

Tendencias de seguridad: Reflexiones sobre el presente y el futuro

En este documento, vamos a reflexionar acerca de la situación actual en el mercado de la seguridad informática. Para compartir nuestras ideas al respecto, será necesario establecer la diferencia entre dos grupos rivales: los desarrolladores de aplicaciones, y los delincuentes cibernéticos.

Comencemos por describir a estos últimos.

Pareciera que los **criminales informáticos modernos**, generan tres tipos importantes de amenazas:

- **Virus de “estilo antiguo”**
Únicos y descubiertos hace tiempo.
- **Código malicioso personalizado**
Diseñado con un fin determinado y dirigido a un grupo definido de ordenadores.
- **Programas espía “legales”**
Por “legales” nos referimos a un factor muy curioso que atañe a las peculiaridades de las leyes internacionales.

Los productos de seguridad no tienen permitido analizar y descomprimir archivos ejecutables para revelar contenidos fraudulentos, debido a que los desarrolladores de compresores de archivos están protegidos por acuerdos de licencia.

Por lo tanto, si un programa fraudulento es empaquetado por ciertos compresores, entonces está legalmente exento de cualquier acción contra código malicioso.

Es de conocimiento público que el código malicioso personalizado, generalmente se disfraza como una aplicación benigna, o que actúa imperceptiblemente. Un usuario no notará cambio o síntoma alguno, hasta que el dinero de su cuenta bancaria desaparezca en manos de un extraño.

El mejor ejemplo de basura contagiosa es el "señor Troyano", acaparando el 90% (según Symantec) de las infestaciones de Internet. Los gusanos de correo electrónico, también han encontrado activamente el camino hacia los datos informáticos desprotegidos.

Sin embargo, los desarrolladores de soluciones de seguridad se mantienen firmes, y demuestran la tendencia unánime de integrar varios componentes de defensa. Aquellos que calificaron bien como creadores de antivirus, agregaron módulos contra programas espía a sus productos, y viceversa, así como también otros incluyeron la detección de este código malicioso. Por ejemplo, Eset NOD32 Antivirus, PC Tools, Zone Alarm, y Agnitum (en Outpost Security Suite, de próxima aparición), decidieron incrementar los elementos antivirus.

La protección compleja parece ser una medida inevitable. Pero todavía necesitamos comprender que el objetivo de los “ingenieros” del código malicioso moderno no es el vandalismo, o la expresión de sí mismos, sino la ganancia financiera.

El resultado de esta situación, es la creación de códigos maliciosos personalizados, que difícilmente puedan ser detectados por un programa antivirus, ni siquiera por los mejores.

Mal que no puede curarse, debe tolerarse o, mejor aún, prevenirse. Por consiguiente, la defensa proactiva se convierte en un factor indispensable en el mundo de las amenazas de seguridad, una especie de estándar de la industria especializada.

Aquellos desarrolladores que no la tienen en cuenta, demostrando una proactividad débil o inexistente, no logran alcanzar el nivel de seguridad apropiado para Internet.

De forma imparcial, los creadores de Outpost siempre han considerado el enfoque preventivo como prioritario.

El resultado de esta política, es que Agnitum pronto presentará un nuevo paquete integrado de seguridad, que reunirá todos los componentes de defensa existentes: antivirus, control de programas espía y de correo no deseado, etc., además de conservar la habilidad de bloquear el código malicioso en sus etapas iniciales.

Evidentemente, no hay nada de original en este principio, y muchos desarrolladores de aplicaciones de seguridad están tomando este camino. La cuestión, entonces, no es llevarlo a cabo, sino cómo hacerlo.

¿Cómo incrementar las medidas proactivas, hasta llegar a un nivel inalcanzable para los delincuentes informáticos?

Alexey Belkin

Gerente de arquitectura de aplicaciones, en Agnitum Ltd.

19-Marzo-2007