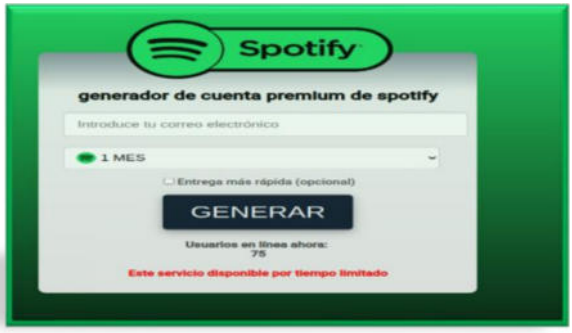
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 075	**Fecha: 16-03-2022**
		Página 7 de 9

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de Alerta	Phishing, suplantando 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

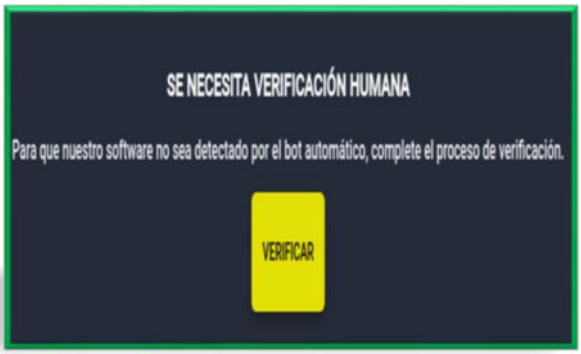
1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes vienen llevando a cabo una campaña de Phishing, a través de los diferentes navegadores web, quienes vienen suplantando la identidad del servicio digital de música, pódcasts y vídeos "Spotify", indicando 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***.

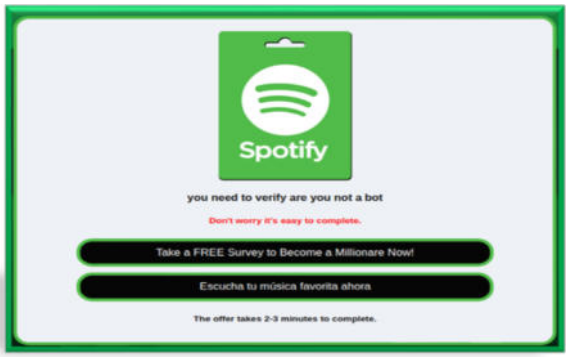


Paso Nº 01
Solicitan la dirección de correo electrónico y el plan que requiere, para obtener el servicio Premiun gratis de Spotify.

Paso Nº 02
Indica que la información está siendo procesada.



Paso Nº 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 Nº 04
Solicita completar los siguientes pasos que se aprecian en la imagen, a fin de determinar que no sea un BOT (robot).

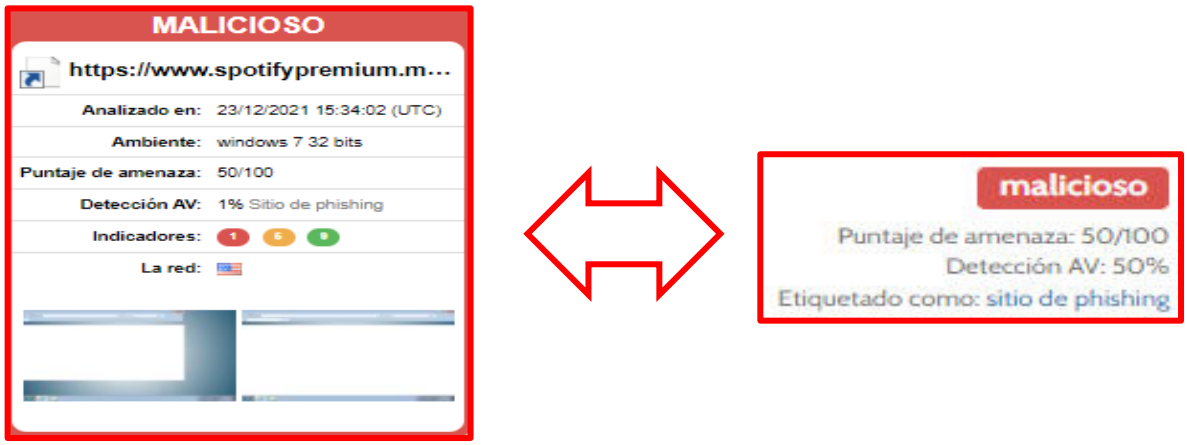
3. ***Se procedió a analizar la URL fraudulenta, obteniendo como resultado que CINCO (05) proveedores de seguridad informática alertan como SUPLANTACIÓN DE IDENTIDAD – PHISHING.***

BitDefender	Malware	CyRadar	Malicioso
ESET	Suplantación de identidad	Fortinet	Suplantación de identidad
G-datos	Malware	Abusix	Limpio

4. ***Indicadores de compromiso (IoC)***

- ✓ SHA-256 :8aed3945a6f514c7c74cf2d80ceada436035746765407a9fadac7dc535a07453
- ✓ URL : hxxps://www[.]spotifypremium[.]my[.]id/
- ✓ Dominio :spotify-premium[.]my[.]id
- ✓ IP : 142[.]250[.]136[.]211

5. ***Otras detecciones:***



6. ***Apreciación de la información*:**

- La presente campaña de Phishing, permite a los actores de amenazas obtener información personal, del correo electrónico y cuentas bancarias.
- La propagación del sitio web fraudulento se realiza mediante envió 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.
- Tener precaución al abrir enlaces de dudosa procedencia.

Fuente de Información	Análisis propio de redes sociales y fuente abierta