Investigadores de seguridad cibernética descubrieron una nueva variedad de malware bancario que además de dirigirse a aplicaciones bancarias, también roba datos y credenciales de aplicaciones de redes sociales, citas y criptomonedas, teniendo un total de 337 aplicaciones no financieras para Android en su lista de objetivos.

Nombrado BlackRock por los investigadores de ThreatFabric, que descubrieron el troyano en mayo de este año, su código fuente se deriva de una versión filtrada del malware bancario Xerxes, que en sí mismo es una cepa del troyano bancario para Android LokiBot, que se vio activo entre 2016 y 2017.

Una de sus características principales es el robo de credenciales del usuario, además de interceptar mensajes SMS, secuestrar notificaciones y grabar pulsaciones de teclas de las apps específicas. También es capaz de esconderse de software antivirus.

> *«No solo el troyano sufrió cambios en su código, sino que también viene con una mayor lista de objetivos y ha estado en curso por un período más largo. Contiene una cantidad importante de aplicaciones sociales, de comunicación y de citas que no se han observado en las listas de objetivos para otros troyanos bancarios existentes»*, dijo ThreatFabric.

BlackRock recopila los datos abusando de los privilegios del Servicio de Accesibilidad de Android, para lo cual, busca los permisos de los usuarios bajo la apariencia de falsas actualizaciones de Google cuando se inicia por primera vez en el dispositivo.

Después, se otorga permisos adicionales y establece una conexión con un servidor de comando y control remoto (C2), para llevar a cabo sus actividades maliciosas mediante la inyección de superposiciones en las pantallas de inicio de sesión y pago de las aplicaciones específicas.

Estas superposiciones de robo de credenciales se han encontrado en aplicaciones bancarias que operan en Europa, Australia, Estados Unidos y Canadá, además de aplicaciones comerciales y de comunicación.

> *«La lista objetivo de aplicaciones no financieras contiene aplicaciones famosas como Tinder, TikTok, PlayStation, Facebook, Instagram, Skype, Snapchat, Twitter, Grinder, VK, Netflix, Uber, eBay, Amazon, Reddit y Tumblr, entre otras»,* dijeron los investigadores.

A inicios del año, los investigadores de IBM X-Force detallaron una nueva campaña de TrickBot, denominada TrickMo, que se encontró dirigida exclusivamente a usuarios alemanes con malware que utilizaba mal las funciones de accesibilidad para interceptar contraseñas de un solo uso (OTP), TAN móvil (mTAN) y códigos de autenticación pushTAN.

Lo que hace que la campaña de BlackRock sea diferente es el gran listado de objetivos específicos (aplicaciones), que van más allá de aplicaciones de banca móvil.

> *«Después de Alien, Eventbot y BlackRock, podemos esperar que los actores de amenazas con motivación financiera construyan nuevos troyanos bancarios y sigan mejorando los existentes. Con los cambios que esperamos que se realicen en los troyanos de banca móvil, la línea entre el malware bancario y el spyware se vuelve más delgada, el malware bancario representará una amenaza para más organizaciones»,* dijeron los investigadores.