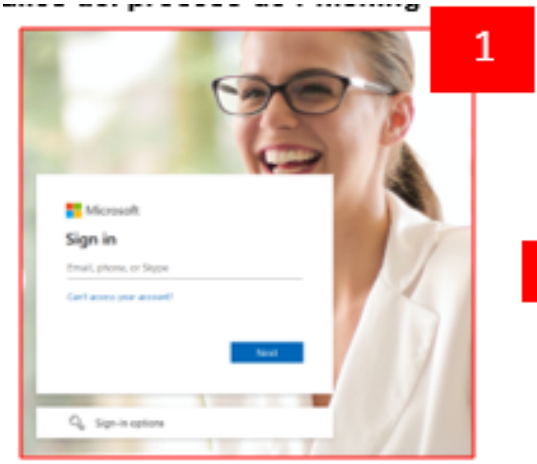
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 131	Fecha: 05-06-2023
		Página 6 de 13

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

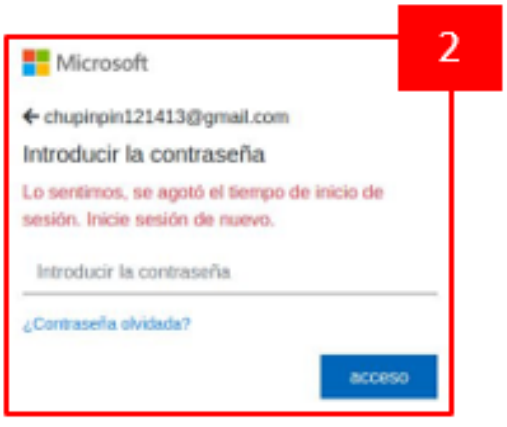
Descripción

1. 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 del proceso de Phishing.



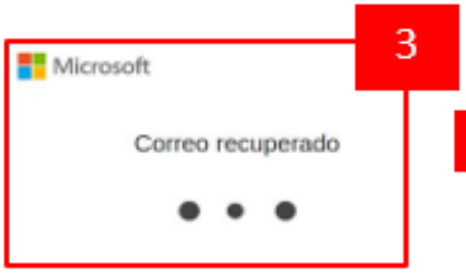
Paso N.º 01

El sitio web fraudulento de Microsoft, el atacante solicita a la víctima que registre el correo electrónico, el número de teléfono o de Skype, para acceder al servicio en la web de la compañía Microsoft (Outlook, Hotmail, etc.)



Paso N.º 02

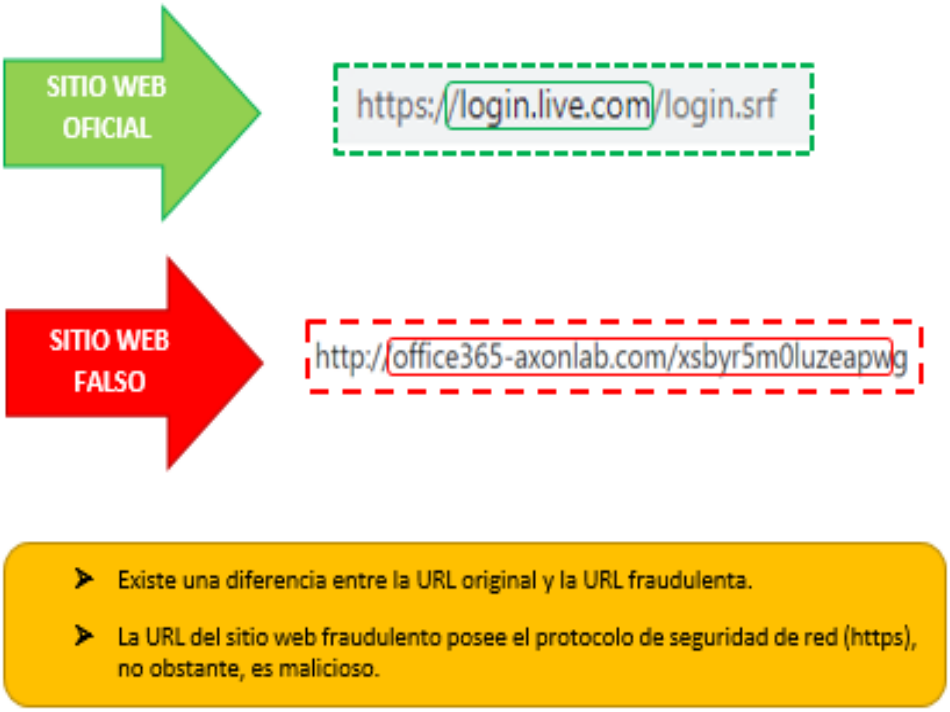
Una vez registrado el usuario y hecho clic en <Próximo>, requiere ingresar la contraseña para continuar con el acceso.



Paso N.º 03

Luego de completar las credenciales de acceso y darle clic en <Acceso> se muestra que el correo se ha recuperado, pero el atacante engaña a la víctima diciendo que no ha podido recuperar por un error.

3. La Comparación del sitio web oficial y fraudulento.

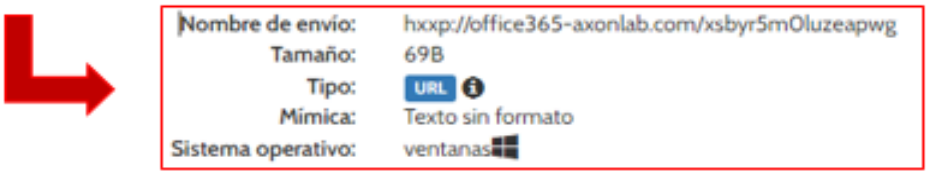


4. Proveedores de seguridad informática alertan como SUPLANTACIÓN DE IDENTIDAD siendo (13) trece de ellas, MALICIOSO (07) siete y MALWARE (02) dos. - PHISHING.

alphaMountain.ai	Suplantación de identidad	AlphaSOC	Suplantación de identidad
Anti-AVL	Malicioso	Avira	Suplantación de identidad
BitDefender	Malware	certego	Suplantación de identidad
CRDF	Malicioso	CyRadar	Malicioso
Emsisoft	Suplantación de identidad	ESET	Suplantación de identidad
Buscador de amenazas de Forcepoint	Suplantación de identidad	Fortinet	Suplantación de identidad
G-datos	Malware	Seguridad Heimdal	Suplantación de identidad
kaspersky	Suplantación de identidad	Leonico	Suplantación de identidad
netcraft	Malicioso	Base de datos de phishing	Suplantación de identidad
Búsqueda segura	Malicioso	Sophos	Suplantación de identidad
VIPRE	Malicioso	raíz web	Malicioso

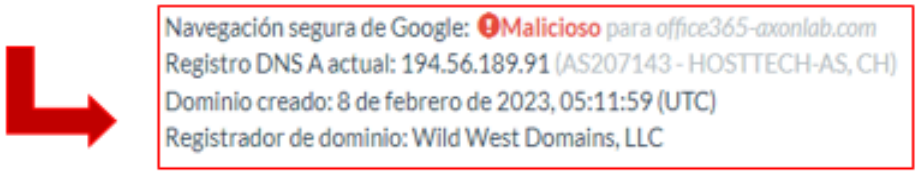
5. Indicadores de compromiso (IoC)

a) URL : hxxps://office365-axonlab[.]com/xsbyr5m0luzeapwg

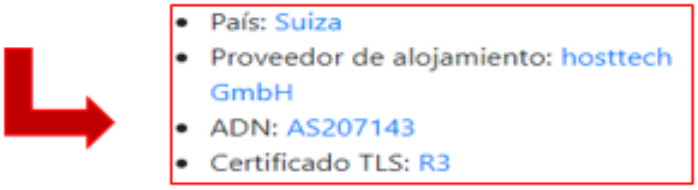


b) Dominio : office365-axonlab[.]com

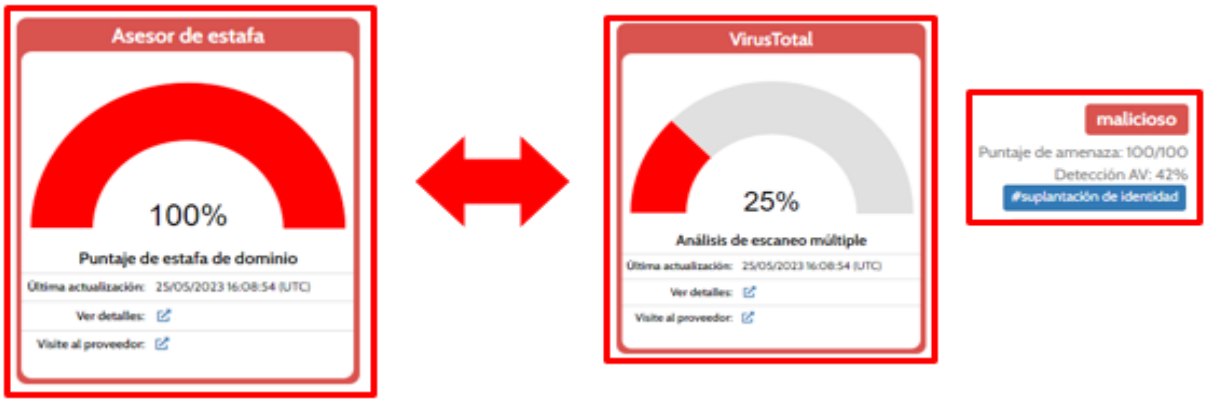
c) IP : 194[.]56[.]189[.]91



d) Proveedor de alojamiento : Hosttech



6. Otras detecciones:



7. Apreciación de la información:

a) 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.).

b) 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, dicho enlace malicioso, es enviado a través de las plataformas digitales como el WhatsApp, Telegram, Messenger y mensajes de textos SMS.

8. Concepto de MICROSOFT:

   a) Es una compañía que ofrece programas y soluciones ofimáticas, que favorecen las áreas profesionales, estudiantiles y domésticas. Por lo que una cuenta de Microsoft es una dirección de correo electrónico y una contraseña que usa con Outlook.com, Hotmail, Office, OneDrive, Skype, Xbox y Windows. Si crea una cuenta de Microsoft, puede usar cualquier dirección de correo como el nombre de usuario, incluidas las direcciones de Outlook.com, Yahoo! o Gmail.

9. Algunas Recomendaciones:

   a) Verificar detalladamente las URL de los sitios web
   b) No abrir o descargar archivos sospechosos.
   c) No seguir las instrucciones de sitio web sospechoso.
   d) Mantener el antivirus actualizado.
   e) Descargar aplicaciones de fuentes confiables.
   f) Realizar las actualizaciones correspondientes desde fuentes originales.

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

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 131	**Fecha: 05-06-2023**
		Página 10 de 13

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 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 ataques de suplantación de identidad o también conocido como 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:

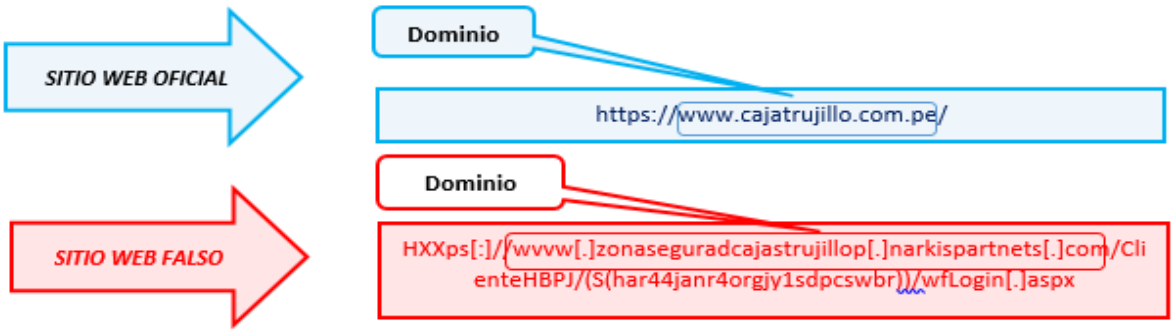
Imagen 1.- Solicitud para ingresar el Nº de tarjeta de la víctima.

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.

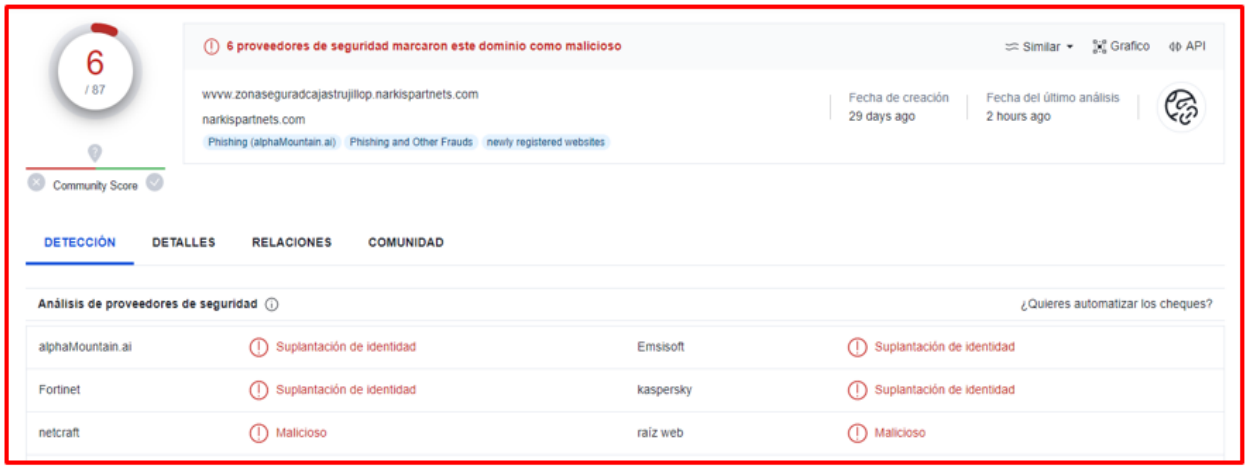
Imagen: 4.- Pasado unos 10 segundos, es redirigido al sitio oficial de la entidad bancaria "Caja Trujillo", aludiendo un aparente error de autenticación, sin embargo, los datos fueron capturados, por los ciberdelincuentes

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



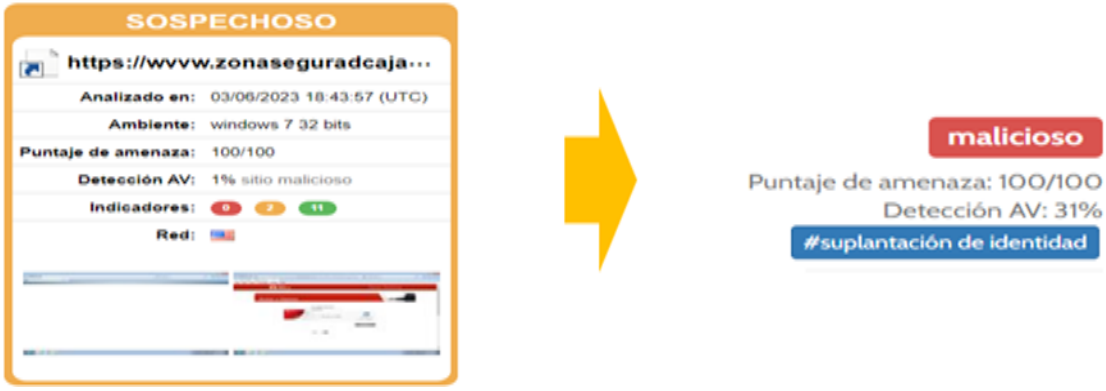
- Existe diferencia entre los dominios del sitio web oficial y fraudulento.
- Ambos sitios web poseen el **PROTOCOLO SEGURO DE TRANSFERENCIA DE HIPERTEXTO (HTTPS),** lo cual hace más convincente a la que las víctimas ingresen a dicho sitio web.

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



- Indicadores de compromiso:
  - URL: hxxps://wvvw[.]zonaseguradcajastrujillop[.narkispartnets[.]com/ClienteHBPJ/(S(har44janr4orgjy1
  - sdpcswbr))/wfLogin[.]aspx
  - Dominio: wvvw[.]zonaseguradcajastrujillop[.]narkispartnets[.]com
  - SHA-256: e89d48a10922e6242c95c6cfa9e0ac433d6c390ce73be06eb831d280537b46f5
  - Dirección IP: 173[.]236[.]155[.]72
  - Tamaño: 6.33 KB

- Otros resultados del análisis:



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 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.

Fuentes de información	▪ Análisis propio de redes sociales y fuente abierta.