	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 070	**Fecha: 11-03-2022**
		Página 5 de 7

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de Alerta	Phishing, suplantando la identidad de la compañía multinacional de comercio electrónico Amazon.		
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			

Descripción

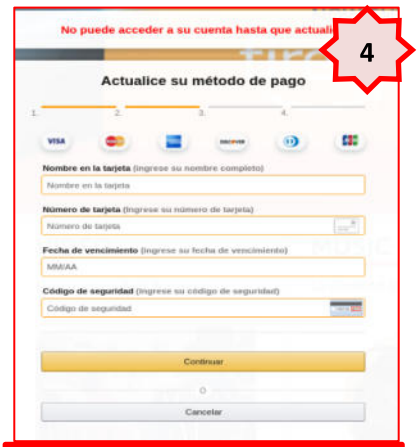
1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes vienen llevando a cabo una campaña de Phishing, propagado a través de los diferentes navegadores web, dirigido a los clientes de la compañía multinacional de comercio electrónico "Amazon", los cuales mediante la creación de un sitio web fraudulento solicitan a las posibles víctimas a ingresar las credenciales de inicio de sesión (dirección de correo electrónico y contraseña) del sitio web Amazon, para luego requieren datos bancarios como nombre y N° de tarjeta (debido, MasterCard, visa, etc.), fecha de vencimiento y código de seguridad, entre otros, a fin de realizar una supuesta actualización de información.

2. Proceso del ataque del Phishing:

Solicitan ingresar dirección de correo electrónico.

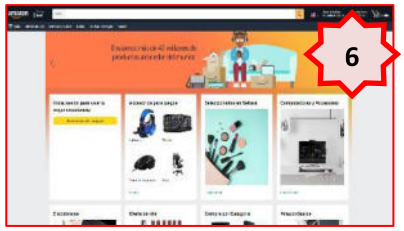
Luego requiere la contraseña o clave web.

A continuación, piden ingresar dirección de facturación, a fin de actualizar la información de la cuenta.



Después, solicitan actualizar método de pago ingresando nombre y N° de tarjeta, fecha de vencimiento y código de seguridad

Piden ingresar la clave de la tarjeta bancaria visa, debido, MasterCard, etc.



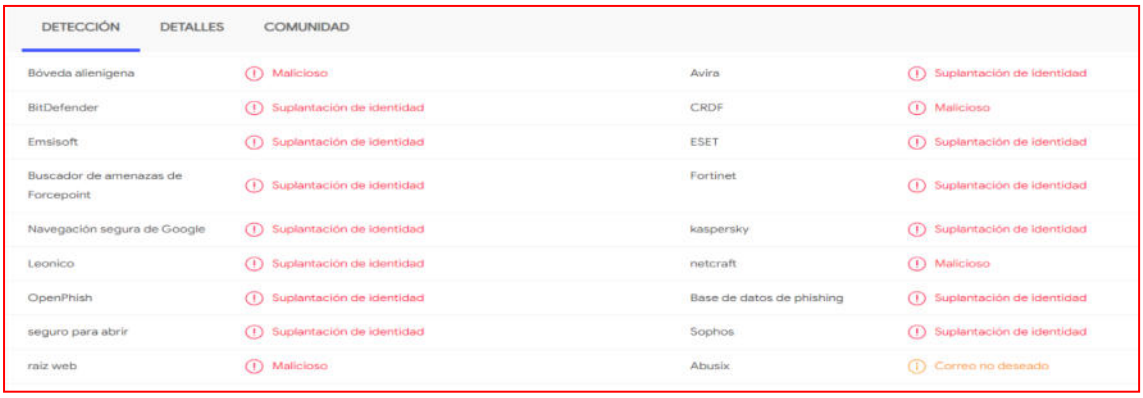
Finalmente, es redirigido automáticamente al sitio web oficial de Amazon, aludiendo un aparente error de autenticación; sin embargo, los datos fueros capturados por los ciberdelincuentes.

3. Comparación del sitio web oficial y fraudulento.

- El sitio web fraudulento utiliza protocolo HTTPS, lo que hace más convincente a que las víctimas accedan a la supuesta red social Instagram; sin embargo, la diferencia está en el dominio toda vez que, no coincide con el dominio de oficial.

4. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como Phishing (suplantación de identidad):

- Indicadores de compromiso:
  - URL: hxxps[:]//amazon[.]sittabarbo[.]com[.]br
  - Dominio: sittabarbo.com.br
  - IP: 162[.]241[.]2[.]248
  - Tamaño: 8.06 KB
  - SHA-256: c1a2c7630b93923f97047427e9950b0d5d1204e4a2c5f2f9e6ea0bcb808499f6



DETECCIÓN	DETALLES	COMUNIDAD			
Bóveda alienígena	Malicioso		Avira	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	
Navegación segura de Google	Suplantación de identidad		kaspersky	Suplantación de identidad	
Leonico	Suplantación de identidad		netcraft	Malicioso	
OpenPhish	Suplantación de identidad		Base de datos de phishing	Suplantación de identidad	
seguro para abrir	Suplantación de identidad		Sophos	Suplantación de identidad	
raiz web	Malicioso		Abusix	Correo no deseado	

- Otras detecciones:

5. Recomendaciones:

- Ingresar al sitio web desde fuentes oficiales o confiables.
- No brindar información personal a sitios web de dudosa procedencia.
- Mantener instalado un software antivirus.
- Ingresar de forma manual la dirección URL del sitio web.
- Verificar si la URL coincide con la del sitio web oficial.

Fuente de Información	Análisis propio de redes sociales y fuente abierta