Nombre

Cryptojacking

Fecha de nacimiento

2011

Origen

Los indicios lo sitúan en Rusia.

Modus Operandi

Cryptojacking utiliza dispositivos ajenos de forma no autorizada para minar criptomonedas ilegalmente.

Los atacantes hacen uso del malware para secuestrar ordenadores, tablets o smartphones, y aprovechar su potencia de procesamiento para minar criptomonedas de manera encubierta, utilizando los recursos energéticos de los dispositivos.

La mayoría de los ataques de cryptojacking utilizan el código Coinhive para minar las criptomonedas.

Detención

Esta amenaza ya ha sido arrestada y neutralizada por Panda Security

Pero si no eres cliente de Panda Security y lo ves en tus dispositivos o en la red de la empresa, contáctanos de inmediato para proceder a su captura:

info@pandasecurity.com

Actividad Criminal

Smominru

A principio de 2018, se descubrió Smominru, un malware para minar Monero que infectó a más de medio millón de máquinas desde mayo del 2017, principalmente en Rusia, India y Taiwán. Se estima que los ciberdelincuentes ya se habían embolsado hasta $ 3,6 millones.

Adylkuzz y Wannamine

Una de las vulnerabilidades que más problemas ha causado en el 2018 es EternalBlue, usado también por Wannacry. Esta vulnerabilidad fue la puerta de entrada para Adylkuzz. Este malware se utilizó para generar Monero, e infectó a miles de ordenadores en todo el mundo. De hecho, se cree que podría haber afectado incluso a más equipos que WannaCry.

Ataque a DoubleClick

A finales de enero de 2018, YouTube descubrió estar afectado por un nuevo ataque, al ver como en sus anuncios se ocultaba código malicioso, perjudicando a numerosos usuarios. En este caso, la plataforma de anuncios DoubleClick fue la víctima de un ataque que escondía en el código de los anuncios de YouTube el script de cryptojacking, CoinHive.

WinstarNssmMiner

En mayo de 2018, otro malware particularmente peligroso, llamado WinstarNssmMiner, infectó a medio millón de equipos en tres días. Éste llegaba a través de emails de phishing o sitios web infiltrados. Una vez dentro del sistema, usaba toda la potencia del ordenador para minar criptomonedas.

HiddenMiner

Descubierto en marzo de 2018, Hiddenminer, llegaba a los dispositivos móviles a través de aplicaciones descargadas en tiendas de apps de terceros, es decir, no oficiales.

Una de las razones que lo hacía tan peligroso es que, en las versiones más antiguas de Android, era casi imposible de desinstalar. Una vez dentro, utilizaba todos sus recursos, sobrecalentándolo y haciendo que fallara.

Nombre

Ransomware

Fecha de nacimiento

1989

Origen

USA

Modus Operandi

Esta modalidad de cibercrimen encripta archivos de los ordenadores y los bloquea hasta que se recibe el rescate requerido, generalmente en forma de bitcoin, una criptomoneda virtual ilocalizable.

No te fíes de él y nunca accedas a pagar el rescate porque no garantiza en absoluto que tus archivos sean liberados.

Detención

Esta amenaza ya ha sido arrestada y neutralizada por Panda Security

Pero si no eres cliente de Panda Security y lo ves en tus dispositivos o en la red de la empresa, contáctanos de inmediato para proceder a su captura:

info@pandasecurity.com

Actividad Criminal

Wannacry

El 12 de mayo del 2017, un malware del tipo ransomware con funcionalidad de gusano de red, afectó a ciertos sistemas Microsoft Windows, aprovechándose de una antigua vulnerabilidad. De este modo consiguieron cifrar todos los archivos de los equipos afectados y los de las unidades de red a las que estuvieran conectadas, infectando al resto de sistemas Windows vulnerables que hubiera en esa red.

El proceso finalizaba con la petición de un rescate para su desencriptación. En concreto, el pago de 300$ por cada equipo liberado mediante el pago de esa suma a través de BitCoin.

Wannacry ha sido descrito como una amenaza sin precedentes en tamaño, infectando más de 230.000 ordenadores en más de 150 países. Provocó costes en torno a los 5.000 millones de dólares.

GoldenEye/Petya

El 27 de junio del 2017 se producía un nuevo ataque de ransomware que paralizó grandes empresas en todo el mundo. Este ataque masivo se realizó con una variante nueva de la familia de Ransomware GoldenEye. Una réplica del temido WannaCry.

Petya se ejecutó en los ordenadores cifrando determinados archivos, al tiempo que bloqueaba el sector de arranque del sistema comprometido. De este modo, impedía el acceso al usuario a su propio ordenador a no ser que introdujera una clave de acceso, después de haber pagado el rescate.

Como novedad frente a WannaCry, este nuevo ciberataque era capaz de apagar el ordenador o programar una tarea para que éste se apagara al cabo de un tiempo.

Nombre

APTs (Amenazas Persistentes Avanzadas)

Fecha de nacimiento

1989

Origen

Moscú

Modus Operandi

Es un conjunto de ataques complejos, sigilosos y continuos, controlados por grupos organizados de ciberdelincuentes y generalmente dirigidos contra gobiernos, grandes empresas o instituciones.

Se denominan avanzados por la coordinación y el uso de técnicas sofisticadas para penetrar en los sistemas informáticos de las víctimas, utilizando vulnerabilidades y puertas traseras de los sistemas operativos.

Las ATPs se caracterizan por intentar permanecer el mayor tiempo posible ocultas, para robar toda la información posible. Buscan el bien más preciado de las empresas u organizaciones: su información corporativa más sensible y aquellos datos que permiten una monetización inmediata del ataque.

Detención

Esta amenaza ya ha sido arrestada y neutralizada por Panda Security

Pero si no eres cliente de Panda Security y lo ves en tus dispositivos o en la red de la empresa, contáctanos de inmediato para proceder a su captura:

info@pandasecurity.com

Actividad Criminal

GhostNet

Ataque a gran escala descubierto en marzo de 2009. Su origen se centró en la República Popular China.

GhostNet se infiltró en los ordenadores de objetivos políticos, económicos y de medios de comunicación en más de 100 países.

Operación Aurora

Serie de ataques cibernéticos lanzados en 2009 que se originaron en China. Utilizó un exploit Zero Day para instalar un troyano diseñado para robar información.

Google, afectada por este ataque, reveló en 2010 que otras muchas compañías también habían sido atacadas. Entre ellas se incluían los principales bancos, contratistas de defensa, proveedores de seguridad, compañías de petróleo, gas y otras empresas de tecnología.

Stuxnet

Gusano informático que afectaba a equipos con Windows, descubierto en junio de 2010. Fue el primer gusano conocido que espiaba y reprogramaba sistemas industriales.

El objetivo del gusano fueron las infraestructuras nucleares de Irán, con sistemas de control de Siemens. Algunos medios atribuyeron su autoría a los servicios secretos estadounidenses e israelíes.

Red October

En octubre de 2012, se descubrió un programa de malware diseñado para robar información confidencial de gobiernos y organizaciones de investigación.

Se cree que estuvo operando en todo el mundo durante, al menos, 5 años antes de su descubrimiento, robando información sensible de organizaciones diplomáticas, comerciales, militares, aeroespaciales e investigación en Rusia, Irán, Estados Unidos y al menos otros 36 países.

Nombre

Phishing

Fecha de nacimiento

1995

Origen

Los indicios lo sitúan en USA.

Modus Operandi

Es una de las estafas más conocidas de los 90s, y a día de hoy continúa siendo uno de los recursos más utilizados por los ciberdelincuentes. Más del 90% del malware en el mundo llega a través del email.

El "phishing" consiste en el envío de correos electrónicos que, aparentando provenir de fuentes fiables (por ejemplo, entidades bancarias), intentan obtener datos confidenciales del usuario, que posteriormente son utilizados para la realización de algún tipo de fraude.

La apariencia y las tácticas del ataque varían, pero el objetivo sigue siendo conseguir datos mediante falsos mensajes para acceder a cuentas personales o corporativas de un usuario.

Detención

Esta amenaza ya ha sido arrestada y neutralizada por Panda Security

Pero si no eres cliente de Panda Security y lo ves en tus dispositivos o en la red de la empresa, contáctanos de inmediato para proceder a su captura:

info@pandasecurity.com

Actividad Criminal

Operación Phish Phry

En 2009, los bancos estadunidenses sufrieron el ataque de phishing Phish Phry, que afectó a más de 500 personas con pérdidas de 1,5 millones de dólares. Más de 100 personas fueron acusadas en los EE. UU. y Egipto por esta operación.

Las instituciones financieras afectadas fueron Bank of America y Wells Fargo. Hasta el momento, ha sido el caso de phishing internacional más grande jamás realizado.

Ataque a la RSA

En marzo 2011, la RSA informó que había sido atacada por un phishing. El ataque explotó una vulnerabilidad de Adobe Flash que no fue parcheada. El correo electrónico que se utilizó decía: "Le reenvío este archivo para que lo revise. Por favor, ábralo y véalo" y adjuntaba un archivos llamado "Plan de contratación 2011".

Dyre Phishing Scam

En octubre de 2014, el phishing Dyre, infectó a más de 20.000 usuarios y consiguió robar más de un millón de dólares. La mayoría de los correos electrónicos se enviaron haciéndose pasar por un asesor fiscal con la intención de que la víctima descargara el software malicioso.

Phishing en Snapchat

En julio de 2018, un ataque de phishing consiguió las credenciales de más de 50.000 usuarios de Snapchat. El informe contenía una lista pública, integrada en un sitio web de phishing llamado klkviral.org. Ahí se incluían 55.851 cuentas de Snapchat, junto con sus nombres de usuario y contraseñas.

Nombre

Zero days

Fecha de nacimiento

2010

Origen

Desconocido

Modus Operandi

Denominamos 'Zero Day' cualquiera ataque lanzado que aprovecha la ventana de oportunidad producida por vulnerabilidades recién descubiertas. Es decir, un ataque rápido desplegado por cibercriminales antes de que los proveedores de seguridad hayan sido capaces de reparar la vulnerabilidad o incluso de que hayan oído hablar de su existencia.

Son un recurso muy utilizado por determinados gobiernos para socavar sistemas críticos de otros países o de las empresas originarias de los mismos.

Detención

Esta amenaza ya ha sido arrestada y neutralizada por Panda Security

Pero si no eres cliente de Panda Security y lo ves en tus dispositivos o en la red de la empresa, contáctanos de inmediato para proceder a su captura:

info@pandasecurity.com

Actividad Criminal

Stuxnet

Gusano informático que afectaba a equipos con Windows, descubierto en junio de 2010. Fue el primer gusano conocido que espiaba y reprogramaba sistemas industriales.

El objetivo del gusano fueron las infraestructuras nucleares de Irán, con sistemas de control de Siemens. Algunos medios atribuyeron su autoría a los servicios secretos estadounidenses e israelíes.

Ataque a Sony Pictures

En 2014, Sony Pictures sufría uno de los peores ataques de su historia. El grupo de Hackers conocidos como "Guardians of Peace" utilizó una ataque Zero Day, para paralizar la red corporativa de Sony y robar durante semanas información sensible de la empresa.

Los datos incluían información personal sobre sus empleados y sus familias, correos electrónicos confidenciales, información sobre los salarios de los ejecutivos de la empresa o copias de películas de Sony que aún no habían sido estrenadas. Gran parte de esta información fue publicada en internet.

Comité Nacional Demócrata

Gracias a 6 vulnerabilidades en Microsoft Windows 10, Adobe Flash y Java, en 2016 hackers rusos respaldados por el servicio de inteligencia, conseguían infiltrarse en el sistema del Comité Nacional Demócrata (el órgano de gobierno interno del Partido Demócrata de los Estados Unidos).

Para poder explotar estas vulnerabilidades enviaron correos electrónicos (phishing) a diferentes miembros del Comité Nacional y objetivos políticos con el fin de robar sus contraseñas.

Los datos obtenidos fueron principamente filtrados a través de Wikileaks.