GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

CCN-CERT IA-25/18

Cryptojacking

Septiembre 2018

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2018.09.12 09:40:54 +02'00'

Fecha de Edición: septiembre de 2018

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1. PRÓLOGO

Actualmente, las criptomonedas son consideradas por muchos como una divisa más, tan válida como cualquier otra. Y es que, desde su aparición en 2009, el mundo de la criptodivisa no ha dejado de evolucionar y de integrarse en el comercio electrónico. Bitcoin es la más famosa y la más usada: su valor inicial no llegaba apenas a la décima parte de céntimo de dólar y, sin embargo, consiguió alcanzar picos de 20.000 dólares en diciembre de 2017.

Con todo, Bitcoin no es la única: Bitcoin cash, Ethereum, Lite Coin, Ripple o Dash son algunos de los ejemplos más significativos de las más de 700 criptomonedas que existen.

La creciente aceptación tanto por parte de empresas, gobiernos y los propios usuarios, así como la posibilidad de intercambiar el dinero digital por físico y el anonimato que caracteriza las transacciones electrónicas de estas nuevas criptodivisas, ha propiciado que los ciberdelincuentes vean esto como una oportunidad de ganar dinero de forma fraudulenta. Nace así lo que se conoce como cryptojacking: el uso ilegítimo de un equipo por parte de los cibercriminales para realizar el proceso de obtención de criptomonedas y obtener el total de las ganancias.

El objetivo de este documento es presentar a un nivel más técnico y con más detalle este nuevo tipo de amenaza: cómo funciona, cuáles son los fundamentos que hay detrás, cómo de dañina puede llegar a ser, los distintos procedimientos que tienen los ciberdelincuentes para propagar la infección y las medidas que son necesarias tomar para protegerse son algunos de los puntos cruciales de este informe.

2. ESTADO ACTUAL

Con el paso del tiempo, el número de variantes de cryptominers ha crecido de manera muy rápida. Concretamente, se estima que en enero de 2018 el número de muestras de este tipo de código dañino rondaba los 94.000, mientras que sólo 3 meses más tarde, esta cifra llego a incrementarse un 74% (127.000 muestras).

Como se comenta a lo largo del documento, se ha observado también una relación entre la crecida del uso de cryptominers y el descenso del uso del ransomware, el cual, en el mismo periodo de tiempo, ha decrecido entre un 30 y un 42 por ciento.

Según Adguard, el cryptomining podría haber afectado a 500 millones de personas, principalmente de países como Estados Unidos, India, Rusia y Brasil.

Al contrario que con el ransomware, calcular las ganancias obtenidas mediante estos métodos no es una tarea tan sencilla. Según la misma fuente, y realizando un estudio sobre las 100.000 páginas más visitadas (Alexa's Top Sites), 220 sitios usaban minadores que podrían producir unas ganancias semanales de 15.000 dólares.

En los últimos meses, las infecciones han evolucionado para propagarse por las plataformas de CMS más usadas, por repositorios públicos (a través de los cuales se infectaron 550 sitios según Sucuri – enero de 2018), dispositivos IoT…

En definitiva, se trata de una amenaza que crece y se propaga a ritmo muy veloz y de la cual es necesario estar muy alerta y conocer cómo funciona para poder prevenir y mitigar los ataques.

Figura 1. Resumen del estudio realizado por Adguard en 100.000 sitios web.

3. PROCESO AL DETALLE

Para entender qué acciones son las que se llevan a cabo es necesario entender el proceso legítimo por el cual se pueden adquirir criptomonedas. En primer lugar, estas divisas pueden adquirirse mediante la compraventa y el intercambio. En segundo lugar, y con más interés, mediante el minado. Para entender el proceso de minado es necesario explicar antes otros términos.

3.1 BLOCKCHAIN

Traducido del inglés, cadena de bloques, se trata de una red descentralizada donde quedan registradas todas las transacciones (bloques) que los usuarios de criptomonedas como Bitcoin o Ethereum realizan. Se podría definir como un libro mayor de cuentas que dota de la posibilidad al usuario de no necesitar intermediario ni ninguna autoridad para participar en una transacción. La propia validación o confirmación de dicha transacción (o bloque) se realiza entre los nodos independientes que conforman la Blockchain. Estos nodos son los conocidos como *mineros*, personas que realizan dos trabajos: confirmar transacciones y escribirlas en el *libro mayor* (Blockchain).

3.2 CONFIRMACIÓN DE BLOQUES. LA BASE DEL MINADO.

La operación para confirmar transacciones es básicamente la siguiente:

Se crea un hash para un bloque en concreto, utilizando como entrada la propia información del bloque y el hash del bloque anterior (así se consigue que se trate de una red cuyos bloques "dependen" unos de otros). Esta operación es computacionalmente sencilla, por lo que se introdujeron una serie de requisitos que

debía cumplir este hash creado. Para ello, se introdujo una tercera variable a la hora de crear el hash conocido como *nonce*, una especie de formato que debe cumplir el hash creado. Si no se ajusta al formato requerido, el *nonce* se cambia y se prueba de nuevo.

Esta última operación tiene un costo computacional alto, pues una de las propiedades de las firmas hash es la no predicción del resultado en base a los datos de entrada, y por lo tanto no queda más remedio que probar combinaciones aleatorias. Debido a esta dificultad, un equipo no trabaja con un bloque en concreto, sino toda una red de mineros.

4. VÍAS DE INFECCIÓN

Las vías de infección no difieren mucho de los métodos que los cibercriminales emplean para distribuir otros códigos dañinos. Se destacan las siguientes vías:

4.1 PHISHING

Se trata de una de las técnicas más usadas para distribuir código dañino. Es un método muy conocido a la par que viejo, y aunque su efectividad se ha visto reducida, sigue siendo muy exitosa al basarse en el factor humano.

Consiste en tratar de conseguir, mediante la ingeniería social (o el engaño) que una persona realice una serie de acciones que faciliten al atacante obtener control de la máquina sin que dicha persona sea consciente. Dichas acciones pueden variar entre hacer clic en un enlace dañino, abrir un archivo (en muchos casos de carácter ofimático), descargar un fichero adjunto o inserción de credenciales en el formulario de una página que aparenta ser legítima (de un banco, de una empresa, etc.) pero que en realidad es una copia creada por el atacante.

Una muestra que utiliza este método de infección es Trickbot, descrito en detalle en la sección 7 de este documento.

4.2 EXPLOIT KITS

Se trata de una vía de infección más sofisticada que la anterior. Los Exploit Kits son herramientas que automatizan la búsqueda de vulnerabilidades en el equipo de la víctima, ya sean vulnerabilidades del propio sistema operativo o del software instalado en él (como los navegadores y sus complementos) que pudieran ser explotadas para ganar acceso.

Un ejemplo de este tipo de ataques se observa en una campaña denominada Ngay que utilizaba RIG Exploit Kit para distribuir cryptominers. En concreto, el software malicioso instalado estaba destinado a las criptomonedas Monero y Electroneum, usando la vulnerabilidad catalogada como CVE-2018-8174.

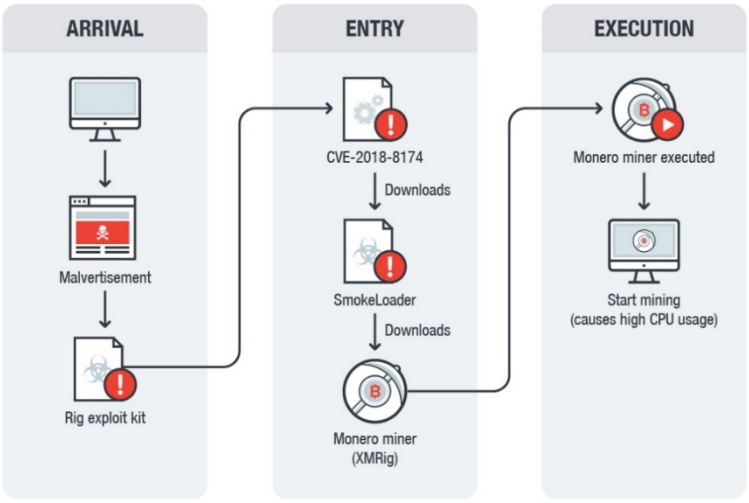


Figura 2. Proceso de infección utilizado por RIG Exploit Kit. Fuente: Trendmicro

Como se puede observar en la figura, la cadena de sucesos sería la siguiente:

Un usuario accede a una página web aparentemente normal pero que en realidad ha sido infectada. Dicho enlace contiene código oculto el cual se ejecuta y redirecciona al visitante a una página de terceros donde, mediante la vulnerabilidad CVE-2018-8174, se ejecuta código remoto que finalmente inicia la descarga de SmokeLoader. Este downloader descarga el payload final, es decir, la carga dañina (el minero de Monero). En algunos casos, el downloader era otro tipo de código dañino muy sofisticado, capaz de evitar antivirus y máquinas de análisis automatizadas (sandbox).

4.3 ATAQUES DE FUERZA BRUTA

Se ha observado como en el último año los ataques mediante fuerza bruta a servicios accesibles desde internet se han incrementado considerablemente. En concreto, los ataques al servicio RDP (Remote Desktop Protocol o escritorio remoto) han sido una de las recientes vías de infección de otros códigos dañinos como el ransomware.

En lo que se refiere al cryptojacking, miles de páginas basadas en Wordpress y Magento fueron infectadas con este tipo de amenaza mediante la recolección de información en fuentes abiertas (OSINT) y el uso de ataques con diccionario y fuerza bruta. En este último caso, se distribuía un minero de Monero llamado XMRig, el cual estaba configurado para ejecutarse tras una cadena de proxys para ocultar la identidad del atacante.

4.4 CÓDIGO DAÑINO

La ejecución de cualquier tipo de malware puede acarrear la instalación de un minador ilícito en el sistema. Esto se debe a que muchos códigos dañinos, como troyanos o botnets, no fueron diseñados en un principio para distribuir explícitamente cryptominers, pero que en los últimos años han evolucionado. En el último año, se ha

observado como cada vez más malware incluye funcionalidades adicionales relacionadas con el uso ilegítimo de los recursos del equipo infectado.

Algunos de estos códigos dañinos son Trickbot, Rakhni, Rarog, Adylkuzz y Smominru. Estas amenazas son explicadas con más detalle en el apartado 7.

4.5 IoT

Según Avast, "15800 aparatos electrónicos serían necesarios para obtener 1000 dólares en 4 días a través del minado de Monero". Según Shodan, más de 58.000 dispositivos son vulnerables sólo en la ciudad de Barcelona.

Es un factor de riesgo que es imprescindible contemplar, ya que con la evolución del mundo IoT (Internet of Things – El internet de las cosas) cada vez más dispositivos como neveras, cámaras o TVs ofrecen una conexión a internet.

Se estima que para 2025 el número de dispositivos IOT alcance los 75 billones.

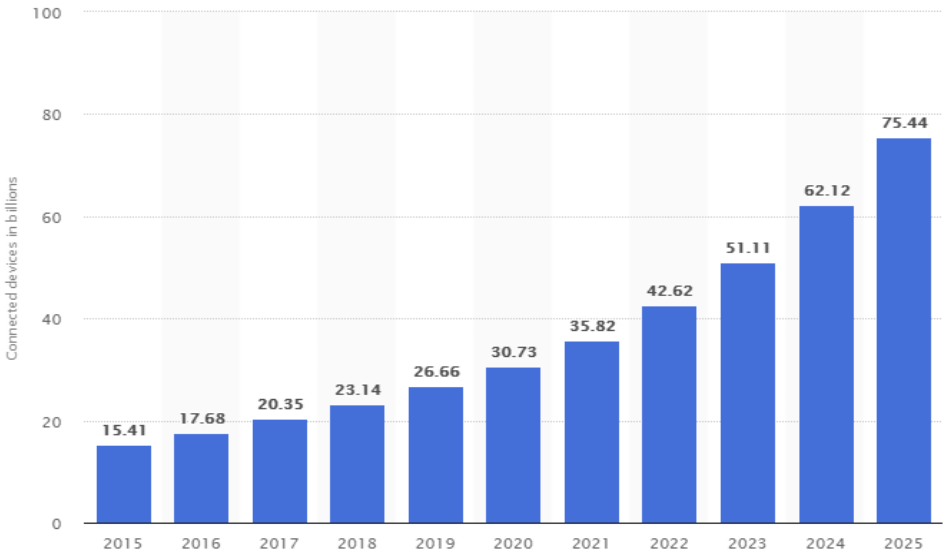


Figura 3. Previsión del número de dispositivos IoT

A la par que el número de dispositivos IoT crece (actualmente el número se sitúa en 23 billones), también crece el número de malware que busca vulnerabilidades en estos dispositivos, como por ejemplo la botnet Mirai. El objetivo principal de esta botnet son las cámaras y los routers, a los que trata de ganar acceso mediante el servicio telnet probando las combinaciones de usuarios y contraseñas más utilizadas. Actualmente posee la capacidad de minar Bitcoins.

4.6 CRYPTOMINERS EN LA WEB

Este apartado incluye a los cryptominers que se ejecutan en una página web y que se aprovechan de los recursos de los visitantes. Su funcionamiento se basa en la

ejecución de un script, la mayoría de los casos en el lenguaje de programación Javascript, incrustado en el código fuente del sitio.

En un principio se trata de los minadores menos dañinos para la víctima, pues no requiere de la infección de la máquina. Si es cierto que la inserción de este código ha podido realizarse de manera ilícita por terceras personas, lo que induce el riesgo de que, además del minador, se haya cargado cualquier otro tipo de código dañino.

El cryptominer más habitual es CoinHive, el cual se encuentra según Shodan en más de 33.000 sitios. El alto número de páginas web y el carácter comercial de la mayoría de los cryptominers indica que la inclusión del código necesario para que se ejecute el cryptominer puede producirse de manera legítima.

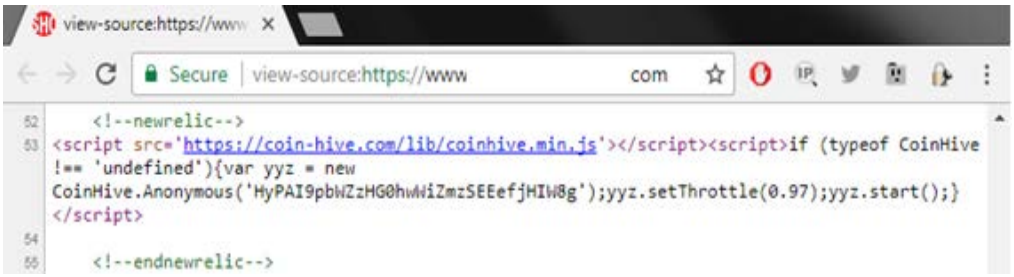


Figura 4. Código de CoinHive insertado en un sitio web.

4.7 DISPOSITIVOS MÓVILES

Al igual que los dispositivos IoT, los teléfonos móviles también se han visto afectados. Los escenarios más frecuentes de infección son, por un lado, aquellas aplicaciones obtenidas de sitios de dudosa reputación que prometen un contenido premium sin realizar ningún pago o que una aplicación totalmente legítima sea modificada por un tercero sin autorización.

A pesar de que existen campañas de propagación de malware muy complejas, la mayoría de los casos consiste en aplicar la ingeniería social para conseguir que un usuario final se descargue y ejecute la aplicación dañina. Este tipo de aplicaciones ilegítimas suelen también ser distribuidas mediante phishing, correos no deseados (spam), a través de anuncios, juegos y extensiones del navegador.

Un caso muy llamativo por los estragos físicos que puede llegar a causar al dispositivo móvil es el del código dañino Loapi, el cual utiliza al máximo los recursos de dicho dispositivo llegando incluso a generar tanto calor que, en algunos casos, ha llegado a provocar deformaciones o quemaduras en la carcasa y/o componentes electrónicos del dispositivo.

Figura 5. Daños producidos por Loapi en un dispositivo móvil.

4.8 VULNERABILIDADES

Muchos de los objetivos de los ciberdelincuentes son aquellos equipos expuestos a internet sin una configuración correcta. Se han detectado ataques a supercomputadores de grandes universidades, los cuales son muy atractivos para los ciberdelincuentes por su gran capacidad de cómputo. Estos ataques, en muchos casos, han tenido éxito por una mala gestión de los servidores (configuraciones por defecto, equipos sin actualizar, etc.).

Los ciberdelincuentes utilizan tanto vulnerabilidades 0-day (extremadamente recientes y que, por escasez de tiempo, no existe un parche preventivo) como vulnerabilidades más antiguas que no han sido parcheadas.

A su vez, se pueden servir de técnicas de ataques más específicas contra servidores como ataques de fuerza bruta, inyecciones SQL, CSRF o buscadores automáticos de vulnerabilidades para tomar control del equipo.

5. MEDIDAS PREVENTIVAS

Como se ha visto en el apartado 4. VÍAS DE INFECCIÓN, la mayoría del software minador ilícito se distribuye mediante la ejecución de otro tipo de malware. Es por ello por lo que, aunque algunas medidas que se presentan a continuación sean específicas para evitar al máximo los cryptominers, muchas de ellas son de carácter genérico y pueden aplicarse para frenar cualquier amenaza.

5.1 SUPERVISIÓN Y MONITORIZACIÓN DE LOS RECURSOS UTILIZADOS.

El uso elevado de recursos de un equipo es la característica más notable de que se está ejecutando un cryptominer. Llevar a cabo una monitorización del uso de CPU y memoria del sistema es clave a la hora de detectar este tipo de amenazas.

A pesar de que existen herramientas de terceros, Windows provee de utilidades nativas sencillas de usar. En el ejemplo que se ilustra a continuación se hace uso del *monitor de recursos*.

Para utilizarlo, en la ventana de inicio, se debe escribir *resmon* y ejecutar.

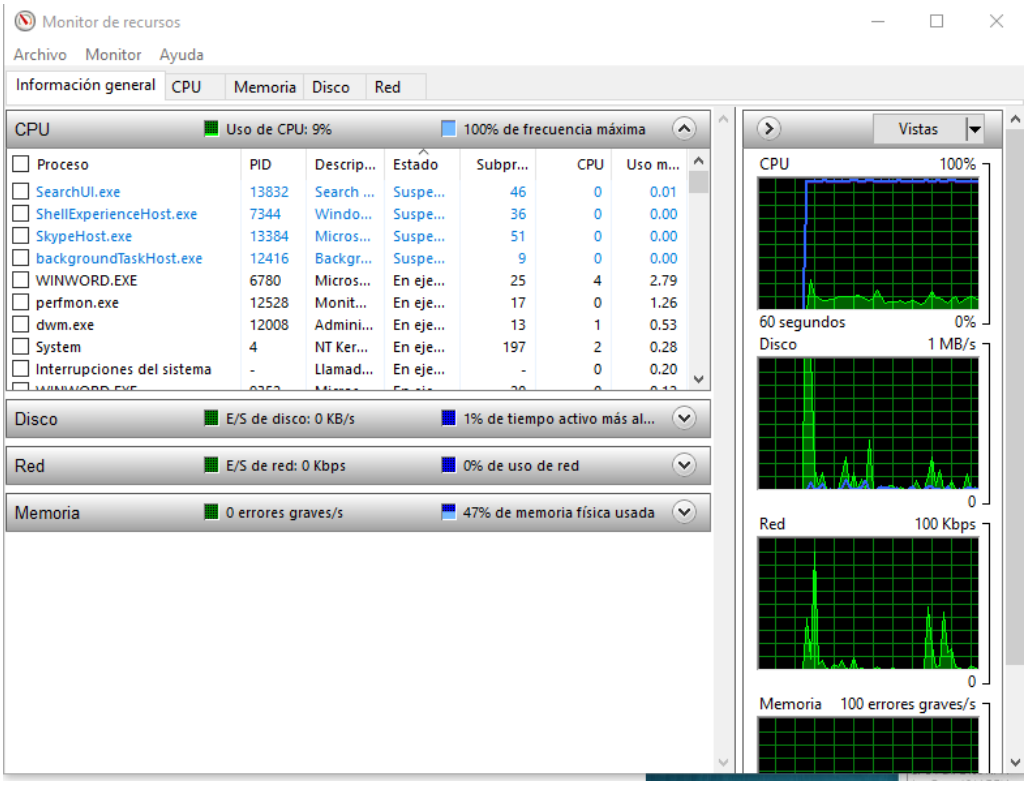


Figura 6. Monitor de recursos de Windows.

Como se observa en la figura, se pueden navegar por las diferentes pestañas para obtener información más detallada sobre el uso de CPU, memoria, operaciones en disco… En la mayoría de los casos será suficiente con la primera pestaña (Información general).

El proceso de monitorización consiste en vigilar un uso constante en el tiempo (no picos puntuales) de una gran carga de CPU o memoria e identificar qué proceso está provocando dichos consumos para poder pararlo e investigarlo más detenidamente. Cabe decir, que existen procesos/aplicaciones que pueden consumir muchos recursos y que no deben confundirse con cryptominers (por ejemplo, juegos con requisitos elevados, procesos de renderizado…).

Adicionalmente, se detalla cómo acceder al monitor de recursos desde otros Sistemas Operativos ampliamente usados:

Para acceder a los recursos utilizados por el sistema en Macintosh, se debe presionar la tecla Comando + la barra espaciadora, introducir en la barra de búsqueda “Activity Monitor” y presionar intro.

Para acceder al monitor de recursos en un sistema Linux se debe introducir el comando *top -i* en la terminal. Acceder a la terminal depende de la distribución (e incluso del gestor de ventanas) instalada en el equipo. En Ubuntu, por ejemplo, se puede acceder presionando las teclas Ctr + Alt + T.

5.2 CUIDADO DEL NAVEGADOR. USO DE EXTENSIONES

Por un lado, son interesantes aquellas extensiones de navegador que se encargan de bloquear ventanas emergentes y anuncios.

Esto es importante pues muchas páginas web lanzan una pequeña ventana que minimizan al instante, con el objetivo de que pase lo más inadvertida posible. En esta ventana minimizada es donde puede comenzar el proceso de minado o la ejecución de otro código dañino. Para este tipo de casos, se recomienda el uso de extensiones como AdBlock (para anuncios) y PopUp Blocker (para ventanas emergentes no deseadas).

Por otro lado, existen extensiones específicas para detectar minadores incrustados en el código fuente de la página web que se esté visitando y bloquearlo.

Se recomienda Minerblock, pues además ofrece un segundo tipo de protección complementaria basada en listas negras actualizadas de sitios online, reportados por el uso de este tipo de software sin autorización de los visitantes.

Es de vital importancia conocer las fuentes desde las que se instalan estas extensiones. Es por ello que solo deben instalarse desde sitios de confianza, tales como Google Play, Microsoft Store, Apple App Store…

A su vez es importante recordar que es primordial mantener las extensiones actualizadas y realizar una comprobación periódica de que no se hayan instalado unas nuevas sin consentimiento, ya que cabe la posibilidad de que al visitar determinados sitios web se instalen extensiones ilegítimas.

Además de todo lo anterior, se recomienda visitar de forma regular el siguiente enlace que determina si el navegador está infectado con cryptominers: https://cryptojackingtest.com/.

5.3 DESHABILITAR JAVASCRIPT

Muchos de los minadores que se ejecutan en navegadores están escritos en Javascript, por lo que desactivarlo puede ser una opción. Sin embargo, esto puede repercutir en aquellas páginas que necesiten legítimamente la ejecución de Javascript para poder funcionar.

Existe la extensión denominada Toggle Javascript (Toggle JS para FireFox) que permite activarlo y desactivarlo rápidamente en vez de tener que acceder a la configuración del navegador.

5.4 SECURIZAR SERVICIOS EXPUESTOS A INTERNET

Los servicios que inevitablemente han de estar expuestos a internet han de estar debidamente protegidos. Como se ha mencionado, numerosos ataques se producen mediante ataques de fuerza bruta a, por ejemplo, el servicio RDP (Remote Desktop Protocol). A su vez, multitudes de máquinas y servidores tienen desplegados multitud

de servicios que, en la mayoría de los casos, no son necesarios para el funcionamiento de la organización, pero que son un potencial vector de entrada para ciberdelincuentes.

Se conoce como Hardening a la práctica que consiste en detectar que recursos de una organización están expuestos a internet, averiguar cuáles son cruciales, deshabilitar aquellos que no lo son e identificar posibles puntos de entrada o vulnerabilidades.

Dada la capacidad técnica que el Hardening requiere, se detallará exclusivamente como proteger (o deshabilitar en caso de que no sea necesario) el servicio RDP de Windows, pero sin lugar a dudas se deberían revisar otros como SSH, servidores SQL…

En Windows 10, deshabilitar las conexiones remotas es una tarea muy sencilla y bastará con seguir estos pasos:

1. En la pestaña de Inicio, escribir "*SystemPropertiesRemote*".
2. En la ventana de Acceso Remoto, en la parte inferior seleccionar "No permitir las conexiones remotas a este equipo".

Se ofrecen otras opciones, como permitir la conexión solo a unos usuarios determinados. Esta opción puede ser la más adecuada si es imposible para la organización o el usuario deshabilitar el servicio.

Asimismo, los usuarios que hagan uso del RDP (y de forma general) deberán usar un par usuario-contraseña robusto y único para cada acceso a los diferentes servicios que dispongan. Una contraseña segura, como norma general, ha de estar formada por una combinación de caracteres alfanuméricos y símbolos, alternando mayúsculas y minúsculas, lo más larga posible y de la mayor aleatoriedad posible.

Dado que este tipo de contraseñas no son fáciles de recordar, existen herramientas como KeePass para gestionarlas.

Además de lo anterior, y si existen los recursos, sería recomendado el uso de Firewalls, IPS/IDS (Sistemas de Prevención y Detención de Intrusos) entre otros.

6. MEDIDAS REACTIVAS

Las medidas que se tomaran para desinfectar un equipo de la presencia de cryptominers dependen de la naturaleza de estos. Es por ello que se crean dos apartados para diferenciar los cryptominers de navegador, y los cryptominers ejecutados por otro código dañino.

6.1 CRYPTOMINERS DE NAVEGADOR.

Si se detecta la ejecución de cryptominers en un sitio web en concreto, como en la mayoría de las ocasiones éstos no cuentan con persistencia en el equipo, bastará con cerrar la pestaña donde se ha cargado la página.

Adicionalmente, se recomienda bloquear los siguientes puertos TCP/UDP (en caso de no ser utilizados): 3333, 5555, 7777, 8000 y 14444 y bloquear aquellos dominios que aparecen en la siguiente blacklist: http://iplists.firehol.org/

6.2 CRYPTOMINERS EJECUTADOS POR OTRO CÓDIGO DAÑINO.

Sin embargo, si se detecta una infección en el sistema es muy poco probable que se trate de un cryptominer aislado, por lo que habrá que identificar el malware que lo lleva como carga.

6.2.1 IDENTIFICAR EL MALWARE

La gran mayoría de código dañino trata de poder ejecutarse a la vez o antes de que se ejecute el sistema operativo (persistencia). Es por ello por lo que un buen punto de partida es identificar aquellos procesos desconocidos que están configurados para ejecutarse en el inicio del sistema.

Para dicha tarea, se puede emplear una herramienta de SysInternals llamada Autoruns. Este programa muestra aquellas aplicaciones que se ejecutan durante el inicio del sistema operativo, cuando se inicia sesión o cuando se lanzan aplicaciones de terceros gracias a que Autoruns comprueba numerosos lugares del sistema donde el malware puede establecer persistencia (entradas de registro, tareas programadas, servicios…).

Para usarla, ha de descargarse desde https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns

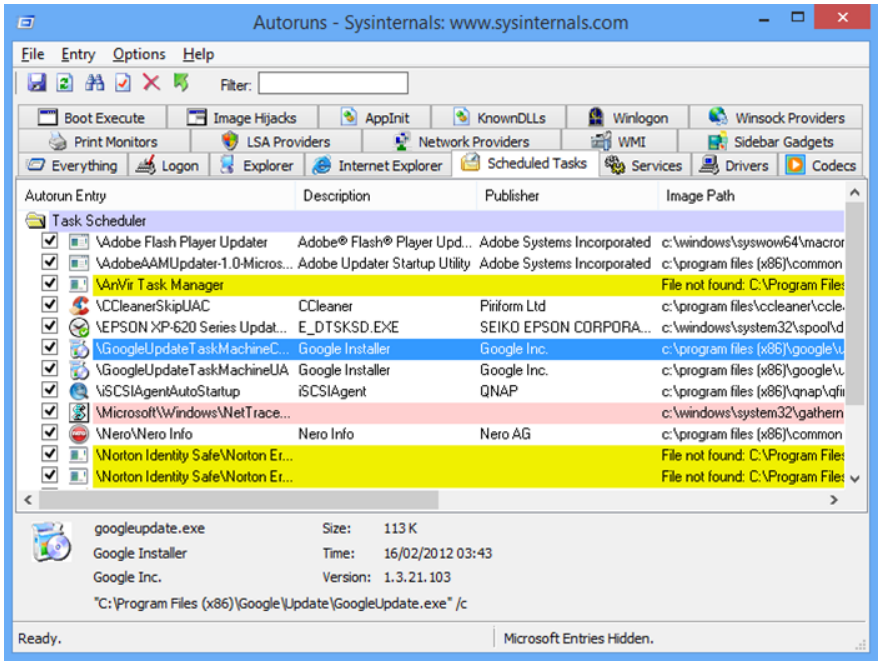


Figura 7. Autoruns. Ejecutables lanzados al inicio del sistema.

Autoruns se ejecutará con la pestaña *Everything* cargada, la cual ofrece mucha información. Si la cantidad de datos presentes en dicha pestaña es demasiado a primera vista, se recomienda visualizar las siguientes pestañas que engloban los puntos de persistencia por tipos: *logon*, *Internet Explorer*, *tareas programadas*, etc.

Si se localizan programas desconocidos sería recomendado deshabilitarlos, siempre y cuando se esté seguro de que dichos procesos son realmente sospechosos e innecesarios para el sistema para su correcto funcionamiento. Para esta tarea, Autoruns facilita la subida del fichero que se considera dañino a VirusTotal para obtener un reporte haciendo click derecho sobre este

6.2.2 IDENTIFICACIÓN DEL MALWARE. DETALLES.

Además, esta herramienta mencionada provee de las rutas donde se encuentra dicho ejecutable. Si se consiguiera aislar, es muy recomendable analizarlo en páginas que ofrezcan análisis de muestras.

Las más recomendadas son VirusTotal o Malwr. Ambas páginas ofrecen un análisis del posible código dañino con un gran número de antivirus diferentes. Esto es muy útil, pues ofrece diversos resultados que sirven para tomar una decisión en cuanto a saber si realmente se trata de código dañino. Malwr, adicionalmente, entrega otros informes mucho más detallados, pues carga el ejecutable en lo que se conoce como “sandbox” para registrar todas las acciones como si de un equipo real se tratara.

Dada la amplia gama de malware que existe y las peculiaridades de cada familia (archivos que extraen, rutas donde se copian, persistencia, inyecciones en procesos…), además de todo lo anterior, es totalmente recomendable analizar el equipo con el antivirus instalado, así como otras soluciones antimalware.

Una vez que la amenaza ha sido eliminada, es muy recomendable vigilar el equipo de cerca para asegurarse de que se ha eliminado completamente o por el contrario se ha vuelto a ejecutar (existen códigos dañinos que permanecen a la espera un determinado tiempo para evitar sospechas).

7. MUESTRAS Y CAMPAÑAS PRINCIPALES

El objetivo de este apartado es dar a conocer las campañas más conocidas relacionadas con cryptojacking. Para ello, se diferencia entre cryptominers de navegador y cryptominer ejecutados por otro código dañino.

7.1 CRYPTOMINERS DE NAVEGADOR

En cuanto a cryptominers web se destaca, como ya se ha mencionado, a CoinHive. Es el cryptominer web más popular, y dado su carácter comercial es usado tanto de manera legítima como ilegítima en multitud de sitios web.

Otros minadores del mismo carácter son JSECoin y AuthedMine, aunque no gozan de tanta popularidad como CoinHive.

7.2 CRYPTOMINERS EJECUTADOS POR OTRO CÓDIGO DAÑINO

En este apartado se describe con más detalle las amenazas expuestas en el apartado 4.4 CÓDIGO DAÑINO.

7.2.1 TRICKBOT

Se trata de un troyano bancario que apareció en 2016 y que en 2017 añadió funcionalidades de cryptojacking. Se distribuye a través de campañas de Phishing en las que se hace pasar por notificaciones legítimas de diferentes bancos.

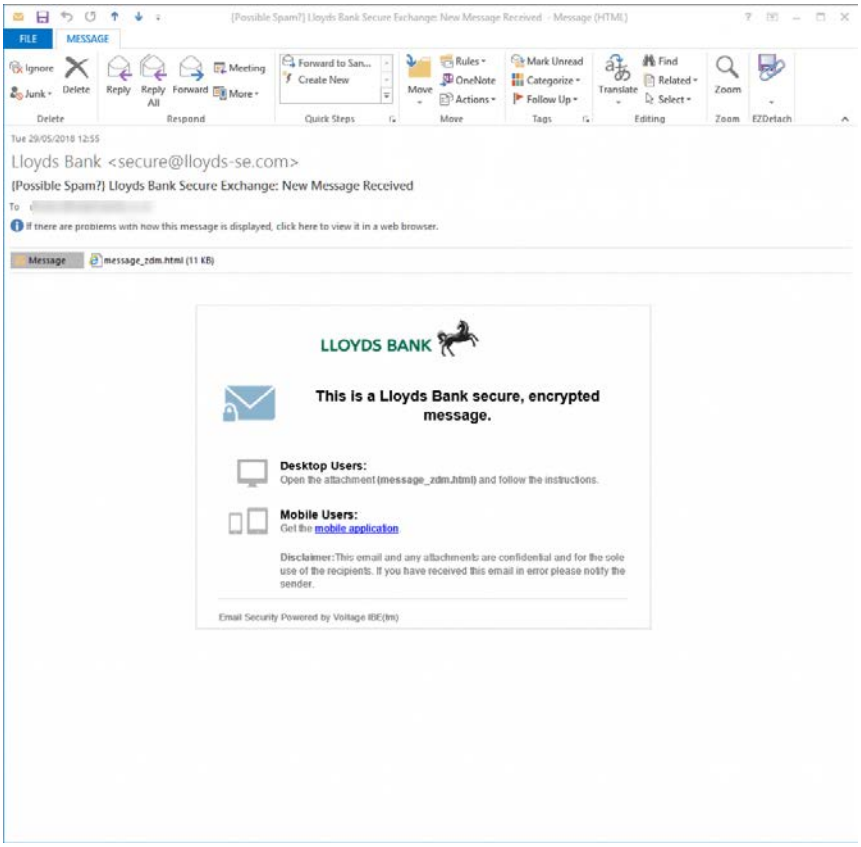


Figura 8. Ejemplo de correo enviado por Trickbot.

El proceso de infección depende de la variante/campaña del momento, pero en el de este caso procedía del siguiente modo: en caso de acceder al enlace que aparece adjunto, se descarga en el equipo del usuario un documento ofimático de tipo Word. Este provoca una redirección a un documento RTF final mediante una vulnerabilidad conocida en el editor de ecuaciones de Word.

Dicho RTF hace uso de una vulnerabilidad catalogada como CVE-2017-11882 para tratar de conectar a un servidor desde el cual se descarga el propio binario Trickbot.

Por otra parte, el troyano trata de usar el exploit EternalBlue (usado también por WannaCry) entre otros para propagarse.

Para más información se pueden consultar los siguientes enlaces: https://www.securityartwork.es/wp-content/uploads/2017/06/Informe_Evoluci%C3%B3n_Trickbot.pdf

7.2.2 ADYLKUZZ

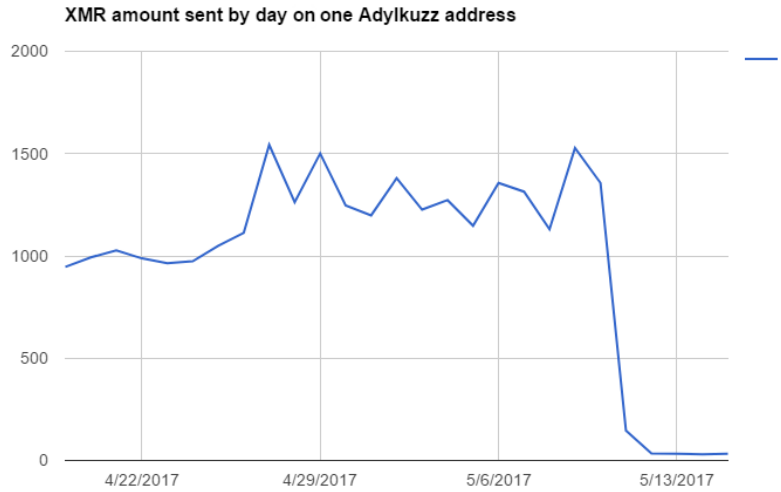
Este cryptominer se empezó a distribuir en 2017 de manera idéntica a como lo hizo WannaCry: usando EternalBlue y DoublePulsar. Las infecciones de WannaCry y de Adylkuzz comenzaron con apenas una semana de diferencia.

Lo interesante de este código dañino es que "protege" el PC de otro tipo de amenazas. Los síntomas de la infección, además de la perdida de potencia por el elevado uso de recursos en el proceso de minado, es la pérdida de acceso a los recursos compartidos de Windows.

Según Avast, los países más afectados han sido Rusia, Ucrania y Taiwán, seguidos de Brasil e India.

Figura 9. Mapa de infecciones de Adylkuzz

La cantidad de dinero que esta campaña ha sido capaz de generar es difícil de estimar, pero estudiando tan solo 3 billeteras asociadas con las campañas (de las múltiples que deben existir), se encuentran sumas de dinero cercanas a los 43.000



dólares.

Figura 10. Moneros obtenidos por día.

7.2.3 SMOMINRU

Se trata de un malware perteneciente a la familia de las Botnet que comprometió más de 526.000 equipos, principalmente servidores. El valor que se pudo obtener con el minado de Monero se estima en 2.3 millones de dólares, lo que la convierte en la botnet de minado más grande hasta la fecha.

Los países más afectados son Rusia, India y Taiwán en orden de relevancia. Para propagarse, hacía uso de los exploits conocidos como EternalBlue y de EsteemAudit (CVE-2017-0176), aunque también intentaba atacar bases de datos Microsoft SQL Server y MySQL.

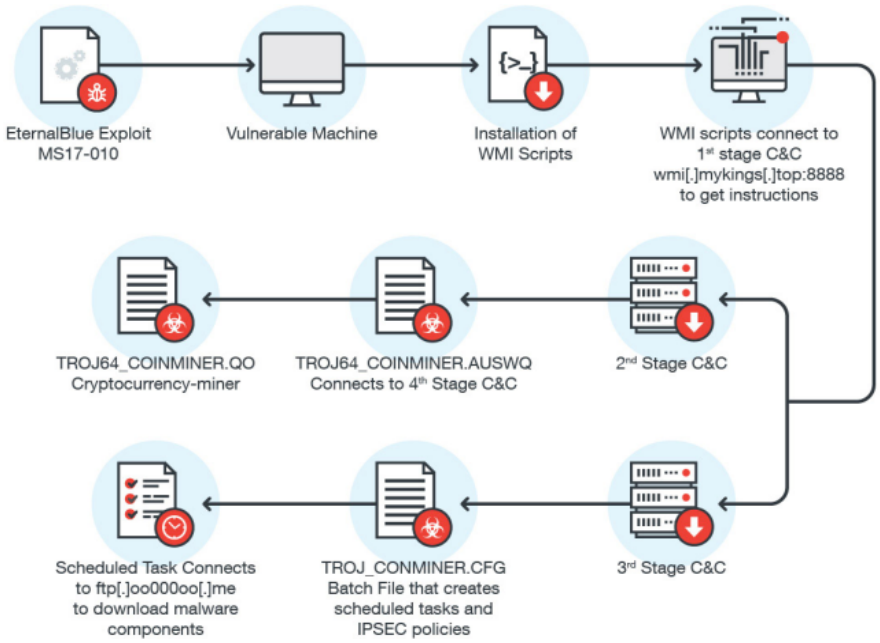


Figura 11. Proceso de infección de Smominru

7.2.4 ROROG

Se trata de un troyano que, a pesar de tener la capacidad de poder minar un amplio abanico de criptomonedas, se ha usado principalmente para minar Monero.

Se promocionó en foros underground como el punto de entrada perfecto para ciberdelincuentes "novatos" dada su sencillez, versatilidad y bajo precio. Según los resultados de diferentes investigaciones (entre las cuales se destaca la del equipo de Palo Alto), el código dañino viene equipado de forma que el atacante pueda configurar y usar cualquier minador en el equipo infectado.

En junio de 2017, más de 166.000 equipos estaban infectados por Rarog. Los analistas descubrieron esta muestra cuando se percataron de que la plataforma Magento estaba siendo atacada por una gran variedad de malware, distribuido por

AZORult, un tipo de código dañino diseñado para robar datos privados y credenciales de aquellos sistemas a los que conseguía acceso.

Además, hasta la fecha se conocen alrededor de 2500 variantes únicas de Rarog, las cuales conectan a 161 servidores de mando y control (C&C) diferentes.

Figura 12. Mapa de infecciones de Rarog

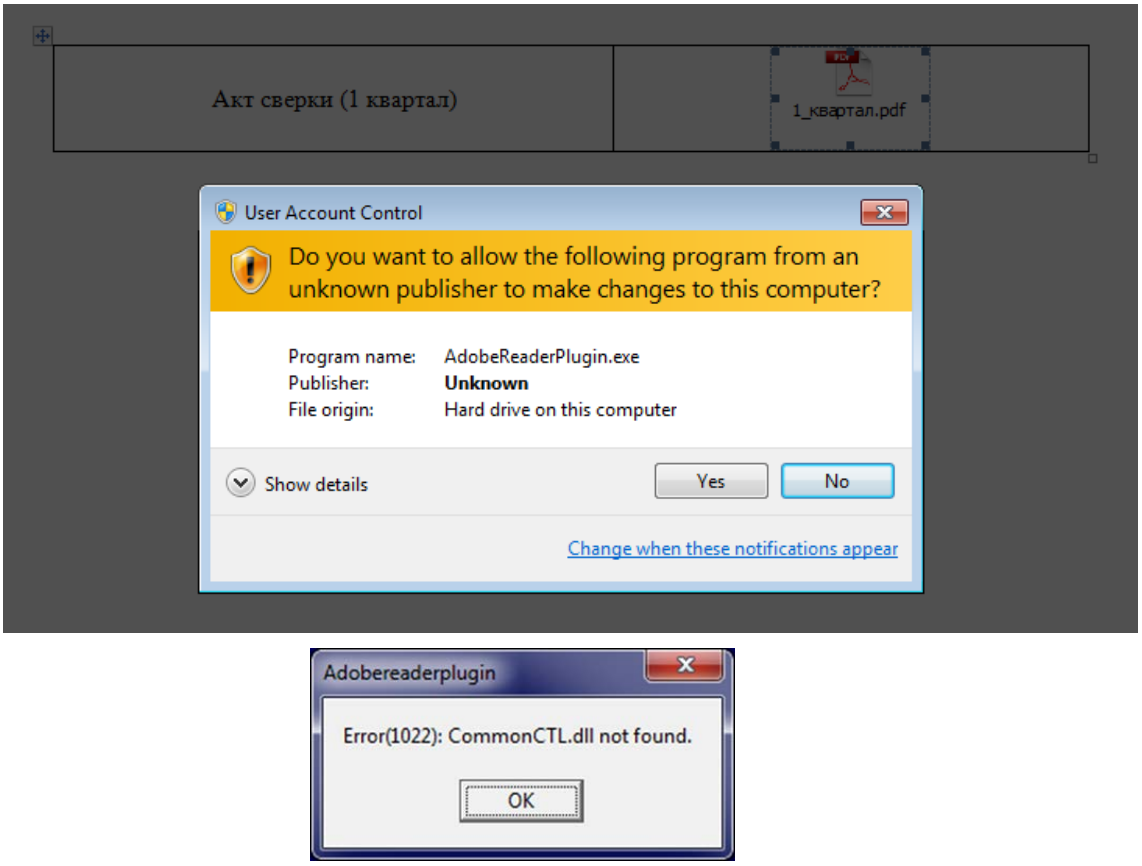
7.2.5 RAKHNI

Se trata de una familia de troyanos que tiene 5 años de antigüedad (en 2013 Kaspersky descubre la primera muestra relacionada con esta familia). Desde entonces, los principales cambios han sido:

- La forma en la que se comunican el C&C con el sistema infectado para el intercambio de claves.
- Los algoritmos usados y las librerías que se usan para procesos de cifrado.
- El método de distribución.

El método de distribución empleado, en líneas generales, ha sido el uso de campañas de spam masivas, como ocurre con la mayoría del malware.

La infección se produce cuando el usuario trata de abrir un documento embebido en el correo, creyéndose que se trata de un fichero ofimático legítimo (PDF) cuando en realidad se está ejecutando una aplicación de manera oculta. En concreto, un downloader que se encargará de mostrar un mensaje de error falso (para no levantar sospechas sobre por qué no se abrió el PDF), así como de realizar la descarga del código dañino tras una serie de comprobaciones en el sistema que se detallan posteriormente.



Figuras 13 y 14. "PDF" embebido y mensaje de error.

Sin embargo, lo más interesante de las nuevas variantes es que deciden por sí solas si en los equipos infectados se desea desplegar ransomware o un cryptominer.

El proceso de infección es el siguiente:

- Se comprueba la existencia de algunas de las siguientes cadenas: *\TEMP, \TMP, \STARTUP o \CONTENT.IE*
- Se comprueban algunas entradas en el Registro de Windows. En el caso de no existir, las crea.
- Se verifica que, de una larga lista de procesos, al menos 26 en concreto se estén ejecutando.

Todo esto se realiza para verificar que no se está ejecutando en una máquina virtual. Si se detecta que se trata de una máquina real, procede a instalar falsos certificados. Con estos certificados (aparecen entregados por Microsoft y Adobe Systems) se firmará todo el malware para que no existan problemas a la hora de su ejecución.

Acto seguido, comprueba si existe la carpeta "%AppData%/Bitcoin". Si existe, se instalará en el equipo un minador de bitcoins, si no, se procederá a instalar un ransomware. Finalmente, intenta propagarse a otros sistemas a través de un gusano. Para más detalles, se recomienda visitar https://securelist.com/to-crypt-or-to-mine-that-is-the-question/86307/

8. TENDENCIA

Según diversas fuentes, los cryptominers podrían llegar a extenderse más que el Ransomware, la mayor ciberamenaza de los últimos años.

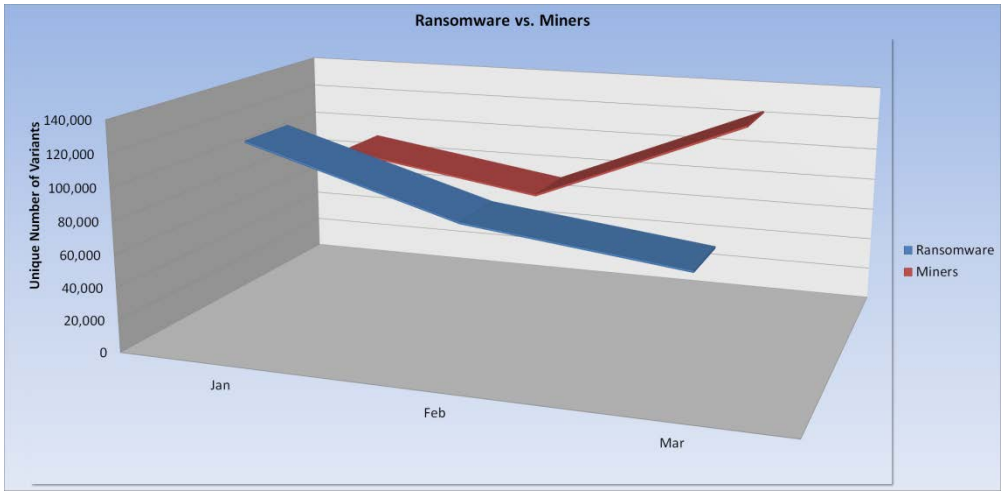


Figura 15. Tendencias de crecimiento de cryptominers y ransomware.

Esto se debe a que los ciberdelincuentes han visto en los cryptominers una vía para ganar dinero de forma más silenciosa, al contrario que el ransomware el cual suele ser bastante ruidoso (ventanas emergentes pidiendo un rescate, cifrado de ficheros…). Esto les permite pasar más desapercibidos y que sus campañas puedan durar más. A esto se le suma la facilidad de desarrollo en comparación con otro tipo de malware, pues existen incluso productos comerciales a la venta preparados para ser usados.

De hecho, fuentes como Quick Heal revelaron que entre enero y mayo de 2018 se detectaron 3 millones de ataques relacionados con cryptojacking. La tendencia es que, al igual que pasó con el ransomware, los cryptominers se vuelvan cada vez más sofisticados y que cada vez afecten a más plataformas. En relación a esto último, la misma fuente hizo público que se ha producido un incremento del 25% en variantes de cryptominers que afectan a dispositivos móviles.

Aunque a día de hoy la mayoría de los ataques se producen contra objetivos concretos (servidores con gran capacidad computacional) y de forma masiva (cualquier equipo, sin discriminación alguna) puede sospecharse que este tipo de ataques se podrían destinar en un futuro contra servicios en la nube donde su alcance es mayor, el posible desarrollo de CaaS (Cryptominer as a Service, como ocurrió con el ransomware) o contra personas/granjas que se dedican exclusivamente al minado.

9. CONCLUSIÓN

Si bien es cierto que la amenaza que suponen los minadores web es muy reducida en la mayoría de los casos (pues no existe infección de la máquina), hay que tener presente que el elevado uso de recursos que estos necesitan para funcionar puede afectar seriamente al rendimiento de la máquina.

Por otro lado, es necesario recordar que existen otros tipos de cryptominers que suelen venir acompañados de otro tipo de malware que los distribuye, como si de un caballo de Troya se tratara. Por lo tanto, es recomendable que, si se detecta la presencia de cryptominers ilegítimos en los sistemas, se realice una búsqueda más amplia de otro tipo de código dañino, pues suelen ir acompañados. Estos últimos (troyanos, botnets,…) pueden ser, potencialmente, mucho más perjudiciales para el sistema que el propio cryptominer. Además, la potencial entrada de ciberdelincuentes en una organización puede repercutir seriamente en la seguridad empresarial, pues se podrían producir robo de datos, credenciales…

Es por ello por lo que, además de este documento, será necesario consultar el resto de los informes disponibles sobre malware en general para poder prevenir y defender el equipo del máximo abanico de amenazas posibles.

10. REFERENCIAS

To crypt, or to mine – that is the question - Securelist
Rarog Trojan 'Easy Entry' For New Cryptomining Crooks, Report Warns | The first stop for security news | Threatpost
Adylkuzz Cryptocurrency Mining Malware Spreading for Weeks Via EternalBlue/DoublePulsar | Proofpoint Adylkuzz Crypto-Miner Removal Report
Informe_Evolución_Trickbot.pdf
The State of Cryptojacking
3 Million cryptojacking hits detected in 2018 so far: Research
The state of malicious cryptomining _ Malwarebytes