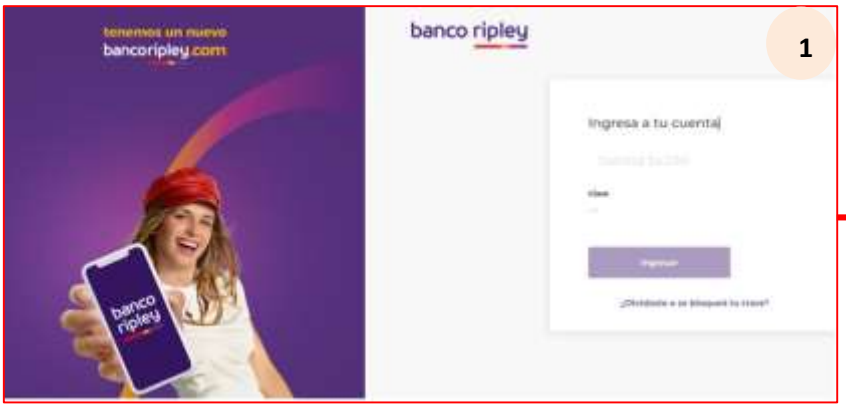
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 288	Fecha: 23-10-2022
		Página 04 de 06

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Campaña de phishing suplantando la identidad del Banco Ripley		
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, por medio de los diferentes navegadores web, dirigido a los clientes y/o usuarios de la entidad bancaria del Banco Ripley; 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, validando datos personas y bancarios como N° de tarjeta bancaria, clave web, fecha de vencimiento, clave de seguridad, número de contacto, entre otros.

2. Proceso de ataque del Phishing.



Solicita ingresar las credenciales de inicio de

Después, requiere realizar una supuesta actualización de datos bancarios

Finalmente, redirige de forma automática al sitio web original de RIPLEY

3. Comparación del sitio web original y sitio web fraudulento:

Sitio web oficial
https://bancaenlinea.bancoripley.com.pe/login

Sitio web fraudulento
hxxps://www.banco-ripley-ingreso-persona[.]letsplayfpl[.]com

- Ambas URL´s utilizan el protocolo https, lo que hace más convincente a que las víctimas accedan al sitio web.
- La diferencia está en la URL, toda vez que el dominio del sitio web fraudulento, no coincide con el oficial.

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

- **URL:** hxxps://www.banco-ripley-ingreso-persona[.]letsplayfpl[.]com
- **Dominio:** www[.]banco-ripley-ingreso-persona[.]letsplayfpl[.]com
- **IP:** 192.30.136.251
- **Tamaño:** 26.45 KB
- **SHA-256:** 2e04cdb36a78d7e73293f7b8874fa4fc373fa313f9573484f02ec468e31832fb

Antiy-AVL	Malicious	Avira	Phishing
BitDefender	Phishing	Certego	Phishing
Comodo Valkyrie Verdict	Phishing	Emsisoft	Phishing
ESET	Phishing	Forcepoint ThreatSeeker	Phishing
Fortinet	Phishing	G-Data	Phishing
Kaspersky	Phishing	Lionic	Phishing
Netcraft	Malicious	Phishing Database	Phishing
Phishtank	Phishing	Sophos	Phishing
Viettel Threat Intelligence	Phishing	Webroot	Malicious

5. Algunas Recomendaciones:

- No abrir correos ni mensajes de dudosa procedencia
- Desconfiar de los enlaces y archivos en los mensajes o correo
- 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