 Centro Nacional de Seguridad Digital	<b>ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°019</b>		<b>Fecha: 22-01-2024</b>
			<b>Página: 4 de 13</b>
Componente que reporta	<b>CENTRO NACIONAL DE SEGURIDAD DIGITAL</b>		
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**

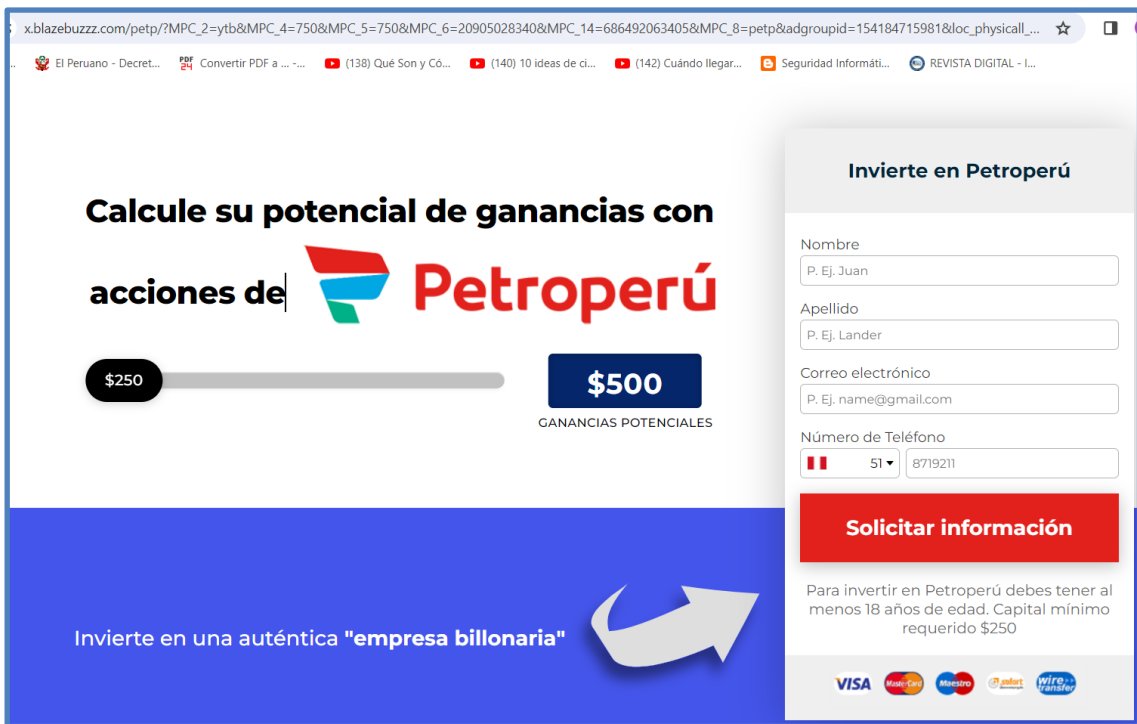
**1. ANTECEDENTES:**

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.

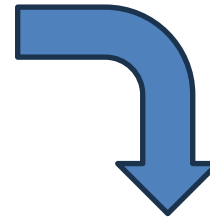


**2. DETALLES:**

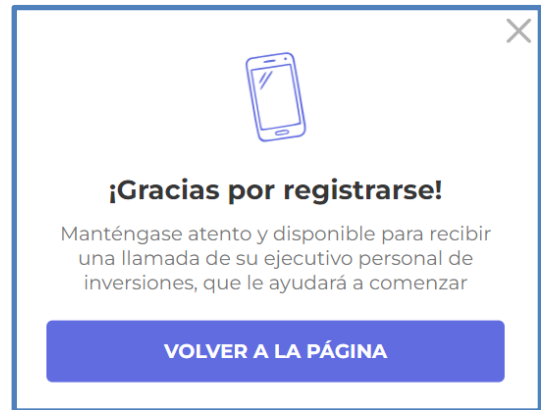
A través del monitoreo de amenazas se detectó una campaña de Phishing que intenta recopilar fraudulentamente la información de pago de los usuarios invitando a participar de la Compra de Acciones de Petroperú. El supuesto sitio web cuenta con logos característicos de la entidad y de los diferentes métodos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



**¡Gracias por registrarse!**

Manténgase atento y disponible para recibir una llamada de su ejecutivo personal de inversiones, que le ayudará a comenzar

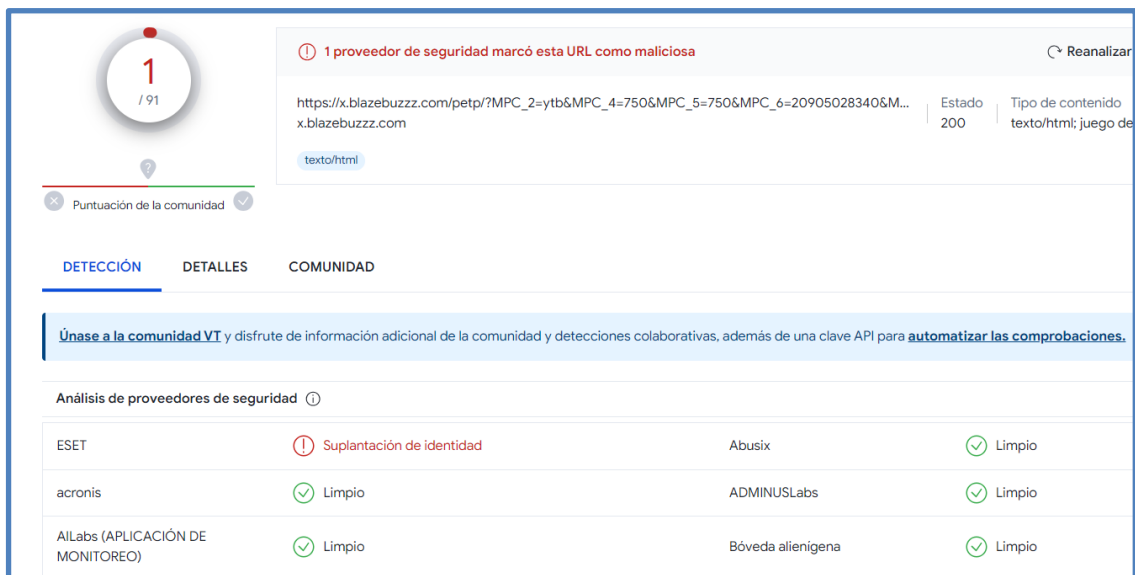
**VOLVER A LA PÁGINA**

**A. INDICADORES DE COMPROMISO**

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

**URL:**

https://x.blazebuzz.com/petp/?MPC\_2=ytb&MPC\_4=750&MPC\_5=750&MPC\_6=20905028340&MPC\_14=686492063405&MPC\_8=petp&adgroupid=154184715981&loc\_physical\_ms=9060932&loc\_interest\_ms=9060932&matchtype=&network=ytv&creative=686492063405&keyword=&placement=youtube.com&targetid=&gclid=CjwKCAiA5L2tBhBTEiwAdSxJX-ikBnpDYCuQgGHcy8xso4vL13xy5zq5XOXhHSYqUIOBRmg3gu-F-xoCwaAQAvD\_BwE&gbraid=0AAAAAqoHFeY\_0a-ZhYP19VEp1ZJJcIK6&wbraid=CjsKQCQiAwbitBhCeARlqAH76de3GWwpAnMV9xTMYyuJTihgy97HW4iDYsTpRI9y38dez8FZ1gvoGgKsBQ



1 / 91

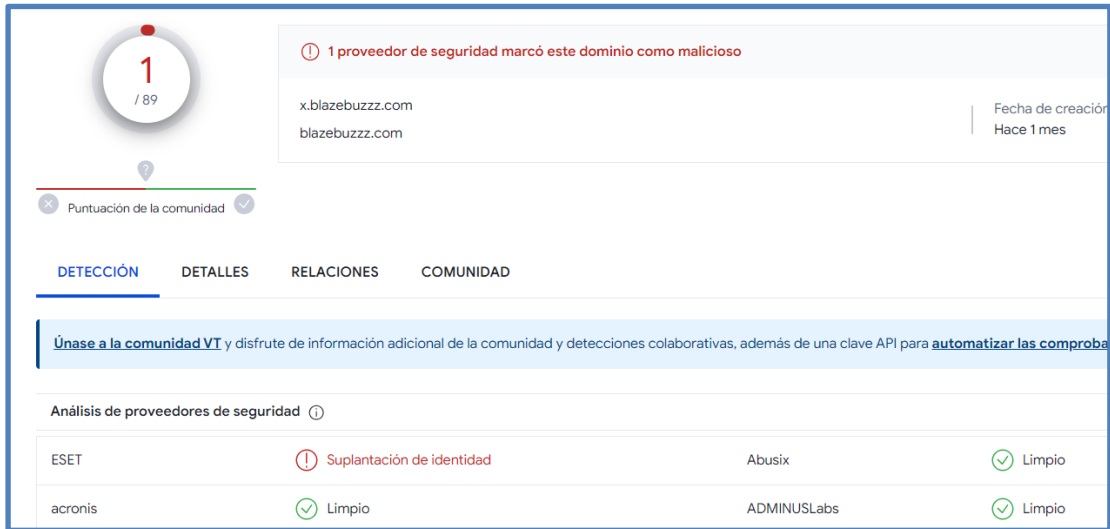
1 proveedor de seguridad marcó esta URL como maliciosa

https://x.blazebuzz.com/petp/?MPC\_2=ytb&MPC\_4=750&MPC\_5=750&MPC\_6=20905028340&M... Estado 200 Tipo de contenido texto/html; juego de

Proveedor de seguridad	Resultado	Detalle	Estado
ESET	Suplantación de identidad	Abusix	Limpio
acronis	Limpio	ADMINUSLabs	Limpio
AILabs (APLICACIÓN DE MONITOREO)	Limpio	Bóveda alienígena	Limpio

**Domain:** blazebuzzz.com

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



1 / 89

1 proveedor de seguridad marcó este dominio como malicioso

x.blazebuzzz.com	Fecha de creación
blazebuzzz.com	Hace 1 mes

Puntuación de la comunidad

DETECCIÓN DETALLES RELACIONES COMUNIDAD

Únase a la comunidad VT y disfrute de información adicional de la comunidad y detecciones colaborativas, además de una clave API para automatizar las comprobaciones.

Análisis de proveedores de seguridad

ESET	Suplantación de identidad	Abusix	Limpio
acronis	Limpio	ADMINUSLabs	Limpio

**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
------------------------	------------------------------------