Así funciona Triada, el nuevo troyano descubierto en Android

La empresa rusa de seguridad **Kaspersky Lab** ha descubierto un troyano, al que ha bautizado como **Triada**, y que ataca al cerebro de los móviles con marca Android. Dicen los expertos que **los smartphones que se ejecutan en Android 4.4.4.** y las versiones anteriores de este sistema operativo son los que más riesgo de infección tienen.

En principio, ningún país latino aparece en la lista de los más atacados por Triada, que afecta más a Rusia, Ucrania e India, pero los expertos advierten que podría llegar a más regiones.

Según el reciente informe **Mobile Virusology de Kaspersky Lab**, casi la mitad del Top 20 de los troyanos de 2015 eran programas maliciosos con capacidad para robar los derechos de acceso de superusuario, incluso **dando la oportunidad al ciberdelincuente de instalar aplicaciones** sin el consentimiento del usuario.

Entre otros asuntos, **Triada puede modificar los mensajes SMS** salientes enviados por otras aplicaciones. Cuando un usuario está haciendo compras en la aplicación a través de SMS para juegos de Android, los ciberdefraudadores modifican los SMS salientes para recibir el dinero ellos.

De acuerdo con los expertos, "existen **11 familias de troyanos móviles conocidos** que utilizan los privilegios de root" y tres de ellos – **Ztorg, Gorpo y Leech** – actúan en cooperación con los demás.

Dice un comunicado de prensa que normalmente, **los dispositivos infectados con estos troyanos se organizan en una red**, creando una especie de red de bots de publicidad que los agentes pueden utilizar para instalar diferentes tipos de programas publicitarios. Además, tras esto, los troyanos descargan e instalan un backdoor.

En este caso, una característica distintiva de Triada es el uso de Zygote, el cual contiene **bibliotecas del sistema y los marcos utilizados** por cada aplicación instalada en el dispositivo.

Por la complejidad de la funcionalidad del troyano, dicen desde Kaspersky que "es evidente que los cibercriminales que están detrás de este malware son muy profesionales, con un profundo conocimiento de la plataforma móvil".