Boletines PandaLabs:

Webs legales en jaque

© Panda Security 2008 | PandaLabs
www.pandasecurity.com/homeusers/security_info | www.pandalabs.com

Índice

1.- Introducción

Hoy en día, a pesar de que existe una mayor concienciación de los usuarios frente a los riesgos de Internet, tendemos a pensar que si evitamos acceder a páginas web de dudosa reputación, no podremos infectarnos con malware.

Cuando pensamos en malware alojado en páginas web, tendemos a relacionarlo con páginas web maliciosas o sospechosas, pero nunca nos imaginaríamos que accediendo a páginas web legítimas, nos podríamos llegar a infectar. Sin embargo, los ciberdelincuentes se aprovechan de la confianza que proporcionan ciertos dominios de reputación a los usuarios, como vía para introducir códigos maliciosos en sus sistemas, ya que no existe ningún sistema totalmente seguro.

Esta técnica se está utilizando principalmente para distribuir malware, aunque también podría emplearse para distribuir spam o almacenar datos robados.

En este artículo trataremos de explicar en qué consisten este tipo de ataques, analizaremos algunos de los casos que han acontecido al respecto y la tendencia que cabe esperar. Además, como medidas preventivas, proporcionaremos una serie de consejos para evitar ser víctima de este tipo de ataques.

2.- Funcionamiento

Esta técnica de infección de páginas web legítimas consiste en modificar el código fuente de dichas páginas web, añadiendo una referencia de tipo iframe que apunta a un servidor malicioso.

Para ello, los ciberdelincuentes pueden infectar las páginas web de diferentes maneras:

1. Aprovechando la existencia de vulnerabilidades en el software instalado en el servidor.
2. Aprovechando una mala configuración de los programas instalados y que estén ejecutándose.
3. Robando las contraseñas de acceso al servidor mediante el uso de troyanos.

Para poder modificar el código fuente de una página web, es necesario que se den, al menos, una de las anteriores 3 condiciones mencionadas.

De esta manera, los ciberdelincuentes no sólo consiguen infectar la web de una empresa, sino también utilizar sus servidores para todo tipo de acciones maliciosas, como alojar en el servidor el programa encargado de llevar a cabo las infecciones, distribuir spam o almacenar datos robados.

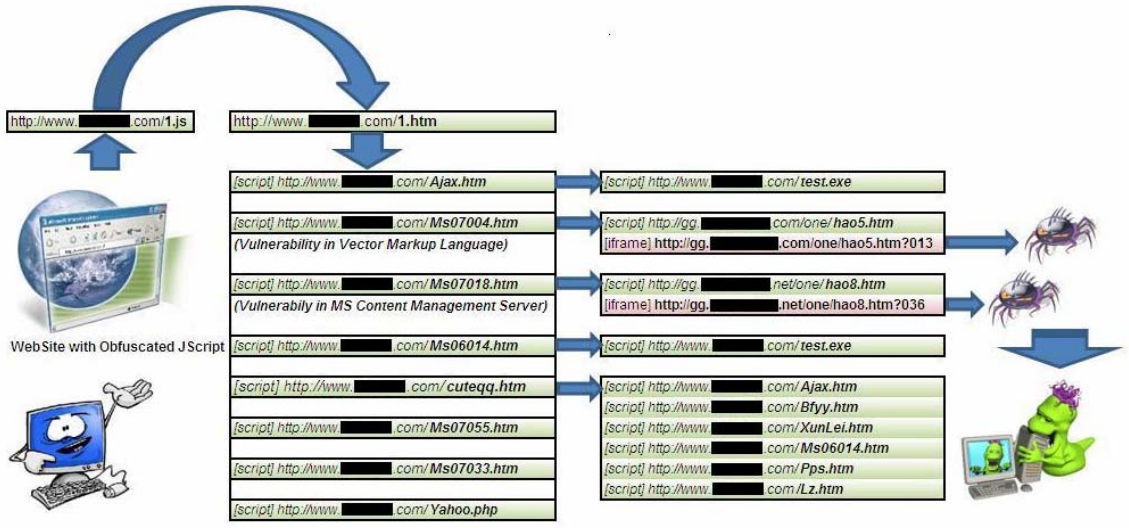
Una vez consiguen acceso a la web, los ciberdelincuentes añaden una referencia de tipo iframe al final del fichero que carga por defecto y que apuntará al servidor malicioso. Inicialmente el usuario no sospechará de la intrusión, dado que la modificación se efectúa en el código HTML de la web legítima, y no será visible para el usuario. Así, cuando un usuario visita una página web en la que han incluido un iframe malicioso, éste establece una conexión, de forma oculta al usuario, con una web que comprueba si el ordenador tiene ciertas vulnerabilidades. Si el equipo está actualizado

frente a esas vulnerabilidades, el usuario no quedará infectado. En el caso de presentar alguna, se procederá automáticamente a la descarga de malware. El tipo de malware que normalmente se descarga esta diseñado para robar contraseñas.

No es casual que el malware elegido para su distribución sea de tipo password stealer, ya que si consiguen un alto grado de efectividad, los ciberdelincuentes podrían obtener grandes beneficios económicos. Este tipo de malware les permite capturar todo tipo de información confidencial, como contraseñas, nombres de usuario, direcciones de correo electrónico, que después podrán utilizar para llevar a cabo acciones fraudulentas.

Respecto a los tipos de exploits utilizados para infectar a los usuarios, en un principio, siempre se optaba por aquellos relacionados con el sistema operativo. Sin embargo, si el usuario tiene parcheado su sistema operativo, no será infectado salvo que se trate de un exploit de día cero, para el que aún no hay parche disponible. Por ello, fueron ampliando el punto de mira de estos exploits a navegadores como Internet Explorer o Firefox y a aplicaciones de uso extendido entre los usuarios como Windows Media Player, QuickTime, Acrobat o Flash Player, entre otros.

Para poder comprender mejor el funcionamiento de este tipo de ataques, ponemos a su disposición el siguiente diagrama:



Ejemplo de ataque a través de iframes

En la imagen se representa el siguiente proceso:

1. Partimos de que existen páginas web legítimas que han sido modificadas mediante la inserción de un iframe malicioso, en este caso *http://www.*<bloqueado>*.com/1.js*.
2. Cuando el usuario visita una página web legítima infectada, dicho iframe establece una conexión con una página web, en este caso: *http://www.*<bloqueado>*.com/1.htm*.
   Esta conexión será imperceptible para el usuario.
3. Esa página web dispone de un listado de vulnerabilidades que intentará explotar en el sistema afectado.
4. En caso de encontrar alguna vulnerabilidad, se procederá a la descarga del malware.

© Panda Security 2008 | PandaLabs

3.- El caso más destacado

En lo que llevamos de año, hay que resaltar los ataques de SQL Injection que han sufrido cientos de miles de servidores. Este tipo de ataques son los que han posibilitado la inserción de los iframes en las páginas web. A principios de abril se detectaron gran cantidad de servidores que habían sido comprometidos. Sus páginas fueron modificadas para incluir un iframe que apuntaba a un servidor que explotaba diversas vulnerabilidades, entre ellas las siguientes:

- MS06-014: Vulnerabilidad en la función de Microsoft Data Access Components (MDAC).
- MS07-004: Vulnerabilidad en el lenguaje de marcado vectorial.
- MS07-018 : Vulnerabilidades en Microsoft Content Management Server.
- MS07-033 : Actualización de seguridad acumulativa para Internet Explorer
- MS07-055 : Vulnerabilidad en el visor de imágenes Kodak.

Estas vulnerabilidades fueron aprovechadas para la distribución de malware.

Se trataba de ataques de SQL Injection muy bien organizados. Dado el gran número de servidores afectados, el ataque debió de realizarse de forma automatizada, mediante alguna herramienta desarrollada específicamente para escanear servidores, analizar las posibilidades de SQL Injection de cada servidor.

Uno de los ataques más efectivos de SQL Injection fue el que se detectó a principios del mes de abril y que llegó a afectar a medio millón de páginas web. Un problema en la programación de ciertas páginas de tipo asp permitió la inserción del iframe malicioso en cientos de miles de páginas.

4.- Tendencias

Cuando estos casos salieron a la luz, se creó una cierta alarma entre los usuarios, ya que en total fueron millones las páginas infectadas y se trataba de páginas legítimas y de total confianza.

A pesar de la gravedad de la situación, el número de páginas afectadas ha disminuido considerablemente, dado que sus correspondientes administradores tomaron las medidas oportunas para solventar el problema y evitar que se puedan modificar las páginas de sus servidores.

La tendencia que cabe esperar es que continúe en descenso puesto que los administradores de los sitios web ya están informados al respecto. Sin embargo, si aparece un exploit de día cero, hasta que se publique el parche correspondiente, los ciberdelincuentes podrían retomar este tipo de ataques.

Al margen de esto, hay que destacar que previamente a estos ataques, se desarrollaron un buen número de kits de instalación de malware a través de exploits, como el MPack. Este tipo de herramientas están diseñadas para explotar vulnerabilidades con el objetivo de distribuir malware. En estos casos, se trata de páginas web diseñadas por los propios ciberdelincuentes y que suelen utilizar nombres similares a los de las páginas legales para engañar a los usuarios.

© Panda Security 2008 | PandaLabs

5.- ¿Cómo puedo estar protegido?

Desde el punto de vista del usuario, para evitar ser infectado mediante esta técnica, es fundamental tener el sistema correctamente actualizado frente a las vulnerabilidades conocidas y complementarlo con un programa antivirus con tecnologías proactivas, que de igual manera, habrá que mantener actualizado.

Desde el punto de vista del administrador, es importante que mantengan sus servidores actualizados para que no presenten vulnerabilidades, asegurarse de que las páginas que permitan un acceso a su base de datos, están debidamente programadas y modificar periódicamente las contraseñas de acceso al servidor para evitar que otras personas con intenciones maliciosas puedan utilizarlas libremente.

© Panda Security 2008 | PandaLabs