Una campaña de malware de phishing de voz de Android (también conocida como vishing), denominada FakeCalls, ha resurgido para apuntar a los usuarios de Corea del Sur bajo la apariencia de más de 20 aplicaciones financieras populares.

> *«El malware FakeCalls posee la funcionalidad de una navaja suiza, capaz no solo de llevar a cabo su objetivo principal, sino también de extraer datos privados del dispositivo de la víctima»,* dijo la compañía de seguridad cibernética Check Point.

FakeCalls fue documentado previamente por Kaspersky en abril de 2022, describiendo las capacidades del malware para imitar conversaciones telefónicas con un agente de atención al cliente del banco.

En los ataques observados, los usuarios que instalan la aplicación bancaria no autorizada son tentados a llamar a la institución financiera ofreciéndoles un préstamo falso a bajo interés.

En el momento en que se produce la llamada telefónica, se reproduce un audio pregrabado con instrucciones del banco real. Al mismo tiempo, el malware oculta el número de teléfono con el número legítimo del banco para dar la impresión de que se está manteniendo una conversación con un empleado del banco real en el otro extremo.

El objetivo final de la campaña es obtener la información de la tarjeta de crédito de la víctima, que según los hackers, es necesaria para calificar para el préstamo inexistente.

La aplicación maliciosa también solicita permisos intrusivos para recopilar datos confidenciales, incluyendo transmisiones de audio y video en vivo, desde el dispositivo comprometido, que después se extraen a un servidor remoto.

Las últimas muestras de FakeCalls implementan además varias técnicas para permanecer fuera del radar. Uno de los métodos implica agregar una gran cantidad de archivos dentro de directorios anidados a la carpeta de activos del APK, lo que hace que la longitud del archivo y la ruta superen el límite de 300 caracteres.

> *«Los desarrolladores de malware tuvieron especial cuidado con los aspectos técnicos de su creación, así como con la implementación de varias técnicas únicas y efectivas contra el análisis. Además, idearon mecanismos para la resolución encubierta de los servidores de comando y control detrás de las operaciones»,* dijo Check Point.

Aunque el ataque se enfoca exclusivamente en Corea del Sur, la compañía de seguridad cibernética advirtió que las mismas tácticas pueden reutilizarse para atacar otras regiones del mundo.

Los hallazgos también surgen cuando Cyble arroja luz sobre dos troyanos bancarios de Android denominados Nexus y GoatRAT que pueden recopilar datos valiosos y llevar a cabo fraudes financieros.

Nexus, una versión renombrada de SOVA, también incorpora un módulo de ransomware que encripta los archivos almacenados y puede abusar de los servicios de accesibilidad de Android para extraer frases iniciales de las billeteras de criptomonedas.

Por el contrario, GoatRAT está diseñado para apuntar a los bancos brasileños y se une a BrasDex y PixPirate para realizar transferencias de dinero fraudulentas a través de la plataforma de pgos PIX mientras muestra una ventana superpuesta falsa para ocultar la actividad.

El desarrollo es parte de una tendencia creciente en la que los atacantes han desatado malware bancario cada vez más sofisticado para automatizar todo el proceso de transferencias de dinero no autorizadas en dispositivos infectados.

La compañía de seguridad cibernética Kaspersky dijo que detectó 196,476 nuevos troyanos

bancarios móviles y 10543 nuevos troyanos de ransomware móviles en 2022, con China, Siria, Irán, Yemen e Irak emergiendo como los principales países atacados por malware móvil, incluyendo el adware.

España, Arabia Saudita, Australia, Turquía, China, Suiza, Japón, Colombia, Italia e India encabezan la lista de los principales países infectados por amenazas financieras móviles.

> *«A pesar de la disminución de los instaladores de malware en general, el continuo crecimiento de los troyanos bancarios móviles es una clara indicación de que los hackers se están enfocando en obtener ganancias financieras»,* dijo la investigadora de Kaspersky, Tatyana Shishkova.