WireLurker, El Malware Ataca Dispositivos De Apple

WireLurker, El Malware Que Ataca Dispositivos Móviles De Apple.

Los investigadores de Palo Alto Networks anunciaron que han descubierto un impresionante **ataque de malware contra los dispositivos de Apple**, que por ahora parece estar limitado a los usuarios de una store de aplicaciones china. La campaña gira en torno a infectar a las aplicaciones de Mac OS X con «**WireLurker**«, el cual recopila registros de llamadas, contactos de la libreta de teléfono y otra información importante en los dispositivos móviles de Apple.

Se encontró que a rededor de 467 **aplicaciones de Mac OS X** que se ofrecen en una tienda de aplicaciones de terceros chino llamada **Maiyadi,** puede ser el foco de **infección de WireLurker**, incluyendo aplicaciones de «Los Sims 3», «Internacional de Snooker 2012» y «Pro Evolution Soccer 2014».

Durante los últimos seis meses, las aplicaciones se han descargado 356.104 veces «y podrían haber afectado a cientos de miles de usuarios», dijo el diario. **Apple** sugiere que los usuarios realicen las descargas de aplicaciones desde la App Store oficial y mantenerse alejados de las **tiendas de terceros por motivos de seguridad**. Al parecer, algunas personas recurren a la **tienda Maiyadi** porque ofrecen aplicaciones gratis, dijo Ryan Olson, director de inteligencia de la Unidad de Palo Alto Red 42, rama inteligencia de amenazas de la compañía.

Palo Alto analiza tres **versiones de WireLurker**, cada uno de los cuales eran mejoras sobre la anterior, dijo Olson en una entrevista telefónica el miércoles. Pero no parece que el ataque WireLurker avanzó más allá de la recolección de datos de los dispositivos móviles. «Desde nuestra perspectiva, todavía se ve como una operación de recopilación de información.»

El **ataque WireLurker** es notable por la forma en que aprovecha las **aplicaciones de escritorio de Mac** como parte del ataque a

iOS. Si alguien descarga una aplicación de escritorio de Mac OS X a partir de Maiyadi, WireLurker llegó junto con él. WireLurker espera entonces cuando un dispositivo iOS se conecta mediante un cable USB. Una segunda versión de WireLurker verifica si el dispositivo de Apple esta liberado con «jailbreak», el plazo para la eliminación de las restricciones que Apple utiliza para evitar que los usuarios ejecuten aplicaciones que no se ha aprobado.

La tercera **versión de WireLurker** dirige los dispositivos iOS que no están con jailbreak también. En esa versión, **WireLurker utiliza un certificado digital** de Apple, el cual es algo bastante dudoso, se presenta para que puedan ejecutar sus propias aplicaciones internas que no aparecen en la **App Store**.

El uso del certificado digital implica que iOS permitiría una aplicación de terceros que se instalará, aunque se muestre una advertencia a los usuarios, dijo Olson. Si un usuario aprueba la instalación, WireLurker podría instalarse junto con una aplicación legítima.

Sin duda, aunque los productos de Apple sean espléndidos, y muchas veces ostenten el título de ser un sistema bastante seguro, vemos que la seguridad en ellos es bastante dudosa, aunque la vulnerabilidad provenga del usuario.