	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 106	Fecha: 06-05-2023
		Página 18 de 20

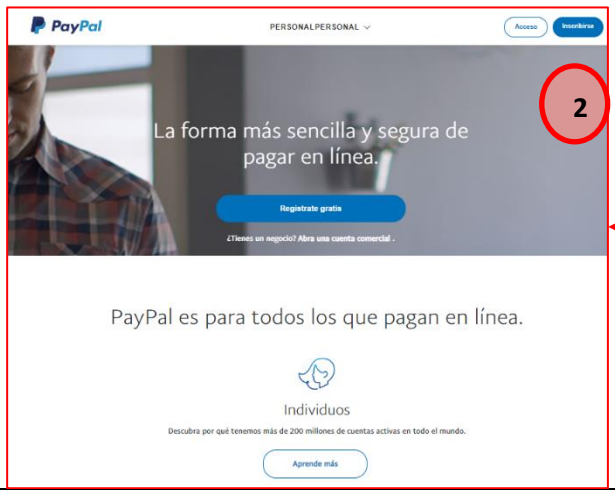
Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Campaña de Phishing suplantando la identidad del servicio de pagos en línea PayPal		
Tipo de ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos 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, por medio de los diferentes navegadores web, dirigido a los clientes y/o usuarios del servicio de pagos en línea PayPal (servicio que permite pagar, enviar dinero y aceptar pagos sin tener que introducir datos financieros continuamente); el cual, mediante la creación de un sitio web similar al original, solicitan a las posibles víctimas a realizar supuestas actualizaciones de información de su tarjeta bancaria.

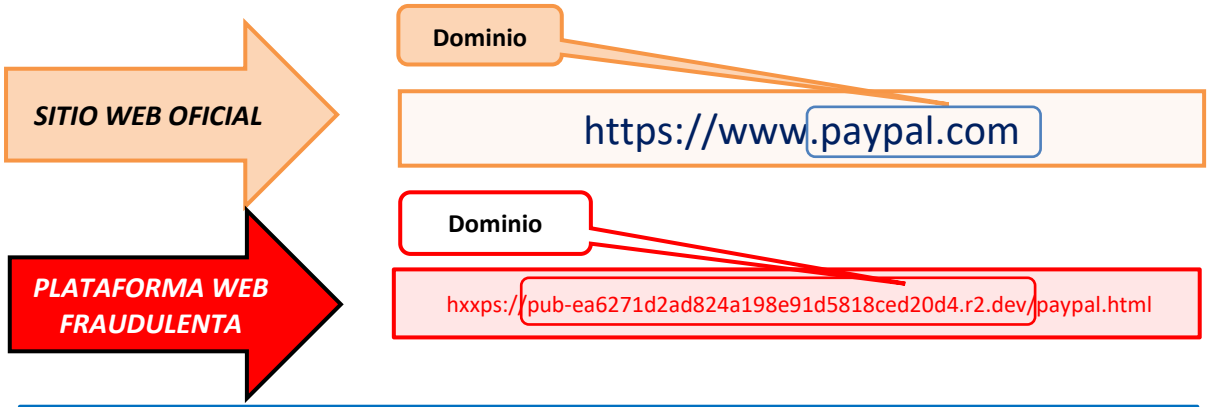
2. Detalles del proceso de Phishing:

Los ciberdelincuentes piden a las víctimas a realizar una supuesta actualización de información de la tarjeta de crédito, ingresando datos bancarios como número de tarjeta, fecha de vencimiento, código de seguridad, titular de la tarjeta, dirección de domicilio, número de teléfono y dirección de correo electrónico.



Una vez ingresado la información solicitada, el sitio web fraudulento redirige de forma automática al sitio web oficial de PayPal; tova vez que los actores de la amenaza ya se apoderaron de los datos requeridos.

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



- Existe una similitud entre el fondo y forma de cada sitio web (oficial y fraudulento).
- Ambos sitios webs poseen el ***PROTOCOLO SEGURO DE TRANSFERENCIA DE HIPERTEXTO (HTTPS)***, lo que hace mas convincente a que las víctimas ingresen a sitio web fraudulento

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

Avira	Phishing	CRDF	Malicious
Emsisoft	Phishing	Netcraft	Malicious
OpenPhish	Phishing	Abusix	Clean

- Indicadores de compromiso:
  - URL: hxxps[:]//pub-ea6271d2ad824a198e91d5818ced20d4[.]r2[.]dev/paypal[.]html
  - Dominio: pub-ea6271d2ad824a198e91d5818ced20d4[.]r2[.]dev
  - SHA-256: 81a5da4538e78adaec494715fe55a1e3ec7260e67de1581c0803d800049b254a
  - Dirección IP: 104[.]18[.]3[.]35
  - Tamaño: 124.56 KB

5. Recomendaciones:

- Verificar la información en la entidad correspondiente.
- No brindar información personal a sitios web sospechosos
- No hacer Click en enlace adjuntados a correos electrónicos o SMS.
- Ingresar al sitio web desde fuentes oficiales.
- Mantener el antivirus actualizado.

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