Crean virus en Corea que llama a un fraude bancario, advierten

Posted on 18 de abril de 2022 by Diario Humano

Los ciberdelincuentes detrás de Fakecalls han combinado troyanos bancarios con la ingeniería social, por lo que sus víctimas tienen más probabilidades de perder dinero y datos personales

Diario Humano | La Paz, Baja California Sur (BCS).-

El troyano bancario "Fakecalls" se hace pasar por una aplicación bancaria e imita el servicio telefónico de atención al cliente de los bancos surcoreanos más populares.

A diferencia de los troyanos bancarios habituales, puede interceptar discretamente las llamadas a los bancos reales utilizando su propia conexión. Bajo la apariencia de empleados bancarios, los ciberdelincuentes intentan obtener de sus víctimas, datos de pago e información confidencial.

Los analistas de Kaspersky descubrieron el troyano bancario Fakecalls y durante su investigación, vieron que cuando una víctima llama a la línea directa del banco, el troyano abre su propia llamada falsa en lugar de la auténtica del banco.

Hay dos posibles escenarios que se desarrollan después de interceptar la llamada; en el primero, Fakecalls conecta a la víctima directamente con los ciberdelincuentes que se presentan como el servicio de atención al cliente del banco. En el segundo, el troyano reproduce un audio pregrabado que imita un saludo y una conversación estándar utilizando un buzón de voz automatizado.

De vez en cuando, el troyano inserta pequeños fragmentos de audio en coreano. Por ejemplo,

“Hola. Gracias por llamar a nuestro banco. Nuestro centro de llamadas está recibiendo un alto volumen de llamadas. Un asesor hablará con usted lo antes posible”. Esto les permite ganarse la confianza de sus víctimas haciéndoles creer que la llamada es real. El objetivo principal de este tipo de llamadas es obtener de las víctimas la mayor cantidad posible de información vulnerable, incluidos los datos de sus cuentas bancarias.

Pantalla de falsa llamada que el troyano abre después de que la víctima intente llamar al banco real

Sin embargo, los ciberdelincuentes que utilizan este troyano no han tenido en cuenta que algunas de sus víctimas potenciales pueden utilizar diferentes idiomas de interfaz, por ejemplo, el inglés en lugar del coreano. La pantalla de Fakecall sólo tiene una versión en coreano, lo que significa que algunos de los usuarios que utilizan el idioma de la interfaz en inglés se darán cuenta de la amenaza.

La aplicación Fakecall, disfrazada de auténtica aplicación bancaria, pide una serie de permisos, como el acceso a los contactos, el micrófono, la cámara, la geolocalización y la gestión de las llamadas. Estos permisos permiten al troyano descartar las llamadas entrantes y borrarlas del historial del dispositivo, por ejemplo, cuando el banco real está intentando contactar con su cliente.

El troyano imita las aplicaciones de los bancos coreanos más populares

El troyano Fakecalls no sólo es capaz de controlar las llamadas entrantes, sino que también es capaz de falsificar las llamadas salientes. Si los ciberdelincuentes quieren contactar con la víctima, el troyano muestra su propia pantalla de llamada sobre la del sistema.

De esta forma, el usuario no ve el número real utilizado por los ciberdelincuentes, sino el número de teléfono del servicio de asistencia del banco mostrado por el troyano.

Fakecalls imita completamente las aplicaciones móviles de conocidos bancos surcoreanos. Insertan los logotipos reales de los bancos y muestran los números de asistencia reales de los bancos tal y como aparecen en la página principal de sus sitios web oficiales.

“A los clientes de la banca se les alerta constantemente para que estén atentos a las llamadas recibidas que puedan ser de ciberdelincuentes.

Sin embargo, cuando ellos intentan contactar directamente con el servicio de atención al cliente del banco, no esperan ningún peligro. Por lo general, confiamos en los empleados del banco: les llamamos para pedir ayuda y, por tanto, podemos decirles a ellos, o a sus suplantadores, cualquier información solicitada”, comenta Igor Golovin, analista de seguridad de Kaspersky.

“Los ciberdelincuentes que crearon Fakecalls han combinado dos tecnologías peligrosas: troyanos bancarios e ingeniería social, por lo que sus víctimas tienen más probabilidades de perder dinero y datos personales.

Cuando descargues una nueva aplicación de banca móvil, ten en cuenta qué permisos te pide. Si intenta obtener un acceso sospechosamente excesivo a los controles del dispositivo, incluido el acceso a la gestión de llamadas, lo más probable es que la aplicación sea un troyano bancario”.

Para evitar que el dinero o datos personales caigan en manos de los estafadores, se recomienda:

Descargar sólo las aplicaciones de las tiendas oficiales. No permitas la instalación desde fuentes desconocidas. Las tiendas oficiales comprueban todos los programas y, si el malware consigue colarse, suele eliminarse rápidamente.

Prestar atención a los permisos que piden las aplicaciones y si realmente los necesitan. No tengas miedo de denegar permisos, especialmente los potencialmente peligrosos como el acceso a las llamadas, los mensajes de texto, la accesibilidad, etc.

No dar nunca información confidencial por teléfono. Los verdaderos empleados del banco nunca te pedirán tus credenciales de acceso a la banca online, el PIN, el código de seguridad de la tarjeta o los códigos de confirmación de los mensajes de texto. En caso de duda, acude al sitio web oficial del banco y averigua qué pueden y qué no pueden preguntar los empleados.

Instala una solución de seguridad de confianza que proteja todos tus dispositivos de troyanos bancarios y otros programas maliciosos.

Puedes leer el informe completo sobre el troyano Fakecalls en Securelist.