Cómo detectar que tu teléfono fue infectado con malware

10/05/2022

Los teléfonos móviles han evolucionado de llamadas y mensajes de texto a dispositivos inteligentes portátiles capaces de realizar tareas que antes se confiaban a computadoras. Tomar fotos, enviar y recibir correos electrónicos, comunicarnos a través de apps de mensajería y redes sociales, gestionar billeteras digitales y aplicaciones bancarias, etc., toda esa riqueza de datos también atrae a actores de amenazas que quieren usarlos para sus propios fines, ya sea desde venderlos en la dark web hasta usarlos para cometer robo de identidad y fraude.

Con Android como el sistema operativo que ocupa la mayor parte del mercado de smartphones, ESET, compañía líder en detección proactiva de amenazas, analiza cómo puede infectarse un teléfono:

- Mediante aplicaciones de mensajería, SMS o redes sociales se envían mensajes de phishing que contienen

enlaces o archivos adjuntos maliciosos. Una vez que la víctima descarga el el archivo adjunto y lo instala en su dispositivo, ese malware permite a los actores maliciosos llevar a cabo sus acciones maliciosas.

- En sitios fraudulentos, donde los ciberdelincuentes se hacen pasar sitios de marcas u organizaciones conocidas e incluyen enlaces maliciosos para la descarga de malware en el dispositivo.
- Aplicaciones falsas que se hacen pasar por apps legítimas. De esta manera los atacantes logran que víctimas desprevenidas descarguen en sus dispositivos programas malicioso como keyloggers, ransomware o spyware disfrazados de apps de seguimiento de fitness o aplicaciones de criptomonedas. Estas aplicaciones generalmente se difunden a través de tiendas de aplicaciones no oficiales.

“**Los signos más comunes de que un dispositivo ha sido comprometido son**: **que la batería se agota más rápido de lo habitual, experimenta picos en su uso de datos de Internet**, aunque sus hábitos de navegación no han cambiado, su función GPS o Internet (ya sea Wi-Fi o datos móviles) se puede habilitar o deshabilitar por sí mismo, y se abren ventanas emergentes que despliegan anuncios o aplicaciones desconocidas sin que el usuario lo autorice”, dice Lukas Stefanko, Investigador de malware de ESET.

Otra señal de que puede haber un código malicioso en el teléfono es que las aplicaciones que anteriormente funcionaban bien comienzan a exhibir un comportamiento extraño. Esto incluye iniciarse repentinamente, cerrarse o fallar por completo y mostrar errores inesperados. Sin embargo, dice Stefanko, esto no se limita solo a las aplicaciones: **es posible que el smartphone y su sistema también comienzan a actuar de manera extraña.**

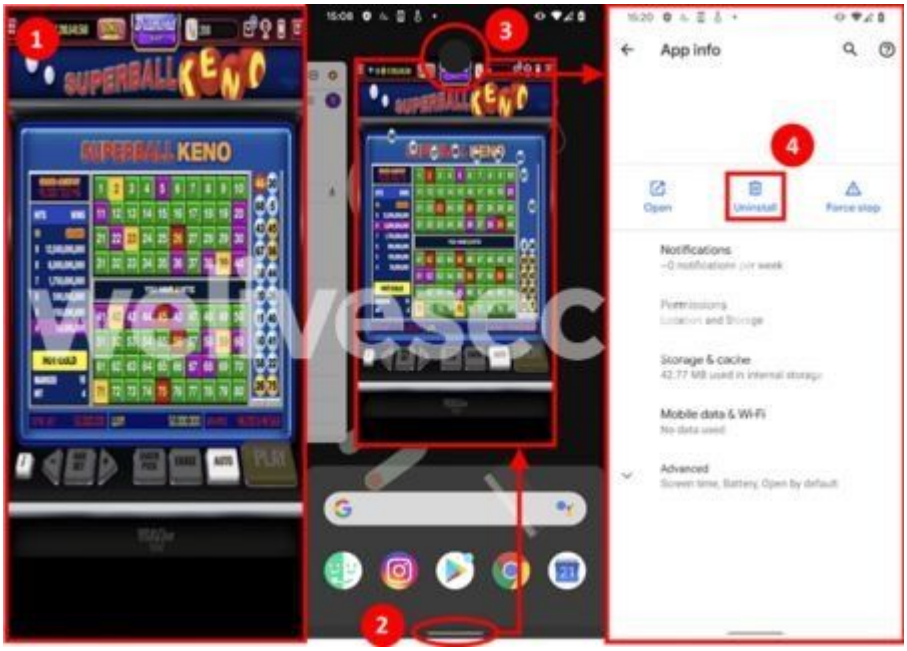
Por otro lado, un signo de que se descargó un malware en un

teléfono incluye que el usuario o sus contactos reciban llamadas o mensajes extraños, o que el historial de llamadas y mensajes de texto incluyan registros extraños y desconocidos, ya que algunos tipos de malware intentan hacer llamadas o enviar mensajes a números internacionales premium. También, hay señales más evidentes, por ejemplo: si un teléfono Android fue comprometido con un ransomware simplemente se bloqueará.

¿Qué hacer si el teléfono fue infectado?

Desde ESET mencionan que en general hay dos formas para eliminar la mayoría de los tipos de malware de un dispositivo infectado: automática y manual. La primera es muy fácil y directa: se descarga e instala en el teléfono una solución antivirus que tenga buenas referencias para escanear el dispositivo en busca de amenazas y que las elimine. La eliminación manual suele ser posible, pero considerablemente más complicada. Eliminar una aplicación maliciosa no siempre es sencillo, porque el malware a menudo incluye mecanismos de prevención codificados para evitar o dificultar que los usuarios logren desinstalarlo.

Una vez que se confirme que se descargó un malware en el smartphone, es necesario identificarlo y eliminarlo. Por ejemplo, en el caso de aplicaciones del tipo adware, que son generalmente los responsables de las ventanas emergentes con publicidad invasiva y molesta, se puede identificar qué aplicación es la responsable de esta actividad abriendo el menú de aplicaciones recientes en el teléfono y manteniendo presionando el icono de la aplicación. Para ilustrarlo, por ejemplo, si una ventana emergente bastante molesta despliega anuncios, se deben abrir las aplicaciones recientes y puede que la aplicación tenga un ícono completamente negro. Luego, se presiona prolongadamente el ícono, se echa un vistazo a los permisos y se la desinstala.



1. Aparece un anuncio emergente en la pantalla completa
2. Al tocar el botón/menú de aplicaciones recientes, se muestra la aplicación responsable de mostrar el anuncio.
3. En este caso, la aplicación tiene un icono negro sólido, lo que hace que sea menos obvio dónde hacer clic.
4. Luego de mantener presionado ese icono, se accede a la información de la aplicación, se inspecciona sus permisos, etc. y se la desinstala.

“Mientras que Android 9 y versiones anteriores del sistema operativo permitían que las aplicaciones maliciosas ocultaran sus iconos, desde Android 10 esto ha sido imposible. Este vacío permitía al malware hacerse pasar por otras aplicaciones o internar ocultarse usando un icono en blanco y sin tener ningún nombre, como se ven en la captura de pantalla anterior”, agrega **Lukas Stefanko** de ESET.

Desde ESET elaboraron un video que muestra cómo eliminar manualmente el malware FluBot de un dispositivo Android y puede servir como guía del proceso: https://youtu.be/dIIDh1AqUKQ. En caso de que se encuentres un problema al intentar desinstalar una aplicación maliciosa de un dispositivo, se puede iniciarlo en modo seguro y eliminar la aplicación que crees que está causando que tu dispositivo realice acciones dañinas, afirma

Stefanko.https://www.youtube.com/embed/dIIDh1AqUKQ

Cuando se trata de mitigar las posibilidades de que un dispositivo se vea comprometido por malware, ESET comparte una combinación de pasos preventivos y proactivos contribuirá en gran medida a mantenerse a salvo de las amenazas:

- **Actualizar tanto el Sistema operativo** como las aplicaciones, tan pronto como estén disponibles las últimas versiones.
- **Realizar backup** de los datos y guardar esta copia de seguridad de forma segura. Será de gran ayuda en caso de que el dispositivo se vea comprometido.
- Para protegerse de la mayoría de las amenazas, **utilizar una solución de seguridad móvil** que tenga un historial comprobado de buena reputación.
- **Descargar aplicaciones solo de las tiendas oficiales** Google Play y App Store, y siempre asegurarse de verificar las opiniones, tanto de la aplicación como de su desarrollador.
- **Tener en cuenta las tácticas comunes que utilizan los ciberdelincuentes** para infiltrarse y comprometer los dispositivos.

Fuente: Ámbito