	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°179	Fecha: 01-08-2023
		Página: 9 de 12

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Suplantación de la identidad web de la Red Social Facebook		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, mensajes de texto, 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 campaña de Phishing, a través de los diferentes navegadores web, quienes vienen suplantando la identidad de la Red Social Facebook; con el objetivo de acceder u obtener credenciales de inicio de sesión de las posibles víctimas.

2. DETALLES:

El proceso del Phishing es el siguiente:

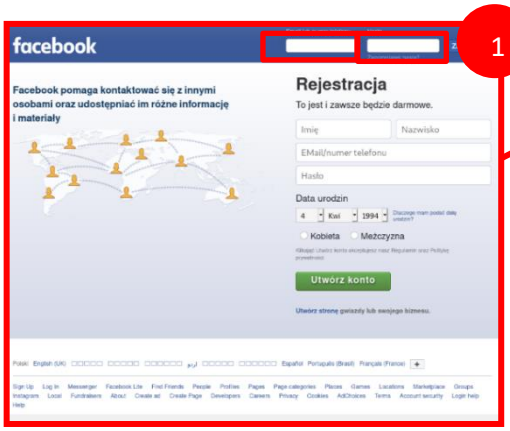


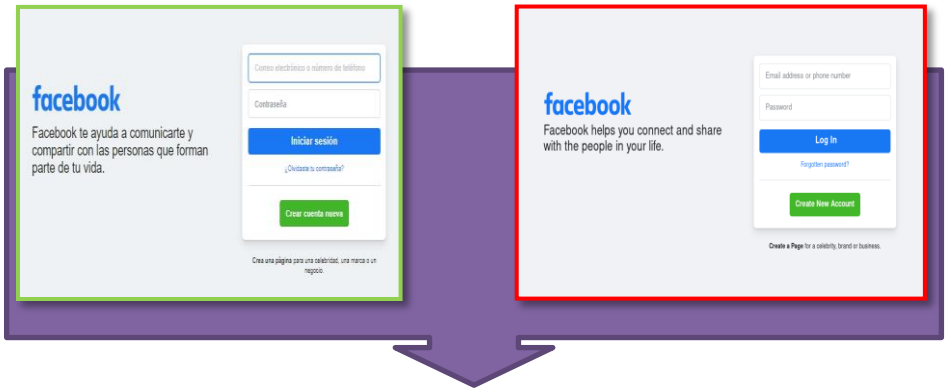
Figura 1.
Solicita a la víctima que ingrese a sus credenciales de acceso de inicio de sesión (correo electrónico o número de celular y la clave o contraseña) de su red social Facebook.

Figura 2.
Una vez registrado lo solicitado en la figura 1, redirige al sitio oficial de Facebook, aludiendo un aparente error de autenticación; sin embargo, los ciberdelincuentes obtuvieron información registrada por la víctima.

Los ciberdelincuentes buscan persuadir a sus víctimas, con la finalidad de que ingresen sus credenciales de acceso.

A. Comparación del sitio web oficial Facebook, con el fraudulento.

SITIO WEB OFICIAL	SITIO WEB FRAUDULENTO
https://www.facebook.com/	hxxp://www[.]facebooktgtisp0[.]indolegion[.]link/vhsfhqpdhdsih6/



- Existe una diferencia entre la URL original y la URL fraudulenta.
- La URL falsa utiliza protocolo HTTPS, no significa que la web sea segura.
- El dominio (indolegion[.]link) del sitio web fraudulento se encuentra reportado por proveedores de seguridad informática como **PHISHING**.
- 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 diez (10), MALICIOSOS en cinco (05), MALWARE en uno (01), SOSPECHOSO en uno (01) de ellas- – PHISHING:

C. Indicadores de compromiso (IoC)

- **URL:** hxxp://www[.]facebook-meta-id-615279.9087431.com/?content_id =Ge70Pfnd8ERE8Zo

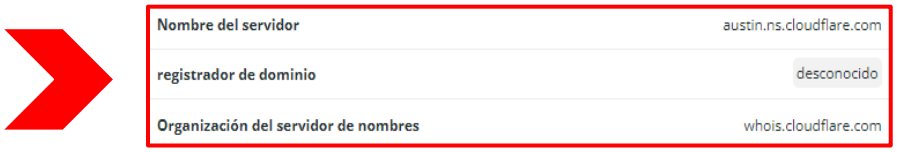
alphaMountain.ai	Suplantación de identidad	Avira	Suplantación de identidad
BitDefender	Suplantación de identidad	CRDF	Malicioso
CyRadar	Malicioso	Emsisoft	Suplantación de identidad
ESET	Suplantación de identidad	G-datos	Suplantación de identidad
Navegación segura de Google	Suplantación de identidad	Seguridad Heimdal	Suplantación de identidad
kaspersky	Suplantación de identidad	Leonico	Suplantación de identidad
netcraft	Malicioso	Búsqueda segura	Malicioso
Sophos	Malware	raíz web	Malicioso
Buscador de amenazas de Forcepoint	Sospechoso		

- **Dominio:** indolegion[.]link

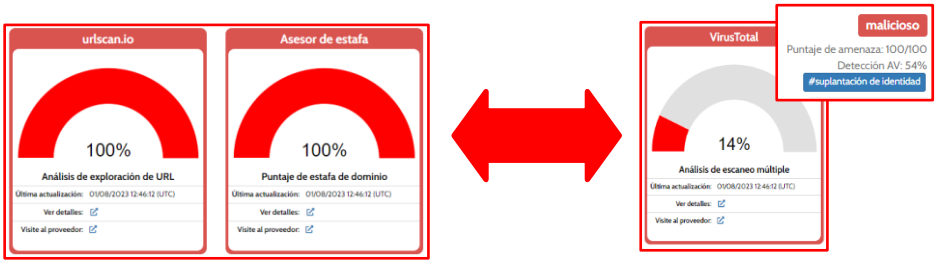
✖	Registro DMARC publicado
✖	Registro DNS publicado
!	Política DMARC no habilitada

- **Dirección IP:** 104[.]21[.]23[.]49

- **Proveedor de alojamiento:** austin.ns.cloudflare[.]com



D. Otras detecciones:



E. 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.)

F. 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