Tu iPhone puede ser hackeado por el simple hecho de visitar un sitio web de aspecto inocente, según un informe publicado hoy por investigadores de Google.

Esto proviene desde una campaña generalizada de hackeo de iPhone que los investigadores de seguridad cibernética del Project Zero de Google, descubrieron a inicios de este año, que involucra al menos cinco cadenas de explotación de iPhone únicas capaces de liberar de forma remota un iPhone e implantar spyware en él.

Esas cadenas de explotación de iOS se encontraron explotando un total de 14 vulnerabilidades separadas en el sistema operativo móvil iOS de Apple, de las cuales 7 fallas residían en el navegador web Safari, 5 en el kernel de iOS y 2 problemas de escape de sandbox separados, dirigidas a dispositivos con casi todas las versiones en ese marco temporal desde iOS hasta la última versión de iOS 12.

Según una publicación de blog de inmersión profunda publicada por el investigador del Project Zero, Ian Beer, solo dos de las 14 vulnerabilidades de seguridad eran de Día Cero, CVE-2019-7287 y CVE-2019-7286, y sin parches en el momento del descubrimiento, y sorprendentemente, la campaña permaneció sin ser detectada durante al menos dos años.

Aunque los detalles técnicos y la historia de fondo de las dos vulnerabilidades de día cero no estaban disponibles en ese momento, las noticias sobre estas fallas se informaron en febrero, luego de que Apple lanzara la versión 12.1.4 de iOS para abordarlas.

> *«Reportamos estos problemas a Apple con un plazo de 7 días el 1 de febrero de 2019, lo que resultó en el lanzamiento fuera de banda de iOS 12.1.4 el 7 de febrero de 2019. También compartimos los detalles completos con Apple, que fueron revelados públicamente el 7 de febrero de 2019»*, dijo Beer.

Como explicó el investigador de Google, el ataque se estaba llevando a cabo por medio de

una pequeña colección de sitios web pirateados con miles de visitantes por semana, dirigidos a todos los usuarios de iOS que aterrizan en esos sitios web sin discriminación.

> *«Simplemente visitar el sitio pirateado fue suficiente para que el servidor exploit ataque su dispositivo, y si fue exitoso, instale un implante de monitoreo»*, agregó Beer.

Una vez que un usuario de iPhone visita uno de los sitios web hackeados a través del vulnerable navegador web Safari, se activan exploits WebKit para cada cadena de exploits en un intento de establecerse inicialmente en el dispositivo iOS del usuario y organizar los exploits de escalada de privilegios para obtener acceso root en el dispositivo, siendo el nivel más alto de acceso.

Los exploits del iPhone se usaron para implementar un implante diseñado principalmente para robar archivos como iMessages, fotos y datos de ubicación de GPS en vivo de los usuarios, y subirlos a un servidor externo cada 60 segundos.

> *«No hay un indicador visual en el dispositivo de que el implante se está ejecutando. No hay forma de que un usuario en iOS vea una lista de procesos, por lo que el binario del implante no intenta ocultar su ejecución del sistema»,* dijo Beer.

El implante de software espía también robó los archivos de la base de datos del dispositivo de la víctima que utilizan las populares aplicaciones de cifrado de extremo a extremo como WhatsApp, Telegram e iMessages para almacenar datos, incluyendo los chats privados en texto sin formato.

Además, el implante también tenía acceso a los datos del keychain del dispositivo de los usuarios que contenían credenciales, tokens de autenticación y certificados utilizados en y

por el dispositivo.

> *«El keychain también contiene los tokens de larga duración utilizados por servicios como el inicio de sesión único de iOS de Google para permitir que las aplicaciones de Google accedan a la cuenta del usuario. Estos se cargarán a los atacantes y luego se pueden usar para mantener el acceso a la cuenta de Google del usuario, incluso una vez que el implante ya no se está ejecutando»,* explicó Beer.

Si bien el implante se eliminaría automáticamente de un iPhone infectado al reiniciar, sin dejar rastro de sí mismo, visitar el sitio pirateado nuevamente reinstala el implante.

Alternativamente, según explica Beer, los atacantes pueden *«mantener un acceso persistente a varias cuentas y servicios mediante el uso de tokens de autenticación robados del keychain, aún después de perder el acceso al dispositivo».*

Adicionalmente, ya que Apple reparó la mayoría de las vulnerabilidades explotadas descubiertas en iPhone, siempre se recomienda a los usuarios mantener sus dispositivos actualizados para evitar ser víctimas de las cadenas de ataque.