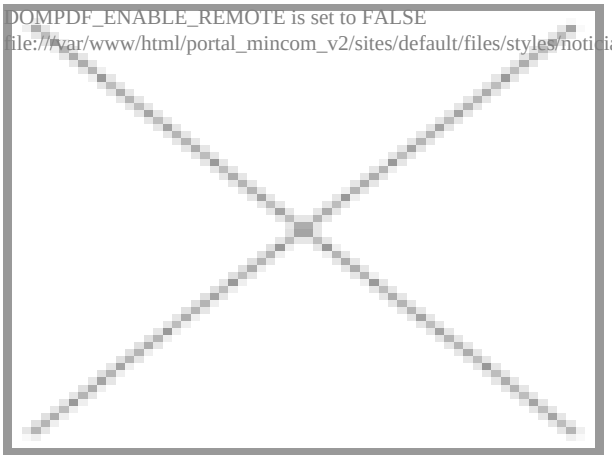

Fuente:
tynmagazine

Investigadores de Check Point Research, la División de Inteligencia de Amenazas de Check Point Software Technologies Ltd., proveedor líder especializado en ciberseguridad a nivel mundial, ha descubierto un nuevo dropper -un programa malicioso diseñado para introducir otro malware en el terminal de la víctima- que se está propagando en la Play Store de Google. Apodado “Clast82” por los investigadores, el dropper ejecuta un malware de segunda fase que proporciona al ciberdelincuente un acceso intrusivo a las cuentas bancarias de las víctimas, así como el control total de sus móviles. CPR encontró Clast82 dentro de 10 apps, que abarcaban funciones como la grabación de pantalla o la VPN.

Clast82 introduce el malware-as-a-service AlienBot Banker, un malware de segunda fase que ataca a las aplicaciones bancarias eludiendo su factor de doble de autenticación. Además, Clast82 está compuesto por un troyano de acceso remoto móvil (MRAT) capaz de controlar el dispositivo con TeamViewer con lo que cibercriminal tiene acceso al como si lo tuviera en sus manos.

¿Cómo actúa el “Clast82”?

Los investigadores de Check Point han señalado el método de ataque que utiliza Clast82:

1. La víctima descarga una app maliciosa desde Google Play, que contiene el dropper Clast82.

2. Clast82 se comunica con el servidor de C&C para recibir la configuración.

3. Clast82 descarga en el dispositivo Android un payload recibido por la configuración, y lo instala – en este caso, el AlienBot Banker.

4. Los ciberdelincuentes acceden a las credenciales bancarias de la víctima y proceden a controlar el terminal por completo.

Clast82 utiliza una serie de técnicas para evitar ser detectado por Google Play Protect:

• Firebase (propiedad de Google) como plataforma para la comunicación del C&C: durante el periodo de evaluación de Clast82 en Google Play, los ciberdelincuentes cambiaron la configuración a nivel de comando y control utilizando Firebase. A su vez, el cibercriminal “desactivó” el comportamiento malicioso de Clast82 durante el periodo de evaluación por parte de Google.

• GitHub como plataforma de alojamiento de terceros para descargar el payload: para cada aplicación, el cibercriminal ha creado un nuevo usuario en la tienda de Google Play, junto con un repositorio en la cuenta de GitHub del cibercriminal, lo que le permite distribuir diferentes payloads a los dispositivos infectados por

cada aplicación maliciosa.

Las 10 apps implicadas

Los ciberdelincuentes utilizaron aplicaciones Android legítimas y conocidas de código abierto:

Name

Cake VPN

Pacific VPN

eVPN

BeatPlayer

BeatPlayer

QR/Barcode Scanner MAX

eVPN

Music Player

tooltipnatorlibrary

QRecorder

“El ciberdelincuente que está detrás de Clast82 ha sido capaz de saltarse las protecciones de Google Play utilizando una metodología creativa. Con una simple manipulación de recursos de terceros fácilmente accesibles -como una cuenta de GitHub o una cuenta de FireBase- aprovechó los recursos para eludir las protecciones de Google Play Store.

Las víctimas pensaban que estaban descargando una aplicación inocua del mercado oficial de Android, pero lo que realmente recibían era un peligroso troyano que iba directamente a sus cuentas bancarias. La capacidad del dropper para pasar desapercibido demuestra la importancia de contar con una solución de seguridad móvil. No basta con escanear la aplicación durante el periodo de evaluación, ya que un ciberdelincuente puede, y lo hará, cambiar el comportamiento de la aplicación utilizando herramientas de terceros fácilmente disponibles”, señala Aviran Hazum, director de investigación de amenazas móviles en Check Point.

En este sentido, Check Point cuenta con un amplio abanico de soluciones de seguridad para ayudar a proteger la información sensible almacenada en dispositivos móviles. Check Point, por su parte, cuenta con Check Point Harmony, la primera solución unificada que permite la conectividad segura a cualquier recurso en cualquier lugar con una protección total de endpoint en todos los dispositivos. Harmony asegura tanto los dispositivos corporativos como los BYOD y las conexiones a Internet frente a los ataques existentes y de día cero, a la vez que proporciona acceso Zero-Trust a las aplicaciones corporativas en una única solución fácil de gestionar.

Disponible en:
https://www.tynmagazine.com/encuentran-un-peligroso-malware-en-10-apps-d... [1]

Links
[1] https://www.tynmagazine.com/encuentran-un-peligroso-malware-en-10-apps-de-la-play-store-de-google/