider-how-eset-fared-in-the-attckr-evaluation/

[167] https://www.welivesecurity.com/2016/12/13/rise-telebots-analyzing-disruptive-killdisk-attacks/

[168] https://www.welivesecurity.com/2017/06/30/telebots-back-supply-chain-attacks-against-ukraine/

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

[170] https://www.eset.com/int/about/newsroom/press-releases/research/eset-takes-part-in-global-operation-to-disrupt-trickbot-a-botnet-that-has-infected-over-a-million-c/

[171] https://twitter.com/ESETresearch/status/1409495354534473728

[172] https://github.com/eset/vulnerability-disclosures/commit/0b456d6fd13abb60407c2491904fd11613ead6c9

[173] https://developer.amd.com/amd-uprof/

[174] https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1016

[175] https://www.brighttalk.com/webcast/5567/537094

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

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

[178] https://help.eset.com/glossary/en-US/adware.html

Acerca de ESET

Por más de 30 años, ESET® ha estado desarrollando software y servicios de seguridad informática líderes en la industria para proteger a las empresas, la infraestructura crítica y los consumidores en todo el mundo ante las amenazas digitales cada vez más sofisticadas. Desde la seguridad para endpoints y dispositivos móviles hasta la detección y respuesta para endpoints, además del cifrado y la autenticación en varias fases, las soluciones de alto rendimiento y fáciles de usar de ESET brindan protección y supervisión en forma discreta las 24 horas, los 7 días de la semana, y actualizan las defensas en tiempo real para mantener a los usuarios seguros y a las empresas funcionando sin interrupciones. Las amenazas en evolución exigen que la empresa de seguridad de TI también esté en constante evolución para permitir el uso seguro de la tecnología. ESET cuenta con el respaldo de sus Centros de Investigación y Desarrollo distribuidos en todo el mundo, que trabajan en pos de nuestro futuro común. Para obtener más información, visite www. eset-la. com o síganos en LinkedIn, Facebook y Twitter.

WeLiveSecurity.com
@ESETresearch
ESET GitHub

Digital Security
Progress. Protected.