	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 107	**Fecha: 08-05-2023**
		Página 5 de 9

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Phishing, suplantando la identidad de la red social LinkedIn.		
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		

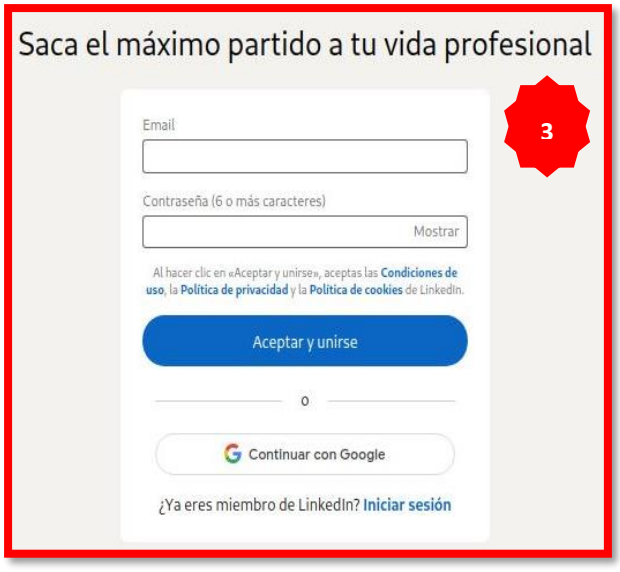
Descripción

1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que ciberdelincuentes vienen llevando a cabo una campaña de Phishing, suplantando la identidad de la red social LinkedIn (orientada para profesionales y empresas); la cual tiene como finalidad apoderarse de manera ilícita de las credenciales de acceso de inicio de sesión (dirección de correo electrónico, contraseña, número telefónico entre otros), de los usuarios.

2. Imagen: Detalles del proceso de estafa del Phishing.

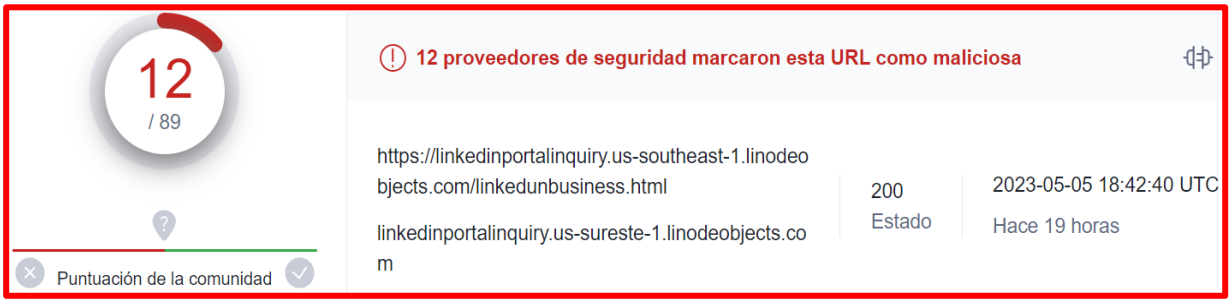
Sitio web falso de LinkedIn, solicita a la víctima ingresar sus credenciales de inicio de sesión (dirección de correo electrónico, contraseña y número telefónico).

Una vez ingresada las credenciales de acceso, y luego <iniciar sesión>, indica a la víctima que la pagina no ha sido encontrada y tiene que regresar para más información.



Por último, es redirigido al sitio web oficial de LinkedIn, aludiendo un aparente error de autenticación; sin embargo, los datos fueron capturado por los cibercriminales.

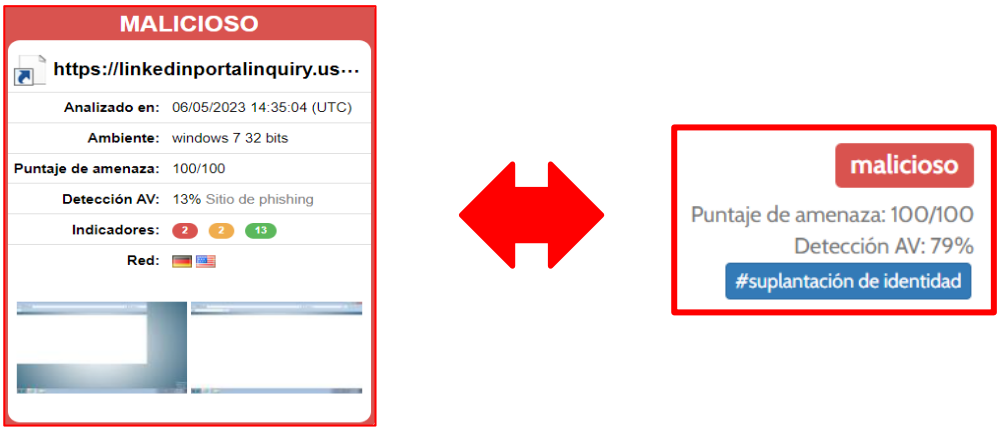
3. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogada como **Phishing (suplantación de identidad):**



- **Indicadores de compromiso** (IoC)

  - ✓ **URL Malicioso:** hxxps://linkedinportalinquiry[.]us-southeast-1[.]linodeobjects[.]com/linkedunbusiness[.]html
  - ✓ **Dominio:** linodeobjetos[.]com
  - ✓ **Dirección IP:** 139[.]177[.]204[.]133
  - ✓ **SHA-256:** 93d859df0db3105b41fab7b96fe22ad7d3e50d7b6f5fa9ea99ff0f4f8838492d
  - ✓ **Tipo:** Text/Html

- Otras detecciones del análisis:



4. **Apreciación de la información:**

- La presente campaña de Phishing permite a los actores de amenazas obtener las credenciales de acceso de la red social LinkedIn.

- 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, dicho enlace malicioso, es enviado a través de las plataformas digitales como el WhatsApp, Telegram, Messenger y mensajes de textos SMS.

5. **Algunas Recomendaciones:**

- Verificar detalladamente las URL de los sitios web.
- Evitar descargar archivos sospechosos.
- Rechazar las instrucciones de sitio web sospechoso.
- Mantener el antivirus actualizado.
- Denegar permisos de instalación de archivos desconocidos o dudosa procedencia.
- Realizar las actualizaciones correspondientes desde fuentes originales.

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