PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

Siempre con el pueblo

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Centro Nacional de Seguridad Digital

asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

Lima, 09 de mayo de 2022

N° 125-2022-CNSD

La presente **Alerta Integrada de Seguridad Digital** corresponde a un análisis técnico periódico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aérea del Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en el marco de la Seguridad Digital del Estado Peruano.

El objetivo de esta alerta **es informar a los responsables de la seguridad digital de las entidades públicas y las empresas privadas sobre las amenazas en el entorno digital** para advertir las situaciones que pudieran afectar la continuidad de sus servicios en favor de la población.

Las marcas y logotipos de empresas privadas y/o entidades públicas se reflejan para ilustrar la información que los ciudadanos reciben por redes sociales u otros medios y que atentan contra la confianza digital de las personas y de las mismas empresas **de acuerdo con lo establecido por el Decreto de Urgencia 007-2020**.

La presente Alerta Integrada de Seguridad Digital es información netamente especializada para informar a las áreas técnicas de entidades y empresas.

Contenido

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 125	Fecha: 09-05-2022
		Página 4 de 9

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Phishing, suplantando la identidad de la aplicación de música "Spotify"		
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 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", con la finalidad de robar información confidencial de las víctimas como, dirección de correo electrónico, contraseña, nombres, dirección de domicilio, datos de tarjeta bancaria, número de teléfono, entre otros.
2. ***Imagen: detalles del proceso de la estafa del Phishing***.

Paso Nº 01

Solicitan la dirección del correo electrónico y clave, para iniciar sesión en Spotify.

Paso Nº 02

Al iniciar sesión, requiere ingresar las credenciales de la tarjeta de crédito (Nombre, número, fecha de caducidad y código de seguridad).

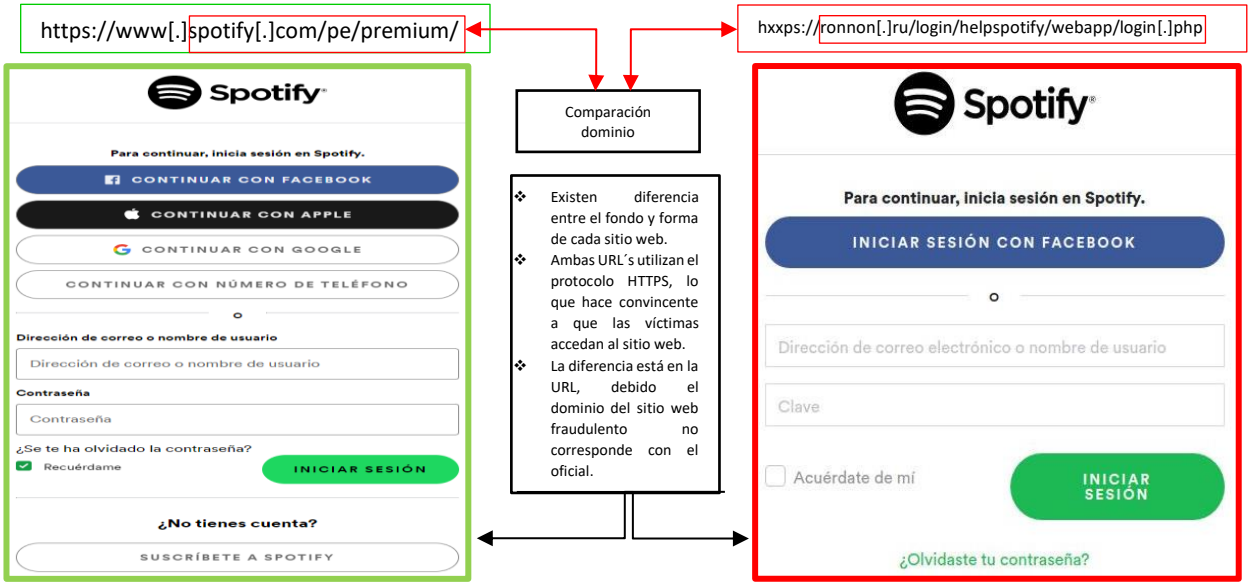
Paso Nº 03

Al continuar, requiere los datos personales (Fecha de nacimiento, Dirección, ciudad, código postal y número de teléfono).

Paso Nº 04

Luego de esperar se envía un código de verificación al número de teléfono, para ser redirigido al sitio web oficial de Spotify. Sin embargo, los ciberdelincuentes obtuvieron los datos brindados por la víctima.

3. *La Comparación del inicio de sesión del sitio web oficial y el sitio web falso.*



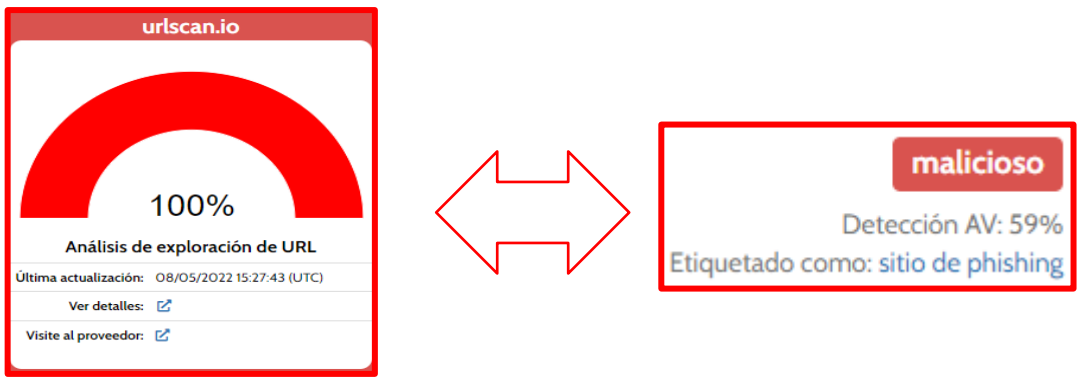
4. *Proveedores de seguridad informática alertan como PHISHING.*

alphaMountain.ai	Suplantación de identidad	BitDefender	Suplantación de identidad
CRDF	Malicioso	Emsisoft	Suplantación de identidad
ESET	Suplantación de identidad	Buscador de amenazas de Forcepoint	Suplantación de identidad
Fortinet	Suplantación de identidad	G-datos	Suplantación de identidad

5. *Indicadores de compromiso (IoC)*

- ✓ URL : hxxp://ronnon[.]ru/login/helpspotify/webapp/login[.]php
- ✓ Dominio : ronnon.ru
- ✓ IP : 92[.]53[.]96[.]200
- ✓ SHA-256 : 1ebe60f82025e74000f53b43918c4235d0cb76dca40e65354e54a253d6b701c7

6. *Otras detecciones:*



7. *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.

Fuentes de información	▪ Análisis propio de redes sociales y fuente abierta

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 125	Fecha: 09-05-2022
		Página 6 de 9

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad crítica de ejecución remota de código en Microsoft Integration Runtim		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. Resumen:

Se ha reportado una vulnerabilidad de severidad CRÍTICA de tipo inyección de código que afecta a Microsoft Integration Runtime (Magnitude Simba Amazon Redshift ODBC Driver). La explotación exitosa de esta vulnerabilidad podría permitir que un usuario privilegiado autenticado remoto/local aumente los privilegios dentro de la aplicación vulnerable.

2. Detalles:

- La vulnerabilidad de tipo inyección de código se debe a que el software construye todo o parte de un segmento de código utilizando la entrada influenciada externamente desde un componente ascendente, pero no neutraliza o neutraliza incorrectamente elementos especiales que podrían modificar la sintaxis o el comportamiento del segmento de código deseado.
- La vulnerabilidad identificada como CVE-2022-29972 podría permitir a un usuario local aumentar los privilegios dentro de la aplicación. La vulnerabilidad existe debido a una vulnerabilidad de inyección de argumentos en el componente de autenticación basado en navegador del controlador ODBC Magnitude Simba Amazon Redshift e implica una validación incorrecta de los tokens de autenticación. Un usuario local puede ejecutar código arbitrario y escalar privilegios dentro de la aplicación afectada.
- La vulnerabilidad CVE-2022-29972 está relacionado con una vulnerabilidad en Magnitude Simba Amazon Redshift ODBC Driver.

3. Productos afectados:

- Microsoft Integration Runtim: versión 1.0.5144.2, 1.1.5526.8, 1.2.5303.1, 1.4.5492.1, 1.4.5549.1, 1.5.5612.1, 1.6.5640.1, 1.6.5658.1, 1.6.5672.1, 1.6.5676.1, 1.6.5696.1, 1.6.5735.1, 1.7.5764.1, 1.7.5795.1, 1.8.5822.1, 1.9.5865.2, 1.10.5892.1, 1.11.5918.1, 1.12.5953.1, 1.13.5979.1, 2.0.6022.1, 2.1.6040.1, 2.2.6072.1, 2.3.6100.2, 2.4.6151.1, 2.5.6164.1, 2.6.6192.2, 2.7.6219.2, 2.7.6240.1, 2.8.6266.1, 2.8.6283.3, 2.9.6313.2, 2.10.6347.7, 2.11.6380.20, 2.12.6414.2, 2.13.6570.1, 3.0.6464.2, 3.1.6498.4, 3.1.6507.1, 3.2.6522.1, 3.3.6550.17, 3.4.6598.1, 3.5.6639.1, 3.5.6659.6, 3.6.6681.4, 3.7.6722.1, 3.8.6743.6, 3.9.6774.1, 3.10.6803.1, 3.10.6836.2, 3.10.6838.1, 3.11.6870.1, 3.11.6876.3, 3.12.6897.1, 3.13.6942.1, 3.14.6980.2, 3.14.6997.1, 3.15.7019.1, 3.16.7033.3, 3.16.7040.1, 3.16.7048.2, 3.16.7050.3, 3.16.7051.4, 3.17.7081.1, 3.18.7101.2, 3.18.7118.1, 3.19.7129.1, 3.19.7144.1, 3.19.7163.1, 3.20.7159.1, 4.0.7171.1, 4.0.7184.1, 4.1.7191.1, 4.1.7202.1, 4.2.7233.1, 4.3.7255.1, 4.3.7262.6, 4.3.7265.1, 4.4.7279.1, 4.4.7292.1, 4.5.7311.1, 4.5.7316.1, 4.6.7339.1, 4.6.7357.1, 4.6.7367.1, 4.7.7368.1, 4.7.7383.1, 4.8.7418.1, 4.9.7430.1, 4.9.7435.1, 4.9.7441.2, 4.9.7445.1, 4.10.7465.1, 4.10.7478.1, 4.11.7491.1, 4.11.7512.1, 4.11.7515.1, 4.11.7521.1, 4.12.7538.2, 4.12.7549.1, 4.12.7566.1, 4.13.7558.2, 4.13.7571.3, 4.14.7586.1, 4.14.7594.1, 4.14.7605.1, 4.15.7611.1, 5.0.7632.4, 5.1.7655.1, 5.1.7681.5, 5.1.7691.1, 5.2.7674.1, 5.2.7681.6, 5.2.7695.1, 5.2.7697.1, 5.2.7713.1, 5.2.7740.4, 5.3.7718.1, 5.3.7720.1, 5.3.7728.2, 5.4.7732.1, 5.4.7741.1, 5.4.7749.1, 5.4.7793.1, 5.4.7803.1, 5.5.7762.1, 5.5.7786.2, 5.5.7815.1, 5.6.7795.1, 5.6.7809.1, 5.6.7829.1, 5.7.7834.1, 5.7.7848.3, 5.8.7856.3, 5.8.7872.1, 5.8.7875.2, 5.9.7885.3, 5.9.7894.1, 5.9.7900.1, 5.9.7935.1, 5.9.7949.2, 5.10.7918.2, 5.10.7949.4, 5.10.7950.3, 5.11.7953.1, 5.11.7971.2, 5.12.7984.1, 5.13.8013.1, 5.14.8040.2, 5.14.8055.1, 5.14.8067.1, 5.15.8079.1 y 5.16.8105.2.

4. Solución:

- Microsoft recomienda actualizar el producto afectado a la versión 5.15.8094.1 que corrige esta vulnerabilidad;
- La explotación de esta vulnerabilidad requiere que un atacante tenga al menos uno de los siguientes roles: administrador de sinapsis, colaborador de sinapsis y operador de cómputo Synapse.

Fuentes de información	▪ hxxps://insightsoftware.com/trust/security/advisories/redshift-and-athena-driver-vulnerability/ ▪ hxxps://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-29972 ▪ hxxps://www.magnitude.com/products/data-connectivity ▪ hXXps://msrc.microsoft.com/update-guide/en-US/vulnerability/ADV220001

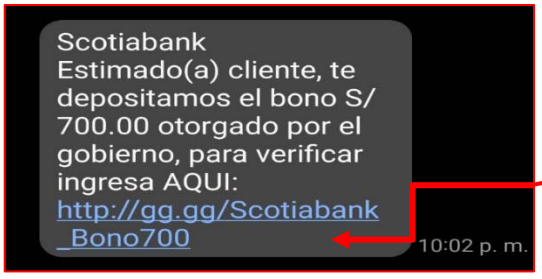
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 125	Fecha: 09-05-2022
		Página 7 de 9

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Smishing, Campaña de envió de SMS fraudulentos, suplantando la identidad del banco Scotiabank.		
Tipo de ataque	Smishing	Abreviatura	Smishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de subfamilia	G03
Clasificación temática familia	Fraude		

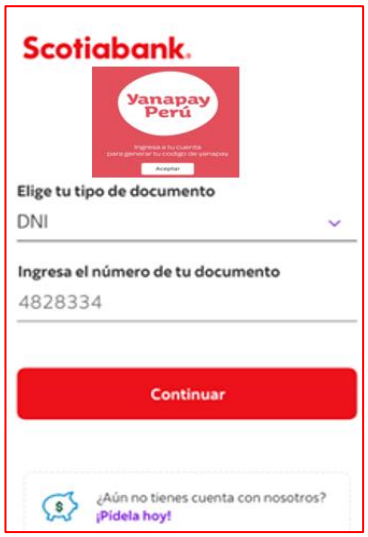
Descripción

1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes vienen llevando a cabo diferentes delitos informáticos empleando la modalidad de "Smishing" (SMS), quienes suplantan la identidad del Banco Scotiabank, indicando que el cliente cuenta con un bono de S/. 700.00, otorgado por el gobierno, para ello se quiere ingresar a un link adjuntado en el mensaje enviado, con la finalidad de robar información confidencial de las víctimas como, dirección de correo electrónico, contraseña, nombres, dirección de domicilio, datos de tarjeta bancaria, número de teléfono, entre otros.

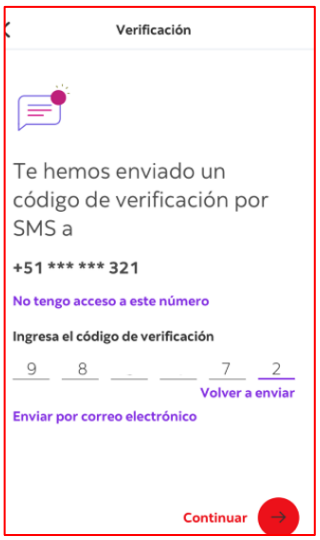
2. Detalles del proceso de estafa del Smishing:



Paso 01:
Mensaje enviado a la víctima.



Paso 02:
Una vez hecho clic, en el enlace del mensaje, es redirigido a un sitio falso que suplanta la identidad del Banco Scotiabank, con el fondo de Yanapay Perú, donde se debe ingresar número de DNI.



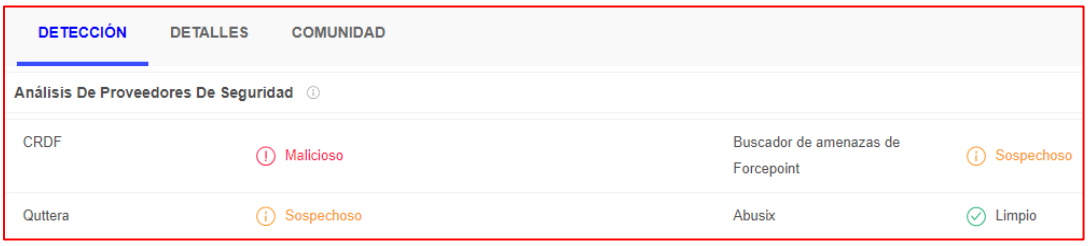
Paso 03:
El sitio web falso requiere el ingreso de un número de <celular> para recibir un <código de verificación por SMS>, al ingresar el supuesto cogido de verificación y hacer clic en continuar.

Paso 04:
Pasado unos segundos, carga una ventana donde requiere el ingreso de credenciales de acceso <número de tarjeta, clave web> y un mensaje indicando la "banca telefónica atenderá de 08:00 a.m. a 6:00 p.m., Sin embargo, los ciberdelincuentes obtuvieron los datos brindados por la víctima.

3. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD:**

- **INDICADORES DE COMPROMISO:**

  - ✓ **URL** : hxxp://gg.gg/Scotiabank_Bono700
  - ✓ **Dominio :** gg.gg/Scotiabank
  - ✓ **IP** : 185[.]15[.]209[.]141
  - ✓ **SHA-256 :** 9341a2a96bfb6b523a8cf02cf79e9d1d858898a1ad1fe18c378ff4af80cc5ab3



- **OTRAS DETECCIONES:**

4. Cómo funciona el Smishing:

- Los correos electrónicos incluyen enlaces de sitios web preparados por los ciberdelincuentes en los que solicitan información personal.
- Medios de propagación del Smishing: WhatsApp, telegram, redes sociales, SMS entre otros.
- Los ciberdelincuentes intentan suplantar a una entidad legitima (organismo público o privado, entidad financiera, servicio técnico, etc.)

5. ALGUNAS RECOMENDACIONES:

- Verificar la información en la entidad correspondiente.
- Acceder al sitio web a través de fuentes oficiales.
- No abrir enlaces de dudosa procedencia.
- No seguir indicaciones de sitios web fraudulentos.
- No compartir la información con terceras personas, amigos o familiares.
- Mantener instalado un servicio de antivirus en el dispositivo.

Fuentes de información	▪ Análisis propio de redes sociales y fuente abierta

Índice alfabético