

	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:

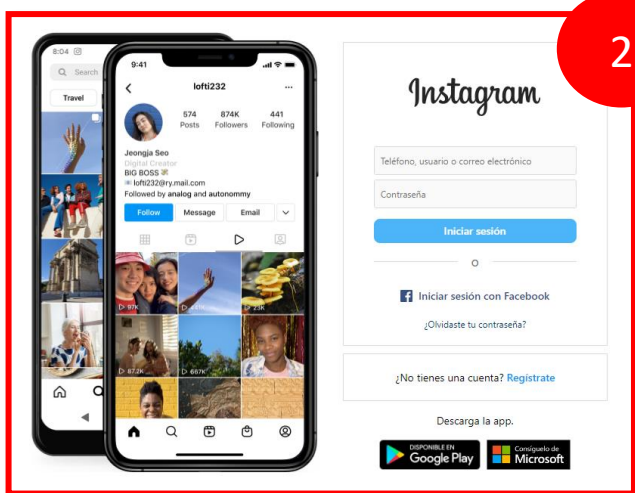
A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes vienen llevando a cabo una campaña de Phishing, a través de diferentes navegadores web, quienes vienen suplantando la identidad del sitio de la red social “Instagram”, el cual tiene como finalidad 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/



Nombre del envío:	hxxps://instagram.hfc2.repl.co/
Tamaño:	55B
Tipo:	URL
Mímica:	Texto sin formato
Sistema operativo:	ventanas
Último análisis antivirus:	15/10/2023 17:09:07 (UTC)
Último informe de Sandbox:	15/10/2023 16:55:03 (UTC)

II. **SHA-256:** 037e517def7176a1f0492a55fcfe5fb54a376b5ded4a01490af9458e45543bde



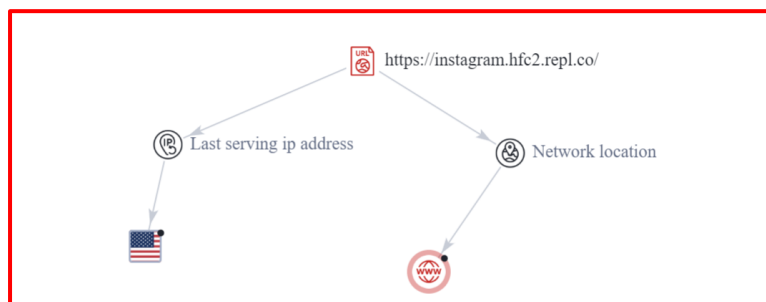
_286046D8-6B6B-11EE-B09E-0800274B4A36_dat	sospechoso
6247e27c482b4b4e8a98e6a2e98d27c7d186a95a5061d0c3d15440bbd6141992	
RecoveryStore_1E9D5849-6B6B-11EE-B09E-0800274B4A36_dat	sospechoso
d5db6f2198e36e1131ec4a8c83df087da0c5100e783483f9f69d8045ba2e19df	
_1E9D584B-6B6B-11EE-B09E-0800274B4A36_dat	sospechoso
2092343c6d83c46e804e28a1cbc5b651d808ff523efb70e066cd643b6fde8f2	

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



Connection		Detection	
Representative Domain	N/A	Proxy IP	False
SSL Certificate	False	VPN IP	False
IP Address Owner	GOOGLE	Tor IP	False
Hostname	175.179.160.34.bc.googleusercontent.com	Hosting IP	! True
Connected Domains	! 7	Mobile IP	False
Country	United States	CDN IP	False
		Scanner IP	False
		Special Issue	0

IV. **TIPOLOGÍA**



Se puede apreciar 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:

MALICIOSO

<https://instagram.hfc2.repl.co/>

Analizado en: 15/10/2023 16:55:03 (...)

Ambiente: Windows 7 de 32 bits

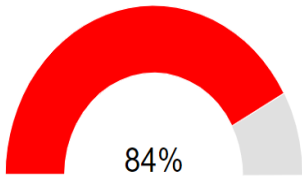
Puntuación de amenaza: 100/100

Detección AV: 10% sitio de phishing

Indicadores: 1 2 10

Red: 🇺🇸

Asesor de estafas



84%

Puntuación de estafa de dominio

Última actualización: 15/10/2023 17:09:07 (UTC)

Ver detalles: [🔗](#)

Visitar proveedor: [🔗](#)

↔

malicioso

Puntuación de amenaza: 100/100

Detección AV: 28%

#suplantación de identidad

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 envío 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:



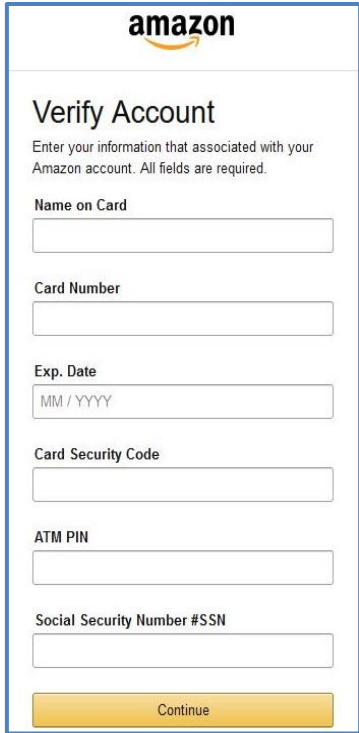
Imagen 1: Sitio web falso de Amazon solicita a la víctima, registrar el Correo electrónico o número de teléfono móvil para continuar.

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


```
hxhps://vidofilm.com/wp-content/2021/am/am/login.php?openid.pape.max_auth_age=0&openid.return_to=hxhps%3A%2F%2Fwww.amazon.ca%2F%3F_encoding%3DUTF8%26ref_%3Dnav_newcust&openid.identity=hxhp%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0%2Fid_entifier_select&openid.assoc_handle=cafex&openid.mode=checkid_setup&openid.claimed_id~hxhp%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0%2Fid_entifier_select&openid.ns=hxp%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).



Puntuación de la comunidad

19 proveedores de seguridad marcaron esta URL como maliciosa

Reanalizar | Buscar | Grafico | API

https://vidofilm.com/wp-content/2021/am/am/login... Estado 200 Fecha del último análisis hace un momento

texto/html

DETECCIÓN | DETALLES | COMUNIDAD

Únase a la comunidad VT y disfrute de información adicional de la comunidad y detecciones colaborativas, además de una clave API para automatizar las comprobaciones.

Análisis de proveedores de seguridad ¿Quieres automatizar

AlfaMontaña.ai	⚠ Suplantación de identidad	AlfaSOC	⚠ Suplantación de identidad
Avira	⚠ Suplantación de identidad	Clúster25	⚠ Suplantación de identidad
CRDF	⚠ Malicioso	CyRadar	⚠ Malicioso
ESET	⚠ Suplantación de identidad	Buscador de amenazas Forcepoint	⚠ Suplantación de identidad
Fortinet	⚠ Suplantación de identidad	Navegación segura de Google	⚠ Suplantación de identidad
Kaspersky	⚠ Suplantación de identidad	leonico	⚠ Suplantación de identidad

a) Indicadores de compromisos:

I. URL:

```
hxhps://vidofilm.com/wp-content/2021/am/am/login.php?openid.pape.max_auth_age=0&openid.return_to=hxhps%3A%2F%2Fwww.amazon.ca%2F%3F_encoding%3DUTF8%26ref_%3Dnav_newcust&openid.identity=hxhp%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0%2Fid_entifier_select&openid.assoc_handle=cafex&openid.mode=checkid_setup&openid.claimed_id~hxhp%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0%2Fid_entifier_select&openid.ns=hxp%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:

SOSPECHOSO

https://vidofilm.com/wp-content/...

Analizado en: 13/10/2023 18:46:45 (UTC)

Ambiente: Windows 7 de 32 bits (so...)

Puntuación de amenaza: 100/100

Indicadores: 0 1 11

Red:

SOSPECHOSO

https://vidofilm.com/wp-content/...

Analizado en: 14/10/2023 14:15:51 (UTC)

Ambiente: Windows 7 de 32 bits

Puntuación de amenaza: 100/100

Indicadores: 0 1 40

Red:



malicioso

Puntuación de amenaza: 100/100

Detección AV: 33%

#suplantación de identidad

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 legítima (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.