	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 149		Fecha: 25-06-2023
			Página 5 de 8
Componente que reporta	DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ		
Nombre de la alerta	Nueva Campaña de Phishing dirigidas a usuarios de 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	C	Código de Sub familia	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 una campaña de ataques de suplantación de identidad (Phishing), dirigidos a usuarios de la entidad bancaria de la Caja Trujillo, con el objetivo robar credenciales de acceso, datos personales y bancarios.
2. Proceso Phishing o suplantación de identidad:

Imagen 1.- Solicitud para ingresar el N° de tarjeta de la víctima.



Imagen: 2.- Luego de haber ingresado el N° de la tarjeta, solicita ingresar clave de internet (6 dígitos)



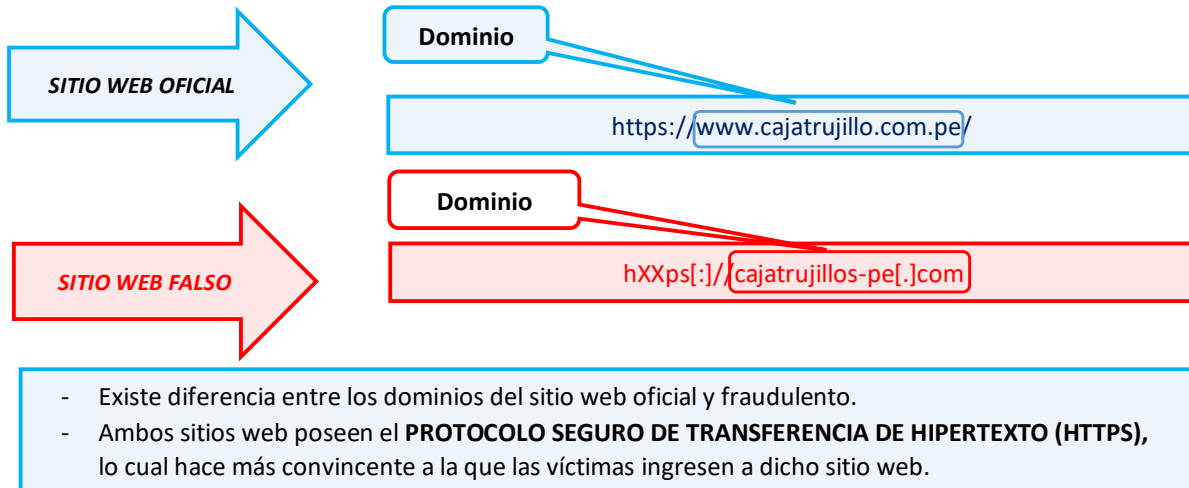
Imagen: 3.- Como paso final aparenta cargar la información proporcionada en los puntos anteriores.



Imagen: 4.- Pasado unos 10 segundos, es redirigido al sitio oficial de la entidad bancaria “Caja Trujillo”, aludiendo un aparente error de autenticación, sin embargo, los datos fueron capturados, por los ciberdelincuentes.



3. Comparación del sitio web oficial y sitio web fraudulento de la entidad bancaria de la Caja Trujillo:



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

DETECCIÓN	DETALLES	ENLACES	COMUNIDAD
alphafontain al	Suplantación de identidad	Anti-AVL	Malicious
Avira	Suplantación de identidad	BitDefender	Malware
CROWD	Malicious	CyRadar	Malicious
Fortinet	Malware	G-data	Malware
Leontix	Malicious	Sophos	Malware
Inteligencia de amenazas de Viettel	Malicious	vuz web	Malicious

- Indicadores de compromiso:
 - URL: `hXXps[:]//cajatrujillos-pe[.]com/`
 - Dominio: `cajatrujillos-pe[.]com`
 - SHA-256: `c0b46041af8dd2f3419c9d4ea69f4b82de79a5df767c69b208804abd8e03fd3a`
 - Dirección IP: `172[.]167[.]128[.]90`
 - Tamaño: 6.78 KB
- Otros resultados del análisis:

MALICIOSO
https://cajatrujillos-pe.com/
 Analizado en: 22/06/2022 15:06:41 (UTC)
 Ambiente: windows 7 32 bits
 Puntaje de amenaza: 75/100
 Detección AV: 13% Sitio de phishing
 Indicadores: [3] [2] [1]
 Red: [US]

malicioso
 Puntaje de amenaza: 75/100
 Detección AV: 5%
 #suplantación de identidad

5. Como 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.)

6. 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.

7. Recomendaciones:

- Evitar hacer clic en enlaces sospechosos que no sea el sitio oficial de la entidad bancaria Caja Trujillo
- 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