Se descubrió un nuevo tipo de malware bancario que abusa de las funciones de accesibilidad de Android para extraer datos confidenciales de aplicaciones financieras, leer mensajes SMS de usuarios y secuestrar códigos de autenticación de dos factores basados en SMS.

Llamado *«EventBot»* por los investigadores de Cybereason, el malware es capaz de apuntar a más de 200 aplicaciones financieras diferentes, incluyendo servicios bancarios, servicios de transferencia de dinero y billeteras de criptomonedas como PayPal Business, Revolut, Barclays, CapitalOne, HSBC, Santander, TransferWise y Coinbase.

> *«Eventbot es particularmente interesante porque está en etapas tan tempranas. Este nuevo malware tiene un potencial real para convertirse en el siguiente gran malware móvil, ya que está bajo constantes mejoras iterativas, abusa de una característica crítica del sistema operativo y apunta a aplicaciones financieras»,* dijeron los investigadores.

La campaña, identificada por primera vez en marzo de 2020, enmascara su intención maliciosa haciéndose pasar por aplicaciones legítimas, como Adobe Flash, Microsoft Word, en tiendas de APK no autorizadas y otros sitios web sospechosos, que al ser instaladas, solicitan permisos extensos del dispositivo.

Los permisos incluyen acceso a la configuración de accesibilidad, la capacidad de leer desde el almacenamiento externo, enviar y recibir mensajes SMS, ejecutarse en segundo plano y ejecutarse después del inicio del sistema.

Si un usuario otorga acceso, EventBot funciona como un keylogger y puede *«recuperar notificaciones sobre otras aplicaciones instaladas y contenido de ventanas abiertas»,* además de explotar los servicios de accesibilidad de Android para obtener el PIN de la pantalla de bloqueo y transmitir todos los datos recopilados en un formato cifrado a un servidor controlado por el atacante.

La capacidad de analizar los mensajes SMS también hace que el troyano bancario sea una herramienta útil para evitar la autenticación de dos factores basada en SMS, lo que les da a los adversarios un fácil acceso a las billeteras de criptomonedas de las víctimas y roba fondos de las cuentas bancarias.

Esta no es la primera vez que el malware móvil se dirige a los servicios financieros. El mes pasado, los investigadores de IBM X-Force detallaron una nueva campaña de TrickBot, llamada TrickMo, que se econtró únicamente dirigida a usuarios alemanes con malware que utilizaba mal las funciones de accesibilidad para interceptar una contraseña de un solo uso (OTP), TAN móvil (mTAN) y códigos de autenticación pushTAN.

> *«Dar acceso al atacante a un dispositivo móvil puede tener graves consecuencias comerciales, especialmente si el usuario final está utilizando su dispositivo móvil para discutir temas comerciales delicados o acceder a información financiera empresarial. Esto puede provocar la degradación de la marca, la pérdida de la reputación individual o la pérdida de la confianza del consumidor»,* dijeron los investigadores.

La familia de aplicaciones maliciosas de EventBot puede no estar activa en Google Play Store, pero es otro recordatorio de por qué los usuarios deberían atenerse a las tiendas de aplicaciones oficiales y evitar la descarga de aplicaciones de fuentes no confiables. Mantener el software actualizado y activar Google Play Protect también ayuda en gran medida a proteger los dispositivos del malware.