	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 080	**Fecha: 03-04-2023**
		Página 5 de 9

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Phishing, suplantando la identidad de Dropbox		
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 Dropbox, con la finalidad de robar las credenciales de acceso (usuarios y contraseñas) de los clientes de los usuarios de este servicio.

2. Detalles del proceso de estafa de Phishing.

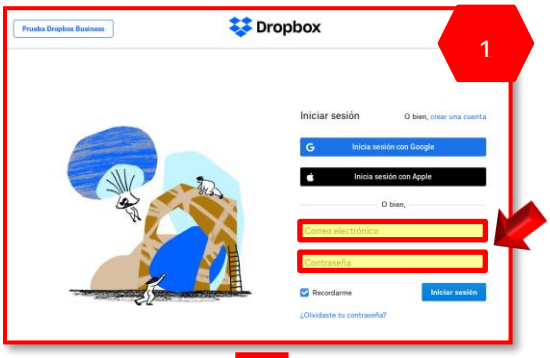


Imagen 1: Sitio web fraudulento; donde los ciberdelincuentes solicitan a sus posibles víctimas introducir sus credenciales de acceso (usuario y contraseña).

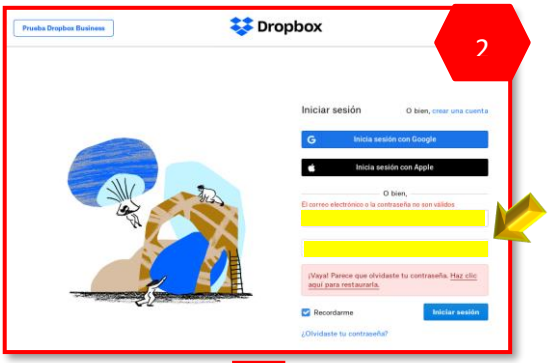
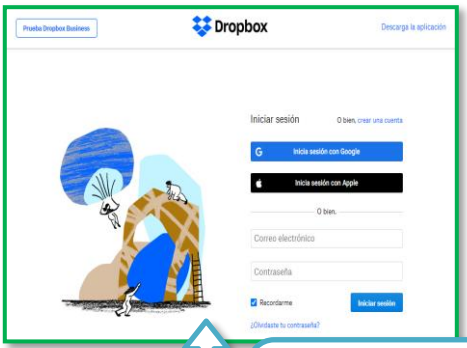


Imagen 2: Una vez ingresado las credenciales de acceso y haber respondido el mensaje de verificación, redirecciona a este mensaje indicando que el e-mail proporcionado es incorrecto; dando así por concluida la estafa.

3. Comparación del sitio web oficial y fraudulento.

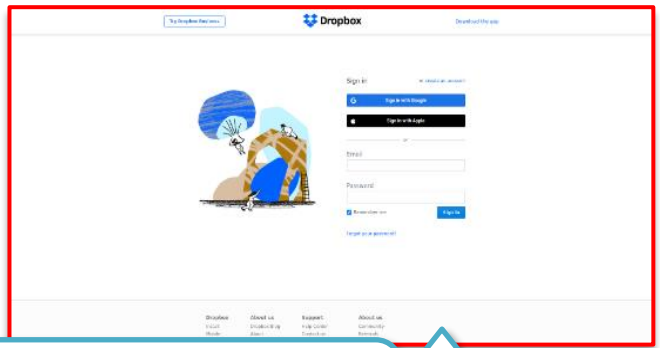
SITIO WEB OFICIAL

https://www.dropbox.com/es/login



SITIO WEB FRAUDULENTO

http://dropboxnotifications.net/landing/form/9337d24a-b5cf-42f3-8cb9-473bce016e25



- **Existe una diferencia entre la URL original y la URL fraudulenta.**
- **El dominio (www-dropbox-com.dropbox.lilyskitchen.skyfencenet.com) del sitio web fraudulento, se encuentra reportado como PHISHING.**
- **Existe una similitud entre ambos sitios web (color y forma); siendo dificultoso reconocer el sitio web fraudulento a simple vista.**

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

- **URL Malicioso:** hxxp://dropboxnotifications[.]net/landing/form/9337d24a-b5cf-42f3-8cb9-473bce016e25
- **Dominio:** dropboxnotifications[.]net
- **Código:** 200
- **Tamaño:** 77.08 KB
- **SHA-256:** fb459c4bde071eb4607ed7371926dccedc3e7b16a34b61e767df5cf0bf14816f

alphaMountain.ai	Phishing	Cluster25	Phishing
CRDF	Malicious	ESET	Phishing
Heimdal Security	Phishing	Phishing Database	Phishing

5. **Cómo funciona el Phishing:**

- Los correos electrónicos incluyen enlaces a sitios web preparados por los ciberdelincuentes en los que solicitan información personal.
- Medios de propagación del Phishing: WhatsApp, Telegram, redes sociales, SMS entre otros.
- Los ciberdelincuentes intentan suplantar a una entidad legitima (organismo público, entidad financiera,
- servicio técnico, etc.)

6. **Apreciación de la información**

- Dropbox, es un servicio de alojamiento de archivos multiplataforma en la nube; este servicio permite a los usuarios almacenar y sincronizar archivos en línea y entre ordenadores; así como compartir archivos y carpetas con otros usuarios y con Tablets y móviles.

7. **Algunas Recomendaciones**

- Evitar acceder a enlaces que llegan inesperadamente por correo electrónico u otros medios.
- No proporcionar datos personales (contraseñas, tarjetas, cuentas bancarias, etc.) por correo, teléfono o SMS.
- Contar con una solución de seguridad confiable tanto en los dispositivos de escritorio como en teléfonos.
- Verifica la fuente de información de tus correos entrantes.
- Introduce tus datos únicamente en webs seguras.
- Ante cualquier sospecha de haber caído en el engaño del Phishing, accede a tu cuenta y cambia la contraseña.

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