Resumen de la solución

Detener la filtración de datos

Garantice la seguridad de sus joyas de la corona.

En el **Informe de McAfee® Labs sobre amenazas de agosto de 2015**, analizamos en detalle uno de los pasos clave en el proceso del robo de datos: la filtración de datos. Este paso requiere que el que realiza la fuga traslade o copie los datos desde la red del propietario hasta una que esté bajo el control del delincuente.

En los últimos 10 años, la industria ha observado un crecimiento sin precedentes de las fugas de datos, así como del volumen de personas y organizaciones afectadas por este fenómeno. Las fugas de información han pasado de limitarse a la obtención de números de tarjetas de crédito y débito, al robo de casi cualquier tipo de información que compartamos online: nombres, fechas de nacimiento, direcciones, números de teléfono, datos sanitarios o credenciales de cuentas, entre muchos otros.

Por desgracia, las personas no son el único objetivo de los ataques. El ciberespionaje llevado a cabo por países, las organizaciones criminales y los hacktivistas ponen en riesgo los datos confidenciales de personas y organizaciones en cualquier lugar del mundo.

Creadores de amenazas y sus motivaciones

El creador de una amenaza es un individuo o grupo que intenta conseguir acceso de manera no autorizada a redes informáticas y sistemas. En la comunidad de seguridad, este tipo de amenazas se clasifican en tres categorías principales: países, delincuentes organizados y hacktivistas. En la tabla siguiente se incluye información sobre sus motivaciones y los tipos de datos que pueden ser de valor para ellos.

	Países	Crimen organizado	Hacktivistas
Motivación general	Ciberespionaje Ventajas estratégicas	Económica	Reputación Social
Ejemplo de tipos de datos	Código fuente Mensajes de correo electrónico Documentos internos Actividad militar Información de identificación personal de empleados de la administración	Información de cuentas bancarias Números de tarjetas de crédito Información de identificación personal (números de documentos de identidad, datos sanitarios)	Mensajes de correo electrónico Información de los empleados Cualquier tipo de información confidencial interna
Volumen de datos buscados	Pequeño o grande	Grande	Pequeño o grande
Sofisticación de las técnicas de filtración	Alta	De media a baja	De media a baja
Ubicación de la red	Desconocida/dispersa	Conocida	Conocida y desconocida/ dispersa

intel Security

Objetivo de datos

Una vez que el agresor ataca un sistema de la red, ya puede comenzar a explorar otros sistemas y descubrir los que albergan datos interesantes. Una red compleja contiene numerosos tipos de datos, por lo que este proceso es largo para los ciberdelincuentes que no disponen de información privilegiada e incrementa las posibilidades de detección. Por este motivo, los delincuentes intentan al máximo pasar desapercibidos y son extremadamente persistentes.

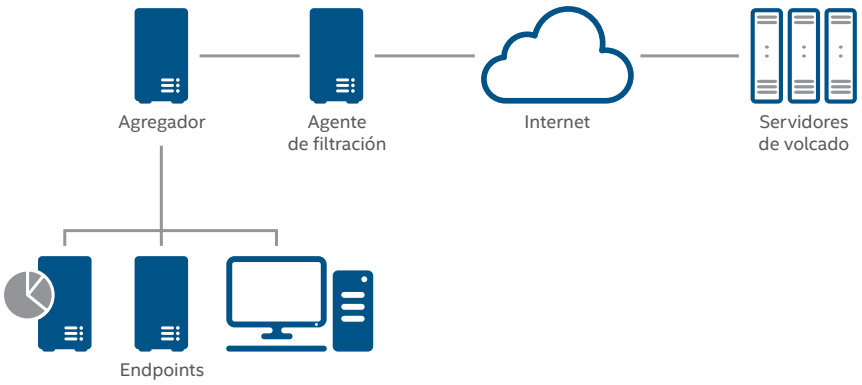
Entre los principales objetivos de datos incluyen:

Objetivo de datos	Tipos de datos	Intereses del agresor
Sistemas de base de datos	Datos sanitarios protegidos, información de identificación personal, tarjetas de crédito, información bancaria y cuentas de usuario	Crimen organizado, hacktivistas
Repositorios de código fuente	Código fuente, credenciales, claves	Países, hacktivistas
Sistemas especializados	Varían	Todo, según el tipo de endpoint
Recursos de archivos compartidos y sistemas similares	Código fuente, diseños, comunicaciones, etc.	Países, hacktivistas
Correo electrónico y comunicaciones	Diseños, comunicaciones	Países, hacktivistas

Filtración de datos

Una vez que los creadores de la amenaza han localizado y obtenido los datos que buscaban, empieza la parte más difícil para ellos: filtrar el botín. Los agresores aprovecharán el entorno del host para que actúe como intermediario entre la red de la víctima y la del agresor. Esta infraestructura intermedia puede ser sencilla o sofisticada, según lo profundos y segmentados que estén en la red los datos que busca el agresor. Los sistemas pueden adoptar distintas funciones en la infraestructura intermedia, como:

- **Endpoints:** uno o varios objetivos de datos en el mismo segmento, o en un segmento que se pueda direccionar al agregador.
- **Agregador:** actúa como un punto de recopilación de los datos de los endpoints atacados y carga dichos datos en el agente de filtración. El agregador puede tener acceso a Internet, aunque no necesariamente. En las campañas más sofisticadas, puede haber varios agregadores que transfieran los datos a varios agentes de filtración con el fin de ocultar la ruta de los datos de salida.
- **Agente de filtración:** recoge los datos del agregador y facilita su transferencia al servidor de volcado del agresor. Puede realizarse mediante una transferencia sencilla o bien retener los datos hasta que el agresor los recupere.



Arquitectura típica de filtración de datos de red

Ya sea mediante el empleo de medios sencillos o sofisticados, el objetivo del agresor es hacerse con los datos que busca y situarlos en un servidor que se encuentra fuera de la red de la víctima. Los servidores de volcado son los primeros puntos en los que reside la información robada fuera del control de la víctima y los agresores pueden acceder a ellos fácilmente. Estos servidores pueden ser:

- **Sistemas comprometidos:** sistemas que han sufrido un ataque del agresor durante otra campaña diferente. Incluyen desde blogs de WordPress personales hasta servidores que pertenecen a empresas que no disponen de controles de seguridad eficaces.
- **Sistemas alojados en determinados países:** los países en los que la legislación sobre la privacidad es muy restrictiva son muy atractivos para los delincuentes, ya que esta circunstancia les permite alojar los sistemas dentro de sus fronteras y que no les molesten mientras gozan de un cierto grado de protección.
- **Sistemas alojados temporalmente:** sistemas temporales que se alojan en la nube a través de proveedores como Amazon Web Services, Digital Ocean o Microsoft Azure.
- **Servicios para compartir archivos en la nube:** sitios para compartir archivos online a los que puede acceder el público general, como DropBox, Box.com, o Pastebin.
- **Servicios alojados en la nube:** otros servicios que funcionan a través de Internet, como Twitter y Facebook, que permiten a los usuarios publicar información.

Transportes de datos

Los transportes de datos son los protocolos y métodos empleados por los ladrones para copiar la información de una ubicación o sistema en otro, ya sean internos (de un endpoint en un agregador) o de una ubicación interna en otra externa (de un agente de filtración en un servidor de volcado). A continuación se incluye un resumen de algunos de los protocolos de transporte más habituales:

Transporte	Descripción	Interno	Externo
HTTP/HTTPS	Debido a la prevalencia de HTTP en las comunicaciones de red es el protocolo ideal para ocultar los datos filtrados entre otro tipo de tráfico. Se ha utilizado como transporte de filtración general mediante la incrustación de comandos en encabezados HTTP y métodos GET/POST/PUT.		■
FTP	El protocolo FTP se emplea habitualmente en los servidores empresariales y es fácil de utilizar mediante comandos nativos del sistema, por lo que es un medio de transporte sencillo.	■	■
USB	Los dispositivos de almacenamiento USB se utilizan con frecuencia para la filtración de datos cuando se atraviesan redes aisladas. Hemos observado malware que busca un dispositivo de almacenamiento USB con un marcador específico y que, a continuación, copia los datos que se van a filtrar en un sector oculto del mismo. La filtración comienza cuando el dispositivo se coloca en otro sistema infectado con acceso a la red. Los dispositivos de almacenamiento USB también pueden ser utilizados por personal interno para copiar fácilmente grandes cantidades de datos y sacarlos físicamente de la empresa.	■	■
DNS	Hay registros DNS específicos, como TXT o incluso los registros A y CNAME, que pueden almacenar datos en su interior hasta cierto punto. Con el control de un dominio y un nombre de servidor, un agresor puede transmitir pequeñas cantidades de datos realizando consultas específicas en el sistema atacado.		■
Tor	La red Tor es cada vez más popular. Esto permite a los agresores enviar datos filtrados a servidores que son difíciles de localizar. Sin embargo, el tráfico Tor en redes empresariales no suele ser legítimo por lo que puede detectarse y detenerse fácilmente.		■
SMTP/correo electrónico	Los servidores SMTP, tanto si son propiedad de la empresa como si no, pueden utilizarse para enviar datos fuera de la empresa como adjuntos o en el cuerpo de los mensajes de correo electrónico.		■
SMB	SMB es un protocolo extremadamente común en entornos Microsoft Windows y puede estar ya disponible en los sistemas.	■	

Transporte	Descripción	Interno	Interno
RDP	El protocolo RDP permite realizar varias actividades, como copiar/pegar y compartir archivos y, en algunos casos, los sistemas que admiten RDP pueden estar desprotegidos en Internet.	■	■
Transportes personalizados	En ocasiones se utilizan transportes personalizados en comunicaciones con los servidores de control y en algunos tipos sofisticados de malware. Un transporte robusto requiere una gran cantidad de trabajo y debido a su exclusividad, el protocolo es fácil de identificar en la red, inclinando la balanza hacia un tipo de transporte ya establecido.	■	■

Manipulación de datos

Al gestionar y filtrar datos confidenciales, los agresores harán todo lo posible para asegurarse de que sus víctimas no descubran sus intenciones. La manipulación de los datos antes de su transferencia puede ayudar a evitar la detección, reducir el tiempo de transferencia e incluso incrementar el tiempo hasta la detección. Algunas de las técnicas que se observan durante esta etapa son:

Técnica	Descripción
Compresión	La compresión con el formato ZIP estándar no solo ofrece un nivel de ocultación sino que además acelera las transferencias de archivos.
Fragmentación	La división de los datos en pequeñas partes antes de su envío permite que la transferencia se confunda en la actividad habitual de la red.
Codificación/ocultación	El tipo de manipulación de datos más común es el empleo de un algoritmo de codificación u ocultación básico. Mediante el empleo de sencillas técnicas, como realizar una operación XOR con una clave estática, utilizar codificación Base64 o simplemente convertir todos los caracteres en código hexadecimal, se pueden manipular los datos lo suficientemente para evitar la detección.
Cifrado	Es sorprendente que el cifrado no se utilice siempre durante la filtración. Es posible que esto se deba a que afecta al rendimiento o simplemente a que no es necesario. Cuando se emplea, lo habitual es observar un cifrado con RC4 o AES.

Cómo puede ayudarle Intel Security a protegerse frente a la filtración de datos

McAfee DLP Discover

El primer paso para proteger los datos convenientemente es saber dónde reside la información y qué datos hay exactamente. **McAfee DLP Discover** protege contra la filtración de datos mediante la simplificación del primer paso gracias a estas funciones:

- **Identificación y protección de los datos confidenciales:** creación de un inventario e indexación de todo el contenido mediante el análisis automático que realiza McAfee DLP Discover de todos los recursos disponibles, lo que le permite conocer mejor sus datos confidenciales dondequiera que residan. Con McAfee DLP Discover, puede consultar y explorar la información para descubrir cómo se utiliza, quién es su propietario, dónde se almacena y dónde se ha propagado.
- **Revisión y solución de las infracciones:** descubrimiento de infracciones de contenido, registro y generación de firmas, y envío de notificaciones de alerta para proteger los datos confidenciales de manera más eficaz. La integración de la administración y el flujo de trabajo de incidentes limita la proliferación de material confidencial.
- **Fácil definición de directivas para la protección:** ofrece creación, comunicación y administración de directivas de manera intuitiva y unificada, para que pueda mejorar el control sobre su estrategia de protección de la información.

McAfee DLP Monitor

McAfee DLP Monitor permite recopilar, rastrear e informar sobre los datos que se transfieren en toda la red. Puede descubrir fácilmente las amenazas desconocidas para sus datos y adoptar las medidas necesarias para protegerlos y garantizar que su empresa no sufra la próxima gran fuga de datos.

- **Examen del tráfico de red:** examen del tráfico de la red a un nivel profundo con la función de análisis y exploración de datos de McAfee DLP Monitor, líder de la industria.
- **Identificación rápida de los datos:** detalla rápidamente cómo se están utilizando los datos, quién los usa y a dónde van mediante su descubrimiento en tiempo real, lo que proporciona al usuario la información que necesita para tomar las medidas adecuadas. McAfee DLP Monitor puede identificar rápidamente más de 300 tipos de contenido que transita por cualquier puerto o protocolo, lo que garantiza la visibilidad para su empresa.
- **Análisis forenses detallados:** realiza análisis forenses para correlacionar los eventos de riesgo actuales y pasados, detectar tendencias de riesgos e identificar amenazas. McAfee DLP Monitor le permite comprender rápidamente la situación y desarrollar las reglas y directivas necesarias para corregir las posibles anomalías.

McAfee DLP Prevent

McAfee DLP Prevent protege frente a la pérdida de información garantizando que solo salga de la red cuando sea conveniente, ya sea a través del correo electrónico, el correo web, la mensajería instantánea, wikis, blogs, portales, HTTP/HTTPS o transferencias FTP. La capacidad para identificar y mitigar rápidamente los intentos de filtración suele marcar la diferencia entre mantener a salvo sus datos más valiosos o ser noticia por robo de información.

- **Visibilidad de los incidentes de seguridad:** ofrece vistas resumidas y detalladas de los incidentes de seguridad, así como de las medidas que ha aplicado, en vistas personalizadas e informes de incidentes.
- **Implementación proactiva de directivas para todos los tipos de información:** implementa directivas para la información que sabe que es confidencial, así como para la que no es tan obvia. Gracias a que la solución integra una amplia variedad de directivas, que van desde el cumplimiento de normativas al uso aceptable y la protección de la propiedad intelectual, es posible comparar documentos completos o parciales con un exhaustivo conjunto de reglas con el fin de garantizar la seguridad de toda su información confidencial.

McAfee DLP Endpoint

McAfee DLP Endpoint le permite supervisar e impedir rápidamente la filtración de datos en la oficina, desde otro lugar y en la nube. Supervise rápidamente los eventos en tiempo real, aplique directivas de seguridad que se administran de manera centralizada y genere detallados informes forenses y de proliferación, sin que se vean afectadas las operaciones cotidianas.

- **Compatibilidad con virtualización ampliada:** implementa una directiva por usuario para varias sesiones e infraestructuras de equipos virtuales, lo que ofrece flexibilidad y mejora el control de los datos que se transfieren a terminales compartidos.
- **Supervisión y generación de informes globales sobre incidentes:** recopila todos los datos necesarios, como el remitente, destinatario, fecha/hora y datos de la red, para facilitar un análisis, investigación y auditoría adecuados, así como la evaluación y reducción de riesgos.
- **Consola de administración centralizada:** emplea la consola de administración de McAfee® ePolicy Orchestrator® (McAfee ePO™) para definir directivas, desplegar y actualizar agentes, supervisar eventos en tiempo real y elaborar informes para cumplir los requisitos de las normativas.

- **Gestión completa de contenido:** controla y bloquea los datos confidenciales copiados en dispositivos USB, unidades flash, smartphones y otros dispositivos de almacenamiento extraíbles, incluidos los soportes ópticos y las copias impresas. Gracias a la integración de DLP y la administración de derechos digitales la protección llega más allá de la red.

McAfee Device Control

McAfee Device Control protege frente a la filtración de datos a través de dispositivos y soportes de almacenamiento extraíbles, como unidades USB, smartphones, y reproductores de CD y DVD. Permite a la organización supervisar y controlar los datos que se transfieren desde los equipos de sobremesa y portátiles, independientemente de su ubicación, ya estén en la oficina o fuera de ella. McAfee Device Control ofrece funciones de bloqueo de dispositivos en función del contenido y el contexto, como:

- **Administración integral de dispositivos y datos:** controla cómo copian los datos los usuarios de su organización en unidades USB, smartphones, CD y DVD grabables y muchos otros dispositivos que se pueden utilizar para la filtración de datos.
- **Controles diferenciados:** permite determinar qué dispositivos se pueden utilizar y cuáles no, así como qué datos pueden transferirse a dispositivos autorizados, además de impedir a los usuarios que copien datos desde determinadas ubicaciones y aplicaciones.
- **Funciones avanzadas de auditoría y generación de informes:** simplifican el cumplimiento de normativas con registros detallados a nivel de usuario y de dispositivo. Se registran y comunican fácilmente datos como el dispositivo, la fecha/hora y las pruebas de datos, con el fin de facilitar las auditorías y consultas sobre cumplimiento de normativas.
- **Administración centralizada:** ofrece supervisión de eventos en tiempo real y administración de directivas e incidentes centralizada gracias a la integración con el software McAfee ePO.

McAfee Next Generation Firewall

Proteja su empresa contra la filtración de datos o los ataques que emplean técnicas de evasión avanzadas con **McAfee Next Generation Firewall**. McAfee Next Generation Firewall realiza una inspección profunda y especializada de paquetes, y lleva a cabo la normalización de pila completa y la inspección horizontal de los flujos de datos a fin de identificar anomalías en el tráfico, como la comunicación del malware con su servidor de control o intentos de filtración de información desde su red.

- **Neutralización de las técnicas de evasión avanzadas:** emplea funciones como la normalización del tráfico multicapa, las huellas digitales basadas en vulnerabilidades y la comparación de huellas digitales independientes del protocolo.
- **Detección de la actividad del servidor de control:** utiliza la detección basada en el descifrado y el análisis de la secuencia de longitud del mensaje, para detectar la actividad del servidor de control o de las redes de bots.
- **Bloqueo basado en la geolocalización:** rechaza las conexiones entrantes y salientes a países con los que su empresa no tiene relación comercial. De esta forma, se reducen las posibilidades de que se reciban comandos del servidor de control desde direcciones IP cuya comunicación con su entorno no está justificada.

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