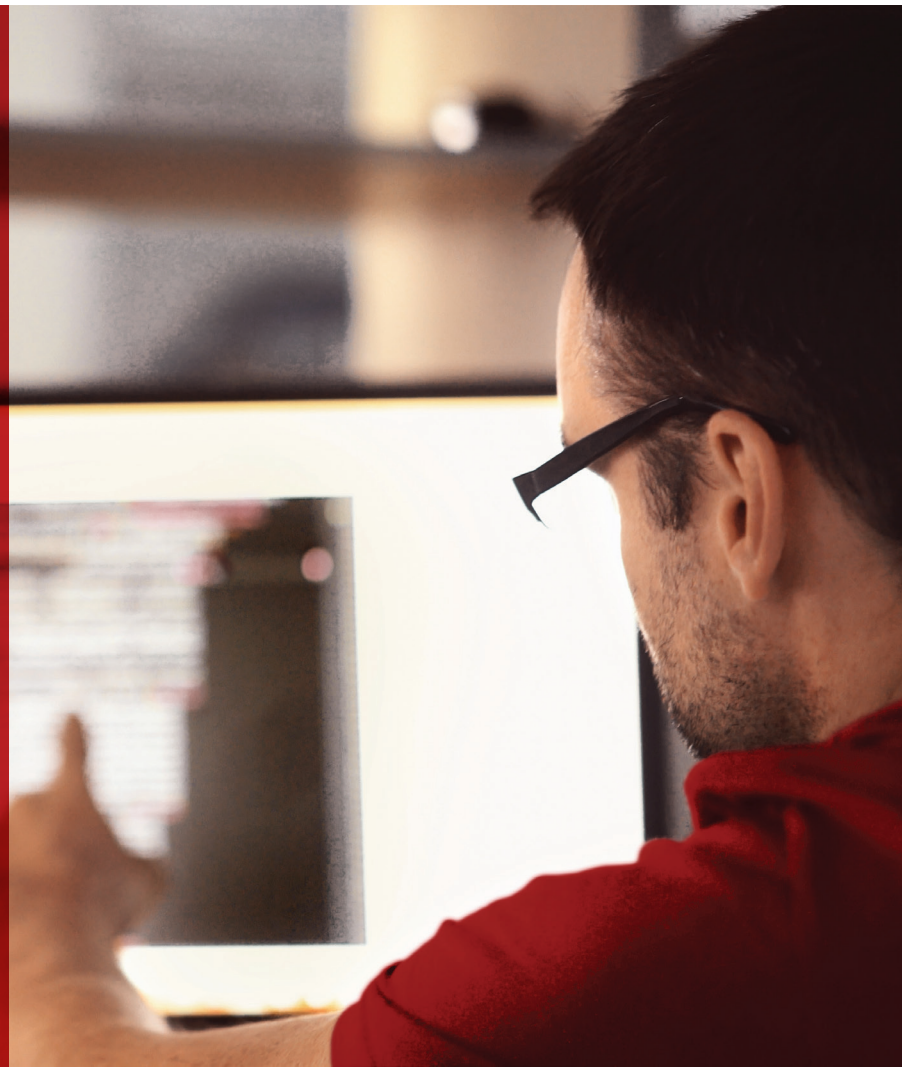
McAfee
Together is power.

Protección contra Pinkslipbot

W32/Pinkslipbot es una familia de malware de propagación automática, creada para robar datos personales y financieros a sus víctimas. Este malware permite al agresor hacerse con el control total de los sistemas infectados, gracias al uso de una puerta trasera basada en comandos que se gestiona desde el servidor de control, y otra basada en computación de red virtual (VCN). Pinkslipbot se puede propagar también a otros sistemas del entorno a través de recursos compartidos de la red y se puede comunicar con su servidor de control para descargar versiones actualizadas de sí mismo.



Esta familia se identificó originalmente en 2007, pero el grupo que la creó ha mantenido el código base y ha añadido actualizaciones incrementales antes de publicar una nueva versión cada varios meses.

Los datos que roba Pinkslipbot permiten a un agresor averiguar la ubicación, organización y propietario de un sistema infectado. Posteriormente, el agresor puede vender esta información (especialmente si se trata de una organización importante) a un tercero y, una vez realizado el pago, desplegar malware selectivo en el sistema atacado.

Para ver un análisis técnico detallado de Pinkslipbot, consulte el *Informe de McAfee Labs sobre amenazas: junio de 2016*. En el informe se describe el proceso de infección inicial, los mecanismos de propagación, los detalles técnicos y los métodos generales de protección.

Recomendaciones y procedimientos para protegerse frente a Pinkslipbot

A continuación se indican algunas recomendaciones y procedimientos generales que le ayudarán a protegerse frente a Pinkslipbot.

Para proteger el perímetro, debe bloquear los puertos que no se utilicen en todos los puntos de salida de la red, las solicitudes de conexión desde y hacia direcciones IP maliciosas asociadas conocidas y el uso de recursos compartidos de la red, con el fin de impedir el desplazamiento lateral de Pinkslipbot. En la mayoría de los entornos, también debe desactivar la función AutoRun de Microsoft Windows. Es fundamental actualizar los sistemas operativos y las aplicaciones Windows con los parches más recientes, así como el software antimalware a la última versión.

En los sistemas que no tienen los últimos parches instalados se pueden aprovechar las vulnerabilidades. Por lo tanto, es esencial una correcta gestión de los parches en todos los entornos. Cuando el proveedor distribuye los parches, se deben probar, verificar e implementar de manera inmediata. Para reducir las posibilidades de que se aprovechen las vulnerabilidades conocidas debe haber previsto otro mecanismo para el caso de que no sea posible aplicar los parches debido a dependencias de una versión anterior. Una estrategia agresiva de aplicación de parches es uno de los métodos más eficaces para reducir los efectos de Pinkslipbot y de otros tipos de malware.

Aunque Pinkslipbot se distribuye principalmente a través de descargas desapercibidas de sitios web que han sufrido un ataque de un kit de exploits, las víctimas suelen llegar a estos sitios web desde mensajes de correo electrónico de phishing. Si se clasifica el correo electrónico como "interno" o "externo", es más fácil para los usuarios identificar los mensajes falsificados o de phishing y pensarlo dos veces antes de hacer clic en enlaces maliciosos.

Pinkslipbot se ejecuta parcialmente en la memoria, por lo que no basta con aplicar los parches a los sistemas, realizar un análisis completo y ejecutar una herramienta de eliminación de malware. En los sistemas infectados es preciso reiniciar para eliminar el malware de la memoria y ejecutar otro análisis a fin de garantizar que el sistema está limpio. Además, recomendamos que se empleen contraseñas seguras para evitar los ataques de diccionario, se desactive AutoRun y se aplique el principio del mínimo de privilegios.

Pinkslipbot es una evolución del tristemente célebre troyano Zeus. Para sufrir una infección de Pinkslipbot basta con utilizar una contraseña no segura para acceder a un sistema Windows, incluso sin la intervención de un kit de exploits ni la interacción del usuario. Una vez que un sistema está infectado, cualquier actividad realizada en él se registra y se envía a los ciberdelincuentes. Tras la introducción de la comunicación personalizada y segura con sus servidores de control, Pinkslipbot es más difícil de detectar y analizar. Además, su historia nos permite concluir que con cada iteración se hará más peligroso. Si conoce su entorno y pone en práctica nuestras recomendaciones, puede minimizar los daños que puede provocar Pinkslipbot.

Cómo puede ayudarle la tecnología de McAfee a protegerse frente a Pinkslipbot

McAfee VirusScan Enterprise (VSE) y McAfee Endpoint Security (ENS) 10

McAfee VirusScan Enterprise y McAfee Endpoint Security 10 proporcionan protección antimalware para los endpoints. McAfee VirusScan Enterprise se ha sustituido por McAfee Endpoint Security 10, que ofrece mejor rendimiento y una plataforma optimizada. Los DAT de McAfee para McAfee VirusScan Enterprise y McAfee Endpoint Security 10 incluyen funciones de detección y limpieza para los componentes de Pinkslipbot. McAfee VirusScan Enterprise y McAfee Endpoint Security 10 proporcionan varios niveles de protección mediante la detección en memoria, protección contra rootkits, análisis de comportamientos y mecanismos estáticos.

Si necesita otros niveles de protección contra nuevas variantes, puede implementar reglas de protección de acceso para evitar que Pinkslipbot infecte los sistemas.

- Cree y pruebe una regla de protección de acceso para impedir la ejecución de procesos y la creación de ejecutables en C:\Users*\AppData\Roaming\Microsoft**.exe.
- Cree y pruebe una regla de protección de acceso para impedir que los procesos cscrpit.exe y wscript.exe puedan leer, ejecutar y crear archivos WPL desde la carpeta %LOCALAPPDATA%\Microsoft\. Normalmente estos son archivos de JavaScript. Al bloquear dichos archivos se impide que el malware descargue nuevas versiones.
- Cree y pruebe una regla de protección de acceso para impedir que los procesos cscrpit.exe y wscript.exe puedan leer y ejecutar archivos desde la carpeta %UserProfile%, cuando sea posible.
- Cree y pruebe una regla de protección de acceso para impedir que "updates_*new.cb", "upd_*.cb" y "updates*_new.cb" puedan ejecutar y crear nuevos archivos. Los archivos de configuración de Pinkslipbot suelen usar estos archivos. Al bloquearlos, se impide que el malware se pueda actualizar.
- Cree y pruebe una regla de protección de acceso para los puertos del 65200 al 65400 para los procesos iexplorer.exe y explorer.exe. Como Pinkslipbot se inyecta en esos procesos, al impedir que se utilicen estos puertos se evita que Pinkslipbot se comunique con su servidor de control.

- Implemente y pruebe reglas de protección de acceso para impedir la ejecución remota de los archivos autorun.inf.

McAfee Host Intrusion Prevention (HIPS)

McAfee Host Intrusion Prevention protege los sistemas frente a amenazas de tipo zero-day mediante la combinación de un sistema de prevención de intrusiones basado en comportamientos y firmas, con un firewall dinámico con seguimiento de estado. Las actualizaciones de contenido programadas protegen los sistemas frente a las vulnerabilidades de las aplicaciones y el sistema operativo, incluso antes de que haya parches disponibles. La protección del entorno mediante el empleo de firmas impide muchos de los métodos que utiliza habitualmente el malware para atacar el software más utilizado.

- Pruebe y active la firma incorporada McAfee HIPS 6010 (Protección frente a interceptación de aplicaciones genéricas).
- Pruebe y active la firma incorporada McAfee HIPS 6011 (Protección frente a invocación de aplicaciones genéricas).
- Aísle los sistemas infectados por Pinkslipbot asignándoles una directiva por la cual el firewall bloquee todos los puertos, excepto los de administración.

McAfee Endpoint Security 10 y McAfee Host Intrusion Prevention se incluyen en McAfee Complete Endpoint Protection.

McAfee Web Gateway (MWG)

Las descargas desapercibidas y los enlaces incluidos en mensajes son métodos muy utilizados por Pinkslipbot para propagarse. McAfee Web Gateway ofrece seguridad web de alto rendimiento, protegiendo los sistemas frente a sitios web maliciosos. Se puede desplegar como un dispositivo de hardware dedicado o como una imagen de máquina virtual.

- Configure McAfee Web Gateway para el filtrado de spam.
  - El filtrado de spam protege contra:
    - IP maliciosas
    - URL maliciosas
    - Mensajes de spam de correo electrónico
- Active la inspección de GAM
- Active McAfee GTI para conocer la reputación de URL y archivos
- Integre la solución con McAfee Advanced Threat Defense para la detección de amenazas de tipo zero-day y de entornos aislados.

McAfee Active Response (MAR)

McAfee Active Response proporciona detección y respuesta continuas para los sistemas afectados por amenazas avanzadas como las de Pinkslipbot. La supervisión de eventos automatizada permite detectar los indicadores de peligro que comunican que un sistema ha sido infectado por malware.

- La presencia de los siguientes dominios en una caché de DNS puede ser síntoma de una infección de Pinkslipbot:
  - gpfbvtuz.org
  - hsdmoyrkeqpcyrtw.biz
  - lgzmtkvnijeaj.biz
  - mfrlilcumtwieyzbfdmpdd.biz
  - hogfpicpoxnp.org
  - qrogmwmahgcwil.com
  - enwgzzthfwhdm.org
  - vksslxpxaoql.com
  - dxmhcvxcmdewthfbnaspnu.org
  - mwtfngzkadeviqtlfrrio.org
  - jynsrklhmaqirhjrtygjx.biz
  - uuwgdehizcuuucast.com
  - gyvwkxfxqdargdooqql.net
  - xwcjchzq.com
  - tqxllcfn.com
  - feqsrxswnumbkh.com
  - nykhliicqv.org
  - ivalhlotxdyvzyxrb.net
  - bbxrsgsuwksogpktqydlkh.net
  - rudjqypvucwwpfejdxqsv.org
- Realice la siguiente consulta de caché de DNS para determinar si los sistemas se han comunicado con uno de los dominios de Pinkslipbot conocidos de la lista.
  - DNSCache where DNSCache hostname equals "[dominio Pinkslipbot]"
- Esta consulta devolverá una lista de las comunicaciones establecidas con dominios de Pinkslipbot desde sistemas del entorno. Puede identificar fácilmente qué sistemas se están comunicando con esos dominios haciendo clic en la entrada y mostrando los sistemas relacionados.
- Utilice un firewall local como McAfee ENS 10 o McAfee HIPS para poner en cuarentena los sistemas afectados por Pinkslipbot. Para poner un sistema en cuarentena, asígnele una directiva de firewall bloqueado en McAfee ePO.
- Ejecute un análisis bajo demanda completo de McAfee ENS 10 o McAfee VSE en el sistema. Para ello, debe asignarle una tarea de análisis bajo demanda que se ejecute inmediatamente en McAfee ePO. Active el agente para iniciar el análisis.

Para ampliar la información

Serie de seminarios web de malware de McAfee: Pinkslipbot

Este vídeo ofrece un análisis de Pinkslipbot por región y por sector, con información de sus características y síntomas, así como recomendaciones sobre su prevención.

McAfee
Together is power.

Avenida de Bruselas nº 22
Edificio Sauce
28108 Alcobendas, Madrid, España
+34 91 347 85 00
www.mcafee.com/es