Panda Adaptive Defense 360

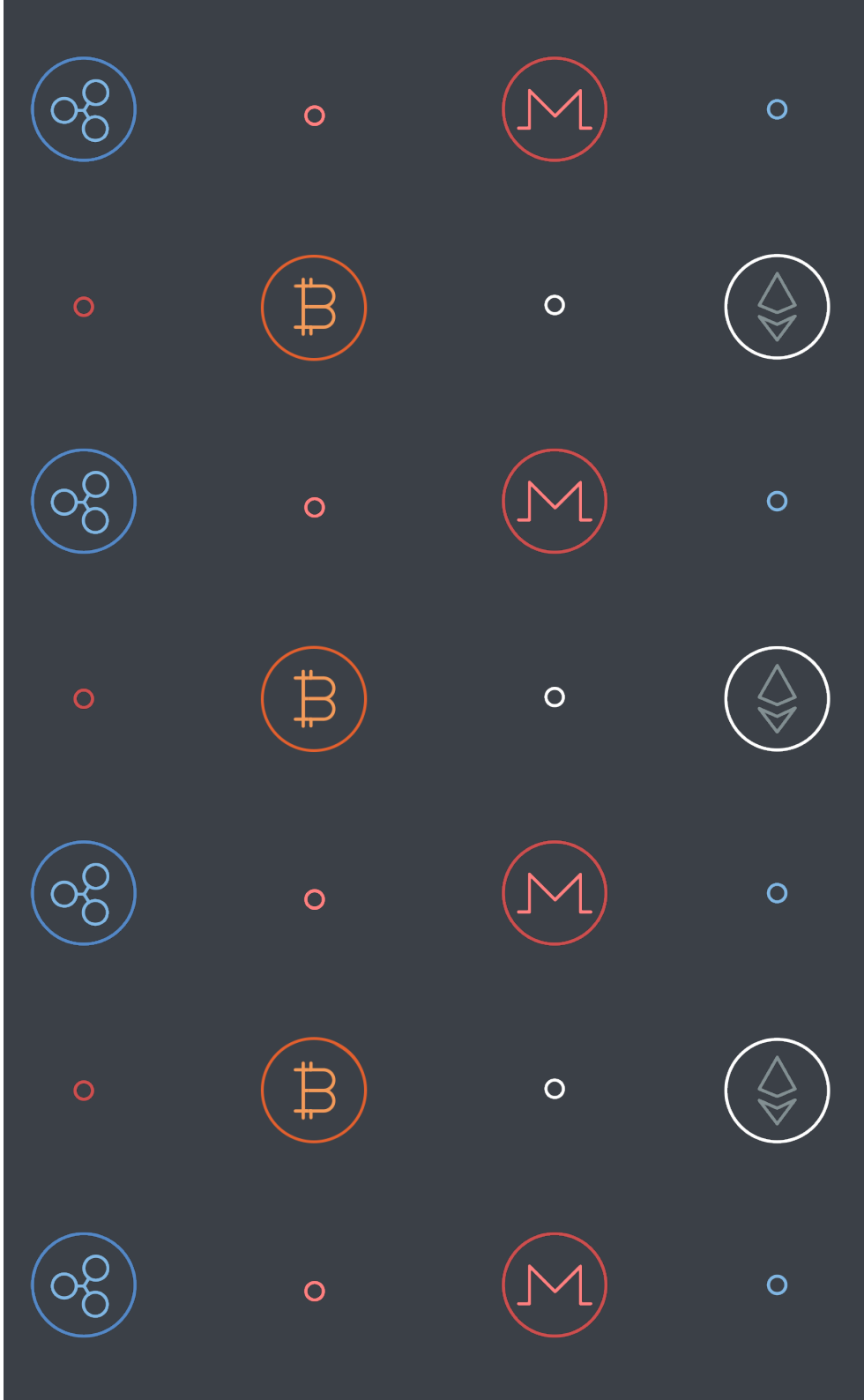
Visibilidad Total, Control Absoluto

CRYPTOJACKING UN COSTE OCULTO

panda

pandasecurity.com/business/adaptive-defense/

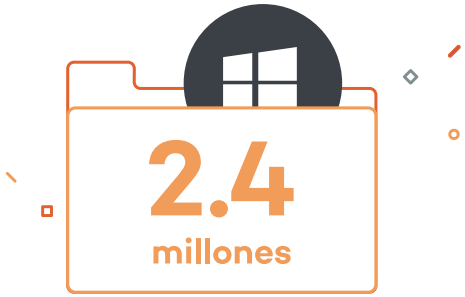
Índice de Contenidos.



panda

1. Un coste oculto

El ***Cryptojacking*** es el concepto que marca este 2018 en ciberseguridad, y que se ha convertido en la principal amenaza para la seguridad y el rendimiento de los dispositivos electrónicos durante la primera mitad del año. Una práctica en auge entre los *black hat*, con **2,4 millones de casos registrados en Windows** en lo que llevamos de año.

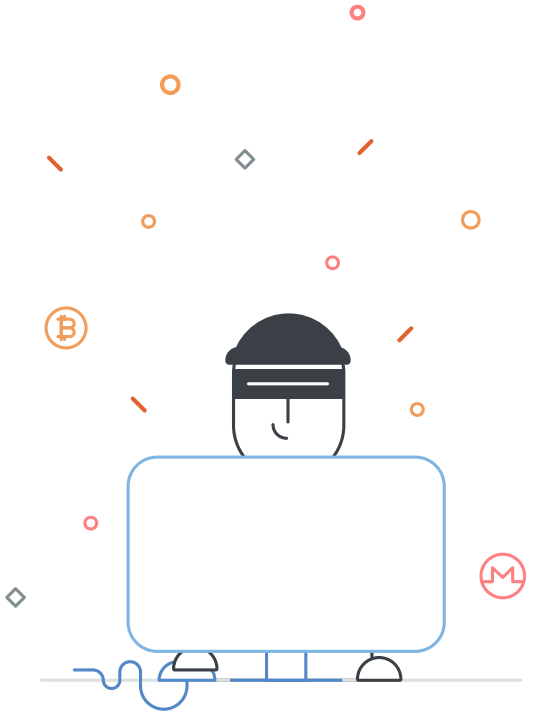


Desde **PandaLabs**, el laboratorio anti-malware de Panda Security, así lo determinan: aunque los tipos de malware "tradicionales" como troyanos o gusanos siguen siendo muy utilizados por los atacantes, las nuevas técnicas de ataque – como los fileless o ataques sin malware, y los cryptominers- muestran las tasas de crecimiento más rápidas.

Tanto es así que **Bitcoin**, la moneda digital más usada en todo el mundo, fue incluida entre las candidatas a palabra del año 2017 de la Fundéu BBVA, lo que es un buen ejemplo de la repercusión que tienen las divisas virtuales en estos momentos.

Y es **en esta esta continua evolución de la ciberdelincuencia**, en la que los ciberdelincuentes se las idean con nuevas tácticas para inflar sus bolsillos, donde estas organizaciones criminales han encontrado un nuevo filón: **la minería de criptomonedas.**

Pero para entender cómo y por qué "los malos" quieren minar criptomonedas a nuestra costa, vamos a explicar el proceso completo...



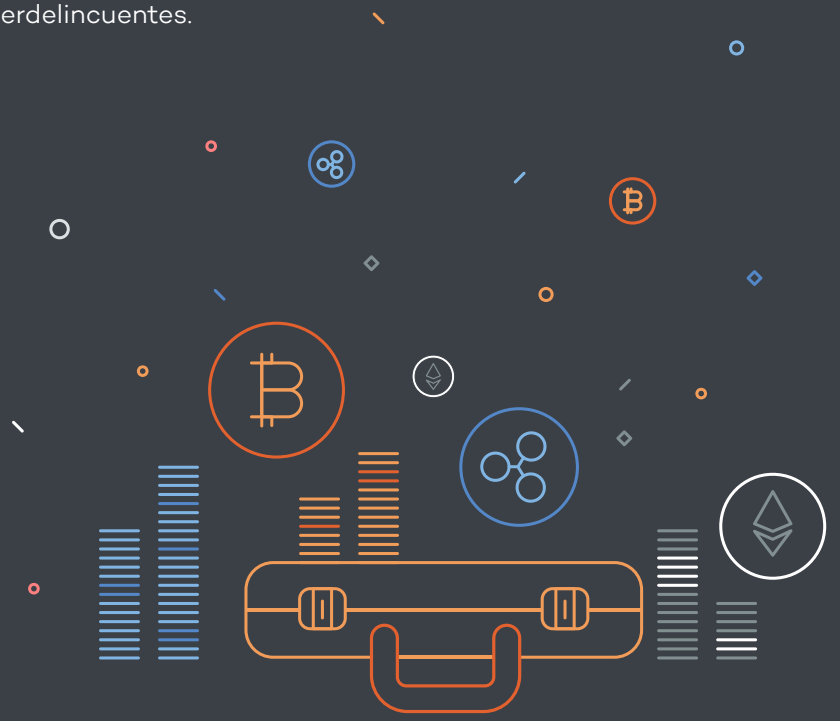
2. ¿Qué son las criptomonedas?

La aparición de las primeras criptomonedas está asociada a la necesidad de crear transacciones anónimas. En 2009 se creó la primera de ellas: el bitcoin. **Actualmente existen más de 1.300 criptomonedas diferentes**, con orígenes y características diversas, pero todas coinciden en su naturaleza digital y en la **intención de asegurar el anonimato de las transacciones.**

Actualmente, la legalidad del uso de criptomonedas es un tema candente, ya que existen países donde se discute su prohibición, mientras en otros el valor de estas divisas permanece en un limbo alegal.

Al fin y al cabo, un arma de doble filo: una moneda digital y que asegura la transparencia y sencillez en la transacción parece la herramienta idónea para pagar los servicios ilegales de un hacker. También lo es para los cibercriminales: actualmente, la práctica totalidad de los ataques de ransomware solicitan el rescate de los datos en bitcoins u otra criptomoneda, por su naturaleza irrastreable.

La subida en la cotización de las criptomonedas como **Bitcoin**, **Ethereum** o **Ripple**, ha hecho que se hayan convertido en uno de los principales ingresos para muchos grupos de bandas organizadas de ciberdelincuentes.



3. Blockchain, la razón de ser de las criptomonedas

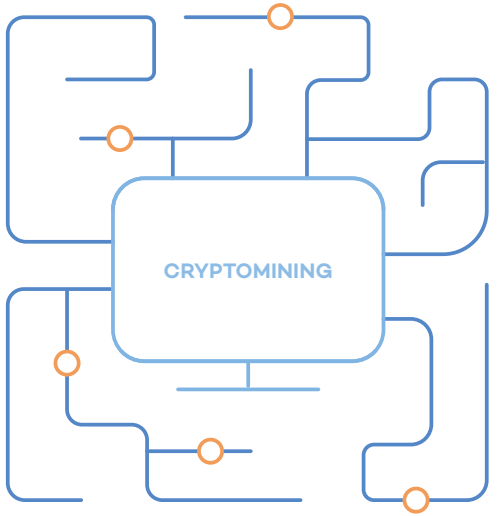
Una de las cuestiones que más dudas provoca sobre las criptomonedas es la posibilidad que tienen de "minarlas", lo que se conoce como minería de criptomonedas. **Muchas de estas divisas digitales pueden ser obtenidas resolviendo operaciones matemáticas**, como si de cualquier otro tipo de computación se tratase.

No obstante, minar en busca de criptomonedas es una tarea cada vez más compleja y que consume más recursos, tanto energéticos como computacionales. Y esto se debe en gran parte a la tecnología basada en blockchain.

Podemos definir al **Blockchain como la piedra angular de la inviolabilidad de las criptomonedas, así como de su naturaleza anónima**. El blockchain nació a para sustentar el bitcoin. La minería de criptomonedas es indispensable para que el sistema funcione: es la actividad computacional necesaria para procesar las transacciones que se realizan en las cadenas de bloques ya existentes. Sirve para emitir nuevos criptoactivos y confirmar las transacciones en la red de blockchain. Es decir, para crear más criptodivisas hay que minarlas. **Sin el minado, el sistema se desmorona.**

Esta tecnología consiste en una base de datos distribuida, y formada por cadenas de bloques **diseñadas para evitar su modificación** una vez que un dato ha sido publicado. Para ello se usa un sellado de tiempo confiable, también conocido como *trusted timestamping*, enlazándolo a un bloque anterior.

No es de extrañar que, para que todo este proceso arranque, haga falta una energía computacional inasumible hasta para la más gran empresa tecnológica. Y es en este contexto donde los hackers han encontrado la forma de hacerlo más fácil: entrando en ordenadores ajenos y haciendo que sean esos los equipos que rastreen la Red, consumiendo sus propios recursos, para minar criptomonedas.



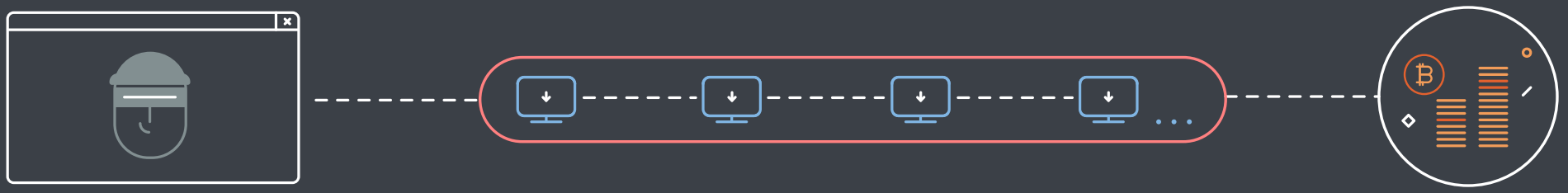
4. Trabajando para el enemigo

El cryptojacking consiste en el uso no autorizado de los dispositivos de un usuario para minar criptomonedas. Básicamente, los atacantes hacen uso del malware para secuestrar esos ordenadores, tablets o smartphones, por ejemplo, y aprovechan parte de su poder de procesamiento para minar criptomonedas de manera encubierta. **Y así es como acabas trabajado para el enemigo, utilizando tus recursos energéticos sin darte cuenta.**

Cómo... El usuario probablemente note un ralentizamiento de sus dispositivos, pero no es consciente de que se debe a un ataque destinado a minar criptomonedas. Una de las técnicas más comunes consiste en **apropiarse de la CPU o GPU de la víctima desde una página web infectada con malware para minar criptomonedas**, como ha ocurrido recientemente con YouTube.

Otra técnica de ataque consiste en **utilizar la funcionalidad de vídeo online de Microsoft Word**, que permite insertar vídeos en documentos sin necesidad de embeberlos o enlazarlos. En este caso, los atacantes aprovechaban esta característica de Word para insertar los scripts maliciosos y sustraer de manera oculta la capacidad de la CPU de la víctima.

¿Por qué? Las criptodivisas se han convertido en el oro del siglo XXI. Por eso, este año estamos viendo cómo aumentan los ataques para minar criptomonedas. Ahora que los equipos de IT y las fuerzas de seguridad estatales tienen el ojo puesto en los ataques de *ransomware*, los cibercriminales optan por métodos más seguros para lucrarse y han encontrado un filón en el robo de recursos informáticos para el minado. **Cuanto más poder de computación roban, más rápido es el minado**. Esto está dando lugar a peleas entre diferentes atacantes por lograr el mayor control de la CPU posible.



Josu Franco, Asesor en Tecnología y Estrategia en Panda Security, afirma que el auge del minado reside en que "es una vía fácil de hacer dinero, y hacerlo es muy barato. Se pueden comprar kits de cryptojacking en la "dark web" por unos $30. El atacante puede instalarlo por ejemplo en 100 máquinas, y todas le darán dinero con las criptomonedas generadas, y de forma continua y con poco riesgo. Además, vemos un incremento importante de páginas legítimas infectadas con Coinhive, un javascript que hace que ni siquiera sea necesario instalar el software de minado, sino que funciona mientras el usuario tenga una sesión activa en esa página. Sin embargo, con el ransomware, conseguirá que quizás unas pocas víctimas le paguen, una sola vez."

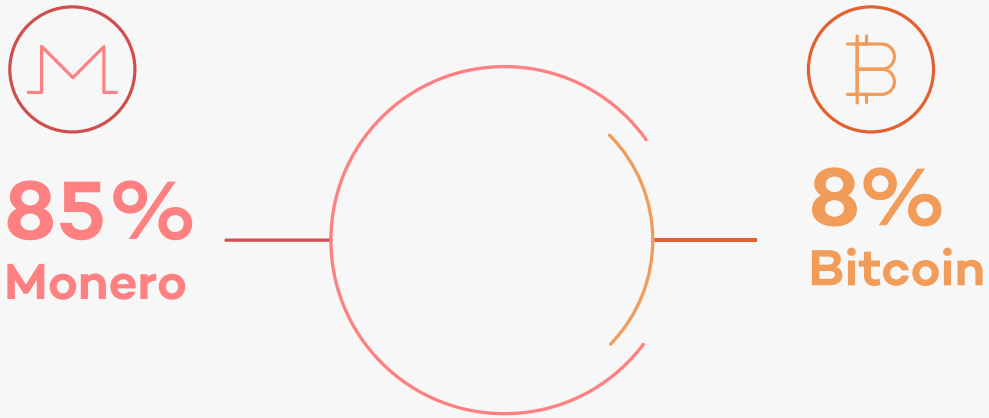
Al igual que pasa con ransomware, **las empresas son hoy el objetivo prioritario de los atacantes en 2018**, ya que si consiguen introducirse en la red corporativa tienen a su disposición una cantidad ingente de recursos informáticos.

Expertos en ciberseguridad aseguran que **los criminales se están pasando del *ransomware* a la minería porque es mucho menos intrusivo y no necesitas utilizar tantos recursos para evitar ser detectado.** Con el *ransomware* no sabes si la víctima pagará el rescate porque podría tener una copia de seguridad de sus archivos. En cambio, con la minería de criptomonedas es seguro que recuperarás el dinero invertido, y es mucho menos invasivo. Se puede ejecutar la minería en cualquier tipo de dispositivo, no está restringido a Windows, Mac o Linux como el *ransomware*, y el sistema de la víctima seguirá funcionando a pesar del ataque.

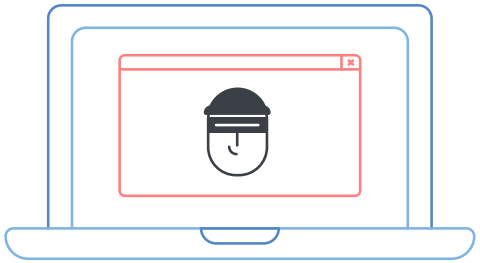
5. ¿Qué criptomonedas buscan los cibercriminales?

La criptomoneda más conocida – y la más 'antigua' - es bitcoin. Sin embargo, hoy en día la minería de esta criptomoneda es casi imposible para los aficionados, ya que requiere tanta energía, junto con procesadores especializados, que sólo es factible para empresas especializadas en su creación. Tanto es así que en los últimos años, Islandia ha visto un auge de empresas dedicadas a la minería de bitcoin, atraídas por el energía barata del país, y también por su clima frío, que elimina la necesidad de gastar más en sistemas para enfriar los procesadores. De hecho, según Johann Snorri Sigurbergsson, que trabaja en el sector energético del país, el consumo de energía de bitcoin podría superar el consumo energético doméstico.

Si los cibercriminales no pueden generar fácilmente bitcoins con el cryptojacking, ¿qué buscan? La respuesta es Monero, una criptomoneda creada en 2014. Esta divisa es idónea para la minería ilícita, ya que no requiere equipos especiales, generarla no requiere tanta potencia computacional, y además, tiene una privacidad aumentada en comparación con otras criptomonedas. De hecho, **el 85% de los ataques de cryptojacking buscan Monero, mientras sólo el 8% buscan bitcoin.**



6. La puerta de entrada en tu equipo



Como muchas de las ciberamenazas que vemos hoy en día, el cryptojacking tiene **múltiples vectores de ataque** para llegar a los equipos y sistemas informáticos, y así empezar a aprovechar la potencia computacional de los ordenadores afectados.

Sitios web infiltrados

Una de las maneras más comunes para aprovecharse del CPU de un usuario son las webs que, sin avisar, recurren a su conexión a internet para el minado, siendo un engaño para las personas **que ponen involuntariamente su equipo al servicio de un tercero.**

El origen de esta técnica está en una empresa llamada **CoinHive**, que en septiembre de 2017 lanzó su servicio como una alternativa legítima a los anuncios en los sitios web. Sin embargo, los ciberdelincuentes no tardaron en aprovecharse del código de este servicio para fines maliciosos.

La técnica implicaba ganar acceso a webs, inyectar el código de CoinHive, y extraer las criptomonedas generadas con el **CPU** de los visitantes de estas webs.

Precisamente, CoinHive es el script más utilizado para desarrollar estos ataques. Un estudio del investigador de seguridad Troy Mursch ha detectado **50.000 sitios web infectados con scripts de *cryptojacking***, con un 80% de ellos recurriendo a CoinHive. Se estima que en total, los códigos como CoinHive generan alrededor de 250.000$ cada mes.

Algo que facilitó mucho la tarea a los hackers era el hecho de que, al principio, CoinHive no requería el permiso de los usuarios de las webs. Esto quería decir que fue posible ejecutar el ataque sin que el visitante se diera cuenta.

Aunque la empresa ahora pide permiso a los usuarios, los ciberdelincuentes pudieron copiar y editar el código para sus propios fines.

Y esto no es algo marginal: entre los sitios web afectados se encuentran los de organizaciones tan conocidas como ***The LA Times***, e instituciones públicas como el gobierno de Australia. De hecho, para los atacantes, **cuanto más importante es la web, mejor**, ya que una mayor cantidad de visitantes significa más CPU y, por lo tanto, más criptomonedas.

Esto fue el caso de YouTube, el segundo sitio web más visitado del mundo. En este caso, la plataforma de anuncios **DoubleClick** fue la víctima de un ataque que ocultaba en el código de los anuncios de YouTube el script de *cryptojacking*, CoinHive.

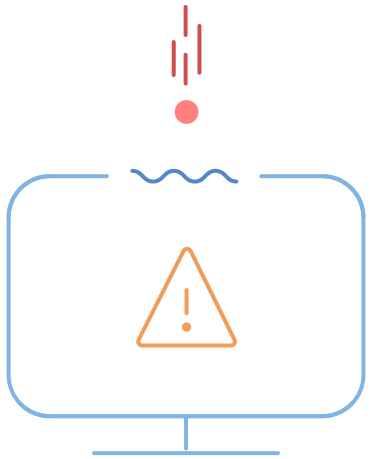
¿Cómo consigue este tipo de código llegar a aparecer en estos sitios web? Muchas veces consigue entrar utilizando una vulnerabilidad en los sistemas de gestión de contenidos utilizados para crear estos sites. Una de las vulnerabilidades más populares para este tipo de ataque es una en Drupal, que ha sido aprovechada en cientos de ocasiones.

Un caso particularmente interesante es el uso de una **vulnerabilidad en Apache Struts** – una herramienta web que ya ha causado bastantes problemas. Se trata de un malware que, una vez dentro de la web, busca otros malware de minería de criptomonedas y, si los hay en el sistema, los desactiva para poder aprovechar al máximo el CPU del usuario.

Vulnerabilidades

Una de las puertas de entrada más comunes para el cryptojacking son las vulnerabilidades. Ya hemos visto algunos casos de sitios web vulnerables, pero los atacantes también se aprovechan de **vulnerabilidades en sistemas operativos para introducir el malware en el endpoint.**

Una de las vulnerabilidades que más problemas ha causado en el último año es en el Server Message Block (SMB) de Microsoft y se llama **EternalBlue**. El uso más infame de EternalBlue fue el ataque global de ransomware, WannaCry. Sin embargo, unos meses después de este ataque, PandaLabs descubrió otra explotación de esta vulnerabilidad: el malware fileless, WannaMine, que se utilizaba para minar Monero. Esta vulnerabilidad también fue la puerta de entrada para Adylkuzz. Este malware, como WannaMine, se utilizó para generar Monero, e infectó a miles de ordenadores en todo el mundo. De hecho, se cree que podría haber afectado a incluso más gente que WannaCry.



Phising

Más del 90% del malware en el mundo llega a través del email. Por lo tanto, no es de sorprender que el malware de cryptojacking no es una excepción.

Una técnica popular es el uso de documentos que, al parecer, son legítimos. Un ejemplo es el **uso de documentos Word**. Aquí, el atacante mete el código de cryptojacking dentro de un vídeo incluido en el documento que se adjunta a un email y, una vez abierto, ejecuta el script de cryptojacking.

Otro malware particularmente peligroso se llama **WinstarNssmMiner**. Éste también llega a través de emails de phishing o sitios web infiltrados. Una vez dentro del sistema, usa toda la potencia del ordenador para minar criptomonedas. Si llega a ser descubierto o si alguien intenta quitarlo del sistema, hace que el ordenador que lo contiene falle.

Internet of Things (IoT)

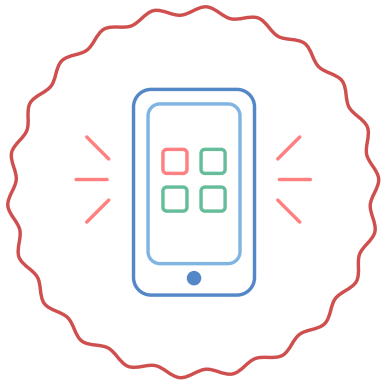
La difusión de los dispositivos móviles con conexión a Internet es algo muy extendido, y el uso de las apps se ha convertido en habitual. Por lo tanto, puede que no sea de extrañar que los black hat hayan llegado a **aprovecharse de las aplicaciones de estos dispositivos para ampliar su actividad criminal.**

Uno de los primeros casos que se vio en este campo del IoT fue HiddenMiner, un malware que llegaba a los dispositivos móviles a través de aplicaciones descargados de tiendas de apps de terceros – es decir, no oficiales. Una de las cosas que lo hace tan peligroso es que, en las versiones más antiguas de Android, es casi imposible de desinstalar. Es más, una vez dentro de un dispositivo, utiliza todos los recursos de éste, **sobrecalentando el dispositivo o haciendo incluso que falle.**

De hecho, se han visto casos en los que **usaba tanta energía que casi causa que el dispositivo infectado – en este caso, un Smartphone- explote.**

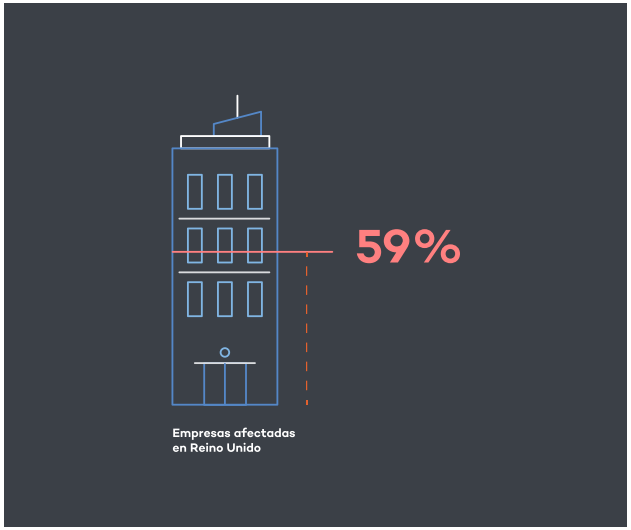
Pero no sólo son las aplicaciones descargadas de fuentes desconocidas las que pueden causar problemas. A principios de este año, se descubrió que **varias apps disponibles en Google Play Store** contenían malware de cryptojacking. Entre las aplicaciones había una app de VPN, juegos e incluso una app que decía donar las criptomonedas minadas a una organización benéfica.

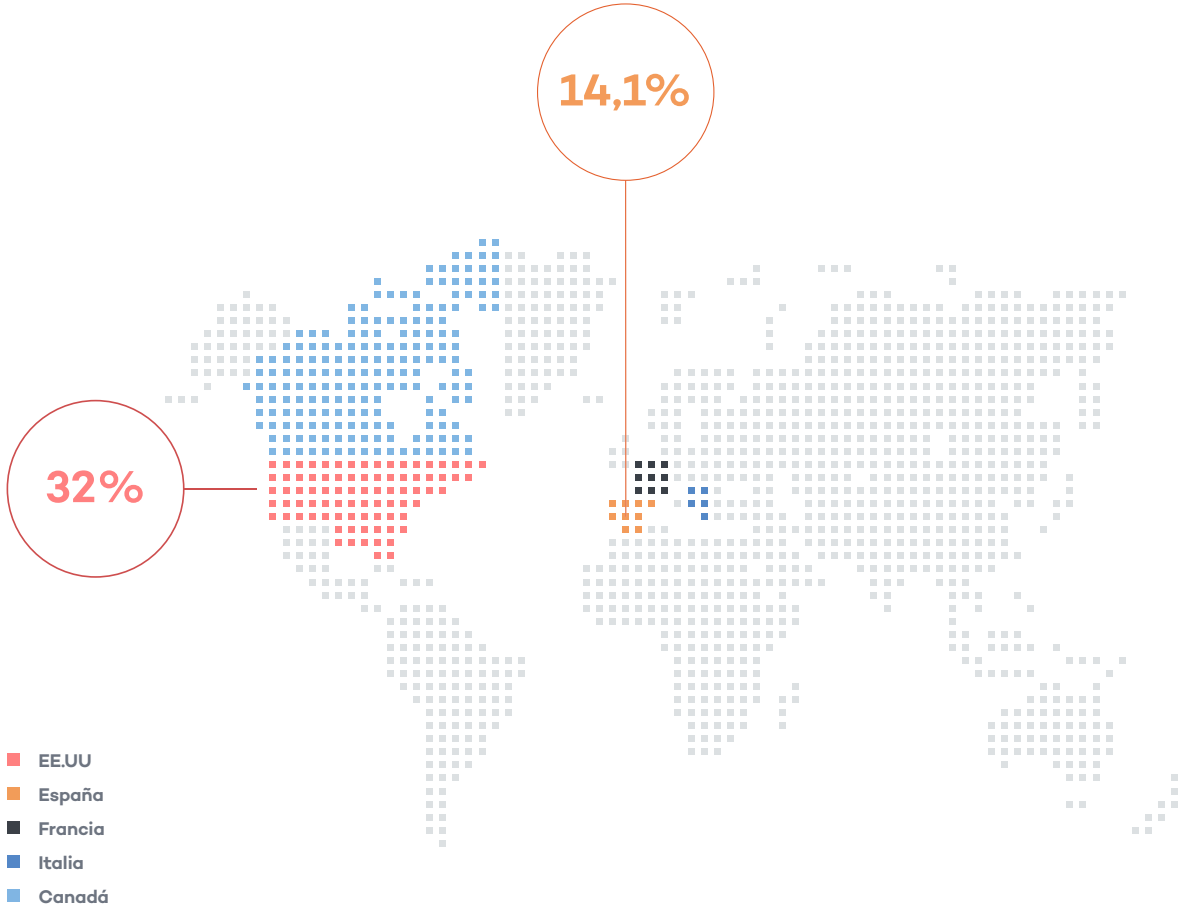
Otros dispositivos móviles, como cámaras de seguridad, **tampoco han escapado a estos ataques de cryptojacking.** Estos dispositivos son especialmente susceptibles a ser atacados debido a que no tienen, a priori, una protección tan rigurosa como otros equipos.



Geografía del Cryptojacker

El cryptojacking es un fenómeno mundial, afectando a casi todos los países del mundo. Hasta un 59% de las empresas en Reino Unido se han visto afectados por un ataque de este tipo en algún momento. Pero los países más afectados son Estados Unidos (32% de los casos) y España (14,1% de los casos), seguidos de Francia, Italia, y Canadá.



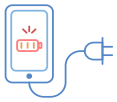


Mediacenter Panda Security: "Del año del ransomware al año del cryptojacking"

Informe Malwarebytes "A look into the global 'drive-by cryptocurrency mining' phenomenon" - Octubre 2017

7. ¿Qué efectos puede tener?

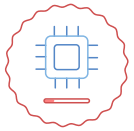
Aunque pueda parecer que es un tipo de malware relativamente inocuo, sobre todo porque algunos tipos se diseñan específicamente para evitar la detección y para usar una cantidad limitada del CPU, realmente no deja de ser como todos los malware: una amenaza **seria para la seguridad informática.**



Alta demanda de energía. Una de las primeras indicaciones de una infección con un malware de cryptojacking es un aumento significativo en el consumo de energía. Según estiman algunas fuentes, la minería de Monero utiliza alrededor de **332 millones de kWh al año**, una cantidad comparable con un país pequeño. Es una de las razones por la que los cibercriminales buscan ordenadores ajenos para minarla, para eludir sus costes.

Su profesionalización es tal que se han ideado ciertos tipos de malware de cryptojacking que contienen códigos para desactivar los modos de hibernación para seguir minando, causando un consumo incluso más elevado de energía, ya que los **equipos afectados estarán minando criptomonedas sin parar 24/7.**

Si un malware de cryptojacking ha llegado a tu empresa, acabarás notando más pronto que tarde el tremendo aumento de la factura energética, ya que el cryptojacking exprimirá cada equipo y recurrirá a él siempre que pueda.



Uso del CPU. El objetivo del cryptojacking es utilizar el CPU de los ordenadores afectados para minar las criptomonedas, así que un aumento en el consumo de éste es de esperar. Si numerosos trabajadores informan del rendimiento lento o el sobrecalentamiento de sus ordenadores, podría ser el caso que haya un caso de cryptojacking en la empresa.

Daños físicos. El uso excesivo del CPU no sólo causa que los equipos de tu empresa se ralenticen; un uso excesivo puede causar la **destrucción de los dispositivos corporativos.** Si el minado se realiza durante un período prolongado, la temperatura de estos y de sus baterías podría alcanzar niveles extremos que acabe con los dispositivos.

Peligros para la ciberseguridad empresarial. Si un malware de cryptojacking ha conseguido llegar a la red informática de tu empresa, quiere decir que **hay alguna puerta abierta**. Y esta puerta abierta quiere decir que hay alguna manera para que entren todo tipo de amenazas – amenazas que pueden poner en peligro tu empresa.

Cambio de estrategia. Hemos visto casos de malware de cryptojacking que antes se usaban como **ransomware**. Podría darse el caso que, viendo que el cryptojacking no es tan rentable como le gustaría, el cibercriminal recurra a un ataque más directo para ganar dinero. Incluso hay un malware que **incluye los dos ataques**, y decide si desplegar el ransomware o el cryptojacking según las características del ordenador.

Un ataque de ransomware no es la única consecuencia secundaria que puede causar un intruso que ha conseguido entrar en la red con un malware de cryptojacking. Una vez dentro del sistema, **el atacante puede tener acceso a todo el contenido del ordenador**, y eso incluye los datos de la empresa. Una manera muy popular entre los cibercriminales para ganar dinero es el robo y venta de datos – ya sean datos personales de clientes, números de tarjetas de crédito, o secretos industriales.

Incluso puede darse el caso de que, una vez que un cibercriminal tenga acceso al sistema informático para el ataque de cryptojacking, **gana más dinero "alquilando" el acceso a otros cibercriminales** para que se aprovechen del sistema de la manera que quieran.

8. ¿Cómo protejo a mi empresa de los cryptojackers?

Los expertos en ciberseguridad de PandaLabs aseguran que la protección sigue siendo la misma que para otro tipo de malware, porque el minado de criptomonedas se realiza con un código malicioso que se ejecuta en tu ordenador. Por tanto, dos consejos básicos son: contar con una solución de ciberseguridad avanzada, como Panda Adaptive Defense 360, y no clicar o descargar archivos desconocidos.

Además, para protegerse de una manera eficaz ante un posible ataque de minado de criptomonedas conviene seguir estas medidas de seguridad:

Realizar evaluaciones periódicas de riesgos para identificar vulnerabilidades. Panda Pacth Management busca automáticamente los parches necesarios para mantener a salvo los equipos de tu sistema, priorizando las actualizaciones más urgentes. Establecer las políticas adecuadas de parcheo permite reducir la superficie de ataque por vulnerabilidades hasta en un 80% según datos del analista Gartner.

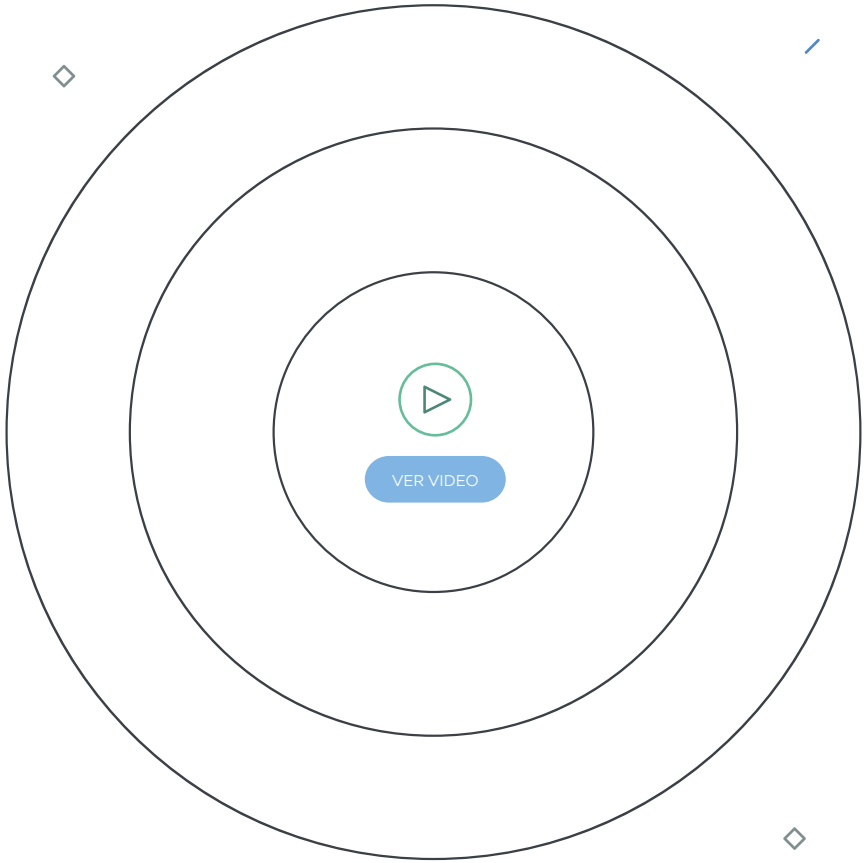
Analizar los recursos. Todos los sistemas operativos tienen alguna herramienta similar al Monitor del Sistema, que analiza los recursos que están siendo consumidos por los equipos de tu empresa en cada momento. Ten esto controlado para asegurarte de que no hay ninguna actividad inusual.

Cuidado con el navegador. Si sospechas que el cryptojacking está llegando a través de páginas webs, instala plugins que los bloqueen en el navegador.

Investigar a fondo picos de un determinado problema informático relacionado con un funcionamiento anormal de las CPU. Si numerosos trabajadores informan del rendimiento lento o el sobrecalentamiento de sus ordenadores, podría estar dándose un caso de cryptojacking.

Actualizar con regularidad todos los sistemas y dispositivos de la empresa, valorando la desinstalación de software que no se esté utilizando.

Crear un entorno de navegación seguro en la empresa: activar el control de acceso a páginas web disponible en soluciones de ciberseguridad avanzada y denegar las URLs de la categoría Minería de Criptomonedas es la mejor manera de proteger tu endpoint y los recursos de tu empresa.



Panda Adaptive Defense 360

Visibilidad Total, Control Absoluto

Estas acciones deben complementarse con la implementación de una solución de ciberseguridad avanzada que aporte características clave como una visibilidad detallada de la actividad en todos los endpoints y permita controlar todos los procesos en ejecución. Este es el caso de **Panda Adaptive Defense 360**, la suite de seguridad de Panda Security, que está preparada para proteger todos los equipos de tu empresa ante todo tipo de ciberamenazas, clásicas o 'de última generación'.

Sigue estos consejos e impide que el Cryptojacking mine la reputación de tu empresa y ponga en riesgo la continuidad de tu negocio.

Panda Adaptive Defense 360

Visibilidad Total, Control Absoluto

Más información en:

pandasecurity.com/business/adaptive-defense/

Hablemos:

900 90 70 80

panda