	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 134	Fecha: 08-06-2023
		Página 19 de 21

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 subfamilia	G01
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 ataques de suplantación de identidad (phishing), dirigidos a usuarios de la plataforma de pago por internet "PayPal", con el objetivo robar credenciales de acceso, datos personales y bancarios.

2. Proceso de estafa de Phishing:

Imagen 1.- Solicitud para ingresar las credenciales (dirección de correo electrónico y contraseña)

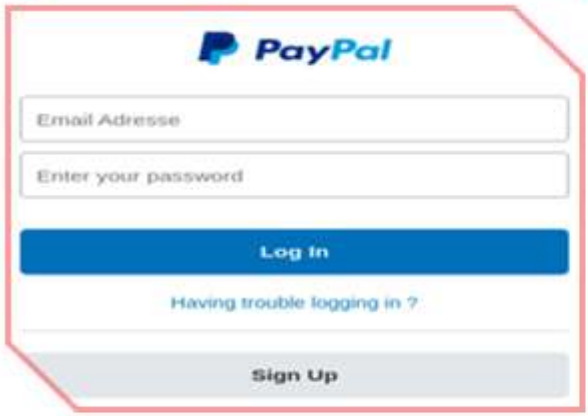

Imagen: 2.- Luego de haber ingresado las credenciales, requiere actualizar los datos personales.

Imagen: 3.- Por último, solicita confirmar los datos de la tarjeta de crédito o débito.

Imagen: 4.- Pasado unos 10 segundos, es redirigido al sitio oficial de PayPal, aludiendo un aparente error de autenticación, sin embargo, los datos fueron capturados, por los ciberdelincuentes.

3. Comparación del sitio web oficial y sitio web fraudulento de PayPal:

- 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. Proveedores de seguridad informática alertan como SUPLANTACIÓN DE IDENTIDAD – PHISHING:

- Indicadores de compromiso:

  - URL: hXXps[:]//paypaal[.]webflow[.]io/
  - Dominio: paypaal[.]webflow[.]io
  - SHA-256: 7bc874316f3060c246624e0280c66d887cc99b2320c4bf536f5530cd35836100
  - Dirección IP: 151[.]101[.]2[.]188
  - Tamaño: 4.36 KB

- Otros resultados del análisis:

5. 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.

6. 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