

Las soluciones contra los programas espía han muerto, ¡larga vida a las aplicaciones contra el código malicioso!

En la bitácora (*blog*) de Ryan Naraine, hemos encontrado un artículo denominado "El mercado de soluciones contra programas espía, que en realidad nunca existió, está oficialmente muerto". Como Agnitum ha estado involucrado en este mercado "inexistente", sentimos que era importante hacer un comentario sobre el problema que presentan este tipo de soluciones.

De acuerdo con nuestra experiencia en Agnitum, la idea del autor es técnicamente correcta. Desde el punto de vista del usuario, es difícil separar la función de las soluciones contra programas espía, de la de los antivirus. Cualquiera de las dos opciones, es un problema que necesita ser removido de su ordenador, tan pronto como sea posible. Sin embargo (y a pesar de esta percepción), afirmar que un mercado multimillonario completo solo ha existido en la imaginación de los distribuidores de aplicaciones, es una idea absolutamente distinta.

Generalmente, los desarrolladores de servicios antivirus, han prestado muy poca atención a los códigos maliciosos como troyanos, puertas traseras (*backdoors*), y otros programas dañinos que no son específicamente virus. Por esta razón se crearon los productos específicos contra troyanos, como nuestro **Tauscan**. Pronto aparecieron más aplicaciones maliciosas "exitosas", como registradores de pulsaciones de teclado, reveladores de contraseñas, y otras aplicaciones de este tipo. Y así, como respuesta a estas novedades, nacieron las soluciones contra programas espía. Previsiblemente, a medida que la cantidad de aplicaciones maliciosas aumentaba, los usuarios se fueron cansando de tener que comprar un producto específico para cada problema nuevo. Por lo tanto, la tendencia al desarrollo de soluciones de seguridad integrales que se encarguen de todas las amenazas existentes, es el resultado de una evolución natural.

Las amenazas informáticas actuales, han sufrido un proceso evolutivo similar. Es inusual ver un virus o gusano que actúe de forma autónoma. Es mucho más probable ver un gusano con código espía embebido, que muestra publicidad y abre ventanas; o un *rootkit* que instale un registrador de pulsaciones de teclado, en el disco duro del usuario. El esfuerzo realizado por los desarrolladores de aplicaciones de seguridad, para mantener el ritmo en el progreso contra el código malicioso, está reflejado en la historia de los productos de estas compañías. En Agnitum, comenzamos combatiendo troyanos y posteriormente extendimos nuestras capacidades para derrotar a los programas espía. En la actualidad, también brindamos protección contra virus y gusanos que atacan a través del correo electrónico. Cada amenaza particular, demanda diferentes tipos de investigación. Por esa razón, contamos con dos laboratorios de análisis de códigos maliciosos: uno para virus y gusanos, ubicado en Hungría, en las instalaciones de nuestros asociados VirusBuster; y otro para troyanos, programas espía, y otras amenazas, en San Petersburgo.

Retomando el concepto de Ryan, nuestra conclusión sería que la expresión que define realmente el camino de la industria de la seguridad es: "Las soluciones contra programas espía han muerto, ¡larga vida a las aplicaciones contra el código malicioso!".

Lo cierto es que las amenazas cibernéticas están evolucionando, volviéndose cada vez más complejas. Y los desarrolladores de productos de seguridad, deben afrontar este desafío. En realidad, la protección total del ordenador no se limita a instalar unas cuantas aplicaciones contra determinados programas maliciosos. También incluye la necesidad de incorporar funciones adicionales: cortafuegos, prevención de intrusiones, protección del equipo anfitrión y ataques del tipo **día cero**.

Hoy en día, los ataques **día cero** son uno de los mayores riesgos que afectan a los usuarios de ordenadores. Esto es en parte, porque los antiguos métodos de detección de peligros mediante firmas, simplemente no funcionan contra las amenazas más recientes. En el intervalo de tiempo que transcurre entre el descubrimiento del nuevo código malicioso y la creación de la firma correspondiente, se pueden infectar cientos de miles de equipos. Por esta razón, es realmente importante incluir un cortafuegos en el arsenal de protección personal de cada usuario, así como una defensa proactiva del equipo anfitrión, para enviar a cuarentena las amenazas desconocidas. Finalmente, los productos tradicionales contra programas maliciosos terminarán por completo con la amenaza, eliminando los objetos en cuarentena, tan pronto como esté disponible el código de limpieza adecuado.

Sin lugar a dudas, la industria de las aplicaciones de seguridad independientes, sobrevivirá por algún tiempo más. Pero, simultáneamente, la mayoría de los desarrolladores de este tipo de productos, se inclinará a la creación de soluciones integrales, para que a los usuarios les resulte cada vez más sencillo mantenerse a salvo mientras están en línea.

Mikhail Penkovsky

Vicepresidente global de ventas y comercialización en Agnitum Ltd.

Publicado: 19-Enero-2008