Internet Security Auditors: Servicio de Vigilancia AntiMalware

Continuamente aparecen noticias del aumento preocupante de *malware* en Internet. Los datos son desalentadores y lo que más preocupa es que incluso sitios en los que se confía pueden haber sido comprometidos y estar contaminando a los propios usuarios sin que los propietarios de las webs tengan conocimiento de ello hasta que es demasiado tarde, teniendo consecuencias catastróficas para la imagen de la empresa. En estos casos, los sistemas antivirus y cortafuegos no son la solución. Ante esta nueva situación, Internet Security Auditors propone su Servicio de Vigilancia AntiMalware, pionero por el innovador acercamiento que ofrece como solución al problema.

Ya hace años que se vivió el *boom* de los *dialers*, donde el lucro económico despertó la astucia de más de uno intentando utilizar sus líneas 906 para enriquecerse. Hoy se vive otro auge, el del *malware* y el de los caballos de Troya bancarios, quienes interceptan las comunicaciones con las web o recolectan datos de los discos duros. El conocimiento se ha re-enfocado hacia el beneficio económico y no hacia el dudoso honor de dejar la firma personal estampada en la web principal de algún conocido sitio de Internet.

La lógica ha empezado a cambiar y ahora quien recibe los ataques en la tranquilidad de su hogar es el usuario. Si se revisan las noticias de tan sólo unos meses atrás, por ejemplo las registradas en abril y mayo, podemos constatar dos grandes oleadas de infecciones automatizadas que afectaron a unos 500.000 sitios y 400.000 sitios web, respectivamente, entre los que se encontraban: **Naciones Unidas**, **Unicef**, el **Departamento de Seguridad Doméstica de EEUU**, el **Servicio Civil del Reino Unido**...[1] o más cercanas a nosotros, la **Agencia Tributaria** española[2].

Algunas veces se es víctima por azar, en otras somos un objetivo específico, como le sucedió al **Banco de la India**, que estuvo ofreciendo un nuevo servicio a sus clientes[3] sin saberlo.

La evolución del *malware* es constante; en lo que llevamos de año prácticamente hemos doblado la cantidad de muestras detectadas (ver **Figura 1**).

La preocupación de las empresas ante estos ataques cada vez es mayor, así como su necesidad de protegerse ante las nuevas técnicas empleadas, que resultan ser cada vez más sofisticadas. La capacidad de detectar un incidente de este tipo limitará enormemente el riesgo al que se expone la organización, teniendo en cuenta las repercusiones que puede tener y el daño que puede causar a su imagen.

Así, resulta necesario disponer de un servicio de vigilancia con capacidad de detectar cualquier *malware* accesible a través de los servicios web de la empresa, y que alerte, en caso necesario y en la mayor brevedad posible, dando la posibilidad de eliminar el riesgo. Éste será un nuevo paso a dar para cubrir un nivel de la seguridad hasta ahora no contemplado.

Éste es el motivo por el que Internet Security Auditors ha desarrollado su **Servicio de Vigilancia AntiMalware**. Este servicio permite reproducir lo que le ocurriría a un usuario que navegara por un determinado sitio web. A diferencia de los *HoneyPots*, donde se simula ser un servidor vulnerable, en los *HoneyClients* se simula un cliente vulnerable que se conecta a las páginas webs para detectar ataques que se produzcan mediante el navegador web del usuario.

Existen dos tipos de *HoneyClients*: de baja-interactividad, que suelen ser servicios o sub-servicios creados simulando la vulnerabilidad, es decir, se programa el error controlado de forma que es posible detectar quién lo aprovecha; y de alta-interactividad, que son sistemas reales a los cuales no se aplican parches de seguridad.

Esta solución está basada en un entorno de alta-interactividad que emplea la virtualización del sistema operativo real, que será capaz de detectar y capturar, incluso los temidos *zero-days –exploits* de vulnerabilidades no publicadas o conocidas– de manera más eficaz y sencilla.

La plataforma está orientada a la navegación de sitios web. Dado que el escenario web es un entorno en continua actualización, resulta necesario determinar mediante una exploración completa todas las posibles URLs a las que podría acceder un usuario que navegara por cada una de las páginas web analizadas. Cualquier modificación o redirección es detectada y analizada por el sistema.

De esta forma, el Servicio de Vigilancia AntiMalware detectará si la URL o, mejor dicho,

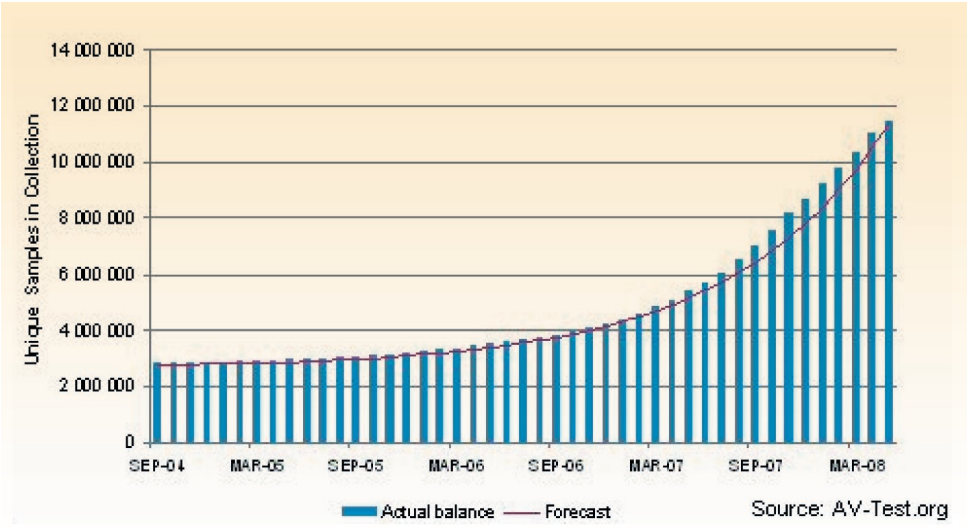

Figura 1: Crecimiento del *malware* entre 2004 y 2008.

[1] Fuente: http://blog.washingtonpost.com/securityfix/2008/04/hundreds_of_thousands_of_micro_1.html

[2] Fuente: http://www.kriptopolis.org/web-hacienda-comprometida

[3] Fuente: http://sunbeltblog.blogspot.com/2007/08/breaking-bank-of-india-seriously.html

si el sitio web contiene algún tipo de *malware* y revelará las acciones que éste realiza contra el sistema operativo. Estas acciones suelen consistir en la alteración de valores del registro de Windows, creación, modificación o eliminación de ficheros del disco, ya sean nuevos ejecutables, librerías del sistema infectadas, o la alteración de los ficheros necesarios para el arranque –como NTDLR–, buscando impedir el inicio correcto del sistema. La plataforma también detectará la aparición de nuevos procesos sospechosos o la muerte inesperada de alguno, como el del navegador web, hecho que alertaría de un intento fallido de explotación de una vulnerabilidad.

Otra característica que sin duda garantiza los resultados del servicio es el análisis desde múltiples entornos de usuario. El hecho de usar diferentes navegadores y sistemas operativos permite cubrir un espectro más amplio de casos y riesgos, por lo que la plataforma amplía el uso a navegadores y versiones con diferentes escenarios como Internet Explorer 6 y 7, FireFox 2 y 3, Safari, Opera, etc.

Aún así, no todos los riesgos los determina el navegador web o el sistema operativo. Fallos en *plugins* de componentes web multimedia como QuickTime, Real Player, Adobe Acrobat, Adobe Flash, Java y un sinfin más de ellos, exponen los sistemas empresariales a una mayor capacidad de explotación por parte del *malware* que puede residir en un sitio *troyanizado*. Recientemente ha trascendido que problemas de seguridad en Adobe Acrobat Reader lo hacen vulnerable ante la simple apertura de un fichero PDF maligno [4] a través del navegador web.

En muchos casos no se aprecia el pequeño cambio que se hace en el sitio legítimo frecuentado habitualmente y que goza de toda confianza, pero una simple referencia hacia un sitio externo truncará toda la seguridad depositada en ese sitio. Y es que, una vez que se carga el sitio web del atacante, el navegador es sometido a un exhaustivo reconocimiento en busca del modelo, versión y *plugins* que tiene, para ser víctima de un *exploit* o varios *exploits* adecuados para cada usuario concreto (ver **Figura 2**).

Cuando la vulnerabilidad haya sido explotada con éxito el sistema del usuario quedará bajo el control del atacante, que desde cualquier lugar, tendrá acceso a toda la información y actividad que se lleve a cabo en ese ordenador.

Si se comete el error de pensar que con un antivirus instalado en el servidor web es suficiente para evitar ésto estaremos equivocados, ya que el resultado de analizar el contenido web es insuficiente debido a que el *malware* no tiene porqué alojarse en el servidor web *troyanizado*, sino simplemente incluir referencias y enlaces externos a sitios malévolos diseñados para alojar el caballo de Troya y que, además, pueden cambiar de IP de forma permanente. Por otro lado, es posible que el usuario con su antivirus personal pueda detectar algunos casos de *malware* que ya lo han infectado, al contrario que la plataforma AntiMalware, que detecta toda la acción de infección sea o no un virus conocido, ya que la detección no se basa en ningún tipo de patrones.

Entre las capacidades del Servicio de Vigilancia AntiMalware se encuentra la habilidad de diferenciar entre las modificaciones producidas por el propio *malware* y las que se corresponden con procedimientos no maliciosos, resultantes de las actualizaciones de software legítimas y de aquellas acciones en las que se confía y son producidas por el uso interno legítimo del sistema operativo y las aplicaciones del sistema.

La plataforma también permitirá modelar las prioridades en las que se deben escanear los dominios según su criticidad o importancia, así como disponer de una notificación ante la detección de actividad malévola prácticamente al instante de producirse, sea ya mediante correo electrónico o SMS.

En definitiva, desde el punto de vista de una empresa, sólo es necesario identificar los dominios, webs o URLs que requieren este análisis y el Servicio de Vigilancia AntiMalware no sólo simulará un usuario navegando por dichos sitios, sino que además proporcionará un exhaustivo informe que advertirá de todas aquellas alteraciones que puedan realizarse en el sistema del usuario. Asímismo, alertará de la situación aportando la información y las evidencias requeridas para poder tomar las medidas de seguridad necesarias y poder realizar un posterior análisis forense sobre el *malware* detectado.

Mientras usted, lector, ha leído este artículo, millones de páginas web se han visto afectadas por *malware,* que, sin saberlo, están distribuyendo códigos dañinos a miles de usuarios. Y esta situación, lejos de desaparecer, crece de forma alarmante, dada la efectividad de este sistema de propagación que, comparado con otros métodos tradicionales, donde la culpa de la *troyanización* recaía enteramente en una posible navegación irresponsable del usuario, ahora se asocia a las empresas que publican sus servicios web en Internet a sus confiados usuarios y clientes. Ante esta nueva situación, el Servicio de Vigilancia AntiMalware implementa un eficaz sistema de detección. ■

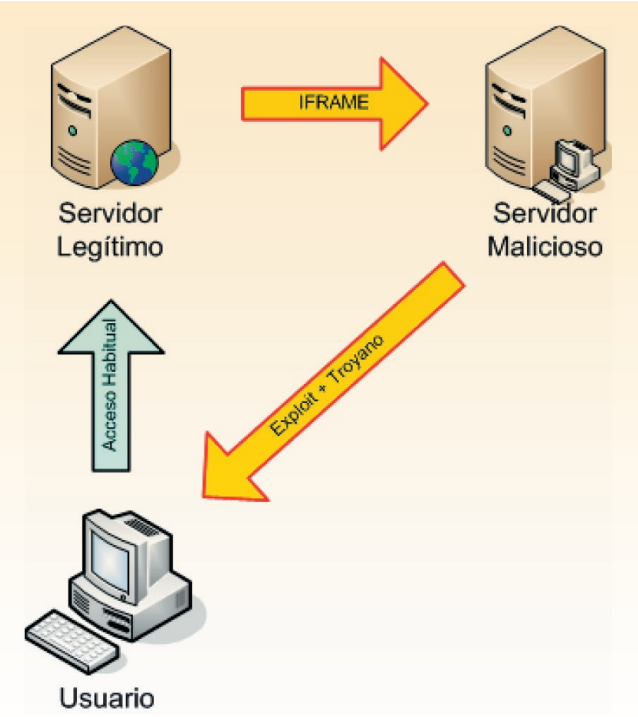

Figura 2: Esquema del funcionamiento de una *troyanización* web.

Nuria Colinas
Responsable de Servicio
ncolinas@isecauditors.com

Ángel Puigventós
Analista de Seguridad
apuigventos@isecauditors.com
Dpto. de Seguridad Gestionada
INTERNET SECURITY AUDITORS

[4] Fuente: http://blog.didierstevens.com/2008/11/10/shoulder-surfing-a-malicious-pdf-author/