Jefatura para la Protección Presidencial

CSIRT

Equipo de Respuesta a Incidentes de Seguridad de la Información

Presidencia de la República

SUPLANTACIÓN DE CUENTAS DE WHATSAPP A través de la funcionalidad "Cambiar Número"

AC-0002-24

15/03/2024

SÍNTESIS

Se ha identificado una modalidad de ingeniería social que tiene como objetivo el robo de cuentas de WhatsApp, aprovechándose de una función legítima de esta aplicación conocida como "Cambiar Número".

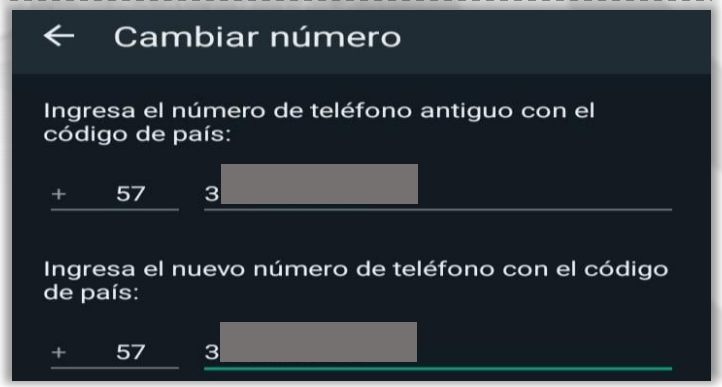
CONTEXTUALIZACIÓN

Mediante las actividades de análisis de vulnerabilidades llevadas a cabo por el CSIRT de la Presidencia de la República, como parte de su labor en la generación de alertas tempranas, se ha detectado el uso ilícito de una función de la aplicación de mensajería WhatsApp para la suplantación de cuentas.

VECTOR DE ATAQUE

A través de la función "Cambiar número", accesible dentro de los ajustes de cuenta de WhatsApp, se vincula el número actual de la cuenta con uno diferente al del legítimo titular. Posteriormente, toda la información y la titularidad de la cuenta se transfieren al número al que se dirige el ataque.

Toda esta configuración se lleva a cabo desde el teléfono del atacante hacia el de la víctima, sin necesidad de intervención por parte de la cuenta objetivo que se pretende afectar. Es decir, el atacante puede ejecutar el proceso de cambio de número y realizar la ingeniería social sin que la cuenta que se quiere usurpar participe activamente en el proceso.



COLOMBIA POTENCIA DE LA VIDA

TLP : GREEN

CONTEXTO DE AFECTACIÓN

Una vez se ha preparado la ejecución del ataque para acceder y suplantar la cuenta, se procede con el trabajo de ingeniería social.

- Esto puede llevarse a cabo mediante un mensaje de texto, un mensaje dentro de la misma aplicación de WhatsApp ó a través de una llamada utilizando una voz pregrabada o el sistema DTMF (Dual-Tone Multi-Frequency). El objetivo es obtener el código de verificación que se generará como una ventana emergente directamente en la aplicación WhatsApp de la víctima**.**

Se desactiva la casilla de "notificar a mis contactos" para que el cambio de número pase desapercibido.

ATAQUE DE INGENIERÍA SOCIAL

En está etapa del ataque, es crucial la interacción de la víctima, para lo cual se pueden emplear diversas técnicas de ingeniería social con el fin de obtener el código de verificación que se generará una vez que se envíe la opción de cambio de número.

- Es importante destacar que está técnica es capaz de eludir la verificación en dos pasos de la cuenta, lo que significa que el código obtenido a través de la aplicación es suficiente para llevar a cabo el cambio de titularidad de la cuenta.

- Entre las técnicas más utilizadas, se encuentra los mensajes engañosos que indica supuestos intentos de acceso y el phishing de WhatsApp Web y/o opciones de validación falsas, logrando que la víctima entregue el código generado de manera inadvertida.

En este punto crítico, la víctima ha proporcionado el código a través de una ventana emergente que parece legítima pero que en realidad es un sitio de phishing de la aplicación WhatsApp. Inmediatamente después, el atacante recibe el código de transferencia y toma el control total de la cuenta, así como el acceso a todos sus contactos e información personal. Además, con acceso al respaldo de la cuenta en la nube, para comprometer la información de la víctima en otros tipos de actividades delictivas, tales como estafas, amenazas, extorsión, etc.

CLASIFICACIÓN TLP : GREEN

Equipo de Respuesta a Incidentes de Seguridad Informática.
Presidencia de la República de Colombia.
csirt@presidencia.gov.co

COLOMBIA POTENCIA DE LA VIDA

Jefatura para la Protección Presidencial
CSIRT
Equipo de Respuesta a Incidentes de Seguridad de la Información

VARIANTE CON WHATSAPP WEB

RECOMENDACIONES DE PREVENCIÓN Y/O MITIGACIÓN

El **Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT**) de la Presidencia de la República, emite las siguientes recomendaciones para prevenir y protegerse contra este tipo de ataques de ingeniería social en la aplicación WhatsApp y servicios de mensajería:

1. **Verificación en dos pasos:** Active esta función para añadir una capa extra de seguridad, que requiere un código de acceso cada vez que se registre el número de teléfono en WhatsApp.

2. **Bloqueo de la aplicación:** Utilice el bloqueo de huella dactilar o reconocimiento facial si su dispositivo lo permite, para añadir una capa adicional de seguridad.

3. **Privacidad de la información**: Configure la privacidad de su última conexión, foto de perfil, estado e información para que solo la vean sus contactos o las personas que usted elija.

4. **Evite compartir información sensible:** Sea cauteloso (a) al compartir información personal o financiera a través de WhatsApp.

5. **Actualizaciones regulares:** Mantenga WhatsApp actualizado para asegurarse de que tiene las últimas funciones de seguridad y correcciones de vulnerabilidades en la App Store o Play Store.

6. **Advertencias de enlaces sospechosos:** Preste atención a las advertencias de WhatsApp sobre enlaces sospechosos y evite hacer clic en ellos.

7. **Reporte y bloquee a usuarios sospechosos:** Si recibe mensajes de números desconocidos o sospechosos, repórtelos y bloquéelos.

8. **Copia de seguridad segura:** Si realiza copias de seguridad de sus chats, asegúrese de protegerlas con cifrado y una contraseña fuerte.

9. **Activación eSIM:** Permite evitar el engaño al proveedor de telefonía móvil para que transfiera la tarjeta SIM de un dispositivo a otro.

CLASIFICACIÓN TLP : GREEN

Equipo de Respuesta a Incidentes de Seguridad Informática.
Presidencia de la República de Colombia.
csirt@presidencia.gov.co

COLOMBIA POTENCIA DE LA VIDA

Jefatura para la Protección Presidencial
CSIRT
Equipo de Respuesta a Incidentes de Seguridad de la Información