



Amenaza silenciosa e inminente a REDES CORPORATIVAS

EL DRAMÁTICO INCREMENTO DE AMENAZAS PROVENIENTES DE LA WEB, COMO SPYWARE, VIRUS, TROYANOS, GUSANOS Y OTROS CÓDIGOS MALICIOSOS, ES UNA PREOCUPACIÓN CRECIENTE PARA LAS REDES CORPORATIVAS



**Moshe
Itzkovich**

SOUTH EUROPE
SENIOR SALES
MANAGER
FINJAN

La definición «Spyware» provoca una reacción inmediata a cualquier persona que haya navegado en la Web en los últimos dos años. La mayoría de nosotros estaríamos de acuerdo que está relacionada a contenidos maliciosos que vienen por la Web. El término más amplio para Spyware es Contenidos Maliciosos y cubre una amplia gama de amenazas basadas en la Web: aplicaciones que exhiben anuncios en el escritorio, aplicaciones que capturan los resultados de las búsquedas, keyloggers que interceptan números de tarjetas de crédito y los envían a direcciones remotas de correo o virus troyanos que abren el escritorio a un Hacker remoto. Desafortunadamente, la industria aun tiene que llegar a una descripción unificada para esta área, a menudo confusa y de rápida evolución.

Para poner este nuevo género de amenazas provenientes de la Web en

una perspectiva histórica, recuerde la última vez en que su red quedó fuera de servicio como consecuencia de un virus. Hace algunos años algunos correos electrónicos con asunto inocuo contenían virus o documentos adjuntos maliciosos que solían dejar fuera de servicio los puestos de trabajo prácticamente cada semana. Los adminis-

Hay quienes ofrecen contenidos interesantes de forma gratuita, para mantener a los usuarios online en sus sitios Web el máximo tiempo posible

tradores de sistemas se gastaban horas y a veces días, después de un nuevo ataque de virus, visitando los PCs de los usuarios para reparar el daño.

La situación actual es diferente; el hecho que algunos escritorios en su organización parece que no sean vulnerables y su personal TI les visite menos a menudo no significa que los PCs de su empresa estén libres de

contenido malicioso. Simplemente significa que las reglas del juego han cambiado. La escasez de noticias que describen «otra intrusión masiva de un virus en el ordenador» es otra indicación que algo fundamental en el entorno de la seguridad TI ha cambiado.

En el entorno informático actual, la conectividad es ilimitada y la Web es accesible universalmente a cualquiera que busque información sobre cualquier tema. La Web provee infinitas fuentes de información así como oportunidades emocionantes de negocio para la corporación moderna. Desde que nosotros escogemos deliberadamente la información que queremos – este método puede ser descrito como «pull» antes que «push».

EL CAMBIO

El cambio del «pushing» al «pulling» de información introdujo una dimensión nueva para la propagación de contenido malicioso como el Spyware. Explo-tando vulnerabilidades en nuestros navegadores de Internet y sistemas operativos, la «silenciosa» instalación del contenido malicioso en nuestras máquinas sin el consentimiento del usuario ha llegado a ser un método muy popular y aparentemente fácil del ataque para el pirata informático ac-



tual. En muchos casos, los usuarios son completamente ignorantes que sus ordenadores han sido comprometidos.

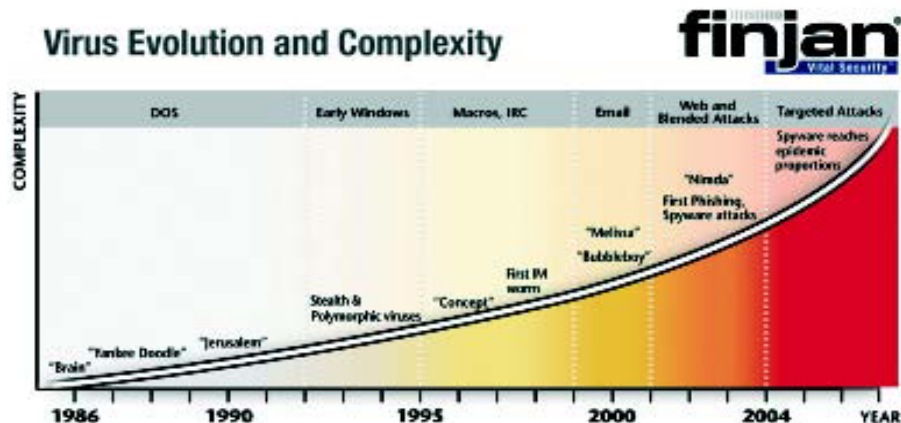
EL NUEVO PANORAMA

Los nuevos modelos de negocio por Internet, están basados en el hecho de que los usuarios están conectados a todas horas. Conociendo los sitios preferidos de los consumidores, así como sus hábitos de navegación y contenidos, las empresas serán capaces de enfocar sus anuncios publicitarios en exactamente lo que el consumidor busca, permitiéndoles incrementar sus ventas. La información corporativa confidencial y su propiedad intelectual también tienen un valor de negocio enorme.

Por este motivo hay quienes ofrecen contenidos interesantes de forma gratuita, para mantener a los usuarios online en sus sitios Web el máximo tiempo posible. Usan códigos maliciosos que «silenciosamente» se instalan en los escritorios de nuestras empresas para espiarnos. Spyware/Adware, Troyanos, y Rootkits son todos nombres de códigos maliciosos que son desarrollados para servir los intereses económicos de criminales «new age».

Estas y otras nuevas amenazas basadas en códigos maliciosos mueven enormes cantidades de dinero. Se estima que Adware por sí solo genera beneficios anuales de cientos de millones de dólares. Los hackers ya no revelan sus «exploits» permitiendo que los fabricantes desarrollen nuevos parches, sino que los venden a criminales. SDKs de Spyware y Troyanos están a la venta, con la garantía de que si el fabricante sacara un nuevo patch, el hacker proporcionara un nuevo exploit desconocido.

Grandes recompensas, financiadas por grandes negocios, por anunciantes y el crimen organizado, están metiendo leña al fuego. El ataque a la priva-



cidad y la propiedad intelectual, así como el robo de identidad están marcando la actividad criminal en la Web.

Está claro que el panorama ha cambiado, conducido por nuevos intereses y ganancias económicas. Hacen falta nuevos métodos para proteger a las empresas y a los usuarios en este nuevo entorno. Es más, para asegurar

**Estas amenazas,
que pueden tomar
control de la red tienen
un impacto directo
sobre los beneficios de
las empresas**

conformidad con requisitos regulatorios, las empresas tienen que tomar medidas para proteger su valiosa información y la privacidad de sus clientes.

¿Qué es lo que realmente entra en mi red?

Muchas organizaciones y grandes empresas no son conscientes de la cantidad y el tipo de tráfico que pasa por sus Firewall, ni tienen una política de seguridad específica para tratar los contenidos activos (como ActiveX,

Java Aplet, Java Scripts, etc.), ni controlan el tráfico encriptado (HTTPS).

Para entender la magnitud de los ataques provenientes de la Web, miremos datos reales y análisis estadísticos de contenidos Web que entran en las redes corporativas. La siguiente información está basada en auditorías de seguridad realizadas en el año 2005 para organizaciones de tres diferentes mercados verticales:

Una empresa de farmacéuticos, una de telecomunicaciones, y una oficina estatal.

Durante un período de dos semanas fue recolectada información en vivo de los contenidos Web, basada en la navegación de unos 5000 usuarios en cada empresa. Estas auditorías fueron realizadas con la aplicación **Vital Web Security™** de Finjan, usando las políticas de seguridad recomendadas por Finjan. Todo el contenido descargado durante ese periodo fue escaneado por la aplicación **X-Ray™** de Finjan. Posteriormente los archivos fueron analizados por los expertos del centro MCRC (Malicious Code Research Center) de Finjan.

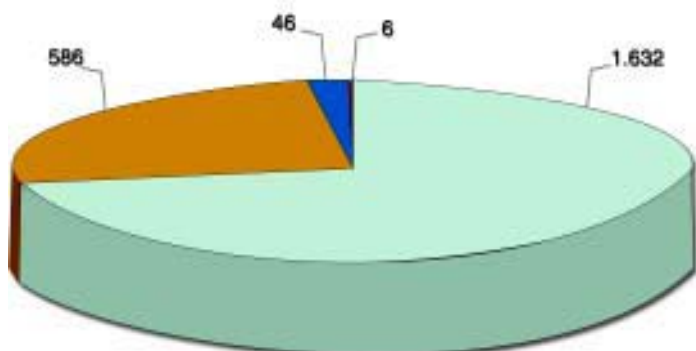
Los principales hallazgos de las auditorías pueden verse en los gráficos.

En vista de los resultados expuestos, la cuestión ya no debería ser si los contenidos activos provenientes de la Web son una verdadera amenaza, sino que es lo que las empresas deben hacer para protegerse de estos tipos



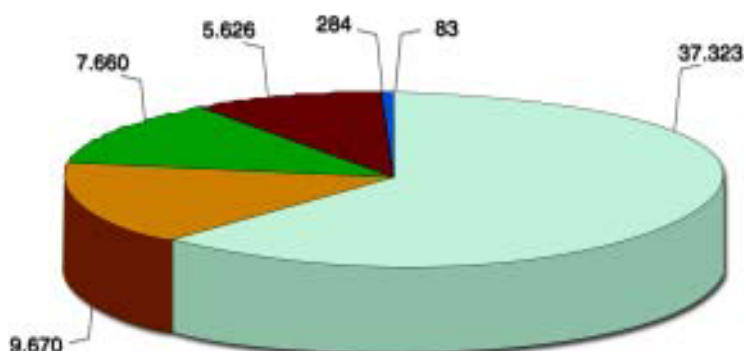
CANTIDAD DE VIOLACIONES SEGÚN TIPO

Empresa de telecomunicaciones

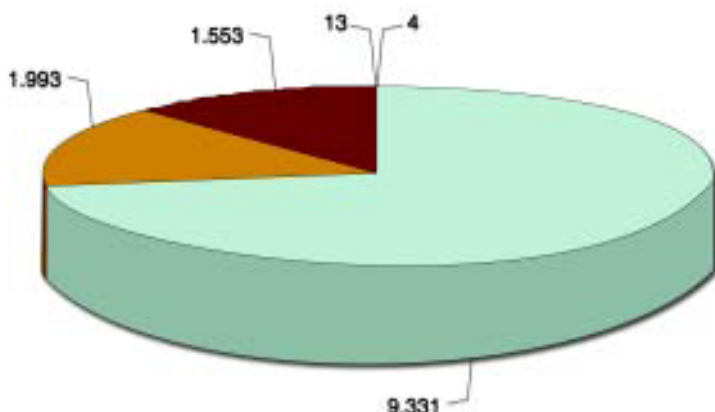


Código malicioso encontrado en el tráfico real de una empresa de telecomunicaciones.

Oficina Estatal



Empresa farmacéutica



Código malicioso encontrado en el tráfico real de una empresa farmacéutica.

de ataques que pueden causar daños enormes.

Un reciente informe de Gartner Group confirma este nuevo enfoque: «Antivirus tradicionales, basados en firmas, ya no son capaces de proteger a las empresas de ataques de código malicioso. Los fabricantes deben elaborar productos y estrategias que se adapten a las nuevas necesidades del mercado para incrementar la protección ante códigos maliciosos». (Gartner, Feb. 2005 Magic Quadrant)

El cambio del «pushing» al «pulling» de información introdujo una dimensión nueva para la propagación de contenido malicioso como el Spyware

El dramático incremento de amenazas provenientes de la Web, como Spyware, Virus, Troyanos, Gusanos y otros códigos maliciosos, es más que una preocupación creciente para las redes corporativas. Estas amenazas, que pueden tomar control de la red, en cuestión de minutos, tienen un impacto directo sobre los beneficios de las empresas, además de exponerlas a robos de identidad, problemas de privacidad y comprometer su propiedad intelectual.

Para hacer frente a estas crecientes amenazas, las empresas realizan grandes inversiones en sus infraestructuras de seguridad de redes.

IDC prevé que el mercado de aplicaciones de seguridad ante amenazas crecerá a un ritmo anual de casi 47.3% entre 2005 y 2009. Este crecimiento se traduce en un volumen de mercado de 2 billones de euros (IDC, Market Analysis, September 2005). ♦