

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°222		Fecha: 20-09-2023
			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		

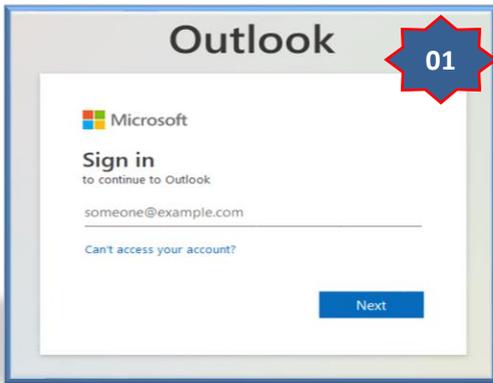
Descripción

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 para poder acceder al servicio en la web de la compañía Microsoft (Outlook, Hotmail, etc.)

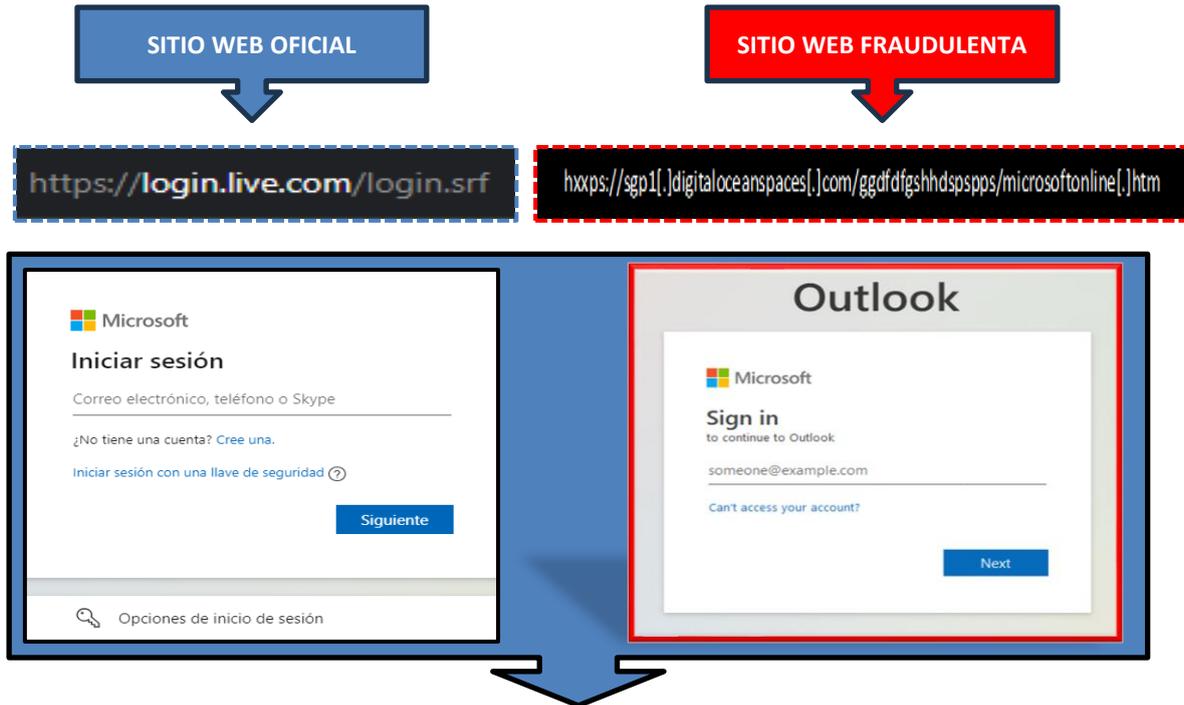


Al completar con las credenciales de acceso, requiere que registre la contraseña de acceso para el servicio web de Microsoft, para luego dar clic en <Iniciar sesión>.



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 POSEE protocolo de seguridad de red (https), 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.**

The screenshot shows the VirusTotal analysis interface. At the top, it states '16 proveedores de seguridad marcaron esta URL como maliciosa'. Below this, a table lists the providers and their detection results:

Proveedor	Resultado	Proveedor	Resultado
Avira	Suplantación de identidad	BitDefender	Suplantación de identidad
Clúster25	Suplantación de identidad	propiedad intelectual criminal	Suplantación de identidad
Emsisoft	Suplantación de identidad	ESET	Suplantación de identidad
Buscador de amenazas Forcepoint	Suplantación de identidad	Datos G	Suplantación de identidad
Kaspersky	Suplantación de identidad	leonico	Suplantación de identidad
Netcraft	Malicioso	Base de datos de phishing	Suplantación de identidad
Phishtank	Suplantación de identidad	Seguro para abrir	Suplantación de identidad

C. Indicadores de compromiso (IoC)

- Dominio : espaciosdigitalocean[.]com
- SHA-256 : b5400d6a0a4305d4f97b8d585014f5cfe829946a893baea4e7b1f7b9a52a5595
- IP : 103[.]253[.]144[.]208
- Tipo Context. : Text/Html

D. Otras detecciones:

MALICIOSO

https://sgp1.digitaloceanspaces...

Analizado en: 20/09/2023 13:51:54 (UTC)

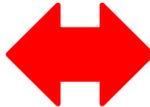
Ambiente: Windows 7 de 32 bits

Puntuación de amenaza: 100/100

Detección AV: 17% Sitio de phishing

Indicadores: 2 3 13

Red: #suplantación de identidad



malicioso

Puntuación de amenaza: 100/100

Detección AV: 77%

#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 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.