	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 290	Fecha: 25-10-2022
		Página 08 de 10

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Phishing, suplantando la identidad de la entidad Bancaria 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		

Descripción

1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes vienen llevando a cabo una campaña de Phishing, por medio de los diferentes navegadores web, dirigido a los clientes y/o usuarios de la entidad bancaria Interbank; el cual, mediante la creación de un sitio web similar al original, requieren a las posibles víctimas a solicitar un supuesto crédito hipotecario en tres simples pasos y de manera online, esto con la finalidad de cumplir el sueño de tener una casa propia.

2. **Imagen**: Detalle del proceso del Phishing:

Piden requerir una solicitud de crédito hipotecario de la siguiente manera:
1. Establece un presupuesto.
2. Encuentra tu casa.
3. Solicita tu crédito.

Pide, realizar una solicitud de calificación de crédito

Por ultimo redirige de manera automática al sitio web oficial del banco interbank

3. Comparación del sitio web oficial y fraudulento.

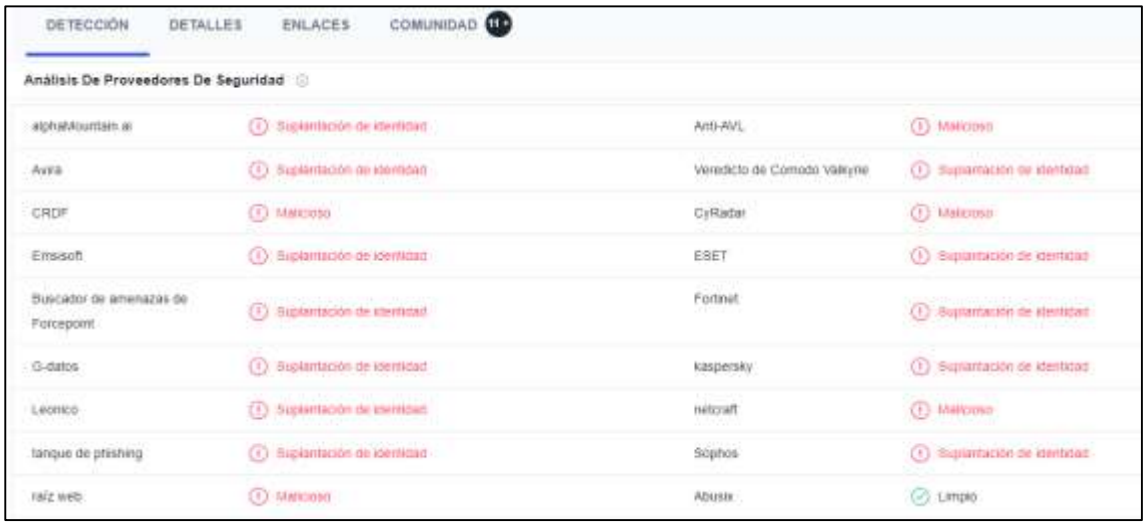
Sitio web oficial
https://micasapropia.interbank.pe

Sitio web fraudulento
hxxp://acgreu2c015hipouat01[.]eastus2.azurecontainer.io

- Existe una similitud entre el fondo y forma de cada sitio web.
- La URL fraudulento no utiliza el protocolo https.
- El dominio del sitio web fraudulento, no coincide con el oficial.

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

- Indicadores de compromiso:
  - URL: hxxp://acgreu2c015hipouat01[.]eastus2[.]azurecontainer[.]io
  - Dominio: azurecontainer[.]io
  - IP: 20[.]65[.]21[.]130
  - Tamaño: 17.43 KB
  - SHA-256: 416f197988bbbba621d3d5fd61b936c8c66d4be4b483c972b7054a7d2605de0b



5. Recomendaciones:

- Verificar la información en la entidad correspondiente
- Las entidades bancarias no solicitan realizar actualización de datos de manera online o virtual.
- No seguir las instrucciones de sitio web sospechoso.
- Mantener el antivirus actualizado.

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