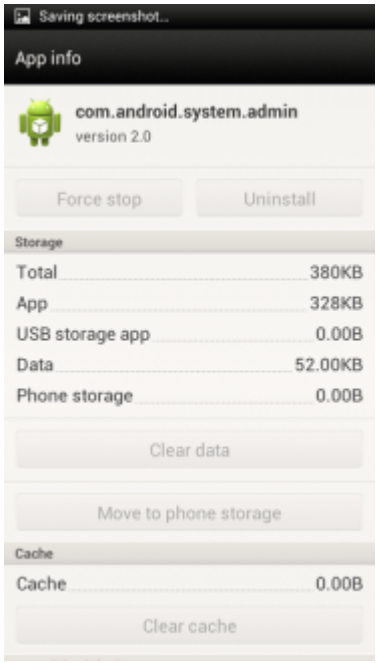
Descubren el troyano más sofisticado jamás creado para Android

Se esperaba que el malware para Android se fuese complicando cada vez más, en términos de patrón de ataques e indectatibilidad, y ya lo está haciendo.



Los expertos de Kaspersky Lab han descubierto un "troyano multifuncional" pensado para causar estragos en terminales gobernados por el sistema operativo de Google con el envío de SMS a números de pago, la descarga de otros programas maliciosos, su instalación y envío a terceros a través de Bluetooth, y el control de comandos de la consola de forma remota. Es decir, toda una joya.

Su nombre es **Backdoor.AndroidOS.Obad.a** o simplemente Obad.a y, más allá de todas sus propiedades, destaca entre el resto de malware para la plataforma del androide verde porque es casi imposible de detectar.

"Es habitual que los creadores de malware intenten que los códigos de sus creaciones sean lo más complicados posible para complicarle la vida a los expertos anti-malware", señalan desde Kaspersky. "Sin embargo, en términos de malware móvil es raro ver un ocultamiento tan avanzado como el de Odad.a", continúan. Y **comparan a este troyano "con el malware para Windows, más que con otros troyanos para Android**, en términos de complejidad y número de vulnerabilidades desconocidas explotadas".

En primer lugar, Obad.a **se sirve de un error en el software DEX2JAR** que los analistas suelen usar para pasar archivos APK a formato JAR. Además, los ciberdelincuentes han encontrado **dos bugs en el propio Android**, uno de ellos relacionado con el procesamiento del archivo AndroidManifest.xml que describe la estructura de una aplicación y define sus parámetros de lanzamiento, y otro que al ser explotado permite a una aplicación maliciosa como ésta ganar privilegios de administrador sin dejar rastro en la lista de apps que disponen de tales privilegios y, por lo tanto, bloquea su eliminación.

Y, por si esto fuera poco, el troyano **carece de interfaz y funciona en segundo plano, lo que dificulta tremendamente su detección**.

Al parecer, lo positivo de todo esto es que Obad.a todavía no está muy extendido y los especialistas en seguridad ya han comenzado a trabajar en métodos para su contención.