El virus para iPhone se pone feo

autor Aparecen versiones diseñadas para hacer daño
Thursday, 12 de November de 2009

En los últimos días, ha saltado la noticia de que se ha diseñado (y puesto en circulación) un virus para iPhone "jailbreakeados". Se trata de un software diseñado por un programador australiano de 21 años llamado Ashley Towns, basado en un bug, que sólo afecta a los iPhones e iPod Touch a los que se ha roto la protección del sistema de archivos de Apple.

Al parecer el virus original es algo más que una prueba de concepto (porque se ha difundido) pero no pretende hacer daño: su efecto final es avisar al usuario del aparato de que ha sido infectado. Aún así, el autor, que anunció orgulloso su pequeña hazaña, lleva desde entonces recibiendo amenazas y llamadas insultantes. Algo que no sorprende mucho teniendo en cuenta que no sólo hacía aparecer una foto de Rick Astley como fondo de pantalla, sino que el código fuente del gusano incorpora comentarios despreciativos hacia los usuarios que se dejan pillar con sus datos sin proteger ("La gente es estúpida y esto lo prueba, así que leéos el puñetero manual. No es tan difícil tíos. Pero a quién le importa, sólo están en juego tus datos bancarios".)

Además, para difundirse el gusano original necesita no sólo que el aparato esté desprotegido, sino que tenga instalado OpenSSH (algo que a veces va asociado, ya que era esencial para uno de los usos comunes pre-iPhone OS 3.0), y que no se hayan cambiado las contraseñas de usuario root.

Pero apenas dos días después, Intego (no podía ser otro) ha detectado una versión nueva, que ha bautizado como "iPhone/Privacy A", y que no es tan benigna. En concreto, cuando está instalado en una máquina, permite a su controlador conectarse a ella y llevarse puestos datos como los SMS, la agenda o casi cualquier dato de usuario o de las aplicaciones. Es una herramienta de hackeo casi ideal. Y dice que la ha encontrado "en libertad", circulando.

Lo malo (y lo bueno) es que ambas piezas de software se basan en la misma vulnerabilidad, y que su funcionamiento interno es de dominio público gracias al señor Towns. La parte mala es que hasta que se corrija esa vulnerabilidad (por parte de los autores del software de jailbreaking, gente que no ofrece garantías anuales precisamente) pueden aparecer todo tipo de variantes. La parte buena es que sabiendo cómo funciona no debería ser muy difícil remediar el problema.

En resumen

Ambas versiones del virus (estrictamente, un gusano) afectan solamente a equipos jailbreakeados en los que no se ha modificado la contraseña root. Es decir, sólo una parte mínima de los (Intego estima) 8% iPhones e iPod Touch existentes… y en concreto una parte que evidentemente tiene asumido que corre un cierto riesgo al romper el entorno que vende Apple, además de una cierta imprudencia en la gestión de sus claves. Aún así, el daño que esta historia (y estos virus) pueden hacer no es despreciable.

Suele pasar que los virus que descubre Intego son criaturas de laboratorio, casi desdentadas. Esto es porque se enfrentan a un Mac OS X sin romper, y detrás de él está una compañía entera reparando cualquier brecha. Los aparatos que han sido modificados son mucho más vulnerables, y este es un buen ejemplo del riesgo de seguridad que suponen para sus usuarios… y que no ha hecho más que empezar. El jailbreaking tenía un cierto sentido cuando era casi imposible encontrar e instalar herramientas apropiadas para tareas esenciales de un smartphone; ahora, como queda resaltado, es muy poco recomendable.

Por otra parte, el nuevo virus sigue siendo un gusano. Es decir, su capacidad de difusión es limitada… salvo casos de imprudencia notables (para ver modos de prevenirlo, pasad por los foros). El próximo caso puede ser peor.

Puedes comentar la noticia en los foros.