	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°251	Fecha: 22-10-2023
		Página: 5 de 8

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 Sub familia	G01
Clasificación temática familia	Fraude		

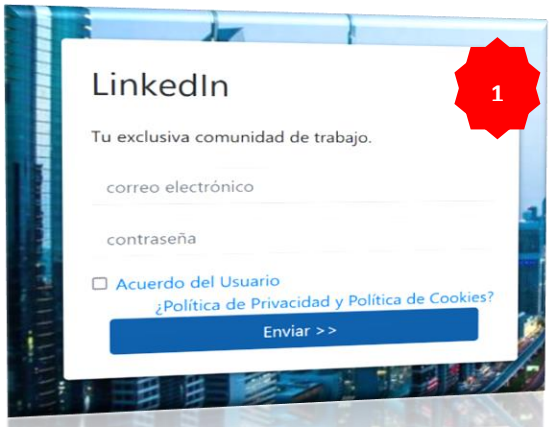
Descripción

1. **ANTECEDENTES:**

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.

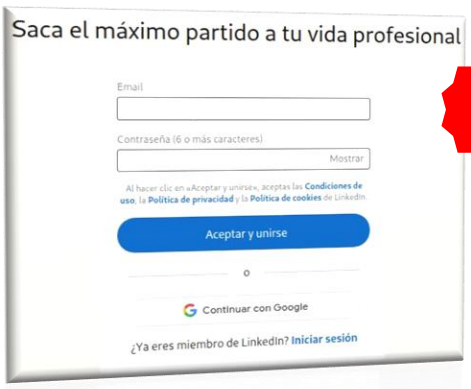
2. **DETALLES:**

Detalles del proceso de estafa del Phishing.



Sitio web falso de LinkedIn, solicita a la víctima ingresar sus credenciales para iniciar sesión de la comunidad de trabajo (dirección de correo electrónico y contraseña).

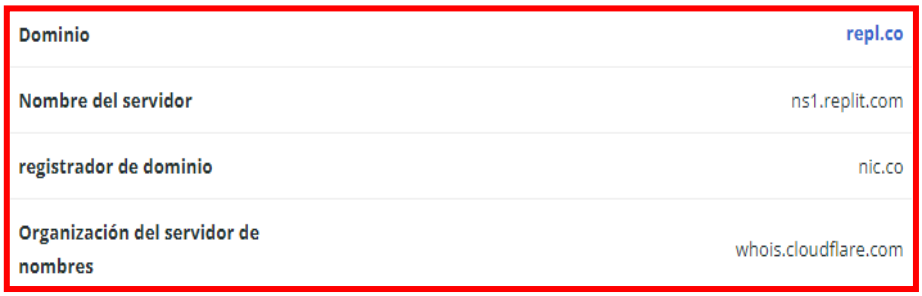
Una vez ingresada las credenciales de acceso y darle clic en <Enviar>, indica a la víctima que el nombre o contraseña son incorrecto y tiene que colocar nuevamente las credenciales.



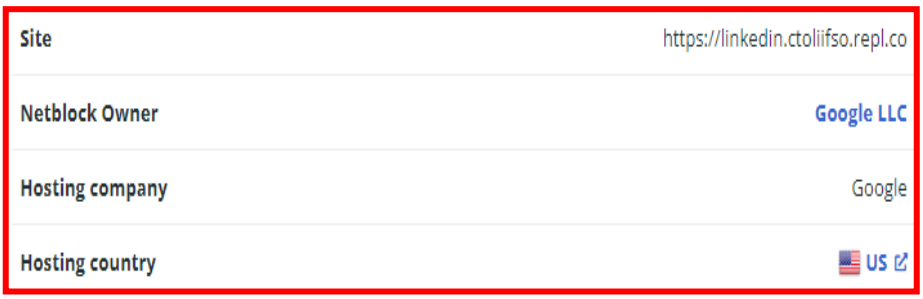
Por último, al colocar nuevamente las credenciales e intentar ingresar es redirigido al sitio web oficial de LinkedIn, aludiendo un aparente error de autenticación; sin embargo, los datos fueron capturado por los cibercriminales.

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

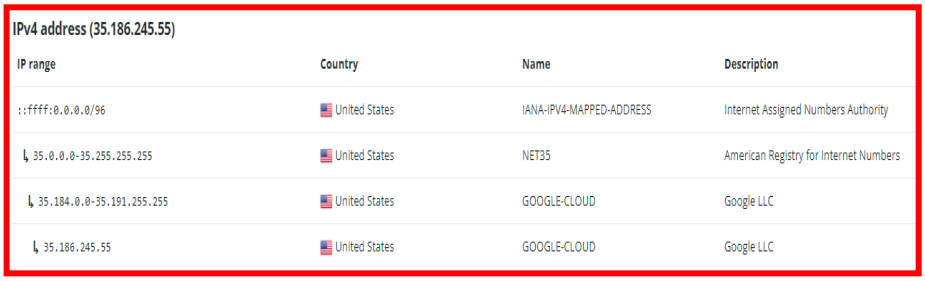
- **Indicadores de compromiso** (IoC)
  - **Dominio:** repl[.]co



  - **URL Malicioso:** hxxps://linkedin[.]ctoliifso[.]repl[.]co



  - **Dirección IP:** 35[.]186[.]245[.]55



  - **SHA-256:** f2d7708f98a8ea2376614f405f536a965820f2c696f73c913a0a413290a5cd4b
  - **Tipo:** Text/Html
  - **Server**: ns1.replit.com

- **Otras detenciones:**

B. 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.

3. 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.

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