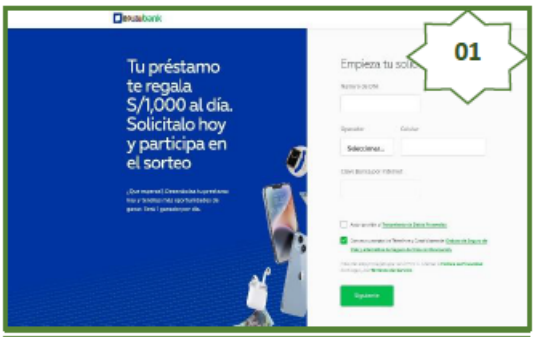
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 125	**Fecha: 29-05-2023**
		Página 6 de 10

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Detección de sitio web fraudulento 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		

Descripción

1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que actores de amenazas vienen llevando a cabo una campaña de Phishing, suplantando el sitio web de solicitud de préstamos del Banco Interbank, con la finalidad de robar información sensible de los usuarios de la entidad financiera como números de documento de identidad, tarjetas bancarias, contraseñas, etc.

2. Imagen: Detalle del proceso del Phishing:

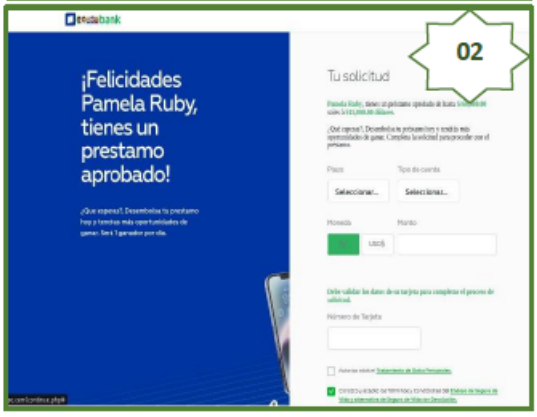


Paso Nº01

Solicitan a la víctima registrar lo siguiente:

- Número del Documento Nacional de Identidad.
- Operador telefónico
- Número de Celular
- Clave intranet de seis dígitos.

Para luego dar clic en <Siguiente>



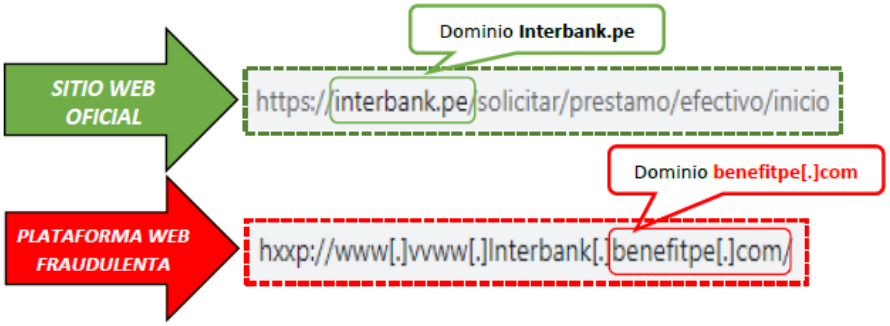
Paso Nº02

Aparece una pantalla requiriendo a la víctima que registre lo siguiente:

- El plazo y tipo de cuenta.
- El monto del préstamo solicitado
- Número de la tarjeta bancaria con la fecha de vencimiento y código de seguridad (CVV).

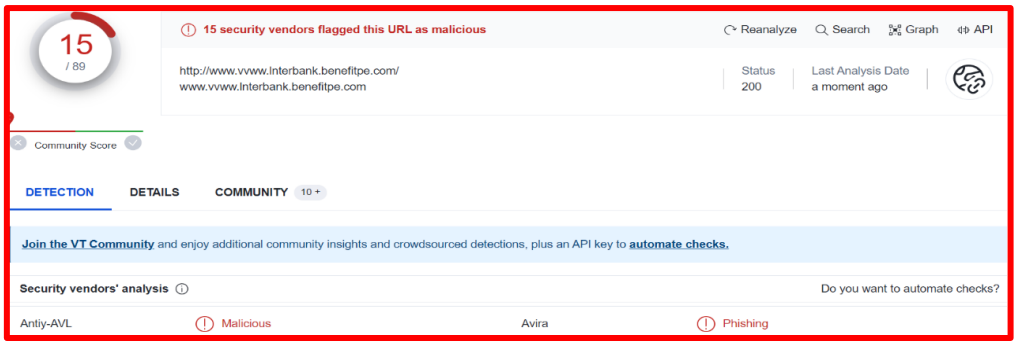
Para luego dar clic en <Siguiente>. Pero, pasado unos segundos, redirige al sitio web oficial de la entidad bancaria; sin embargo, los ciberdelincuentes obtuvieron los datos proporcionados por la víctima.

3. Comparación del sitio web oficial y fraudulento.



- Existe diferencias en las URL del sitio web oficial y fraudulenta.

4. Proveedores de seguridad informática alertan como **SUPLANTACIÓN DE IDENTIDAD - PHISHING.**



5. **INDICADORES DE COMPROMISO (IoC)**

- **Dominio :** benefitpe[.]com
- **IP :** 192[.]254[.]233[.]182
- **SHA-256 :** 969c37017f47c4ceeb911e431f8f99d9f20b48baa6789213926337d9ea593db2

6. **Otras detenciones:**

7. **Apreciación de la información:**

- La presente campaña de Phishing permite a los actores de amenazas obtener información financiera de los usuarios del Banco Interbank.

- 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.

8. **Algunas Recomendaciones:**

- Verificar detalladamente las URL de los sitios web
- No abrir o descargar archivos sospechosos.
- No seguir las instrucciones de sitio web sospechoso.
- Mantener el antivirus actualizado.
- Comunicar a la entidad financiera si ha realizado un registro de acceso en un sitio web sospechoso.

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

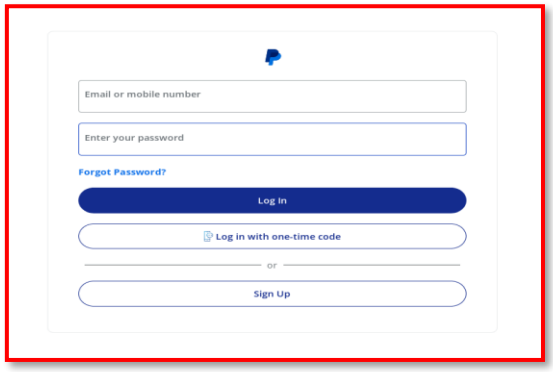
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 125	Fecha: 29-05-2023
		Página 8 de 10

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Suplantación de identidad a la empresa de pagos en línea PayPal		
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, a través de los diferentes navegadores web, quienes vienen suplantando la identidad de la empresa de pagos en línea "PayPal", el supuesto sitio web cuenta con colores y logos característicos idénticos al sitio web oficial, el cual tiene como finalidad robar información confidencial de las posibles víctimas, como dirección de correo electrónico, contraseña, datos bancarios (nombre, número, fecha de expiración de la tarjeta).

2. **Imagen: detalles del proceso de Phishing**.

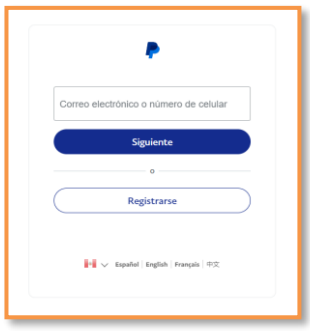


Sitio web fraudulento, donde solicita a las posibles víctimas ingresar sus credenciales de acceso (E-mail y contraseña).

3. **Diferencias del sitio web legítimo de PayPal y sitio web Fraudulento:**

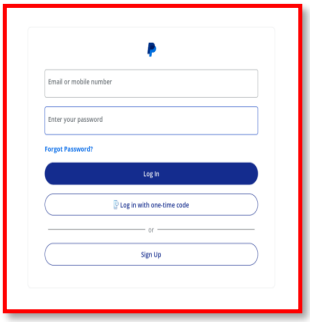
SITIO WEB OFICIAL

URL: https://www.paypal.com/pe/signin



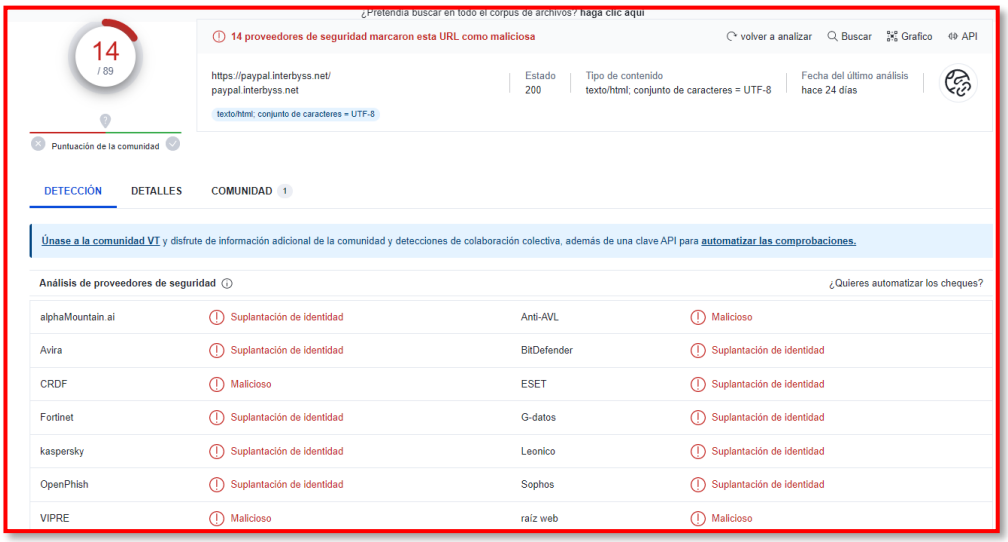
SITIO WEB FRAUDULENTO

URL: hxxps[:]//paypal[.]interbyss[.]net/



- Existe similitud entre ambas páginas, en imagen, fondo y escritura la diferencia se encuentra en la URL.
- La URL falsa utiliza protocolo HTTPS, no significa que la web sea segura.
- El dominio (paypal[.]interbyss[.]net) del sitio web fraudulento se encuentra reportado como **PHISHING.**
- La URL falsa está mal escrita y los caracteres ambiguos.

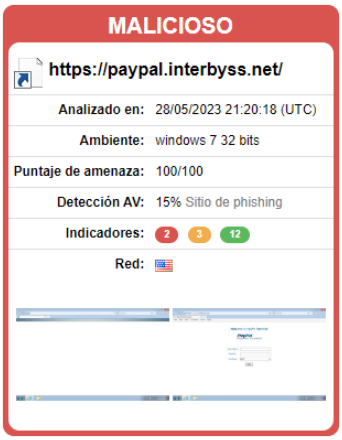
4. La URL sospechosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, obteniendo como resultado que CATORCE (14) proveedores de seguridad informática alertan como ***SUPLANTACIÓN DE IDENTIDAD - PHISHING.***



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

- ✓ **URL** : hxxps[:]//paypal[.]interbyss[.]net/
- ✓ **DOMINIO** : paypal[.]interbyss[.]net
- ✓ **SHA-256** : 36c3564615979dfa76d5c02c965fb7ae88e0d31bd20e2c83c0107d89e1134881
- ✓ **IP** : 50[.]31[.]174[.]199
- ✓ **Tamaño** : 2.44 KB

6. ***Otras detecciones:***



7. ***Algunas recomendaciones:***

- Verificar detalladamente las URL de los sitios web
- No abrir o descargar archivos sospechosos.
- No seguir las instrucciones de sitio web sospechoso.
- Mantener el antivirus actualizado.
- Contar con una solución de seguridad, constantemente actualizada tanto en dispositivos de escritorio como en móviles, ya que sirven como barrera inicial protectora ante sitios web maliciosos.

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