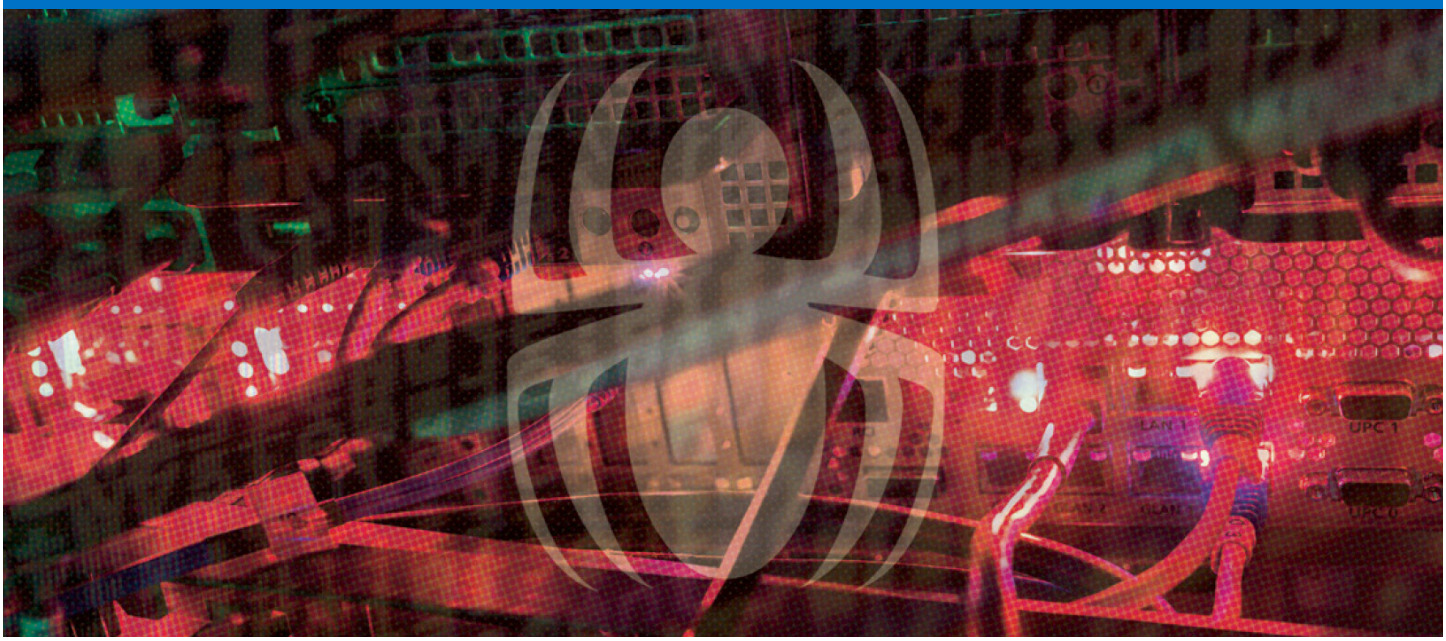
helpsystems

GUIDE *(Cybersecurity)*



Cuando un malware ataca sus servidores IBM i, AIX y Linux

Historias reales

Las empresas de todo el mundo observan que los ataques de malware, incluidos los ransomware como WannaCry y Petya están en aumento. Estos ataques, no solo pueden dar lugar a semanas de inactividad, sino que han sido la causa de algunas de las vulneraciones de datos más dañinas de la historia.

Ante un ataque de malware, una compañía con una defensa sólida podría ahorrarse millones de dólares en pérdida de productividad, investigaciones de vulnerabilidad y corrección, publicidad negativa, pérdida de clientes y demandas judiciales. Esta guía es un manual para proteger sus servidores de virus y otros tipos de malware.

Los malware han existido desde hace décadas, y las empresas saben que deben proteger sus PC de estos programas maliciosos.

Sin embargo, muchas organizaciones no se dan cuenta de que la protección contra malware a nivel servidor también es importante.

Un software anti-malware para sus servidores IBM i, AIX y Linux no reemplazará al software de su PC. Es otra capa de protección y es esencial, a pesar de que a menudo, no se le dé importancia.

"Una organización con la que trabajé no había escaneado su servidor para detectar malware en años. No vieron la necesidad de hacerlo con regularidad y no esperaban que un escaneo fuera a descubrir algo malicioso", afirma Robin Tatam, Director de Tecnologías de Seguridad de HelpSystems.

"Cuando finalmente escanearon su servidor IBM i, se sorprendieron al encontrar 248.095 archivos infectados con CryptoWall, un tipo de ransomware altamente destructivo".

Respecto a Linux, los ataques de malware aumentaron un 300% en 2016, en relación al año anterior.

"Los servidores Linux albergan un número considerable de aplicaciones críticas en el data center. Los atacantes apuntan a ellos porque saben que la infección se extenderá a todos los usuarios que accedan a esos servidores", expresa Bob Erdman, Gerente de Productos de Seguridad de HelpSystems.

En esta guía analizaremos las consecuencias reales de los ataques de malware en los servidores IBM i, AIX y Linux, e investigaremos por qué los programas anti-malware de PC son insuficientes para estas plataformas. También explicaremos las alternativas disponibles, con consejos para implementar una sólida solución de protección contra malware.

```
Browse : /StandGuard/./LOGS/System virus scan task.log
Record : 747947   of  747960 by 14          Column :  1    132 by 79
Control :

....+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....
  Skipped . . : 0
  Errors  . . : 105
  Infected  . : 248095

  Cleaned . . : 0
  Moved . . . : 248095
  Deleted . . : 0

1  File is locked or cannot be opened.
104  Caller denied engine access to either scan or repair.

Completed at Saturday, Aug 01 08:55 PM
2282743 files processed in 78947 seconds (28.91 files/sec)
Task 'System virus scan task' completed with errors. 248095 virus(es) found, 0 f
 ************End of Data*******************

 F3=Exit   F10=Display Hex   F12=Exit  F15=Services  F16=Repeat find
 F19=Left   F20=Right
 1 records folded.
```

¿Qué es el malware y cómo afecta a los servidores?

Encontrar 248.095 archivos infectados no es bueno, pero el efecto del malware en los servidores puede ser mucho peor. Por definición, el malware es cualquier software diseñado para dañar o deshabilitar el sistema informático. Cuando el daño ocurre en un servidor que ejecuta aplicaciones de misión crítica, los efectos pueden propagarse rápidamente. En una compañía de energía estadounidense, las operaciones se interrumpieron después de que un virus afectara a un servidor e impidiera el acceso de muchos usuarios a los datos, causando costosos tiempos de inactividad.

Ahora imagine lo que ocurriría en su organización si una persona desconectara sus servidores, y los datos y las aplicaciones en los que los usuarios confían no estuvieran disponibles. Eso es básicamente lo que sucede con el malware. La pérdida de productividad y la dificultad para restaurar la información desde los backups, insumen recursos valiosos. El escaneo a nivel del servidor lo ayuda a evitar estos resultados.

¿El software anti-malware basado en PC no protege los servidores?

Proteger las estaciones de trabajo es una parte importante de su defensa contra malware, pero confiar únicamente en el software de PC deja a sus sistemas vulnerables de muchas formas. Estas son algunas situaciones en las que el escaneo de malware basado en PC no protegerá a los servidores:

1. Software desactualizado y software que no se ejecuta
Cada vez que salen nuevos virus o malware, las compañías de software deben obtener una copia del programa para identificarlo. Esas definiciones son las que permiten a los motores de escaneo de malware detectar los programas maliciosos. Un malware no definido puede llegar al sistema sin ser detectado.

Una vez que el virus o malware está en su sistema, comienza el daño.

Sin las últimas actualizaciones, su software anti-malware no sabrá cuáles son las nuevas amenazas existentes y no será capaz de proteger su sistema.

"Algunos virus mutan para evitar la actualización del anti-virus. Un virus que ha mutado mientras se encontraba en el sistema no será detectado con la definición original del virus", explica Sandi Moore, Consultora Técnica Senior de HelpSystems. Moore ha dedicado más de una década a ayudar a las empresas de distintas industrias a proteger sus activos de IT contra ataques de malware.
Sin las últimas actualizaciones, su software anti-malware no sabrá cuáles son las nuevas amenazas y no podrá proteger su sistema.

Si un usuario de PC deja de ejecutar el software, usted no tendrá protección. Esto puede sonar exagerado, pero los usuarios son una variable que no puede controlar. Algunos pueden apagar accidentalmente el escaneo de malware y virus; o bien, una persona de la Mesa de Ayuda puede apagarlo intencionalmente mientras soluciona un problema y olvidarse de habilitarlo nuevamente.

No importa cuál sea la razón, el resultado es el mismo: no hay protección contra malware para ese equipo, y sin una protección a nivel del servidor, toda su organización está en peligro.

2. Conexiones VPN
Los empleados que trabajan de forma remota a menudo utilizan una VPN para conectar sus dispositivos personales a la red. Según el software VPN que utilice, es posible que no tenga ningún control si estos equipos ejecutan software anti-virus o anti-malware o, en caso de que lo hagan, si el software está actualizado. Si los dispositivos que usan sus empleados no tienen protección contra malware, la protección está desactualizada o el software no se ejecuta, un virus podría llegar a su red.

3. Las estaciones de trabajo no son la única fuente de virus y malware

El malware a menudo llega a un servidor cuando una persona carga un documento infectado a un directorio, pero esa no es la única forma.

Muchas empresas usan EDI (intercambio de datos electrónico) para e-commerce. Toman pedidos recibiendo un archivo en un directorio mediante FTP, pero como el servidor FTP que envía los archivos no tiene ningún software anti-virus en ejecución, corren el riesgo de recibir un archivo infectado y no hay manera de identificar si un archivo estaba infectado antes de que se subiera al directorio.

Si usa FTP para intercambiar archivos con sus socios de negocios y el servidor de origen carece de protección contra malware, su sistema está en riesgo. Esto es real incluso si sus estaciones de trabajo cuentan con un sólido mecanismo de escaneo.

4. El uso de software de PC para escanear un servidor requiere un nivel de acceso peligrosamente alto

Esta es la situación: usted utiliza una computadora portátil con protección anti-malware y desea usarla para escanear un servidor. Asigna su unidad al servidor y tiene una lista de todas las carpetas que desea escanear desde la PC. El problema es que el software de escaneo todavía se encuentra en la PC, no en el servidor, pero como los datos se encuentran en el servidor, deben transferirse a la PC para realizar el escaneo. Este método produce numerosas exposiciones de seguridad y pone en riesgo a los datos.

Además, este proceso provoca un tráfico significativo en la red, especialmente si el directorio contiene miles de archivos, como ocurre en muchas organizaciones.

Los datos se envían sin encriptar a través de la red, lo que posibilita que una persona pueda "espiar" o leer los datos a medida que pasan entre el servidor y la PC.

A su vez, la ejecución de escaneos desde una PC contra un servidor a menudo da lugar a falsos positivos, ya que el software basado en PC no entiende los matices de los archivos creados en otros sistemas operativos.

Para habilitar el escaneo, se debe definir un recurso compartido para el directorio en el servidor. A menudo este recurso compartido es el directorio raíz, para permitir que se escanee todo el servidor. Esto en sí mismo genera una vulnerabilidad. Terceros podrían asignar una unidad a este recurso compartido y, de esta manera, ampliar las oportunidades para que el malware infecte el servidor.

Por último, para poder escanear todos los archivos y poner en cuarentena y/o solucionar problemas, el usuario que asigna la unidad al servidor debe ser un usuario poderoso, que tenga permiso para ejecutar cada directorio y escanear cada archivo.

Si el usuario poderoso deja permanentemente su PC conectada al servidor, y el acceso a la PC del usuario no está asegurado, esta conexión podría ser usada para obtener acceso a los datos y descargar, destruir o reemplazar archivos y ejecutables, así como también puede ser un medio a través del cual el malware infecte el servidor.

"Cuando usted escanea la PC, necesita acceder a todo lo que se encuentra en el servidor para poder escanearlo en su totalidad. Tener nivel de acceso tan alto desde una computadora portátil que no está siendo monitorizada de cerca, que no tiene definiciones de virus actualizadas, o que podría haber sido hackeada, significa que los hackers y los virus también podrían tener acceso total a su sistema," afirma Moore.

El malware afectó todo el sistema y tomó casi un mes restaurar todo desde los backups.

*"Uno de los peores casos que he visto fue en una compañía que usaba un servidor IBM i, y en la que una persona con permisos especiales para objetos (*ALLOBJ) mapeó una unidad a su servidor un viernes por la tarde. En IBM i, *ALLOBJ otorga el permiso para manipular casi cualquier objeto en el sistema. Esta persona no se dio cuenta de lo que había hecho y dejó la PC en funcionamiento todo el fin de semana. En algún momento antes de irse, abrió un correo electrónico con archivos de ransomware. El malware atravesó todo el servidor, el IFS en su IBM i, y encriptó más de 500.000 archivos, por lo que las actividades regulares que se realizan al cierre del día, se detuvieron. Finalmente, el ataque se descubrió a la semana siguiente. El malware afectó todo el sistema y tomó casi un mes restaurar todo desde los backups".*

¿Qué es el escaneo nativo y cómo protege a los servidores de malware?

Escanear sus servidores con software de PC es una preocupación de seguridad para todas las plataformas. El escaneo nativo de malware elimina estos riesgos mediante el uso de software diseñado específicamente para el sistema operativo que busca proteger.

El escaneo de un servidor desde una estación de trabajo crea un riesgo de seguridad debido a las vulnerabilidades asociadas con mapear una unidad a la PC. El escaneo nativo elimina la necesidad de mapear la unidad y ofrece otras ventajas.

Seguridad: El escaneo nativo no requiere una PC, ni una unidad mapeada conectada a la carpeta raíz con permiso ilimitado y no se transfieren datos sin encriptar a través de la red.

Confiabilidad: El escaneo nativo utiliza cualquier soporte de escaneo de virus integrado en el sistema operativo, como los exit points de anti-virus de IBM i y los valores del sistema. El proceso está completamente automatizado y los archivos se pueden escanear fácilmente, detectando y eliminando todas las amenazas inmediatamente.

Estabilidad: Problemas en la conexión, pop-up de advertencia o cortes de energía pueden hacer que un escaneo basado en PC se detenga. Las soluciones nativas eliminan este problema.

Rendimiento: El escaneo nativo es más rápido que el escaneo de PC, ya que el programa nativo sabe qué atributos de escaneo utilizar para todos los archivos del sistema. Los programas nativos no aumentan la carga de la red, no restablecen el "momento del último acceso" de un archivo y permiten un escaneo más frecuente.

"No importa qué plataforma esté escaneando, debe utilizar el software creado para ese sistema operativo. Eso es el escaneo nativo", dice Moore.

Según lo que se cree habitualmente, el escaneo de malware no es necesario para AIX y Linux porque no hay muchos programas maliciosos que afecten a esos sistemas operativos. Sin embargo, esto no es cierto y los profesionales de IT comienzan a darse cuenta.

"Si sus servidores AIX y Linux son vulnerables, entonces los sitios web y los servicios que proporcionan estos sistemas también lo son. Las personas que utilizan estos servicios pueden infectarse o transferir su infección a su data center. Los atacantes están aprovechando todas las vulnerabilidades para comprometer y tomar el control de los recursos del data center", explica Erdman.

Durante años, muchos profesionales de IT no escanearon los servidores IBM i porque creían en el mito de que IBM i es inmune a los virus. Es cierto que un virus de PC no puede infectar al sistema operativo de IBM i, pero el IFS de IBM i puede facilitar la propagación de malware.

Si el IFS del sistema operativo se utiliza como un servidor de archivos para archivos de PC, los archivos almacenados en el IFS pueden transportar virus. Por ejemplo, un archivo infectado que se mueve o guarda de una PC al IFS y luego se redistribuye a otra PC, puede transmitirle un virus a la nueva PC.

Moore explica: *"Con malware, IBM i es como María Tifoidea. Es posible que su servidor IBM i no se vea afectado por el programa malicioso, pero puede actuar como un huésped y mecanismo de entrega y, de esta manera, propagar el malware al resto de su red".*

Es comprensible creer que su sistema es seguro si no usa el IFS. *"Sin embargo, el mismo sistema operativo de IBM i utiliza el IFS, lo que significa que cualquier persona que ejecute IBM i utiliza el IFS",* afirma Robin Tatam.

La amenaza de malware para estos servidores es real y el daño puede ser devastador, especialmente si se tiene en cuenta que IBM i, AIX y Linux se utilizan a menudo en industrias que valoran la confiabilidad, como las de finanzas, ventas al por menor y salud.

Recientemente, el sector de salud se ha convertido en un objetivo común para los ataques de ransomware. Ofrecer a los profesionales de salud acceso oportuno a los datos de los pacientes es esencial para brindar atención de calidad. Los atacantes lo saben y creen que es muy probable que los hospitales paguen un rescate para restaurar el acceso a esos datos.

El equipo de Servicios de Seguridad de HelpSystems trabajó con una organización de salud que se vio afectada por dos ataques diferentes de malware en una semana.

El primero estuvo dirigido a los directorios y les cambió el nombre; el segundo fue un ransomware. Mientras se ocupaban de resolver el primer ataque, la compañía dejó de compartir la raíz. Afortunadamente, esto redujo los datos que se encriptaron a solo los de la PC del usuario que abrió el archivo adjunto infectado.

Hay tres cosas que todo administrador de sistemas IBM i debe hacer para evitar que el malware se propague por todo el sistema:

1. **No comparta el directorio raíz.** Compartir la raíz no solo significa compartir el IFS sino también /QSYS.LIB (todas las bibliotecas del sistema). Si se debe compartir el directorio raíz, reduzca su acceso a un recurso compartido de solo lectura.
2. **Reduzca la autoridad *PUBLIC del directorio raíz.** Cambie el valor predeterminado de DTAAUT (*RWX) OBJAUT (*ALL) a DTAAUT(*RX) OBJAUT (*NONE). Esto es el equivalente de cambiar *PUBLIC (*ALL) a *PUBLIC(*USE).
3. **Ejecute un software anti-virus nativo** en todos los servidores y manténgalo actualizado.

Independientemente del servidor que utilice, identifique vulnerabilidades con regularidad y asegúrese de que el servidor esté configurado de forma segura.

"Al desactivar los servicios y puertos de red de las aplicaciones que no necesita, minimiza la posibilidad de ataque y limita el espacio para que actores maliciosos lo alcancen. Esto reduce su vulnerabilidad incluso antes de ejecutar un análisis de virus", afirma Erdman.

Mejores prácticas para la protección contra malware en IBM i, AIX y Linux

La idea de que no existen virus en los entornos de IBM i, AIX y Linux, aún está vigente. Si bien pueden no ser los objetivos más comunes, los actores maliciosos cambian cada vez más su enfoque a objetivos secundarios como estos servidores con la expectativa de que estén menos protegidos. Muchas organizaciones ya lo han experimentado: el malware puede tener un efecto devastador en los servidores IBM i, AIX y Linux.

Si usted es responsable de proteger estos entornos, el escaneo de malware debe formar parte de su plan de seguridad informática, especialmente si está cubierto por una normativa de cumplimiento que lo requiere, como PCI DSS (Estándares de Seguridad de Datos de la Industria de Tarjetas de Pago) o HIPAA (Ley de Transferencia y Responsabilidad de Seguro Médico).

Independientemente del servidor que utilice, identifique vulnerabilidades con regularidad y asegúrese de que el servidor esté configurado de forma segura.

Proteja mejor sus servidores críticos:

- Asegúrese de utilizar software anti-malware que se ejecute de forma nativa en el sistema operativo.
- Actualice las definiciones de virus a diario.
- Programe escaneos semanales del sistema completo.
- Programe escaneos diarios en directorios con datos confidenciales.
- La programación se puede realizar mediante el comando cron tab (para AIX y Linux) o por softwares externos.
- Revise los registros de los resultados del escaneo.

Si aún no escaneó sus servidores IBM i, AIX y Linux, este es el momento de hacerlo. ¿Recuerda la compañía con 248.095 archivos infectados por CryptoWall? No tenían idea de que el malware estaba en su sistema hasta que pudieron escanearlo. Si la infección no hubiera sido controlada, es muy probable que la compañía hubiese experimentado tiempo de inactividad y operaciones interrumpidas.

Comience hoy mismo

La recuperación de un ataque de malware es costosa y difícil, pero proteger su sistema es muy simple. Compruébelo usted mismo con un escaneo gratuito de virus de HelpSystems. Lo guiaremos a través del proceso, y detectaremos y eliminaremos todos los virus en su servidor.

helpsystems

www.helpsystems.com

Acerca de HelpSystems

Organizaciones de todo el mundo confían en HelpSystems para simplificar su vida informática y mantener sus negocios funcionando sin problemas. Nuestros programas y servicios monitorizan y automatizan procesos, cifran y protegen datos y proporcionan un fácil acceso a la información que las personas necesitan.

HelpSystems, LLC. Todas las marcas comerciales y las marcas registradas son propiedad de sus respectivos dueños.