Vuelve el virus Joker a los celulares, tenemos la lista de las aplicaciones con malware para que las desinstale

26/11/2021

En el pasado el **malware de Joker, alojado en aplicaciones,** ya había sido controlado por **Google** para que dejara de infectar a dispositivos con sistema operativo **Android**, sin embargo, ha vuelto con una nueva metodología que ha afectado a miles de usuarios.

Por lo anterior, se está alertando a los usuarios para que desinstalen las aplicaciones infectadas con el malware, o no las bajen y puedan evitar que su información personal sea vulnerada.

La analista rusa de malware en Android, **Tatyana Shishkova**,

informó que un **virus troyano** de nombre **Joker** estaba en varias aplicaciones las cuales, algunas de ellas tenían hasta más de 30 mil descargas. Encontró que por lo menos 20 aplicaciones entre las que había juegos, lectores de documentos, animaciones de carga y más, con apariencia inocente, fueron usadas como carnada.

Algunas ya fueron eliminadas de **Google Play** sin embargo, existe una app infectada en proceso de ser bajada del sistema, por lo que el usuario debe evitarla sin dudar. Las aplicaciones eliminadas son: App que contenía el malware Joker (Foto: Captura de pantalla)

-Volume Hearing Boost

-Battery Charging Animation Bubble Effects

-Flashlight Flash Alert on Call

-Easy PDF Scanner

-Smart TV Remote

-Halloween Coloring

-Classic Emoji Keyboard

-Volume Booster Louder Sound Equalizer

-Super Hero Effect

-Battery Charging Animations Battery Wallpaper

-Dazzling Keyboard

-EmojiOne Keyboard

-New QRCode Scan Aplicación infectada que fue bajada de la tienda (Foto: Captura de pantalla)

Aunque ninguna de las anteriores sigue disponible en la tienda

Google Play, hay otra vinculada al malware Joker que se llama **Dedicated SMS** que **sigue activa** al momento de la publicación de esta nota y no debe ser descargada.

En caso de que alguien tenga alguna app del listado previo debe desinstalarla lo antes posible y no volverla a abrir para evitar que el código malicioso espíe o haga fraude.

Cómo funciona Joker

Joker ingresa al móvil del usuario para copiar los mensajes SMS y contactos, no obstante, se presume que su principal objetivo es **robar dinero** mediante diversos métodos. Por ejemplo, haciendo suscripciones automáticas a servicios SMS premium sin necesidad de que el usuario interactúe, ya que solo basta con que se abra la aplicación.

Cómo los ciberdelincuentes burlan la seguridad de Google

En el caso de Joker, pese a que **Google** ha hecho mejoras en su **sistema de detección de malware**, ha logrado adaptarse continuamente, pues los ciberdelincuentes hacen las modificaciones pertinentes para burlar los controles de **Google Play Protect**. Según la gigante tecnológica, serían un equipo capaz de lanzar **decenas de apps maliciosas** en un solo día.Aplicación infectada con Joker que hasta este momento sigue activa en la tienda de aplicaciones de Google (Foto: Captura de pantalla)

Se presume que logran pasar los filtros de seguridad porque mandan las apps a revisión “limpias” y cuando llegan a la tienda son inyectadas con el malware, o a través de una actualización, luego de que **se hacen desatacar con reseñas falsas**.

Pese a los esfuerzos de Google, **Joker continúa encontrando el**

método para filtrarse hasta la tienda oficial de aplicaciones, en donde se supone no debería haber peligro para los usuarios de la plataforma.

Aunque por el momento parece que Google suprimió casi en su totalidad el malware Joker, es posible que en el futuro el equipo de ciberdelincuentes encuentren un nuevo modo para filtrarse en las aplicaciones de la **Play Store** y hacer fraude a través de suscripciones a servicios premium sin autorización del usuario.

SI bien el Joker es uno de los malware que más fama se ha hecho, existen **otros troyanos** que se filtran hasta la Google Store como **Face Stealer** que se alojaba en la app **Super-Click VPN** y que recientemente fue bajada de la tienda.

Fuente: Infobae