	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°196	Fecha: 21-08-2023
		Página: 9 de 12

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Detección de una nueva campaña de Phishing a 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 Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

1. **ANTECEDENTES:**

A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes se encuentran desarrollando una nueva campaña de Phishing, a través de los diferentes navegadores web, quienes vienen suplantando la identidad de Amazon (Plataforma de comercio electrónico), con el objetivo robar credenciales de acceso, datos personales y bancarios del usuario.

2. **DETALLES:**

Imagen 1: Sitio web falso de Amazon solicita a la víctima, registrar las credenciales de acceso (Correo electrónico y contraseña), para

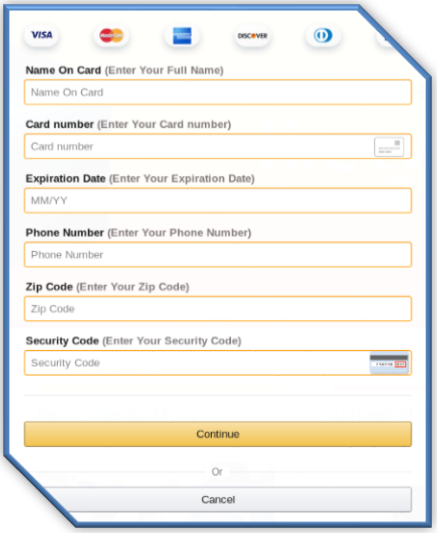


Imagen 2: Al ingresar, se visualizará un formulario, en el cual solicitará ingresar los datos personales del usuario.

Imagen 3: Después de haber completado toda la información personal y/o bancario, requiere enlazar el correo electrónico ingresando la contraseña.

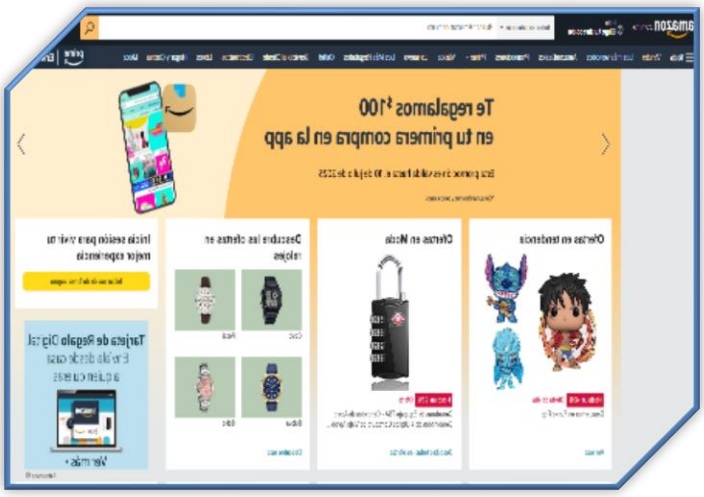


Imagen 4: Finalmente, es redirigido al sitio web oficial de Amazon, aludiendo un aparente error de autenticación; sin embargo, los datos fueron capturados por los ciberdelincuentes.

A. Comparación del sitio web oficial y fraudulento.

SITIO WEB OFICIAL

URL: https://www.amazon.com

SITIO WEB FRAUDULENTO

hxxps://www.na-amazon-creturns.com/&openid.identity=hxxp:/specs.openid.net/auth/2.0/identifier_select&openid.assoc_handle=amzn_returns_na&openid.mode=checkid_setup&marketPlaceId=A1YOV8979VXAH1&openid.claimed_id=hxxp:/specs. openid.net/auth/2.0/identifier_select&pageId=FCCustomerReturns&openid.ns=hxxp:/specs.openid.net/auth/2.0&suppressSignInRadioButtons=1

- Existe una diferencia entre la URL original y la URL fraudulenta.
- La URL falsa utiliza protocolo HTTPS, no significa que la web sea segura.
- Existe una similitud entre ambas páginas, en imagen, fondo y colores de ambos sitios web.

B. URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD en NUEVE (09) y MALICIOSOS en TRES (03).**

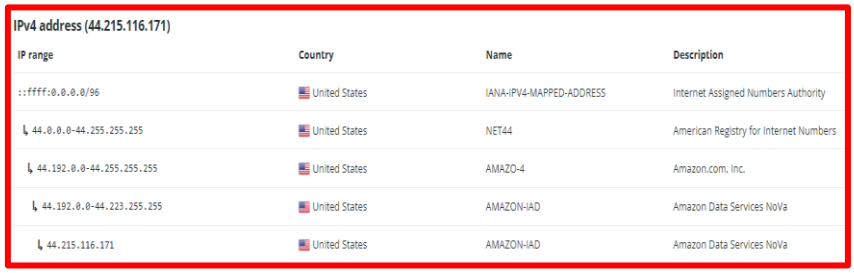
a) Indicadores de compromisos:

I. URL:

hxxps://www.na-amazon-creturns.com/&openid.identity=hxxp:/specs.openid.net/auth/2.0/identifier_select&openid.assoc_handle=amzn_returns_na&openid.mode=checkid_setup&marketPlaceId=A1YOV8979VXAH1&openid.claimed_id=hxxp:/specs. openid.net/auth/2.0/identifier_select&pageId=FCCustomerReturns&openid.ns=hxxp:/specs.openid.net/auth/2.0&suppressSignInRadioButtons=1

Site	https://www.na-amazon-creturns.com
Netblock Owner	Amazon Data Services NoVa
Hosting company	Amazon - US East (Northern Virginia) datacenter
Hosting country	us

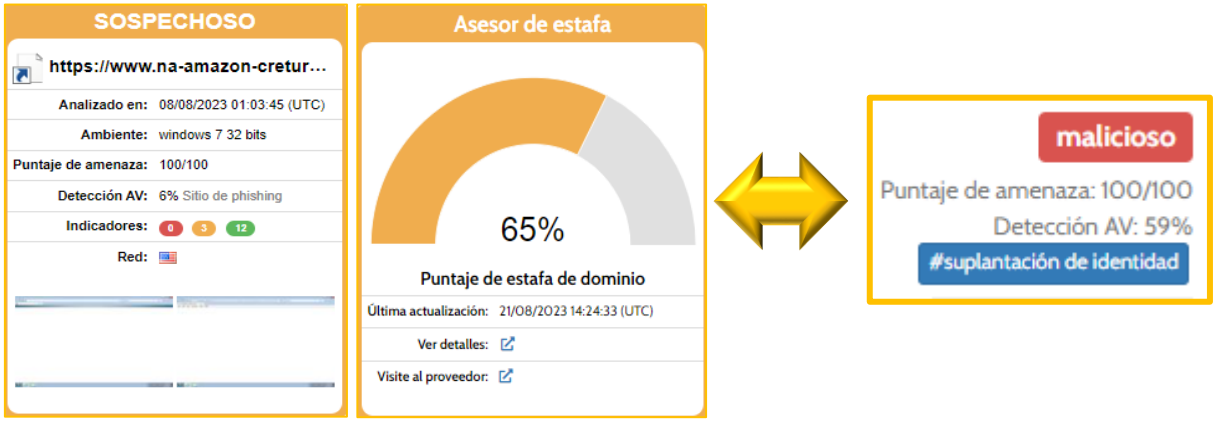
II. IP: 44[.]215[.]128[.]155



III. SHA-256: **3c32a623ae03991e431259cc9c3b2711546efb8a2cb5f434d1eff38d45693108**

IV. SERVIDOR: **Server**

C. Otras detecciones:



D. Cómo funciona el Phishing:

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

E. 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.

3. RECOMENDACIONES:

- Mantener instalado un servicio de antivirus en el dispositivo.
- Verificar la información del sitio web 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.

Fuente de Información:	Análisis propio de redes sociales y fuente abierta