Los autores del malware TrickBot, un troyano bancario, desarrollaron una nueva aplicación para Android que es capaz de interceptar códigos de autorización únicos enviados a clientes de banca por Internet por medio de SMS o notificaciones push relativamente más seguras, y completar las transacciones fraudulentas.

La aplicación de Android, llamada «TrickMo» por los investigadores de IBM X-Force, está en desarrollo activo y se ha dirigido exclusivamente a usuarios alemanes cuyos escritorios fueron infectados previamente con el malware TrickBot.

> *«Alemania es uno de los primeros campos de ataque a los que se extendió TrickBot cuando surgió por primera vez en 2016. En 2020, parece que el gran fraude bancario de TrickBot es un proyecto en curso que ayuda a los hackers a monetizar cuentas comprometidas»,* dijeron los investigadores de IBM.

El nombre TrickMo es una referencia directa a un tipo similar de malware bancario para Android, llamado ZitMo, que fue desarrollado por el grupo criminal de Zeus en 2011 para burlar la autenticación de dos factores basada en SMS.

El desarrollo es la última incorporación al arsenal de capacidades en evolución del troyano bancario que desde ese entonces, se ha transformado para entregar otros tipos de malware, como el ransomware Ryuk, que actúa como un ladrón de información, roba billeteras Bitcoin y roba credenciales de correos electrónicos.

El CERT-Bund detectó en septiembre pasado, que la campaña TrickMo funciona al interceptar una amplia gama de números de autenticación de transacciones (TAN), incluida la contraseña de un solo uso (OTP), TAN móvil (mTAN) y códigos de autenticación PushTAN después de que las víctimas lo instalan en sus dispositivos Android.

El aviso del CERT-Bund siguió advirtiendo que las computadoras con Windows infectadas por TrickBot emplearon ataques de hombre en el navegador (MitB) para solicitar a las víctimas sus números de teléfono móvil y tipos de dispositivos bancarios en línea para solicitar la

instalación de una aplicación de seguridad falsa, ahora llamada TrickMo.

Sin embargo, debido a las amenazas de seguridad planteadas por la autenticación basada en SMS, los mensajes pueden ser secuestrados fácilmente por aplicaciones de terceros maliciosas y también son vulnerables a los ataques de SIM Swapping, los bancos comienzan a depender cada vez más de las notificaciones automáticas para los usuarios, que contienen la transacción y detalles, además del número TAN.

Para superar este obstáculo, TrickMo utiliza las funciones de accesibilidad de Android que le permiten grabar un video de la pantalla de la aplicación, raspar los datos que se muestran en la pantalla, monitorear las aplicaciones que se ejecutan actualmente e incluso establecerse como la aplicación de SMS predeterminada.

Características de TrickMo

Una vez que se instala, TrickMo también puede ganar persistencia al iniciarse luego de que el dispositivo se vuelve interactivo o después de recibir un nuevo mensaje SMS. Además, presenta un mecanismo de configuración elaborado que permite a un atacante remoto emitir comandos para activar/desactivar funciones específicas (como permisos de accesibilidad, estado de grabación, estado de la aplicación de SMS), por medio de un servidor de comando y control (C2) o un mensaje SMS.

Cuando se ejecuta el malware, extrae una amplia gama de información, que incluye:

- Información personal del dispositivo
- Mensajes SMS
- Grabar aplicaciones específicas para una contraseña de un solo uso (TAN)
- Fotos

Para evitar levantar sospechas al robar los códigos TAN, TrickMo activa la pantalla de

bloqueo, evitando de ese modo que los usuarios accedan a sus dispositivos. Específicamente, utiliza una falsa pantalla de actualización de Android para enmascarar sus operaciones de robo de OTP.

Por último, cuenta con funciones de autodestrucción y eliminación, lo que permite a los hackers detrás de TrickMo eliminar los rastros de la presencia del malware de un dispositivo luego de una operación exitosa.

El accionador de interrupción también se puede activar por SMS, pero los investigadores de IBM descubrieron que era posible descifrar los comandos SMS cifrados utilizando una clave privada RSA codificada incrustada en el código fuente, lo que permite generar la clave pública y crear un mensaje SMS que puede activar la función de autodestrucción.

Aunque esto significa que el malware puede eliminarse de forma remota mediante un mensaje SMS, es posible suponer que una versión futura de la aplicación podría rectificar el uso de cadenas de clave codificadas para el descifrado.

> *«El troyano TrickBot fue una de las cepas de malware bancario más activas en el ámbito del delito cibernético en 2019»*, dijeron los investigadores de IBM.
>
> *«Según nuestro análisis, es evidente que TrickMo está diseñado para ayudar a TrickBot a romper los métodos más recientes de autenticación basada en TAN. Una de las características más importantes que posee TrickMo es la función de grabación de aplicaciones, que es lo que brinda a TrickBot la capacidad de superar validaciones de aplicaciones pushTAN más nuevas implementadas por los bancos»,* agregaron.