	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°246	Fecha: 17-10-2023
		Página: 13 de 18

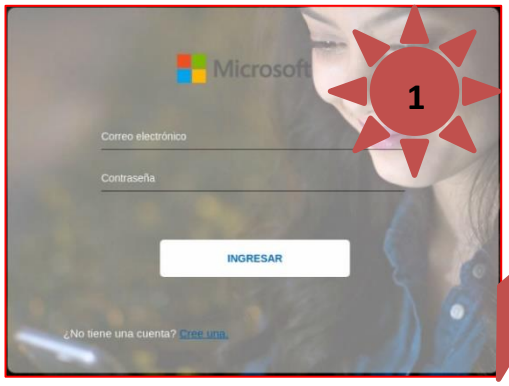
Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Detección de campaña de Phishing suplantando la identidad de la empresa de tecnología multinacional Microsoft		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, 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 vienen llevando a cabo una campaña de Phishing, a través de los diferentes navegadores web, quienes vienen suplantando la identidad de la empresa de tecnología multinacional Microsoft, con el objetivo robar credenciales de inicio de sesión, como dirección de correo electrónico, contraseña, etc.

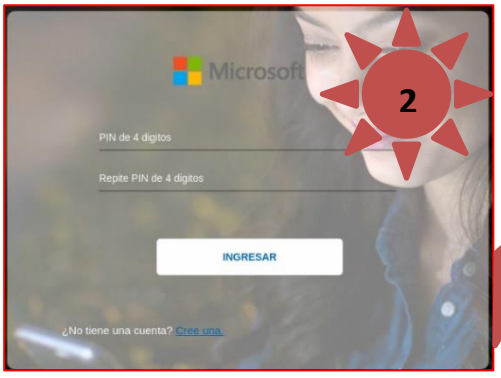
2. DETALLES:



PASO No 01

Al ingresar a supuesto sitio web solicita lo siguiente:

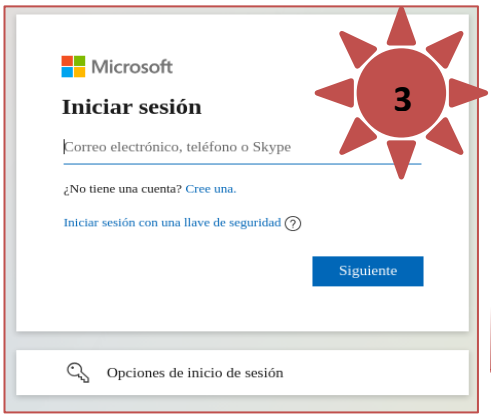
1. Correo electrónico
2. Contraseña



PASO No 02

Después, requiere ingresar un código de seguridad de cuatro dígitos:

1. Ingresar PIN 4 dígitos
2. Repetir el PIN de 4 dígitos

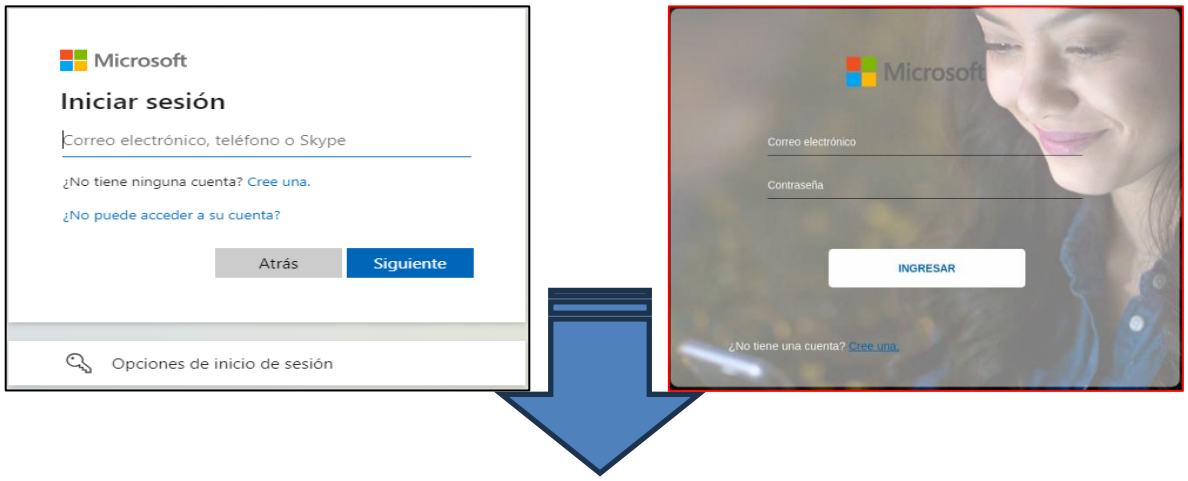


PASO No 03

Al ingresar los datos requeridos redirige de manera automática al sitio web oficial de Microsoft, solicitando nuevamente iniciar sesión; toda vez que los ciberdelincuentes ya se apoderaron de la información brindada.

A. Comparación del sitio web oficial y fraudulento.

SITIO WEB OFICIAL	SITIO WEB FRAUDULENTO
https://login.microsoftonline.com	**hxxps://web000digital007.webcindario.com**



- Existe una diferencia entre la URL original y la URL fraudulenta.
- La URL falsa utiliza protocolo HTTPS, lo que hace más convincente a que las víctimas ingresen a dicho sitio web.
- Existe una similitud entre ambas páginas, en imagen, fondo y colores de ambos sitios web.

B. URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD - PHISHING**.

Análisis de proveedores de seguridad			¿Quieres automatizar
alfaMontaña.ai	Suplantación de identidad	AlfaSOC	Suplantación de identidad
Avira	Suplantación de identidad	Clúster25	Suplantación de identidad
CRDF	Malicioso	CyRadar	Malicioso

C. Indicadores de compromisos:

I. Dominio: web000digital007.webcindario.com

II. IP : 5[.]57[.]226[.]202

III. SHA-256: 57aef267fca58cd9327619e78054dc9f7ce6aac11a3a15492c319aaa670a8665

3. RECOMENDACIONES:

- Mantener instalado un servicio de antivirus en el dispositivo.
- Verificar la información del sitio web correspondiente.
- Acceder al sitio web a través de fuentes oficiales.
- No abrir enlaces de dudosa procedencia.
- No seguir indicaciones de sitios web fraudulentos.
- No compartir la información con terceras personas, amigos o familiares.

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

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°246	**Fecha: 17-10-2023**
		Página: 15 de 18

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Nueva campaña de Phishing que suplanta la entidad bancaria de BBVA		
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 vienen llevando a cabo avanzados ataques cibernéticos, por medio de envíos de correos electrónicos fraudulentos, o también conocidos como Phishing, simulado ser la entidad bancaria BBVA, en cual tiene el objetivo de robar credenciales de acceso, datos personales y/o bancarios.

2. DETALLES:

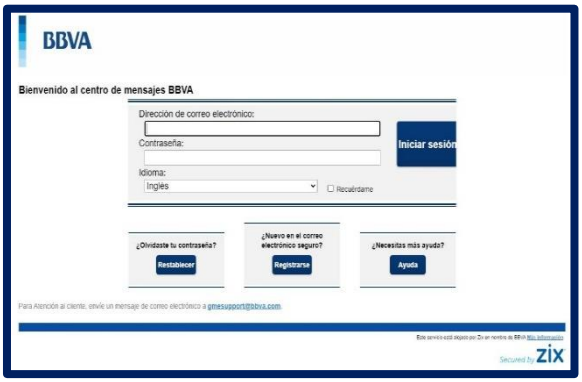


IMAGEN 1:

Sitio web fraudulenta del Banco BBVA, solicita a las víctimas registrar la dirección del correo electrónico, la contraseña y el idioma para iniciar sesión.

IMAGEN 2:

Luego de no poder iniciar sesión y darle click en "olvidaste la contraseña" requiere registrar la dirección del correo electrónico, el tipo de idioma y volver a introducir la contraseña para continuar

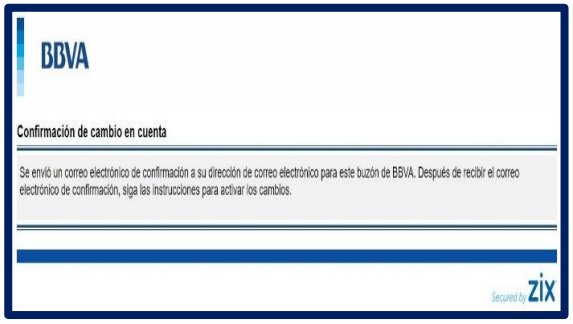


IMAGEN 3:

Por último, solicita a la víctima confirmar la cuenta, lo cual tendría que ingresar al correo electrónico y completar lo requerido por los atacantes, para luego informar a la víctima que ha ocurrido un error de autenticación; sin embargo, los datos fueron capturados por los cibercriminales.

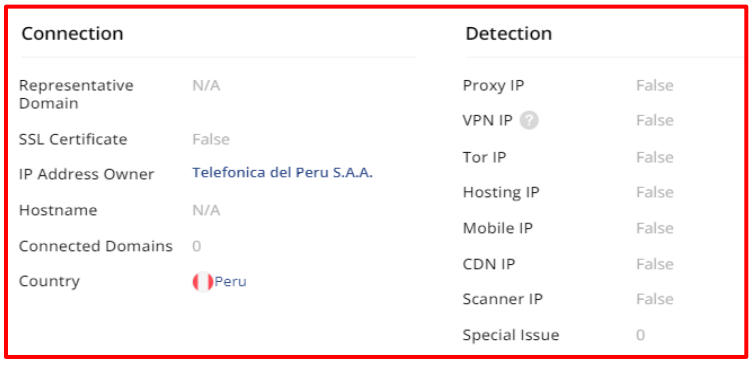
A. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD:**

a) Indicadores de compromisos:

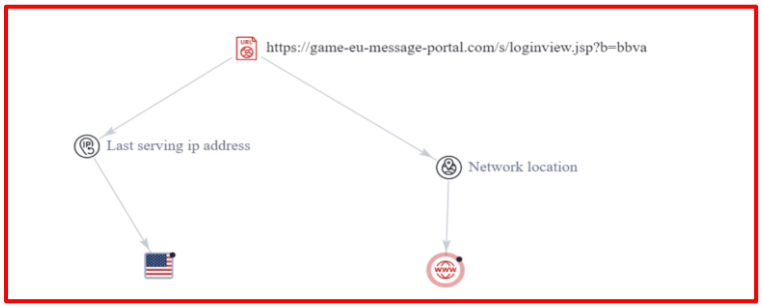
IV. URL: hxxps[:/]/game-eu-message-portal[.]com/s/loginview[.]jsp?b=bbva

V. SHA-256: 3720bde0c5e3502dba8ed4e701b01c7344fa289175e40807579a947323bcf2bd

VI. IP: 181[.]65[.]44[.]126



VII. Tipología:

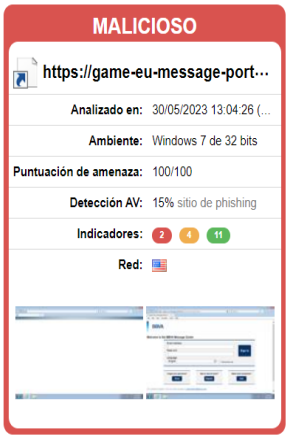


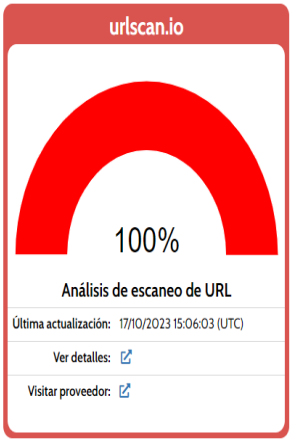
Se puede aprecia como la URL, esta alojada en un servidor ubicado en **EE.UU.**

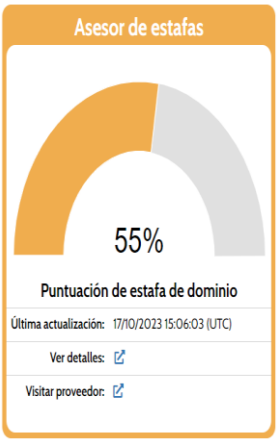
B. Se hallaron **14 proveedores** de seguridad que marcaron este dominio como malicioso.

Avira	Phishing	BitDefender	Malware
Criminal IP	Phishing	ESET	Phishing
Forcepoint ThreatSeeker	Phishing	Fortinet	Phishing
G-Data	Malware	Kaspersky	Phishing
Lionic	Phishing	Seclookup	Malicious
SOCRadar	Phishing	Sophos	Phishing
Trustwave	Phishing	VIPRE	Malicious

C. Otras detecciones:







D. Apreciación de la información:

- Es una técnica de ingeniería social basada en el engaño, que usan los ciberdelincuentes, con la finalidad de obtener información confidencial de los usuarios de forma fraudulenta y así apropiarse de las credenciales de acceso a los diferentes sitios web e información sensible.

E. Phishing:

- Es un término informático que distingue a un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza, para manipularla y hacer que realice acciones que no debería realizar.

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.