| | | |
|---|---|---|
| | **ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 111** | **Fecha: 12-05-2023**<br>**Página 10 de 13** |

| | | | |
|---|---|---|---|
| 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, 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 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 del proceso de Phishing.

Sitio web fraudulento; donde los ciberdelincuentes buscan persuadir a sus víctimas, solicitando ingresar sus credenciales de acceso.

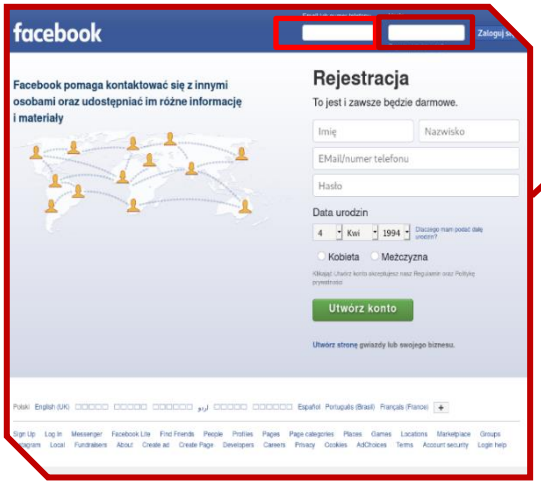



**Figura 1.** El sitio fraudulento que suplanta la identidad de Facebook, solicita al usuario que ingrese de las credenciales de acceso de inicio de sesión (correo electrónico o número de celular y la clave o contraseña).


**Figura 2.** Una vez que el sitio de Phishing ha logrado capturar la dirección del correo electrónico o número de celular como la contraseña. La víctima, es redirigido hacia el sitio oficial de Facebook, aludiendo un aparente error de autenticación.

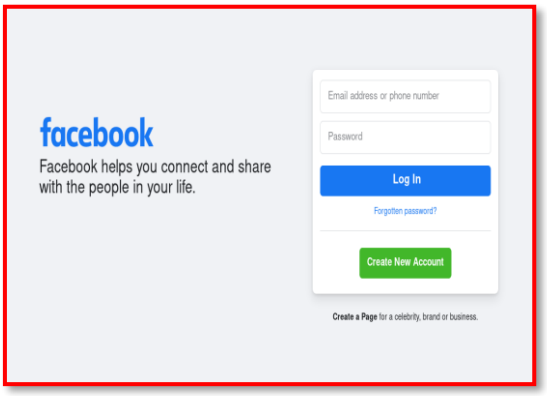
**3.** Comparación del sitio web oficial Outlook Web App, con el fraudulento.

**SITIO WEB OFICIAL**

URL: https://www.facebook.com


**SITIO WEB FRAUDULENTO**

http://facebook-clone-react.pages.dev

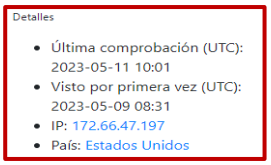



1) Existe una diferencia entre la URL original y la URL fraudulenta.
2) La URL falsa utiliza protocolo HTTPS, no significa que la web sea segura.
3) El dominio (facebook-clon-react.pages.dev) del sitio web fraudulento se encuentra reportado como **PHISHING**.
4) Existe una similitud entre ambas páginas, en imagen, fondo y colores de ambos sitios web.

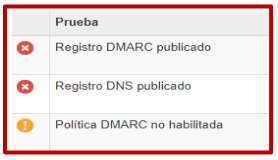
**4.** La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD** en ocho (08) de ellas- **– PHISHING:**

**a) INDICADORES DE COMPROMISO:**

✓ **URL Malicioso:** hxxp://www[.]facebook-clone-react[.]pages[.]dev

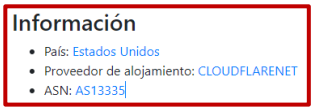



✓ **Dominio:** facebook-clon-react[.]pages[.]dev




✓ **Dirección IP:** 172[.]66[.]47[.]197

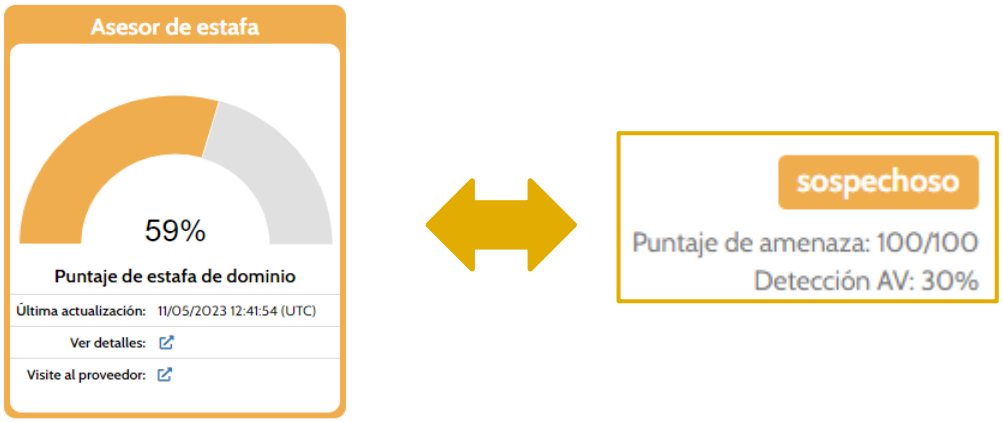

✓ **Proveedor de alojamiento:** CLOUDFLARENET




✓ **SHA-256:** 5761399a935b1bcf6a3dcfbdb763cc338c2a6269e00941612edf1d53993344a8

| | | | |
|---|---|---|---|
| CRDF | Malicioso | CyRadar | Malicioso |
| ESET | Suplantación de identidad | G-datos | Suplantación de identidad |
| Navegación segura de Google | Suplantación de identidad | Leonico | Suplantación de identidad |
| OpenPhish | Suplantación de identidad | Segasec | Suplantación de identidad |
| Sophos | Malware | Onda de confianza | Suplantación de identidad |

**b) OTRAS DETECCIONES:**




**5. 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.)

**6. 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.

**7. Concepto de Facebook:**

- Es una red social cuyo objetivo es conectar personas con personas: amigos, familiares, compañeros de trabajo o gente con aficiones comunes. Es una de las redes sociales con más usuarios, con cerca de 2.200 millones de personas registradas.

**8. Algunas 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.

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