Resumen de la solución

La "troyanización" del software legítimo

Evite las infecciones y limite la propagación con los productos de Intel® Security

La distribución del software a través de Internet emplea mecanismos que podrían convertirse en vectores de ataque de malware y virus. Hay una clara evolución desde los archivos ***binder*** maliciosos que se empleaban hace una década hasta los avanzados métodos de distribución actuales que utilizan software legítimo "troyanizado" previamente o durante la fase de distribución.

Independientemente del nivel de sofisticación de un troyano, los pasos fundamentales son los mismos:

- Adaptación del software para añadirle poder destructivo: inserción de malware en una aplicación que se va a distribuir.
- Distribución: transmisión del software "troyanizado" no detectado al objetivo del ataque.
- Ataque: activación del código del troyano e intento de evitar la detección.
- Instalación: establecimiento de la persistencia e intento de desplazamiento lateral.

La técnica de ataque más innovadora se basa en un sofisticado mecanismo que actúa de manera inmediata inyectando código en una descarga legítima con el fin de evitar la detección. El ataque se basa en fusionar la aplicación original y el código malicioso.

Esta técnica de ataque podría utilizar dos componentes para localizar un punto de acceso al objetivo: un agente de escucha que capta y modifica la solicitud de descarga HTTP y un enlazador (o *binder*) que infecta y distribuye los archivos binarios.

Los algoritmos actuales despliegan las rutinas de infección del malware y los ataques de redirección de red sin modificar el código de la aplicación. De esta forma abren la puerta al software comercial o de código abierto que ha sido adaptado con función destructiva, y permiten incluir archivos ejecutables con una firma incrustada. El ataque triunfará si la firma no se verifica de manera automática y completa antes del intento de ejecución inicial.

Una vez que la aplicación troyanizada se ha ejecutado en la víctima, un proceso de enlace (*binder*) crea su propio archivo para otros ejecutables incrustados en los que se reconstruye todo el código inyectado para su posterior ejecución, superando así todos los controles de seguridad. La aplicación original permanece intacta, por lo que el malware se puede anexar a cualquier archivo con cualquier firma, y siempre funcionará.

intel Security

Políticas y procedimientos

Las últimas mejores prácticas de ciberdefensa de Intel Security recomiendan la adopción de determinadas estrategias de mitigación de amenazas generales para redes y endpoints:

- Utilizar una red privada virtual para conectarse a una red no segura. Los administradores deben mantener actualizado el software de seguridad y confiar solo en indicadores claros de confianza, y no en los que han podido ser falsificados en un ataque. Las aplicaciones deben firmarse y verificarse con una cadena de confianza. Los análisis forenses deben incluir la correlación de hashes con fuentes de confianza.
- El software de seguridad debe incluir análisis dinámicos para detectar acciones no fiables con independencia de la inspección de archivos binarios inicial, que es lo máximo que permite el análisis estático. Una solución completa debe incluir funciones de supervisión del comportamiento, reputación web y de direcciones IP, análisis de la memoria y contención de aplicaciones.
- En las descargas de software de proveedores deben utilizarse únicamente conexiones seguras y todo el código debe ir firmado. Esto reduce drásticamente los ataques de intermediario. Los proveedores de software deben incluir la autovalidación en sus aplicaciones, auditar regularmente el código, utilizar herramientas de análisis de código estático y someterse a revisiones independientes. Es siempre recomendable tener un repositorio centralizado de aplicaciones empresariales de confianza y solamente permitir a los usuarios descargar los instaladores aprobados que estén en este repositorio.
- Debe configurarse un software antimalware para identificar la presencia de *binders*.
- Se deben utilizar aplicaciones de detección y prevención de intrusiones en host para las inspecciones de paquetes que pueden identificar cargas útiles maliciosas.
- Solo deben utilizarse arquitecturas de virtualización de confianza, combinadas con una segmentación de la red adecuada. Las arquitecturas de virtualización de confianza emplean un proceso de arranque seguro y verificable. Una buena segmentación de la red permite supervisar el tráfico y mantener las aplicaciones aisladas en caso de ataque. Además, esta combinación protege contra el desplazamiento lateral del malware.
- Debe supervisarse el tráfico saliente con el fin de identificar la presencia de malware que ha llegado a través de software troyanizado. Para detectar los equipos infectados y poder solucionar su problema, se debe examinar el tráfico que intentan enviar a Internet.

Intel Security

Los productos de Intel Security permiten identificar software legítimo troyanizado, detectar y bloquear amenazas de malware incrustadas, visualizar los riesgos y responder rápidamente.

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 8.8 Enterprise: PD22940.
  - Consulte las mejores prácticas de configuración para McAfee Endpoint Security: KB86704.

Resumen de la solución

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 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 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-ROM, 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: Program
   - 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 software troyanizado.

Resumen de la solución

McAfee Threat Intelligence Exchange y McAfee Advanced Threat Defense

- Configuración de directivas de 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 Threat Intelligence Exchange.
  - **Clean at: Known Malicious** (Limpiar si el nivel es Malicioso conocido).
  - **Block at: most likely malicious** (Bloquear si el nivel es 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: aceptar reputaciones de Advanced Threat Defense de archivos que Threat Intelligence Exchange aún no haya visto.
- Intervención manual de 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 incluidas en los productos:
  - Detección basada en firmas: McAfee Labs mantiene más de 600 millones de firmas.
  - Detección basada en la reputación: McAfee GTI
  - Análisis y emulación estáticos 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.
  - Aislamiento de aplicaciones (sandboxing) para su análisis dinámico
- Creación de perfiles de analizador donde es probable que se ejecute el software troyanizado:
  - 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.

Resumen de la solución

McAfee Network Security Platform

- 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 Advanced Threat Defense para nuevas variantes de ataques:
  - Configure la integración con Advanced Threat Defense en una directiva de malware avanzado.
  - Configure Network Security Platform para enviar archivos .exe, de Microsoft Office, Java Archive y PDF a Advanced Threat Protection para su inspección.
  - Verifique que la configuración de 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 Gateway Anti-Malware.
- Active GTI para conocer la reputación de las URL y los archivos.
- Integración con 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 Intel Security).

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 Labs, 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 a las aplicaciones troyanizadas.
- 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

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

Este artículo de la base de datos de conocimientos ofrece a los clientes información detallada sobre Trojan-Powelike: Vectores de infección y propagación: PD25582

SIEM Orchestration: Orchestration Triggers Signs of Malware Infection and Anomalous Behaviors (Organización de SIEM: Desencadenadores de la organización, síntomas de infección de malware y comportamientos maliciosos): PD24830

Informe: *Seguridad más allá de las firmas*

FAQs for Network Security Platform: Advanced Malware Detection (Preguntas frecuentes sobre Network Security Platform: Detección de malware avanzado): KB75269

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

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