Resumen de la solución

# Abuso de la confianza

**Aprovechándose de los más confiados.**

No en vano se afirma que la confianza hay que ganársela, y todos conocemos buenos ejemplos de ello. Por otra parte, lo que se tarda años en conseguir, se puede perder en cuestión de segundos. La confianza no se ha basado nunca en un modelo estático, y esto, ahora que la población de todo el mundo depende cada vez más de Internet, es incluso más notorio.

## ¿Qué es un abuso de la confianza?

En el **informe de McAfee sobre amenazas de noviembre de 2014** se analiza en profundidad en qué consiste el abuso de la confianza. En el mundo de Internet, asumimos que lo que vemos es de fiar, ya sea una aplicación descargada en un dispositivo móvil, un anuncio aparentemente sin malas intenciones en un sitio web conocido o un mensaje de correo electrónico de una empresa con la que mantenemos una relación comercial. Los agresores sacan partido de la confianza de diversas formas, aprovechándose principalmente de víctimas desprevenidas. Estos son algunos de los tipos de ataques que se abordan en el informe:

- **Publicidad engañosa:** cuando los anuncios inofensivos del sitio web de una empresa se convierten en la fuente de ataques a consumidores desprevenidos, estos se preguntan si quizás han sido demasiado confiados. **Las redes de publicidad maliciosa como "Kyle y Stan"** distribuyen malware a través de anuncios maliciosos en sitios web como amazon.com y youtube.com, así como a través de **redes importantes de publicidad como DoubleClick y Zedo**.
- **Malware firmado:** una táctica cada vez más común consiste en que los autores de malware adquieran certificados de una autoridad de certificación (CA) que intente sacar partido de la confianza de empresas establecidas o bien hacerse pasar por una empresa legítima. Los agresores se aprovechan de la confianza que no dudamos en depositar en las autoridades de certificación. Recientemente, una campaña de publicidad engañosa distribuyó variantes firmadas del troyano CryptoWall a través de la red publicitaria Zedo, que **supuestamente afectó a usuarios de los sitios web mejor puntuados por Alexa**. La firma digital que se concedió a "Trend" probablemente perseguía hacerse pasar por el proveedor de seguridad Trend Micro, lo que es un ejemplo claro de cómo se puede pecar de inocente al fiarse de lo que parece ser de confianza.
- **Aplicaciones falsificadas:** las marcas comerciales invierten una cantidad de tiempo y esfuerzo considerable en proteger a sus clientes de productos falsificados que pretenden sacar provecho de la sólida confianza que los consumidores han depositado en dichas marcas. Cuando las aplicaciones ofrecen funciones que no se limitan al mundo digital, no es de extrañar que los agresores más emprendedores hayan recurrido a la creación de aplicaciones clonadas a partir de programas legítimos y normalmente muy conocidos.

Durante el pasado trimestre, McAfee detectó a timadores intentando distribuir una aplicación que se hacía pasar por Adobe Flash Player 11. A juzgar por el recuento de descargas de la tienda Google Play y la telemetría de detección de McAfee Mobile Security, los timadores consiguieron su objetivo y engañaron a los usuarios para que descargasen su falsificación maliciosa.

- **Carga en DLL:** los delincuentes saben que si sus códigos maliciosos pueden subirse a una aplicación de confianza, la probabilidad de acertar con el ataque es mayor. El malware ha aprovechado esta circunstancia durante años mediante una técnica de ataque conocida como carga en DLL. Esta técnica consiste en ejecutar una aplicación legítima que, a su vez, ejecute el código de una biblioteca DLL. Los delincuentes diseñan su carga útil para que asuma la función de la biblioteca DLL externa, con lo que consiguen que la aplicación limpia ejecute el código malicioso.

  A lo largo del tercer trimestre, McAfee Labs observó ataques dirigidos a la aplicación Google Updater. La nueva variante de la familia de malware PlugX asume la función de la DLL goopdate.dll importada, pero la variante PlugX va más allá para ocultar sus acciones. El módulo goopdate.dll no es más que un intermediario que lee el contenido de un archivo de datos cifrado, goopdate.dll.mpa, lo descifra en la memoria y transfiere el control de ejecución a ese código malicioso.

- **Sistemas operativos y software de red:** son muchos los ejemplos de ataques en los que se abusa de la confianza dentro y entre los sistemas operativos y el software de red. En algunos ataques, se saca partido del software que establece conexiones seguras en Internet. Las aplicaciones desprevenidas confían en las conexiones que reciben por parte del sistema operativo, que, a su vez, confía en el software de red que, supuestamente, ha establecido conexiones seguras. En el caso de otros ataques, se aprovechan las vulnerabilidades de los sistemas operativos o el software de red. Con frecuencia, estos ataques sacan partido del software de código abierto incorporado en el sistema operativo o la pila de software de red.

  BERserk es una vulnerabilidad basada en la falsificación de firmas que **se ha dado a conocer recientemente** y que saca partido de la confianza depositada en el sistema operativo y el software de red. BERserk permite a usuarios malintencionados perpetrar ataques de intermediario (MITM) permitiéndoles falsificar firmas RSA y burlar la autenticación en los sitios web que emplean los protocolos SSL/TLS.

## Soluciones de McAfee

La tecnología de seguridad de McAfee ofrece protección frente a ataques que persiguen abusar de la confianza que su empresa ha depositado en sus operaciones diarias. A continuación, presentamos algunos de los productos de McAfee con los que su empresa podrá asegurarse de que ningún agresor saque partido de su modelo de confianza.

### McAfee Application Control

Proteger su empresa y sus aplicaciones legítimas frente a código malicioso como BERserk es fundamental. **McAfee Application Control** permite a su empresa controlar qué aplicaciones se pueden ejecutar en su entorno por medio de listas blancas dinámicas y directivas de implementación, tanto en los endpoints conectados como en los desconectados.

- **Listas blancas dinámicas:** permita que su organización administre de forma eficaz sus aplicaciones desarrollando de forma automática una lista blanca a medida que los sistemas se revisen con parches y se actualicen. McAfee Application Control reduce su exposición a BERserk al impedir que se ejecuten las aplicaciones que invocan código de verificación de firmas RSA vulnerable.

- **Reputación de archivos:** la integración con McAfee Global Threat Intelligence permite a McAfee Application Control consultar información en tiempo real sobre tipos de archivos conocidos, legítimos y maliciosos, y desconocidos para asegurarse de que su empresa esté al tanto de vulnerabilidades como BERserk.
- **Protección con conexión o sin ella:** implemente controles en los servidores conectados y desconectados, las máquinas virtuales, los endpoints y los dispositivos fijos, como los terminales punto de venta.

**McAfee Email Gateway**

Si un mensaje de correo electrónico recibido en la bandeja de entrada de un usuario es inofensivo o malicioso es algo que preocupa enormemente a las empresas. Los agresores hacen uso del phishing selectivo para atraer a víctimas desprevenidas y embaucarlas para que ellas mismas comprometan su seguridad por medio de malware incrustado o direcciones URL maliciosas. **McAfee Email Gateway** ofrece protección frente a este tipo de ataques con diversas funciones:

- **ClickProtect:** elimine las amenazas asociadas a las direcciones URL incrustadas en mensajes de correo electrónico analizando dichas direcciones URL en el mismo momento en que se hace clic en ellas. Esta inspección incluye la comprobación de la reputación de la dirección URL y la emulación proactiva del motor McAfee Gateway Anti-Malware Engine.
- **Integración con McAfee Advanced Threat Defense:** detecte malware sofisticado y evasivo con análisis de código estático en profundidad y análisis dinámicos de archivos sospechosos adjuntos a mensajes de correo electrónico, de manera que los archivos maliciosos no lleguen nunca a la bandeja de entrada.
- **Integración con McAfee Global Threat Intelligence:** combina información de la red local con datos de reputación de McAfee Global Threat Intelligence a fin de proporcionar el modelo más completo de protección frente a malware, spam y amenazas entrantes.

**McAfee Global Threat Intelligence**

**McAfee Global Threat Intelligence (GTI)** es un servicio de información sobre amenazas integral, en tiempo real y basado en la nube, que permite a los productos de McAfee bloquear las ciberamenazas procedentes de todos los vectores: archivos, la Web, mensajes y redes. Ofrece protección de forma proactiva frente al abuso de confianza por medio de las funciones siguientes:

- **Reputación de certificados:** consulte la información en tiempo real sobre certificados conocidos legítimos y maliciosos con el fin de proteger su empresa frente a amenazas, como el malware firmado, que se pueden distribuir por medio de redes de publicidad engañosa.
- **Reputación de archivos:** protéjase frente a aplicaciones falsificadas en el equipo de sobremesa y manténgase informado sobre qué aplicaciones pueden ser vulnerables a ataques como BERserk. Consulte información en tiempo real sobre archivos conocidos, legítimos y maliciosos, y desconocidos para permanecer protegido.
- **Inteligencia por medio de correlación de vectores:** recopile y correlacione datos de todos los vectores de amenazas principales (archivos, Web, correo electrónico y redes) para detectar amenazas combinadas, como las redes de publicidad que distribuyen malware firmado, los mensajes de correo electrónico de phishing selectivo de supuestas fuentes de confianza y las descargas inadvertidas alojadas en sitios web maliciosos o sitios web "de confianza" que se han visto comprometidos.
- **Security Connected:** implemente integraciones con otros productos de seguridad de McAfee para ofrecer la información sobre amenazas más amplia, la correlación de datos más profunda y la integración de productos más completa disponibles actualmente, y garantizar así una sólida protección frente a los ataques que abusan de la confianza.

## Resumen de la solución

**McAfee Vulnerability Manager**

Ataques como BERserk son ejemplos de las amenazas en constante cambio que afectan al modelo de confianza. Ser consciente de a qué riesgos está expuesto y el grado de vulnerabilidad ante estos nuevos ataques puede resultar una tarea abrumadora. A continuación, detallamos algunas de las formas en las que **McAfee Vulnerability Manager**, junto con **McAfee Asset Manager**, puede contribuir a que su empresa esté al tanto de vulnerabilidades como BERserk y tome las medidas necesarias para ponerles remedio de manera eficaz:

- **Análisis completo de vulnerabilidades:** McAfee Vulnerability Manager es un producto independiente y altamente escalable de descubrimiento de hosts, administración de activos, evaluación de vulnerabilidades y generación de informes en cualquier dispositivo conectado a la red. McAfee Vulnerability Manager comprueba la presencia de BERserk buscando sistemas que ejecuten versiones vulnerables de Firefox, Chrome y otros productos que invoquen código de verificación de firmas RSA vulnerable.
- **Análisis personalizados de nuevas amenazas:** el editor Foundstone Scripting Language (FSL) es capaz de ampliar las comprobaciones predefinidas y las actualizaciones para mejorar la detección de amenazas y vulnerabilidades zero-day, como BERserk, escribiendo secuencias de comandos personalizadas y comprobaciones para evaluar su entorno. McAfee Vulnerability Manager es capaz ahora de detectar sistemas vulnerables a BERserk en el marco de sus comprobaciones predefinidas a partir del 24 de septiembre de 2014.
- **Generación de informes y medidas correctivas de gran flexibilidad:** McAfee Vulnerability Manager y McAfee Asset Manager funcionan en colaboración para proporcionar una supervisión y una administración automatizadas de los análisis, las medidas correctivas, la implementación y la generación de informes. De esta manera, podrá evitar laboriosos simulacros de emergencia y procesos ad hoc, eliminar errores y proteger un mayor número de sistemas de forma más eficaz.
- **Información sobre su exposición:** McAfee Asset Manager permite a su empresa saber qué sistemas son vulnerables a BERserk mediante la correlación de análisis de vulnerabilidades con análisis de descubrimiento de hosts. La identificación en tiempo real de los sistemas que están ejecutando versiones vulnerables de las aplicaciones permite reducir el tiempo para saber si se corren riesgos, y disponer de más tiempo para aplicar medidas correctivas.

**McAfee Web Gateway**

La publicidad engañosa, las descargas inadvertidas y las direcciones URL maliciosas incrustadas son algunos de los métodos de ataque basados en el abuso de la confianza. **McAfee Web Gateway** impulsará la protección de su empresa frente a este tipo de amenazas.

- **McAfee Gateway Anti-Malware Engine:** el análisis de intenciones sin firma filtra el contenido malicioso del tráfico de la Web en tiempo real. La emulación y los análisis de comportamiento ofrecen protección de forma proactiva frente a los ataques selectivos y de tipo zero-day. McAfee Gateway Anti-Malware Engine inspecciona los archivos e impide que los usuarios los puedan descargar si son maliciosos. McAfee Web Gateway es la solución número uno del mercado gracias a su capacidad de bloquear las descargas de malware por medio de la función de inspección exclusiva de este motor.
- **Integración con McAfee GTI:** la información sobre la reputación de archivos, la reputación de la Web y la categorización de la Web de McAfee GTI ofrecen protección frente las últimas amenazas, ya que McAfee Web Gateway deniega los intentos de conexión a sitios web maliciosos o sitios web que hacen uso de redes de publicidad engañosa.

**McAfee SiteAdvisor® Enterprise**

Mantenerse en primera línea en un panorama con amenazas en constante cambio es todo un desafío, especialmente si se intenta proteger a los usuarios online frente a amenazas como el abuso de la confianza sin aplicar estrictas directivas que echen a perder la experiencia de usuario.

- **Identifique fácilmente amenazas como sitios web maliciosos que pretenden hacerse pasar por legítimos:** por medio de un intuitivo sistema de clasificación por colores, **McAfee SiteAdvisor Enterprise** proporciona un nivel adicional de protección en el escritorio. McAfee SiteAdvisor Enterprise deniega las conexiones a sitios web maliciosos conocidos e informa a los usuarios de estos peligros.
- **Seguridad mejorada con la tecnología de McAfee GTI:** McAfee GTI proporciona información sobre amenazas en tiempo real a McAfee SiteAdvisor Enterprise para que este evalúe los sitios web basándose en los datos más actualizados.

**McAfee Threat Intelligence Exchange**

El abuso de la confianza puede darse de diversas formas, así que es esencial disponer de una plataforma inteligente que se adapte a medida que pasa el tiempo para ser capaz de responder a las necesidades de su entorno. **McAfee Threat Intelligence Exchange (TIE)** reduce significativamente la exposición a los ataques gracias a la visibilidad de las amenazas que proporciona, lo que permite, por ejemplo, detectar certificados maliciosos en su entorno.

- **Reputación de certificados:** la integración con McAfee GTI permite a su empresa protegerse en tiempo real frente a ataques que aprovechan de código malicioso firmado consultando información en tiempo real sobre certificados conocidos legítimos y maliciosos. McAfee TIE puede proteger sus endpoints frente a certificados maliciosos por medio de directivas administradas de forma centralizada que se pueden implementar de manera que ofrezcan protección para los endpoints conectados y desconectados.
- **Rechace las cargas en DLL, las aplicaciones falsificadas y otros tipos de ataque:** la avanzada tecnología de protección de endpoints decide si un archivo se puede ejecutar con una lógica basada en reglas que combina el contexto de los endpoints (atributos de archivo, proceso y entorno) con la información colectiva sobre amenazas.
- **Indicadores de peligro:** importe hashes de archivos maliciosos conocidos y certificados maliciosos conocidos en McAfee TIE para inmunizar su entorno contra ellos, por medio de la implementación de directivas. Si se activa alguno de los indicadores de peligro en el entorno, McAfee TIE puede eliminar todos los procesos y las aplicaciones asociados.

**McAfee VirusScan® Mobile Security**

- **Evite las aplicaciones falsificadas:** con el respaldo de McAfee GTI, **McAfee VirusScan Mobile Security** es capaz de frustrar los ataques de aplicaciones falsificadas que contienen malware prácticamente en tiempo real. Puede detectar malware en menos de 200 milésimas de segundo sin interrumpir la conectividad ni las operaciones inalámbricas.

Proteger su empresa frente al enemigo que pretende sacar provecho de este modelo de confianza dinámico puede ser una tarea de enormes proporciones. La tecnología de seguridad de McAfee permite a su empresa protegerse de forma proactiva frente a ataques que persiguen abusar de la confianza de los usuarios.



**McAfee. Part of Intel Security.**
Avenida de Bruselas n.º 22
Edificio Sauce
28108 Alcobendas
Madrid, España
Teléfono: +34 91 347 8500
www.intelsecurity.com