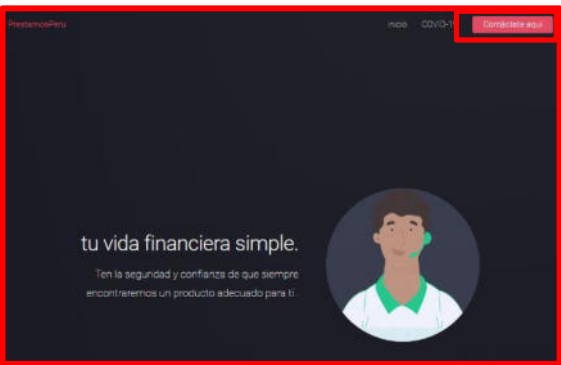
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 079		Fecha: 20-03-2022	
			Página 4 de 6	
Componente que reporta	DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ			
Nombre de Alerta	Phishing, suplantando la identidad del sitio web del banco Interbank			
Tipo de Ataque	Phishing	Abreviatura	Phishing	
Medio 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, a través de los diferentes navegadores web, quienes suplantando la identidad del sitio web del Banco Interbank (banca en línea), el cual simulan ser el sitio web online de la entidad bancaria, a fin de robar datos confidenciales de las posibles víctimas como número de tarjeta, número de documento nacional de identidad (DNI) y contraseña web.

- Detalles del proceso del Phishing.



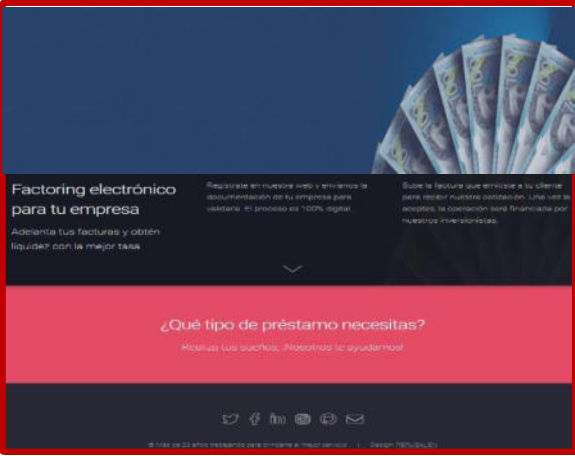
PASO N°01

Al hacer clic en <contactase>, es redirigido al sitio web falso que suplanta la identidad de banco Interbank, solicita a la víctima contactarse para poder adquirir préstamos.



PASO N°02

El sitio web falso de Interbank, Solicita a las víctimas ingresar sus credenciales de acceso (número de la tarjeta, DNI y clave web).



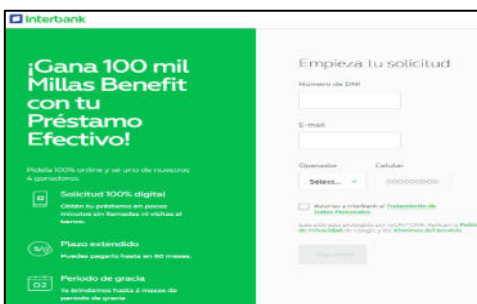
PASO N°03

Transcurrido unos 10 segundos, aparece en la pantalla información sobre “¿Qué tipo de préstamo necesitas?”, bloqueando el sitio web falso, aludiendo un aparente error del sistema, sin embargo; los datos fueron capturados por los ciberdelincuentes.

2. Comparación de inicio de sesión del sitio web oficial y falso de Interbank.

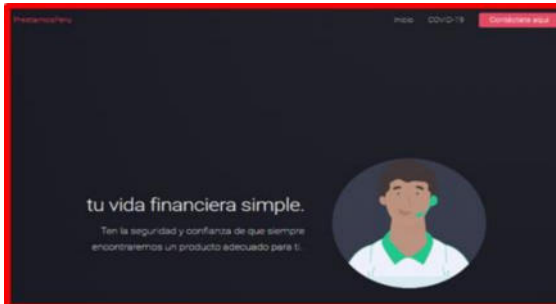
Sitio web oficial

URL: <https://interbank.pe/solicitar/prestamo/efectivo/inicio>



Sitio web fraudulento

URL: [https://plataforma-virtual-interbank\[.\]bambucha-mu\[.\]com/](https://plataforma-virtual-interbank[.]bambucha-mu[.]com/)



- ❖ Ambas URL,s poseen el protocolo de seguridad de red (https).
- ❖ Existen diferencias entre la URL original y la URL fraudulenta.
- ❖ Diferencia entre el fondo de color y forma.

3. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, obteniendo la siguiente información:

- URL Malicioso: [https://plataforma-virtual-interbank\[.\]bambucha-mu\[.\]com/](https://plataforma-virtual-interbank[.]bambucha-mu[.]com/)
- Dominio: [plataforma-virtual-interbank\[.\]bambucha-mu\[.\]com](https://plataforma-virtual-interbank[.]bambucha-mu[.]com/)
- IP: 172.67.202.160
- Tamaño: 8.30 KB
- SHA-256: 7c2eace38234a72d920efcd0e16528029b7e1926245bb4c23bd44a248b6e36b4

DETECTION	DETAILS	COMMUNITY
Avira	Phishing	BitDefender
CRDF	Malicious	CyRadar
Emisoft	Phishing	ESET
Fortinet	Phishing	G-Data
Kaspersky	Phishing	Lionic
Netskraft	Malicious	Phishtank
Sophos	Phishing	Webroot

• Otras detecciones:

MALICIOSO

https://plataforma-virtual-inter...


Analizado en: 20/03/2022 16:32:06 (UTC)

Ambiente: windows 7 32 bits

Puntaje de amenaza: 82/100

Detección AV: 15% Sitio de phishing

Indicadores: 2 5 10

La red: 

➔

malicioso

Puntaje de amenaza: 82/100

Detección AV: 8%

Etiquetado como: sitio de phishing

#suplantación de identidad

4. Algunas Recomendaciones:

- Verificar la información en la entidad bancaria.
- Acceder al sitio web a través de sus fuentes oficiales.
- No abrir enlaces de dudosa procedencia.
- No seguir indicaciones de sitios web fraudulentos.
- No brindar información personal a sitios web sospechosos.
- Mantener instalado un servicio de antivirus en el dispositivo.