



# Defiéndase contra amenazas críticas • de la actualidad

Reporte de amenazas de 2019

## Contenido

	Mire hacia atrás, avance hacia delante	3
	Tipos de ataques y protección	5
1	El giro de Emotet: de la banca a la distribución	6
	<b>Correo electrónico: El vector de amenazas más común</b>	<b>6</b>
2	Maquinaciones de IoT: El caso de VPNFilter	9
3	Gestión de dispositivos móviles: La bendición y la maldición	12
	<b>Una foto de incidentes de seguridad ¿Qué</b>	<b>12</b>
	<b>ocurrió con el ransomware?</b>	<b>14</b>
4	Criptominería: un lobo vestido de oveja sigue siendo un lobo	15
	<b>En el radar</b>	<b>17</b>
5	El invierno venía: Olympic Destroyer	18
	Acerca de la Serie de Ciberseguridad de Cisco	20

## Mire hacia atrás, avance hacia delante

### Cuando se trata del panorama de amenazas, es importante echar un vistazo en el retrovisor de vez en cuando.

Como al conducir, no solo echa un buen vistazo a lo que está detrás de usted, también, a menudo, puede detectar lo que se acerca rápido para pasarlo.

Ese es el espíritu de este reporte sobre amenazas. Hemos elegido cinco historias clave del año pasado no solo porque eran grandes eventos, sino también porque creemos que estas amenazas, o similares, podría perfectamente aparecer en el futuro cercano.

Por ejemplo, amenazas modulares como Emotet y VPNFilter. Estas son las amenazas que pueden ofrecer un menú de ataques y amenazas a pedido, dependiendo del dispositivo que se ve infectado o el objetivo esperado del atacante. Vimos muchas de estas amenazas modulares en la historia reciente y no se sorprenda si vemos más en el futuro.

El correo electrónico sigue siendo el método de entrega preferido de los atacantes, con amenazas desde criptominería hasta Emotet, usándolo para propagarse. También es muy probable que lo utilicen otros tipos de amenaza, como el perfil de MDM no autorizado. Esto destaca lo fundamental que es estar atento a lo que llega a la bandeja de entrada.

### Modo de operar

La generación de ingresos sigue siendo una de las principales motivaciones para los atacantes: el malware va atrás del dinero. Por ejemplo, las amenazas de criptominería se enfocan mucho en este objetivo. Mientras tanto, Emotet ha pasado a una red de distribución de amenazas, aprovechando así una variedad de opciones para generar dinero.

La filtración de datos también ha llegado a ser el centro de atención. Era uno de los principales motivos de muchas amenazas recientes, como VPNFilter, que parecía haber sido configurada para robar información. Además de robar credenciales de red para propagarse, también se detectó que Emotet propaga Trickbot, otro popular troyano bancario de robo de información.

**Hemos elegido cinco historias clave porque creemos que estas amenazas, o similares, podrían volver a aparecer.**

Por último, algunas amenazas solo desean crear caos, como es el caso de Olympic Destroyer. Observamos un número de amenazas como esta en el último año, pero ninguna acaparó los titulares tanto como un ataque cuyo único propósito parece haber sido interrumpir los Juegos Olímpicos de Invierno.

A medida que analizamos algunas de las amenazas de mayor impacto de 2018, es importante ser conscientes de lo que las hizo tan efectivas. Por el momento, muchas de estas pueden estar en el retrovisor; sin embargo, ¿las ha superado o están avanzando para superarlo a usted y su estrategia de seguridad?





Cuando se trata del panorama de amenazas, es importante echar un vistazo en el retrovisor de vez en cuando. Como al conducir, no solo puede visualizar lo que está detrás de usted, sino que también, a menudo, puede detectar lo que se acerca rápido para pasarlo.





## Tipos de ataques y protección

Siempre se recomienda un enfoque por capas a la seguridad. Hemos incluido íconos al final de cada historia para indicar vectores de amenazas clave utilizados (o que se sospecha que fueron utilizados) y herramientas que pueden brindar protección contra ellos en cada caso. A continuación, decodificamos los íconos y analizamos las ventajas de implementar los diferentes tipos de protección como parte de una arquitectura de seguridad integrada.



La **tecnología de detección y protección de malware avanzada** (por ejemplo, [Cisco Advanced Malware Protection o AMP](#)) puede monitorear archivos desconocidos, bloquear archivos maliciosos conocidos y evitar la ejecución de malware en terminales y dispositivos de red.



Los **sistemas de seguridad de la red**, como [el Firewall de próxima generación de Cisco \(NGFW\)](#) y el [Sistema de prevención de intrusiones de próxima generación \(NGIPS\)](#), pueden detectar archivos maliciosos que intentan penetrar una red desde Internet o moverse dentro de una red. Las plataformas de visibilidad de red y análisis de seguridad, como [Cisco Stealthwatch](#), pueden detectar anomalías de red internas que pueden implicar que un malware está activando su carga. Por último, la segmentación puede prevenir el movimiento lateral de las amenazas dentro de una red y contener la propagación de un ataque.



Con el **Escaneo de la web en un Gateway web seguro (SWG)** o un **Gateway de Internet seguro (SIG)** como [Cisco Umbrella](#), puede bloquear la conexión de usuarios a dominios, IP y URL maliciosos, independientemente de si los usuarios se encuentran conectados a la red empresarial o no. De esta manera, se puede evitar que las personas permitan involuntariamente que el malware acceda a la red y que el malware que logra penetrar se conecte nuevamente a un servidor de comando y control (C2).



La **Tecnología de seguridad de correo electrónico** (por ejemplo, [Cisco Email Security](#)), implementada en las instalaciones o en la nube, bloquea correos electrónicos maliciosos enviados por agentes de amenaza como parte de sus campañas. De esta manera, se reduce la cantidad total de spam, se elimina spam malicioso y se realiza un análisis de todos los componentes de un correo electrónico (como ser, remitente, asunto, archivos adjuntos y URL integradas) para encontrar mensajes que puedan contener una amenaza. Estas capacidades son fundamentales, ya que el correo electrónico sigue siendo el principal vector utilizado por agentes de amenaza para efectuar ataques.



La **Tecnología de detección y protección frente a malware avanzado**, como [Cisco AMP para terminales](#), puede evitar la ejecución de malware en el terminal. También puede ayudar a aislar, investigar y corregir los terminales infectados para el uno por ciento de los ataques que penetra incluso las defensas más sólidas.

## El giro de Emotet: de la banca a la distribución

Muy a menudo, en el panorama de amenazas, las historias que llegan a los titulares son las que cuentan algo nuevo o novedoso: el descubrimiento de una vulnerabilidad que afecta una gran cantidad de dispositivos o la revelación de un ataque contra una importante organización.

Sin embargo, **algunas de las amenazas más frecuentes no son las que se roban el centro de atención. Pueden depender de métodos probados, en lugar de las mejores y más recientes técnicas.** Y esto beneficia a los atacantes. Una amenaza que puede pasar desapercibida tiene el potencial de crecer, mientras que no así una amenaza que llame más la atención.

Emotet es un ejemplo perfecto de ello. Mientras los titulares fueron acaparados por debates sobre amenazas como WannaCry y NotPetya, Emotet permaneció en segundo plano durante años. Esta táctica lo benefició, ya que se ha convertido en una de las familias de amenazas más efectivas de la actualidad.

El éxito de Emotet radica en la forma en que ha evolucionado. Desde sus comienzos "humildes" como troyano bancario, los agentes de amenaza pasaron rápidamente a convertir la amenaza en una plataforma modular capaz de llevar a cabo una variedad de ataques. En la actualidad, otras familias de amenazas, que antiguamente se veían como competidoras, ahora lo utilizan para propagar sus programas. Y, a medida que el panorama de amenazas vuelve a cambiar, Emotet parece estar elevándose a la cima en el radar de todos.

### De modesto a modular

Cuando Emotet apareció en escena, fue uno más entre varios troyanos bancarios. La amenaza se propagaba a través de campañas de spam, generalmente mediante correos electrónicos de spam relacionados con facturas o pagos. A menudo, se adjuntaban como

documentos de Office con macros habilitados o archivos JavaScript, o se incluían como enlace malicioso. Las técnicas de distribución variaban, aunque muchas de las campañas apuntaban a bancos en regiones específicas, particularmente, en países de habla alemana en Europa y en los Estados Unidos.

En un principio, la amenaza se centraba principalmente en el robo de información bancaria: nombres de usuario, contraseñas, direcciones de correo electrónico y demás información financiera. Con el tiempo, Emotet comenzó a propagarse a un público más



*Emotet ha permanecido en segundo plano durante años. Esta táctica le ha sido beneficiosa.*



### Correo electrónico: El vector de amenazas más común

**Un tema que vemos relacionado con la mayoría de las principales amenazas actuales es el correo electrónico. Sigue siendo el vector de infección más popular para que los agentes de amenazas propaguen sus programas, y probablemente continúe siéndolo en el futuro cercano.**

**Observe Emotet, por ejemplo. Semana tras semana, los atacantes detrás de esta amenaza lanzan nuevas campañas de suplantación de identidad.**

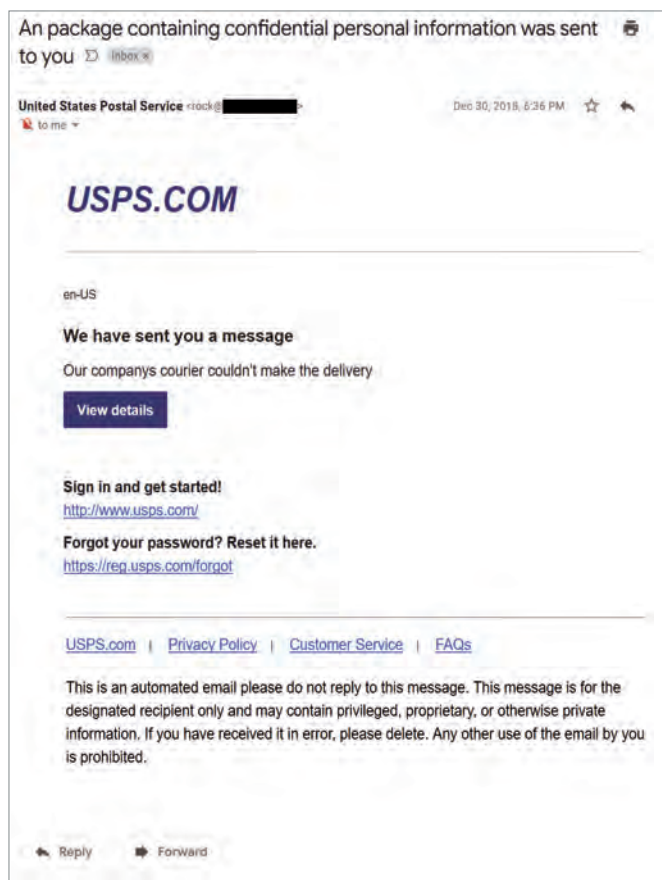
**Lo mismo ocurre con la criptomoneda maliciosa, en la que las campañas de spam engañan constantemente a los usuarios para que descarguen programas de minería en sus computadoras.**

**Y en cuanto a las amenazas a la administración de dispositivos móviles (MDM), es probable que los ataques se hayan diseminado a partir de correo electrónico con ingeniería social.**

**(Cont.)**

general. Una nueva versión de la amenaza estableció las bases de la configuración modular actual, la cual contiene diferentes herramientas para diversas funciones. Algunos módulos roban credenciales de correo electrónico, mientras que otros se centran en nombres de usuario y contraseñas almacenados en el navegador. Algunos proporcionan capacidades de denegación de servicio distribuido (DDoS), mientras otros pueden distribuir ransomware.

Figura 1 Un correo electrónico de spam de muestra de Emotet



**No es ninguna sorpresa, dado el diseño convincente de muchos correos electrónicos de suplantación de identidad, especialmente los que se visualizan en un teléfono móvil. Y para un usuario ocupado, el riesgo y la urgencia del correo electrónico podrían llevar al destinatario a tomar medidas inmediatas, pasando por alto los indicadores de una amenaza a la espera.**

**No es de extrañar que los atacantes continúen acudiendo al correo electrónico para propagar su malware.**

## Muéstrame el dinero

El objetivo principal de Emotet es descubrir una forma de lucrar con la computadora en riesgo, y es aquí donde actúan los módulos. Pareciera como si **los módulos instalados en un dispositivo concreto dependieran de la mejor forma en que puede lucrar con el dispositivo infectado**. Piense en los siguientes casos:

- ¿El historial del navegador de la computadora muestra visitas frecuentes a sitios web bancarios? Implemente módulos bancarios para robar credenciales y transferir dinero.
- ¿Es el dispositivo una computadora portátil que probablemente indica que el objetivo de ataque dispone de ingresos? Implemente módulos de distribución de malware e instale software de ransomware o criptominería.
- ¿Es la máquina un servidor en una red de ancho de banda elevado? Instale módulos para la distribución de correo electrónico y la red, y continúe propagando Emotet.

## Honor entre ladrones

Lo que realmente diferencia a Emotet de muchas amenazas en el panorama de amenazas actual no es solo su alcance y modularidad, sino que los agentes detrás de la amenaza parecen estar promocionándolo como canal de distribución para otros grupos de ataque.

Por ejemplo, hemos observado situaciones en donde Emotet infecta una computadora solo para subir Trickbot al sistema como carga útil. En este caso aparentemente contradictorio, Emotet, que tiene una reputación bien conocida como troyano bancario, de hecho, está lanzando otro troyano bancario en lugar de utilizar sus propios módulos de robo de información. Lo que es aún más interesante es que Trickbot, después de haber sido subido por Emotet, a veces también lanza el ransomware Ryuk.

Por más extraño que parezca, la cooperación entre grupos simplemente podría deberse al hecho de que el trabajo en equipo genera los sueldos más elevados. Si Emotet no puede utilizar un dispositivo para continuar propagándose, Trickbot puede robar los registros bancarios. Si no se encuentran registros bancarios, Ryuk puede cifrar el dispositivo y exigir un rescate. Por supuesto que nadie sabe cuánto tiempo durará esta alianza maliciosa.

## Qué deparará el futuro

Se sabe que una amenaza que crece no suele permanecer oculta al radar. En los últimos meses de 2018, el sector de seguridad comenzó a tomar nota del tamaño de Emotet. Lo que llamó la atención de su perfil es que los distribuidores de spam por correo electrónico parecen haber abandonado las cargas útiles de criptomoneda y adoptado la distribución de Emotet y troyanos de acceso remoto (RAT). Y su impacto se está

## Los agentes detrás de Emotet parecen estar promocionándolo como canal de distribución para otros grupos de ataque.

sintiendo. De hecho, la limpieza de algunas infecciones de Emotet ha llegado a costar hasta \$1 millón, según US-CERT.

No es probable que Emotet desaparezca y puede llegar a dominar el panorama de amenazas en el futuro inmediato. Y si el pasado puede predecir el futuro, con el tiempo, Emotet desaparecerá, solo para ser sustituido por otro agente dominante en el panorama de amenazas.



## Para una mirada más profunda sobre este tema, consulte:

<https://blog.talosintelligence.com/2019/01/Return-of-emotet.html>

<https://www.US-CERT.gov/ncas/Alerts/TA18-201a>

<https://Duo.com/Decipher/The-Unholy-Alliance-of-emotet-trickbot-and-the-Ryuk-ransomware>

<https://blog.talosintelligence.com/2018/12/cryptocurrency-Future-2018.html>



## Maquinaciones de IoT: El caso de VPNFilter

En la última década, ha habido un número de amenazas notables relacionadas con Internet de las Cosas (IoT). Por ejemplo, el botnet Mirai infectó cámaras IP y routers para llevar a cabo ataques de DDoS. ¿Y quién puede olvidar los ataques a monitores para bebés, en donde los padres entraban a los cuartos de los niños y oían a los hackers hablarles a sus hijos después de haber interceptado el dispositivo?



Imagen: Talos

*VPNFilter permanece como un presagio de lo que aún está por venir casi inevitablemente.*

Le guste o no, IoT ha penetrado nuestros hogares y negocios, desde asistentes inteligentes a dispositivos de hospitales con conexión a Internet. Por desgracia, en muchos casos, las prácticas de seguridad adecuadas se han pasado por alto en el proceso. Como resultado, hemos visto a agentes maliciosos dirigir sus ataques a este tipo de dispositivos.

Sin embargo, **nada ha sido tan pernicioso como VPNFilter. Esta amenaza apuntó a una amplia gama de routers de una variedad de fabricantes, probablemente aprovechándose de vulnerabilidades no revisadas para ponerlos en riesgo.** Uno de sus propósitos parecía ser la filtración de datos confidenciales de las redes que puso en riesgo, aunque también contaba con un sistema modular que le permitía hacer mucho más, lo cual es de especial preocupación.

En total, la amenaza infectó, al menos, a medio millón de dispositivos en 54 países. Afortunadamente, los investigadores del grupo Cisco Talos detectaron la amenaza desde un principio. Cuando aumentó el número de infecciones, estaban preparados para detener su avance. Hoy en día, la amenaza que supone el VPNFilter ha disminuido en gran medida, gracias a la labor de partners de inteligencia de amenazas del sector público y privado, como también de la autoridad encargada del orden público. Aún así, VPNFilter permanece como un presagio de lo que aún está por venir casi inevitablemente.

### Cómo se desarrolla

**Etapas:** VPNFilter tiene tres componentes principales o "etapas" que componen la amenaza. El objetivo principal de la etapa uno es instalarse de manera persistente en un dispositivo. Hasta VPNFilter, generalmente, el malware que atacaba dispositivos de IoT podía eliminarse con solo reiniciar el dispositivo. En el caso del componente de la fase uno de VPNFilter, el malware sobrevive a dicho intento. La etapa uno también incluye varias opciones para conectarse al servidor de comando y control (C2), que indica al malware lo que debe hacer.

**Etapas dos:** Esta etapa, que representa el principal componente utilizado para llevar a cabo los objetivos maliciosos de VPNFilter, posee funciones como recopilación de archivos, ejecución de comandos, filtración de datos y gestión de dispositivos. Algunas versiones de la etapa dos también incluían un "switch de eliminación", que, de activarse, podía dejar el dispositivo infectado permanentemente fuera de uso.

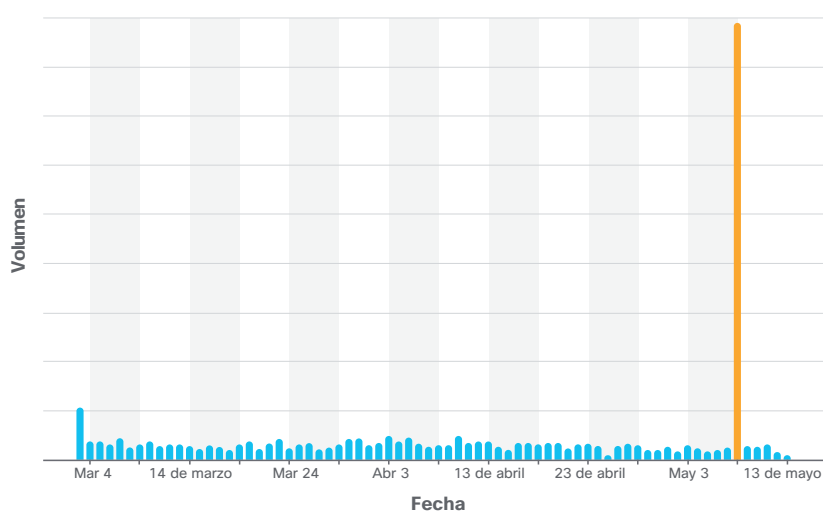
**Etapas tres:** la tercera etapa amplía la funcionalidad de la etapa dos, implementando plugins que faciliten aún más las acciones maliciosas. Entre algunos de los plugins notables, se incluye una funcionalidad para:

- Supervisar el tráfico de red
- Robar diferentes credenciales
- Supervisar el tráfico de dispositivos de IoT industrial específicos
- Cifrar la comunicación con el servidor C2
- Asignar redes
- Aprovechase de sistemas de terminales
- Propagarse a otras redes
- Llevar a cabo ataques de DDoS
- Construir una red de proxy que se pueda utilizar para ocultar el origen de futuros ataques

## VPNFilter (casi) se implementa

Talos había estado investigando VPNFilter durante varios meses y la tasa de infección había permanecido relativamente estable. El equipo había estado supervisando y escaneando dispositivos infectados para obtener una mejor comprensión de la amenaza y las capacidades presentes en el malware.

**Figura 2** Nuevas infecciones de VPNFilter por día



Fuente: Talos

Hasta el 8 de mayo de 2018, cuando se produjo un fuerte aumento en la actividad de infección. No solo eso, la mayoría de las infecciones se producían en Ucrania. El 17 de mayo, se produjo un segundo aumento en las infecciones por VPNFilter en Ucrania, cerca del primer aniversario de NotPetya. Dado que Ucrania contaba con un historial de ataques destructivos, Talos consideró que lo mejor era abordar este ataque a la infraestructura lo antes posible, aunque se haya continuado con la investigación.

Talos continuó investigando y publicando información sobre botnet hasta que, en septiembre de 2018, pudo declarar la neutralización de la amenaza.

## Se eliminó, pero no se olvidó

Lamentablemente, si bien VPNFilter puede ser una amenaza del pasado, se continúan descubriendo vulnerabilidades en dispositivos de IoT. Es inevitable que, en el futuro, aparezca otra amenaza dirigida a IoT.

Resulta difícil defenderse ante amenazas como esta. Dispositivos de IoT, como routers, suelen conectarse directamente a Internet. Si combina esto con el hecho de que muchos usuarios no tienen los conocimientos técnicos para repararlos o no los consideran una amenaza, la situación se vuelve muy peligrosa.

A fin de cuentas, **se sabe que IoT como parte de la red continuará creciendo. VPNFilter nos muestra lo que puede ocurrir si no tomamos las medidas adecuadas para proteger estos dispositivos en el futuro.**



**Para una mirada más profunda sobre este tema, consulte:**

<https://blog.talosintelligence.com/2018/05/VPNFilter.html>

<https://blog.talosintelligence.com/2018/06/vpnfilter-update.html>

<https://blog.talosintelligence.com/2018/09/vpnfilter-part-3.html>

<https://blog.talosintelligence.com/2018/12/Year-in-malware-2018-Most-ProMinent.html>





Lamentablemente, si bien VPNFilter puede ser una amenaza del pasado, se continúan descubriendo vulnerabilidades en dispositivos de IoT. Es inevitable que, en el futuro, aparezca otra amenaza dirigida a IoT.



# Gestión de dispositivos móviles: La bendición y la maldición

La funcionalidad Administración de dispositivos móviles (MDM) ha sido una bendición para la empresa. Permite que una organización tenga mucho más control de los dispositivos en su red. Sin embargo, como descubrimos en 2018, también ha posibilitado el ingreso de agentes maliciosos bien financiados.



Talos detectó que los agentes maliciosos descubrieron la forma de utilizar MDM con fines maliciosos.

Cuando se trata de malware móvil, los sistemas operativos móviles pueden ser difíciles de vulnerar. En la mayoría de los casos, el jardín amurallado creado en torno al sistema operativo móvil lo ha protegido contra aplicaciones maliciosas.

Eso no quiere decir que los agentes maliciosos no hayan intentado dirigir sus ataques a teléfonos móviles. Se han detectado aplicaciones maliciosas en las tiendas de aplicaciones oficiales, pero, en la mayoría de los casos, los atacantes se han visto limitados a poner en riesgo dispositivos desbloqueados, o si están disponible, aquellos que permiten aplicaciones de terceros.

Si bien el jardín amurallado puede ser seguro, también puede ser una prisión. La desventaja de este nivel de restricción y la seguridad que ofrece, es que solo puede instalar aplicaciones desde una tienda oficial, o si está disponible, desbloquear su dispositivo para todas las aplicaciones de terceros. Esto se vuelve un problema en el caso de empresas que crean aplicaciones exclusivas a las que solo sus empleados puedan acceder, pero que también desean proteger sus dispositivos.

## La introducción de MDM

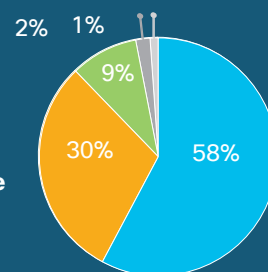
Para abordar esta necesidad, se introdujeron los sistemas MDM. Esto permite a una empresa tomar teléfonos móviles de la empresa, instalar perfiles registrados a su empresa y en última instancia, instalar aplicaciones de su elección. A menudo, MDM ofrece otras funciones afines

a la empresa, como la capacidad de controlar la configuración del dispositivo, impedir el acceso a sitios web no deseados o encontrar dispositivos perdidos.

## Una foto de incidentes de seguridad

¿Cuáles son los incidentes de seguridad más habituales a los que se enfrentan las organizaciones? Nuestros colegas del grupo Cisco Cognitive Intelligence calcularon la cifra para nosotros.

En esta foto, se muestra las cinco categorías principales, obtenidas de julio de 2018.



Por lo general, los botnets y RAT dominan los incidentes de seguridad. En esta categoría, se incluyen amenazas como Andromeda y Xtrat.

La segunda categoría principal de amenazas es la criptominería, que contiene incidentes que detectaron programas de minería no autorizados, como Moneo y Coinhive, entre otros.

Lo más notable es la pequeña proporción que representan los troyanos bancarios. Sin duda, esta tendencia cambiará a medida que aumente la actividad de Emotet.

En informes futuros, repasaremos esta métrica para ver cómo cambia.





Imagen: Talos

Indudablemente, MDM es una herramienta poderosa. Es tan poderosa que Cisco Talos detectó que los agentes maliciosos descubrieron la forma de utilizarla con fines maliciosos.

### Comenzó en India

Nuestros investigadores en [Talos descubrieron dispositivos en India afectados mediante un sistema MDM de código abierto](#). Los atacantes habían logrado instalar perfiles maliciosos en los dispositivos, lanzar aplicaciones con el fin de interceptar datos, robar mensajes SMS y descargar fotos, contactos, y monitorear la ubicación de los dispositivos, entre otras cosas.

Entre las aplicaciones, se incluía versiones modificadas de aplicaciones populares, como WhatsApp y Telegram, que contaban con funciones adicionales añadidas o "transmitidas" a estas, lo que permitía a los atacantes supervisar conversaciones en cada dispositivo afectado.

Lo que permanece un misterio es cómo estos dispositivos se vieron afectados por el ataque. Es posible que los atacantes hayan tenido acceso físico a los dispositivos, lo que les permitió instalar un perfil que les otorgó control. Sin embargo, también es posible que los atacantes hayan empleado ingeniería social para convencer a los usuarios a instalar el perfil.

Esta alerta maliciosa puede haber llegado por correo electrónico o mensaje de texto, con el fin de engañar al usuario para que piense que debía instalar el perfil malicioso. Aún así, el usuario debe seguir una serie de instrucciones y hacer clic en indicaciones antes de que el dispositivo quede totalmente afectado.

### Cuidar de su jardín

Sin duda, este es un método de ataque poderoso y preocupante. Por suerte, también es poco frecuente. La campaña de ataque detectada por Talos es la única campaña de este tipo conocida públicamente. También es

*Dadas las posibles recompensas, es probable que veamos más de estos ataques en el futuro, llevados a cabo por agentes de amenazas bien financiados.*

difícil de implementar, teniendo en cuenta la cantidad de pasos que un usuario debe realizar para configurar un dispositivo para actividad maliciosa. Sin embargo, debido a las posibles recompensas, Talos ya está detectando más ataques a dispositivos móviles, llevados a cabo por agentes de amenazas bien financiados.

Irónicamente, la mejor protección contra MDM malicioso es...MDM.

Las organizaciones deben garantizar que los dispositivos de la empresa cuenten con perfiles instalados que puedan monitorear y prevenir la instalación de perfiles o aplicaciones maliciosos desde tiendas de aplicaciones de terceros.

También es importante explicar a los usuarios el proceso de instalación de MDM y capacitarlos acerca de estos ataques para evitar que instalen un MDM malicioso.



**Para una mirada más profunda sobre este tema, consulte:**

<https://blog.talosintelligence.com/2018/07/Mobile-malware-Campaign-uses-Malicious-MDM.html>

<https://blog.talosintelligence.com/2018/07/Mobile-malware-Campaign-uses-Malicious-MDM-part2.html>

## ¿Qué ocurrió con el ransomware?

**En 2017, parecía que el ransomware dominaría el panorama de amenazas durante mucho tiempo. Amenazas como SamSam y Bad Rabbit habían acaparado los titulares y se exigían pagos en criptomoneda, o de lo contrario, se perderían todos sus datos.**

**Al avanzar hasta poco más de un año atrás, las cosas ciertamente han cambiado.**

**El ransomware ha perdido su trono, principalmente, en manos de la criptomoneda maliciosa.**

**¿Por qué el cambio repentino? Con el ransomware, solo un pequeño porcentaje de las víctimas paga el rescate. Y aunque lo hayan logrado, era solo un pago único, en lugar de una fuente constante de ingresos.**

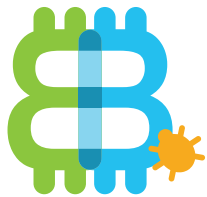
**Se volvió aún más arriesgado, ya que autoridades encargadas del orden público de todo el mundo comenzaron a tomar medidas contra los atacantes de ransomware. A medida que aumentaron los arrestos relacionados con el ransomware, los adversarios se vieron obligados a optar por tipos de ataques de menor riesgo.**

**Esto no quiere decir que el ransomware haya desaparecido; hemos detectado algunas de estas amenazas en 2018. GandCrab continuó estando presente y Ryuk se propagó a través de infecciones por Emotet y Trickbot. Entonces, si bien el ransomware ya no es la principal amenaza, sigue presente, lo cual requiere vigilancia para evitar nuevos ataques.**

# Criptominería: Un lobo vestido de oveja sigue siendo un lobo

Por lejos, el esquema de amenazas lucrativo más destacado de 2018 fue la criptominería maliciosa. Este es un tema que el grupo de inteligencia de amenazas de Cisco Talos ha estado investigando durante algún tiempo. Desde el punto de vista de un atacante, es prácticamente el crimen perfecto: los programas de minería a menudo trabajan en segundo plano, sin el conocimiento de los usuarios, apoderándose de su capacidad de procesamiento al tiempo que generan ingresos para el atacante.

A medida que las empresas perfeccionaron su estrategia para lidiar con el ransomware y las autoridades encargadas del orden público de todo el mundo comenzaron a tomar medidas contra los atacantes de ransomware, cada vez más atacantes se inclinaron por la opción menos riesgosa de traficar software malicioso de criptominería.



*Hay poca diferencia entre el software de criptominería que un usuario instala y el software de criptominería instalado por un agente malicioso.*

## La oveja se encuentra con el lobo

A menudo, hay poca o no hay diferencia entre el software de criptominería que un usuario instala por su cuenta y el software de criptominería instalado por un agente malicioso. El matiz radica en el consentimiento; el software de criptominería malicioso se está ejecutando sin el conocimiento del propietario. En este caso, hay un atractivo obvio para los atacantes, ya que pueden lograr su objetivo sin el conocimiento de las víctimas.

En el juego del riesgo y la recompensa, es menos probable que la criptominería llame la atención de las autoridades encargadas del orden público. Por el contrario, cualquier software que se ejecuta en un dispositivo sin el conocimiento del propietario causa preocupación.

Y la criptominería (maliciosa o no) puede ser muy lucrativa. En los últimos dos años y en la primera mitad de 2018, el valor de la criptomoneda se disparó. Como con cualquier cosa valiosa y relacionada con software,

los agentes maliciosos lo percibieron, especialmente debido a que coincide con una disminución de ransomware. Y la criptomoneda reporta ingresos recurrentes, mientras que, con el ransomware, normalmente, la víctima realiza un único pago.

## Los peligros de la criptominería maliciosa

Desde la perspectiva del defensor, hay muchas razones para estar preocupados con la criptominería maliciosa. Como cualquier tipo de software en una computadora, la criptominería tendrá un impacto negativo en el rendimiento general del sistema y necesitará alimentación adicional. Puede no representar demasiado en un solo sistema, pero multiplicando el costo por el número de terminales en una organización, podría producirse un importante aumento en los costos de energía.

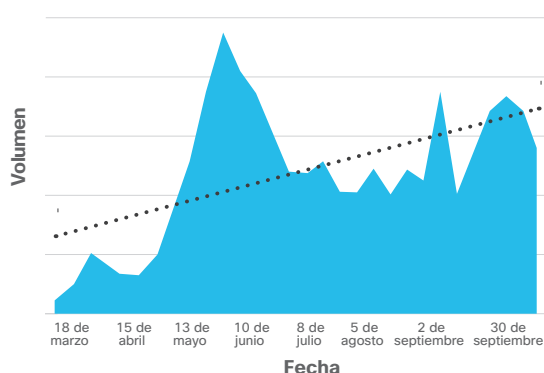
Además, **puede haber implicaciones de cumplimiento normativo si los programas de criptominería están obteniendo ingresos en redes corporativas.** Esta situación se presenta especialmente en el sector financiero, donde se pueden aplicar reglas estrictas en relación a los ingresos generados mediante recursos corporativos, independientemente de si los responsables son conscientes de la práctica o no.

Sin embargo, quizá lo más preocupante sea la presencia de una infección de criptominería maliciosa, desconocida para quienes ejecutan una red, que podría revelar vulnerabilidades de seguridad en la configuración de la red o las políticas de seguridad general. Los atacantes podrían fácilmente aprovechar dichas vulnerabilidades para otros fines. Básicamente, si se encuentra una infección de criptominería en una red, ¿qué podría evitar que otras amenazas maliciosas se aprovechen de las mismas vulnerabilidades para llevar a cabo otras actividades maliciosas?

### ¿Cuál es la situación actual?

Si bien han habido picos drásticos y estancamientos, en base al volumen global del tráfico relacionado con la criptomonera, que Cisco ha observado en la capa de DNS, se deduce que la criptomonera ha mantenido una tendencia a la alta con el paso del tiempo.

**Figura 3** Volumen de tráfico de criptomonera DNS corporativa



Fuente: Cisco Umbrella

Lo interesante es que el valor de muchas criptomonedas populares ha disminuido durante el mismo período, con tendencias a la baja. Por ejemplo, Monero, una moneda popular utilizada en criptomonera maliciosa.

**Figura 4** Valores de cierre de Monero



Fuente: coinmarketcap.com

Los agentes maliciosos continúan subiendo criptomonera maliciosa debido a la facilidad de implementación y el bajo riesgo si se descubre. Lo cierto es que, una vez que se instala en un dispositivo, continúa generando dinero para el agente malicioso mientras se esté ejecutando.

### ¿Cómo se instala la criptomonera maliciosa en un sistema?

Existen diversas formas en que la criptomonera maliciosa puede afectar su entorno, tales como:

- La explotación de vulnerabilidades
- El envío de correos electrónicos con adjuntos maliciosos
- El empleo de botnets
- El uso de la criptomonera en el navegador web
- El uso de amenazas de adware que instalan complementos en el navegador
- Un agente malicioso interno

Por desgracia, la criptomonera maliciosa llegó para quedarse en el futuro inmediato. Los distribuidores de spam continuarán enviando amenazas de criptomonera.

**La presencia de la criptomonera, desconocida para los administradores de red, podría señalar otras vulnerabilidades de seguridad en la red.**



El dinero es, y probablemente será siempre, uno de los principales factores de motivación para los agentes maliciosos. En muchos aspectos, los atacantes pueden ver la criptomonera maliciosa como una forma de lucrar rápidamente con poca sobrecarga. Esto es posible, principalmente porque las víctimas están menos preocupadas por las consecuencias de la criptomonera en sus dispositivos, en relación con otras amenazas. Es una situación perfecta para que los lobos se vistan de ovejas y observen cómo ingresan las ganancias.



Para una mirada más profunda sobre este tema, consulte:

<https://blogs.cisco.com/security/cryptomining-a-sheep-or-a-wolf>

<https://blog.talosintelligence.com/2018/12/cryptocurrency-future-2018.html>

<https://blog.talosintelligence.com/2018/12/cryptomining-campaigns-2018.html>



## En el radar

Analizamos una amplia variedad de amenazas para incluir en este informe. Si bien no se pudo incluir todo en el informe, tenemos previsto abordar los siguientes temas en los próximos meses, a través de nuestra serie de blogs sobre la **Amenaza del mes**. Este es un ejemplo de lo que está por venir:

**Extorsión digital.** Una de las campañas de suplantación de identidad más insidiosas últimamente se ha aprovechado de los temores de los destinatarios con el fin de obtener pagos en Bitcoin. Algunas campañas afirman haber descubierto por la cámara al destinatario mirando sitios web de pornografía. Otros incluyen amenazas de bomba falsas. En última instancia, las amenazas son totalmente inventadas, con la esperanza de engañar a suficientes destinatarios para que los atacantes se llenen los bolsillos de Bitcoins.

**Suplantación de identidad de Office 365.** Otra importante campaña de suplantación de identidad se basa en el robo de credenciales de cuentas de Microsoft Office 365. Los atacantes han utilizado un número de métodos para lograrlo. En nuestra siguiente publicación del blog, describiremos las diferentes campañas y cómo reconocerlas

Para mantenerse al tanto de nuestra serie de blogs sobre la Amenaza del mes, asegúrese de suscribirse a nuestra lista de correo y visite la página de Amenaza del mes.

Suscríbese: <http://cs.co/9002ERAWM>

Amenaza del mes: <http://cisco.com/go/threatofthemoth>

## El invierno venía: Olympic Destroyer



Imagen: Talos

*Si bien el ataque en los Juegos Olímpicos fue único, el grupo por detrás de este no descansará.*

El año pasado empezó con una explosión. Expertos en seguridad informática aún sentían los efectos del doble golpe de WannaCry y NotPetya y esperaban tener un comienzo de año más tranquilo. Estas esperanzas quedaron sepultadas rápidamente cuando Talos detectó que las interrupciones de la ceremonia inaugural de los Juegos Olímpicos de Invierno 2018 en Pyeongchang, Corea del Sur, eran causadas por malware.

El malware era muy destructivo y estaba hecho a medida para el entorno en que se encontraba. Su nombre puede estar relacionado con una ocasión histórica, pero la amenaza de Olympic Destroyer aún está presente.

Durante la ceremonia inaugural, la señal de Wifi había dejado de funcionar en el estadio y el área de medios de comunicación durante los Juegos Olímpicos de Invierno y dejó de funcionar el sitio web oficial de los juegos. Una interrupción a gran escala como esta plantea muchos desafíos que incluyen riesgos para la privacidad de datos, pérdida de reputación de la marca y una disminución en la satisfacción del cliente.

Con el tiempo, se hizo evidente que esta interrupción se debía a un ataque cibernético y una investigación a más largo plazo demostraría que el malware mostraba dos características: 1) era un malware limpiador diseñado para destruir activos (en lugar de ejecutarse como ransomware, por ejemplo) y 2) lo más interesante es que fue diseñado para ocultar su origen y engañar a los investigadores. **Este fue un ataque avanzado que combinaba técnicas sofisticadas de malware con una estrategia retorcida.**

### ¿Cómo destruye exactamente Olympic Destroyer?

El método de entrega de Olympic Destroyer es motivo de especulación. Lo que está claro es que, una vez dentro de una red de destino, se propaga rápidamente dentro de esta.

Nuestro mejor análisis posterior al ataque en Pyeongchang es que se movía como un gusano: muy veloz y destructivo. El archivo roba contraseñas, borra datos de copia de seguridad y está dirigido a datos almacenados en servidores, causando la máxima destrucción en el menor tiempo posible.

**Olympic Destroyer era altamente destructivo y estaba diseñado para destruir información.**

Los atacantes utilizaron herramientas legítimas para realizar el movimiento lateral, en este caso, PsExec (protocolo de Windows que permite ejecutar programas en computadoras remotas). Debido a la sincronización muy específica del ataque para que coincida con la ceremonia inaugural de los Juegos Olímpicos, el ataque se activó en forma remota.


Probablemente, los autores de Olympic Destroyer quería crear negación plausible mediante el uso de partes de código antiguo asociadas a otros agentes de amenazas. Algunos investigadores de seguridad quedaron desconcertados por esto, ya que algunos de ellos se apresuraron a atribuirse el ataque.

## El invierno continúa viniendo...

Sean cual fueren los motivos reales, Cisco Talos detectó los marcadores de un agente sofisticado en el malware Olympic Destroyer. Esto nos indica que, si bien Olympic Destroyer fue un ataque dirigido, el grupo por detrás de este no descansará. Probablemente vuelvan a utilizar este método muy eficaz para promover más caos, o para llevar a cabo robos u otras acciones nefastas. Por lo tanto, se debe estar atento al buscar malware de este tipo.

Y es así cómo comenzó 2018. Esperemos que 2019 no nos depare nada malicioso ni sofisticado para cualquier otro evento importante.



 Para una mirada más profunda sobre este tema, consulte:

<https://blog.talosintelligence.com/2018/02/olympic-destroyer.html>

<https://blog.talosintelligence.com/2018/02/who-wasnt-responsible-for-olympic.html>

<https://blog.talosintelligence.com/2018/12/year-in-malware-2018-most-prominent.html>

## Acerca de la Serie de Ciberseguridad de Cisco

A lo largo de la última década, Cisco ha publicado una gran cantidad de información crucial de seguridad e inteligencia de amenazas para profesionales de seguridad interesados en el estado de la ciberseguridad global. Estos informes exhaustivos proporcionan explicaciones detalladas de los panoramas de amenazas y las consecuencias para las organizaciones, así como mejores prácticas para defenderse frente a los efectos adversos de violaciones de datos.

En nuestro nuevo enfoque del liderazgo intelectual, la Seguridad de Cisco está realizando una serie de publicaciones basadas en investigaciones e impulsadas por datos bajo el banner **Serie de ciberseguridad de Cisco**. Hemos ampliado el número de títulos para incluir diversos informes para profesionales de seguridad con intereses diferentes. Invocando la amplitud y profundidad de conocimientos de los investigadores de amenazas e innovadores en el sector de seguridad, la recopilación de informes de la serie 2019 incluye el Reporte de referencia de privacidad de datos, el Reporte de amenazas, y el Reporte de referencia de CISOs, pero vendrán otros a lo largo del año.

Para más información, visite [www.cisco.com/mx/securityreports](http://www.cisco.com/mx/securityreports).

**Sede central en América**

Cisco Systems, Inc.  
San José, CA

**Sede central en Asia Pacifico**

Cisco Systems (USA), Pte. Ltd.  
Singapur

**Sede Central en Europa**

Cisco Systems International BV Amsterdam,  
Países Bajos

Cisco tiene más de 200 oficinas en todo el mundo. Las direcciones, y los números de teléfono y fax, están disponibles en el sitio web de Cisco en [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Publicado en febrero de 2019

THRT\_01\_0219\_r2

© 2019 Cisco y/o sus filiales. Todos los derechos reservados.

Cisco y el logotipo de Cisco son marcas registradas o marcas comerciales de Cisco y/o de sus filiales en los Estados Unidos y otros países. Para ver una lista de las marcas comerciales de Cisco, visite: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Todas las marcas comerciales registradas de terceros mencionadas en este documento pertenecen a sus respectivos propietarios. El uso de la palabra partner no implica una relación de asociación entre Cisco y cualquier otra empresa. (1110R)

Adobe, Acrobat y Flash son marcas comerciales registradas o marcas comerciales de Adobe Systems Incorporated en los Estados Unidos y/o en otros países.