| | ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°057 | Fecha: 05-03-2024 |
|---|---|---|
| | | Página: 13 de 18 |

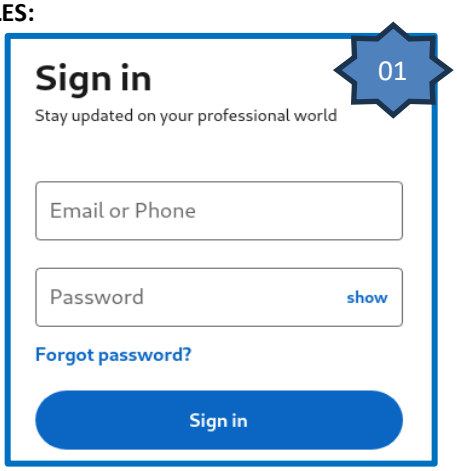
| | | | |
|---|---|---|---|
| Componente que reporta | **DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ** | | |
| Nombre de la alerta | Phishing, suplantando la identidad de la red social LinkedIn | | |
| Tipo de Ataque | Phishing | Abreviatura | Phishing |
| Medios de propagación | Redes sociales, SMS, correo electrónico, videos de internet, entre otros | | |
| Código de familia | G | Código de Sub familia | G01 |
| Clasificación temática familia | Fraude | | |

Descripción

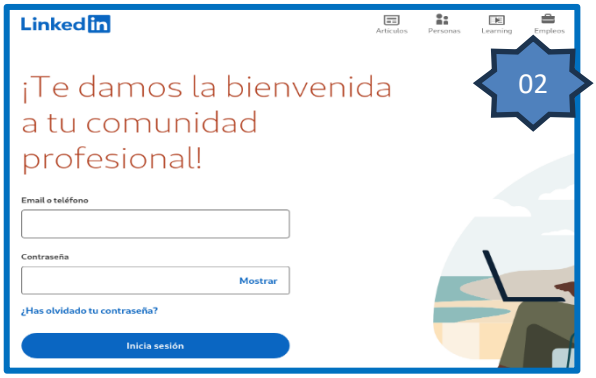
1. **ANTECEDENTES:**

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:**

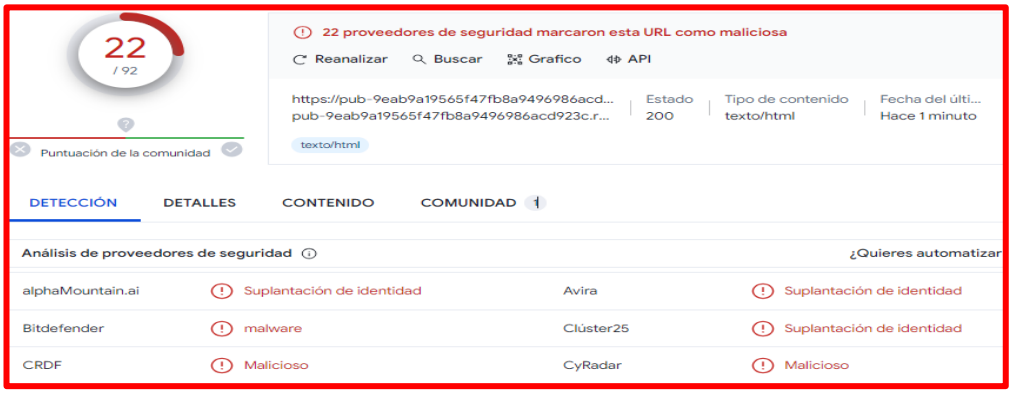



Sitio web falso de LinkedIn, solicita a la víctima ingresar sus credenciales para iniciar sesión de la comunidad de trabajo (dirección de correo electrónico o número de celular y contraseña).



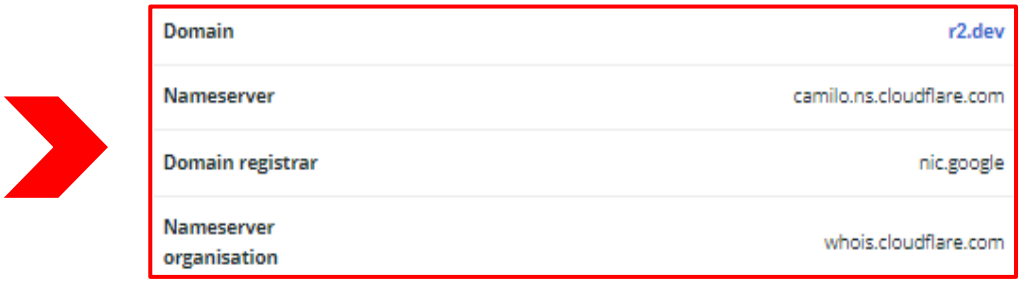

Por último, al intentar reiteradas veces las credenciales e intentar ingresar es redirigido al sitio web oficial de LinkedIn, aludiendo un aparente error de autenticación; sin embargo, los datos fueron capturado por los cibercriminales.

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



**B. Indicadores de compromiso** (IoC)

- **Dominio:** r2[.]dev




- **URL Malicioso:** hxxps[:]//pub-9eab9a19565f47fb8a9496986acd923c[.]r2[.]dev/indexmex[.]html


- **Dirección IP:** 104[.]18[.]3[.]35


- **SHA-256:**73f738e705de2585a4c3773857f71e2c7caa692b06d1448c0ccad1331d911f6c
- **Tipo:** Text/Html
- **Server**: cloudflare

**C. 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 |
|---|---|