

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°017		Fecha: 19-01-2024
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		

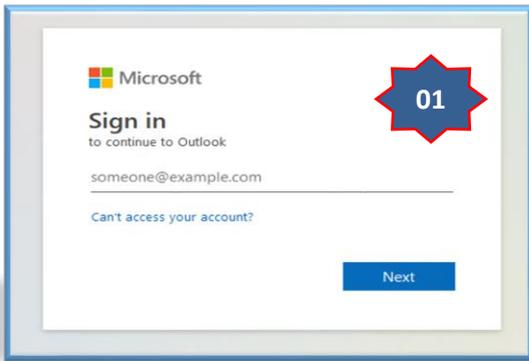
Descripción

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.

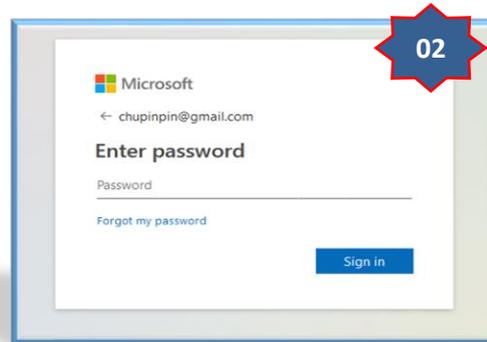
2. DETALLES:

El proceso del Phishing es el siguiente:



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

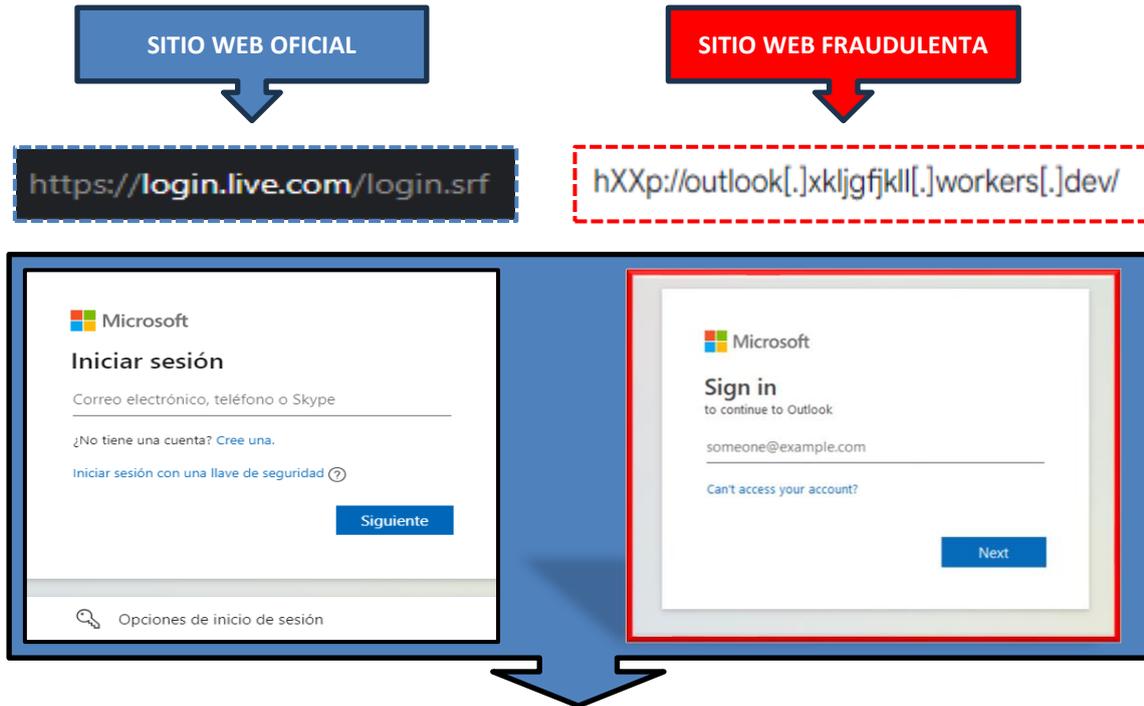
Al completar con las credenciales de acceso, requiere que registre la contraseña de acceso para el servicio web de Microsoft, para luego dar clic en <Iniciar sesión>.



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 NO POSEE protocolo de seguridad de red (http), pero al analizar la URL es malicioso.
- 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)

- Url : hXXp://Outlook[.]xkljgfkll[.]workers[.]dev/



Site	http://outlook.xkljgfkll.workers.dev
Netblock Owner	Cloudflare, Inc.
Hosting company	Cloudflare
Hosting country	US

- Dominio : workers[.]dev



Domain	workers.dev
Nameserver	clyde.ns.cloudflare.com
Domain registrar	nic.google
Nameserver organisation	whois.cloudflare.com

- IP : 172[.]67[.]212[.]189



IPv4 address (172.67.212.189)			
IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
↳ 172.0.0.0-172.255.255.255	United States	NET172	Various Registries (Maintained by ARIN)
↳ 172.64.0.0-172.71.255.255	United States	CLOUDFLARENET	Cloudflare, Inc.
↳ 172.67.212.189	United States	CLOUDFLARENET	Cloudflare, Inc.

- SHA-256 : b0a98acfb36cf33b66d162f411aaec60daa480b4592f74d6b300afdbd3b245b8

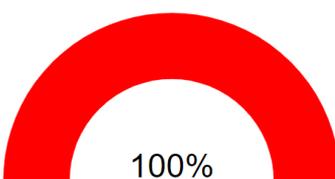


TarC9D0.tmp 4276af3669a141a59388bc56a87f6614d9a9bdddf560636c264219a7eb11256f	malicioso
SH6X3X5F.htm b0a98acfb36cf33b66d162f411aaec60daa480b4592f74d6b300afdbd3b245b8	malicioso
opciones de inicio de sesión_4e48046ce74f4b89d45037c90576bfac.svg 8e6db1634f1812d42516778fc890010aa57f3e39914fb4803df2c38abbf56d93	sospechoso

- Tipo Contex. : Text/Html
- Servidor : cloudflare

D. Otras detecciones:

urlscan.io



100%

Url Scan Analysis

Last Update: 01/19/2024 15:49:31 (UTC)

View Details: [🔗](#)

Visit Vendor: [🔗](#)



malicioso

Detección AV: 46%

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 envío 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.

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.