Redes sociales y web 2.0: riesgos y tendencias para el futuro

La web 2.0 está caracterizada por un aumento de las acciones online en detrimento de las acciones realizadas en el punto final. Este aumento del uso de Internet no ha pasado desapercibido a los ciber-delincuentes que han buscado infectar páginas web (tanto tradicionales como 2.0) que en principio parecían confiables, para hacer llegar sus creaciones a los equipos de los usuarios. Para dirigir a estos hacia esas páginas web maliciosas los hackers han enviado correos que incitaban a visitar esas páginas usando como gancho un asunto noticioso o sensacionalista (ingeniería social), han "manipulado" los resultados de los buscadores, etc.

03 Feb 2008 | **PANDASOFTWARE**

A

demás, muchas de las páginas web modificadas son elementos claves de la cultura 2.0., como MySpace. En esta página se han registrado ya varios ataques, por ejemplo, mediante la incrustación de código malicioso en los perfiles de los usuarios, de esta manera, todo aquel que visitase esos perfiles sería redirigido a una página maliciosa y quedaría a su vez infectado. También la Wikipedia contuvo durante un breve período de tiempo un link que conducía a una página maliciosa que descargaba en los sistemas un ejemplar de malware.

Los ataques sobre Facebook, Twitter, Orkut, etc., confirman que los ciber-delincuentes siguen a los usuarios allí donde van con el fin de robarles datos confidenciales y obtener con ellos algún tipo de beneficio económico.

Además, con la web 2,0 se ha potenciado la tecnología de contenido dinámico. Sin embargo, las aplicaciones web, pese a su apariencia de sencillez, siguen siendo muy complejas y, además, han añadido a las páginas web una variedad de nuevos códigos y lenguajes, cuya seguridad, en ocasiones, no ha sido del todo verificada. Varios gusanos, por ejemplo, han empleado el lenguaje de AJAX para comprometer la información confidencial de los usuarios de manera online. Estas capacidades remotas pueden proporcionar nuevos métodos de infección a través del navegador, por ejemplo.

Por otro lado, marcos RIA corriendo en XML, Flash, applets y JavaScripts añaden nuevos vectores de ataques posibles. La intoxicación de XML o los ataques XSS en AJAX que

tanto se oyen últimamente son algunos de los nuevas puertas de entrada a los ataques abiertas por la web 2.0.

¿En este sentido, qué se puede esperar para 2008? Principalmente, un aumento de tendencias ya observadas como la infección de páginas web legales mediante el uso de herramientas especialmente diseñadas para automatizar estos procesos y el ataque a redes sociales populares.

También, comenzarán a verse más casos de ataques que intenten aprovechar vulnerabilidades en los nuevos lenguajes ligados a la web 2.0 para distribuir malware.

Además, es probable que también haya que prestar atención a los resultados ofrecidos por los buscadores, ya que la aparición destacada en su índice de páginas que descargan malware ha sido una de las constantes en los últimos meses de 2007 y podría aumentar en 2008.

Para evitar este tipo de ataques, hay una serie de medidas que los usuarios deben tomar:

- Es importante contar con una solución de seguridad instalada en el equipo. Ésta debe estar actualizada y debe contar con tecnologías proactivas, capaces de detectar y bloquear códigos maliciosos (troyanos, gusanos, virus, etc.) desconocidos.

- Es necesario contar con soluciones capaces de bloquear páginas web maliciosas (aquellas que descargan malware en los equipos). De esta manera, si el usuario pincha sobre un link que ha recibido por correo o que le ha ofrecido un buscador y que conduce a una página peligrosa, la solución de seguridad le impedirá el acceso y le avisará del peligro.

Tags: **futuro**, **malware**, **redes_sociales**, **web_2.0**