

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°163		Fecha: 11-07-2023
			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:



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

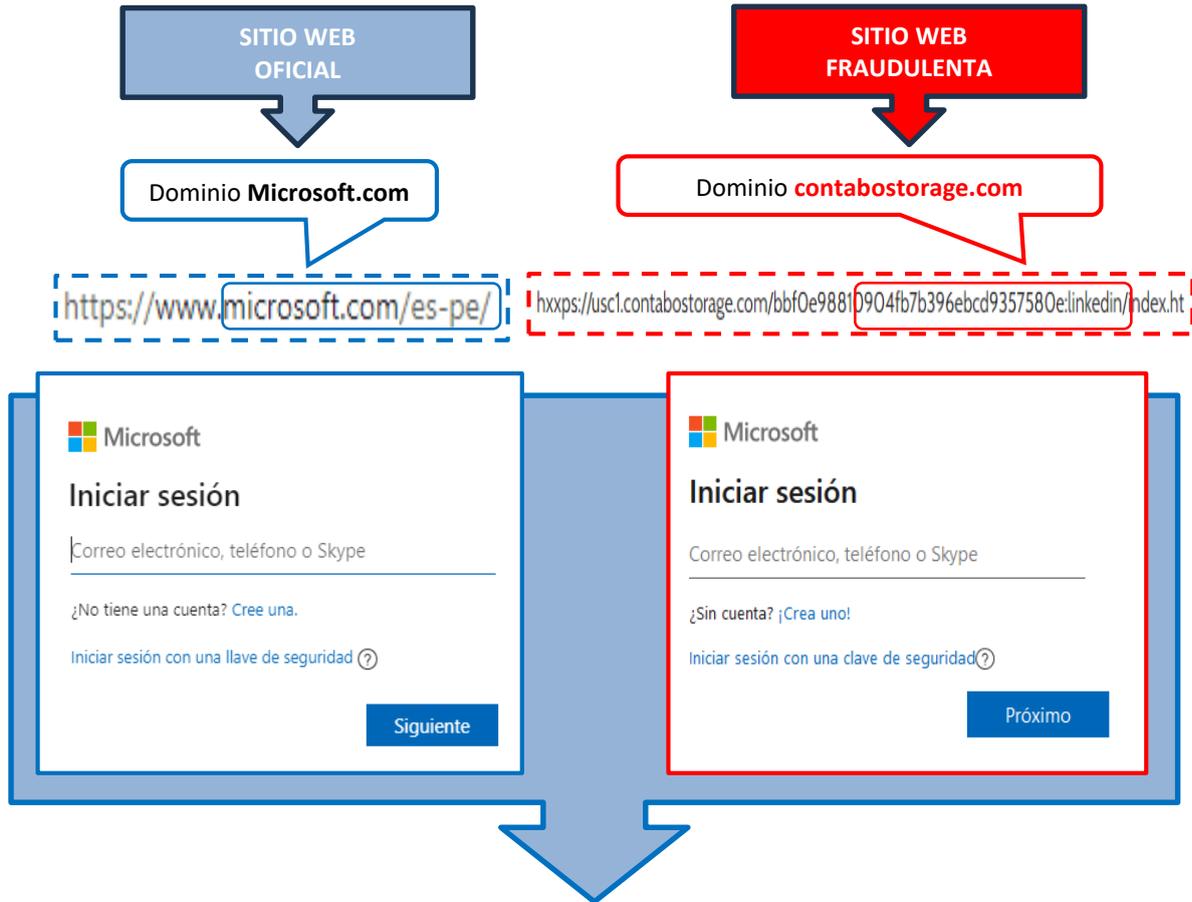
Luego de registrar el correo electrónico, requiere la contraseña de acceso para iniciar sesión del sitio web de Microsoft.



Paso N.º 03

Por último, después de unos segundos le dirige 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**.

15 / 90
 15 proveedores de seguridad marcaron esta URL como maliciosa

https://usc1.contabostorage.com/bbf0e98810904fb7b396ebcd9... Estado 200 Tipo de contenido texto/html; conjunto de caracteres = UTF-8 Fecha de actualización 1 hora

Proveedor	Alerta	Clase	Proveedor	Alerta
Avira	Suplantación de identidad	Clúster25	Clúster25	Suplantación de identidad
CRDF	Malicioso	CyRadar	CyRadar	Malicioso
Emsisoft	Suplantación de identidad	ESET	ESET	Suplantación de identidad
Buscador de amenazas de Forcepoint	Suplantación de identidad	netcraft	netcraft	Malicioso
OpenPhish	Suplantación de identidad	Base de datos de phishing	Base de datos de phishing	Suplantación de identidad
SCUMWARE.org	Malware	Sophos	Sophos	Suplantación de identidad

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



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 : de85e818f58f739f051915ab68f695221240a044edaac59b034abba0da12d413

D. Otras detecciones:

MALICIOSO

https://usc1.contabostorage.co...

Analizado en: 11/07/2023 14:38:06 (UTC)

Ambiente: windows 7 32 bits

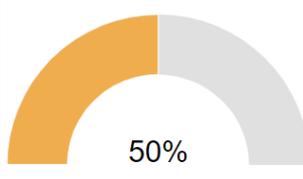
Puntaje de amenaza: 100/100

Detección AV: 16% Sitio de phishing

Indicadores: 1 4 11

Red: 🇺🇸 🇩🇪

Asesor de estafa



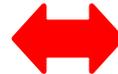
50%

Puntaje de estafa de dominio

Última actualización: 11/07/2023 14:38:39 (UTC)

Ver detalles: [🔗](#)

Visite al proveedor: [🔗](#)



malicioso

Puntaje de amenaza: 100/100

Detección AV: 75%

#suplantación de identidad

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 envíos 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