

Panda detecta más de 15.000.000 de códigos maliciosos en 2008

2009-02-20 18:28:11



Durante el año 2008, PandaLabs, el laboratorio de Panda Security, detectó cada día una media de 35.000 ejemplares de malware, 22.000 de los cuales eran nuevas infecciones. A final de año, el número de amenazas detectadas por Panda superó los 15 millones, sobrepasando la previsión inicial de la compañía que era de cinco millones. Para 2009 se espera que estas cifras continúen en aumento.

El informe anual de PandaLabs demuestra que los troyanos, con un 70,1 por ciento del total, fueron el tipo de malware que más ordenadores infectó, seguido del adware (19,9 por ciento) y de los gusanos (4,22 por ciento). Esto supone, pues, que más del 94 por ciento del malware encontrado en los ordenadores de los usuarios era de alguna de estas tres categorías.

Los troyanos bancarios fueron una de las principales amenazas durante 2008. Se trata de un tipo de troyanos cuyo objetivo es conseguir datos bancarios de los usuarios afectados y, así, robarles su dinero. Normalmente, estos troyanos se quedan residentes en memoria y solo se activan en el momento que el usuario accede a la página web de ciertas entidades bancarias. Para ello, los troyanos cuentan con una lista de bancos a los que atacar.

“Para los ciberdelincuentes es relativamente sencillo recibir estos programas maliciosos, ya que existe todo un mercado de venta de troyanos diseñados a la carta y de los denominados kits bancarios, que permiten no solo crear troyanos con múltiples funcionalidades sino controlarlos y enviarles nuevas instrucciones”, explica Luis Corrons, director técnico de PandaLabs.

Respecto a las amenazas que más han crecido en 2008, el informe destaca el papel de los falsos antivirus, un tipo especial de adware que hace pensar al usuario que está infectado con decenas de ejemplares de malware para, a continuación, ofrecerles una versión de pago de un falso antivirus que supuestamente elimina esas infecciones. Los precios de esos falsos antivirus están en torno a los 50 euros y, según las estimaciones de PandaLabs, podrían estar generando unas ganancias a los ciberdelincuentes de unos 10 millones de euros mensuales.

La crisis económica también se ha convertido en un arma para los ciberdelincuentes. Así, en 2008 se ha podido comprobar como a cada bajada de la bolsa le seguía una subida de nuevos ejemplares de malware, y cómo a cada subida del paro le seguía un creció del mandó de spam, especialmente el relacionado con falsas ofertas de trabajo, falsas hipotecas o el destinado a captar muleros (personas que mueven dinero procedente de acciones ilegales de una cuenta a otra para blanquearlo).

El uso cada vez más extendido de las redes sociales ha hecho que sean cada vez más utilizadas por los ciberdelincuentes para distribuir sus creaciones. Junto a ello, la infección de páginas web mediante ataques de inyección de SQL, ha sido otra tendencia al alza, así como la utilización de virus de boot para ocultar troyanos.

El informe anticipa que en 2009 la distribución de malware usando ataques de inyección SQL irá en aumento, y que las redes sociales serán cada vez más explotadas, ya no sólo por gusanos que se propagan entre usuarios, sino por códigos maliciosos diseñados para robar datos confidenciales.

Una tendencia que comenzará a tomar notoriedad en 2009 será el uso de packers y ofuscadores más personalizados para tratar de evitar que los antivirus detecten las muestras de malware. Asimismo, el uso de técnicas antivirus cada vez más avanzadas provocará que los ciberdelincuentes comiencen a realizar uso de viejos códigos adaptados a nuevas necesidades, tales como boots.

Vía | [IDG](#)