	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°207	Fecha: 03-09-2023
		Página: 7 de 13

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Campaña de Phishing, suplantando la identidad del Banco Santander		
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:

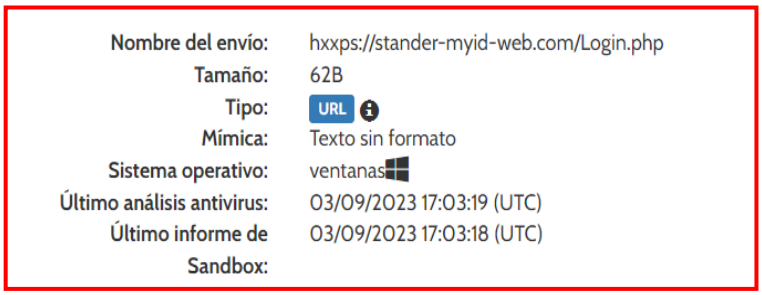
A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes vienen llevando a cabo una campaña de Phishing que se difunde en los diferentes navegadores web, dirigido a los clientes y/o usuarios del Banco Santander; el cual, mediante la creación de un sitio web similar al original, solicitan a las posibles víctimas a iniciar sesión en la Banca Por Internet de la entidad bancaria, a fin de robar información bancaria, como credenciales de inicio de sesión (identificación personal y el número de seguridad).

2. DETALLES:

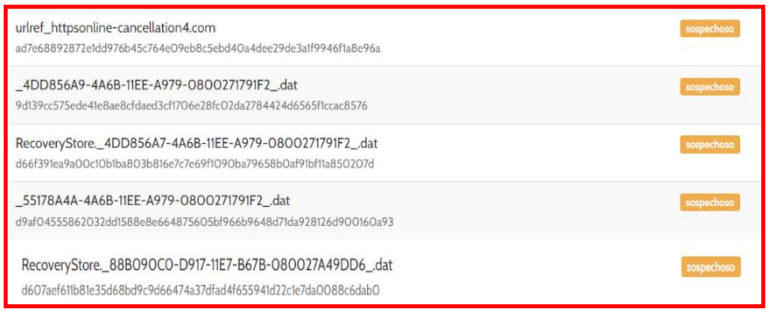
A. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD:**

a) Indicadores de compromisos:

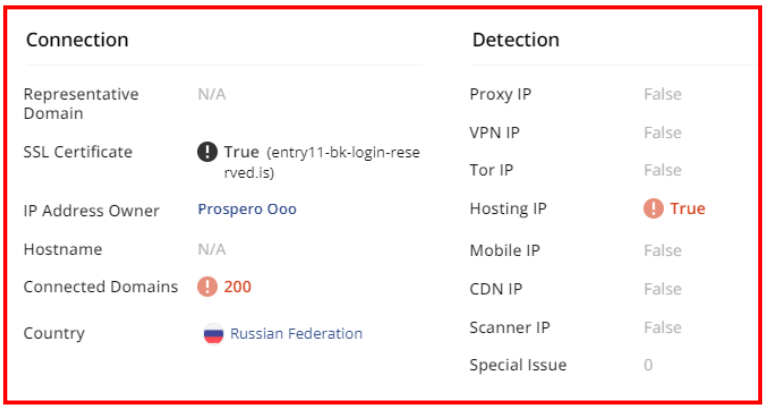
I. URL: |[:]//stander-myid-web[.]com/Login[.]php



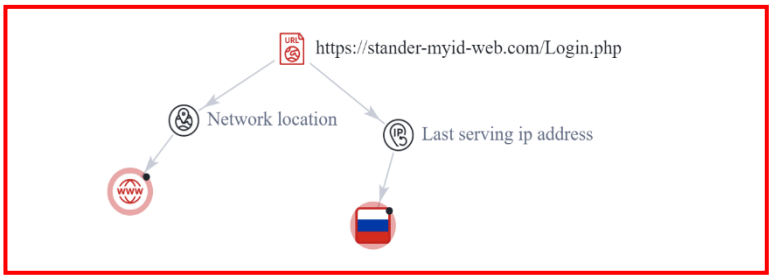
II. SHA-256: dc46ce46c9f5c78a9ceb99ef1eb655b9994b2d4c51440c166fe128d7fcff7e8d



III. IP: 91[.]215[.]85[.]14



IV. TIPOLOGÍA:

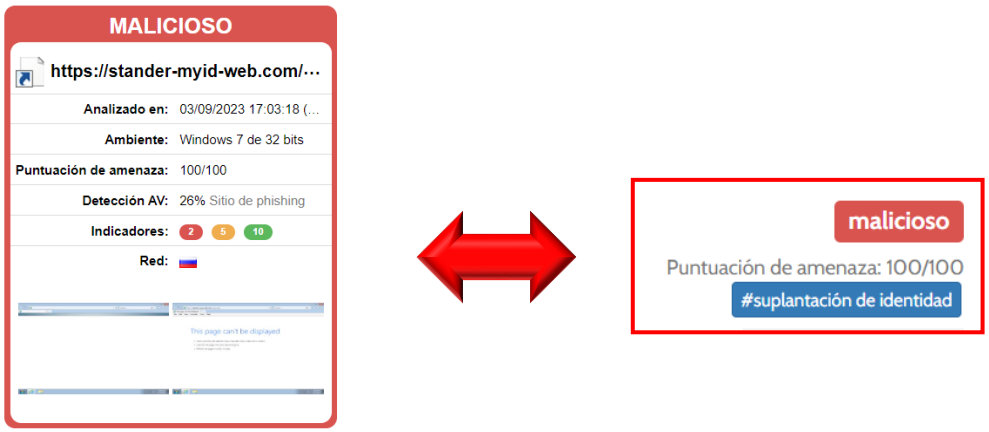


Se puede aprecia como la URL, esta alojada en un servidor ubicado en RUSIA.

B. Se hallaron **24 proveedores** de seguridad que marcaron este dominio como malicioso.

AlphaSOC	Phishing	Avira	Phishing
BitDefender	Phishing	Cluster25	Phishing
CRDF	Malicious	CyRadar	Malicious
Emsisoft	Phishing	ESET	Phishing
Forcepoint ThreatSeeker	Phishing	Fortinet	Phishing
G-Data	Phishing	Google Safebrowsing	Phishing
Kaspersky	Phishing	Lionic	Phishing
Netcraft	Malicious	OpenPhish	Phishing
Phishing Database	Phishing	SafeToOpen	Phishing
Seclookup	Malicious	Segasec	Phishing
Sophos	Malware	Trustwave	Phishing
VIPRE	Malicious	Webroot	Malicious

C. Otras detecciones:



D. 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 legitima (organismo público o privado, entidad financiera, servicio técnico, etc.).

3. RECOMENDACIONES:

- Evitar acceder a enlaces que llegan inesperadamente por correo electrónico u otros medios.
- No proporcionar datos personales (contraseñas, tarjetas, cuentas bancarias, etc.) por correo, teléfono o SMS.
- No introducir datos confidenciales en sitios web sospechosas o de dudosa procedencia.
- Verificar la fuente de información de tus correos entrantes.
- Introducir tus datos únicamente en webs seguras.
- Tener siempre actualizado el sistema operativo y el antivirus. En el caso del antivirus, comprobar que está activo.

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

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°207	Fecha: 02-09-2023
		Página: 10 de 13

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	G01
Clasificación temática familia	Fraude		

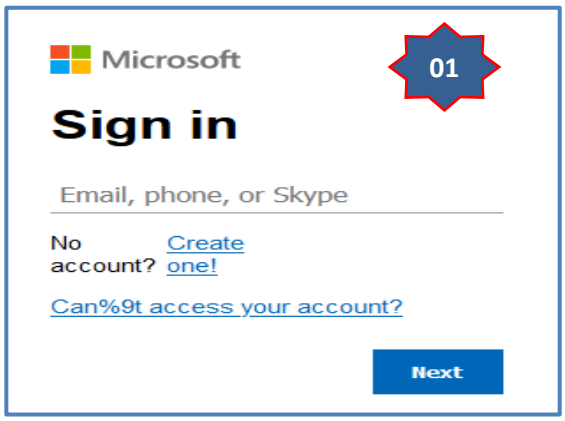
Descripción

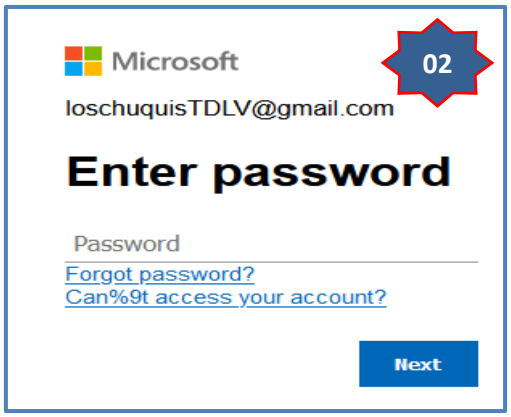
1. ANTECEDENTES:

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:



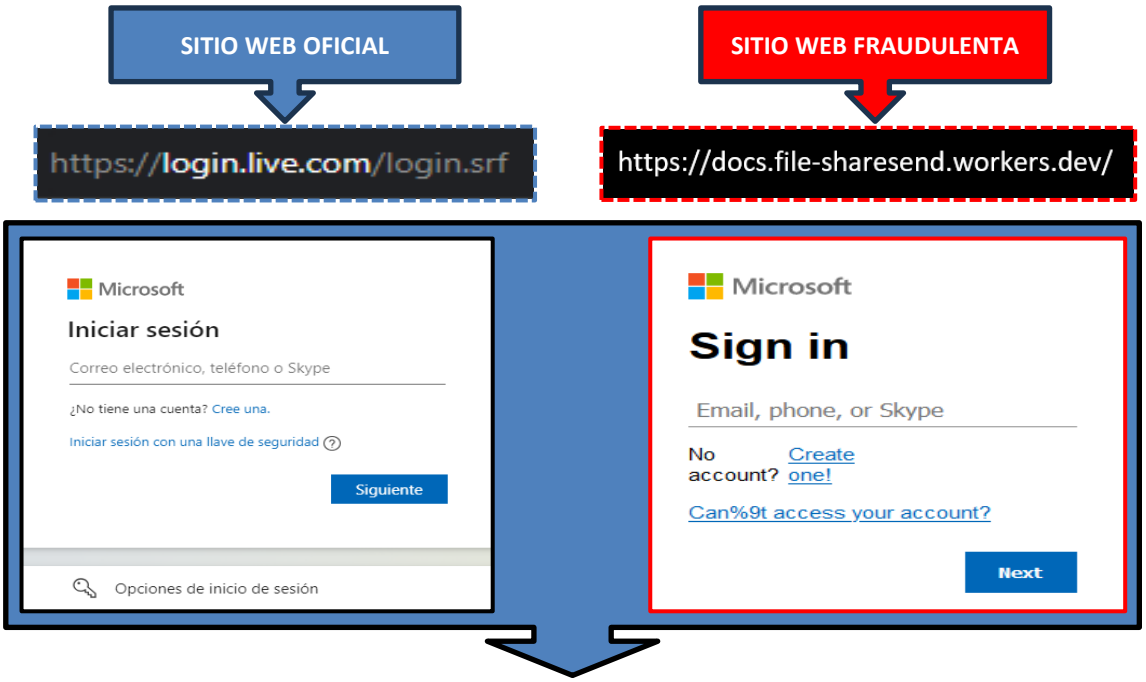


Sitio web fraudulento de Microsoft, solicita a la víctima registrar las credenciales de acceso (Correo electrónico, celular o Skype) para poder acceder al servicio en la web de la compañía Microsoft (Outlook, Hotmail, etc.)

Al completar con las credenciales de acceso, requiere que registre la contraseña de acceso para el servicio web de Microsoft, para luego dar clic en <Next>.

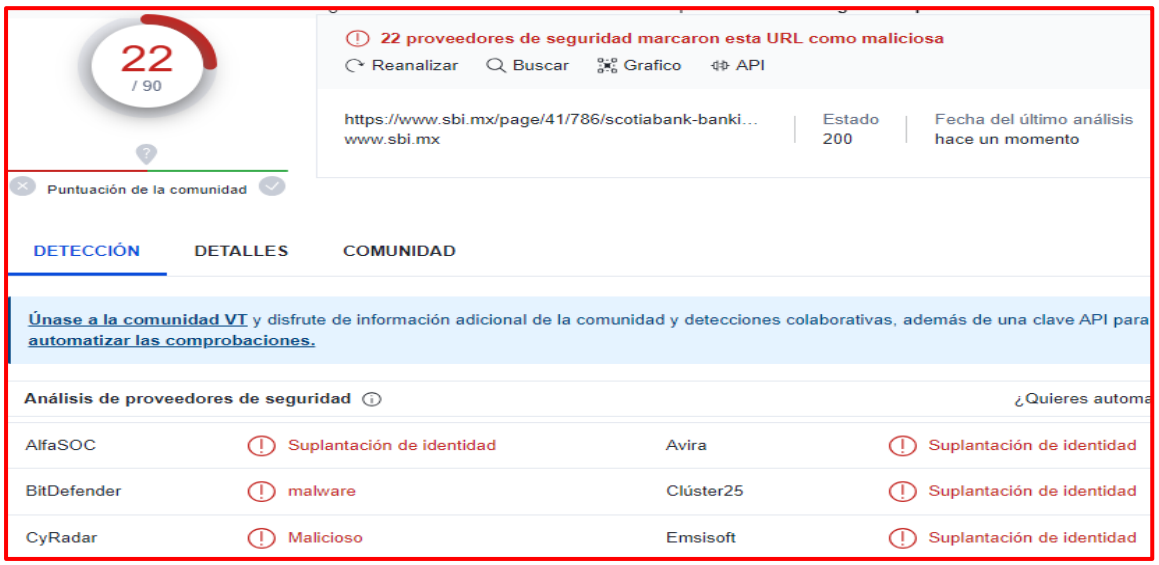
Por último, después de unos segundos le redirige al servicio del correo electrónico de la compañía Microsoft oficial aparentando un error de autenticación, sin embargo, los datos fueron capturados por los cibercriminales.

A. Comparación del sitio web oficial y fraudulento.



- Existe diferencias entre la URL original y la fraudulenta.
- La URL del sitio web fraudulento posee protocolo de seguridad de red (https), pero al analizar la URL es malicioso.
- No existe una similitud entre ambas páginas en imagen, fondo y colores de ambos sitios web.

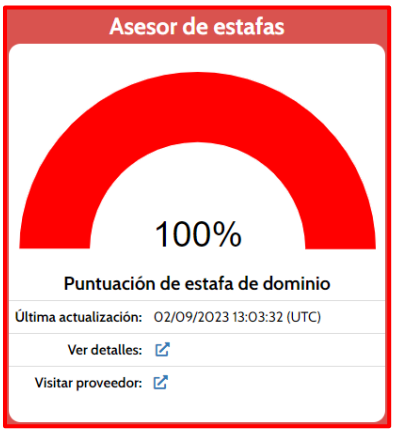
B. Proveedores de seguridad informática alertan como SUPLANTACIÓN DE IDENTIDAD - PHISHING.



C. Indicadores de compromiso (IoC)

- Dominio : sbi[.]mx
- Servidor : apache
- SHA-256 : 439be6d1d5f8b212ea490a87d47a869e52c237518a2d7a11b7b1584b40097ae7
- IP : 64[.]251[.]8[.]144

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

F. 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:

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

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