Neutralización de los troyanos de puerta trasera

La herramienta de administración remota (RAT) conocida como Adwind es un troyano de puerta trasera basado en Java que ataca varias plataformas que admiten archivos Java. Adwind no aprovecha ninguna vulnerabilidad. Lo más normal para que se produzca una infección es que el usuario tenga que ejecutar el malware haciendo doble clic en el archivo .jar que suele enviarse adjunto a un mensaje de correo electrónico, o abrir un documento infectado de Microsoft Word. La infección se inicia si el usuario tiene instalado Java Runtime Environment. Una vez que el archivo .jar malicioso se ejecuta correctamente en el sistema objetivo, el malware se instala inadvertidamente y se conecta a un servidor remoto a través de un puerto previamente configurado para recibir comandos del agresor remoto y llevar a cabo actividades maliciosas.

Una breve introducción

Adwind es una evolución de la herramienta de administración remota Frutas. Frutas es una herramienta de administración remota basada en Java que se descubrió a principios de 2013 y que se ha utilizado de forma generalizada en campañas de correo electrónico de phishing contra empresas destacadas de telecomunicaciones, minería, sector público y finanzas de Europa y Asia.

Desde el inicio del primer trimestre de 2015, McAfee® Labs ha observado un aumento significativo de envíos de archivos .jar identificados como Adwind.

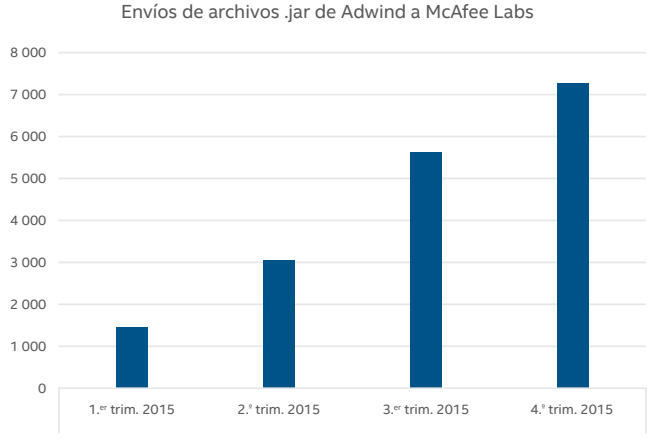

Figura 1. El número de envíos de archivos .jar de Adwind a McAfee Labs ha aumentado hasta los 7295 en el 4.º trimestre de 2015 respecto a los 1388 del 1.er trimestre de ese año, un aumento del 426 %.

intel Security

Cadena de infección

Adwind se propaga normalmente a través de campañas de spam que emplean adjuntos de correo electrónico cargados de malware, páginas web infectadas y descargas desapercibidas. Su mecanismo de distribución ha evolucionado: al principio, las campañas de spam duraban días y semanas, y utilizaban el mismo asunto de correo electrónico o nombre de archivo adjunto. Este uso sistemático ayudaba a los proveedores de seguridad a detectar y mitigar rápidamente Adwind. Sin embargo, ahora las campañas de spam tienen poca duración, los asuntos cambian con frecuencia y los archivos adjuntos están especialmente diseñados con el fin de evitar la detección.

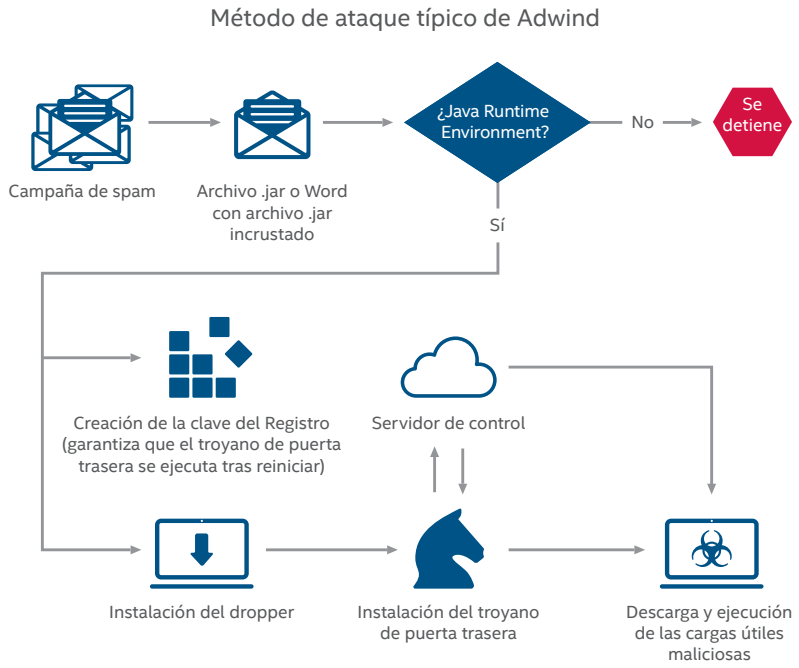

Figura 2. La cadena de infección de Adwind.

Una vez que Adwind consigue infectar un sistema, sabemos que es capaz de registrar pulsaciones de teclas, modificar y eliminar archivos, descargar y ejecutar más malware, realizar capturas de pantalla, acceder a la cámara del sistema, controlar el ratón y el teclado, actualizarse, y otras muchas operaciones.

Cómo ayuda Intel Security en la protección contra Adwind y otros troyanos de puerta trasera

La tecnología de Intel Security facilita la protección contra troyanos de puerta trasera como Adwind. Estos son algunos de los productos que permiten detener este tipo de ataque.

McAfee® Threat Intelligence Exchange

Es importante disponer de una plataforma inteligente que pueda adaptarse a medida que pasa el tiempo para responder a las necesidades del entorno. **McAfee Threat Intelligence Exchange** reduce significativamente la exposición a los troyanos de puerta trasera, gracias a que ofrece visibilidad de las amenazas inmediatas, como archivos o aplicaciones desconocidos que intentan ejecutarse en el entorno.

- **Información integral sobre amenazas:** combine fácilmente la información exhaustiva sobre amenazas que recibe de las fuentes de datos globales. Pueden ser datos de **McAfee Global Threat Intelligence** (McAfee GTI) o aportaciones de terceros, con la información local sobre amenazas procedente de los eventos en tiempo real y los datos históricos recibidos de endpoints, gateways y otros componentes de seguridad.
- **Prevención de ejecución y medidas correctivas:** McAfee Threat Intelligence Exchange puede intervenir para impedir la ejecución de aplicaciones desconocidas en el entorno. Si se descubre que una aplicación cuya ejecución estaba autorizada es maliciosa, McAfee Threat Intelligence Exchange puede desactivar en todo el entorno los procesos en ejecución asociados a dicha aplicación, gracias a sus potentes funciones de administración centralizada e implementación de directivas.
- **Visibilidad:** McAfee Threat Intelligence Exchange puede realizar un seguimiento de todos los archivos ejecutables empaquetados y de su ejecución inicial en el entorno, así como de todos los cambios que se produzcan a partir de ahí. Gracias a este grado de visibilidad de las operaciones de una aplicación o un proceso desde la instalación inicial hasta el momento actual, la respuesta y la resolución pueden ser más rápidas.
- **Indicadores de peligro:** importe hashes de archivos maliciosos conocidos e inmunice su entorno contra estos archivos mediante la implementación de las directivas adecuadas. Si se activa alguno de los indicadores en el entorno, McAfee Threat Intelligence Exchange puede eliminar todos los procesos y las aplicaciones asociados a él.

McAfee Advanced Threat Defense

McAfee Advanced Threat Defense es un producto de detección de malware multicapa que combina varios motores de inspección. Los motores realizan una inspección basada en firmas y reputación, una emulación en tiempo real, análisis del código completamente estático y utilizan entornos aislados dinámicos con objetos sospechosos con el fin de proteger frente al malware que deposita un archivo binario en el sistema de la víctima.

- **Detección basada en firmas:** detecta virus, gusanos, spyware, bots, troyanos, ataques por desbordamiento del búfer y ataques combinados. Su exhaustiva base de conocimientos ha sido creada por McAfee Labs, que también se ocupa de su mantenimiento.
- **Detección basada en la reputación:** consulta la reputación de los archivos utilizando McAfee GTI para detectar las amenazas de nueva aparición.
- **Análisis y emulación estáticos en tiempo real:** proporciona emulación y análisis estático en tiempo real para localizar rápidamente los troyanos de puerta trasera y las amenazas de tipo zero-day no identificadas, mediante técnicas basadas en firmas o en la reputación.
- **Análisis del código completamente estático:** revierte la ingeniería del código de los archivos con el fin de evaluar todos sus atributos y conjuntos de instrucciones, y analiza íntegramente el código fuente sin ejecutarlo. Sus completas funciones de descompresión abren todo tipo de archivos empaquetados y comprimidos para facilitar su análisis total y la clasificación del malware, de manera que su empresa pueda entender la amenaza que supone dicho malware.
- **Análisis dinámico en entornos aislados:** con los archivos cuya seguridad no puede determinarse mediante los motores de inspección mencionados, McAfee Advanced Threat Defense puede ejecutar el código en un entorno virtual de tiempo de ejecución y observar cómo se comporta. Los entornos virtuales pueden configurarse como los entornos de host. McAfee Advanced Threat Defense admite imágenes personalizadas de los sistemas operativos Microsoft Windows XP (de 32 y 64 bits), Windows 7 (de 32 y 64 bits), Windows 8 (de 32 y 64 bits), Windows Server 2003, Windows Server 2008 (de 64 bits) y Android.

McAfee Network Security Platform

McAfee Network Security Platform es una solución de seguridad exclusiva que descubre y bloquea las amenazas sofisticadas en las redes. Gracias a sus técnicas avanzadas de detección y emulación, va más allá de la comparación con patrones para ofrecer protección contra los ataques ocultos con extremada precisión. Nuestra estrategia de administración de la seguridad simplifica las operaciones de seguridad al combinar la información en tiempo real de McAfee GTI y los datos contextuales completos sobre usuarios, dispositivos y aplicaciones, con el fin de responder de manera rápida y precisa a los ataques que se propagan por la red.

- **Protección sin firmas:** las amenazas avanzadas y desconocidas, como el malware oculto, las amenazas persistentes avanzadas, los bots y los ataques de tipo zero-day, a menudo evaden las protecciones basadas en firmas. McAfee Network Security Platform tiene varios motores avanzados que no requieren firmas para proteger frente a estas amenazas avanzadas y desconocidas. La detección sin firmas analiza el contenido web, los archivos PDF, los archivos Flash y el comportamiento de JavaScript casi en tiempo real mediante el uso de emulación.
- **Endpoint Intelligence Agent:** McAfee Network Security Platform proporciona correlación del tráfico de los endpoints en tiempo real y por flujo. El agente combina el análisis del tráfico de red basado en comportamientos con varias fuentes de información sobre reputación. Esta tecnología hace uso de la información disponible en la red y en cada host Windows para revelar las relaciones entre los ejecutables que hay en los endpoints y los flujos de tráfico de la red con el fin de identificar las conexiones y los ejecutables maliciosos de la red en tiempo real. El agente incorpora contexto detallado de los procesos de los ataques, bloquea las comunicaciones maliciosas, evita la propagación del malware avanzado y, por último, pone en cuarentena y da solución a los sistemas host atacados.

McAfee Web Gateway

Algunos de los principales métodos para distribuir troyanos de puerta trasera son la publicidad engañosa, las descargas secundarias y las URL maliciosas incorporadas en mensajes de correo electrónico de phishing. **McAfee Web Gateway** es un producto robusto que mejorará significativamente la protección de su empresa frente a este tipo de amenazas.

- **McAfee Gateway Anti-Malware Engine:** el análisis de intenciones sin firmas 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.
- **Integración con McAfee GTI:** la información en tiempo real sobre la reputación de archivos, la reputación de la Web y la categorización de la Web de McAfee GTI ofrecen protección frente a las últimas amenazas, ya que McAfee Web Gateway deniega los intentos de conexión a sitios web maliciosos o sitios web conocidos por actuar como servidores de control.

Además de estos productos de Intel Security, recomendamos una clase más de tecnología de seguridad.

- **Seguridad del gateway de correo electrónico:** la mayor parte de los troyanos de puerta trasera entran en el sistema a través de los adjuntos a mensajes de correo electrónico, por lo que cualquier buena defensa frente a este tipo de ataque debe contar con un producto robusto de seguridad del gateway de correo electrónico que analice los adjuntos para detectar malware.

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