PROTECCIÓN ANTE LA INCERTIDUMBRE

TECNOLOGÍA PROACTIVA B-HAVE DE BITDEFENDER PARA LUCHAR FRENTE A MÚLTIPLES AMENAZAS

El panorama actual de las amenazas en la red

Tanto el panorama de la seguridad como la tipología de amenazas a las que se tienen que enfrentar las empresas hoy en día han sufrido importantes cambios durante estos últimos años. Hasta hace poco tiempo, la creación de *malware* partía de la búsqueda de notoriedad por parte de aficionados. Hoy, en cambio, son creadores de código con fines criminales los que crean el *malware* para obtener beneficios económicos. Esta explotación comercial por parte de la industria del *malware* ha sido utilizada para dirigir tanto la frecuencia como la sofisticación de los ataques.

El *malware* alcanza niveles epidémicos

Debido a las más de 3.000 muestras identificadas cada día durante el 2007[1], se ha vuelto extremadamente difícil para los fabricantes de seguridad crear una base de firmas de virus completa y actualizada para proteger los equipos informáticos. Actualmente hay más de un millón de muestras de *malware* conocidas en propagación.

Los ataques de *malware* se han vuelto altamente sofisticados

Hace pocos años, resultaba relativamente fácil mitigar los antiguos riesgos debido a su simplicidad. Las amenazas actuales son mucho más sofisticadas y han sido diseñados específicamente para explotar las vulnerabilidades de las arquitecturas de seguridad tradicionales:

- Amenazas polimórficas transitorias pueden eludir la detección tanto de soluciones de seguridad como de los sistemas de Detección/Prevención de intrusiones (IDSs e IPSs) que se basan en firmas de *malware* reactivas.
- Los ataques web basados en *scripts* buscan constantemente vulnerabilidades potenciales hasta que encuentran una por donde “colarse”. Cada vez más hacen uso de módulos empaquetados, que les permiten ocultar su carga dañina.
- Las técnicas de fragmentación, intercalado e inyección SQL se utilizan para eludir las arquitecturas estáticas y *deeppacket* de muchas soluciones de seguridad perimetral.
- Los equipos portátiles, así como cualquier otro dispositivo móvil y de almacenamiento, pueden actuar como vectores; pueden utilizarse para transportar *malware* dentro de las redes de manera que traspasen completamente el perímetro de las soluciones de seguridad.
- Uso de métodos de distribución muy rápidos para infectar el mayor número de sistemas y en el menor tiempo posible, antes de que los fabricantes de Seguridad puedan lanzar una actualización con nuevas firmas de *malware*.
- El tiempo que transcurre entre el descubrimiento de una amenaza y el lanzamiento de la actualización de firmas de la media de los fabricantes de *software* de Seguridad puede ser de varias horas, o incluso días, lo que constituye una ventana de riesgo mientras el sistema es vulnerable.
- Cada vez son más los equipos infectados que se encuentran interconectados través de la red. Es el caso de los denominados *botnets*[2]. Esta estrategia es una forma altamente efectiva de actualizar el código malicioso residente en los equipos infectados debido a la disminución del tiempo de vida de las firmas de virus – algunas familias de *bots* son actualizadas diariamente-.

---

[1] El malware roza niveles epidémicos: http://www.darkreading.com/document.asp?doc_id=143424

[2] Botnet un término acuñado derivado de las redes zomi. Un botnet puede entenderse como una colección de robots de software malicioso (abreviado bots), cuya finalidad es activar diferente tipo de aplicaciones del equipo controlados por el propietario o diseminador

- En la actualidad, existe *malware* dirigido exclusivamente a un cierto tipo de público o a organizaciones específicas. Este tipo de ataques son más difíciles de detectar por los fabricantes de antivirus que aquellos que van dirigidos a la red en general, retrasando por tanto la creación y puesta en circulación de firmas de *malware*, y por tanto expandiendo la ventana de riesgo.

En pocas palabras, actualmente, el *malware* técnicamente avanzado está demostrando las limitaciones intrínsecas que tienen las soluciones de Seguridad que se basan exclusivamente en firmas reactivas. Esto no quiere decir que este tipo de soluciones estén obsoletas, al contrario, la detección basada en firmas reactivas es aún uno de los métodos de detección de amenazas más preciso. Sin embargo, para hacer frente a las amenazas anteriormente mencionadas este tipo de protección debe complementarse con otras técnicas de detección que:

1. Reduzcan la ventana de riesgo entre el descubrimiento de una amenaza y el lanzamiento de una firma de virus adecuada.
2. Creen una inmunidad ante las técnicas de evasión como las denominadas polimórficas.

Soluciones actuales para las limitaciones de seguridad

La mayoría de las soluciones que cubren la innumerable lista de necesidades de seguridad actuales se basan en el método denominado **Detección Heurística**.

¿Qué es la Detección Heurística?

El funcionamiento de la detección heurística se basa en el principio que dice que si un programa tiene una serie de características o comportamientos parecidos a lo que conocemos como *malware*, posiblemente lo sea. Tanto los virus como el *malware* suelen realizar una serie de acciones específicas diferentes a las de los programas legítimos, haciéndoles detectables.

Aunque conceptualmente parece sencillo, la tecnología que está detrás del proceso es mucho más compleja. El análisis clásico posee una base de datos de firmas de virus (secuencias de bytes extraídas de muestras de *malware*) que se compara con los archivos que se están analizando. Si se encuentra algún archivo que contenga la misma secuencia que la firma con la que se compara en la base de datos, se asume que ese archivo está infectado.

En el análisis Heurístico, además de mantener la base de datos de firmas de virus como en el caso del análisis tradicional, cada firma representa una característica o comportamiento particular exhibido por el *malware*.

Para conocer cómo funciona la detección heurística tomemos como ejemplo un ataque de *phishing* a través de la plataforma de pago PayPal™. Para poder conectarse a la página web de PayPal, se necesita encontrar su dirección IP. Para ello el equipo busca en el archivo Hosts para ver si la dirección IP se encuentra en la lista. (Este archivo contiene un listado que marca los nombres de los hosts con sus correspondientes direcciones de IP).

Si la dirección IP se encuentra, se usará para conectar con la página. En caso de no encontrarse, , el equipo intentará contactar con el equipo del Servidor de Nombres de Dominio (DNS). Un ataque de *phishing* modifica el archivo de Hosts, lo que permite al *malware* la redirección de los usuarios a otra página cuando acceden a la dirección www[punto]paypal[punto]com en la barra de direcciones del navegador web, y llevarlos a una página de *phishing* creada para robar información de los clientes de PayPal. Existen relativamente pocos programas legítimos que modifiquen el archivo de Hosts, por lo que es razonablemente seguro suponer que cualquier programa cuyo objetivo sea el anteriormente citado sea *malware*.

Tipos de Detección Heurística

Existen dos tipos de análisis heurístico: estático y dinámico. Ambos se basan en las “firmas de comportamiento” para identificar *malware*, pero ahí es donde comienzan y terminan sus similitudes.

El **análisis estático** examina la estructura del programa y la programación lógica para comprobar las acciones que realiza la aplicación y determinar qué acciones coinciden con el comportamiento del *malware*.

El **análisis dinámico**, sin embargo, ejecuta el programa en un ambiente virtual para así comprobar exactamente cómo se comporta el programa y determinar qué acciones coinciden con el comportamiento del *malware*.

Cada método tiene sus pros y sus contras. Debido a que los creadores de *malware* suelen utilizar técnicas de cifrado y ofuscación para camuflar su código, puede resultar extremadamente difícil para un análisis estático determinar qué tipo de comportamiento posee el programa. Para superar esta traba, el análisis estático intenta identificar otras características, como la presencia de rutinas de descifrado, que podrían indicar si un programa es o no malicioso. Esto, ciertamente ayuda a mejorar la eficacia, pero sigue significando que el análisis estático tiene una visibilidad limitada de las acciones que realiza un programa.

Por otra parte, los análisis dinámicos no tienen una visibilidad limitada, pero en cambio sufren otra carencia. El ambiente virtual previamente mencionado es, de hecho, un ordenador dentro de otro ordenador, y por tanto requiere recursos adicionales. Además, ejecutar un programa y analizar su comportamiento es un proceso que consume tiempo, un tiempo que degrada el rendimiento del sistema hasta el punto de afectar a la viabilidad operacional.

A esto hay que añadirle que la detección heurística es una ciencia inexacta, y puede ser extremadamente difícil para los fabricantes encontrar el punto medio entre detectar un alto porcentaje de amenazas y mantener un bajo nivel de incidencias de clasificación incorrecta. La viabilidad operacional de las soluciones heurísticas ha sido limitada durante mucho tiempo por los falsos positivos -programas legítimos identificados erróneamente como amenazas. Esto puede causar interrupciones en el trabajo, un uso adicional de soporte técnico, y por tanto, un alto coste total de propiedad (TCO).

La solución heurística ideal debería combinar la rapidez del análisis estático con las habilidades de detección del análisis dinámico, y a la vez mantener un alto grado de precisión. Esto es exactamente lo que ha logrado BitDefender con la tecnología **B-HAVE**.

La Tecnología B-HAVE de BitDefender – La Protección Avanzada Alternativa

B-HAVE, de BitDefender, es un análisis heurístico dinámico especialmente concebido para complementar la tecnología de seguridad actual y ofrecer protección proactiva de última generación, a la vez que supera muchas de las limitaciones de arquitectura inherentes a muchas otras soluciones dinámicas.

Una máxima aproximación

B-HAVE crea un entorno virtual, es decir, un ordenador dentro de otro. Un emulador de sistemas construye un entorno virtual, incluyendo un conjunto de dispositivos de *hardware* virtuales, que imitan la configuración típica de un equipo. El entorno virtual está completamente aislado tanto del equipo como de su sistema operativo u otras aplicaciones instaladas. Cualquier programa puede ejecutarse dentro del entorno virtual sin que su comportamiento o características constituyan el más mínimo riesgo para el equipo.

Para determinar si un programa es malicioso o no, B-HAVE busca aquellas características asociadas con el *malware*. Por ejemplo, puede ser considerado malicioso si intenta modificar ciertos archivos, leer o escribir un área sensible de la memoria o crear un archivo que se asemeje a un virus conocido.

Cuando intente usar un programa sospechoso, B-HAVE retrasará su puesta en marcha hasta que su comportamiento y características sean analizados y catalogados en el entorno virtual. Si no son detectadas acciones maliciosas, B-HAVE lo ejecutará normalmente; si, por el contrario, detecta una conducta sospechosa, B-HAVE automáticamente lo pondrá en cuarentena o eliminará la aplicación (en función de la acción escogida por el usuario)

B-HAVE ofrece al sistema del usuario las siguientes características de seguridad adicionales:

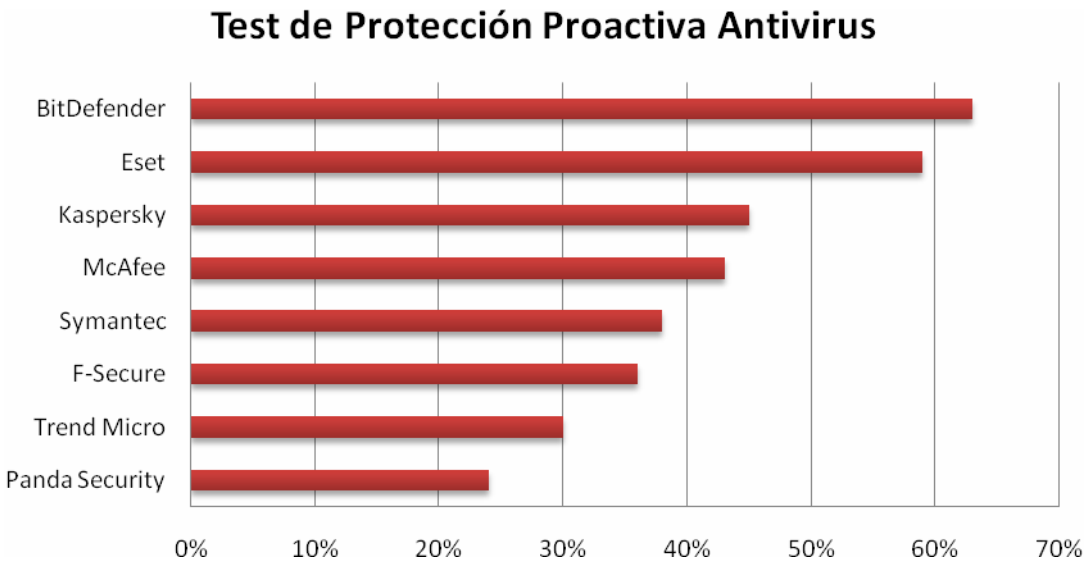
- Métodos genéricos de desempaquetado con soporte de “día cero” para nuevos sistemas de empaquetado
- Tecnología de rutina Visual Basic para la detección proactiva de virus específicos
- Soporte COM para emular por completo virus VB
- Soporte de desempaquetado estático avanzado
- Plataforma independiente bajo sistemas Windows, Linux y FreeBSD
- Emulación embebida BAT/CMD en entorno virtual

Exactitud y Precisión

La tecnología B-HAVE de BitDefender equilibra exactitud y precisión a través de una solución que detecta un alto porcentaje de amenazas junto con unos mínimos falsos positivos sin afectar al rendimiento. Los falsos positivos se evitan mediante una combinación de soluciones técnicas clásicas y avanzadas como:

- Una base de datos de archivos inocuos como son las muestras de *software* instalado o archivos (multi)media
- Un mecanismo inteligente que mantendrá su sistema y archivos en un estado óptimo. Para mantenerlo protegido, B-HAVE marca de forma predeterminada cualquier comportamiento pernicioso. Puede elegir si jerarquizar el análisis del sistema enviando los archivos sospechosos a los laboratorios de virus de BitDefender, mientras los mantiene en cuarentena, en espera de saber si es o no *malware*

Por lo tanto, B-HAVE ofrece protección proactiva inmediata frente a amenazas nuevas o emergentes. Según el estudio independiente realizado en enero de 2008 por el **Anti-Malware Test Lab**[3] el 63% de las amenazas fueron detectadas por ésta tecnología sin necesidad de ninguna actualización de firmas.



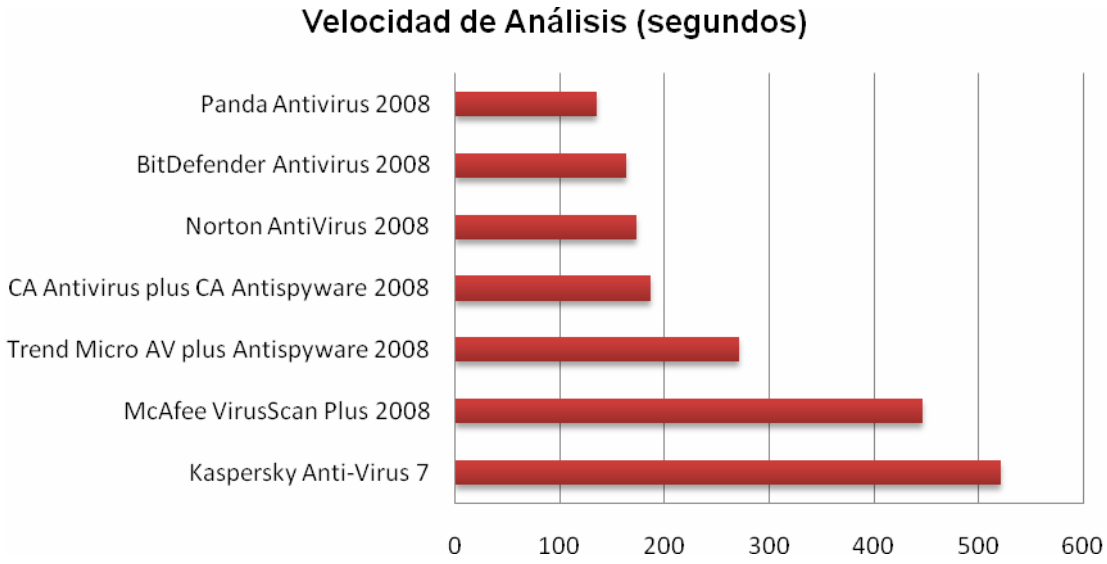
[3] Estudio de Análisis mediante Protección Proactiva: http://www.anti-malware-test.com/?q=node/39

Seguridad dinámica para amenazas dinámicas

Para evitar un descenso de rendimiento, B-HAVE mantiene una lista de secuencias de código conocido, métodos de empaquetado y llamadas del sistema que son funcionalmente emuladas por una rutina acelerada que disminuye en gran medida el tiempo que lleva ejecutar secuencias de código conocido en un entorno virtual.

Además, para reducir el impacto de B-HAVE en los recursos del sistema, el usuario tiene la opción de excluir del análisis aquellos programas que sepa de confianza.

Aunque a primera vista puede parecer un proceso algo lento y complejo, la realidad es que B-HAVE es capaz de completarlo en una fracción de segundo, mostrando las acciones en curso y las posibilidades de elección. El mismo estudio del Anti- Malware Test Lab muestra que la tecnología heurística B-HAVE de BitDefender se encuentra entre los 3 fabricantes con mayor rapidez de análisis:



Sobre BitDefender

BitDefender es el fabricante de una de las líneas más efectivas y rápidas de software de seguridad, certificado a nivel internacional. Desde sus comienzos en el 2001, no ha parado de mejorar y crear nuevos estándares en cuanto a protección proactiva se refiere. La gama de productos de BitDefender protege diariamente a 10 millones de hogares y empresas en todo el mundo, dándoles la tranquilidad de saber que sus gestiones digitales se realizarán de forma segura. Las soluciones BitDefender se distribuyen a través de una red global de distribuidores con valor añadido en más de 100 países de todo el mundo. Para más información, visite: www.bitdefender.es