BOLETÍN DE ALERTA

Boletín Nro.: 2020-12
Fecha de publicación: 30/04/2020
Tema: Incremento en casos de SIM Swapping para robo de información de cuentas vinculadas

Descripción:

Recientemente en nuestro país han ocurrido nuevos casos de **SIM Swapping (duplicado de tarjeta SIM)**, mediante la cual un delincuente consigue una copia de la tarjeta SIM con el, **número telefónico** de la víctima a través de engaños a las **compañías telefónicas**, **con lo que posteriormente puede acceder a las cuentas que se encuentren vinculadas a dicho número telefónico (correo electrónico, cuentas de redes sociales, Whatsapp, cuentas bancarias, etc.)**

¿Cómo funciona esta técnica?

Un delincuente **recopila o utiliza información pública disponible** sobre la víctima con el fin de engañar a las **compañías telefónicas**, haciéndose pasar por el **titular de la línea**, y así convencer al operador de **bloquear la tarjeta SIM del titular**. Este engaño depende de la **"creatividad"** del delincuente, un engaño creíble sería **por ejemplo**, reportar el robo del teléfono, y que por ello la llamada es desde un número distinto, recalcando la urgencia del bloqueo del número telefónico. Seguidamente, el delincuente acude a un puesto o local de reactivación de chip de la compañía telefónica y se hace pasar por la víctima para obtener un **duplicado** de la **tarjeta SIM** con el número de teléfono deseado y así suplantar la identidad del titular. En todo este proceso, tanto para el bloqueo del chip como su posterior reimpresión, la validación de la identidad del titular por parte de la compañía es escasa y/o poco efectiva.

Si bien, este tipo de ataque no es nuevo, hace un tiempo los criminales han empezado a usarlo para, de esta manera, una vez que tienen en su poder el número de teléfono de la víctima, lograr acceder a las cuentas digitales asociadas al número, tales como las cuentas de correo electrónico, redes sociales, Whastapp, cuentas bancarias, etc., teniendo en cuenta que la gran mayoría de las plataformas hoy en día exigen que la cuenta se vincule a un número de teléfono. El delincuente puede utilizar la funcionalidad de recuperación de contraseña; en la mayoría de las plataformas, una de las opciones de verificación es el envío de un código

mediante **SMS** al número de teléfono asociado. Como el delincuente ya está en posesión de ese número, él recibe el código y puede acceder a la cuenta. En el caso de Whatsapp, así como en la mayoría de las aplicaciones de mensajería instantánea, la aplicación verifica que el teléfono en la que está instalada, esté asociado al número de la víctima (lo cual, debido al SIM swapping es así) y automáticamente se abre la cuenta de la víctima.

Esta técnica puede ser utilizada para diversos fines, desde espionaje, extorsión, estafas, robo de dinero y muchos otros. Desde al menos un año, se ha observado un aumento importante de estos casos en nuestro país, afectando a políticos, periodistas, personalidades públicas, entre otros. Igualmente, muchos ciudadanos han sido víctima de estos ataques, ya sea por motivos personales como también para fines financieros (robos).

Impacto:

Un delincuente que tenga acceso al número de teléfono con el duplicado de la tarjeta SIM, podría descargar distintas aplicaciones que están asociadas normalmente al número de teléfono, simplemente seleccionar la opcion de "**Olvide mi contraseña**" y a partir del **código de recuperación** enviado por **SMS**, obtener la acceso a la cuenta de la víctima.

En el caso de **WhatsApp** podría registrarse con el número telefónico y seguidamente obtener acceso total a la aplicación.

Además el delincuente sería capaz de, leer y/o enviar mensajes entrantes, recibir y/o realizar llamadas y difundir información falsa en nombre del titular, lo que constituye un grave problema de seguridad y privacidad.

Solución y prevención:

- Una posible señal de un ataque **SIM Swapping** es perder la señal del servicio telefónico, ante esto se recomienda actuar rápidamente y contactar de inmediato con la compañia telefonica para tener conocimiento sobre lo sucedido.
- No compartir demasiada **información personal** en las redes sociales, ya que esto facilita a los delincuentes la obtención de dicha información, facilitando el proceso de engaño y seguida suplantación.
- Activar la **autenticación de doble factor**, pero evitando utilizar la opción de SMS y llamada, utilizando otros métodos (correo alternativo o aplicación de generación de

códigos). **. Algunas plataformas no permiten deshabilitar la opción de SMS para la recuperación de cuentas, por lo que serán vulnerables al SIM Swapping.**

- Utilizar una **aplicación de generación de códigos** (como **Google Authenticator**, por ejemplo) con la autenticación de doble factor, en vez del envío de SMS o llamadas. Esto, si bien podría reducir el riesgo de acceso a las cuentas vinculadas en algunos casos, no evita todos los problemas, ya que los SMS y llamadas igualmente serán recibidos por el delincuente, y algunas plataformas igualmente permiten SMS como mecanismo de verificación secundario, siendo la vinculación con un número telefónico obligatorio (y recomendable) en muchos casos.

- En el caso de **WhatsApp**, activar la verificación de dos pasos con esto, cualquier intento de verificación de un número de teléfono en WhatsApp estará acompañado de un PIN de seis dígitos, el mismo puede ser establecido al activar la función, de la siguiente manera: En la aplicación de WhatsApp diríjase a Ajustes/Configuración > Cuenta > Verificación en dos pasos > Activar.

- Ante la duda o indicios de un ataque de **SIM Swapping**, **desvincular** inmediatamente todas las cuentas ligadas al **número de teléfono**, y vincularla a otro número que no esté comprometido, aunque sea de manera temporal, además de **cambiar las contraseñas** de todas las **cuentas posiblemente comprometidas**. Como se trata de un ataque manual, desde el momento que el delincuente solicitó el bloqueo y logró el duplicado, suele haber un lapso de varios minutos o incluso horas, durante las cuales es posible actuar.

Para las **operadoras telefónicas**:

- Las compañías telefónicas deben robustecer los controles durante los procesos de **bloqueo** y **reimpresión** de SIM, asegurándose fehacientemente que quien está reportandolo o solicitándolo es efectivamente el titular. Para ello se debe considerar qué tipo de información o datos personales son fáciles de adivinar, descubrir o suplantar.

Información adicional:

- https://www.cert.gov.py/index.php/noticias/ataques-sim-swapping-que-son-como-protegerte
- https://www.pandasecurity.com/spain/mediacenter/dispositivos-moviles/sim-swapping/
- https://www.welivesecurity.com/la-es/2014/02/19/doble-factor-autenticacion-que-es-porque-lo-necesito/
- https://faq.whatsapp.com/26000021?lang=es