El actor estatal vinculado a China, conocido como APT41, ha sido relacionado con dos variantes de spyware para Android hasta ahora desconocidas, denominadas WyrmSpy y DragonEgg.

> *«Reconocido por su explotación de aplicaciones web y la infiltración de dispositivos tradicionales, el hecho de que APT41, un actor de amenazas bien establecido, incluya malware dirigido a dispositivos móviles en su arsenal, demuestra que estos puntos finales móviles son objetivos de alto valor, con datos corporativos y personales muy codiciados»*, informó Lookout en un reporte.

APT41, también conocido como Axiom, Blackfly, Brass Typhoon (anteriormente Barium), Bronze Atlas, HOODOO, Wicked Panda y Winnti, ha estado operativo desde al menos 2007, enfocándose en robar propiedad intelectual de diversas industrias.

Recientes ataques realizados por este colectivo adversario han utilizado una herramienta de pruebas de intrusión de código abierto conocida como Google Command and Control (GC2), como parte de ataques dirigidos a plataformas de medios y empleo en Taiwán e Italia.

Aunque se desconoce el vector de intrusión inicial utilizado en la campaña de vigilancia móvil, se sospecha que podría haber involucrado el uso de ingeniería social. Lookout informó que detectó WyrmSpy por primera vez en 2017 y DragonEgg a principios de 2021, habiendo encontrado nuevas muestras de este último tan recientemente como en abril de 2023.

WyrmSpy se disfraza principalmente como una aplicación de sistema predeterminada utilizada para mostrar notificaciones al usuario. Sin embargo, variantes posteriores han empaquetado el malware en aplicaciones que simulan contenido de video para adultos, Baidu Waimai y Adobe Flash. Por otro lado, DragonEgg se ha distribuido en forma de teclados y aplicaciones de mensajería de terceros, como Telegram.

No existen pruebas que indiquen que estas aplicaciones maliciosas hayan sido propagadas a través de la tienda oficial de Google Play.

Las conexiones entre WyrmSpy y DragonEgg con APT41 provienen del uso de un servidor y comando (C2) con la dirección IP 121.42.149[.]52, que se resuelve en un dominio («vpn2.umisen[.]com») previamente identificado como asociado con la infraestructura del grupo.

Una vez instalados, ambos tipos de malware solicitan permisos invasivos y cuentan con capacidades sofisticadas de recolección y extracción de datos, recopilando fotos, ubicaciones, mensajes SMS y grabaciones de audio de los usuarios.

También se ha observado que el malware depende de módulos descargados de un servidor C2 que ahora está fuera de línea, después de la instalación de la aplicación, para facilitar la recolección de datos y evitar la detección.

WyrmSpy, por su parte, tiene la capacidad de deshabilitar el Seguridad Mejorada de Linux (SELinux), una función de seguridad en Android, y utilizar herramientas de enraizamiento como KingRoot11 para obtener privilegios elevados en los dispositivos comprometidos. Una característica destacada de DragonEgg es que se comunica con el servidor C2 para obtener un módulo terciario desconocido, que se hace pasar por un programa forense.

> *«El descubrimiento de WyrmSpy y DragonEgg sirve como un recordatorio de la creciente amenaza que representa el malware avanzado para Android. Estos paquetes de spyware son altamente sofisticados y pueden ser utilizados para recolectar una amplia variedad de datos de dispositivos infectados»,* señaló Kristina Balaam, una investigadora de amenazas senior en Lookout.

Estos hallazgos se dan a conocer mientras Mandiant revela las tácticas en evolución adoptadas por los grupos de espionaje chinos para pasar desapercibidos, incluyendo el uso de dispositivos de red y software de virtualización como herramientas, emplear botnets para ocultar el tráfico entre la infraestructura C2 y los entornos de las víctimas, y canalizar el tráfico malicioso dentro de las redes de las víctimas a través de sistemas comprometidos.

> *«El uso de botnets, la ocultación del tráfico en una red comprometida y el enfoque en dispositivos periféricos no son tácticas nuevas, ni exclusivas de actores de ciberespionaje chinos. Sin embargo, durante la última década, hemos seguido el uso de estas y otras tácticas por parte de actores de ciberespionaje chinos como parte de una evolución más amplia hacia operaciones más intencionales, furtivas y efectivas»*, comentó Mandiant, la empresa de inteligencia de amenazas propiedad de Google.