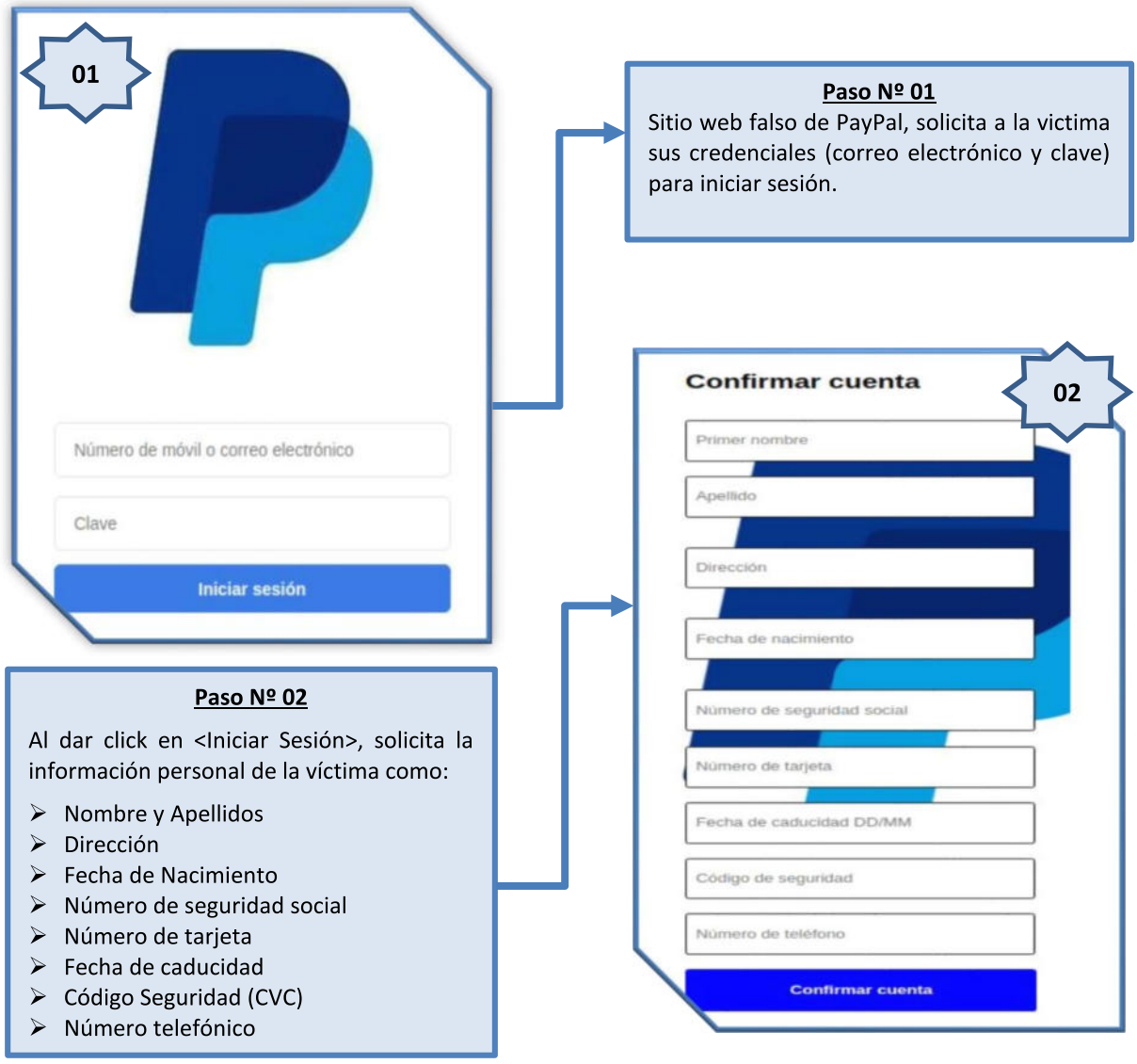
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 095	Fecha: 05-04-2022
		Página 6 de 8

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 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 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. ***Imagen: detalles del proceso de Phishing***.



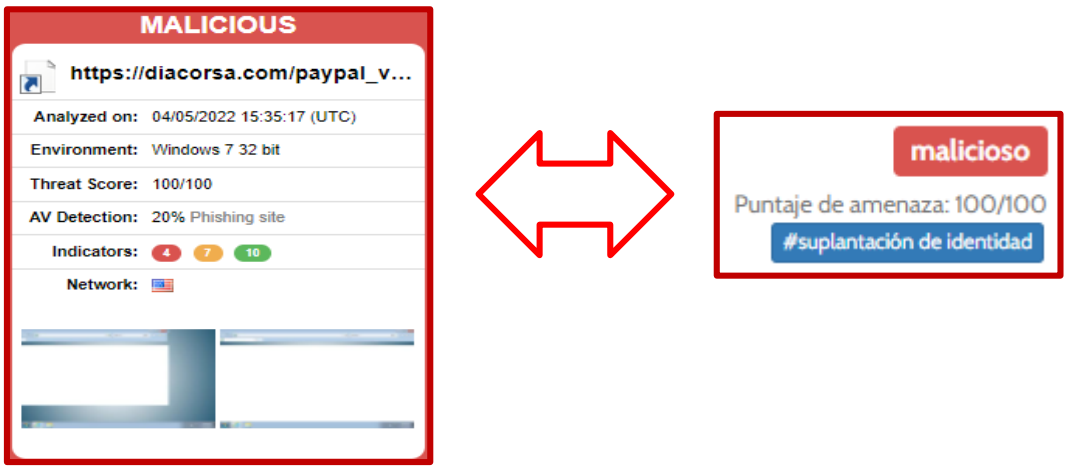
3. ***Proveedores de seguridad informática alertan como SUPLANTACIÓN DE IDENTIDAD - PHISHING.***

Bóveda alienígena	Malicioso	alphaMountain.ai	Suplantación de identidad
Avira	Suplantación de identidad	BitDefender	Malware
CRDF	Malicioso	CyRadar	Malicioso
ESET	Suplantación de identidad	Buscador de amenazas de Forcepoint	Suplantación de identidad
Fortinet	Suplantación de identidad	G-datos	Malware

4. ***Indicadores de compromiso (IoC)***

- ✓ URL : hxxps:// diacorsa[.]com/paypal_verification_support/secure_verify/
- ✓ DOMINIO : diacorsa[.]com
- ✓ SHA-256 : 0a083fe1469ce348ba2fa35897aef483245923c2a8bdf2f15705d222ae9dc823
- ✓ SERVIDOR : Apache
- ✓ IP : 162[.]241[.]163[.]215

5. ***Otras detecciones:***



6. ***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).

7. ***Algunas 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.

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