Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Suplantación de identidad de la empresa Petroperú en Campaña de Inversiones		
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		

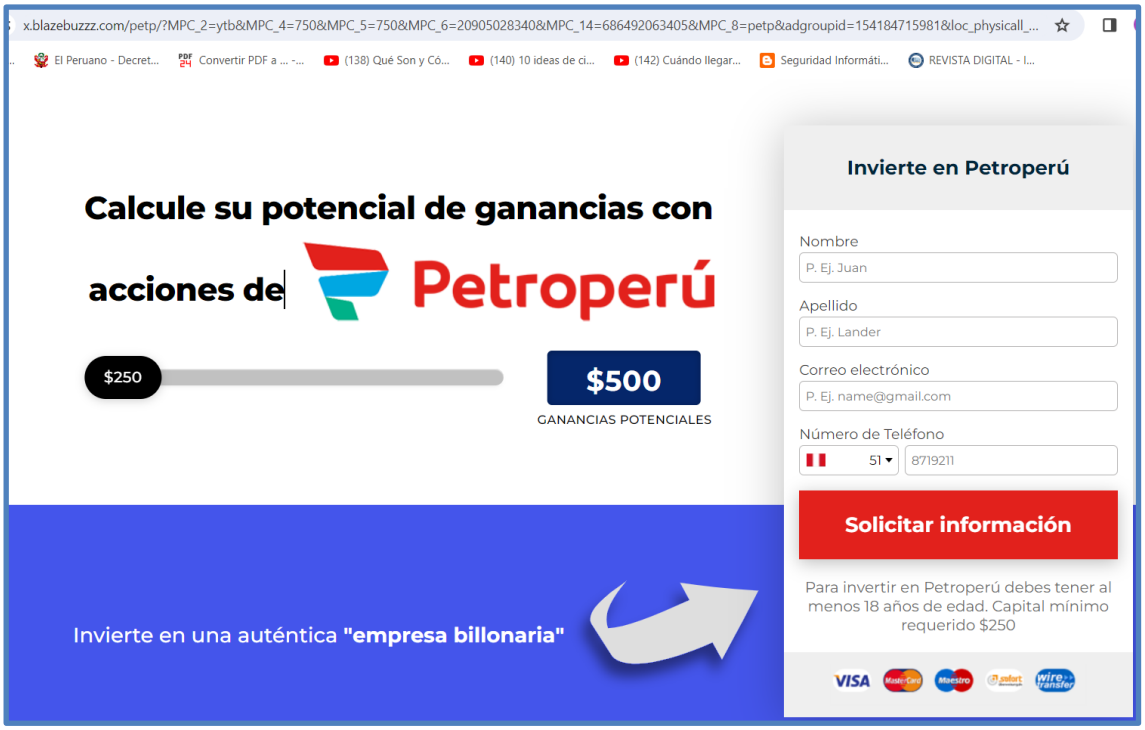
Descripción

1. **ANTECEDENTES**:

Anteriormente, desde mayo 2022, Petroperú ha publicado en su portal oficial que ha sido víctima de suplantación de identidad y que no ofrece productos financieros ni premios monetarios ni ganancias millonarias en base a la inversión de capital. Más bien alerta a la población a no ingresar a los enlaces enviados por WhatsApp o cualquier otra red social, en las que se solicite información personal, pues el objetivo sería estafarlos y/o robarles dicha información, ya sea para vender sus credenciales o para un perjuicio más directo en sus cuentas.

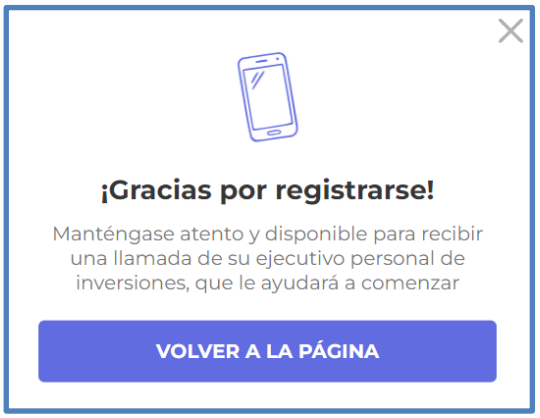
2. **DETALLES:**

A través del monitoreo de amenazas se detectó una campaña de Phishing que intenta recopilar fraudulentamente la información de pago de los usuarios invitando a participar de la Compra de Acciones de Petroperú.
El supuesto sitio web cuenta con logos característicos de la entidad y de los diferentes métodos de pago por los cuales se puede comprar dichas acciones.



Al ingresar datos de algún usuario

Se ingresa un Teléfono fijo y la página respondió la siguiente información

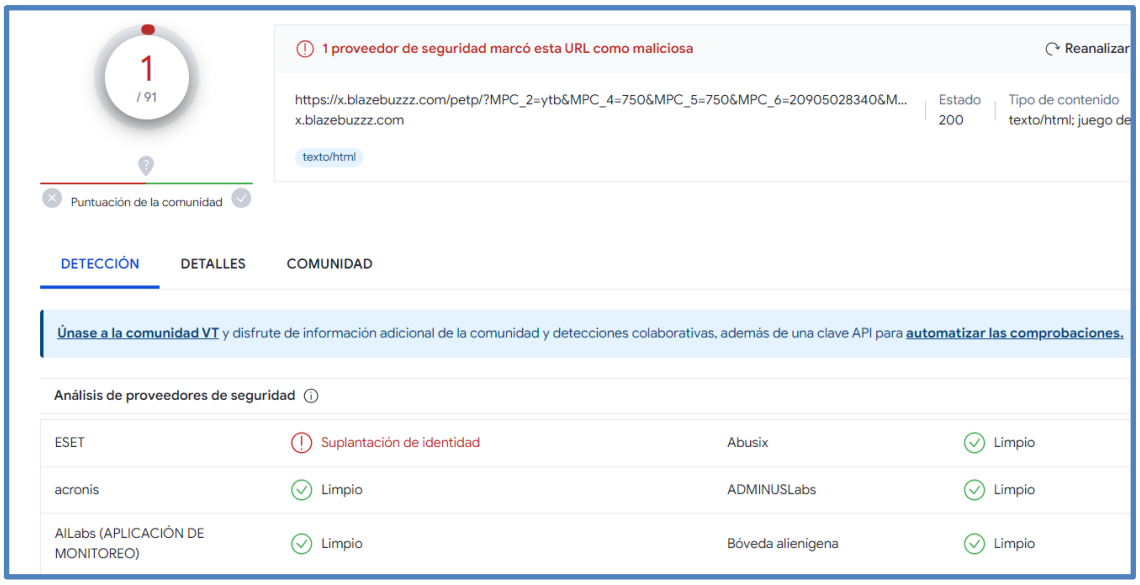


A. INDICADORES DE COMPROMISO

La URL Maliciosa, fue analizada en plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD**:

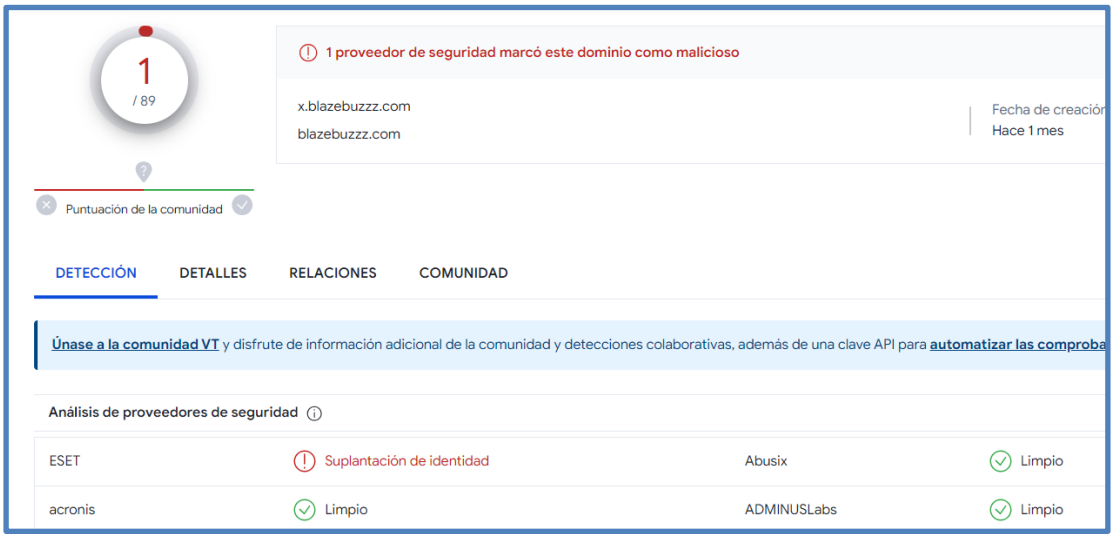
URL:

https://x.blazebuzzz.com/petp/?MPC_2=ytb&MPC_4=750&MPC_5=750&MPC_6=20905028340&MPC_14=686492063405&MPC_8=petp&adgroupid=154184715981&loc_physicall_ms=9060932&loc_interest_ms=9060932&matchtype=&network=ytv&creative=686492063405&keyword=&placement=youtube.com&targetid=&gclid=CjwKCAiA5L2tBhBTEiwAdSxJX-ikBnpDYCuQgGHcy8xso4vL13xy5zq5XOXhHSYqUlOBRmg3gu-F-xoCwaAQAvD_BwE&gbraid=0AAAAAqoHFeY_0a-ZhYP19VEp1ZJJjcIK6&wbraid=CjsKCQiAwbitBhCeARIqAH76de3GWwpAnMV9xTMYyuJTTihgy97HW4iDYsTpRI9y38dez8FZ1gvoGgKsBQ



Domain: blazebuzzz.com

- hosting lp-assets.blazebuzzz.com
- hosting x.blazebuzzz.com



IPs:

- 173.222.108.242
- 104.126.37.162
- 23.53.41.99
- 224.0.0.252
- 104.21.21.123
- 172.67.198.156
- 142.250.185.187

IPs V6:

- 2606:4700:3037::ac43:c69c
- 2606:4700:3035::6815:157b

3. RECOMENDACIONES:

- Realizar campañas de sensibilización, informando sobre las campañas de phishing a los usuarios de sus entidades.
- Verificar detalladamente la URL que corresponda al sitio web oficial de Petroperú.
- 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.
- Ingresar desde fuentes oficiales (https://www.petroperu.com.pe).

Fuente de Información:	Análisis del Monitoreo de Amenazas