

Programas espía

Un 31% de las infecciones registradas por ActiveScan en marzo fueron provocadas por programas espía

En marzo, el spyware supuso un 31% de las infecciones registradas por ActiveScan, la solución online de Panda Software. Estos programas espía se caracterizan por recoger información sobre los hábitos de los usuarios con distintos fines, como puede ser, el de mostrar publicidad personalizada.

Los programas espía infectan un alto número de ordenadores gracias a su forma de distribución. Últimamente, hemos visto un importante aumento en el uso de exploits a través de páginas web como medio para instalar adware. De esta manera, el usuario ni siquiera llega a aceptar las condiciones de instalación de ese código malicioso, como sí ocurría antes. Además, como los usuarios no los han instalado conscientemente, tienen más problemas para detectarlos, lo que facilita su permanencia en los equipos, señala Luis Corrons, Director técnico de PandaLabs.

Los troyanos, con una cuarta parte de las infecciones registradas, fueron el segundo tipo de malware que más daño causó en marzo. Como en meses anteriores, los códigos maliciosos destinados a hacerse con el dinero de los usuarios, como son el spyware y los troyanos, han sido los más detectados.

Un 6% de las infecciones de marzo correspondieron a los troyanos y un 5% a los dialers. Los backdoors y los bots supusieron ambos un 4% de las infecciones registradas.

Como en otras ocasiones, una gran parte de las infecciones corresponden a la categoría denominada otros. Es una muestra más de que no podemos denominar virus a todos los códigos maliciosos. Actualmente, el malware es más variado que nunca. En esta categoría, además de los virus propiamente dichos, encontraríamos Jokes, Hacking Tool, cookies, etc., explica Luis Corrons.

Respecto al malware más activo, destaca el alto número de novedades de la lista. En especial, es llamativa la rápida ascensión de Lozyt.A. Este malware apareció hace apenas un mes y ya es el segundo que más infecciones provoca.

Lozyt.A es un troyano que finaliza los procesos de varias herramientas de seguridad. De esta manera, se asegura de que el sistema que ha infectado queda expuesto a nuevas amenazas. A continuación, él mismo se conecta a un determinado servidor y descarga el adware ErrorSafe.

El malware que más infecciones causó en marzo fue Sdbot.ftp, la detección genérica del script creado para sus descargas por los gusanos de la familia Sdbot. Este código malicioso lleva más de un año encabezando la lista de los más activos.

El tercer puesto es para Brontok.H. Se trata de un gusano que se propaga creando copias de sí mismo en el sistema afectado. El cuarto lugar es para el troyano Clicker.ZJ. Este código malicioso permite llevar a cabo intrusiones contra el ordenador infectado. Es otra de las principales novedades de este mes.

Puce.E ha bajado del tercer puesto al quinto, con respecto al mes anterior. Es un gusano que, para

propagarse, utiliza las redes P2P. El sexto puesto es para Bagle.HX, que ha protagonizado la caída más significativa, pues el mes anterior fue el segundo malware que más infecciones causó. Bagle.HX es una variante de la familia de gusanos Bagle. Para dificultar su detección, esta variante cuenta con funcionalidades rootkit y está diseñada para finalizar los procesos de varias soluciones de seguridad.

Malware % infecciones Puesto anterior
W32/Sdbot.ftp.worm 1,72 1=
Trj/Lozyt.A 1,36 Nuevo
W32/Brontok.H.worm 1,33 4 sube
Trj/Clicker.ZJ 1,26 Nuevo
W32/Puce.E.worm 1,24 3 baja
W32/Bagle.HX.worm 1,16 2 baja
Application/SpyDawn 1,01 Nuevo
Bck/PcClient.DU 0,96 7 =
Trj/KillAV.FG 0,93 Nuevo
Trj/Downloader.NBT 0,91 Nuevo

La séptima posición es para el PUP (Potentially Unwanted Program o programa potencialmente no deseado) SpyDawn. Es otra de las novedades de este mes. Se trata de un supuesto anti-spyware que se instala en el sistema sin el pleno conocimiento del usuario.

PcClient.DU ocupa el octavo lugar. Es un backdoor. Abre un puerto del ordenador para que éste pueda ser controlado por un atacante remoto.

Los dos últimos puestos son para otras tantas novedades. KillAV.FG ha sido el noveno código más activo del mes. Es un troyano que impide el correcto funcionamiento de varias soluciones de seguridad. Además, se conecta a un servidor para permitir el control remoto del ordenador infectado.

El último puesto es para el troyano Downloader.NBT. Este troyano reduce el nivel de seguridad del ordenador al modificar la configuración de seguridad de Internet Explorer.

Fuente: [PandaLabs](http://www.pandalabs.com)

Fecha artículo: 2007-04-03 16:12:40 - url artículo: <http://www.internautas.org/html/4153.html>

Logos y marcas propiedad de sus respectivos autores.

Los comentarios son propiedad y responsabilidad de cada autor.

© 1998-2009 Asociación de Internautas - <http://www.internautas.org>

Inscrita en el Registro Nacional de Asociaciones con el número 164343 - e-mail: asociacion@internautas.org