Una vulnerabilidad de seguridad de día cero en la aplicación móvil de Telegram para Android, conocida como EvilVideo, permitía a los atacantes enviar archivos maliciosos disfrazados como videos inofensivos.

ESET informó que el exploit apareció a la venta en un foro clandestino por un precio desconocido el 6 de junio de 2024. Tras una divulgación responsable el 26 de junio, Telegram solucionó el problema en la versión 10.14.5 lanzada el 11 de julio.

> *«Los atacantes podían distribuir cargas maliciosas de Android a través de canales, grupos y chats de Telegram, haciéndolas parecer archivos multimedia»*, explicó el investigador de seguridad Lukáš Štefanko en un informe.

Se cree que la carga útil se genera usando la interfaz de programación de aplicaciones (API) de Telegram, que permite la carga programada de archivos multimedia en chats y canales. Esto permite a los atacantes camuflar un archivo APK malicioso como un video de 30 segundos.

Los usuarios que hacían clic en el video recibían un mensaje de advertencia que indicaba que el video no se podía reproducir y les instaba a intentarlo con un reproductor externo. Si seguían adelante, se les pedía que permitieran la instalación del archivo APK a través de Telegram. La aplicación en cuestión se llamaba «*xHamster Premium Mod.*«

> *«Por defecto, los archivos multimedia recibidos a través de Telegram están configurados para descargarse automáticamente. Esto significa que los usuarios con esta opción habilitada descargarán automáticamente la carga maliciosa una vez que abran la conversación donde se compartió»,* dijo Štefanko.

Aunque esta opción se puede desactivar manualmente, la carga útil todavía se puede descargar tocando el botón de descarga que acompaña al supuesto video. Es importante

señalar que el ataque no funciona en los clientes de Telegram para la web o en la aplicación dedicada para Windows.

Actualmente, no está claro quién está detrás del exploit ni cuán ampliamente se utilizó en ataques reales. Sin embargo, el mismo actor había anunciado en enero de 2024 un criptador de Android totalmente indetectable que supuestamente puede evadir Google Play Protect.

Éxito Viral de Hamster Kombat Genera Imitadores Maliciosos

Este desarrollo se produce mientras los ciberdelincuentes están aprovechando el juego de criptomonedas basado en Telegram, Hamster Kombat, para obtener ganancias. ESET ha descubierto tiendas de aplicaciones falsas que promocionan el juego, repositorios de GitHub que alojan Lumma Stealer para Windows bajo la apariencia de herramientas de automatización para el juego, y un canal no oficial de Telegram que se utiliza para distribuir un troyano de Android llamado Ratel.

El popular juego, lanzado en marzo de 2024, se estima que cuenta con más de 250 millones de jugadores, según el desarrollador del juego. El CEO de Telegram, Pavel Durov, ha llamado a Hamster Kombat el *«servicio digital de más rápido crecimiento en el mundo»* y ha dicho que *«el equipo de Hamster acuñará su token en TON, introduciendo los beneficios de blockchain a cientos de millones de personas».*

Ratel, ofrecido a través de un canal de Telegram llamado «*hamster_easy*«, está diseñado para hacerse pasar por el juego («Hamster.apk») y solicita a los usuarios que le otorguen acceso a notificaciones y lo establezcan como la aplicación de SMS predeterminada. Luego, se comunica con un servidor remoto para obtener un número de teléfono como respuesta.

En el siguiente paso, el malware envía un mensaje SMS en ruso a ese número de teléfono, probablemente perteneciente a los operadores del malware, para recibir instrucciones adicionales a través de SMS.

> *«Los actores de la amenaza pueden controlar el dispositivo comprometido a través de SMS: el mensaje del operador puede contener un texto para enviar a un número específico, o incluso instruir al dispositivo para que llame al número. El malware también puede verificar el saldo de la cuenta bancaria de la víctima para Sberbank Rusia enviando un mensaje con el texto баланс (traducción: balance) al número 900»,* dijo ESET.

Ratel abusa de sus permisos de acceso a notificaciones para ocultar notificaciones de al menos 200 aplicaciones, según una lista codificada en su interior. Se sospecha que esto se hace para suscribir a las víctimas a varios servicios premium y evitar que sean alertadas.

La firma de ciberseguridad eslovaca también observó tiendas de aplicaciones falsas que afirmaban ofrecer Hamster Kombat para descargar, pero que en realidad dirigían a los usuarios a anuncios no deseados, y repositorios de GitHub que ofrecían herramientas de automatización de Hamster Kombat que desplegaban Lumma Stealer en su lugar.

> *«El éxito de Hamster Kombat también ha atraído a ciberdelincuentes, que ya han comenzado a desplegar malware dirigido a los jugadores del juego. La popularidad de Hamster Kombat lo hace propenso a abusos, lo que significa que es muy probable que el juego atraiga a más actores maliciosos en el futuro»,* dijeron Štefanko y Peter Strýček.

Se filtra el malware BadPack de Android

Además de Telegram, los archivos APK maliciosos dirigidos a dispositivos Android también han adoptado la forma de BadPack, que se refiere a archivos de paquetes especialmente diseñados en los que la información del encabezado utilizada en el formato de archivo ZIP ha sido alterada para obstruir el análisis estático.

Al hacerlo, se pretende evitar que el archivo AndroidManifest.xml – un archivo crucial que

proporciona información esencial sobre la aplicación móvil – sea extraído y analizado correctamente, permitiendo así que los artefactos maliciosos se instalen sin levantar alertas.

Esta técnica fue documentada extensamente por Kaspersky en abril pasado en relación con un troyano de Android conocido como SoumniBot que ha atacado a usuarios en Corea del Sur. Los datos de telemetría recopilados por Palo Alto Networks Unit 42 desde junio de 2023 hasta junio de 2024 han detectado casi 9,200 muestras de BadPack en circulación, aunque ninguna de ellas se ha encontrado en Google Play Store.

> *«Estos encabezados manipulados son una característica clave de BadPack, y tales muestras generalmente plantean un desafío para las herramientas de ingeniería inversa de Android. Muchos troyanos bancarios basados en Android como BianLian, Cerberus y TeaBot usan BadPack»,* dijo el investigador de Unit 42, Lee Wei Yeong, en un informe publicado la semana pasada.