Centro Nacional de Seguridad Digital	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°088**	**Fecha: 15-04-2024**
		Página: 4 de 11

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Alerta con una nueva estafa que suplanta a Spotify, con timadores haciendo de gancho en grupos de Whatsapp		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

1. **ANTECEDENTES:**

Se detecta una nueva estafa que tiene a la plataforma musical Spotify como gancho. Con la falsa premisa de mejorar tu visibilidad si eres músico, o de ganar dinero escuchando canciones si no lo eres, te pueden vaciar la cuenta corriente.

Desde el 2018, se propagaban mensajes por WhatsApp donde se prometía un año de suscripción gratis en el servicio de música vía 'streaming' Spotify Premium, el cual era un engaño que infectaba su teléfono de publicidad maliciosa.

Al ingresar al enlace, la víctima es redireccionada a una página en la cual se presenta una encuesta que se debía llenar. Luego de responder a la encuesta, debías compartir la promoción con tus contactos a través de WhatsApp, asegurándose que el mensaje siga difundiéndose. Durante el procedimiento el dispositivo de la víctima quedaba infectado. Con ello también lograban robar los datos de acceso a la cuenta de Spotify de la víctima y venderlos luego en el mercado negro.

2. **DETALLES:**

Se trata de una nueva modalidad de timo por Whatsapp. El Periódico de España, del grupo Prensa Ibérica, ha corroborado con la propia multinacional sueca que no se trata de ninguna promoción real. "Confirmamos que esto no tiene nada que ver con Spotify y que este tipo de fraudes son bastante comunes", han aclarado fuentes de comunicación de la plataforma a este diario.

La innovación que incorpora es que la víctima sufre una especie de acoso y por parte de otros timadores. Personas que hacen el papel de usuarios de Spotify, pero que en realidad sirven como cebo para completar la estafa.

Hasta la fecha, las formas más habituales de fraude por redes sociales han contado con un método muy concreto: un estafador que se pone en contacto con la víctima simulando una identidad. Sea para fingir enamoramiento, darle trabajo o prometerle una herencia. Pero la estructura siempre suele ser esa: uno para uno. Un estafador para una víctima.

Pero esta actual estafa de Spotify tiene la particularidad de que la víctima se ve asediada por mensajes de muchas otras presuntas personas. Se le introduce en un grupo de chat con un montón de supuestos usuarios de Spotify, que simulan llevar a cabo la tarea que el incauto debe completar para ser integrado.

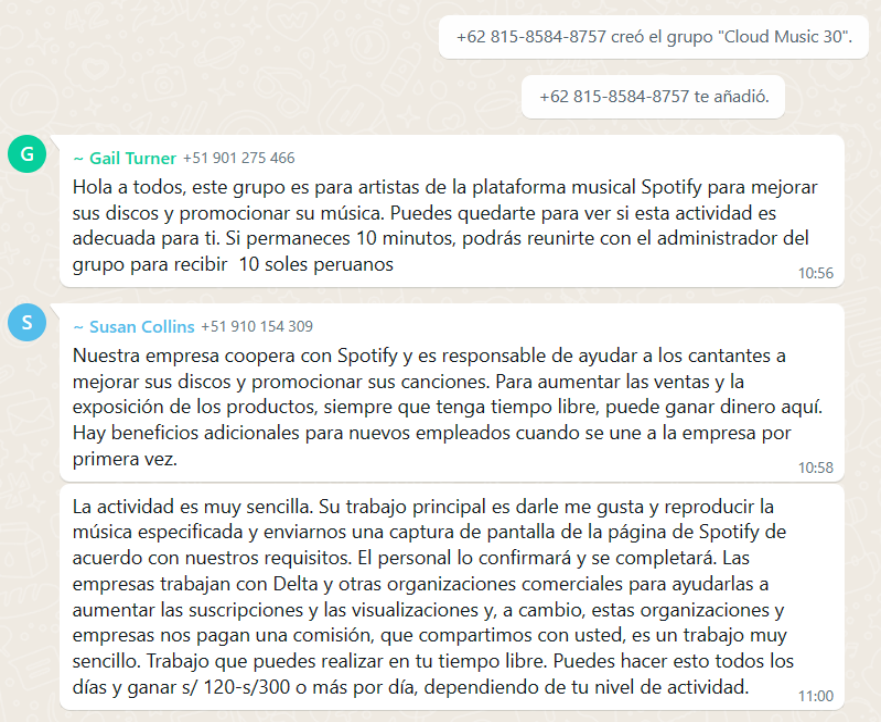
Actualmente están llevando este ataque a diferentes países latinos como el Perú.

La forma de proceder es la siguiente: la víctima abre la aplicación de Whatsapp y comprueba que ha sido incluido en un grupo de Whatsapp, de nombre "Spotify" o similar. Hay cerca de una veintena de supuestas personas más. Personas a las que no conoce, pero que, curiosamente, tienen todos número de teléfono local, es decir, de su país actual.

En este caso, sólo el creador del grupo tiene un teléfono extranjero.

Pero el resto de la veintena de personas son todos +51. Es decir, peruanos. Con esa maniobra intentan transmitir confianza, aunque no lo consiguen. En primer lugar, por el castellano del traductor que emplean los supuestos usuarios. En segundo lugar, porque, aunque los números sean peruanos, sus nombres son todos británicos. Aún no han pulido esa parte los estafadores.

Una vez dentro, un mensaje redactado por el administrador del grupo (que no es el mismo que el creador y también tiene número peruano), te da la bienvenida, tal como muestra la imagen (Aquí también se puede distinguir el código de teléfono de Indonesia).



Te invita a que escuches canciones mediante sus enlaces. Por cada canción que escuches y le des like, vas a recibir dinero. Lo único que tienes que hacer es enviar un pantallazo conforme has llevado a cabo dicha tarea. Así de sencillo.

A partir de ahí, el resto de los usuarios intervienen, algunos con sorpresa ("¿Quién me ha metido en este grupo? ¿Para qué sirve?"). Otros, con convencimiento ("Suena interesante, me gustaría intentarlo"). Otros, planteando dudas ("¿Necesito descargar canciones de Spotify o simplemente listarlas?"). Dudas que aprovecha el administrador para explicar, paso por paso, lo que hay que hacer para ganar ese dinero fácil.

Rápidamente, los supuestos usuarios empiezan a aportar pantallazos, demostrando que han llevado a cabo la más simple de las tareas encomendadas: escuchar una canción, darle "me gusta" y subir al grupo una captura. De hecho, esos mismos usuarios suben pantallazos de plataformas bancarias con supuestas transferencias recibidas, demostrándole a todo el mundo que han cobrado los 10 soles iniciales.

"Puedes hacer esto todos los días y ganar entre 120 y 300 soles o más por día, dependiendo de tu nivel de actividad", insiste el administrador, que va recibiendo mensajes de los otros usuarios, agradeciéndole las transferencias y animando a los demás a llevar a cabo dicha tarea. El detalle es que el resto de los usuarios son ganchos. De hecho, no son ni personas.

En realidad, el único número real es el del administrador. Es decir, el estafador. Tiene dos números distintos, pero son la misma persona. El estafador, en este caso, procede de Indonesia. Y tiene un número de su país, con el que crea el grupo. Pero se ha hecho con una línea de teléfono peruana. Con ella simula ser un empleado de Spotify.

Con ese número de teléfono le resulta relativamente fácil conseguir los denominados números virtuales. Se adquieren en plataformas de internet. Se trata de un segundo número de teléfono, vinculado a una línea principal. La gente suele recurrir a ellos, por ejemplo, para vender un departamento o un coche, para que no vaya circulando el número personal por internet. Una vez que lo vendes, te deshaces de él.

Una vez el estafador tiene esos números virtuales, los asocia a bots. Es decir, a cuentas de inteligencia artificial que tienen ya sus respuestas programadas. Las emplean a menudo las empresas para dar servicio de atención al cliente y prescindir de un trabajador. Los bots de Whatsapp están programados para dar respuestas automáticas. Esos son los integrantes del grupo: máquinas.

Vincular una línea a un bot se lleva a cabo con programas informáticos. Lo único que hay que hacer es programar las respuestas que tiene que dar ese bot en Whatsapp. A algunos les programa los mensajes de sorpresa. A otros, de alegría. A otros, las dudas. Y a la mayoría, los pantallazos que sirven de gancho para que el incauto se confíe.

Una vez que la víctima se ha creído que puede obtener dinero fácil escuchando música, el timo pasa a la siguiente fase, que es llevar a cabo las tareas requeridas. El incauto le da like a una de las canciones que ordena el administrador y envía el pantallazo, con la esperanza de cobrar.

A partir de ahí, se establece una conexión financiera con el estafador que puede, o bien pedir los datos de la tarjeta de la víctima para hacerle un ingreso (y ahí hacerle el destrozo) o bien pedirle que se abran una cuenta en una plataforma bancaria concreta con una cantidad de dinero determinado. Un dinero que la víctima no volverá a ver jamás. La estafa, para entonces, ya habrá sido completada.

IOCs:

- Teléfono creador del grupo fraudulento: +62 815-8584-8757
- Grupo: Cloud Music 30

3. RECOMENDACIONES:

- Evitar abrir archivos adjuntos o enlaces sospechosos, tanto en correos electrónicos no solicitados, como en mensajes de redes sociales tal como grupos de whatsapp donde no tengas plena confianza de la persona que lo envió.
- Usar solo aplicaciones esenciales. Mientras más software tengas, más vulnerabilidades potenciales tendrás.
- Capacitar a los usuarios sobre las mejores prácticas de ciberseguridad.
- Utilizar una solución oficial de software antivirus completa.
- Practicar una higiene estricta de sus contraseñas. Utilizar contraseñas únicas y complejas, y distintas para cada una de las cuentas, y cambiarlas periódicamente.

Fuente de Información:	• hxxps://amp.elperiodico.com/es/sociedad/20240414/alerta-nueva-estafa-suplanta-spotify-101043505 • hxxps://www.movilzona.es/2018/01/25/estafa-whatsapp-spotify/