Solution Brief

Protección frente al malware basado en macros

En el ***Informe sobre amenazas de McAfee® Labs de noviembre de 2015***, analizamos en profundidad el malware basado en macros, una reliquia de los años 90 que resurge ahora debido a lo mucho que se utilizan las macros en las empresas y a la mayor sofisticación de los ataques de ingeniería social que propagan malware nuevo y más sigiloso a base de macros. Una macro es un acceso directo que sirve para automatizar tareas empleadas con frecuencia. Es una cadena de código incorporada en un documento —normalmente de Microsoft Office— y escrita en el lenguaje de programación Visual Basic for Applications. Cuando se graba una macro, en realidad se genera un programa en Visual Basic for Applications. Para luchar contra el malware basado en macros, Microsoft generó un paso que requería permisos para activar las macros y que servía como verificación. Ahora Microsoft Office desactiva todas las macros de manera predeterminada, de forma que no es posible ejecutar macros sin el permiso del usuario. Esta iniciativa aplacó el entusiasmo de los desarrolladores de malware basado en macros y redujo la influencia de las macros maliciosas. Sin embargo, durante el último año los agresores han recurrido a malware nuevo y más sigiloso que combina macros e ingeniería social para atacar persistentemente a las empresas. El número de muestras de malware de macros está en su nivel máximo en seis años.

Los delincuentes que utilizan este malware lo propagan principalmente a través de adjuntos de correo electrónico de phishing, así como campañas de spam, páginas web atacadas y descargas secundarias. En la actualidad estas técnicas son mucho más sofisticadas que en los 90, década en la que apareció el malware para macros por primera vez. Para los usuarios es bastante difícil identificar estas campañas, porque son selectivas, de corta duración y contienen archivos adjuntos cuidadosamente diseñados para eludir la detección.

A continuación incluimos las prácticas y procedimientos recomendados para protegerse contra los ataques de malware basado en macros:

- Active las actualizaciones automáticas de los sistemas operativos o descargue con regularidad las actualizaciones para que estos cuenten con los parches necesarios para estar protegidos frente a las vulnerabilidades conocidas.

intel Security

- Utilice el software de Microsoft Office actualizado, que ofrece mejor protección frente a este tipo de ataques.
- Asegúrese de que la configuración predeterminada de la seguridad de macros está definida como alta en todos los productos de Microsoft Office.
- Configure el software antimalware para que analice automáticamente los archivos adjuntos de todos los mensajes instantáneos y de correo electrónico. Asegúrese de que los programas de correo electrónico no abran automáticamente los archivos adjuntos ni procesen automáticamente los gráficos, así como de que el panel de vista previa esté desactivado.
- Establezca la configuración de seguridad del navegador como mínimo al nivel medio.
- Preste especial atención al abrir adjuntos, sobre todo si tienen la extensión .doc o .xls.
- No abra nunca mensajes de correo electrónico no deseados ni archivos adjuntos que no esperaba recibir, incluso aunque provengan de personas que conoce.
- Tenga cuidado con el phishing basado en spam. No haga clic en enlaces de mensajes instantáneos o de correo electrónico.
- Controle los pings no previstos dirigidos a direcciones IP como 1.3.1.2 o 2.2.1.1 desde ordenadores internos.
- Tenga en cuenta que normalmente las facturas y recibos no necesitan macros.
- Desconfíe de los documentos vacíos que piden a los usuarios activar las macros para ver el contenido.

Cómo puede ayudarle Intel Security a protegerse frente al malware basado en macros

McAfee Web Gateway

Algunos de los principales métodos para distribuir malware basado en macros 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 Global Threat Intelligence (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 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 VirusScan® Enterprise

Con **McAfee VirusScan Enterprise** detectar y eliminar el malware basado en macros es muy fácil. McAfee VirusScan Enterprise emplea el galardonado motor de análisis de McAfee Labs para proteger sus archivos frente a virus, gusanos, rootkits, troyanos y otras amenazas avanzadas. Ofrezca una mayor protección a su empresa con la capacidad de McAfee VirusScan Enterprise de bloquear puertos, nombres de archivos, carpetas, directorios y el uso compartido de archivos, así como de realizar un seguimiento y bloqueo de las infecciones.

- **Protección proactiva contra ataques**: integra tecnología antimalware con prevención de intrusiones para proporcionar protección frente a los exploits que emplean desbordamiento del búfer aprovechando las vulnerabilidades de las aplicaciones de Microsoft.

- **Insuperable en detección y desinfección de malware**: protege frente a amenazas tales como rootkits y troyanos con análisis avanzado de comportamientos. Detiene el malware de raíz por medio de técnicas entre las que se incluyen el bloqueo de puertos, el bloqueo de nombres de archivo, el bloqueo de carpetas y directorios, el bloqueo del uso compartido de archivos, y el seguimiento y el bloqueo de infecciones.
- **Seguridad en tiempo real con integración en McAfee GTI**: protección frente a amenazas conocidas y desconocidas en todos los vectores de entrada —archivos, Web, correo electrónico y redes— con el respaldo de la plataforma de información sobre amenazas más exhaustiva del mercado.

McAfee Advanced Threat Defense

McAfee Advanced Threat Defense es un producto de detección de malware multicapa que combina varios motores de inspección. Al utilizar varios motores de inspección que aplican inspección basada en firmas y reputación, emulación en tiempo real, análisis del código completamente estático y entornos aislados dinámicos, McAfee Advanced Threat Defense no solo detecta los documentos que se sirven de macros para distribuir malware, sino que asegura la detección y protección frente al malware que se descarga tras su ejecución.

- **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 estático en tiempo real y emulación**: proporciona emulación y análisis estático en tiempo real para localizar rápidamente las amenazas de malware de macros y 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 de aplicaciones en entornos aislados**: con los archivos cuya seguridad no puede determinarse mediante los motores de inspección mencionados antes, 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 Windows XP SP2 y SP3, 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 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 ataques del malware basado en macros gracias a la 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, como McAfee GTI o las aportaciones de terceros, con la información local 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.

Además de estos productos de Intel Security, recomendamos otras dos clases de tecnologías de seguridad.

- **Seguridad del gateway de correo electrónico**: la mayor parte del malware basado en macros entra 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.
- **Firewall**: en todo sistema de seguridad es básica una buena tecnología de firewall. Un firewall puede detectar muchas amenazas en el perímetro antes de que entren en la red de confianza.

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