

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°201			Fecha: 27-08-2023
				Página: 5 de 11
Componente que reporta	DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ			
Nombre de la alerta	Detección de sitio web fraudulento del Banco Interbank			
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 actores de amenazas vienen llevando a cabo una campaña de Phishing, suplantando el sitio web de solicitud de préstamos del Banco Interbank, con la finalidad de robar información sensible de los usuarios de la entidad financiera como números de documento de identidad, tarjetas bancarias, etc.

2. DETALLES:

El proceso del Phishing es el siguiente:

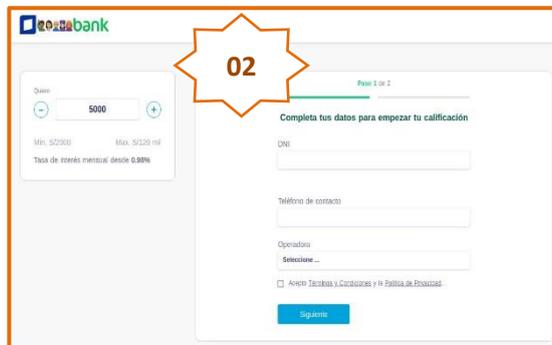


Paso N°01

Solicitan a la víctima registrar lo siguiente:

- El monto del préstamo solicitado.

Para luego dar clic en <Calificar ahora>.

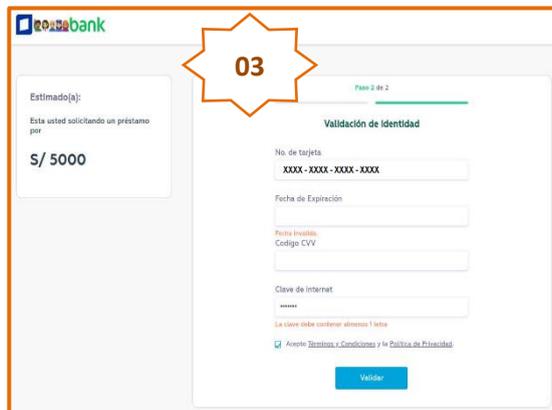


Paso N°02

Solicita a la víctima datos como:

- El número del Documento Nacional de Identidad (DNI).
- Número de celular
- Operador telefónico

Para luego dar clic en <Siguiente>.



Paso N°03

Una vez brindado los datos solicitados en el paso N.º 02, aparece una pantalla requiriendo información como el numero de la tarjeta bancaria, la fecha de expiración, el código de seguridad (CVV) y la clave de seis dígitos del intranet, para luego dar clic en <Validar>. Pero, pasado unos segundos, redirige al sitio web oficial de la entidad bancaria; sin embargo, los ciberdelincuentes obtuvieron los datos proporcionados por la víctima.

A. Comparación del sitio web oficial y fraudulento.

SITIO WEB OFICIAL

`https://interbank.pe/inscripcion/prestamo-paso-1`



Dominio: Interbank.pe

SITIO WEB FRAUDULENTA

`https://Interbanksolicitudampliacionprestamo[consultas-pe].online`



Dominio: consultas-pe[.]online

- Existe una diferencia entre la URL original y la URL fraudulenta.
- La URL del sitio web fraudulento posee protocolo de seguridad de red (https)
- Existe una similitud entre ambas páginas en imagen, fondo y color.

B. Proveedor de seguridad informática no alerta como SUPlantación DE IDENTIDAD - PHISHING.



C. Indicadores de compromiso (IoC)

- Dominio : consultas-pe[.]online
- IP : 47[.]251[.]51[.]148
- Servidor : Apache
- SHA-256 : e8e9e46833d1a5d5c6437e62730ec3850b49be76ef5b1c38e41962f76bc707ff

D. Comparación de DOMINIOS

```

Domain Name: interbank.pe
Sponsoring Registrar: NIC.PE
Domain Status: ok
Registrant Name: jaime arroyo vilcara
Admin Name: BANCO INTERNACIONAL DEL PERU-INTERBANK
Admin Email: dominiosibk@intercorp.com.pe
Name Server: ns1-08.azure-dns.com
Name Server: ns2-08.azure-dns.net
Name Server: ns3-08.azure-dns.org
Name Server: ns4-08.azure-dns.info
>>> Last update of WHOIS database: 2023-08-21T23:58:04.815Z <<<
    
```

```

Domain Name: CONSULTAS-PE.ONLINE
Registry Domain ID: D382540404-CNIC
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com
Updated Date: 2023-07-31T11:53:47.0Z
Creation Date: 2023-07-22T19:12:11.0Z
Registry Expiry Date: 2024-07-22T23:59:59.0Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
    
```

E. Apreciación de la información:

- La presente campaña de Phishing permite a los actores de amenazas obtener información bancaria de los usuarios del Banco Interbank.
- La propagación del sitio web fraudulento se realiza mediante envío masivos de email, adjuntando enlaces de sitios web fraudulentos con la finalidad de obtener información sensible de las víctimas; asimismo, a través de las aplicaciones de mensajería instantánea entre ellos WhatsApp, Telegram, Messenger, etc. y mensajes de textos SMS.

3. RECOMENDACIONES:

- Verificar detalladamente las URL de los sitios web.
- No abrir o descargar archivos sospechosos.
- No aceptar permisos de instalación de archivos desconocidos o dudosa procedencia.
- Mantener actualizado el sistema operativo y aplicaciones del equipo de cómputo.
- Mantener actualizado el sistema antivirus (el antivirus debe ser licenciado).
- Comunicar a la entidad financiera si ha realizado un registro de acceso en un sitio web sospechoso.

Fuente de Información:

Análisis propio de redes sociales y fuente abierta

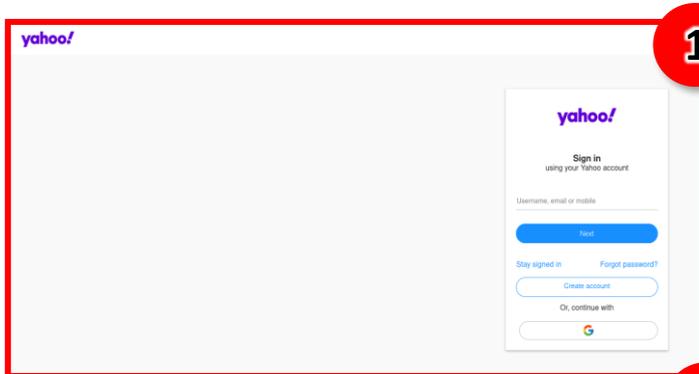
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°201		Fecha: 27-08-2023
			Página: 8 de 11
Componente que reporta	DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ		
Nombre de la alerta	Detección de una campaña de Phishing a la plataforma de YAHOO!		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medios 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:

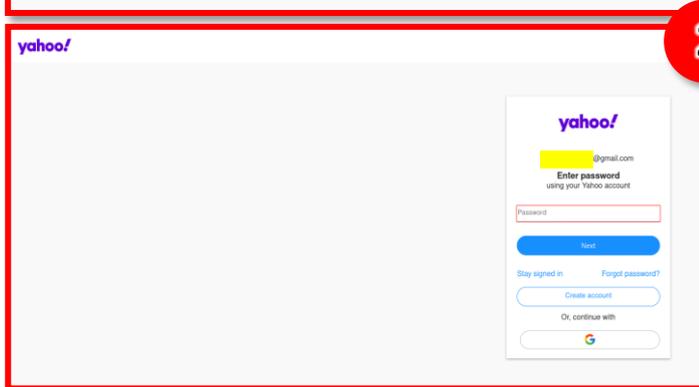
A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes se encuentran desarrollando una nueva campaña de Phishing, a través de los diferentes navegadores web, quienes vienen suplantando la identidad de la plataforma de Yahoo!, con la finalidad obtener credenciales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

2. DETALLES:



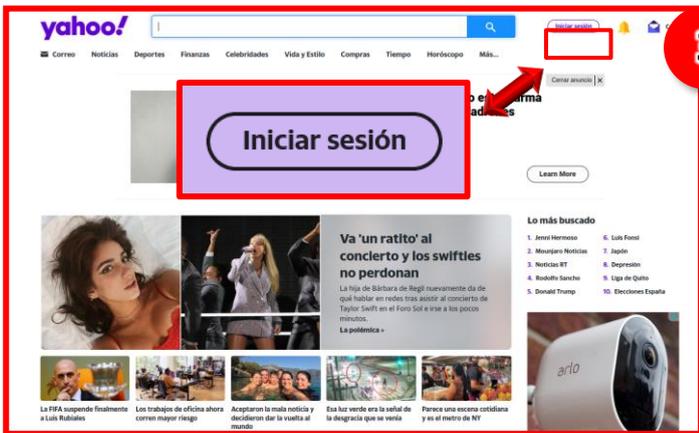
1

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



2

Imagen 2:
Solicita ingresar el password (contraseña).



3

Imagen 3:
Por último, es redirigido a la página web oficial de Yahoo!; la cual indica **Iniciar sesión**, 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[:]//hola-mundo-withered-field-7eef[.]shelgilhuys12[.]workers[.]dev/



Nombre del envío:	hxxps://hola-mundo-campo-marchitado-7eef.shelgilhuys12.workers.dev/
Tamaño:	90B
Tipo:	URL
Mímica:	Texto sin formato
Sistema operativo:	ventanas
Último análisis antivirus:	26/O8/2023 17:55:12 (UTC)
Último informe de Sandbox:	26/O8/2023 17:55:10 (UTC)

II. **SHA-256:**

5cc8efcf7768b73a7af93615a9fca3136009fa0a5d2d62a530edfa82672ecb45



FF2VXRNP.htm	malicioso
5cc8efcf7768b73a7af93615a9fca3136009fa0a5d2d62a530edfa82672ecb45	
Tar3543.tmp	ninguna amenaza específica
bc3a6e84e41faeb57e7c21aa3b60c2a6477107009727c5b7c0ed8fe658909e5	

III. **IP:**

172[.]67[.]206[.]24



Connection		Detection	
Representative Domain	N/A	Proxy IP	False
SSL Certificate	False	VPN IP	False
IP Address Owner	CLOUDFLARENET	Tor IP	False
Hostname	N/A	Hosting IP	! True
Connected Domains	! 347	Mobile IP	False
Country	United States	CDN IP	False
		Scanner IP	False
		Special Issue	0

B. Se hallaron **24 proveedores** de seguridad que marcaron este dominio como malicioso.

alphaMountain.ai	! Phishing	AlphaSOC	! Phishing
Avira	! Phishing	BitDefender	! Phishing
Cluster25	! Phishing	CRDF	! Malicious
CyRadar	! Malicious	Emsisoft	! Phishing
ESET	! Phishing	Forcepoint ThreatSeeker	! Phishing
Fortinet	! Phishing	G-Data	! Phishing
Google Safebrowsing	! Phishing	Kaspersky	! Phishing
Netcraft	! Malicious	OpenPhish	! Phishing
Phishing Database	! Phishing	Phishtank	! Phishing
Quick Heal	! Phishing	Segasec	! Phishing
Sophos	! Phishing	Trustwave	! Phishing
VIPRE	! Malicious	Webroot	! Malicious

C. Otras detecciones:



MALICIOSO

<https://hola-mundo-withered-fi...>
 Analizado en: 26/08/2023 17:55:10 (...)
 Ambiente: Windows 7 de 32 bits
 Puntuación de amenaza: 100/100
 Detección AV: 26% Sitio de phishing
 Indicadores: 3 3 10
 Red: 🇵🇪 🇺🇸

malicioso
 Puntuación de amenaza: 100/100
 #suplantación de identidad

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 sospechosos 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