| | ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 003 | Fecha: 03-01-2022 |
|---|---|---|
| | | Página: 3 de 5 |

| | | | | |
|---|---|---|---|---|
| Componente que reporta | **DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ** | | | |
| Nombre de la alerta | Nueva campaña de phishing que suplanta la identidad del Banco Interbank. | | | |
| 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 Financiero | | | |

Descripción

1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes vienen llevando a cabo una nueva campaña de phishing que se distribuye a través de navegadores webs, en donde suplantan la identidad de la Banca por Internet de Interbank, con el objetivo robar credenciales de acceso, datos personales y bancarios vinculado a la cuenta.

2. Proceso de ataque phishing:

**Imagen 01:** Sitio fraudulento que suplanta la identidad de la Banca por Internet de Interbank, insta al usuario, ingresar sus credenciales de acceso (número de tarjeta, DNI y clave web).

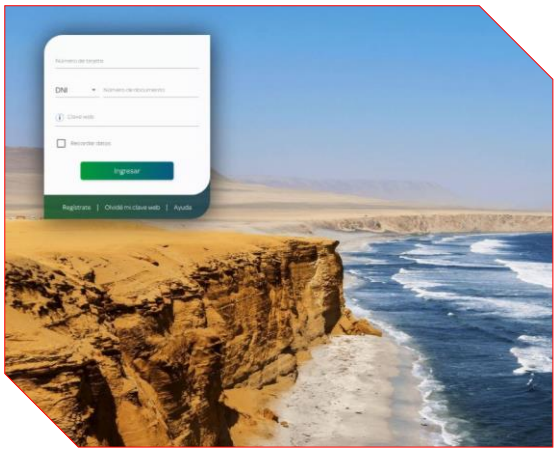


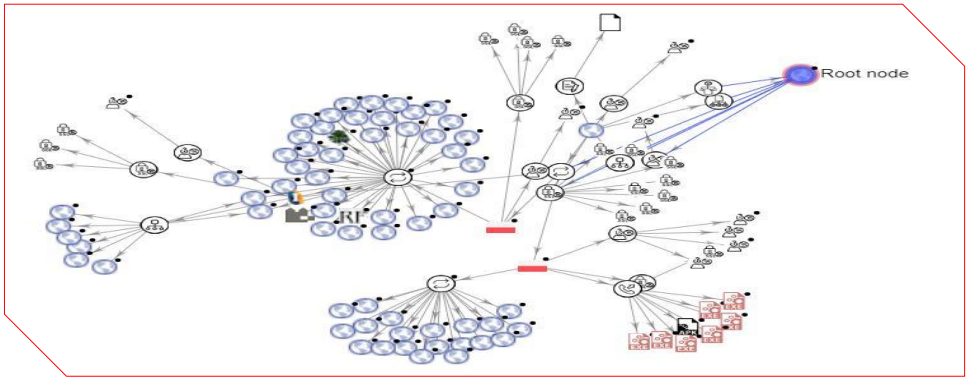

**Imagen 02:** Pasados unos segundos es redirigido al sitio web oficial del Banco Interbank, aludiendo un aparente error de autenticación, sin embargo, los datos fueron capturados por los ciberdelincuentes.


3. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, obteniendo como resultados que cinco (05) proveedores de seguridad informática alertan como: **PHISHING.**

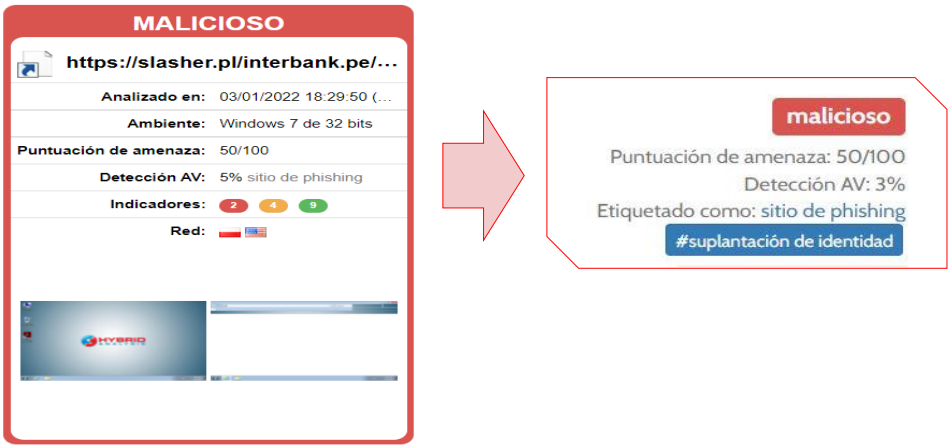
- Análisis de la URL: hXXps[:]//slasher[.]pl/interbank[.]pe/login


- Indicadores de compromiso:
  - URL Final: hXXps[:]//slasher[.]pl/interbank[.]pe/login
  - Dirección IP: 5[.]252[.]229[.}113
  - Código: 200
  - Longitud: 315,00 B
  - SHA-256: d5a89e26beae0bc03ad18a0b0d1d3d75f87c32047879d25da11970cb5c4662a3

- Tipología de Red:




4. Otros resultados:




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, entidad financiera, servicio técnico, etc.).

6. Referencia:
   - Phishing o suplantación de identidad: Es una técnica fraudulenta consiste en engañar al usuario solicitando información personal, contraseñas, datos bancarios etc., a través del correo electrónico o redirigiendo a la víctima a una copia falsa de una página web donde se le solicita el ingreso de los datos que se quieren obtener.

7. Recomendaciones:
   - No introducir datos confidenciales en sitios web sospechosas o de dudosa procedencia.
   - Prestar atención en los detalles de los mensajes o redes sociales.
   - Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas.
   - Visualizar los sitios web que se ingresen sean los oficiales.

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