Se ha detectado una nueva campaña maliciosa que utiliza aplicaciones Android maliciosas para robar mensajes SMS de los usuarios desde al menos febrero de 2022, como parte de una operación a gran escala.

Estas aplicaciones maliciosas, que abarcan más de 107,000 muestras únicas, están diseñadas para interceptar contraseñas de un solo uso (OTP) utilizadas para la verificación de cuentas en línea y así cometer fraude de identidad.

> *«De esas 107,000 muestras de malware, más de 99,000 de estas aplicaciones eran desconocidas y no estaban disponibles en repositorios accesibles. Este malware estaba monitoreando mensajes de OTP de más de 600 marcas globales, algunas de las cuales tienen cientos de millones de usuarios»*, informó la firma de seguridad móvil Zimperium en un informe.

Se han identificado víctimas de esta campaña en 113 países, con India y Rusia a la cabeza, seguidos por Brasil, México, EE. UU., Ucrania, España y Turquía.

El ataque comienza con la instalación de una aplicación maliciosa que la víctima es inducida a instalar en su dispositivo, ya sea a través de anuncios engañosos que imitan listados de aplicaciones de Google Play Store o a través de alguno de los 2,600 bots de Telegram que se hacen pasar por servicios legítimos (por ejemplo, Microsoft Word).

Una vez instalada, la aplicación solicita permiso para acceder a los mensajes SMS entrantes, y luego se comunica con uno de los 13 servidores de comando y control (C2) para transmitir los mensajes SMS robados.

> *«El malware permanece oculto, monitoreando constantemente los nuevos mensajes SMS entrantes. Su objetivo principal son las OTP utilizadas para la verificación de cuentas en línea»,* explicaron los investigadores.

Actualmente, no está claro quién está detrás de esta operación, aunque se ha observado que los actores de la amenaza aceptan varios métodos de pago, incluyendo criptomonedas, para impulsar un servicio llamado Fast SMS (fastsms[.]su) que permite a los clientes comprar acceso a números de teléfono virtuales.

Es probable que los números de teléfono asociados con los dispositivos infectados se utilicen sin el conocimiento del propietario para registrarse en diversas cuentas en línea mediante la recolección de las OTP necesarias para la autenticación de dos factores (2FA).

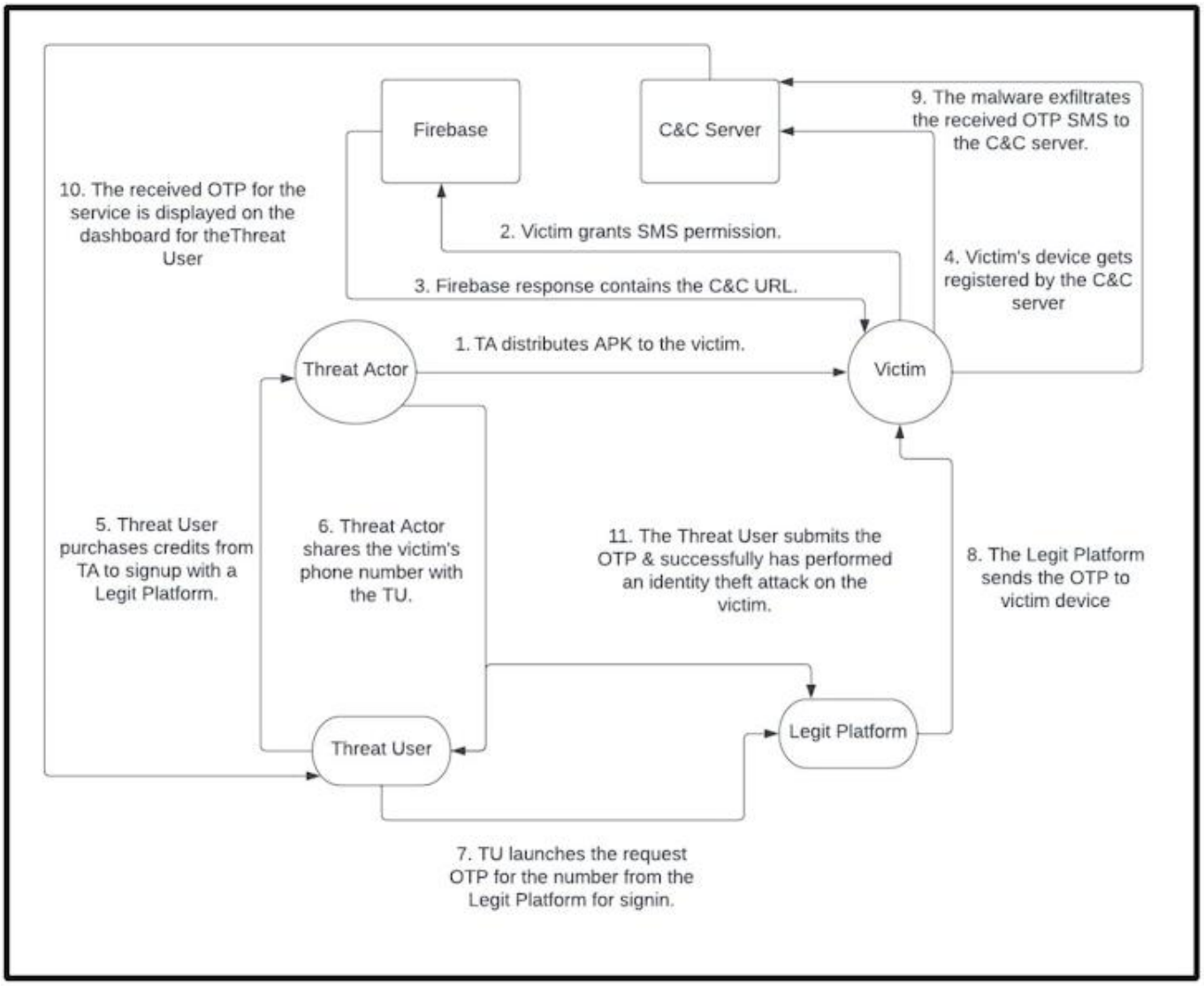

Figure: complete attack flow

A principios de 2022, Trend Micro destacó un servicio similar motivado por ganancias financieras que reunía dispositivos Android en una botnet que podía utilizarse para *«registrar cuentas desechables en masa o crear cuentas verificadas por teléfono para realizar fraudes y otras actividades delictivas.»*

> *«Estas credenciales robadas sirven como trampolín para actividades fraudulentas adicionales, como crear cuentas falsas en servicios populares para lanzar campañas de phishing o ataques de ingeniería social,»* dijo Zimperium.

Los hallazgos subrayan el continuo abuso de Telegram, una aplicación de mensajería instantánea popular con más de 950 millones de usuarios activos mensuales, por actores maliciosos para diversos fines, desde la propagación de malware hasta C2.

A principios de este mes, Positive Technologies reveló dos familias de ladrones de SMS llamadas SMS Webpro y NotifySmsStealer que apuntan a usuarios de dispositivos Android en Bangladesh, India e Indonesia, con el objetivo de enviar los mensajes a un bot de Telegram controlado por los actores de la amenaza.

También identificados por la empresa rusa de ciberseguridad están las cepas de malware ladrón que se hacen pasar por TrueCaller y ICICI Bank, y son capaces de extraer fotos de los usuarios, información del dispositivo y notificaciones a través de la plataforma de mensajería.

> *«La cadena de infección comienza con un ataque de phishing típico en WhatsApp. Con pocas excepciones, el atacante utiliza sitios de phishing que se hacen pasar por un banco para que los usuarios descarguen aplicaciones de ellos»*, dijo la investigadora de seguridad Varvara Akhapkina.

Otro malware que utiliza Telegram como servidor C2 es TgRAT, un troyano de acceso remoto para Windows que recientemente ha sido actualizado para incluir una variante de Linux. Está equipado para descargar archivos, tomar capturas de pantalla y ejecutar comandos de forma remota.

> *«Telegram es ampliamente utilizado como un mensajero corporativo en muchas empresas. Por lo tanto, no es sorprendente que los actores de amenazas puedan*

> *utilizarlo como vector para distribuir malware y robar información confidencial: la popularidad del programa y el tráfico rutinario a los servidores de Telegram facilitan disfrazar el malware en una red comprometida»,* dijo Doctor Web.