	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°192	Fecha: 16-08-2023
		Página: 13 de 16

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Detección de una campaña de Phishing a la plataforma de YAHOO!		
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 Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

1. ANTECEDENTES:

A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes se encuentran desarrollando una nueva campaña de Phishing, a través de los diferentes navegadores web, quienes vienen suplantando la identidad de la plataforma de Yahoo!, con la finalidad obtener credenciales de acceso; para luego utilizarlas por los ciberdelincuentes para cumplir con sus falsos propósitos.

2. DETALLES:

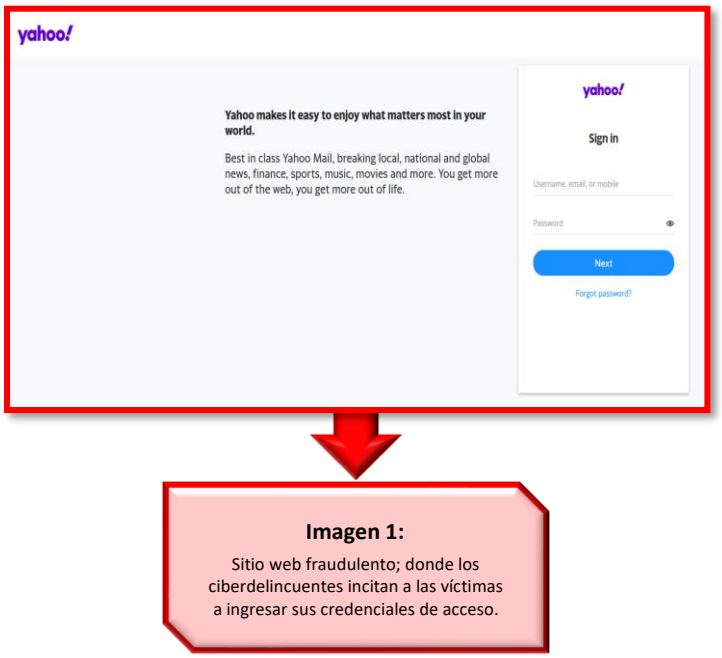


Imagen 1:
Sitio web fraudulento; donde los ciberdelincuentes incitan a las víctimas a ingresar sus credenciales de acceso.

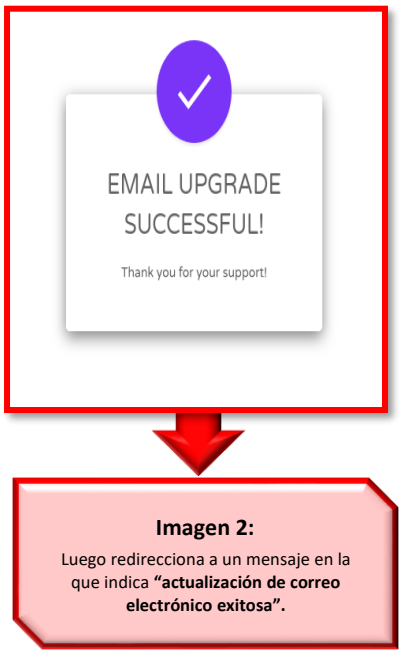


Imagen 2:
Luego redirecciona a un mensaje en la que indica **"actualización de correo electrónico exitosa".**

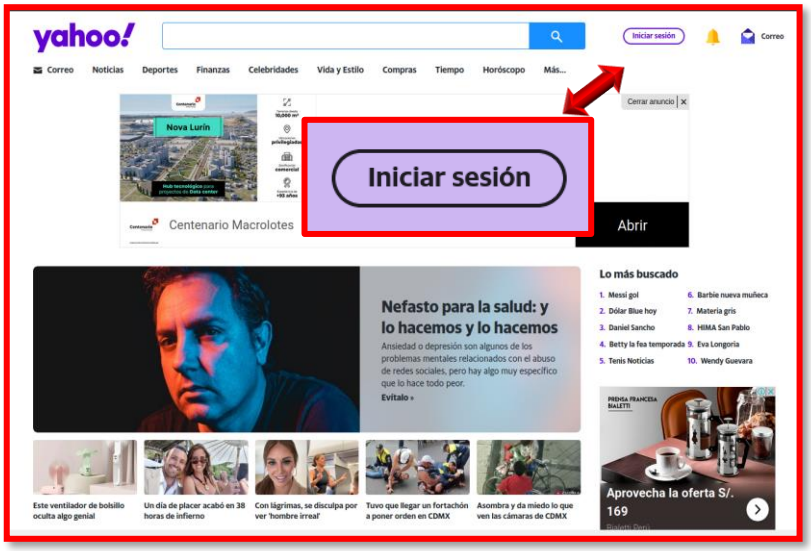


Imagen 3:
Por último, es redirigido a la página web oficial de Yahoo!; la cual continuar un enlace de inicio de sesión al servicio de correo electrónico gratuito de Yahoo!

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

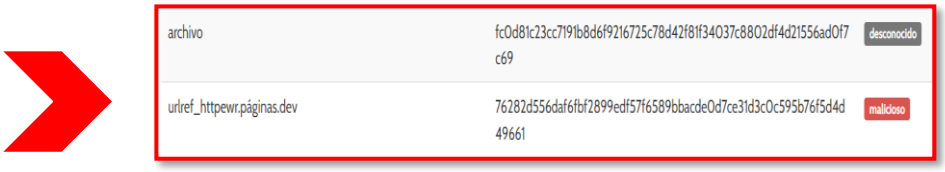
a) Indicadores de compromisos:

I. URL:

Hxxps[:]//hsbw[.]pages[.]dev/

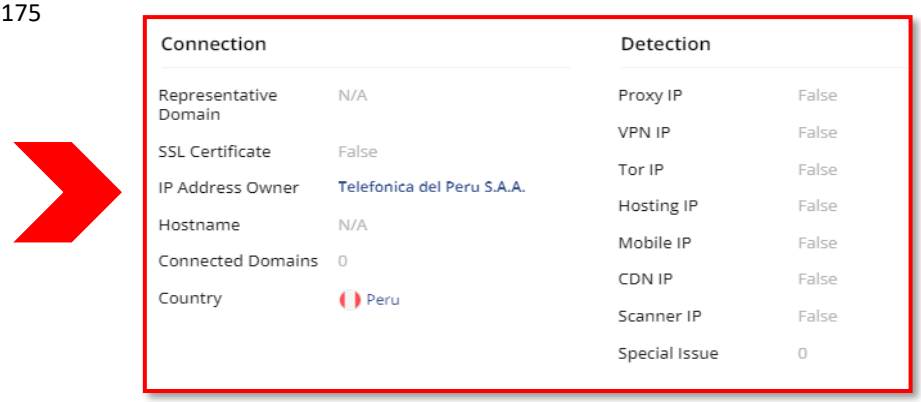
II. SHA-256:

76282d556daf6fbf2899edf57f6589bbacde0d7ce31d3c0c595b76f5d4d49661



III. IP:

172[.]66[.]47[.]175



B. Se hallaron **26 proveedores** de seguridad que marcaron este dominio como malicioso.

alphaMountain.ai	Phishing	AlphaSOC	Phishing
Antiy-AVL	Malicious	Avira	Phishing
BitDefender	Malware	Cluster25	Phishing
CRDF	Malicious	CyRadar	Malicious
Emsisoft	Phishing	ESET	Phishing
Forcepoint ThreatSeeker	Phishing	Fortinet	Phishing
G-Data	Malware	Google Safebrowsing	Phishing
Kaspersky	Phishing	Lionic	Phishing
Netcraft	Malicious	Phishing Database	Phishing
Phishtank	Phishing	SCUMWARE.org	Malware
Segasec	Phishing	SOCRadar	Phishing
Sophos	Phishing	Trustwave	Phishing
VIPRE	Malicious	Webroot	Malicious

C. Otras detecciones:

D. Apreciación de la información:

- Yahoo! es una empresa global de medios la cual posee un portal de internet, un directorio web y una serie de servicios, incluido el correo electrónico Yahoo!; entre otros.
- La presente campaña de Phishing, permite a los ciberdelincuentes acceder u obtener credenciales de acceso; para sus propósitos.

3. 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.
- No introducir datos confidenciales en sitios web sospechosas o de dudosa procedencia.
- Verificar la fuente de información de tus correos entrantes.
- Introducir tus datos únicamente en webs seguras.
- Tener siempre actualizado el sistema operativo y el antivirus. En el caso del antivirus, comprobar que está activo.

Fuente de Información:	Análisis propio de redes sociales y fuente abierta.