

## **NOTICIA DE INTERES**

La nueva versión del virus **Zeus**, también conocido como **ZBOT**, puede propagarse a través de los navegadores Explorer y Firefox, según la empresa de seguridad Trusteer.

El virus roba la información registrando las claves que el usuario infectado introduce cuando accede a un listado predeterminado de sitios de Internet. Según se ha hecho público Zeus ha logrado romper recientemente la seguridad del navegador Firefox, y se encuentra en uno de cada 3.000 PC escaneados de los 5 millones analizados.

Su forma de actuar es coleccionar los datos bancarios del afectado, así como sus contraseñas, números de las tarjetas de crédito y otros datos confidenciales para posteriormente venderlos a organizaciones de cibercriminales.

Según parece la tasa de infección de esta versión de **Zeus** es superior a la de ediciones anteriores de este troyano. Como siempre, mantener nuestro equipo actualizado y disponer de un software de seguridad son los mejores consejos para evitar ser infectados por **Zeus**.

### **Panda Security y Defence Intelligence coordinan el cierre de una importante red de bots con autoridades policiales internacionales**

- El trabajo conjunto de investigación conduce a tres arrestos, y aún hay más pendientes
- El robo de datos personales y económicos consecuencia de este ataque informático masivo ha afectado a casi 13 millones de direcciones IP, incluyendo la mitad de las 1000 compañías americanas más importantes.
- Según estimaciones, se calcula que los daños preliminares ascienden a varios millones de dolares.

Según las empresas de seguridad informática **Defence Intelligence** y **Panda Security**, la red de bots Mariposa, diseñada para robar información confidencial, ha sido cerrada por las autoridades y ha dejado de estar en poder de tres presuntos delincuentes informáticos acusados de controlar la red. Los datos robados incluyen información de cuentas bancarias, tarjetas de crédito, nombres de usuario y contraseñas de una red global de unos 12 millones 700.000 equipos comprometidos pertenecientes a usuarios domésticos, empresas, agencias gubernamentales, y universidades de más de 190 países. La red de botnets fue desactivada el 23 de diciembre de 2009 gracias al esfuerzo conjunto de diversos expertos de seguridad y agencias y cuerpos de seguridad, incluyendo Defence Intelligence, Panda Security, el FBI y la Guardia Civil española.

Con casi 13 millones de ordenadores comprometidos, se estima que Mariposa es una de las mayores redes de bots de la historia. Christopher Davis, CEO de Defence Intelligence, la primera empresa en descubrir esta red de bots, explica: "Sería más sencillo para mí dar una lista de las empresas del índice Fortune 1000 que no se han visto afectadas por esta amenaza, que dar el enorme listado de las que sí lo han sido".

Tras el descubrimiento de Mariposa en mayo de 2009, Defence Intelligence, Panda Security y el Georgia Tech Information Security Center crearon el Mariposa Working Group con el objetivo de aunar esfuerzos con otros expertos de seguridad y agencias y cuerpos de seguridad de diferentes países para tratar de eliminar la botnet y llevar a los criminales ante la justicia. El principal botmaster conocido como "Netkairo" y "hamlet1917", así como otros colaboradores, "Ostiator" y "Johnyloleante", han sido arrestados.

"Los primeros análisis indicaron que los botmasters no tenía conocimientos avanzados de hacking. Esto resulta muy preocupante ya que demuestra lo sofisticado y efectivo que se ha vuelto el software de distribución de malware, que permite a criminales sin experiencia causar daños y pérdidas muy importantes.", afirma Pedro Bustamante, Senior Research Advisor de Panda Security. "Estamos muy orgullosos del esfuerzo coordinado realizado por todos los integrantes del Mariposa Working Group y de la rapidez con la que hemos conseguido eliminar esta importantísima red de bots y atrapar a los responsables." A finales del año pasado, el Mariposa Working Group consiguió infiltrarse en la estructura de control de Mariposa y estudiar los canales de comunicación utilizados por los presuntos botmasters. Dichos canales reenviaban información de los ordenadores afectados a los criminales, y son los habituales y muy similares a los también empleados en Zeus, Conficker y Koobface u otros como los utilizados recientemente en las operaciones Google/Aurora. Tras analizar los principales servidores de control ubicados el Working Group fue posible la operación coordinada de cierre de la red de bots Mariposa el 23 de diciembre. En la actualidad, Panda Security está liderando el análisis exhaustivo del malware, así como coordinado las labores de comunicación internacional con otras empresas antivirus para asegurar que sus identificadores de virus están actualizados. Los datos más importantes del análisis preliminar de Panda Security son los siguientes:

- Una vez el cliente de Mariposa infectaba los sistemas afectados, el botmaster instalaba diferentes ejemplares de malware (keyloggers, troyanos bancarios avanzados como Zeus, troyanos de acceso remoto, etc.) para poder realizar más acciones en los ordenadores zombies.
- El botmaster conseguía dinero de diversas formas: alquilando partes de la botnet, instalando toolbars y empleando los datos bancarios y las tarjetas de crédito robadas para hacer transacciones a muleros en el extranjero.
- La red de botnets Mariposa se propaga de forma efectiva a través de redes P2P, dispositivos USB, y enlaces MSN.