	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 092	Fecha: 19-04-2023
		Página 12 de 14

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Nueva campaña de Phishing suplanta 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. Como parte de la simulación se obtuvo la siguiente información:

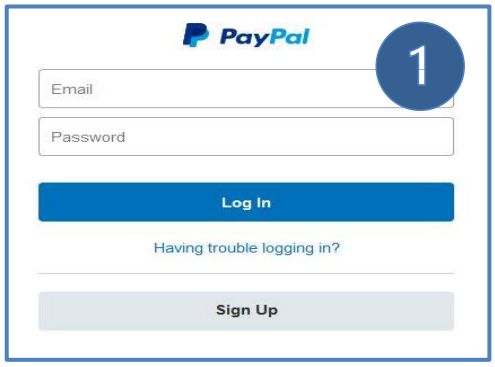
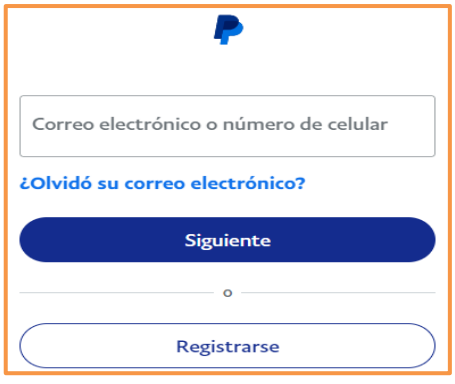


Imagen 1: Sitio web falso usado por los ciberdelincuentes solicita a la víctima, ingresar sus credenciales de acceso tales como (dirección de correo electrónico y contraseña).

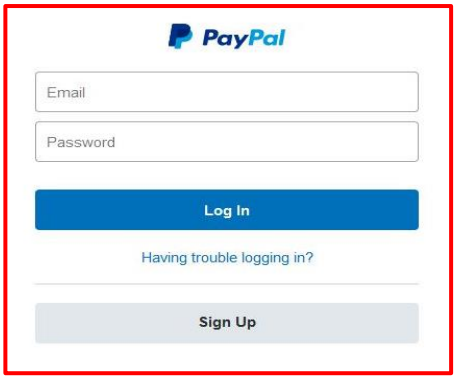
Imagen 2: Una vez ingresado las credenciales de acceso, es redirigido al centro de ayuda del sitio web legítimo de PayPal, aludiendo un aparente error; sin embargo, los datos fueron capturados.

3. Diferencias del sitio web legítimo de Twitter y sitio web Fraudulento:

SITIO WEB LEGÍTIMO
URL: https://twitter.com/



SITIO WEB FRAUDULENTO
URL: hxxps://protection[.]paypal[.]navigoperu[.]com/login[.]html



DIFERENCIAS

- **Existe una diferencia debido a que el URL y el dominio de sitio web fraudulento no coincide con el oficial.**
- **Ambos sitios webs, presentan diferencias en la tipografía y el color de diseño del sitio web.**

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

   - **URL:** hxxps://protection[.]paypal[.]navigoperu[.]com/login[.]html
   - **Dominio:** navigoperu.com
   - **Direcciones IP:** 108[.]167[.]172[.]163
   - **Tamaño:** 17.71 KB
   - **SHA-256:** 479da2cebc1ff38139d901928e26d22fa6a8b3ce35b888b45e0c84f0a839b109.

Avira	Suplantación de identidad	Emsisoft	Suplantación de identidad
Fortinet	Suplantación de identidad	kaspersky	Suplantación de identidad
netcraft	Malicioso	raíz web	Malicioso

5. **Otras detecciones**:

6. **Apreciación de la información:**

   - La presente campaña de Phishing, permite a los actores de amenazas obtener información bancaria de los usuarios de la empresa de pagos en línea PayPal.

   - La propagación del sitio web fraudulento se realiza mediante envió masivos de email (SPAM), con la finalidad de obtener información sensible de las víctimas; asimismo, a través de las aplicaciones de mensajería instantánea entre ellos WhatsApp, Telegram, Messenger y mensajes de textos (SMS).

7. **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