	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 104	Fecha: 04-05-2023
		Página 8 de 10

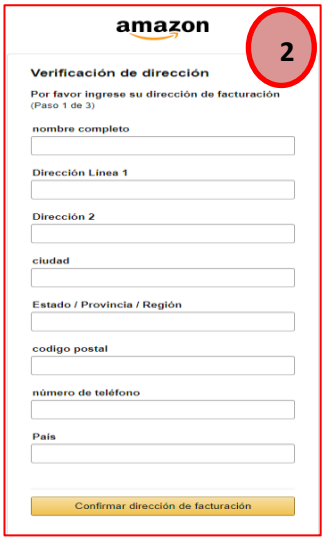
Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Campaña de Phishing suplantando la identidad de la compañía de comercio electrónico Amazon		
Tipo de ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de subfamilia	G02
Clasificación temática familia	Fraude		

Descripción

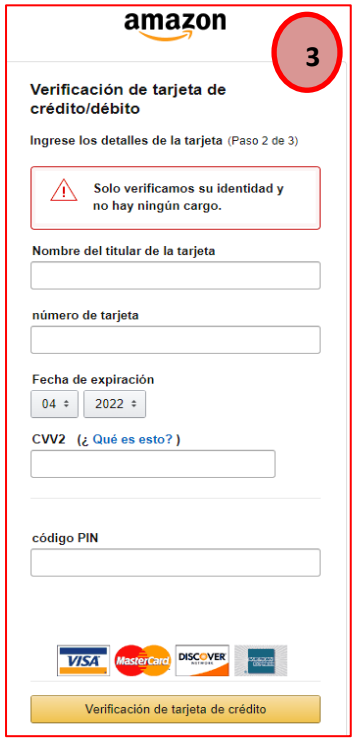
1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes vienen llevando a cabo una campaña de Phishing, por medio de los diferentes navegadores web, dirigido a los clientes y/o usuarios de la compañía de comercio electrónico Amazon; el cual, mediante la creación de un sitio web similar al original, solicitan a las posibles víctimas a ingresar información personal y bancaria como credenciales de inicio de sesión, contraseña, dirección de correo electrónico, clave, N° de tarjeta, fecha de expiración, etc.

2. Detalles del proceso de Phishing:

FOTOCAPTURA Nª01
Solicita ingresar las credenciales de inicio de sesión como dirección de Gmail y contraseña



FOTOCAPTURA Nª02
Pide dirección de domicilio, país, región, provincia, a fin de realizar una verificación de

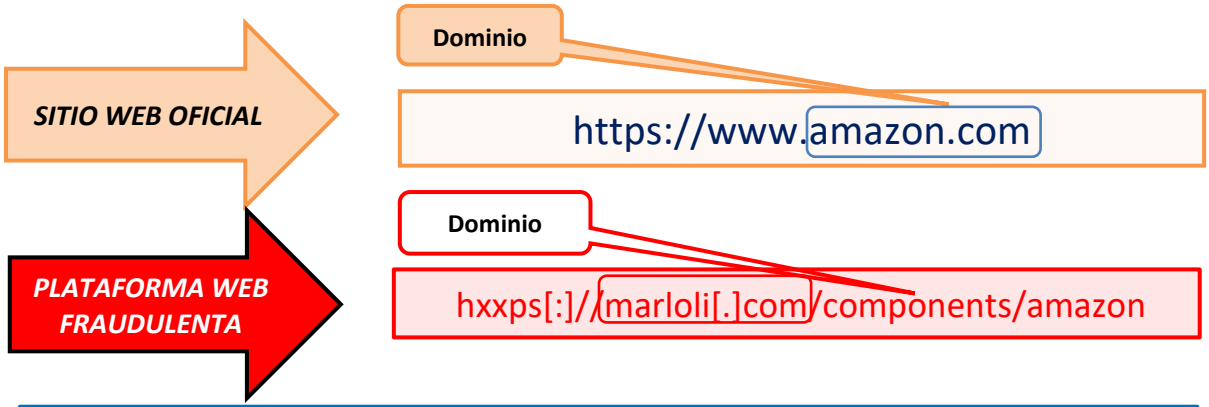


FOTOCAPTURA Nª03
Requiere, datos de tarjeta bancaria, a fin de realizar una verificación de identidad

FOTOCAPTURA Nª04
Después, indica que ingrese el código de autenticación enviado a través de mensaje de texto

FOTOCAPTURA Nª05
Una vez ingresa los datos solicitados, redirige de forma automática al sitio web oficial de Amazon; toda vez que los autores de la amenaza ya se apoderaron de los datos brindados

3. Comparación del sitio web oficial y sitio web fraudulento de Amazon:



- Existe una similitud entre el fondo y forma de cada sitio web (oficial y fraudulento).
- Ambos sitios webs poseen el ***PROTOCOLO SEGURO DE TRANSFERENCIA DE HIPERTEXTO (HTTPS)***, lo que hace mas convincente a que las víctimas ingresen a sitio web fraudulento

4. Proveedores de seguridad informática alertan como **SUPLANTACIÓN DE IDENTIDAD – PHISHING**:

alphaMountain.ai	Malicious	BitDefender	Malware
CyRadar	Malicious	Emsisoft	Phishing
Fortinet	Phishing	G-Data	Malware
Lionic	Malicious	Netcraft	Malicious
Trustwave	Phishing	Abusix	Clean

- Indicadores de compromiso:
  - URL: hxxps[:]//marloli[.]com/components/amazon
  - Dominio: marloli[.]com
  - SHA-256: 05193241298ec54241b307d8379da6953244404d7878f72ba797fa8776ab2cc1
  - Dirección IP: 45[.]79[.]148[.]55
  - Tamaño: 26.15 KB

5. Recomendaciones:

- Verificar la información en la entidad correspondiente.
- No seguir las instrucciones de sitio web sospechoso.
- Mantener el antivirus actualizado.
- No ingresar información confidencial a enlaces de dudosa procedencia.

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