Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°177	Fecha: 30-07-2023
		Página: 4 de 10

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Nueva campaña de suplantación de la entidad bancaria de Banco de la Nación		
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

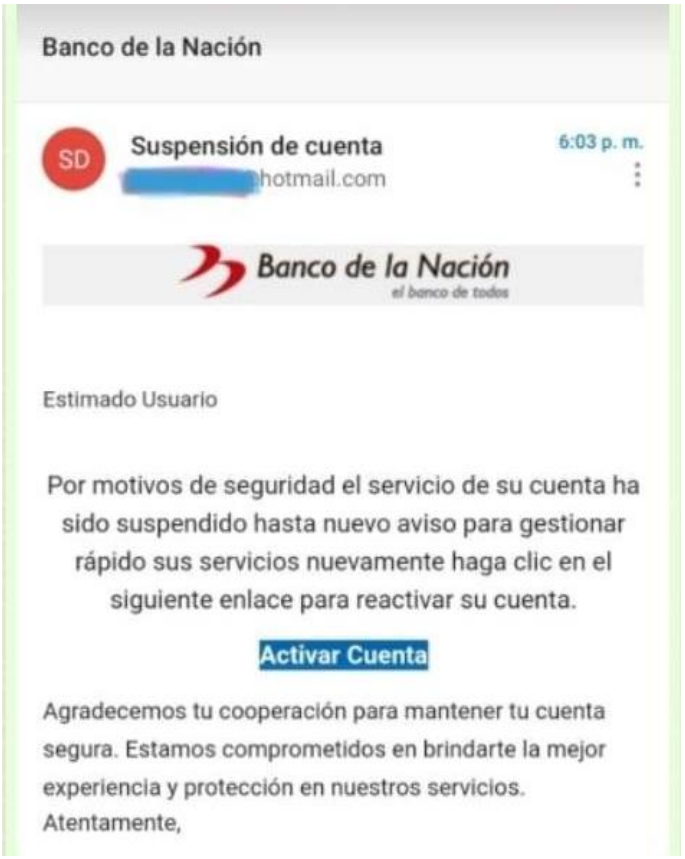
1. ANTECEDENTES:

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 (Phishing), simulado ser la entidad el Banco de la Nación, en cual tiene el objetivo de robar credenciales de acceso, datos personales y/o bancarios.

2. DETALLES:

El phishing bancario es una técnica que utilizan los ciberdelincuentes para suplantar la identidad de una persona o entidad legítima y obtener información personal y bancaria de sus víctimas, con el objetivo de apoderarse de dinero de sus cuentas y tarjetas.

Ciberdelincuentes vienen llevando campañas para robar credenciales de acceso a cuentas bancarias, a través de correos electrónicos fraudulentos, correos como los que se muestran en la imagen.



El objetivo del ciberdelincuente es que, a través de estos correos, redirigir a su víctima a una web similar al de la entidad bancaria (Banco de la Nación) y lograr obtener sus datos de accesos.

El phishing bancario puede afectar significativamente al sector bancario y a los clientes. Los bancos pueden perder dinero y sufrir daños en su reputación, mientras que los clientes pueden sufrir pérdidas financieras y daños a su crédito. Además, los clientes pueden perder su confianza en la banca en línea y en la seguridad de sus cuentas.

En caso de que un cliente sea víctima de phishing bancario, el banco puede ser considerado responsable en caso de que no haya implementado medidas de seguridad adecuadas o no haya informado al cliente sobre los riesgos del phishing.

Los clientes también pueden ser responsables si no han tomado medidas de seguridad adecuadas, como proteger sus contraseñas y no revelar información confidencial a través de correos electrónicos o sitios web falsos.

3. RECOMENDACIONES:

- Verificar que la URL corresponda al sitio web oficial del Banco de la Nación.
- Evitar seguir las instrucciones del correo electrónico y sitio web sospechoso o de dudosa procedencia.
- Evitar compartir la URL con amigos y/o familiares.
- Ingresar desde fuentes oficiales (www.bn.com.pe).

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

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°177	**Fecha: 27-07-2023** **Página: 7 de 10**

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de Alerta	Nueva campaña de suplantación de la entidad bancaria de BBVA		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medio de Propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Subfamilia	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:**

   Proceso de Phishing:

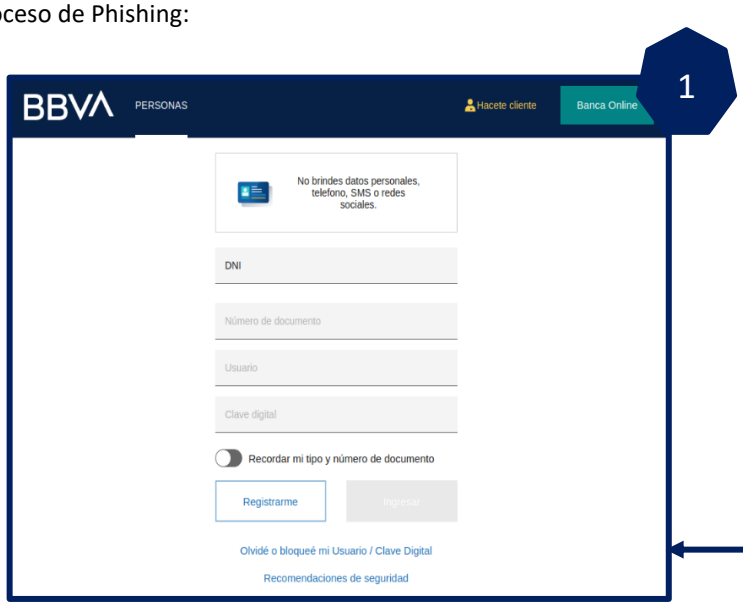
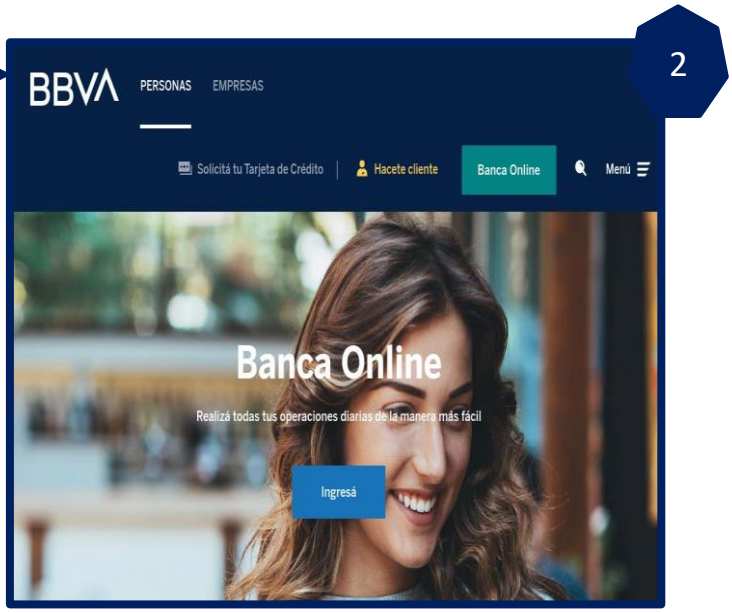
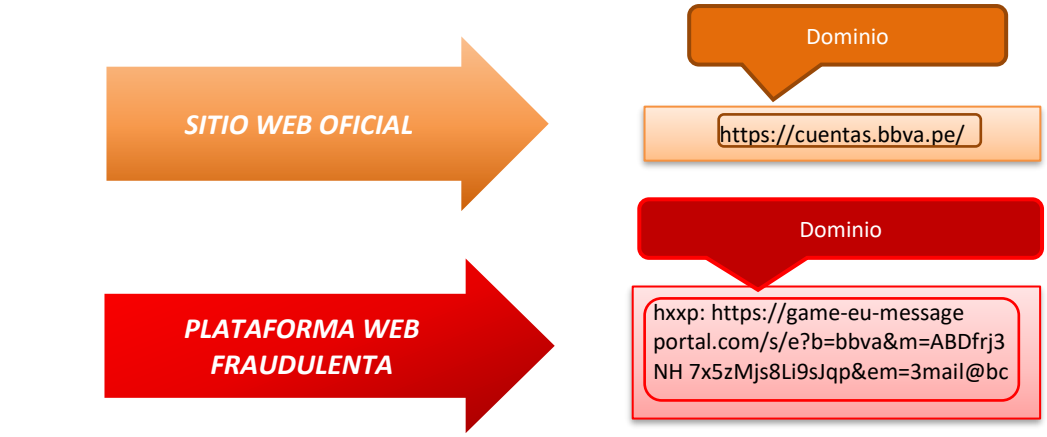


Imagen 1.
Plataforma web fraudulenta del Banco BBVA, solicita a la víctima el documento de identidad (DNI), el usuario y clave digital.

Imagen 2.
Después de completar lo requerido por los atacantes, dentro de unos segundos es redirigido, a la web oficial del banco BBVA, aludiendo un aparente error de autenticación; sin embargo, los datos fueron capturados por los cibercriminales.



A. Comparación del sitio web oficial y sitio web fraudulento del banco BBVA:



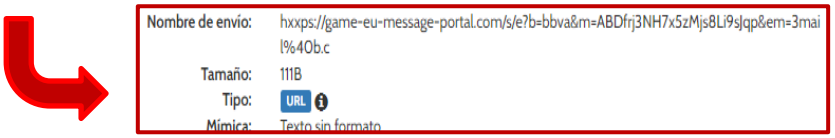
- Existe diferencia en el dominio de sitio web fraudulento, no coincide con el oficial.
- El sitio web fraudulento no posee el **PROTOCOLO SEGURO DE TRANSFERENCIA DE HIPERTEXTO (HTTPS)**, lo que hace que no puedan convencer a la víctima, a la hora de ingresar al sitio web.

B. Proveedores de seguridad informática alertan como **SUPLANTACIÓN DE IDENTIDAD – PHISHING**

ADMINUSLabs	Malicioso	AlphaSOC	Suplantación de identidad
Avira	Suplantación de identidad	BitDefender	Malware
CRDF	Malicioso	CyRadar	Malicioso
G-datos	Malware	kaspersky	Suplantación de identidad
Leonico	Malicioso	Búsqueda segura	Malicioso
VIPRE	Malicioso	raíz web	Malicioso

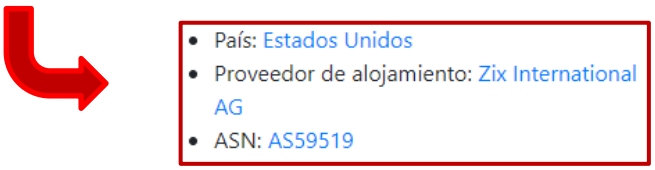
C. Indicadores de compromiso:

- URL: https://game-eu-message-portal[.]com/s/e?b=bbva&m=ABDfrj3NH7x5zMjs8Li9sJqp&em=3mail@bc

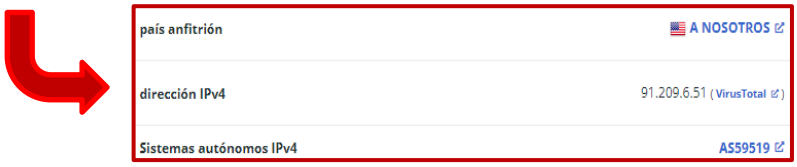


- Dominio: juego-eu-mensaje-portal[.]com

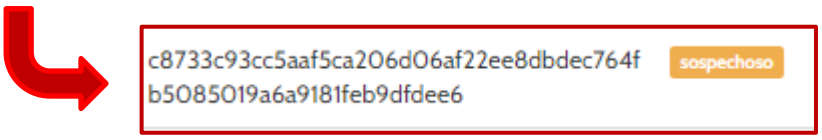
- Proveedor de alojamiento: Cloudflarenet



- IP: 188[.]114[.]96[.]3



- SHA – 256: c8733c93cc5aaf5ca206d06af22ee8dbdec764fb5085019a6a9181feb9dfdee6



D. Otros resultados del análisis:

3. RECOMENDACIONES:

- Verificar detalladamente la URL, que corresponda al sitio web oficial del banco BBVA.
- Evitar seguir las instrucciones de sitio web sospechoso o de dudosa procedencia.
- Mantener el antivirus actualizado, ya que es la primera barrera ante posibles ataques cibernéticos.
- Evitar compartir la URL con amigos y/o familiares.
- Ingresar desde fuentes oficiales (www.bbva.pe).

Fuente de Información	Análisis propio de redes sociales y fuente abierta