Resumen de la solución

Protección frente a los ladrones de contraseñas

Ante nuestra creciente dependencia de los dispositivos personales electrónicos y el auge del traslado a la nube de los datos más valiosos de las empresas, ha aumentado el atractivo de las credenciales de acceso. Hoy día, los ciberdelincuentes utilizan contraseñas robadas en las primeras fases de casi todas las amenazas persistentes avanzadas.

El objetivo de los ladrones de contraseñas es franquear el sistema de seguridad de la red y los sistemas para conseguir obtener credenciales de acceso fundamentales. Las funciones robustas y potentes del ladrón de contraseñas Fareit lo han convertido en el malware de robo de contraseñas más utilizado en los últimos cinco años. Desde su descubrimiento en 2012, Fareit ha cambiado continuamente para eludir las últimas estrategias de ciberdefensa.

Originalmente, Fareit se centraba en el robo de credenciales de inicio de sesión de navegadores web con el fin de conseguir acceso a aplicaciones como las de banca online o a cuentas de correo electrónico, o bien para el robo de identidades. Desde entonces, Fareit ha evolucionado y se ha convertido en un ladrón de información más agresivo, que se oculta mediante el empleo de tácticas de mimetismo, como cambiar su hash de archivos en cada infección. En 2016, surgió una nueva generación del malware Fareit que utilizaba un activo de red infectado para llevar a cabo ataques de denegación de servicio distribuido. Además, Fareit se ofrece ahora como un servicio de pago por infección, lo que significa que los ciberdelincuentes ganan dinero por distribuir malware. Cuantas más infecciones consiguen, más cobran.

Los ataques de phishing que distribuyen ladrones de contraseñas, como Fareit, se cuentan entre los principales vectores de ataque observados en la última década.

Prácticas y procedimientos recomendados para protegerse frente a los ataques de ladrones de contraseñas

McAfee recomienda a las organizaciones que tomen las siguientes medidas para protegerse frente a los ataques de ladrones de contraseñas.

- Los ladrones de contraseñas suelen distribuirse a través del malware, por lo que una norma básica de seguridad es mantener siempre actualizados los productos antimalware.
- Los usuarios desprevenidos pueden descargar malware mientras navegan. Mantenga siempre actualizados los navegadores web, así como los complementos, para añadir una capa extra de protección.

McAfee™
Together is power.

- Ejecute las aplicaciones como un usuario con privilegios limitados, en lugar de como administrador.
- Proteja el perímetro de la red. Los firewalls pueden impedir que los agresores externos accedan a las aplicaciones internas que ya han sido víctimas de un ataque de ladrón de contraseñas.
- Utilice las credenciales de autenticación de la empresa (como los de proxis web para navegar en Internet, aplicaciones de bases de datos, carpetas compartidas, etc.) solo cuando se usan activos corporativos. No permita que se conecten a la red de confianza sistemas que no hayan sido distribuidos y certificados por el grupo de seguridad de TI de la empresa.
- Es posible que haya malware que podría contener ladrones de seguridad incrustado en el interior de software legítimo previamente troyanizado por un ciberdelincuente. Para evitar ataques de este tipo, recomendamos que se refuerce la protección de los mecanismos de distribución y entrega del software. Es siempre aconsejable tener un repositorio central de aplicaciones corporativas del que los usuarios pueden descargar el software aprobado.
- En los casos en los que los usuarios están autorizados a instalar aplicaciones que no han sido validadas previamente por el grupo de seguridad de TI, se les debe informar de que únicamente deben instalar aplicaciones con firmas de confianza procedentes de proveedores conocidos. Es muy habitual que aplicaciones que se ofrecen online supuestamente "inofensivas" contengan ladrones de seguridad, u otro malware.
- Evite descargas de aplicaciones de fuentes distintas de la Web. Son muy elevadas las probabilidades de descargar malware de grupos USENET, canales IRC, clientes de mensajería instantánea o sistemas P2P. Los enlaces a sitios web vistos en IRC y la mensajería instantánea suelen apuntar a descargas infectadas.
- Ponga en práctica un programa educativo para evitar ataques de phishing. Normalmente los ladrones de contraseñas se distribuyen mediante el phishing.

Si cree que tiene sistemas afectados por un ladrón de contraseñas, estas recomendaciones le ayudarán a frenar la propagación lateral de la infección:

- Reduzca la superficie de ataque con autenticación de dos factores en las aplicaciones que la admiten. Es posible que el agresor ya haya robado una contraseña, pero el segundo factor detendrá la filtración.
- Un firewall para endpoints restringirá la expansión de las intrusiones con contraseñas robadas si el ordenador infectado tiene una limitación de tráfico entrante y saliente impuesta mediante las reglas del firewall.

Cómo pueden protegerle los productos de McAfee frente a los ladrones de contraseñas

McAfee VirusScan® Enterprise 8.8 o McAfee Endpoint Security 10

- Mantenga el software antimalware totalmente actualizado con el último parche, versión de DAT y motor de análisis. Compruebe que se utiliza McAfee Global Threat Intelligence (McAfee GTI).
- 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 Knowledge Base: KB81095 y KB54812.
  - Consulte las mejores prácticas de configuración para McAfee VirusScan Enterprise 8.8: PD22940.
  - Consulte las mejores prácticas de configuración para McAfee Endpoint Security: KB86704.

McAfee Host Intrusion Prevention

Las herramientas de prevención de intrusiones no son eficaces para sacar a la luz un ataque de robo de contraseñas que ha conseguido su objetivo. Sin embargo, McAfee Host Intrusion Prevention puede impedir el desplazamiento lateral de la carga útil del malware, que puede incluir un ladrón de contraseñas.

- 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 McAfee 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 McAfee 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 un carácter comodín en la ruta, comience el nombre del archivo por "**\" o "?:\". Si desea utilizar un carácter comodín en la letra de unidad, utilice, 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, de disco duro, CD, USB, red o 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: Programa
     - Operations: Ejecutar ejecutable de destino
     - 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 ladrones de contraseñas.

McAfee Threat Intelligence Exchange y McAfee Advanced Threat Defense

- Configuración de directivas de McAfee 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 McAfee Threat Intelligence Exchange.
  - Limpiar si el nivel es Known Malicious (Malicioso conocido).
  - Bloquear si el nivel es Most likely malicious (Probablemente malicioso) (bloquear si el nivel es Unknown [Desconocido] aumentaría la protección, pero quizá también añadiría más carga de trabajo administrativo).
  - Submit files to Advanced Threat Defense (Enviar archivos a McAfee Advanced Threat Defense) si el nivel es Unknown (Desconocido) e inferiores.
  - Directiva de McAfee Threat Intelligence Exchange: aceptar reputaciones de McAfee Advanced Threat Defense de archivos que McAfee Threat Intelligence Exchange aún no haya visto.
- Intervención manual de McAfee 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: el "zoo" de malware de McAfee Labs mantiene más de 600 millones de muestras.
  - 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.
  - Análisis dinámico en entornos aislados.
- Creación de perfiles de analizador donde es probable que se ejecute malware de robo de contraseñas:
  - Sistemas operativos habituales como Windows 7, 8, 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.

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 ladrones de contraseñas.

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

McAfee Active Response

- McAfee Active Response es una solución que busca 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 ladrones de contraseñas.
- 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

Phishing Attacks Employ Old but Effective Password Stealer (Los ataques de phishing emplean un ladrón de contraseñas antiguo, pero eficaz)

Perfil de virus de Fareit

Perfil de virus de Fareit

McAfee Ireland Ltd.
Building 2000, City Gate
Mahon, Cork, Ireland
www.mcafee.com/es