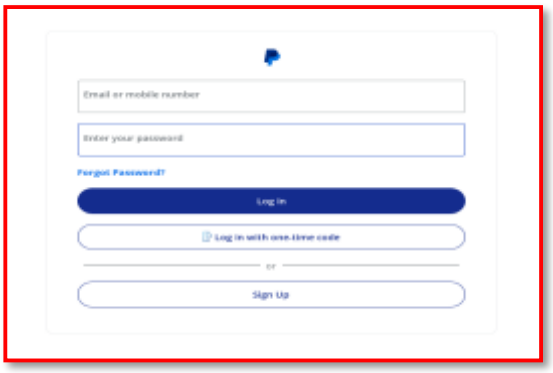
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 141	Fecha: 16-06-2023
		Página 8 de 11

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Nueva campaña de phishing que suplanta la identidad de 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 Sub familia	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. Proceso de estafa 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 y sitio web Fraudulento de PayPal:

SITIO WEB OFICIAL

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

SITIO WEB FRAUDULENTO

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

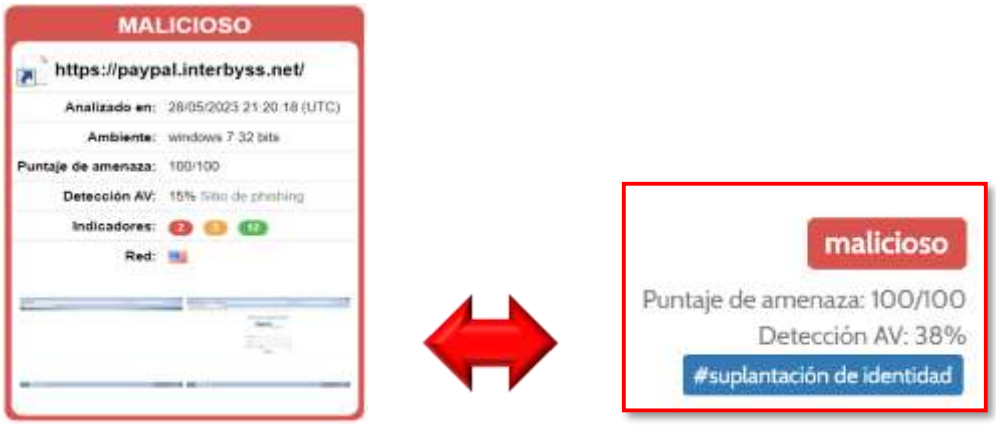
- Existe diferencia entre los dominios del sitio web oficial y fraudulento.
- Ambos sitios web poseen el PROTOCOLO SEGURO DE TRANSFERENCIA DE HIPERTEXTO (HTTPS), lo cual hace más convincente a la que las víctimas ingresen a dicho sitio web.

4. La URL sospechosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, obteniendo como resultado que 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. Como funciona del 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.)

8. 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.

9. Algunas recomendaciones:

- Evitar hacer clic en enlaces sospechosos que no sea sitio oficial de PayPal.
- Verificar detalladamente la URL, que corresponda al sitio web oficial.
- Evitar seguir las instrucciones de sitio web sospechoso o de dudosa procedencia.
- Mantener el antivirus actualizado, ya que es la primera barrera ante posibles ataques cibernéticos.
- Evitar compartir la URL con amigos y/o familiares.

Fuentes de información	Análisis propio de redes sociales y fuente abierta