PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

Siempre con el pueblo

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Centro Nacional de Seguridad Digital

asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

Lima, 13 de noviembre de 2022

308-2022-CNSD

La presente **Alerta Integrada de Seguridad Digital** corresponde a un análisis técnico periódico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aérea del Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en el marco de la Seguridad Digital del Estado Peruano.

El objetivo de esta alerta **es informar a los responsables de la seguridad digital de las entidades públicas y las empresas privadas sobre las amenazas en el entorno digital** para advertir las situaciones que pudieran afectar la continuidad de sus servicios en favor de la población.

Las marcas y logotipos de empresas privadas y/o entidades públicas se reflejan para ilustrar la información que los ciudadanos reciben por redes sociales u otros medios y que atentan contra la confianza digital de las personas y de las mismas empresas **de acuerdo con lo establecido por el Decreto de Urgencia 007-2020**.

La presente Alerta Integrada de Seguridad Digital es información netamente especializada para informar a las áreas técnicas de entidades y empresas.

Contenido

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 308	Fecha: 13-11-2022
		Página 4 de 7

Componente que reporta	DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ		
Nombre de la alerta	Phishing, suplantando la identidad a la plataforma 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	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 nueva campaña de Phishing, dirigido a usuarios de PayPal (Servicio de pago por internet) con el objetivo de robar las credenciales de acceso de inicio de sesión, datos personales y bancarios.

2. **Imagen**: Proceso del ataque Phishing:

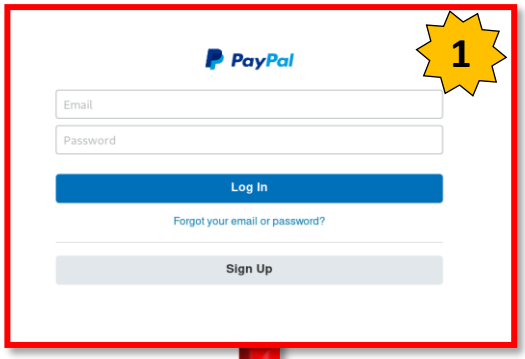


Imagen 1

Sitio web fraudulento, donde solicita a las posibles víctimas ingresar sus credenciales de acceso (E-mail y contraseña).

Imagen 2

Una vez ingresado las credenciales de acceso, redirige al sitio web oficial de la plataforma PayPal.

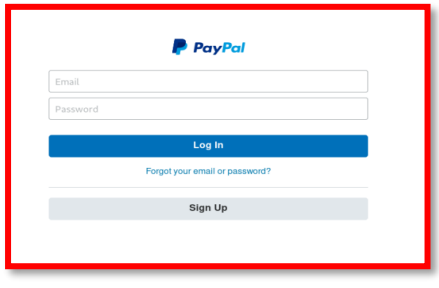
3. Comparación del sitio web oficial de PayPal, con el fraudulento:

SITIO WEB OFICIAL

URL: https://www.paypal.com/pe/signin

SITIO WEB FRAUDULENTO

URL: hxxps[:]//paypal-support-01[.]duckdns[.]org/login[.]html

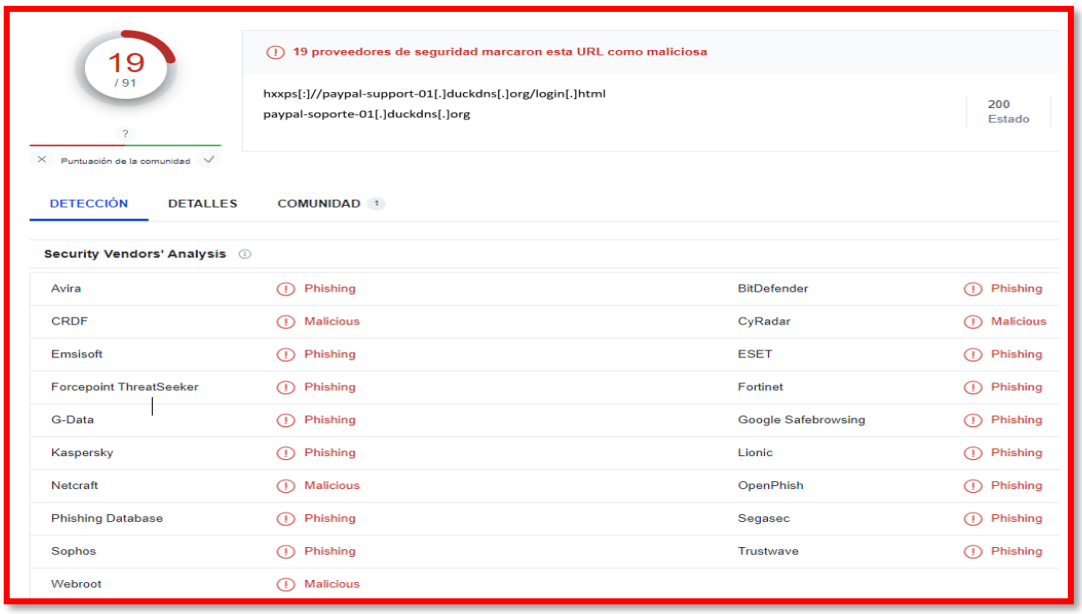


- Existe una diferencia entre la URL original y la URL fraudulenta.
- La URL falsa utiliza protocolo HTTPS, no significa que la web sea segura.
- El dominio (saudi-tech.com.sa) del sitio web fraudulento se encuentra reportado como **PHISHING**.
- Existe una similitud entre ambas páginas, en imagen, fondo y colores de ambos sitios web.

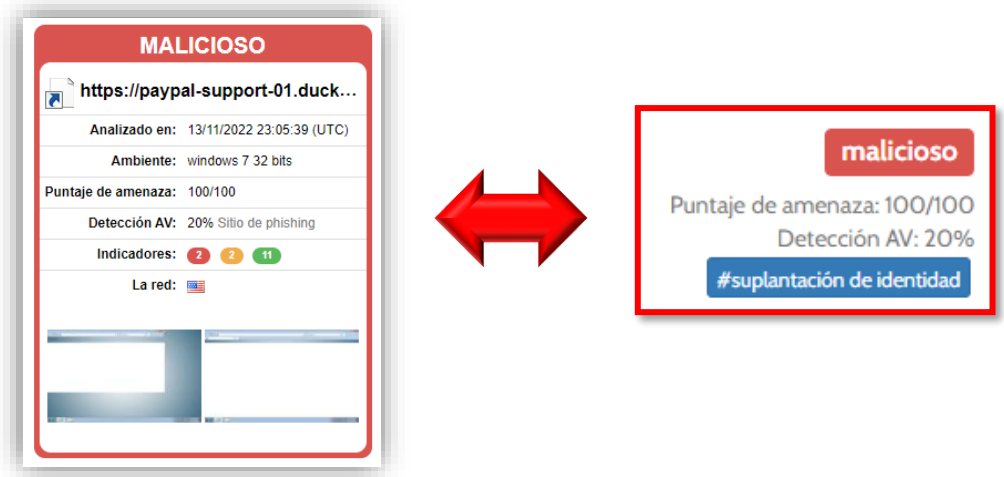
4. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD:**

- **INDICADORES DE COMPROMISO:**

  - ✓ **URL:** hxxps[:]//paypal-support-01[.]duckdns[.]org/login[.]html
  - ✓ **Dominio:** paypal-soporte-01[.]duckdns[.]org
  - ✓ **IP:** 51[.]81[.]203[.]63
  - ✓ **Código:** 200
  - ✓ **Longitud:** 94.19 KB
  - ✓ **SHA-256**: 6ecd99459ce467a9ec7fa7b4a29768c8cff3759fd0af890eb5bfe6dfc32b9959



- **OTRAS DETECCIONES:**



5. ALGUNAS RECOMENDACIONES:

- Verificar la información en la entidad correspondiente.
- Acceder al sitio web a través de fuentes oficiales.
- No abrir enlaces de dudosa procedencia.
- No seguir indicaciones de sitios web fraudulentos.
- No compartir la información con terceras personas, amigos o familiares.
- Mantener instalado un servicio de antivirus en el dispositivo.

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

Índice alfabético