Un equipo de investigadores canadienses de seguridad cibernética descubrió una campaña de piratería móvil y dirigida que tiene como objetivo a miembros de alto perfil de distintos grupos tibetanos con exploits de un solo clic para dispositivos iOS y Android.

Denominado como Poison Carp por el Citizen Lab, de la Universidad de Toronto, el grupo de hackers detrás de esta campaña envió enlaces web maliciosos personalizados a sus objetivos por medio de WhatsApp, que, cuando se abren, explotan el navegador web y las vulnerabilidades de escalada de privilegios para instalar spyware en dispositivos iOS y Android de forma sigilosa.

> *«Entre noviembre de 2018 y mayo de 2019, miembros de alto rango de grupos tibetanos recibieron enlaces maliciosos en intercambios de texto de WhatsApp personalizados con operadores que se hicieron pasar por trabajadores de ONG, periodistas y otras personas falsas»*, dijeron los investigadores.

Además, los investigadores dijeron que encontraron *«superposiciones técnicas»* de Poison Carp con dos campañas recientemente descubiertas contra la comunidad uigur en China: la campaña de pirateo de iPhone reportada por expertos en Google y la campaña Evil Eye publicada por Volexity el mes pasado.

Sobre la base de las similitudes de las tres campañas, los investigadores creían que el gobierno chino patrocina al grupo Poison Carp.

La campaña Poison Carp explota un total de 8 exploits distintos del navegador de Android para instalar un spyware de Android previamente indocumentado con todas las funciones, llamado MOONSHINE y una cadena de exploits de iOS para instalar sigilosamente el spyware de iOS en el dispositivo de los usuarios.

> *«Cuatro de los exploits de MOONSHINE se copian claramente del código de exploits de trabajo publicado por investigadores de seguridad en rastreadores de errores o*

> *páginas de GitHub»,* dice el informe.

Los investigadores observaron un total de 17 intentos de intrusión contra objetivos tibetanos que se realizaron durante ese período, 12 de los cuales contenían enlaces al exploit iOS.

Una vez instalado, el implante malicioso permite a los atacantes lo siguiente:

- Obtener el control total del dispositivo de las víctimas, extraer datos, incluidos mensajes de texto, contactos, registros de llamadas y datos de ubicación
- Acceder a la cámara y micrófono del dispositivo, extraer datos privados de Viber, Telegram, Gmail, Twitter y WhatsApp
- Descargar e instalar complementos maliciosos adicionales.

Aparte de esto, los otros investigadores también observaron una aplicación OAuth maliciosa que el mismo grupo de atacantes usó para acceder a sus cuentas de Gmail al redirigirlas a una página señuelo diseñada para convencerlos de que la aplicación tenía un propósito legítimo.

Entre las víctimas que fueron atacadas por los piratas informáticos de la carpa venenosa entre noviembre de 2018 y mayo de 2019 se incluyen la oficina privada del líder budista tibetano, el Dalai Lama, la Administración Central Tibetana, el Parlamento Tibetano, los grupos tibetanos de derechos humanos y las personas que ocupan cargos de alto nivel en organizaciones respectivas.

Aunque este no es el primer caso que intenta atacar al gobierno tibetano, los investigadores dicen que la nueva campaña de la carpa venenosa es *«el primer caso documentado de exploits móviles con un solo clic utilizados para atacar a los grupos tibetanos».*

> *«Representa una escalada significativa en las tácticas de ingeniería social y la*

> *sofisticación técnica en comparación con lo que típicamente hemos observado que se utiliza contra la comunidad tibetana»,* dice el informe.

Después de la divulgación de la campaña de piratería de iPhone, Apple lanzó una declaración el mes pasado confirmado que la campaña de iOS se dirigió a la comunidad uigur y dijo que la compañía parchó las vulnerabilidades en febrero de este año.

Debido a que ninguna de las vulnerabilidades de iOS y Android explotadas en la campaña es de día cero, se recomienda a los usuarios que siempre mantengan sus dispositivos móviles actualizados para convertirse en víctimas de dichos ataques.