Enero 2018 Número 15

Coinminer Malware

RUBYMINER

Se ha descubierto una campaña de *malware* que **explota varias vulnerabilidades antiguas en servidores Linux y Windows**, **que permiten la ejecución remota de código y se están utilizando para descargar un troyano denominado 'RubyMiner'**, el cual se ocupa de minar la criptomoneda **Monero** (XMR). El 30% de las redes de todo el mundo se han visto comprometidas por esta amenaza.

Los atacantes se han ayudado de estas vulnerabilidades para tomar el control de los servidores web e instalar el programa malicioso. Este malware es una versión modificada de **XMRig**, también conocido por sus capacidades para la minería de la criptomoneda Monero (XMR). Los ciberdelincuentes lo han modificado para que todas las ganancias se envíen a su monedero, ya que la versión original dona el 5% de las ganancias al autor del malware.

APT

DARK CARACAL

Se ha descubierto una **campaña de ciberespionaje masiva** que ha supuesto el robo de información confidencial de **periodistas, militares y ejecutivos de empresas de al menos 21 países distintos**.

El grupo APT (Advanced Persistent Threat) relacionado con esta campaña se denomina **Dark Caracal** y según diferentes investigaciones, puede estar vinculado al Gobierno del Líbano, ya que han sido ubicados en un edificio propiedad del Directorio de Seguridad Libanés.

Dark Caracal, cuyo nombre se inspira en un mamífero de la zona que puede permanecer oculto durante mucho tiempo, utiliza un *malware* que **permite activar las cámaras y el micrófono de smartphones para grabar o fotografiar aquello que se encuentre dentro de su perímetro de grabación.** La campaña de ciberespionaje afecta fundamentalmente a miles de personas en más de 20 países donde **cientos de Gigabytes de información de sensible, han sido sustraídos**.

Dictation

Herramientas

Se trata de una herramienta muy eficiente para la escritura mediante el uso de la voz (micrófono) a través del navegador, dando unos resultados bastante exactos. Sólo hay que hablar claro y pronunciar de manera adecuada. Además se le pueden añadir signos de puntuación y hasta emoticonos solamente hablando al micrófono.

Existe una larga lista de comandos para interactuar con la aplicación, tanto en español como en múltiples idiomas que soporta la herramienta, aunque tiene como limitación que solo puede usarse en Chrome, dentro de su propio bloc de notas.

ÚLTIMAS TENDENCIAS

Los ataques de minería y Blockchain se disparan

A medida que **aumenta el precio de Ethereum y otras criptomonedas**, los ciberdelincuentes comienzan a crear *exploits* de Blockchain para invadir estos mercados digitales. Tienen como objetivo infectar las aplicaciones de monedero móvil y los intercambios en línea donde se almacenan criptomonedas, a través de **campañas de *phishing* especializadas** para penetrar en estos sistemas.

Por su parte, el *malware* de minería a menudo usa las herramientas preferidas por otros actores de amenazas, como el *exploit* **EternalBlue**, que se usó en el brote de *ransomware* de **WannaCry**. Estos programas de minería pueden ser muy difíciles de detectar porque a menudo se combinan con otras técnicas, como los métodos ***fileless***, para ocultar el rastro.

El gran incremento valor de las criptomonedas ha dado paso a una nueva ola de cibercrimen financiero. Estos exploits y esquemas de minería de Blockchain son cada vez más sofisticados y más efectivos a medida que los inversores acuden en masa para comprar criptomonedas.

FRAUDE

FRAUDE MASIVO EN SURTIDORES DE GASOLINA EN RUSIA

Las fuerzas de la ley rusas han detectado una **campaña de fraude masivo que afectaba a decenas de gasolineras**, donde los empleados mediante un programa malicioso (***malware***) falseaban la cantidad de gasolina repostada por los usuarios, donde se les cobraba un importe superior por menos litros de combustible. En la estafa masiva, **los empleados desviaron el coste entre un 3 y un 7 por ciento**. El Servicio Federal de Seguridad (SFS) de Rusia encontró los programas maliciosos a partir de una serie de clientes que se quejaron de haber perdido combustible sin que hubiese una razón técnica detrás (insinuando un robo).

OTRAS NOTICIAS DE INTERÉS

- Un bug en la popular cartera Electrum permite a cualquier sitio web robar todos tus bitcoins
- PyCryptoMiner. Una nueva Botnet de minería de criptomonedas se propaga a través del protocolo SSH
- Anonymous Italia hackeó la base de datos de las cámaras de velocidad y se hizo cargo de los sistemas policiales en la ciudad de Correggio
- El Cibercalifato podría actuar contra las infraestructuras críticas de Reino Unido
- Una visión general accesible de Meltdown y Spectre
- Samsung estaría fabricando chips para minar criptomonedas
- Los soldados estadounidenses han mapeado accidentalmente con FitBit los complejos militares
- Más de 500 millones de dólares robados a CoinCheck

Un ciberdelincuente compromete la red de un hospital

En la noche del 11 de enero, el Hospital de Hancock (Greenfield. Indiana) sufrió un sofisticado ciberataque que afectó a toda su red. El ciberdelincuente llegó a mostrar un mensaje dentro de sistema informático donde **exigía dinero en Bitcoin por el rescate**.

Durante una conversación con el CEO el Hospital, Steve Long, se confirmó el hackeo pero éste se abstuvo de proporcionar más información, incluido los daños sufridos o si el hospital llegó a pagar algún tipo de rescate (y la cuantía del mismo). A pesar de ello, Steve Long comunicó que no tenía constancia de que se hubiera producido algún tipo de robo de información médica de carácter personal.

El gasto en ciberseguridad en empresas incrementará un 8% este año

Según la encuesta de comportamiento de compra de seguridad 2016 de Gartner, **el 53 por ciento de las organizaciones mencionaron los riesgos de seguridad como el principal impulsor de los gastos de seguridad**. El mayor porcentaje de encuestados dijo que una brecha de seguridad es el principal riesgo de seguridad que influye en sus gastos de seguridad.

El gasto de las empresas en ciberseguridad alcanzará este año 2018 los 79.773 millones de euros debido a las nuevas regulaciones, el cambio de mentalidad del comprador, una nueva conciencia respecto a las amenazas emergentes y la evolución hacia estrategia de negocios.

La expansión del fraude del BEC (*Business Email Compromise*)

Los ataques de **Business Email Compromise (BEC)** se han expandido enormemente en los últimos años, con un crecimiento proyectado de más de **nueve mil millones de dólares en 2018**. La combinación de simplicidad y efectividad ha asegurado que BEC continuará siendo uno de los ataques más populares. Los ataques BEC se pueden llegar a reducir en dos técnicas principalmente:

- **Captura de credenciales** (combinación de ingeniería social y malware): incluye el uso de *keyloggers* y kits de *phishing* para robar credenciales y acceder al correo web de organizaciones objetivo. En estas campañas de *phishing*, los documentos adjuntos suelen estar presentados como recibos de pago, deuda acumulada, recetas, avisos, transferencia, orden de compra, etc.
- **Solo ingeniería social a través del correo**: incluye un correo electrónico enviado a alguien en el departamento de finanzas (generalmente el CFO) de la empresa objetivo. Los atacantes diseñan el correo electrónico para que parezca que lo envió un ejecutivo de la compañía, generalmente instruyendo al objetivo para que transfiera el dinero. La solicitud de transferencia generalmente tiene como objetivo el pago a un proveedor o trabajador, o como un favor personal.

Campaña de *phishing* de Meltdown y Spectre

Las autoridades alemanas han advertido recientemente de la existencia de una campaña de *phishing*, que trataba de comprometer los equipos de sus víctimas a través de un falso parche contra las vulnerabilidades de **Meltdown** y **Spectre**.

La web fraudulenta trataba de suplantar a la web de la Oficina Federal Alemana para la Seguridad de la Información (BSI) y a pesar de que el dominio contaba con un certificado SSL, no estaba relacionado con ninguna entidad gubernamental legítima u oficial. El mismo dominio fraudulento tenía un enlace a un archivo **ZIP** que realmente se trataba de un *malware*, que al ejecutarlo, los usuarios quedaban infectados por **Smoke Loader**.

Brecha en el sistema de salud noruego

Un grupo de cibercriminales podría haber robado los registros médicos de más de la mitad de la población de Noruega, según información proporcionada por la prensa local.

El ataque tuvo lugar el 8 de enero y salió a la luz a mediados de mes cuando la organización sanitaria que gestiona los hospitales de la región del sudeste de Noruega, anunció una brecha de seguridad en su web.

Según **HelseCERT**, la división CERT del país para el sector sanitario, habría identificado tráfico sospechoso procedente de la red informática de **Health South-East**. Tras una investigación realizada por el personal IT de la organización sanitaria, se pudo llegar a encontrar evidencias de una brecha de seguridad grave.