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, 12 de noviembre de 2022

307-2022-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

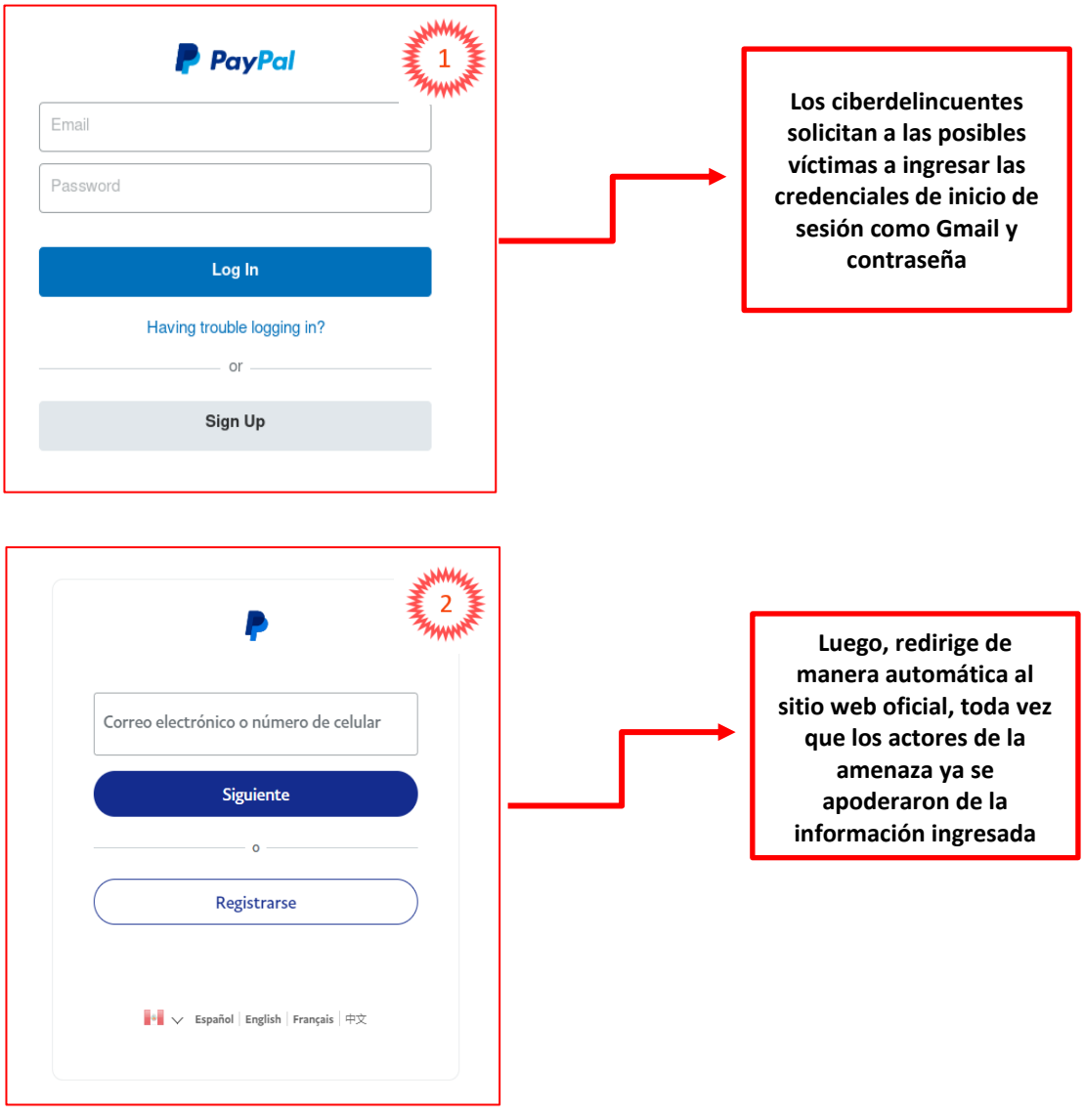
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 307	**Fecha: 12-11-2022**
		Página 4 de 6

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Phishing, suplantando la identidad de la empresa de pagos en línea PayPal		
Tipo de ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Enlaces de internet		
Código de familia	C	Código de subfamilia	C07
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 de la empresa de pagos en línea PayPal; el cual, mediante la creación de un sitio web similar al original, solicitan a las posibles víctimas a ingresar las credenciales de inicio de sesión, con la finalidad de robar la información ingresada.

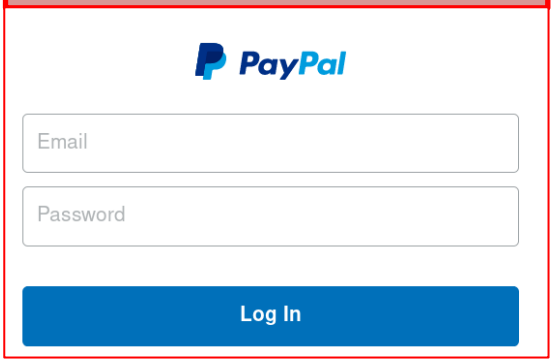
2. Proceso del ataque Phishing:



3. Comparación del sitio web oficial y fraudulento:

Sitio web oficial
https://www.paypal.com/signin

Sitio web fraudulento
hxxps://paypal-support-01[.]duckdns[.]org/login[.]html



- La diferencia está en la URL, toda vez que el dominio del sitio web fraudulento, no coincide con el oficial.
- Ambos sitios webs utilizan el protocolo https, lo que hace más convincente para que las víctimas ingresen a duchi sitio web.

4. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, obteniendo la siguiente información:

- **URL:** hxxps://paypal-support-01[.]duckdns[.]org/login[.]html
- **Dominio:** paypal-soporte-01[.]duckdns[.]org
- **IP:** 51.81.203.63
- **Tamaño:** 94.19 KB
- **SHA-256:** 6ecd99459ce467a9ec7fa7b4a29768c8cff3759fd0af890eb5bfe6dfc32b9959

alphaMountain.ai	Phishing	Antiy-AVL	Malicious
Avira	Phishing	BitDefender	Phishing
CRDF	Malicious	CyRadar	Malicious
Emsisoft	Phishing	ESET	Phishing
Forcepoint ThreatSeeker	Phishing	Fortinet	Phishing
G-Data	Phishing	Google Safebrowsing	Phishing
Kaspersky	Phishing	Lionic	Phishing
Netcraft	Malicious	Phishing Database	Phishing
Phishtank	Phishing	Scantitan	Phishing
Segasec	Phishing	Sophos	Phishing
Webroot	Malicious	Abusix	Clean

5. **Recomendaciones:**

- No abrir correos ni mensajes de dudosa procedencia
- Desconfiar de los enlaces y archivos enviados a través de mensajes o correos electrónicos
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Prestar atención en los detalles de los mensajes o redes sociales
- Evaluar el bloqueo preventivo de los indicadores de compromisos
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
- Visualizar los sitios web que se ingresen sean los oficiales

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

Índice alfabético