	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°280	Fecha: 23-11-2023
		Página: 10 de 12

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 la "Caja Trujillo"		
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 que suplanta la entidad bancaria de la "Caja Trujillo", con el objetivo robar credenciales de acceso, datos personales y bancarios.

2. **DETALLES:**

Imagen 1.- Solicitud para ingresar el Nº de tarjeta de la víctima.

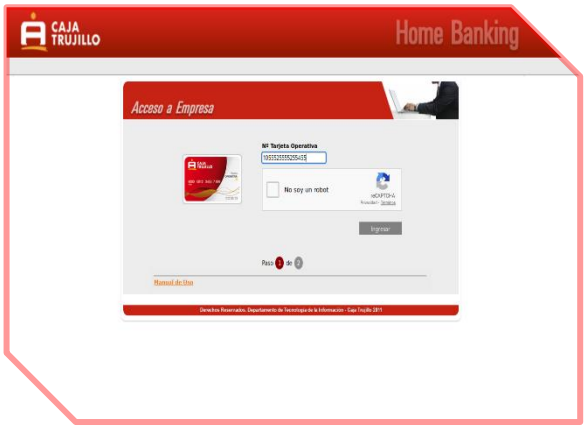


Imagen: 2.- Luego de haber ingresado el Nº de la tarjeta, solicita ingresar clave de internet (6 dígitos)

Imagen: 3.- Como paso final de la estafa, aparenta cargar la información proporcionada en los puntos anteriores.

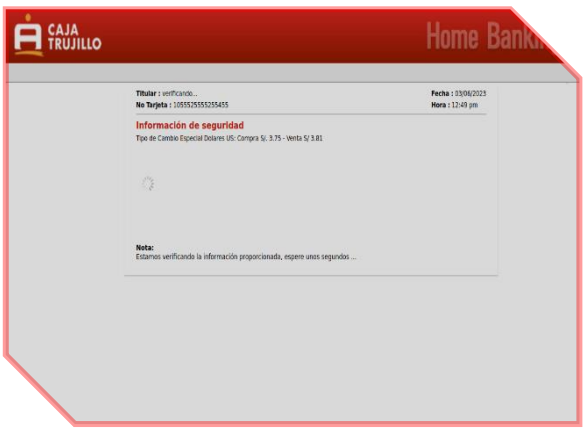
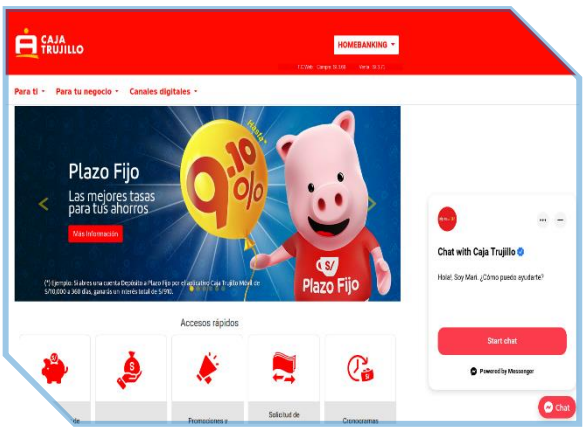
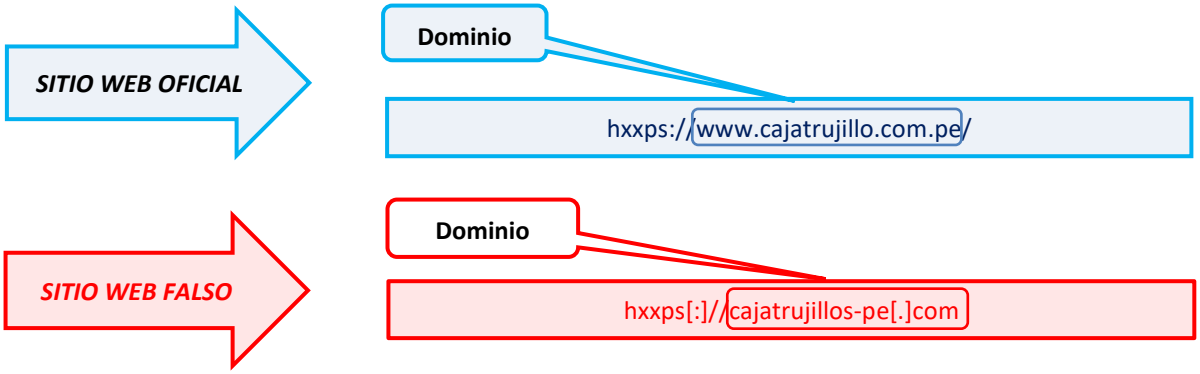


Imagen: 4.- Pasado unos 20 segundos, es redirigido al sitio web oficial de la entidad bancaria de la "Caja Trujillo", aludiendo un aparente error de autenticación, sin embargo, los datos fueron capturados, por los ciberdelincuentes.



A. Comparación del sitio web oficial y el sitio web fraudulento de la "Caja Trujillo":



- Existe diferencia entre los dominios del sitio web oficial y el sitio web fraudulento.
- Ambos sitios webs poseen el **PROTOCOLO SEGURO DE TRANSFERENCIA DE HIPERTEXTO (HTTPS),** lo cual hace convincente a las víctimas al momento de ingresar y proporcionar sus datos sensibles.

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

Análisis de proveedores de seguridad			
alfaMontaña.ai	Suplantación de identidad	Avira	Suplantación de identidad
BitDefender	Suplantación de identidad	CyRadar	Malicioso
Fortinet	Suplantación de identidad	Datos G	Suplantación de identidad
Kaspersky	Suplantación de identidad	leonico	Malicioso
Sofos	Suplantación de identidad	raíz web	Malicioso

- Indicadores de compromiso:
  - URL: hxxps[:]//cajatrujillos-pe[.]com/
  - Dominio: cajatrujillos-pe[.]com
  - SHA-256: c60aac0876aaf8f799da5979052c75f557bf678be6a1e0aed69e305797c20a02
  - Dirección IP: 208[.]91[.]197[.]13
  - Tamaño: 2.14 KB

C. 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.

3. RECOMENDACIONES:

- Evitar hacer clic en enlaces sospechosos que no sea el sitio web oficial.
- Verificar detalladamente la URL, que corresponda al sitio web oficial.
- 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.

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