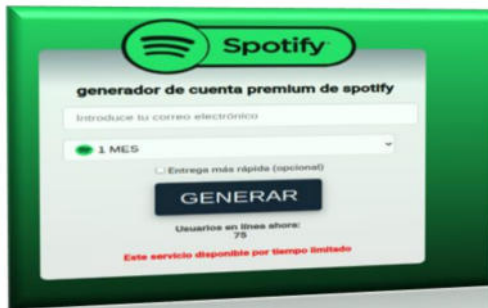
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 084		Fecha: 25-03-2022
			Página 8 de 10
Componente que reporta	DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ		
Nombre de Alerta	Suplantación de la identidad de la aplicación de música "Spotify"		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medio de Propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Subfamilia	G02
Clasificación temática familia	Fraude		

Descripción

1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes vienen llevando a cabo una campaña de Phishing, a través de los diferentes navegadores web, quienes vienen suplantando la identidad del servicio digital de música, podcasts y vídeos "Spotify", indicando que la compañía cuenta con un generador de cuenta Premium online, para todas las personas que desean adquirir un plan mensual, trimestral o anual del servicio.

2. Imagen: detalles del proceso de la estafa del Phishing.



Paso N° 01

Solicitan la dirección de correo electrónico y el plan que requiere, para obtener el servicio Premium gratis de Spotify.

Paso N° 02

Indica que la información está siendo procesada.

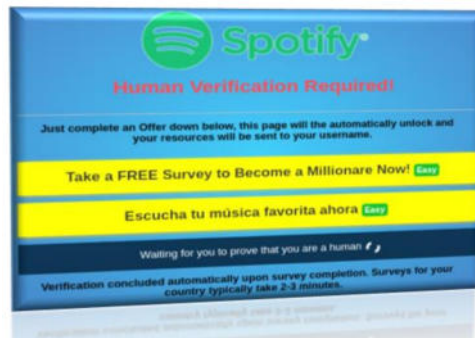


Paso N° 03

Luego de a ver esperado un cierto tiempo carga una ventana donde se requiere la verificación humana, para corroborar si es una persona real.

Paso N° 04

Solicita completar los siguientes pasos que se aprecian en la imagen, a fin de determinar que no sea un BOT (robot).



3. Se procedió a analizar la URL fraudulenta, obteniendo como resultado que ONCE (11) proveedores de seguridad informática alertan como **SUPLANTACIÓN DE IDENTIDAD – PHISHING.**

BitDefender	Phishing	CyRadar	Malicious
ESET	Phishing	ESTsecurity-Threat Inside	Phishing
Forcepoint ThreatSeeker	Phishing	Fortinet	Phishing
G-Data	Phishing	Kaspersky	Phishing
Lionic	Phishing	Phishing Database	Phishing

4. Indicadores de compromiso (IoC)

- ✓ SHA-256 : b10dfd5bd65f20aea367ee2cce8a41999a220285bd8a2929ac5c41d35d2fa234
- ✓ URL : hxxps://www[.]spotifyaccounts[.]tk/
- ✓ Dominio : spotifycuentas[.]tk
- ✓ IP : 74[.]125[.]193[.]121

5. Otras detecciones:

MALICIOSO

https://www.spotifyaccounts.tk/

Analizado en: 23/03/2022 15:03:03 (UTC)

Ambiente: windows 7 32 bits

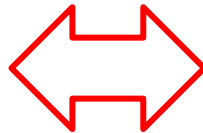
Puntaje de amenaza: 100/100

Detección AV: 11% Sitio de phishing

Indicadores: 4 8 7

La red:





malicioso

Puntaje de amenaza: 100/100

Detección AV: 56%

Etiquetado como: sitio de phishing

#suplantación de identidad #sumidero

6. Apreciación de la información:

- La presente campaña de Phishing, permite a los actores de amenazas obtener información personal y del correo electrónico.
- La propagación del sitio web fraudulento se realiza mediante envío masivos de email (SPAM), con la finalidad de obtener información sensible de las víctimas; asimismo, a través de las aplicaciones de mensajería instantánea entre ellos WhatsApp, Telegram y Messenger.

7. Referencia.

- Phishing o suplantación de identidad: Es un método que los ciberdelincuentes, utilizan para engañar a los usuarios para conseguir que revele información personal, como contraseñas, datos de tarjetas de créditos, números de cuentas bancarias, entre otros.

8. Algunas recomendaciones:

- Verificar detalladamente las URL de los sitios web.
- No abrir o descargar archivos sospechosos.
- No seguir las instrucciones de sitio web sospechoso.
- Mantener el antivirus actualizado.

Fuente de Información	Análisis propio de redes sociales y fuente abierta
-----------------------	--