Folleto

Mantenga alejado a The Wolf

Riesgos de seguridad en las películas «The Wolf» y soluciones de HP

Los cortafuegos por sí solos no pueden detener los complejos ataques de hackers como The Wolf. Debe aplicar varios niveles de protección en todos los puntos de conexión de la infraestructura. Proteja sus dispositivos, datos, identidades y documentos con las soluciones de seguridad de HP.

1.ª temporada: The Wolf

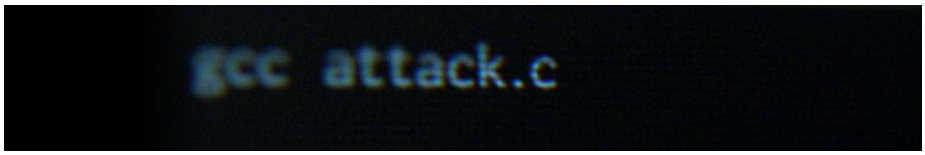
The Wolf arruina una institución financiera internacional al atacar sus puntos de conexión más vulnerables. Emplea un dispositivo móvil para acceder a una impresora e inyecta malware para interceptar y leer datos. A continuación, el correo electrónico de «suplantación de identidad» de The Wolf engaña a un usuario para que envíe a una impresora un código malicioso que se encuentra oculto en un archivo PDF.

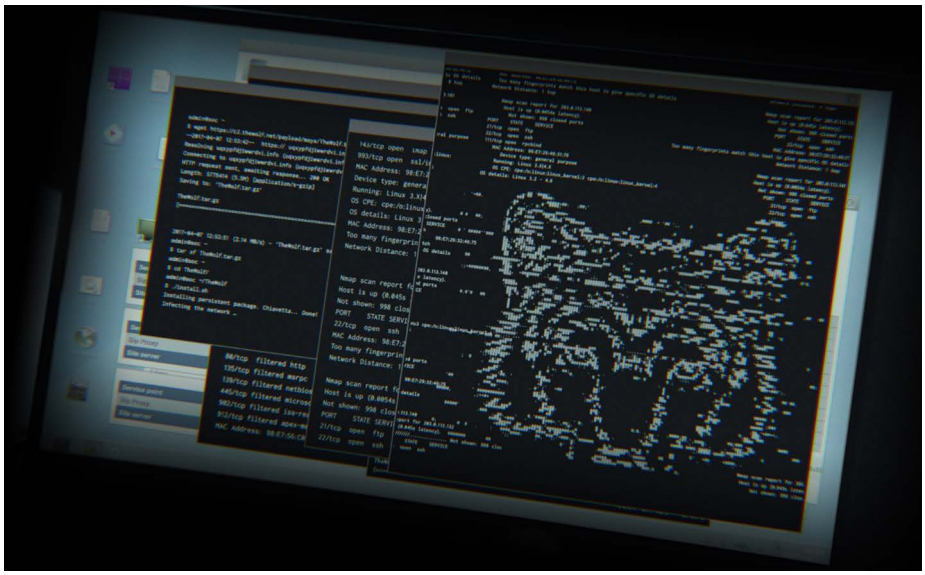
El malware de la impresora provoca una brecha en el cortafuegos y llega al nivel de la BIOS de los ordenadores de la empresa para recopilar datos e incluso restituirse cuando se despliegan las defensas de la red.

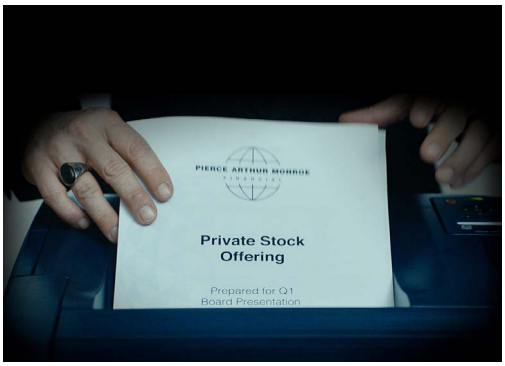
The Wolf se apodera de un documento impreso abandonado en la bandeja de salida de una impresora y sabotea la siguiente operación bursátil de la empresa, lo que destruye la confianza de los accionistas.

Vulnerabilidades

- La conexión Wi-Fi o Bluetooth de la impresora está abierta y no requiere autenticación de usuario
- Los archivos de datos de la impresora no están cifrados
- Los usuarios no reconocen los mensajes de correo electrónico o archivos de impresión sospechosos
- Las impresoras y los ordenadores no disponen de protección de malware a nivel de la BIOS
- Los documentos confidenciales quedan expuestos en las bandejas de salida







2.ª temporada La caza continúa

The Wolf dirige su ataque a los registros de pacientes que almacena una de las empresas de gestión de registros más grandes del mundo. Piratea un ordenador y utiliza el puerto USB de una impresora para cargar malware detrás del cortafuegos y buscar dispositivos conectados que pueda poner en peligro.

Dado que la impresora reside en una red no segmentada, The Wolf puede acceder a los servidores conectados a las bases de datos donde se encuentra la información confidencial. Roba millones de registros confidenciales de pacientes, que además son legibles porque los datos no están cifrados.

Tanto el hospital como la empresa de software son declarados responsables y afrontan sanciones importantes, además de daños en su reputación.

Vulnerabilidades

- El puerto USB de la impresora no requiere autenticación para su uso
- Los archivos de datos no están cifrados
- Las impresoras carecen de protección de malware
- No se supervisan las impresoras para evitar incidencias de seguridad

3.ª temporada Un auténtico alfa

The Wolf interrumpe las operaciones de una de las empresas de transporte más grandes del mundo y de un aeropuerto internacional.

Con el envío por correo electrónico de un archivo PDF de aspecto inofensivo, consigue que un oficinista de la empresa de transporte envíe un archivo Postscript malicioso a una impresora. El malware oculto se extiende por la red cuando el archivo se envía a la impresora, donde permanece sin ser descubierto. Acto seguido, The Wolf obtiene acceso a la presentación de una conferencia de alto nivel del director general, a las grúas de carga de un puerto y al software del piloto automático de los buques que se encuentran en el mar.

Posteriormente, The Wolf se centra en un aeropuerto de gran importancia, donde demuestra sus habilidades al controlar las luces y amenazar con acceder a varios sistemas críticos de su red. Las impresoras HP permitieron al personal de TI investigar y detener el ataque.

Vulnerabilidades

- Se añaden impresoras de emplazamientos temporales a la red sin configurar correctamente su seguridad
- Los navegadores de Internet de los ordenadores no disponen de protección frente a descargas accidentales
- No se supervisan los dispositivos del IoT y tampoco incluyen funcionalidades de detección de malware
- Los registros del sistema de las impresoras no están conectados a herramientas de supervisión de amenazas

¿Cómo puede protegerse de ataques similares?

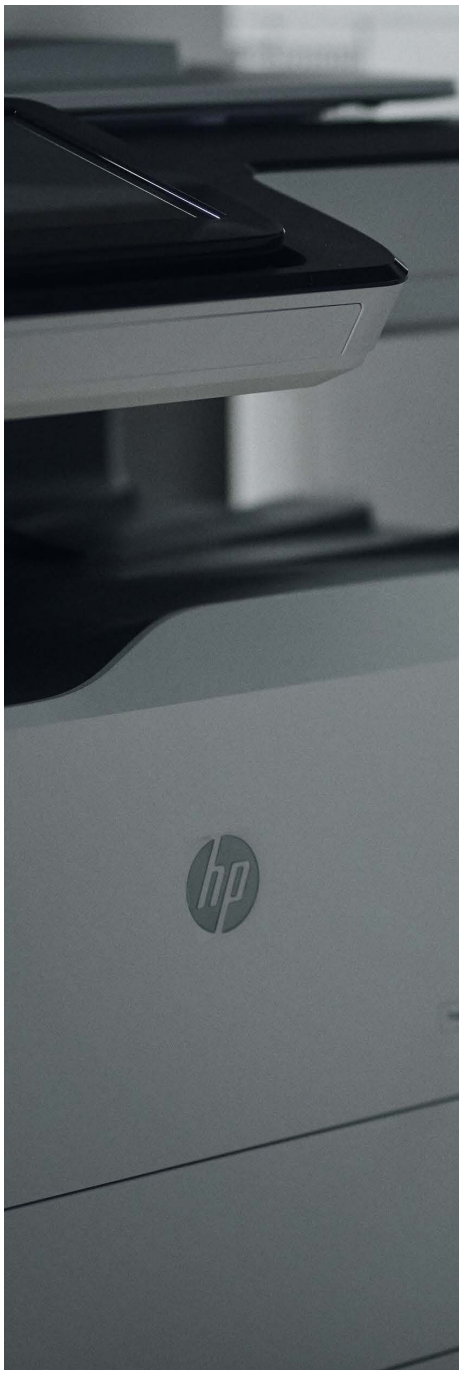
Proteja la identidad: mejore la seguridad de inicio de sesión con la autenticación multifactor consolidada de los ordenadores HP Elite.

Proteja el dispositivo: actualice su entorno con ordenadores HP Elite, así como con impresoras e impresoras multifunción HP Enterprise, que ofrecen protección frente a malware para detectar, detener y recuperarse automáticamente de los ataques. Cierre los puertos USB que no necesite, o controle el acceso con controles de usuario. Aísle físicamente las pestañas de los navegadores con HP Sure Click con el fin de evitar que se extienda el malware basado en Internet.[1]

Proteja los datos: aplique una solución de autenticación y cifrado para impresoras, como HP Access Control[2]. Solicite la autenticación de usuario y cifre los datos utilizando las funciones Wi-Fi y Bluetooth de las impresoras. Implemente una solución de autenticación y cifrado móvil, como PrinterOn Enterprise. Cifre los datos inactivos y en tránsito.

Proteja el documento: implemente una solución de impresión pull, como HP Access Control[2].

Mejore la supervisión y gestión: configure automáticamente las políticas de seguridad de la flota con HP JetAdvantage Security Manager[3] o el complemento de seguridad de impresoras HP para Microsoft® SCCM para impresoras y HP Manageability Integration Kit (MIK)[4] para ordenadores. Active los registros del sistema para realizar el seguimiento de eventos de seguridad y conecte los dispositivos a herramientas de gestión de eventos e información de seguridad (SIEM) para recibir alertas en tiempo real. Póngase en contacto con un proveedor de servicios gestionados de impresión (MPS) con formación sobre seguridad de HP para configurar y mantener la seguridad de las impresoras.



Proteja su negocio con la seguridad integral de HP

La impresión más segura del mundo[5]

Las impresoras e impresoras multifunción HP Enterprise pueden detectar, detener y recuperarse automáticamente de un ataque sin la intervención de TI gracias a funciones como la detección de intrusiones en tiempo real, HP Sure Start y HP Connection Inspector. Otros tipos de protección incluyen discos duros cifrados, firmware actualizable y la capacidad de enviar alertas de seguridad a herramientas SIEM.

hp.com/go/PrintersThatProtect

Los ordenadores más seguros y cómodos del mundo[6]

Los ordenadores HP Elite protegen a su empresa de las amenazas más habituales mediante la protección integral del SO. La autenticación multifactor de HP refuerza la protección de la identidad y HP Manageability Integration Kit[4] facilita la gestión de la seguridad en toda la flota de ordenadores. Otros tipos de protección incluyen el cifrado de discos duros, HP Sure Recover[7], HP Sure Click[1] y HP Sure View.

hp.com/go/ComputerSecurity

PrinterOn Enterprise

Consiga una impresión móvil, fiable y segura en la red de la empresa. Conecte prácticamente cualquier dispositivo de sobremesa o móvil a impresoras de diversos proveedores, tanto dentro como fuera de la red de confianza.

hp.com/go/businessmobileprinting

HP Access Control[2]

Restablezca el control, refuerce la seguridad y reduzca los costes mediante una autenticación de la impresión basada en roles, autorización y funcionalidades de impresión pull segura en toda su organización.

hp.com/go/hpac

HP JetAdvantage Security Manager[3]

Reduzca el coste y los recursos necesarios para mantener la seguridad de la flota con una completa herramienta de cumplimiento de la seguridad basada en políticas. Establezca una política de seguridad en toda la flota, automatice la corrección de la configuración de los dispositivos, instale y renueve certificados exclusivos, y genere informes de cumplimiento para toda la flota.

hp.com/go/securitymanager

Más información en
hp.com/go/hpsecure

[1] HP Sure Click se encuentra disponible en la mayoría de los ordenadores HP y es compatible con Microsoft® Internet Explorer y Chromium™. Entre los archivos adjuntos compatibles, se incluyen los archivos de Microsoft Office (Word, Excel, PowerPoint) y los archivos PDF en modo de solo lectura, siempre y cuando se haya instalado Microsoft Office o Adobe Acrobat.

[2] HP Access Control debe comprarse por separado. Para obtener más información, consulte hp.com/go/hpac.

[3] HP JetAdvantage Security Manager debe comprarse por separado. Para obtener más información, consulte hp.com/go/securitymanager.

[4] HP Manageability Integration Kit no se instala de forma predeterminada y se encuentra disponible en hp.com/go/clientmanagement.

[5] Basado en el análisis de HP de las funciones de seguridad publicadas en 2018 de las impresoras de la competencia de la misma categoría. Solo HP ofrece una combinación de funciones de seguridad que pueden supervisar para detectar y detener de forma automática un ataque y, a continuación, autovalidar la integridad del software en un reinicio. Para ver una lista de impresoras, visite: hp.com/go/PrintersThatProtect. Puede obtener más información en: hp.com/go/printersecurityclaims.

[6] Basado en las funcionalidades de seguridad exclusivas y completas de HP sin coste adicional alguno, y en la gestión de cada aspecto de un ordenador por parte de HP Manageability Integration Kit, que incluye el hardware, la BIOS y la gestión de software con el gestor de configuración de Microsoft System Center, entre proveedores con más de un millón de unidades vendidas al año en noviembre de 2016 de ordenadores HP Elite con procesadores Intel® Core® de 7.ª generación y posteriores, gráficos integrados Intel® e Intel® WLAN.

[7] HP Sure Recover se encuentra disponible en los ordenadores HP Elite con procesadores Intel® o AMD de 8.ª generación y requiere una conexión de red abierta por cable. No disponible en plataformas con varias unidades de almacenamiento interno, Intel® Optane™. Para evitar la pérdida de datos, debe realizar copias de seguridad de los datos importantes, archivos, fotografías, vídeos, etc.

Suscríbase para recibir actualizaciones
hp.com/go/getupdated

Compartir con compañeros

4AA7-0231ESE, agosto de 2018, rev. 1