El actor de amenazas identificado como Patchwork probablemente utilizó engaños de romance para atrapar a víctimas en Pakistán e India e infectar sus dispositivos Android con un troyano de acceso remoto llamado VajraSpy.

La empresa de ciberseguridad eslovaca ESET informó que descubrió 12 aplicaciones de espionaje, de las cuales seis estaban disponibles para su descarga desde la tienda oficial de Google Play y fueron descargadas colectivamente más de 1,400 veces entre abril de 2021 y marzo de 2023.

> *«VajraSpy cuenta con diversas funciones de espionaje que pueden ampliarse según los permisos concedidos a la aplicación empaquetada con su código. Roba contactos, archivos, registros de llamadas y mensajes SMS, pero algunas de sus implementaciones incluso pueden extraer mensajes de WhatsApp y Signal, grabar llamadas telefónicas y capturar imágenes con la cámara»*, explicó el investigador de seguridad Lukáš Štefanko.

Se estima que aproximadamente 148 dispositivos en Pakistán e India fueron comprometidos en el entorno real. Las aplicaciones maliciosas distribuidas a través de Google Play y otros medios se presentaban principalmente como aplicaciones de mensajería, siendo las más recientes propagadas hasta septiembre de 2023.

- Privee Talk (com.priv.talk)
- MeetMe (com.meeete.org)
- Let’s Chat (com.letsm.chat)
- Quick Chat (com.qqc.chat)
- Rafaqat رفاق (com.rafaqat.news)
- Chit Chat (com.chit.chat)
- YohooTalk (com.yoho.talk)
- TikTalk (com.tik.talk)
- Hello Chat (com.hello.chat)
- Nidus (com.nidus.no o com.nionio.org)

- GlowChat (com.glow.glow)
- Wave Chat (com.wave.chat)

Rafaqat رفاق destaca por ser la única aplicación no relacionada con mensajería, ya que se promocionaba como una vía para acceder a las últimas noticias. Fue subida a Google Play el 26 de octubre de 2022, por un desarrollador llamado Mohammad Rizwan, acumulando un total de 1,000 descargas antes de ser retirada por Google.

El vector exacto de distribución del malware no está claro en este momento, aunque la naturaleza de las aplicaciones sugiere que las víctimas fueron persuadidas para descargarlas como parte de una estafa de romance, donde los atacantes las convencen de instalar estas aplicaciones fraudulentas bajo el pretexto de tener una conversación más segura.

Este no es el primer episodio en el que Patchwork, un actor de amenazas con presuntos vínculos con India, utiliza esta técnica. En marzo de 2023, Meta reveló que este grupo de hackers creó identidades ficticias en Facebook e Instagram para compartir enlaces a aplicaciones falsas y atacar a víctimas en Pakistán, India, Bangladesh, Sri Lanka, Tíbet y China.

Tampoco es la primera vez que se observa a los atacantes empleando VajraRAT, previamente documentado por la empresa de ciberseguridad china QiAnXin a principios de 2022, como parte de una campaña dirigida a entidades gubernamentales y militares de Pakistán. El término Vajra proviene de la palabra sánscrita que significa rayo.

En noviembre de 2023, Qihoo 360, al realizar su propia evaluación del malware, lo asoció a un actor de amenazas que sigue bajo el alias de Fire Demon Snake (también conocido como APT-C-52).

Más allá de Pakistán e India, es probable que entidades gubernamentales de Nepal hayan sido objetivo de una campaña de phishing que distribuye una puerta trasera basada en Nim. Se ha atribuido al grupo SideWinder, otra entidad señalada por operar con intereses indios.

Este desarrollo se presenta mientras actores de amenazas con motivación financiera de Pakistán e India han sido descubiertos atacando a usuarios indios de Android mediante una aplicación de préstamos falsa (Moneyfine o «com.moneyfine.fine») como parte de una estafa de extorsión que manipula la selfie cargada como parte de un proceso de conocimiento del cliente (KYC) para crear una imagen comprometedora y amenazar a las víctimas con realizar un pago o arriesgarse a que las fotos manipuladas se divulguen entre sus contactos.

> *«Estos actores desconocidos con motivación financiera hacen promesas atractivas de obtener préstamos rápidos con procesos mínimos, distribuyen malware para comprometer sus dispositivos y emplean amenazas para extorsionar dinero»,* indicó Cyfirma en un análisis a finales del mes pasado.

Esto también se da en el contexto de una tendencia más amplia en la que las personas caen presas de aplicaciones de préstamos depredadoras, conocidas por extraer información sensible de dispositivos infectados y utilizar tácticas de chantaje y acoso para presionar a las víctimas para que realicen los pagos.

Conforme a un informe reciente publicado por el Network Contagion Research Institute (NCRI), adolescentes de Australia, Canadá y Estados Unidos son cada vez más blanco de ataques de sextorsión financiera llevados a cabo por un grupo de ciberdelincuentes con base en Nigeria conocido como Yahoo Boys.

> *«Casi la totalidad de esta actividad está vinculada a ciberdelincuentes de África Occidental conocidos como los Yahoo Boys, quienes se dirigen principalmente a menores y jóvenes adultos que hablan inglés en Instagram, Snapchat y Wizz»,* comentó el NCRI.

Wizz, cuyas aplicaciones para Android e iOS han sido retiradas de la Apple App Store y Google Play Store, desestimó el informe del NCRI, afirmando que *«no tiene constancia de*

intentos exitosos de extorsión que hayan tenido lugar durante la comunicación en la aplicación Wizz».