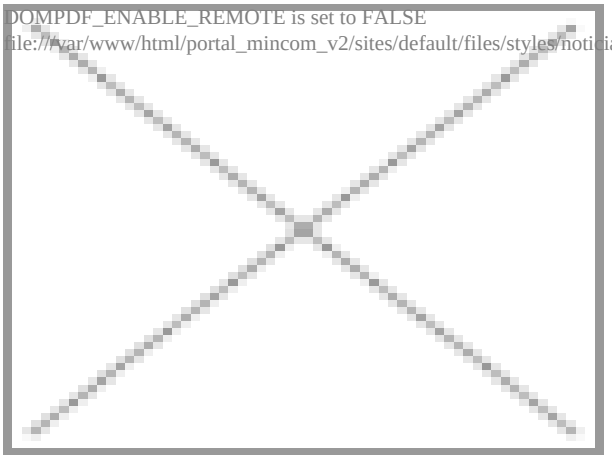

Source:
Diario TI

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.

Kaspersky Lab ha descubierto Triada, un nuevo troyano dirigido a dispositivos Android comparable, por su complejidad, con el malware basado en Windows. Según la empresa de seguridad informática, el malware es sigiloso, modular, persistente y creado por ciberdelincuentes muy profesionales. Los dispositivos que ejecutan la versión de Android 4.4.4. y anteriores son los que presentan mayor riesgo de infección.

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, es decir, que dan a los cibercriminales la posibilidad de instalar las aplicaciones en el teléfono sin el conocimiento del usuario. Este tipo de malware se propaga a través de aplicaciones que los usuarios se descargan/instalan de fuentes no fiables. Otras veces, estas aplicaciones se pueden encontrar en la tienda oficial Google Play y se hacen pasar por una aplicación de juego o entretenimiento. También se pueden instalar durante la actualización de las aplicaciones, incluso en las que están preinstaladas en el dispositivo móvil.

Existen 11 familias de troyanos móviles conocidos que utilizan los privilegios de root. Tres de ellos – Ztorg, Gorpo y Leech – actúan en cooperación con los demás. 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. Pero eso no es todo, poco después de rootear el dispositivo, los troyanos descargan e instalan un backdoor. Esta descarga activa dos módulos que tienen la capacidad de descargar, instalar y ejecutar aplicaciones.

El cargador de aplicaciones y sus módulos de instalación se refieren a diferentes tipos de troyanos, pero todos ellos se han añadido a las bases de datos antivirus de Kaspersky Lab bajo un nombre común – Triada.

Entrar en el proceso de Android

Una característica distintiva de este malware es el uso de Zygote – el creador del proceso de aplicaciones en un dispositivo Android – que contiene bibliotecas del sistema y los marcos utilizados por cada aplicación instalada en el dispositivo. En otras palabras, es un "demonio" cuyo objetivo es poner en marcha aplicaciones de Android y esto significa que tan pronto como el troyano entra en el sistema, se convierte en parte del proceso de aplicación y puede incluso cambiar la lógica de todas sus operaciones.

Las prestaciones de este malware son muy avanzadas. Tras entrar en el dispositivo del usuario, Triada se implementa en casi todos los procesos de trabajo y sigue existiendo en la memoria a corto plazo. Esto hace que sea casi imposible de detectar y eliminar. Triada opera en silencio, lo que significa que todas las actividades maliciosas están ocultas tanto desde el usuario como desde otras aplicaciones.

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

El modelo comercial de Triada

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.

"La Triada de Ztrog, Gorpo y Leech marca una nueva etapa en la evolución de las amenazas basadas en Android. Son los primeros programas maliciosos con potencial de escalar sus privilegios a casi todos los dispositivos. La mayoría de los usuarios atacados por los troyanos se encuentra en Rusia, India y Ucrania, así como los países en APAC. Su principal amenaza está en que proporciona acceso a aplicaciones maliciosas mucho más avanzadas y peligrosas. También tienen una arquitectura bien pensada, desarrollada por los ciberdelincuentes que tienen un profundo conocimiento de la plataforma móvil de destino", afirma Nikita Buchka, analista junior de malware de Kaspersky Lab.

Ya que es casi imposible desinstalar este malware desde un dispositivo, los usuarios tienen dos opciones para deshacerse de él. La primera es rootear el dispositivo y borrar las aplicaciones maliciosas de forma manual. La segunda opción es hacer jailbreak al sistema Android en el dispositivo.

Disponible en: http://diarioti.com/detectan-troyano-que-ataca-al-cerebro-de-los-moviles-android/93061 [1]

Links
[1] http://diarioti.com/detectan-troyano-que-ataca-al-cerebro-de-los-moviles-android/93061