Software basado en listas negras vs software basado en listas blancas

Libro blanco

Simplifying Computer Management eurosales@faronics.com www.faronics.com
Venture House, 2 Arlington Square, Downshire Way, Bracknell, RG12 1WA, England **Tel:** +44 (0) 1344 741057 · **Fax:** +44 (0) 1344 741067
Faronics EMEA · Registered in England and Wales No. 6923261 · Registered Office: 130 Wood Street, London EC2V 6DL

Introducción

El riesgo causado por el malware en forma de rootkits, virus y troyanos aumenta diariamente. De acuerdo con un informe reciente, las amenazas aumentan exponencialmente, con una media de 73.000 elementos de malware únicos detectados diariamente en el primer trimestre de 2011 . Esto representa un aumento del 26% en los niveles de creación de malware, en comparación con el mismo periodo de 2010.

En respuesta al explosivo crecimiento del malware, las organizaciones demandan soluciones de seguridad más robustas, que a menudo presentan dos enfoques opuestos: listas negras y listas blancas. Este informe analiza el software basado en listas negras, una de las soluciones más comunes que se centra en el manejo de las crecientes amenazas del malware. También analiza el enfoque relativamente nuevo, y menos común, del software basado en listas blancas, para combatir el problema.

Objetivos del malware

Desde que en 1986 se detectó el primer virus en un PC, los niveles de malware han explosionado en los últimos 25 años. Lo que comenzó como una afición de los fanáticos de la tecnología que perseguían el desafío y la fama, se ha convertido en una herramienta esencial para las redes delictivas. Los ciber delincuentes de hoy, son profesionales motivados por los beneficios económicos provenientes del robo y venta de datos protegidos, registros financieros, ficheros de empleados, registros médicos, listas de clientes, y mucho más.

Las herramientas son fáciles de obtener, con paquetes de malware disponibles en Internet. Ahora, hasta personas no técnicas pueden convertirse en hackers en minutos, configurar troyanos y establecer negocios ilegales. El pirateo se está convirtiendo en una profesión tan bien pagada, que los delincuentes están invirtiendo en investigación, programadores y evaluadores para sus ataques, para ir un paso por delante de la seguridad de las tecnologías de la información.

Hoy en día, la web está plagada de riesgos. El 90% de las violaciones de seguridad son provocadas por organizaciones delictivas cuyo objetivo es la información corporativa. Prácticamente todas las violaciones de 2009 estaban relacionadas con malware a medida, que reveló más de 140 millones de registros. Dado el crecimiento de las violaciones de seguridad, las organizaciones están reforzando sus infraestructuras de seguridad en TI.

Efectos del malware

Ahora el malware es más perjudicial, dañino y costoso que nunca. Los informes recientes indican un incremento alarmante en los costes de malware y violaciones de datos.

Coste de las violaciones de datos

Algunas estimaciones dicen que los costes de la ciber delincuencia para la economía de los EE. UU. totalizan apenas millones, mientras que otras, los estiman en cientos de miles de millones. Un estudio de 2010 realizado por el Instituto Ponemon, estimaba que el coste anual medio de la ciber delincuencia para una organización individual víctima de ella oscila entre uno y cincuenta y dos millones de dólares, y la media ronda los 7,2 millones de dólares, lo que muestra un incremento del 7% con respecto al 2009.

Coste de la usurpación de identidad

De acuerdo con un estudio de Javelin Strategy and Research publicado en 2011, el coste anual por usurpación de identidad es de 37.000 millones de dólares, incluyendo todos los tipos de usurpación de identidad y no sólo los medios cibernéticos. Según un artículo publicado en enero de 2011, 11,1 millones de adultos en los EE. UU. fueron víctimas de usurpación de identidad, lo que representa un incremento del 12% con respecto al año 2008. El fraude en los EE. UU. totalizó 31.000 millones de dólares, y en todo el mundo, las empresas perdieron 221.000 millones de dólares anuales a causa de la usurpación de identidad.

Coste de los ataques de día cero

Otra preocupación es el problema de los ataques de virus de día cero, contra los cuales no hay actualmente ninguna defensa garantizada. Las vulnerabilidades explotadas por los ataques de día cero proporcionan una puerta trasera para acceder a cualquier sistema operativo, y representan una seria amenaza para las organizaciones. De acuerdo con el último estudio, las mutaciones del malware están al alza a medida que los atacantes se hacen

cada vez más sofisticados. De media, sólo 15 sistemas se ven afectados por un elemento de malware en particular antes de que este cambie para evitar ser detectado y continúe haciendo estragos.
La sanidad y la educación son los dos sectores objetivo de la mayoría de las violaciones de datos, mientras que los sectores financiero y de administraciones públicas son responsables del mayor número de identidades desprotegidas. Los titulares más recientes indican que no hay sector invencible, ya que incluso algunos de los gigantes empresariales y los líderes en seguridad, han sido víctimas de ataques.

Descripción general de la solución

Una de las categorías más amplias de respuesta tradicional al malware, es la tecnología de listas negras, que incluye soluciones tradicionales de listas negras, como los antivirus y el software antiespía.

Soluciones tradicionales de listas negras

Una lista negra es una lista de entidades específicas, ya sean nombres de dominio, direcciones de correo electrónico o virus, que contiene elementos que se consideran peligrosos o causantes de daños, y a los que por ello se les deniega la entrada a la infraestructura en la que intentan penetrar. Por ejemplo, un sitio web puede encontrarse en una lista negra, porque se sabe que es fraudulento o porque explota las vulnerabilidades del navegador para enviar software espía o cualquier otro software no deseado al usuario.
El concepto de lista negra puede también usarse para prevenir el spam en el correo electrónico. Los usuarios pueden crear una regla en un programa de filtro anti spam para evitar que los correos de un destinatario en particular (o los que coincidan con otros criterios especificados) se entreguen, aunque el programa de filtro anti spam normalmente lo habría permitido.
Son ejemplos comunes de soluciones tradicionales de listas negras, los antivirus y el software anti espía. El software de listas negras funciona bloqueando los riesgos conocidos. Las compañías de software antivirus mantienen una base de datos de virus conocidos que suministran a su suscriptores. Cuando se identifica un nuevo virus, las compañías antivirus crean una defensa específica contra él, y suministran esa actualización a sus usuarios.

Beneficios de la solución de lista negra:

- Las actualizaciones de las listas de virus son automáticas y no requieren un mantenimiento tedioso.
- Permite identificar el malware, y a veces, eliminarlo.
- Las actualizaciones pueden hacerse sobre la marcha, desde un servidor de servicios de actualización.
- Ofrece seguridad y protección completas contra las amenazas actualmente conocidas.
- Es versátil: combate todos los tipos de amenazas de malware.

Inconvenientes de la solución de lista negra:

- Sólo protege contra las amenazas conocidas, lo que a menudo significa que alguien fue víctima de la nueva amenaza para que esta pudiera identificarse por primera vez.
- El malware infecta a una media de 15 sistemas antes de mutar y cambiar su firma, haciéndolo indetectable para las soluciones de lista negra.
- De media, las soluciones de antivirus sólo bloquean el 19% de las amenazas.
- La solución requiere que se identifiquen y se añadan a la lista los virus o el software espía, dejando las máquinas y redes vulnerables frente a ataques de día cero.

- En esencia, los usuarios están dando el control de sus redes a un tercero, y necesitan actualizar continuamente las definiciones de virus y del software espía, lo que aumenta la carga sobre el hardware y sobre el ancho de banda de la red.
- Debido a su propia naturaleza, consume muchos recursos y ralentiza los ordenadores.

Joe, el gestor de la lista de invitados VIP, y la tecnología de lista negra

Joe es el gestor de la lista de invitados VIP en el Bar de la Alta Tecnología. Cada noche, cuando el bar abre sus puertas, es responsabilidad de Joe decidir quién entra y quién se queda fuera. Para ayudar a Joe en este proceso, sus supervisores le proporcionan una lista de personas a las que no se les permite la entrada en el bar. Cuando estas personas llegan a la puerta esperando que les dejen entrar, Joe comprueba la lista, detecta que están en ella, y les deniega el acceso al bar.

Sin embargo, si una persona de la lista se afeita la cabeza y se deja un tupido bigote, la próxima vez que vaya al bar, es posible que Joe no la reconozca. En este caso, lo más probable es que Joe la deje pasar dentro, donde podrá hacer lo que quiera. Además, sólo porque alguien no esté en la lista de "Acceso no permitido", no significa que él o ella no supongan una amenaza para el bar. Sólo significa que el bar todavía no ha pillado a esta persona mostrando un comportamiento no deseado, pero Joe no tiene forma de saber quién puede llegar a ser peligroso.

Soluciones avanzadas de lista negra

Las soluciones de lista negra han evolucionado más allá de la simple prohibición de las amenazas conocidas, incluyendo la heurística. La heurística es la práctica de aplicar el conocimiento basado en la experiencia para resolver un problema. A veces se utiliza junto con el software antivirus para describir la capacidad de investigar y filtrar los ficheros que es probable que contengan un virus informático u otro malware.

El software heurístico busca fuentes conocidas, textos comúnmente utilizados, y patrones de transmisión o de contenidos que históricamente han estado asociados con ficheros que contenían virus. La heurística es un término acuñado por los investigadores de antivirus para describir un programa antivirus que detecta virus a base de analizar la estructura del programa, su comportamiento, y otros atributos, en lugar de buscar simplemente las firmas.

Beneficios de la solución heurística:

- No necesita actualizaciones del fichero de definición.
- Es potencialmente capaz de interceptar ataques de día cero.
- Proporciona otra capa de protección porque no confía totalmente en los ficheros de definición. A veces puede descubrir una amenaza que no esté en la lista negra.

Inconvenientes de la solución heurística:

- Hace suposiciones acerca del problema que intenta resolver y puede producir resultados no siempre óptimos.
- Puede que algunos ficheros legítimos coincidan con el patrón, produciendo muchos "falsos positivos" y retrasando la entrega de ficheros o correos electrónicos válidos.
- La tecnología es relativamente nueva. Hará falta tiempo para desarrollarla y mejorarla.

Joe, el gestor de la lista de invitados VIP, y las soluciones heurísticas

Volviendo al Bar de la Alta Tecnología, nos encontramos con que los supervisores de Joe han decidido probar otro enfoque. En lugar de crear una lista con nombres específicos y fotos de personas a las que no se permite la entrada en el bar, están usando un conjunto más general de reglas para determinar quién puede y quién no puede entrar. Para crear esas reglas, se basan en los tipos de personas que han causado problemas en el pasado. Por ejemplo, a Joe le han dicho que no deje pasar a personas con la cabeza afeitada y bigote tupido, porque en el pasado las personas con este aspecto han causado problemas.

Sin embargo, para sorpresa del dueño del Bar de la Alta Tecnología, su hijo acaba de regresar de un viaje mochilero por Asia con la cabeza afeitada y un mostacho tupido. Joe le echa una mirada y le impide la entrada porque su aspecto encaja con el perfil de persona problemática, a pesar de que el hijo del dueño es un cliente bueno y digno de confianza.

Un enfoque diferente: la solución de lista blanca

La tecnología de lista blanca es opuesta a la tecnología de lista negra. La lista de entidades, ya sean nombres de dominio, direcciones de correo electrónico, o ficheros ejecutables, es una lista sólo de aquello que tiene permitida la entrada en el sistema. Por ejemplo, una lista blanca de nombre de dominio es una lista de URLs que pueden visualizarse, sin tener en cuenta las reglas del programa bloqueador de spam de correo.
El ejemplo más familiar de solución de lista blanca es el correo electrónico en el que los usuarios pueden crear una lista de direcciones de correo electrónico autorizadas, para las que permiten la recepción de mensajes, una vez más sin tener en cuenta las reglas del programa anti spam.
Una de las áreas más importantes de utilización de las listas blancas, la constituyen las listas blancas de aplicaciones. Con las listas blancas de aplicaciones, sólo los programas previamente aprobados tienen autorización para ejecutarse en una máquina, y los programas que no tengan la condición de aprobados, no tienen permiso para ejecutarse.

Beneficios de la solución de lista blanca de aplicaciones:

- Proporciona protección contra el malware, y contra los ataques de día cero y los ataques selectivos, ya que no pueden ejecutarse los ficheros ejecutables no autorizados.
- Mejora la productividad de los empleados y la eficiencia de procesamiento del ordenador, porque no se instalarán ni ejecutarán programas no deseados, como programas de chateo, P2P, software espía, o troyanos.
- Elimina el riesgo de costosas auditorías y multas por falta de cumplimiento de las licencias, ya que no se instalará software ilegal o no licenciado.
- Ahorra dinero a la organización, al reducirse los tiempos de parada de los sistemas, ampliarse los ciclos de vida de los PC, y reducirse el volumen de incidencias, lo que permite crear oportunidades para transferir los costes, haciendo más con menos.

Inconvenientes de la solución de lista blanca:

- La creación de la lista blanca puede ser tediosa, a menos que se utilice una aplicación avanzada de lista blanca.
- La gestión de actualizaciones sin controles avanzados puede representar un reto, ya que las actualizaciones pueden alterar ligeramente la identidad de la aplicación aprobada con respecto a la que ya está aprobada en la lista blanca existente, haciendo que el programa no se ejecute.

Joe, el gestor de la lista de invitados VIP, y la tecnología de lista blanca

Joe, el gestor de la lista de invitados VIP, sigue trabajando en el Bar de la Alta Tecnología. Ahora está probando un tercer enfoque para mantener a los indeseables fuera del bar. Esta vez, sus supervisores han decidido dar a Joe una lista de las personas que tienen autorización para entrar en el bar. Ya no se preocupan por saber quién no tiene permiso para entrar.
Joe no presta atención a quién tiene aspecto de problemático según un conjunto de reglas generales. Simplemente deja entrar en el bar a las personas que están en la "Lista aprobada". Ahora no comete errores y no tiene que preocuparse de si acertará o no. Es mucho más feliz.

Anti-Executable de Faronics

El software Anti-Executable de Faronics utiliza un enfoque diferente para tratar el malware. Anti-Executable permite a los administradores elegir qué aplicaciones tienen autorización para ejecutarse en un ordenador. Cualquier ejecutable no autorizado por Anti-Executable no se instalará ni se ejecutará nunca. Anti-Executable se

basa en el concepto de lista blanca, así que en lugar de configurarse para bloquear ejecutables no deseados en el sistema, se configura para autorizar ejecutables deseados en el sistema.
El valor de las listas blancas de aplicaciones se ha reconocido en la comunidad de TI desde hace tiempo. Sin embargo, las dificultades relacionadas con la creación de la lista blanca inicial y la sobrecarga del mantenimiento de la lista blanca, han impedido que muchas organizaciones adopten esta estrategia de seguridad. Aprovechando las funcionalidades avanzadas, Anti- Executable de Faronics ofrece a las organizaciones los beneficios de la lista blanca de aplicaciones, sin aumentar la carga de trabajo del equipo de TI.

En términos de seguridad, Anti-Executable llena el vacío que las soluciones de antivirus no pueden cubrir solas. Con las decenas de miles de malware que emergen cada día, los programas antivirus no pueden estar a la altura de los terribles niveles de creación. Dada la amenaza que representan el malware mutante, los ataques dirigidos y las amenazas de día cero, confiar en detectar las amenazas conocidas ya no es suficiente. Sabiendo que un programa antivirus tarda una media de 11,6 días en detectar una nueva amenaza, esto deja a las redes corporativas expuestas a riesgos graves durante demasiado tiempo.
Anti-Executable evita que las dos herramientas principales utilizadas en un ataque estén al alcance de los hackers. Protege frente a la ejecución de programas de registro de teclado no autorizados y de programas de control de acceso remoto, que abren las redes corporativas a los delincuentes. Anti-Executable es la protección definitiva frente a ataques de día cero, simplemente porque el software no reconocerá a estos programas ejecutables maliciosos como aplicaciones autorizadas. Como consecuencia de esto, los tiempos de parada provocados por el malware disminuyen significativamente.
Anti-Executable de Faronics ofrece tecnología avanzada de lista blanca para ayudar a los profesionales de TI a minimizar los desafíos que representan las soluciones de lista blanca tradicionales. Incluyendo una opción para configurar la lista blanca en la instalación, que alivia la necesidad de que el personal de TI cree manualmente una nueva lista blanca por máquina. Además, la posibilidad de asignar un estado de editor de confianza a los fabricantes de software como Microsoft, ayuda a los profesionales de TI a gestionar mejor sus actualizaciones, asegurando la continua disponibilidad de las máquinas.
Las soluciones de lista blanca son una opción simple y segura para el control total de los sistemas. El concepto de lista blanca aplicado a la seguridad de ordenadores deja todo el control en manos del administrador, para una tranquilidad aún mayor.

Acerca de Faronics

Con un sólido registro de empresas a las que ha ayudado a gestionar, simplificar, y asegurar sus infraestructuras de TI, Faronics hace posible hacer más con menos, maximizando el valor de la tecnología existente. Nuestras soluciones proporcionan una total fiabilidad de los ordenadores, un completo control de los sistemas, y una gestión de los ordenadores sin interrupciones de energía.

Constituida en 1996, Faronics tiene oficinas en los EE .UU, Canadá, y el Reino Unido, así como una red global de distribuidores. Nuestras soluciones se implementan por todo el mundo en más de 150 países, y están ayudando a más de 30.000 clientes.

Copyright

Venture House, 2 Arlington Square, Downshire Way, Bracknell, RG12 1WA, England **Tel:** +44 (0) 1344 741057 · **Fax:** +44 (0) 1344 741067
Faronics EMEA · Registered in England and Wales No. 6923261 · Registered Office: 130 Wood Street, London EC2V 6DL