

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 293		Fecha: 28-10-2022
			Página 08 de 10
Componente que reporta	DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ		
Nombre de la alerta	Phishing, suplantando la identidad de la aplicación de "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, a través de los diferentes navegadores web, quienes vienen suplantando la identidad del servicio digital de Amazon (Compañía de comercio electrónico), con la finalidad de obtener información confidencial de las víctimas como, dirección de correo electrónico, contraseña, fecha de nacimiento, país, número telefónico, datos bancarios, entre otros.

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



Paso N° 01

El sitio web, solicita ingresar la dirección de correo electrónico y dar clic en CONTINUAR.



Paso N° 02

Luego de haber ingresado el correo electrónico, requiere ingresar la contraseña, para iniciar sesión.



Paso N° 03

Al introducir las credenciales y hacer clic en <Iniciar sesión>, se cargará otro formulario en el cual solicitará ingresar los datos personales del usuario.



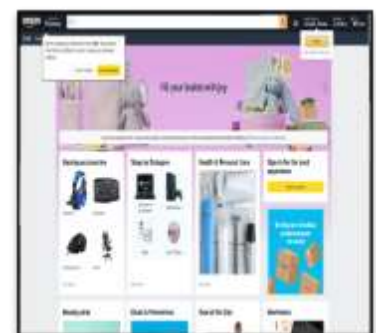
Paso N° 04

Después de haber completado toda la información personal, requiere el método de pago (Número de la tarjeta, Fecha de nacimiento y Código de seguridad).



Paso N° 05

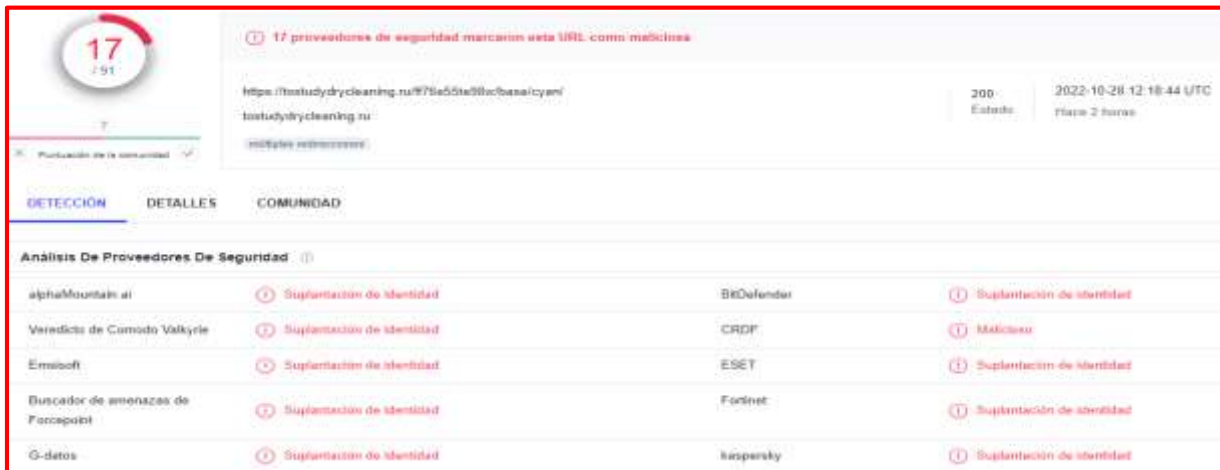
Después de haber completado toda la información del método de pago, requiere enlazar el correo electrónico ingresando la contraseña.



Paso N° 06

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

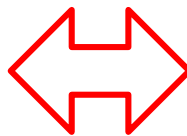
3. Se procedió a analizar la URL fraudulenta, obteniendo como resultado que DIECISIETE (17) proveedores de seguridad informática alertan como **SUPLANTACIÓN DE IDENTIDAD – PHISHING**.



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

- ✓ **SHA-256** : 619e33239f02fdc40f958860d348347a2631bd1a50f326cd62db0e50d7df6f53
- ✓ **URL** : hxtps://tostudydrycleaning[.]ru/ff76e55te98w/base/cyan/
- ✓ **IP** : 81[.]177[.]135[.]102
- ✓ **Dominio** : tostudydrycleaning.ru
- ✓ **Tamaño** : 6.44 KB

5. **Otras detecciones:**



6. **Que es un Phishing:**

Es un término informático que distingue a un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza, para manipularla y hacer que realice acciones que no debería realizar.

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.
- Tener precaución al abrir enlaces de dudosa procedencia.

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