

	<b>ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 135</b>			<b>Fecha: 09-06-2023</b>
				<b>Página 8 de 11</b>
Componente que reporta	<b>DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ</b>			
Nombre de la alerta	Nueva campaña de suplantación de 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 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 avanzados ataques cibernéticos, por medio de envíos de correos electrónicos fraudulentos, o también conocidos como Phishing, simulando ser la entidad bancaria BBVA, en cual tiene el objetivo de robar credenciales de acceso, datos personales y/o bancarios.
2. Detalles del proceso de Phishing:



**1**

**Imagen 1.**

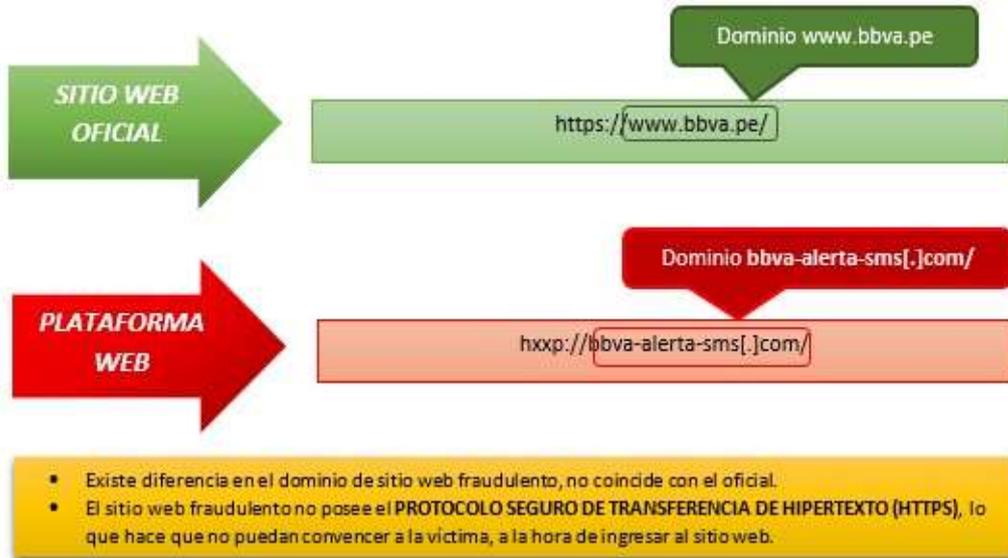
Plataforma web fraudulenta del Banco BBVA, solicita a la víctima el documento de identidad (DNI), el usuario y clave digital.

**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.



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



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

alphaMountain.ai	⚠ Suplantación de identidad	Avira	⚠ Suplantación de identidad
BitDefender	⚠ Suplantación de identidad	CRDF	⚠ Malicioso
CyRadar	⚠ Malicioso	ESET	⚠ Suplantación de identidad
Fortinet	⚠ Suplantación de identidad	G-datos	⚠ Suplantación de identidad
Navegación segura de Google	⚠ Suplantación de identidad	Seguridad Heimdal	⚠ Suplantación de identidad
Leonico	⚠ Suplantación de identidad	Búsqueda segura	⚠ Malicioso
Sophos	⚠ Suplantación de identidad	Inteligencia de amenazas de Viettel	⚠ Suplantación de identidad
VIPRE	⚠ Malicioso	raiz web	⚠ Malicioso
Buscador de amenazas de Forcepoint	⚠ Sospechoso	Abusix	✅ Limpio

5. Indicadores de compromiso:

a) URL: hxxp:// bbva-alerta-sms[.]com

Nombre de envío: hxxps://bbva-alerta-sms.com/  
 Tamaño: 52B  
 Tipo: URL  
 Mimica: Texto sin formato.  
 Sistema operativo: ventanas  
 Último análisis antivirus: 08/06/2023 13:29:51 (UTC)  
 Último informe de Sandbox: 08/06/2023 13:34:57 (UTC)

b) Dominio: bbva-alerta-sms[.]com

Prueba	
⚠	Registro DMARC publicado
⚠	Registro DNS publicado
⚠	Política DMARC no habilitada

c) Proveedor de alojamiento: Cloudflarenet

- Última comprobación (UTC): 2023-06-08 07:05
- Visto por primera vez (UTC): 2023-05-16 06:13
- IP: 188.114.96.2
- País: Países Bajos
- Proveedor de alojamiento: CLOUDFLARENET
- ASN: AS13335
- Certificado ILS: E1

d) IP: 188[.]114[.]96[.]13



Dirección IPv4	104.21.46.138 (VirusTotal #1)
Sistemas autónomos IPv4	AS13335 #2
Dirección IPv6	2806:4700:3030:0:0:0:6815:2e8a
Sistemas autónomos IPv6	AS13335 #2

e) SHA – 256: c44b3da1c3752dc73d73f6bf37d871884181d809ab1d921792dc5a52a1aca579



shopping_frame_other.p	45e167fe1542b3a1388484cb909810a7ef35e4dc25a8c38a144ac1038	Ingresar amenaza específica
monedero.html	D10239e87ec649914efbc9e2576e83ee70c338889089108c4890e95146d9b5	Ingresar amenaza específica
tolentec-cantibunde.p	c44b3da1c3752dc73d73f6bf37d871884181d809ab1d921792dc5a52a1aca579	Examinar
uief_httpbbva-alerta-sms.com	c982409f7431e440b6a30c987469145f1d2584e7363765eeebded7aee906	Ingresar amenaza específica

6. Otros resultados del análisis:



7. Cómo funciona el Phishing:

- Los correos electrónicos incluyen enlaces a sitios web preparados por los ciberdelincuentes en los que solicitan información personal.
- Medios de propagación del Phishing: WhatsApp, telegram, redes sociales, SMS entre otros.
- Los ciberdelincuentes intentan suplantar a una entidad legítima (organismo público o privado, entidad financiera, servicio técnico, etc.)

8. Referencia:

- Phishing o suplantación de identidad: Es un método que los ciberdelincuentes, utilizan para engañar a los usuarios para conseguir que revele información personal, como contraseñas, datos de tarjetas de créditos, números de cuentas bancarias, entre otros.

9. 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 ).

Fuentes de información	Análisis propio de redes sociales y fuente abierta
------------------------	--