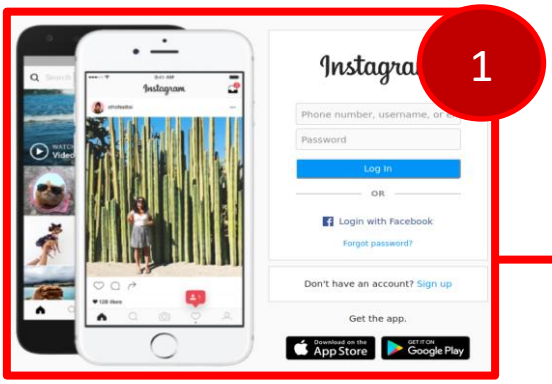
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 098	Fecha: 26-04-2023
		Página 11 de 13

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Suplantación de la identidad del sitio web 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 subfamilia	G02
Clasificación temática familia	Fraude		

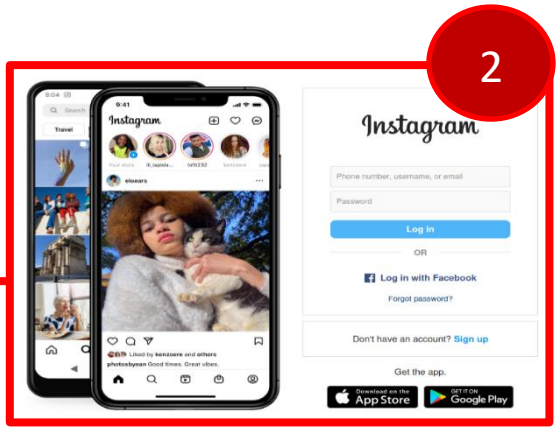
Descripción

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 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 del proceso de Phishing**.

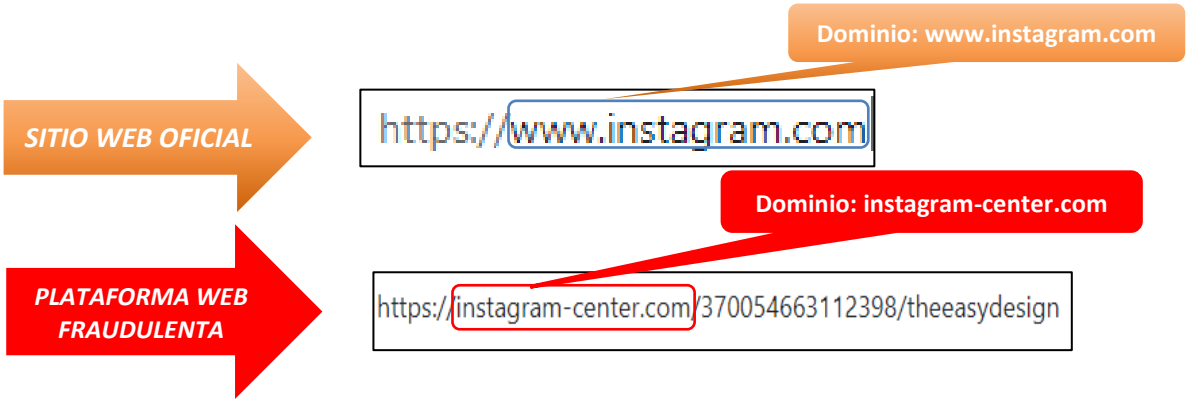


PASO 1: Solicitan a las víctimas, ingresar las credenciales de inicio de sesión (usuario y contraseña).



PASO 2: Al terminar el proceso del paso 1 con el proceso, redirige de manera automática al sitio web oficial, toda vez que los ciberdelincuentes ya se apoderaron de la información ingresada.

3. **Comparación del sitio web oficial y fraudulento**.



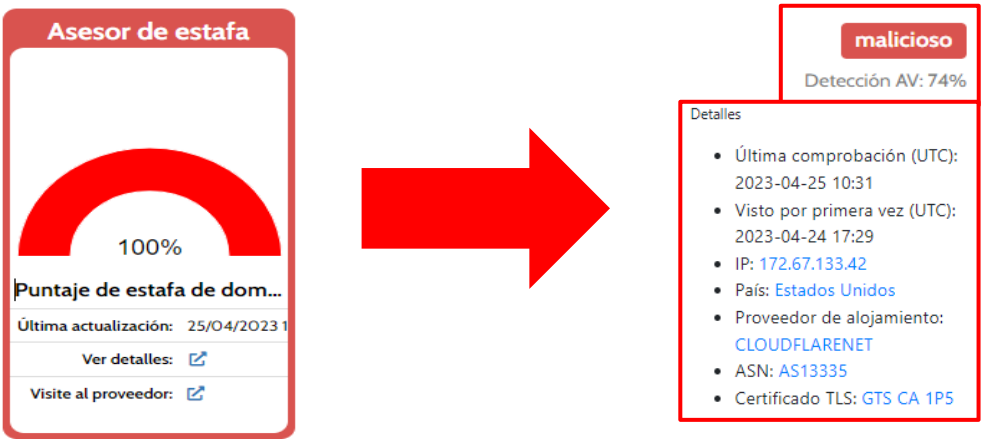
- ✓ Existe una diferencia debido a que el dominio de sitio web fraudulento no coincide con el oficial.
- ✓ Ambos sitios webs, poseen el *PROTOCOLO SEGURO DE TRANSFERENCIA DE HIPERTEXTO* (HTTPS), lo que hace más convincente a que las víctimas accedan a dicho sitio web.

4. Proveedores de seguridad informática alertan como SUPLANTACIÓN DE IDENTIDAD - PHISHING.

alphaMountain.ai	Suplantación de identidad	Anti-AVL	Malicioso
Avira	Suplantación de identidad	BitDefender	Malware
CRDF	Malicioso	CyRadar	Malicioso
ESET	Suplantación de identidad	Fortinet	Suplantación de identidad
G-datos	Malware	Navegación segura de Google	Suplantación de identidad
Seguridad Heimdal	Suplantación de identidad	kaspersky	Suplantación de identidad
Base de datos de phishing	Suplantación de identidad	Búsqueda segura	Malicioso
Sophos	Malware	VIPRE	Malicioso
raíz web	Malicioso	Navegación segura de Yandex	Suplantación de identidad

5. Indicadores de compromiso (IoC)

- ✓ URL : hxxps:// instagram-center[.]com/370054663112398/theeasydesign
- ✓ DOMINIO : instagram[.]xiple[.]in
- ✓ Prov. De alojamiento: Cloudflarenet
- ✓ IP : 172[.]67[.]133[.]42



6. Concepto de Instagram:

- Es una red social principalmente visual, donde un usuario puede publicar fotos y videos de corta duración, aplicarles efectos y también interactuar con las publicaciones de otras personas, a través de comentarios y me gusta.

7. Algunas *recomendaciones:*

- Ingresar desde fuentes oficiales VERIFICA.
- Verificar detalladamente las URL o enlace de los sitios web
- No seguir las instrucciones de sitio web sospechoso.
- Mantener el antivirus actualizado.
- No compartir los enlaces maliciosos con amigos y/o familiares.

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