	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°244	Fecha: 15-10-2023
		Página: 6 de 12

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Phishing, suplantando la identidad de la red social Instagram		
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 vienen llevando a cabo una campaña de Phishing, a través de diferentes navegadores web, quienes vienen suplantando la identidad del sitio de la red social "Instagram", el cual tiene como finalidad robar información sensible de las víctimas como usuario, correo electrónico y/o contraseña.

2. **DETALLES:**

IMAGEN 1:

Sitio web fraudulenta de la red social Instagram, solicita a las víctimas, ingresar las credenciales de inicio de sesión.

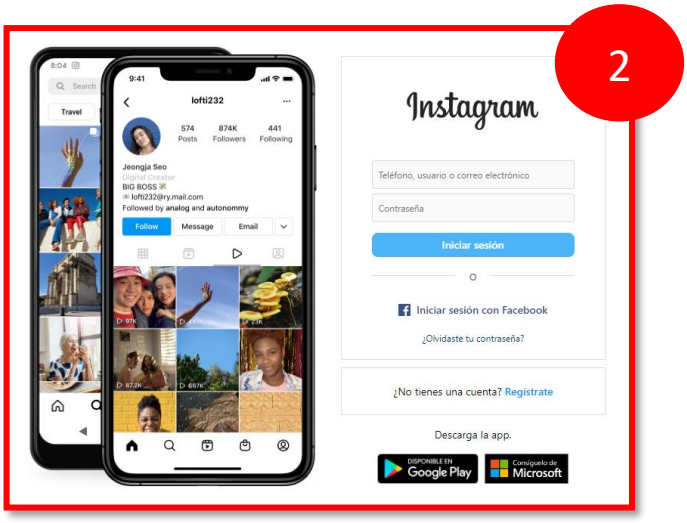


IMAGEN 2:

Al continuar con el proceso, redirige de manera automática al sitio web oficial, toda vez que los ciberdelincuentes ya se apoderaron de la información ingresada.

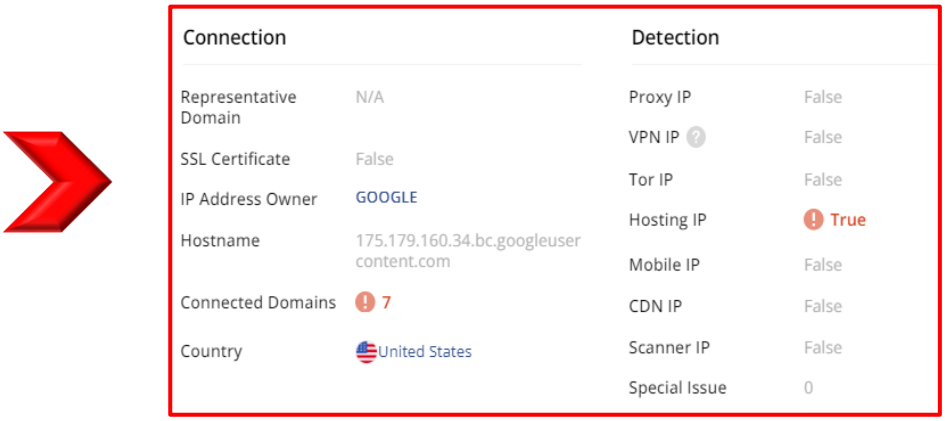
A. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD:**

a) Indicadores de compromisos:

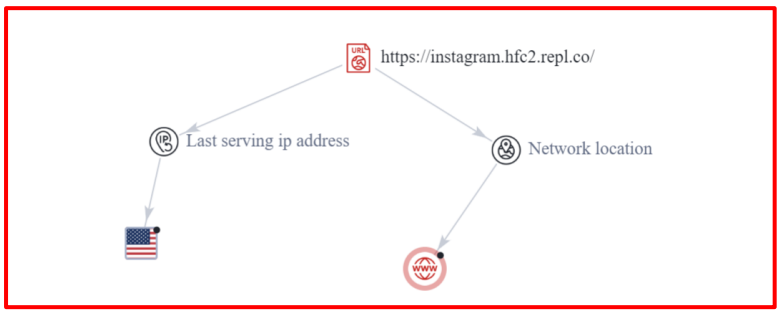
I. URL: hxxps[:]//Instagram[.]hfc2[.]repl[.]co/

II. SHA-256: 037e517def7176a1f0492a55fcfe5fb54a376b5ded4a01490af9458e45543bde

III. IP: 34[.]160[.]179[.]175



IV. TIPOLOGÍA

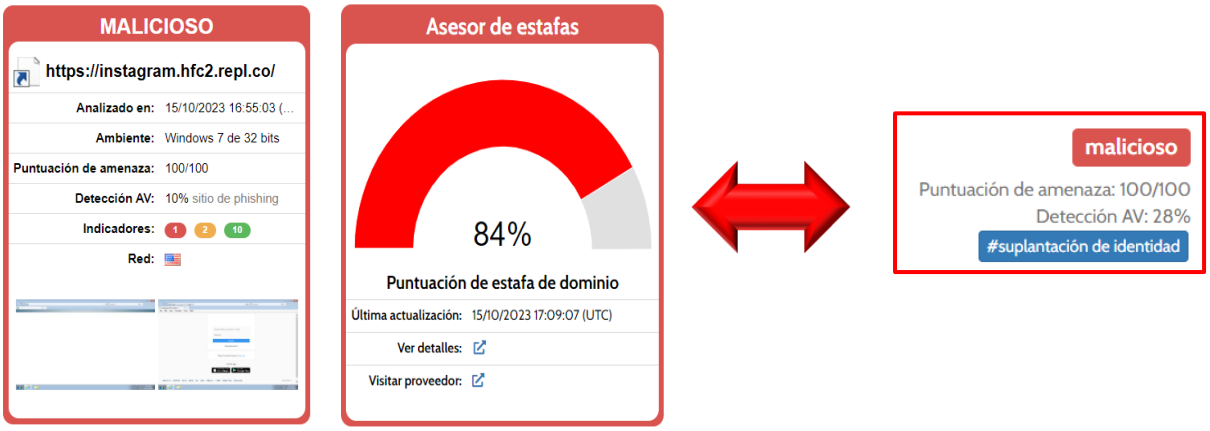


Se puede aprecia como la URL, esta alojada en un servidor ubicado en EE.UU.

B. Se hallaron **9 proveedores** de seguridad que marcaron este dominio como malicioso.

Avira	Phishing	BitDefender	Phishing
ESET	Phishing	G-Data	Phishing
Google Safebrowsing	Phishing	Kaspersky	Phishing
Netcraft	Malicious	PhishLabs	Phishing
Sophos	Phishing	Abusix	Clean

C. Otras detecciones:



D. Apreciación de la información:

- La presente campaña de Phishing permite a los actores de amenazas obtener las credenciales de acceso de la red social Instagram.
- La propagación del sitio web fraudulento se realiza mediante envió masivos de email, adjuntando enlaces de sitios web fraudulentos con la finalidad de obtener información sensible de las víctimas; asimismo, a través de las aplicaciones de mensajería instantánea entre ellos: WhatsApp, Telegram, Messenger, mensajes de textos - SMS, etc.

E. Referencia:

- 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.

3. RECOMENDACIONES:

- Evitar acceder a enlaces que llegan inesperadamente por correo electrónico u otros medios.
- No proporcionar datos personales (contraseñas, tarjetas, cuentas bancarias, etc.) por correo, teléfono o SMS.
- No introducir datos confidenciales en sitios web sospechosas o de dudosa procedencia.
- Verificar la fuente de información de tus correos entrantes.
- Introducir tus datos únicamente en webs seguras.
- Tener siempre actualizado el sistema operativo y el antivirus. En el caso del antivirus, comprobar que está activo.

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

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°244	Fecha: 14-10-2023
		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 la empresa 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 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 el Correo electrónico o número de teléfono móvil para continuar.

Imagen 2: Luego de continuar, el atacante le solicita a la víctima que registre la contraseña para ingresar a la cuenta.

Imagen 3: Al ingresar a la cuenta, le indica que tiene ingresar información personal como nombre completo, dirección, ciudad, estado, código postal, número de teléfono y fecha de nacimiento.

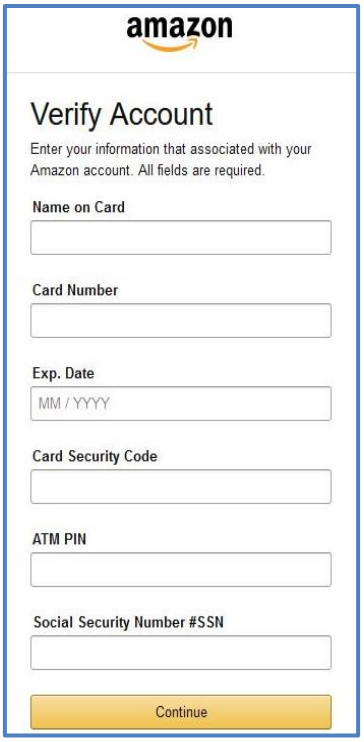


Imagen 4: Para finalizar, tiene que completar información bancaria como nombre de tarjeta, número de tarjeta, fecha de expiración, código de seguridad, numero de PIN y numero de seguridad social, luego de completar lo requerido es redirigido al sitio web oficial de Amazon, aludiendo un aparente error de autenticación; sin embargo, los datos fueron capturados por los ciberdelincuentes.

A. Comparación del sitio web oficial y fraudulento.

SITIO WEB OFICIAL

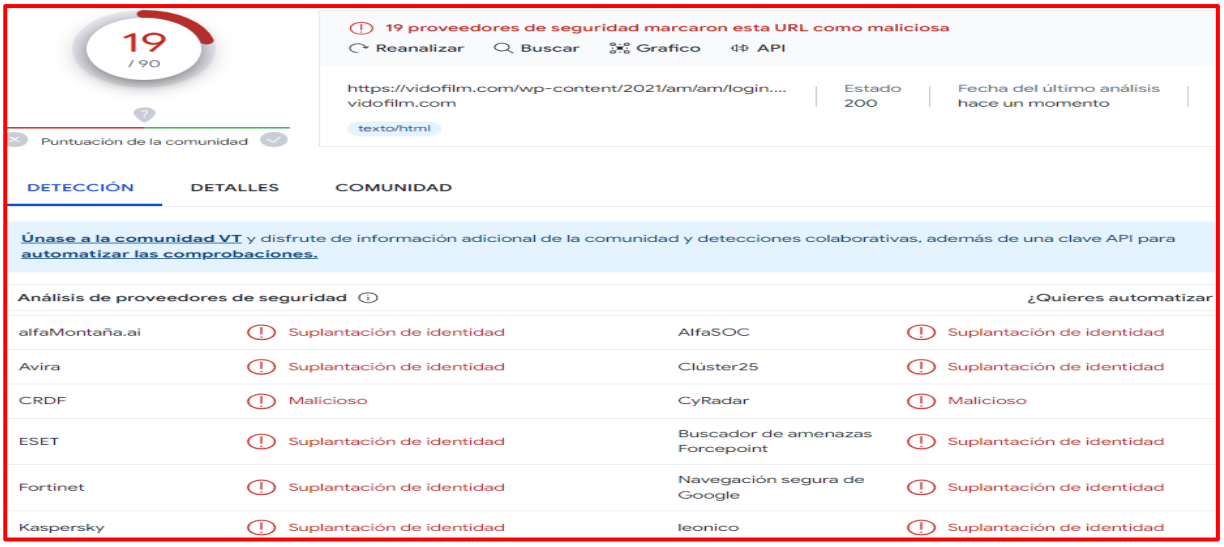
URL: https://www.amazon.com

SITIO WEB FRAUDULENTO

hxxps://vidofilm.com/wp-content/2021/am/am/login.php?openid.pape.max_auth_age=0&openid.return_to=hxxps%3A%2F%2Fwww.amazon.ca%2F%3F_encoding%3DUTF8% 26ref_%3Dnav_newcust&openid.identity=hxxp%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0%2Fidentifier_select&openid.assoc_handle=caflex&openid.mode=checkid_setup&openid.claimed_id=hxxp%3A%2F%2Fspecs.openid.net%2Fauth% 2F2.0%2Fidentifier_select&openid.ns=hxxp%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0

- 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).**



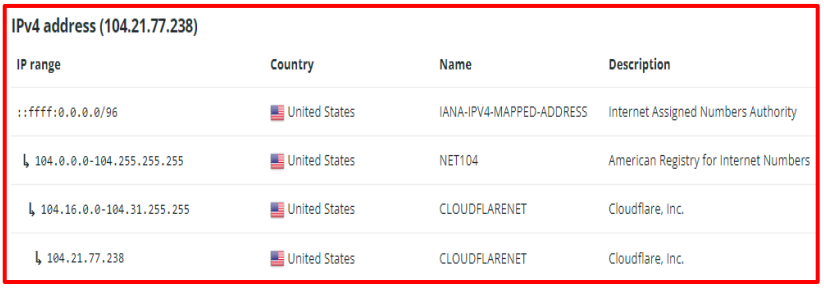
a) Indicadores de compromisos:

I. URL:

hxxps://vidofilm.com/wp-content/2021/am/am/login.php?openid.pape.max_auth_age=0&openid.return_to=hxxps%3A%2F%2Fwww.amazon.ca%2F%3F_encoding%3DUTF8% 26ref_%3Dnav_newcust&openid.identity=hxxp%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0%2Fidentifier_select&openid.assoc_handle=caflex&openid.mode=checkid_setup&openid.claimed_id=hxxp%3A%2F%2Fspecs.openid.net%2Fauth% 2F2.0%2Fidentifier_select&openid.ns=hxxp%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0

Site	**https://vidofilm.com**
Netblock Owner	**Cloudflare, Inc.**
Hosting company	Cloudflare
Hosting country	US

II. IP: 104[.]21[.]77[.]238



IPv4 address (104.21.77.238)

IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
↳ 104.0.0.0-104.255.255.255	United States	NET104	American Registry for Internet Numbers
↳ 104.16.0.0-104.31.255.255	United States	CLOUDFLARENET	Cloudflare, Inc.
↳ 104.21.77.238	United States	CLOUDFLARENET	Cloudflare, Inc.

III. SHA-256: **418f09446ea7a30c9fbe8fb49936387c1c1dbb72f00309ec50541199a629a815**

IV. SERVIDOR: **cloudflare**

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.