McAfee
Together is power.

Proteja los dispositivos IoT para prevenir ataques

El ataque de denegación de servicio distribuido (DDoS) perpetrado con éxito en octubre de 2016 contra la infraestructura de servicios DNS gestionados de Dyn fue objeto de un profundo análisis en el *Informe de McAfee Labs sobre amenazas de abril de 2017*.

El ataque se efectuó utilizando el protocolo DNS, lo que hace extremadamente difícil que la tecnología de seguridad distinga el tráfico legítimo del hostil. Para agravar el problema, tanto el ataque como el tráfico legítimo procedían de millones de direcciones IP de todo el mundo.

Este tipo de ataque DDoS está en aumento debido a la seguridad deficiente de la infraestructura del Internet de las cosas (IoT). El malware Mirai empleado en el ataque a Dyn hizo uso de una amplia variedad de dispositivos IoT mal protegidos, como videograbadoras, impresoras, cámaras de vigilancia, frigoríficos, termostatos, etc. Tras infectar un dispositivo IoT, el malware extendió la infección a otros dispositivos IoT hasta formar una "red de bots" y después utilizó la capacidad de proceso conjunta para ejecutar el ataque DDoS.

Según el equipo de seguridad de Dyn, en el momento álgido del ataque la red de bots de Mirai estaba formada por decenas de millones de dispositivos IoT maliciosos.

No es fácil averiguar si un dispositivo de la red está infectado ni en qué fase de infección se encuentra, es decir, si está en las etapas iniciales de detonación del código, desplazamiento lateral y comunicación con el servidor de control o en la de captación de redes de bots para ataques DDoS coordinados. Sin embargo, para proteger los dispositivos IoT y salvaguardar la red de confianza pueden seguirse algunas recomendaciones de seguridad.

Cómo proteger los dispositivos IoT

Para hacerse con el control de los dispositivos IoT, los agresores toman la vía que ofrece menos resistencia, normalmente a través de las credenciales poco seguras, pero saben adaptarse ante las credenciales sólidas y otros controles de seguridad. Este es el patrón que hemos visto en muchos vectores de ataque.

McAfee recomienda bloquear los exploits conocidos y las posibles estratagemas futuras de los agresores. Adopte estas tres medidas para proteger los dispositivos IoT desde su fabricación hasta su baja:

Protección de dispositivos IoT

1. Diseñe los dispositivos IoT pensando en la seguridad.

Los fabricantes de dispositivos IoT deben incorporar la seguridad en la arquitectura, la interfaz y el diseño de sus productos. Establezca y pruebe los conceptos y las funciones de seguridad básicos, como la compartimentación de datos y código, la comunicación entre interlocutores de confianza, la protección de datos en uso y en reposo, y la autenticación de usuarios. En el futuro los productos serán más potentes, almacenarán más datos y tendrán más funciones. Esto significa que deberán ofrecer actualizaciones de seguridad, bloqueo de funciones, validación de compilaciones, examen del software y configuraciones predeterminadas conforme a las mejores prácticas del sector.

Todo empieza con el fabricante: la garantía de futuro comienza en los cimientos. El hardware, el firmware, los sistemas operativos y el software deben estar diseñados para adentrarse en un entorno hostil y sobrevivir. Los compradores de dispositivos IoT deben tenerlo en cuenta a la hora de considerar una posible compra. ¿Ha diseñado y desarrollado el fabricante el dispositivo IoT pensando en la seguridad?

2. Aprovisione y configure con seguridad.

La mayoría de los dispositivos IoT requieren algún tipo de configuración y aprovisionamiento durante la instalación. La identificación y la autenticación del dispositivo son una parte fundamental de este proceso de dos etapas. Es importante que la configuración predeterminada sea correcta, que siga las mejores prácticas de seguridad y que resulte fácil de entender para los usuarios. Las normas de uso no deben autorizar contraseñas predeterminadas, pero sí exigir que los parches y las actualizaciones lleven firma, que los datos estén cifrados y que se utilicen únicamente conexiones web seguras. En una empresa, para mantener seguros los dispositivos IoT puede ser de gran ayuda limitar el acceso a la red, instalar parches cuando corresponde y solo permitir que se ejecute software autorizado. En los aparatos que lo permitan, el nivel defensivo mejora si se implementa software de seguridad, como programas antimalware, sistemas de prevención de intrusiones e incluso firewalls locales. También deben configurarse funciones de detección y telemetría para detectar si los sistemas son víctimas de un ataque o funcionan de formas no previstas en la organización. Deben definirse políticas de privacidad, retención de datos, acceso remoto, seguridad de claves y procedimientos de revocación.

3. Aplique procedimientos correctos de gestión y administración.

Cuando un dispositivo es propiedad de un consumidor, es este quien debe tener la última palabra sobre cómo gestionarlo. Los fabricantes y los proveedores de servicios online participan en el aprovisionamiento, pero el propietario debe conservar el control sobre el uso que se le dará al dispositivo. Aprovisionar no significa administrar. Por ejemplo, durante la instalación de cámaras domésticas es normal conectar con el fabricante para instalar los últimos parches y quizá incluso configurar el almacenamiento en la nube. Pero ningún cliente quiere que el fabricante controle sus cámaras. Este no debe tener la posibilidad de manejar los dispositivos sin la autorización del comprador. El propietario debe conservar la facultad de activar y desactivar sus productos y de elegir los servicios online autorizados a conectarse. Esta facultad exige la correcta identificación y autenticación del usuario. No es recomendable utilizar una contraseña predeterminada común porque cualquiera puede actuar como administrador. Imagine que Microsoft Windows se distribuyera con una contraseña de inicio de sesión predeterminada para todos los sistemas.

Sería una pesadilla para la seguridad, porque muchos usuarios no la cambiarían nunca y los agresores podrían iniciar sesión como usuario. En primer lugar, los sistemas IoT deben ser capaces de autenticar a su propietario. Las funciones de gestión también ampliarse para permitir que este defina límites, directivas de datos y parámetros de privacidad que sean más restrictivos que los de cualquier otro posible proveedor. Deben instalarse en cuanto estén disponibles todas las actualizaciones de seguridad con firma. Si el propietario es hábil, puede configurar límites para conexiones entrantes y salientes, tipos de datos, puertos y parámetros de seguridad. Los errores y las actividades imprevistas e inusuales deben captarse en registros que puedan enviarse a un sistema de confianza o visualizarse de forma local. En algunos dispositivos es de agradecer la presencia de un sistema de notificaciones de advertencia remota por correo electrónico o SMS. Por último, hace falta una función de reinicio en caso de ataque irrecuperable o transferencia de la propiedad.

Directivas y procedimientos eficaces para proteger los dispositivos IoT

- **Investigue el historial de seguridad del dispositivo IoT.** Antes de comprar un dispositivo IoT, compruebe si el aparato o la empresa que lo ofrece han tenido problemas. Basta con una rápida búsqueda en Internet. Si busca en el sitio web de la Comisión Federal de Comercio de Estados Unidos, averiguará si las fuerzas de seguridad han intervenido en el pasado. Tras una investigación básica, probablemente descubrirá que hay empresas que ignoran los problemas de seguridad, mientras que habrá otras que son más proactivas.
- **Mantenga actualizado el software de todos los dispositivos IoT.** A menudo esta sencilla práctica puede eliminar vulnerabilidades, especialmente las descubiertas y hechas públicas recientemente. Establezca un procedimiento de aplicación de parches y compruebe que los parches se han aplicado correctamente.
- **Para los dispositivos IoT en los que no se pueden aplicar parches, debe reducir los riesgos.** Para ello, utilice listas blancas de aplicaciones que protegen los sistemas y evitan la ejecución de programas no aprobados.
- **Separe estos sistemas y dispositivos de otras partes de la red** mediante un firewall o un sistema de prevención de intrusiones. Desactive los servicios o puertos no necesarios en estos sistemas para reducir la exposición a posibles puntos de entrada de infecciones. Mirai aprovecha los puertos que no se utilizan.
- **Cambie las contraseñas predeterminadas y utilice contraseñas seguras.** El empleo de contraseñas predeterminadas que no son lo bastante seguras es la principal amenaza para los dispositivos IoT. Adopte buenos hábitos para las contraseñas, como utilizar frases largas, caracteres especiales, mayúsculas y minúsculas, y números. Las contraseñas deben ser seguras y difíciles de adivinar.

- **Aproveche la configuración de seguridad de los dispositivos IoT.** Algunos de ellos ofrecen configuraciones avanzadas y debe sacarles el máximo provecho. Es posible que algunos productos IoT ofrezcan conexiones de red independientes además de la conexión principal, como una red Wi-Fi para invitados. Es solo una función, puede que otros productos ofrezcan otras.
- **Conecte los dispositivos IoT a una Wi-Fi segura.** Cree contraseñas seguras y utilice los últimos protocolos de seguridad, como WPA2.
- **Restrinja el acceso físico a los dispositivos IoT.** La manipulación directa del dispositivo IoT también puede favorecer los ataques.
- **Desactive la función Universal Plug and Play (UPNP).** Muchos dispositivos IoT admiten UPnP, lo que permite que el dispositivo se localice en Internet y esté expuesto a las infecciones de malware. Desactive esta opción cuando sea posible.
- **Reinicie los dispositivos IoT periódicamente.** El malware suele almacenarse en una memoria volátil y puede borrarse apagando el dispositivo y volviendo a encenderlo.

Cómo protege McAfee los sistemas y redes frente a ataques a dispositivos IoT

Además de la lista anterior de buenas prácticas que resultan útiles con dispositivos IoT, los productos de McAfee pueden contribuir a reducir el riesgo de infección de malware en estos dispositivos y bloquear actividades maliciosas de redes de bots. Las siguientes configuraciones de productos de McAfee pueden ayudar a salvaguardar los dispositivos IoT y a proteger sistemas y redes de ataques procedentes de estos dispositivos:

McAfee VirusScan® Enterprise 8.8 o McAfee Endpoint Security 10

- Mantenga actualizados los archivos DAT.
- Utilice **McAfee Global Threat Intelligence** (McAfee GTI), que contiene más de 600 millones de firmas de malware diferentes.
- Elabore reglas de protección de acceso para detener la instalación y las cargas útiles del malware:
  - Consulte los siguientes artículos sobre reglas de protección de acceso en la base de conocimientos: **KB81095** y **KB54812**.
  - Consulte las mejores prácticas de configuración para McAfee VirusScan Enterprise 8.8: **PD22940**.
  - Consulte las mejores prácticas de configuración para McAfee Endpoint Security: **KB86704**.

McAfee Host Intrusion Prevention

- McAfee Host Intrusion Prevention ayuda a prevenir la propagación del malware. Mediante el uso de firmas IPS personalizadas, puede crear reglas para prevenir las operaciones con archivos generadas por malware (creación, escritura, ejecución, lectura, etc.).
- Active la firma de McAfee Host Intrusion Prevention 3894: "Access Protection—Prevent svchost.exe executing non-Windows executables" (Protección de acceso: impedir que svchost.exe ejecute archivos ejecutables que no son de Windows).

- Active las firmas de McAfee Host Intrusion Prevention 6010 y 6011 para bloquear la inyección de forma inmediata.
- Para ello, hay dos tipos de reglas secundarias:
  - 1) Cree una firma IPS personalizada mediante el motor de Files y una regla secundaria con los siguientes criterios:
    - Name: <insertar nombre>
    - Rule type: Files
    - Operations: Create, Execute, Read, Write
    - Parameters: Include - Files - <ruta/nombre de archivo del malware>
      - El nombre de archivo debe incluir la ruta. Si desea utilizar caracteres comodín en la ruta, comience el nombre de archivo por "**\" o "?:\" para utilizar un carácter comodín para la letra de unidad (por ejemplo: "**\nombrearchivo.exe" o "?:\nombrearchivo.exe").
      - No puede utilizar hashes MD5 con el parámetro "Files", solo ruta/nombrearchivo.
      - También puede utilizar el tipo de unidad para limitar la ruta a una unidad específica (por ejemplo, el disco duro, CD, USB, la red o un disquete).
    - Executables: se puede dejar vacío a menos que desee limitar la firma a procesos específicos para realizar operaciones con archivos (por ejemplo, explorer.exe, cmd.exe, etc.).
  - 2) Cree una firma IPS personalizada mediante el motor de Program y una regla secundaria con los siguientes criterios:
    - Name: <insertar nombre>
    - Rule type: Programa
    - Operations: Run target executable
    - Parameters: <dejar en blanco>
    - Executables: se puede dejar vacío a menos que desee limitar la firma a un proceso específico como el ejecutable de origen (por ejemplo, para evitar que explorer.exe ejecute un ejecutable de destino (Target Executable) (como notepad.exe)).
    - Target Executables: defina las propiedades de los ejecutables cuya ejecución desea evitar (por ejemplo, si quiere evitar la ejecución de notepad.exe, especifique la ruta/nombre de archivo del ejecutable). El ejecutable puede definirse mediante uno o varios de los criterios (descripción de archivo, nombre de archivo, huella dactilar, firma).

McAfee SiteAdvisor® Enterprise o McAfee Web Protection

- Utilice las reputaciones de sitios web para impedir el uso o advertir a los usuarios de sitios web que distribuyen malware.

McAfee Threat Intelligence Exchange y McAfee Advanced Threat Defense

- Configuración de directivas de McAfee Threat Intelligence Exchange:
  - Comience en modo de observación: a medida que se descubran procesos sospechosos en los endpoints, utilice etiquetas del sistema para aplicar las directivas de implementación de McAfee Threat Intelligence Exchange.
  - Limpiar si el nivel es Known Malicious (Malicioso conocido).
  - Bloquear si el nivel es Most likely malicious (Probablemente malicioso) (bloquear si el nivel es Unknown [Desconocido] aumentaría la protección, pero quizá también añadiría más carga de trabajo administrativo).
  - Submit files to McAfee Advanced Threat Defense (Enviar archivos a McAfee Advanced Threat Defense) si el nivel es Unknown (Desconocido) e inferiores.
  - Directiva de Threat Intelligence Exchange Server: aceptar reputaciones de McAfee Advanced Threat Defense de archivos que McAfee Threat Intelligence Exchange aún no haya visto.
- Intervención manual de McAfee Threat Intelligence Exchange:
  - Implementación de la reputación de archivos (según el modo operativo). Most Likely Malicious (Probablemente malicioso): limpiar/eliminar.
  - Might be Malicious (Posiblemente malicioso): bloquear.
- La reputación de la empresa (organización) puede reemplazar la de McAfee GTI:
  - Puede optar por bloquear procesos no deseados, por ejemplo, una aplicación no admitida o vulnerable.
  - Marque el archivo como Might be Malicious (Posiblemente malicioso).
- O bien, puede autorizar un proceso no deseado para probar:
  - Marque el archivo como Might be Trusted (Posiblemente de confianza).

McAfee Advanced Threat Defense

- Funciones de detección:
  - Detección basada en firmas: McAfee GTI contiene más de 600 millones de firmas.
  - Detección basada en reputación: McAfee GTI.
  - Emulación y análisis estático en tiempo real: utilizados para la detección sin firmas.
  - Reglas YARA personalizadas.
  - Análisis del código completamente estático: revierte la ingeniería del código de los archivos con el fin de evaluar todos los atributos y conjuntos de funciones, y analizar íntegramente el código fuente sin ejecutarlo.
  - Análisis dinámico en entornos aislados.
- Creación de perfiles de analizador donde es probable que se ejecute el ransomware:
  - Sistemas operativos habituales, Windows 7, Windows 8, Windows 10.

  - Instalación de aplicaciones Windows (Word, Excel) y activación de macros.
- Concesión de acceso a Internet al perfil de analizador:
  - Numerosas muestras ejecutan una secuencia de comandos de un documento de Microsoft que establece una conexión saliente y activa el malware. Al proporcionar conexión a Internet al perfil de analizador aumentan las tasas de detección.

McAfee Network Security Platform

- McAfee Network Security Platform también tiene firmas en sus directivas predeterminadas para identificar la red TOR, que puede utilizarse para transferir archivos relacionados con malware.
- Integración con McAfee Advanced Threat Defense para nuevas variantes de ataques:
  - Configure la integración con McAfee Advanced Threat Defense en una directiva de malware avanzado.
  - Configure McAfee Network Security Platform para enviar archivos .exe, de Microsoft Office, Java Archive y PDF a McAfee Advanced Threat Protection para su inspección.
  - Verifique que la configuración de McAfee Advanced Threat Protection se aplica a nivel de sensor.
- Actualice las reglas de detección de devoluciones de llamadas (para luchar contra las redes de bots).

McAfee Web Gateway

- Active la inspección antimalware de McAfee Web Gateway.
- Active McAfee GTI para conocer la reputación de URL y archivos.
- Integración con McAfee Advanced Threat Defense para la detección de amenazas de tipo zero-day y el uso de entornos aislados.

VirusTotal Convicter: intervención automatizada

- Convicter es una secuencia de comandos Python que activa el sistema de respuesta automática de McAfee ePolicy Orchestrator® (McAfee ePO™) para contrastar con VirusTotal los archivos que generan eventos de amenazas en McAfee Threat Intelligence Exchange.
- Es posible modificar la secuencia de comandos para incluir otros sistemas de intercambio de información sobre amenazas, como GetSusp.
- Si se alcanza el umbral de confianza de la comunidad, la secuencia de comandos establece automáticamente la reputación de la empresa. Umbral recomendado de identificación como malicioso: deben estar de acuerdo el 30 % de los proveedores y dos grandes compañías.
- Filtro: "Target File Name Does Not Contain (El nombre de archivo seleccionado no contiene): McAfeeTestSample.exe".
- Esta es una herramienta gratuita que financia la comunidad (no McAfee).

McAfee Endpoint Threat Defense and Response

- McAfee Endpoint Threat Defense and Response detecta y responde a las amenazas avanzadas. Cuando se utiliza junto a la información sobre amenazas que suministran McAfee GTI, Dell SecureWorks o ThreatConnect, es posible buscar y eliminar amenazas nuevas antes de que tengan oportunidad de propagarse.
- Los recopiladores personalizados permiten crear herramientas específicas para buscar e identificar indicadores de peligro asociados al malware.
- El usuario crea desencadenadores y reacciones para definir acciones cuando se cumplen determinadas condiciones. Por ejemplo, cuando se encuentran hashes o nombres de archivo, puede emprenderse automáticamente una acción de eliminación.

Para ampliar la información

Informe: ***More Confidence, Safety, and Security in the Digital World*** (Más confianza, seguridad y protección en el mundo digital)

Best practices for how to use Host IPS rules for a malware outbreak (Mejores prácticas sobre el uso de reglas de McAfee Host Intrusion Prevention en caso de brote de malware): **KB84507**

Organización de SIEM. How McAfee Enterprise Security Manager can drive action, automate remediation, and increase situational awareness (Cómo puede McAfee Enterprise Security Manager impulsar la acción, automatizar la corrección e incrementar el conocimiento de la situación): **PD24830**

Informe: **Seguridad más allá de las firmas**

Preguntas frecuentes sobre McAfee Network Security Platform. Detección de malware avanzado: **KB75269**

Guía del producto de McAfee Web Gateway. Filtrado web: **PD26339**

McAfee
Together is power.

Avenida de Bruselas nº 22
Edificio Sauce
28108 Alcobendas, Madrid, España
+34 91 347 85 00
www.mcafee.com/es