Publicado en el 13/12/2013

2014 batirá record de amenazas en Android

A menos de un mes para que comience 2014, Panda Security, The Cloud Security Company, a través del blog de PandaLabs, hace un pronóstico de cuáles serán las principales tendencias en materia de seguridad durante el año que viene. Entre ellas, se augura un crecimiento considerable en lo que a creación de malware respecta; y una continuidad en la existencia de vulnerabilidades en entornos Java y de los ataques en redes sociales.

Ya en el ámbito de la empresa, veremos surgir nuevas soluciones que ofrezcan un nivel de protección que garanticen de forma mucho más efectiva la seguridad de la información. “Ante ataques cada vez más agresivos en el ámbito corporativo, las antiguas soluciones perimetrales siguen siendo necesarias, aunque en determinados escenarios a los que se enfrentan las empresas son completamente irrelevantes. Por ello, veremos surgir nuevas soluciones que respondan a esta demanda y ofrezcan un nivel de fortificación que garantice de forma mucho más efectiva la seguridad de la información”, ha comentado al respecto Luis Corrons, Director Técnico de PandaLabs.

Por otra parte, en materia de movilidad, Android seguirá siendo el principal objetivo de los ciberdelincuentes, y se batirá un nuevo récord de amenazas para esta plataforma. Y todo ello sin olvidar que, junto con los troyanos bancarios y bots, los protagonistas de los ataques que amenazarán a los usuarios serán aquellos que utilizan técnicas de ransomware.

Finalmente, a lo largo de 2014 veremos crecer sustancialmente el número de ataques perpetrados en todo tipo de dispositivos.

A continuación un breve resumen de las principales tendencias en seguridad de cara a 2014, también disponibles en el blog de PandaLabs:

Creación de malware. 2014 será el año de la historia en el que más malware se cree. “La mayoría de este nuevo malware son variantes de malware conocido, que mediante diferentes técnicas cambia de forma para evitar que los productos de seguridad puedan detectar las nuevas creaciones”, agrega Luis Corrons.

Vulnerabilidades. Java ha sido la causa de la mayoría de infecciones ocurridas a lo largo de 2013, y todo indica que lo seguirá siendo a lo largo del año 2014. El hecho de que este lenguaje se encuentre instalado en miles de millones de ordenadores y que tenga un número aparentemente infinito de agujeros de seguridad, hace que sea una de las elecciones predilectas por parte de los ciberdelincuentes. No existe en el mercado negro un Exploit Kit que se precie que no incluya al menos un puñado de vulnerabilidades de Java en su “menú”.

Ingeniería Social. La ingeniería social es un apartado en el que los ciberdelincuentes han brillado por su creatividad. Tras el uso de vulnerabilidades, la segunda causa de de las infecciones que sufren los

usuarios son ellos mismos, tras caer víctimas de algún engaño. Aunque muchos engaños llegarán a través de mensajes de correo electrónico, la mayoría tendrán lugar en redes sociales.

Móviles. Android seguirá siendo el principal objetivo de los ciberdelincuentes, y se batirá un nuevo récord de amenazas para esta plataforma.

Ransomware. Junto con los troyanos bancarios y bots, los protagonistas de los ataques que amenazarán a los usuarios serán aquellos que utilizan técnicas de ransomware: pidiendo un rescate para volver a utilizar el equipo, poder recuperar información (CryptoLocker), eliminar una supuesta infección (Falso Antivirus) o incluso pagar una supuesta multa (virus de la policía). Es un método mediante el que los ciberdelincuentes pueden obtener una ganancia económica directa, motivo por el que estos ataques aumentarán e incluso se extenderán a otro tipo de dispositivos, como los smartphones.

Seguridad en empresas. Ante ataques cada vez más agresivos (como los llevados a cabo por Cryptolocker), las empresas demandarán medidas extras de seguridad que vayan mucho más allá de la protección que les proporciona un antivirus “tradicional”.

Internet of Things. El número de todo tipo de dispositivos conectados a Internet no deja de aumentar, y va a seguir por este camino. Cámaras IP, televisores, o reproductores multimedia ya forman parte de Internet, y en muchos casos además cuentan con una característica que los diferencia de los ordenadores o móviles y tabletas: raramente son actualizados por parte de los usuarios. Esto significa que son extremadamente vulnerables a agujeros de seguridad, por lo que es muy probable que comencemos a ver ataques que tengan como objetivo este tipo de dispositivos.

Datos de contacto:

Nota de prensa publicada en:

Categorías: Ciberseguridad

NotasdePrensa
https://www.notasdeprensa.es