Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°173	Fecha: 23-07-2023
		Página: 4 de 8

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Phishers explotando Google Docs para recolectar credenciales criptográficas		
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:

Los investigadores de Check Point han descubierto una nueva campaña de estafa de phishing que distribuye URL ilegítimas mediante la explotación de Google Docs, con el objetivo de robar las credenciales de criptomonedas de la víctima.

Según un informe de investigación escrito por Jeremy Fuchs, investigador de seguridad cibernética y analista de Check Point Software, Google Docs es el último vector de ataque que utilizan los phishers para redirigir a los usuarios a sitios de recolección de credenciales.

Los investigadores de Check Point observaron que los servicios legítimos de Google Docs están siendo explotados para enviar mensajes o URL ilegítimos, como el correo electrónico, las páginas y las funciones de comentarios en Google Docs, lo que indica la naturaleza evolutiva de las campañas de Business Email Compromise (BEC).

2. DETALLES:

Este ataque comienza con la creación de un documento de Google enviado directamente al usuario por correo electrónico desde esta dirección: NO-REPLY@GOOGLE.COM. Después de hacer clic en el enlace incluido en el correo electrónico, el usuario es redirigido a una página legítima de Google Docs, supuestamente una página de imitación de OneDrive, y ahí es donde el usuario es engañado y se le obliga a visitar una página de criptomonedas falsa.

La explotación de los servicios de Google Docs indica que los piratas informáticos trabajan continuamente para mejorar sus tácticas de phishing, especialmente en BEC.

BEC 3.0 ha eliminado gran parte de la incertidumbre que existía anteriormente entre los piratas informáticos, ya que no implica la descarga de archivos o software maliciosos. Ahora solo requieren la respuesta o el compromiso del usuario para recolectar credenciales de criptomonedas y robar fondos. "Aprovecha algo en lo que todos confiamos, Google, y procesos en los que todos confiamos: obtener un documento compartido de Google Docs", dijo Fuchs.

Se espera un aumento en los ataques BEC 3.0, por lo que es vital contar con una infraestructura de ciberseguridad completa y herramientas adecuadas para identificar y emular el comportamiento malicioso más allá del correo electrónico.

3. RECOMENDACIONES:

- Implementar medidas de seguridad robustas como autenticación multifactor.
- Capacitar en concienciación sobre seguridad informática e ingeniería social.
- Implementar políticas de verificación rigurosas antes de realizar transferencias de dinero y supervisión continua de las actividades de correo electrónico sospechosas.
- Mantenerse actualizado sobre las últimas tácticas y técnicas utilizadas por los ciberdelincuentes y adoptar soluciones de seguridad avanzadas para detectar y prevenir estos ataques.
- Utilizar mecanismos de seguridad impulsados por IA para rastrear simultáneamente todos los indicadores de phishing, utilizando un programa de seguridad de conjunto completo e implementando una sólida seguridad de URL para que todos los documentos, archivos y páginas web se escaneen rápidamente.

Fuente de Información:	• hxxps://www.hackread.com/phishers-google-docs-harvest-crypto-credentials/ • hxxps://cybersecuritynews.es/los-ataques-bec-3-0-se-vuelven-mas-sofisticados-y-peligrosos/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°173	Fecha: 22-07-2023
		Página: 5 de 8

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		

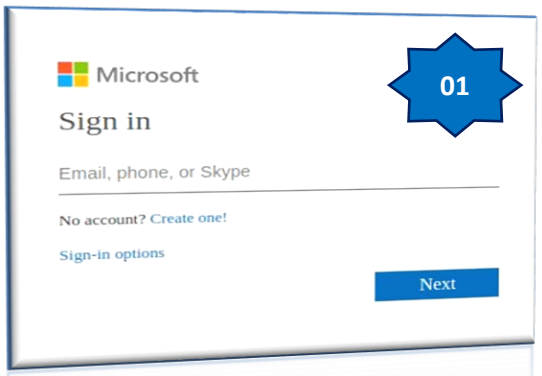
Descripción

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.)

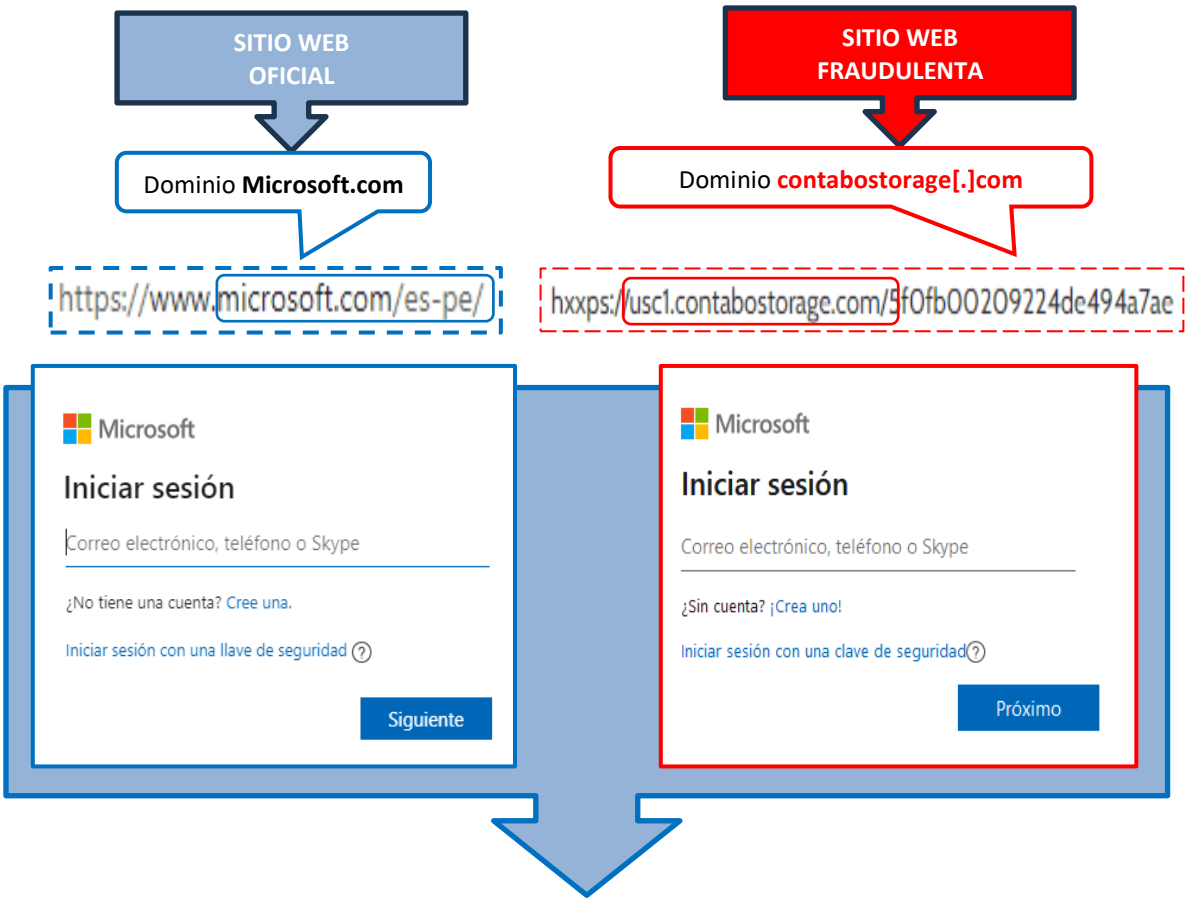
Paso N.º 02

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

Paso N.º 03

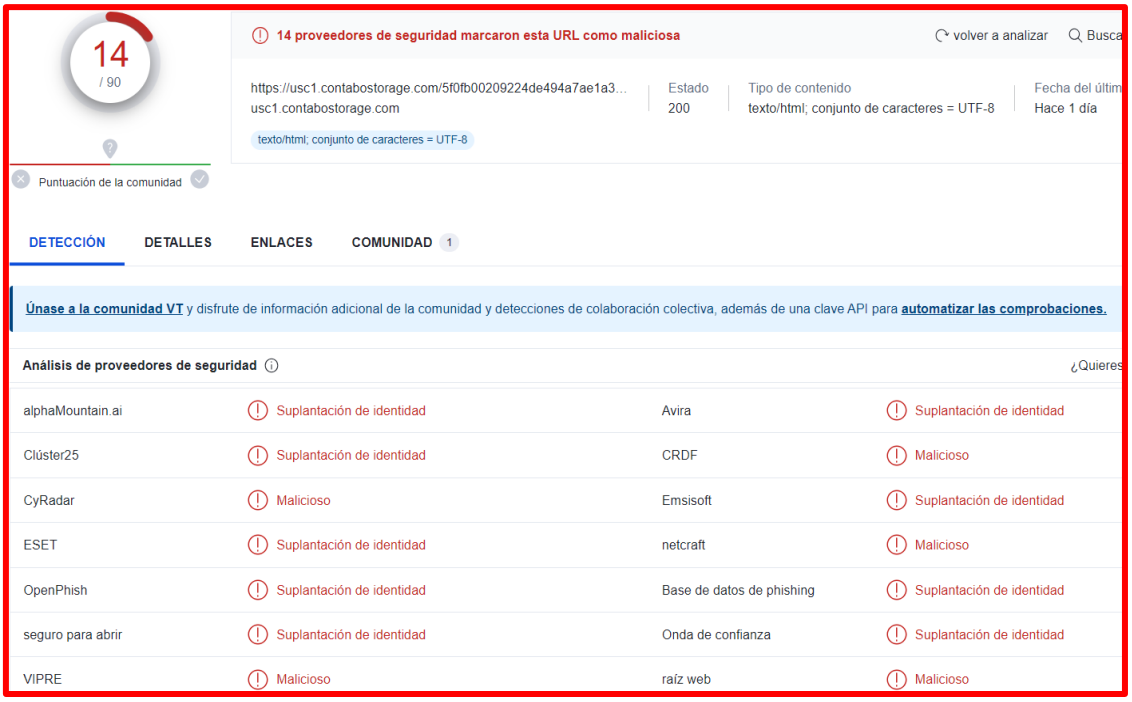
Por último, después de unos segundos le redirige al servicio del correo electrónico de la compañía Microsoft oficial aparentando un error de autenticación, sin embargo, los datos fueron capturados por los cibercriminales.

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

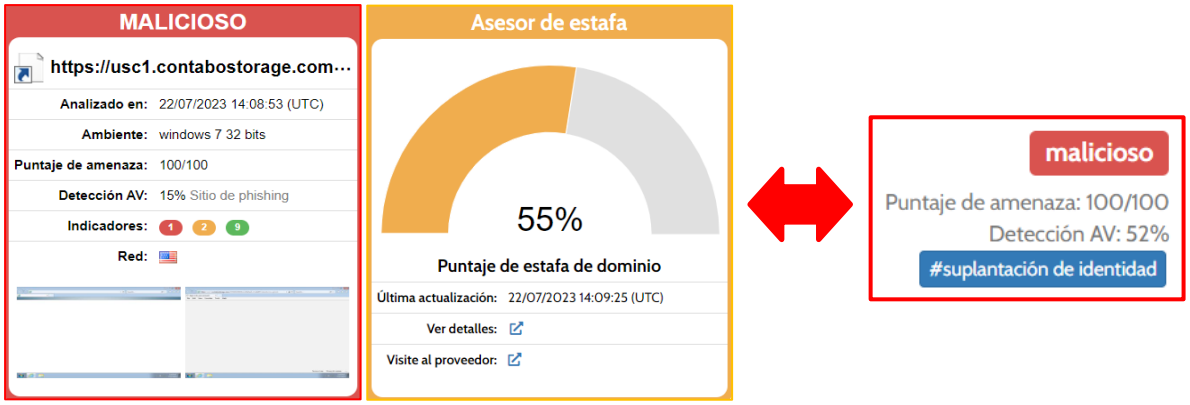
- IP : 209[.]126[.]15[.]85

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:



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