	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°155	Fecha: 01-07-2023
		Página: 5 de 10

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Detección de falso servicio del correo electrónico de 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	G02
Clasificación temática familia	Fraude		

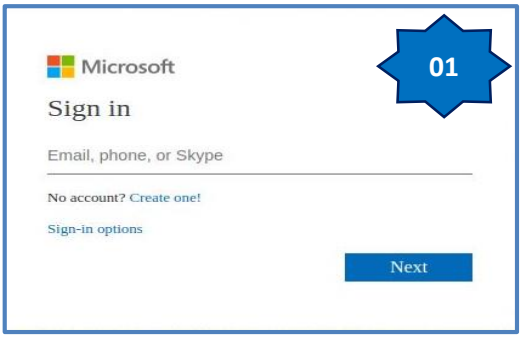
Descripción

1. ANTECEDENTES:

A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que actores de amenazas vienen realizando una campaña de Phishing, activando un falso servicio del correo electrónico de la compañía Microsoft (Outlook, Hotmail, etc.), con la finalidad de obtener las credenciales de acceso (correos y contraseñas) de los usuarios de la compañía tecnológica.

2. DETALLES:

El proceso del Phishing es el siguiente:



Paso N.º 01

Sitio web fraudulento solicita a la víctima registrar el correo electrónico, teléfono o Skype, para acceder al servicio en la web de la compañía Microsoft (Outlook, Hotmail, etc.)

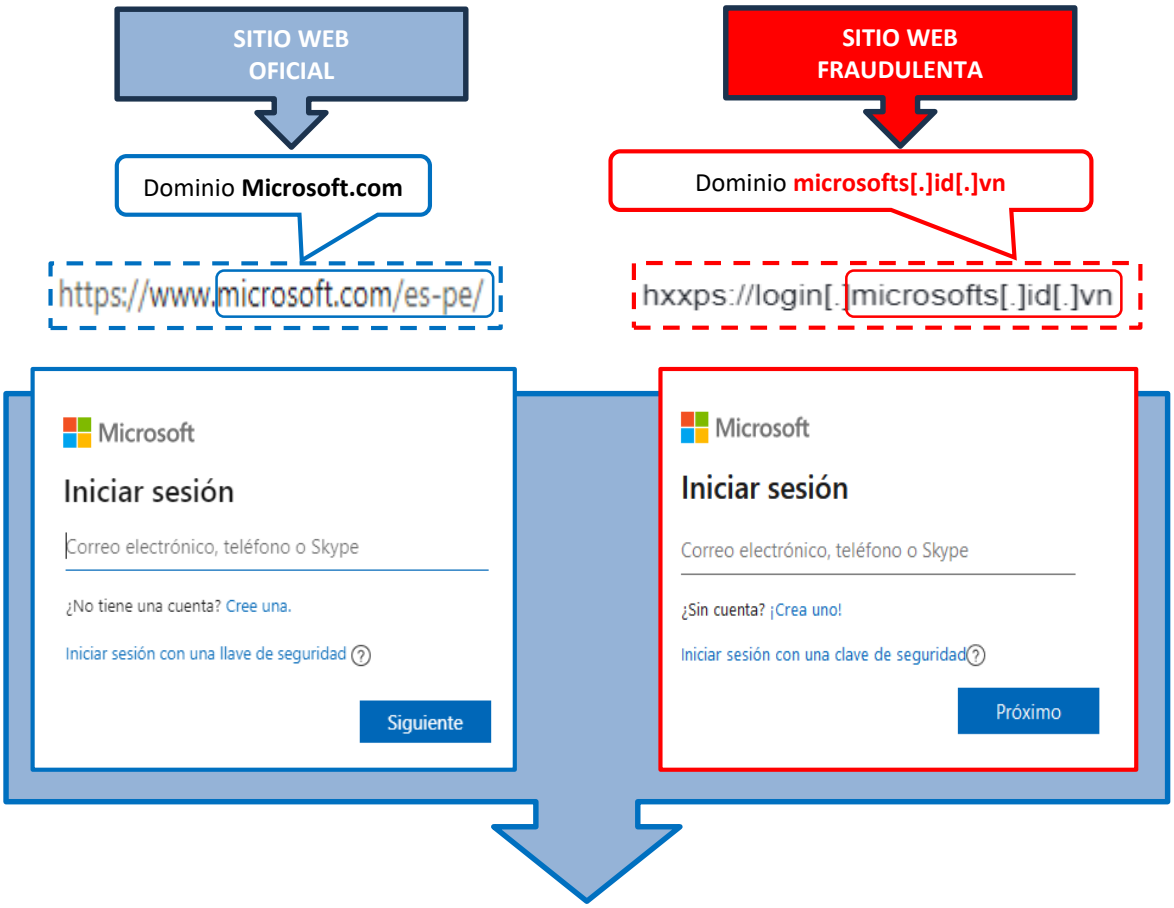
Paso N.º 02

Luego de registrar el correo electrónico, requiere la contraseña de acceso para iniciar sesión del sitio web de Microsoft.

Paso N.º 03

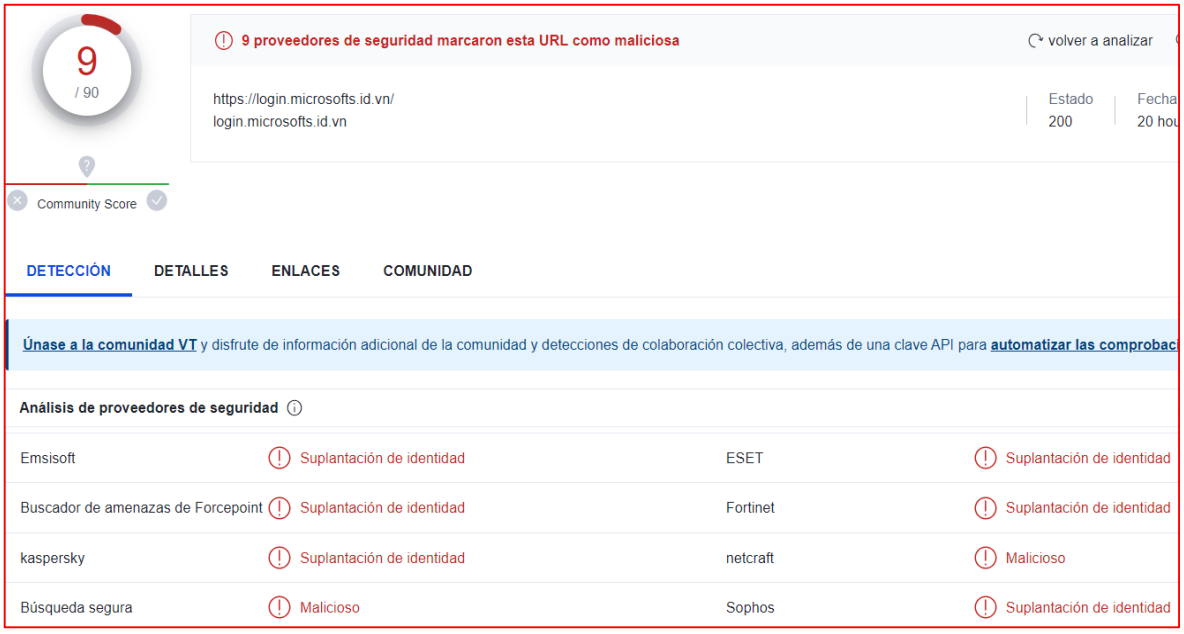
Por último, después de unos segundos le redirige al servicio del correo electrónico de la compañía Microsoft oficial aparentando un error de autenticación, sin embargo, los datos fueron capturados por los cibercriminales.

A. Comparación del sitio web oficial y fraudulento.



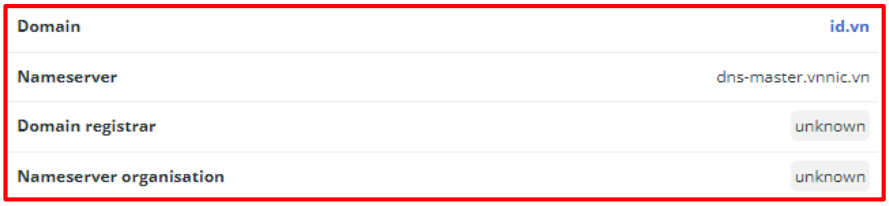
- Existe una diferencia entre la URL original y la URL fraudulenta.
- La URL del sitio web fraudulento posee protocolo de seguridad de red (https)
- Existe una similitud entre ambas páginas en imagen, fondo y color.

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

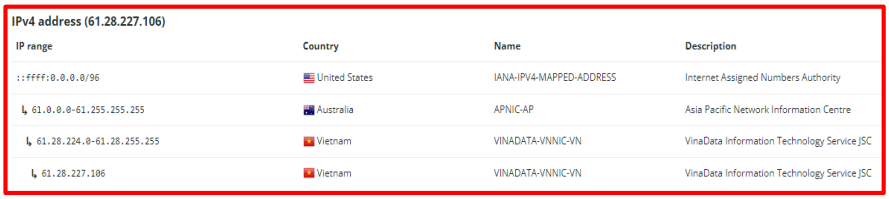


C. Indicadores de compromiso (IoC)

- **Dominio : id.vn**



- **IP : 61[.]28[.]227[.]106**



- **Servidor : Apache/2.4.52 (Ubuntu)**
- **SHA-256 : 1d4bb1655352451514c25b8eb923b711f6730a900c8fa1133acb128c75ed2444**

D. Otras detecciones:

E. Apreciación de la información:

- La presente campaña de Phishing permite a los actores de amenazas obtener las credenciales de acceso del servicio del correo electrónico en la web de la compañía Microsoft (Outlook, Hotmail, etc.).
- La propagación del sitio web fraudulento se realiza mediante envió masivos de email, adjuntando enlaces de sitios web fraudulentos con la finalidad de obtener información sensible de las víctimas; asimismo, a través de las aplicaciones de mensajería instantánea entre ellos WhatsApp, Telegram, Messenger, etc. y mensajes de textos SMS.

3. RECOMENDACIONES:

- Verificar detalladamente las URL de los sitios web.
- No abrir o descargar archivos sospechosos.
- No seguir las instrucciones de sitio web sospechoso.
- No aceptar permisos de instalación de archivos desconocidos o dudosa procedencia.
- Mantener actualizado el sistema operativo y aplicaciones del equipo de cómputo.
- Mantener actualizado el sistema antivirus (el antivirus debe ser licenciado).
- Comunicar a la entidad financiera si ha realizado un registro de acceso en un sitio web sospechoso.

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

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°155	Fecha: 02-07-2023
		Página: 8 de 10

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	G	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 Nº de tarjeta de la víctima.

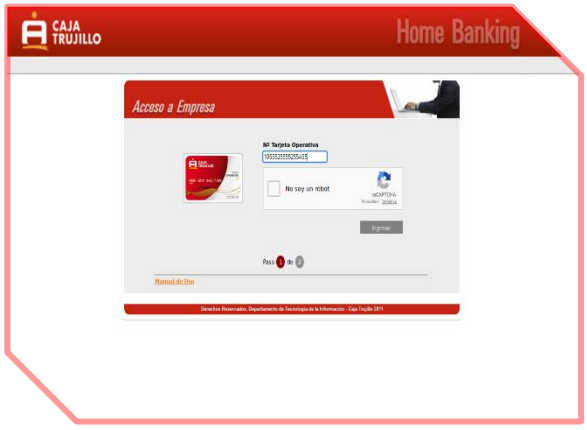


Imagen: 2.- Luego de haber ingresado el Nº de la tarjeta, solicita ingresar clave de internet (6 dígitos)

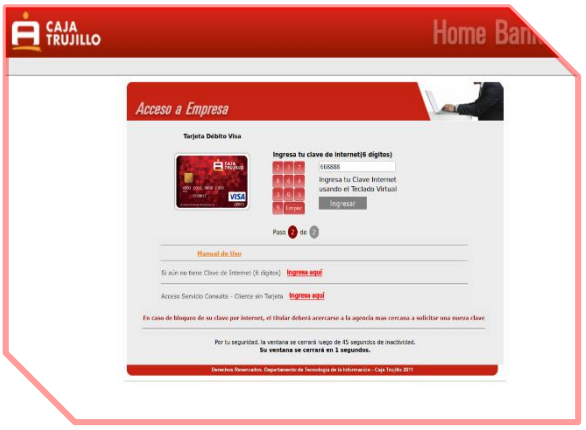


Imagen: 3.- Como paso final aparenta cargar la información proporcionada en los puntos anteriores.

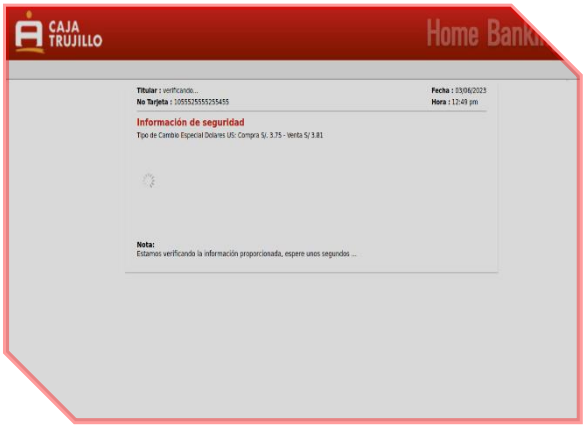
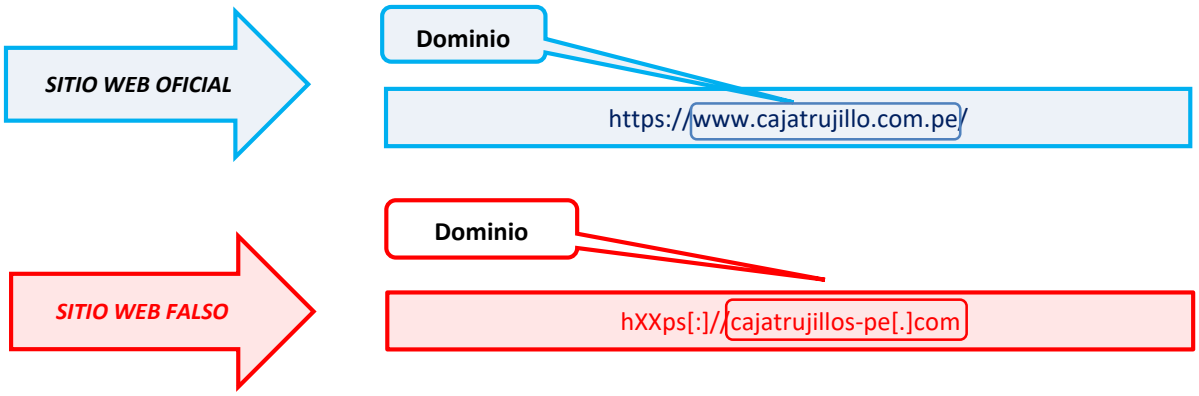


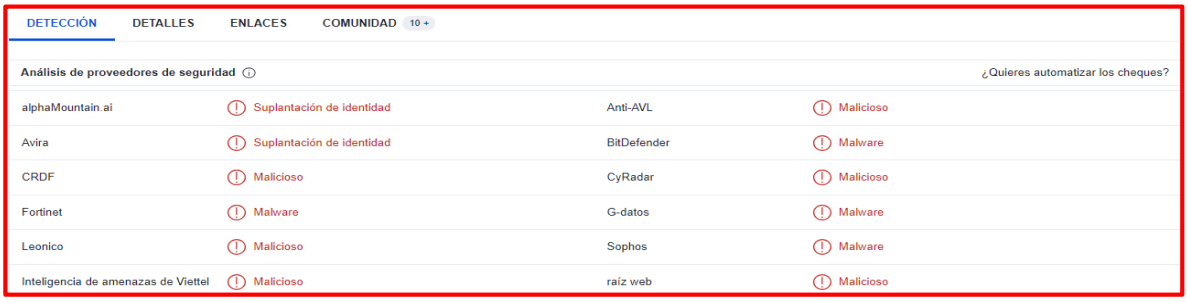
Imagen: 4.- Pasado unos 10 segundos, es redirigido al sitio oficial de la entidad bancaria "Caja Trujillo", aludiendo un aparente error de autenticación, sin embargo, los datos fueron capturados, por los ciberdelincuentes.

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



- Existe diferencia entre los dominios del sitio web oficial y fraudulento.
- Ambos sitios web poseen el **PROTOCOLO SEGURO DE TRANSFERENCIA DE HIPERTEXTO (HTTPS),** lo cual hace más convincente a la que las víctimas ingresen a dicho sitio web.

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



DETECCIÓN | DETALLES | ENLACES | COMUNIDAD 10+

Análisis de proveedores de seguridad ⓘ — ¿Quieres automatizar los cheques?

alphaMountain.ai	Suplantación de identidad	Anti-AVL	Malicioso
Avira	Suplantación de identidad	BitDefender	Malware
CRDF	Malicioso	CyRadar	Malicioso
Fortinet	Malware	G-datos	Malware
Leonico	Malicioso	Sophos	Malware
Inteligencia de amenazas de Viettel	Malicioso	raíz web	Malicioso

- Indicadores de compromiso:
  - URL: hXXps[:]//cajatrujillos-pe[.]com/
  - Dominio: cajatrujillos-pe[.]com
  - SHA-256: c0b46041af8dd2f3419c9d4ea69f4b82de79a5df767c69b208804abd8e03fd3a
  - Dirección IP: 172[.]67[.]128[.]90
  - Tamaño: 6.78 KB

5. 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.

6. 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