	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°013	Fecha: 15-01-2024
		Página: 10 de 13

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 Sub familia	G01
Clasificación temática familia	Fraude		

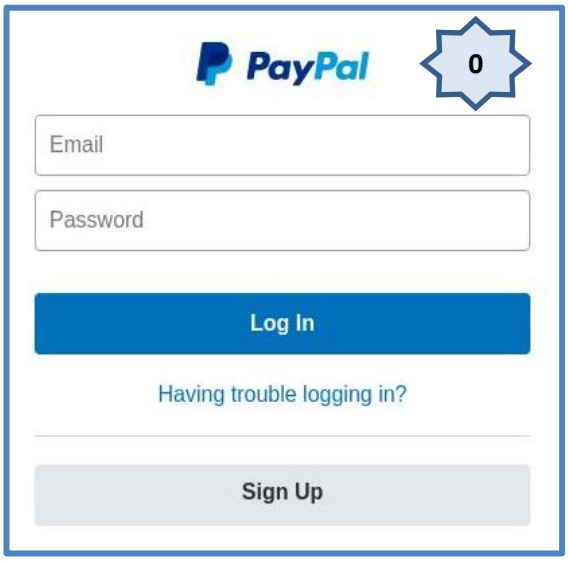
Descripción

1. **ANTECEDENTES:**

   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. **DETALLES:**

   Detalles del proceso de Phishing.



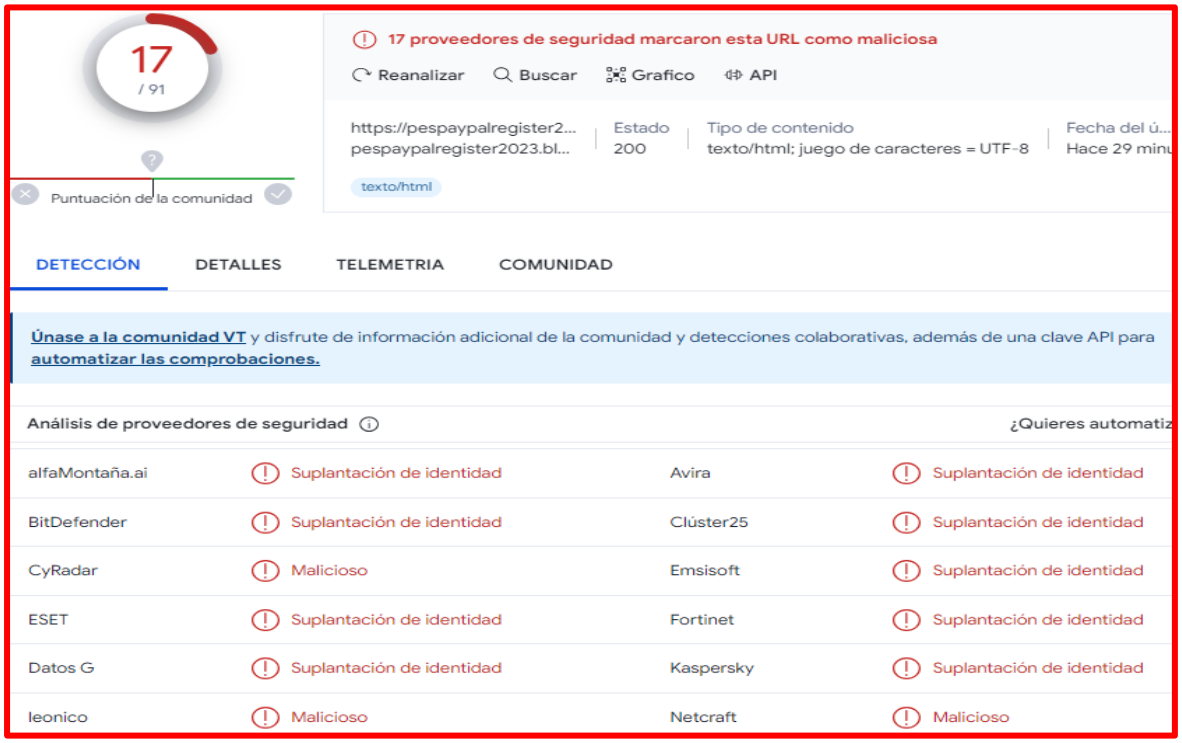
Paso N.º 01

Sitio web falso que suplanta la identidad de PayPal, solicita a la víctima registrar las credenciales de acceso (correo electrónico y la contraseña) para iniciar sesión.

Paso N.º 02

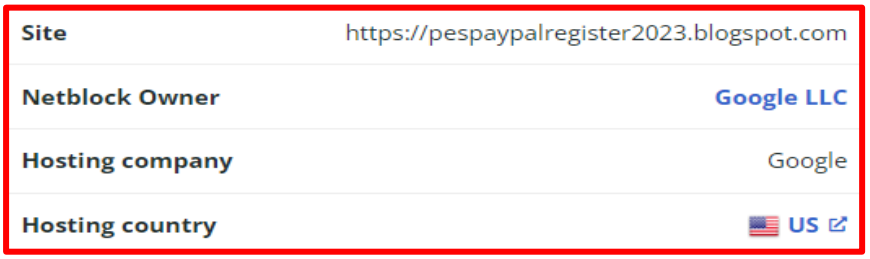
Al darle clic en <iniciar sesión>, le informa que "**Desafortunadamente, el servicio esta temporalmente inactivo debido a la gran cantidad de solicitudes en el sitio**"; sin embargo, luego de ingresar las credenciales de acceso los datos fueron capturados por los atacantes.

A. La URL sospechosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, obteniendo como resultado que DIECISIETE (17) proveedores de seguridad informática alertan como ***SUPLANTACIÓN DE IDENTIDAD - PHISHING.***

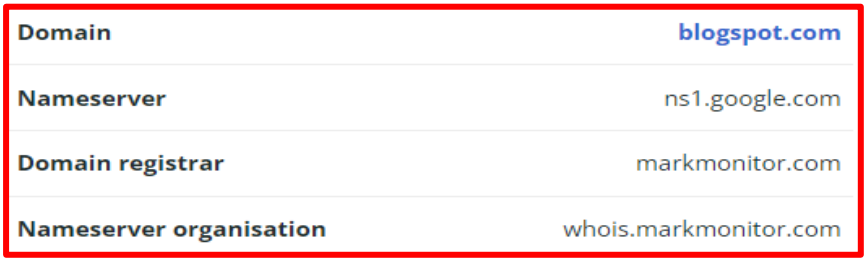


B. Indicadores de compromiso (IoC)

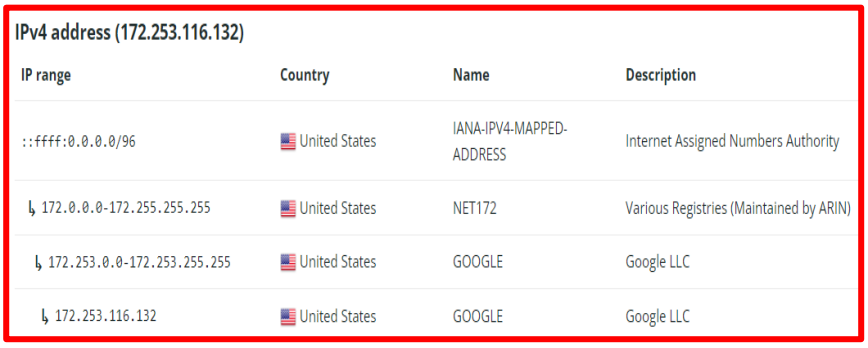
✓ **URL** : hxxps://pespaypalregister2023[.]blogspot[.]com/?m=1



✓ **DOMINIO** : blogspot[.]com

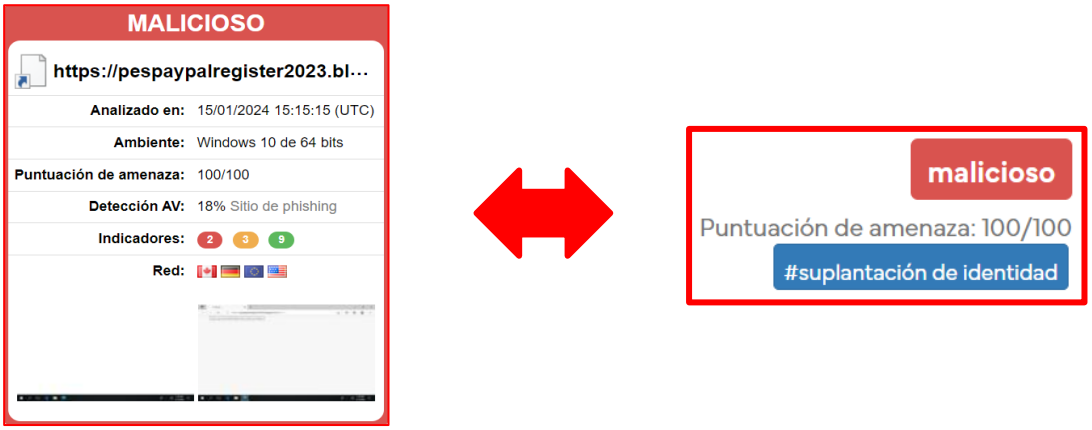


✓ **IP** : 108[.]177[.]111[.]132



- ✓ **SHA-256** : 92cdb28bba83f1495c83c75611db63ba9edd8c90c0d71fce4c8ee803cda6e6cd
- ✓ **Tamaño** : 32.08 KB
- ✓ **Servidor** : GSE

C. *Otras detecciones:*



D. 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).

3. 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.

Fuente de Información:	Análisis propio de redes sociales y fuente abierta.