PANDA
CLOUDINTERNETPROTECTION

Simply... Evolution

NAVEGADORES DESACTUALIZADOS
¿ POR QUÉ ES TAN IMPORTANTE LA VERSIÓN?

PANDA CLOUD
OFFICE PROTECTION

PANDA CLOUD
EMAIL PROTECTION

PANDA CLOUD
INTERNET PROTECTION

PANDA SECURITY

INDICE

INTRODUCCIÓN

El software evoluciona con el tiempo. Los parches de seguridad, las correcciones a errores existentes y la inclusión de características adicionales hacen que los fabricantes publiquen nuevas versiones de su software. La mayoría de las empresas entienden la necesidad de instalar dichos parches (y los riesgos de no hacerlo) implementan procesos para hacerlo de la forma más eficaz; sin embargo, ¿qué ocurre con el software que llega al final de su ciclo de vida?

Lo que parece una pregunta sencilla oculta en realidad un dilema bastante complejo. Hay muchísimos casos en el mundo de software antiguo que se sigue utilizando; después de todo, si aún funciona ¿por qué vamos a actualizarlo o reemplazarlo? En otras palabras: "Si no esta roto, ¿por qué arreglarlo?"… Sin embargo, ¿cómo sabemos de verdad si nuestro software esta 'roto'?

He aquí el problema: Si un fabricante anuncia que la versión 1.x de su producto ya no se fabrica y ha sido reemplazada por la versión 2.x, pero luego se descubre un problema grave de seguridad en la nueva versión, ¿también está afectada la versión 1.x? ¿Podemos esperar que el fabricante testee la versión 1.x para determinar si es vulnerable o no, a pesar de que oficialmente ya no haya soporte para al producto? Y si resulta que la versión 1.x es vulnerable, ¿podemos esperar que el fabricante publique un parche para un software que ya no se fabrica?

En un mundo perfecto, la respuesta a todas estas preguntas sería 'Sí', ya que nos gusta creer que los fabricantes cumplirán siempre con la responsabilidad de mirar por la seguridad de sus clientes. Y aunque esto puede ser válido para el software vigente, el anuncio público de que una versión de software ha llegado a su fin de vida también es un aviso de que el fabricante ya no se siente obligado a preocuparse por la seguridad de la versión —lo que supone que el usuario debe seguir utilizándola "bajo su propia responsabilidad".

En caso de que las versiones posteriores de un software sufran vulnerabilidades, existe un riesgo considerable de que las versiones anteriores (discontinuadas) también sean vulnerables debido a la práctica habitual de reciclar código. Sin embargo, es probable que no haya ninguna notificación pública, ni por parte del fabricante ni por parte de terceros, de que la versión antigua es vulnerable. Los investigadores de seguridad no suelen dedicar sus recursos a analizar versiones antiguas o discontinuadas desoftware en busca de nuevas vulnerabilidades, ya que la respuesta del fabricante es siempre la misma: sólo nos preocupa la versión nueva.

Echemos un vistazo al caso de los navegadores Web. La última versión de Internet Explorer es la versión 8, aunque las versiones 6 y 7 siguen todavía siendo utilizadas por una gran parte de la comunidad de usuarios. Pero ¿qué pasa con la versión 5.5 (discontinuada)? ¿Debería seguir siendo utilizada o representa un riesgo de seguridad demasiado grande? ¿Y qué sucede con versiones anteriores (y discontinuadas) como la 5.0 o la 4? La versión 5.5 fue la última versión compatible con Windows 2000 y es bien sabido que Windows 2000 incluye vulnerabilidades de seguridad no resueltas.

Tomemos otro ejemplo. La última versión de Mozilla Firefox es la 3.6, aunque las versiones 3.0 y 3.5 siguen siendo utilizadas por un gran número de usuarios. Pero ¿qué hay de las versiones (discontinuadas) 1.5.x, 1.0.x, o incluso las versiones anteriores a la 1.0 (0.x)? Por lo menos se ha encontrado una vulnerabilidad en la última versión de la serie Firefox 1.5.x (publicada unos meses después del fin de vida del producto).

NAVEGADORES DESACTUALIZADOS: DESAFÍOS Y PROTECCIÓN

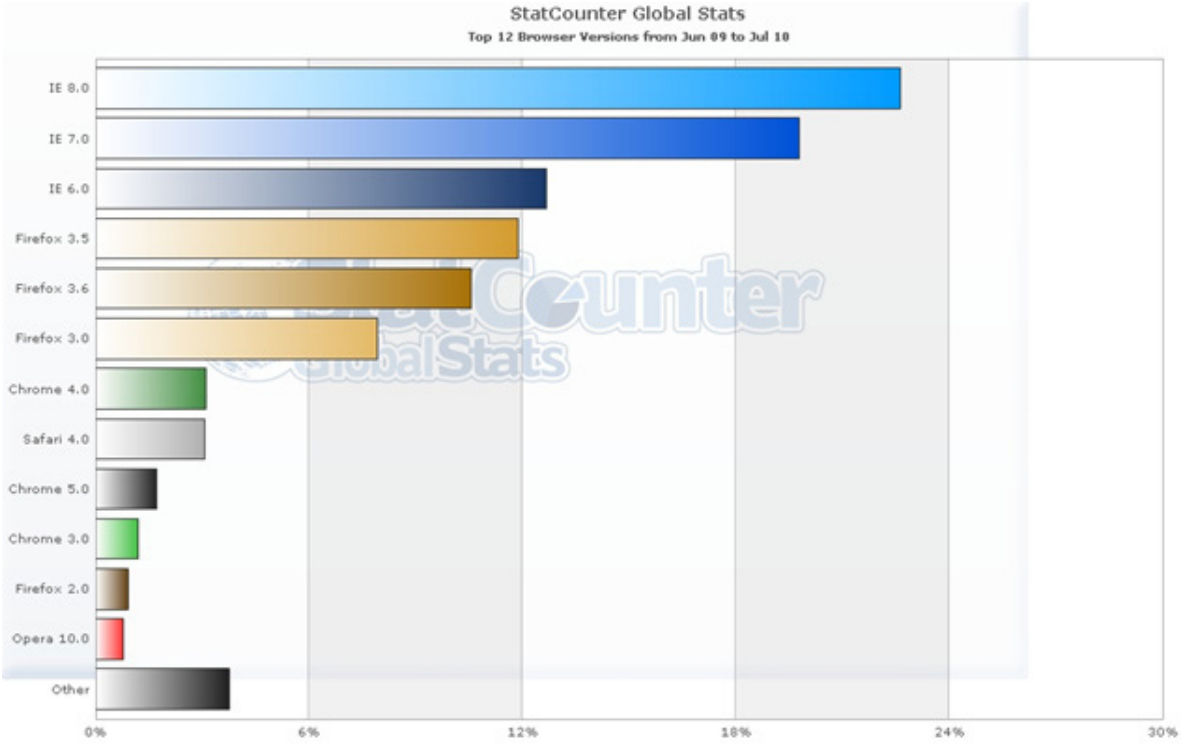


Imagen 1 – Cuota de mercado de las diferentes versiones de los navegadores, junio 2010; Información cortesía de StatCounter

AMENAZAS QUE AFECTAN A LOS NAVEGADORES DESACTUALIZADOS

Los riesgos principales que implica tener un navegador desactualizado son los siguientes:

- Los navegadores desactualizados o discontinuados pueden estar afectados por las mismas vulnerabilidades descubiertas en versiones posteriores de los mismos.
- Como el fabricante no ofrece soporte para la versión, no publicará parches para sus vulnerabilidades y probablemente ni siquiera habrá notificaciones públicas de su existencia.
- Las funciones de seguridad más avanzadas (alertas integradas de phishing, verificación extendida SSL, cuadros de diálogo sobre opciones de seguridad, etc.) sólo se encuentran en las versiones más recientes de los navegadores.

LA SOLUCIÓN PANDA CLOUD INTERNET PROTECTION (PCIP)

La solución PCIP es capaz de reconocer y clasificar los navegadores Web a través de su identificador Usuario-Agente. La solución ofrece la posibilidad de establecer políticas que especifiquen qué navegadores (y versiones) pueden o no tener acceso a Internet.

Esto ofrece un control granular sobre los navegadores que se usan en la empresa, minimizando el riesgo de que navegadores antiguos o desactualizados sean atacados, ya que no tendrán acceso a Internet.

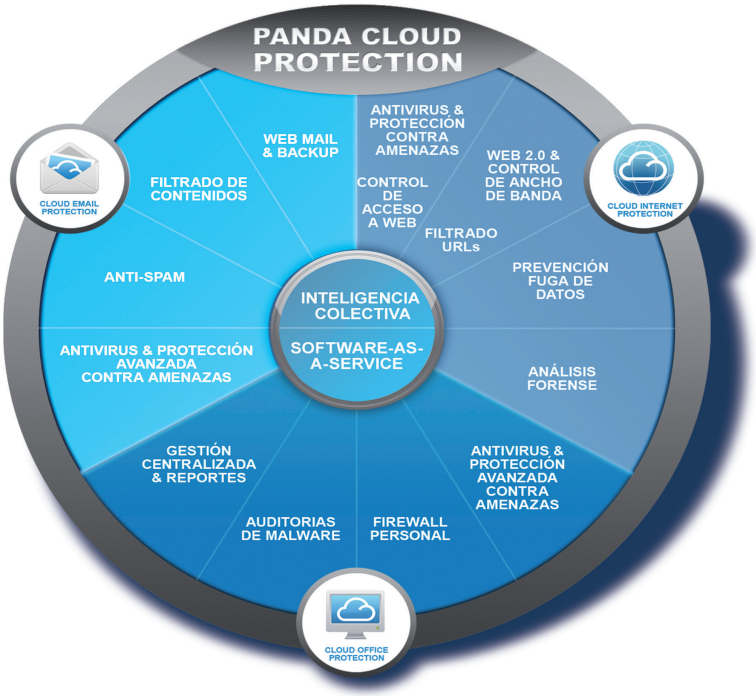
SUITE PANDA CLOUD PROTECTION

Panda Cloud Internet Protection es parte de la suite Panda Cloud Protection, una completa solución de seguridad SaaS que protege los principales puntos de entrada de las amenazas -endpoints, correo electrónico y tráfico Web- contra el malware, spam, cross-site scripting y otros ataques avanzados Web 2.0, mediante una solución ligera, segura y sencilla.

Esta suite de seguridad está basada en la nube, ofreciendo máxima protección, reduciendo el gasto y aumentando la productividad. La solución se despliega en cuestión de minutos y se gestiona de forma sencilla gracias a la intuitiva Consola de Administración en la Nube única de Panda. La suite Panda Cloud Protection se beneficia de la gran capacidad de la Inteligencia Colectiva: un sistema basado en la nube que almacena 21 terabytes de conocimiento y experiencia obtenidos directamente de millones de usuarios.

Panda Cloud Protection ofrece protección completa para el mundo real, no intrusiva e instantánea contra el malware conocido y desconocido.

Panda Cloud Protection se beneficia del poder de la nube para proporcionar protección en tiempo real contra las amenazas conocidas y desconocidas en cualquier momento y en cualquier lugar, gracias al poder de la Consola de Administración en la Nube.



PANDA SECURITY

EUROPE
Ronda de Poniente, 17
28760 Tres Cantos, Madrid, SPAIN

Phone: +34 91 806 37 00

USA
230 N. Maryland, Suite 303
P. O. Box 10578, Glandle CA 91209 - USA

Phone: +1 (818) 5436 901

www.pandasecurity.com