	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°267	Fecha: 08-11-2023
		Página: 9 de 12

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:

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.)

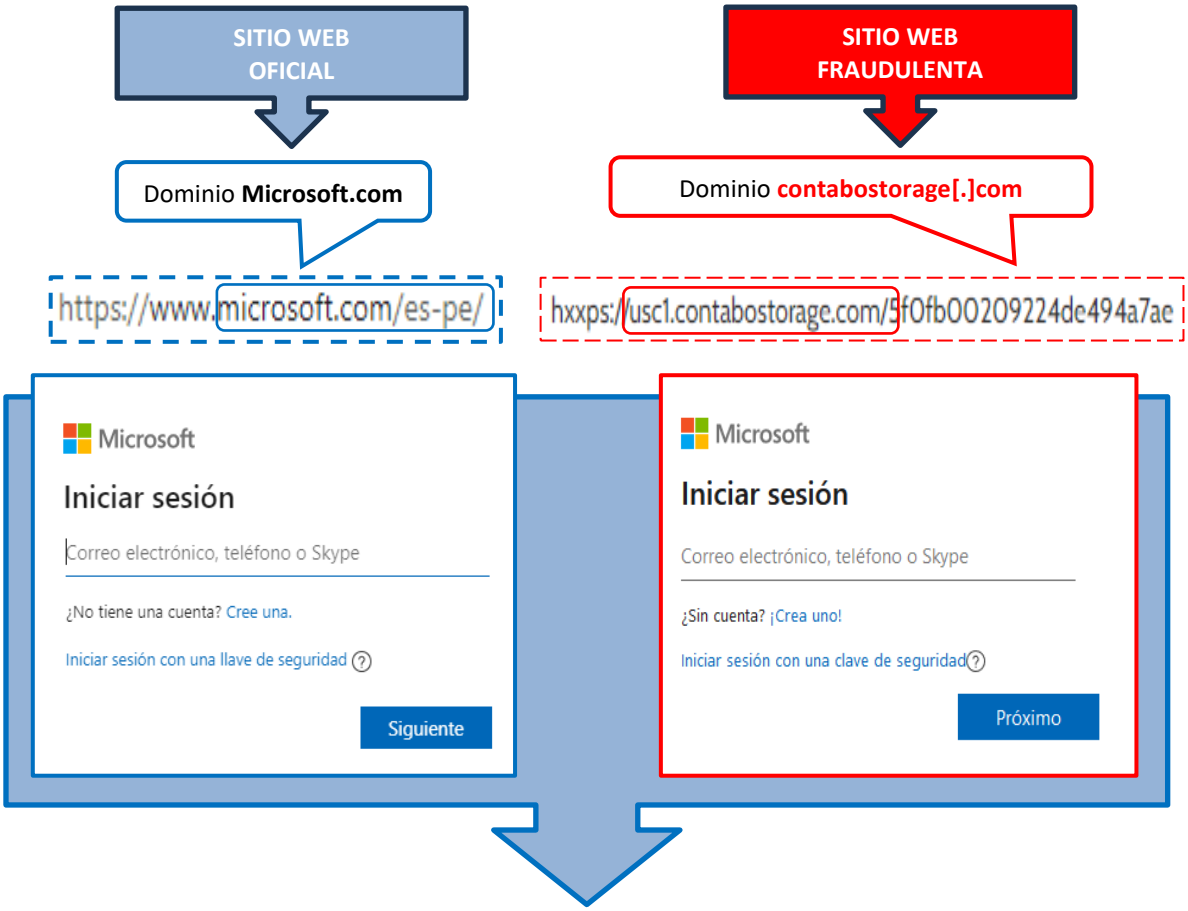
Paso N.º 02

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

Paso N.º 03

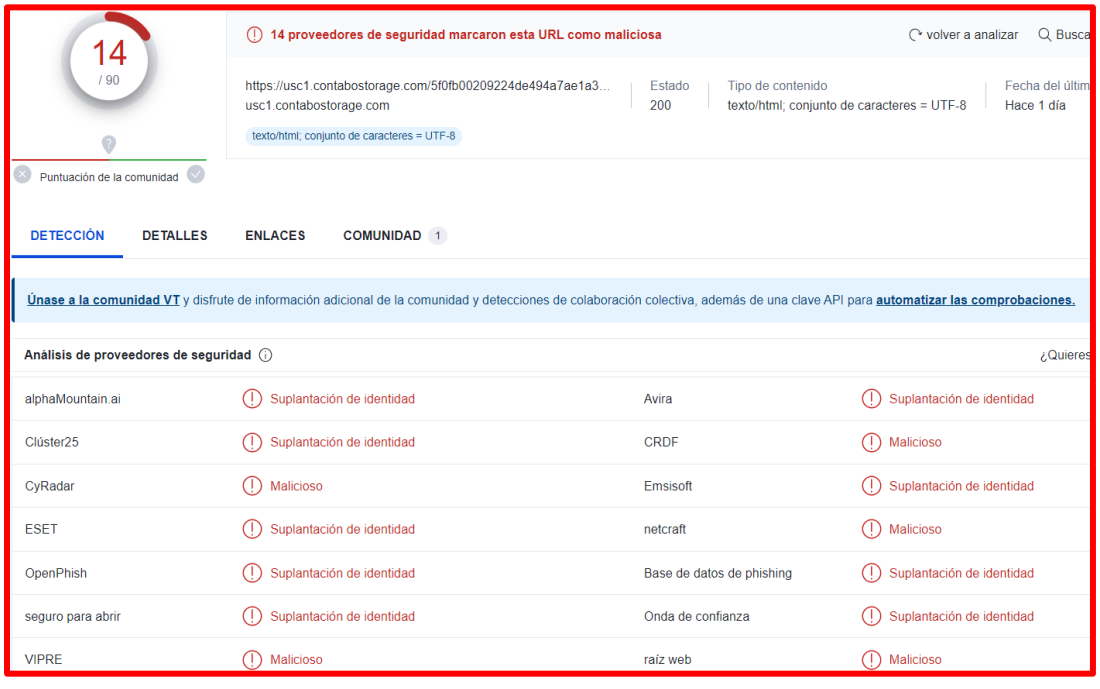
Por último, después de unos segundos le redirige al servicio del correo electrónico de la compañía Microsoft oficial aparentando un error de autenticación, sin embargo, los datos fueron capturados por los cibercriminales.

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)
- No 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 : contabostorage.com

Domain	contabostorage.com
Nameserver	ben.ns.cloudflare.com
Domain registrar	registrygate.com
Nameserver organisation	whois.cloudflare.com

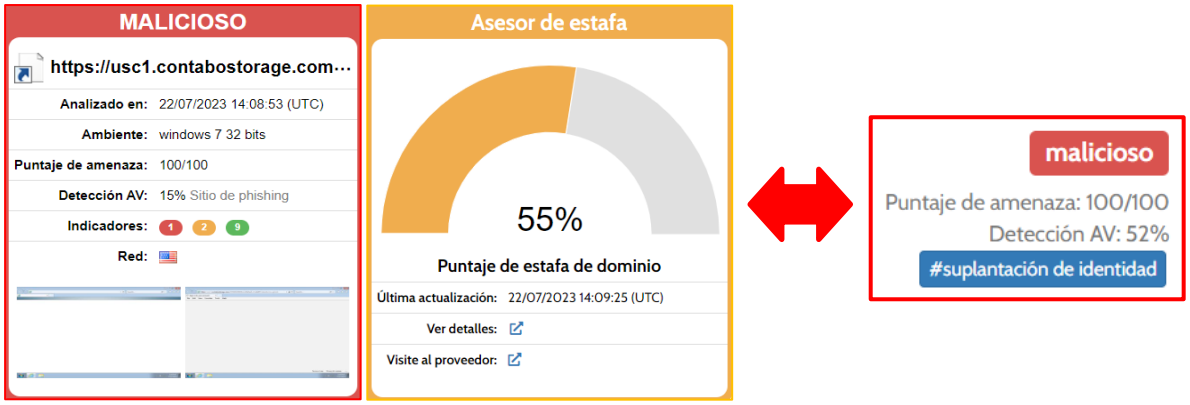
- IP : 209[.]126[.]15[.]85

IPv4 address (209.126.15.85)

IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
209.0.0.0-209.255.255.255	United States	NET209	American Registry for Internet Numbers
209.126.0.0-209.126.15.255	United States	CONTA-48	Contabo Inc.
209.126.15.85	United States	CONTA-48	Contabo Inc.

- Servidor : nginx
- SHA-256 : b286e74781833d61e04efc4d74958074aa9c88d9b307339ca4bf8c24c7878631

D. Otras detecciones:



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.