

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°059		Fecha: 08-03-2024
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:

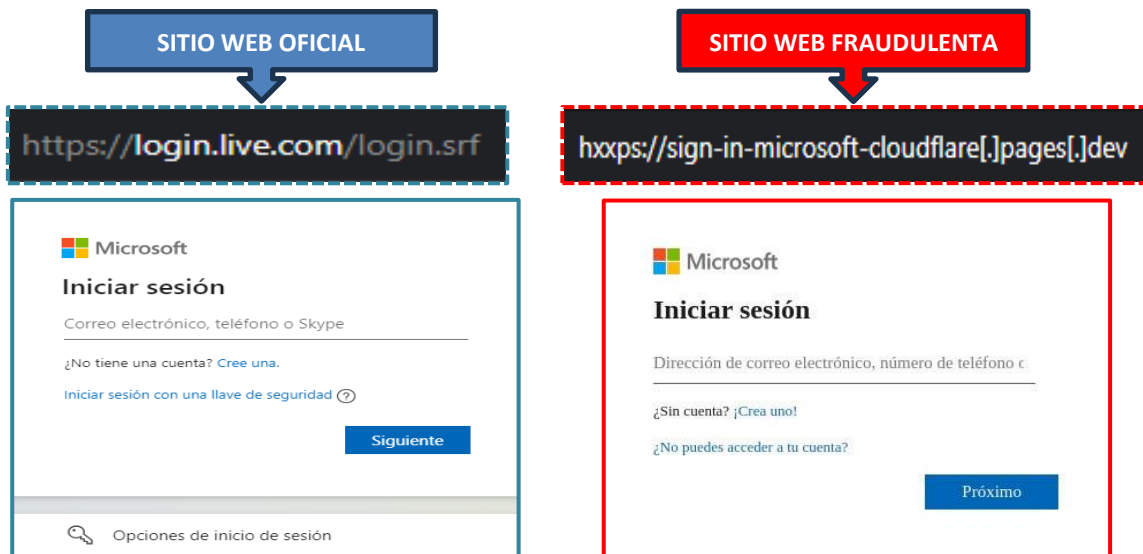
A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que actores de amenazas vienen realizando una campaña de Phishing, activando un falso servicio del correo electrónico de la compañía Microsoft (Outlook, Hotmail, etc.), con la finalidad de obtener las credenciales de acceso (correo y contraseña) de los usuarios de la compañía tecnológica.

2. DETALLES:

El proceso del Phishing es el siguiente:

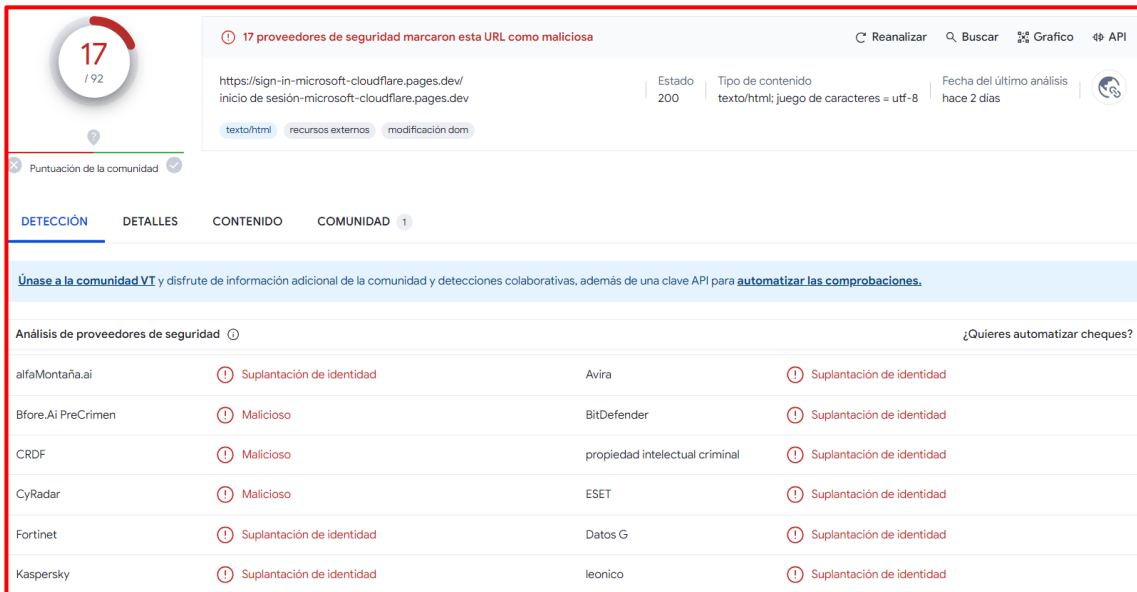


A. Comparación del sitio web oficial y fraudulento.



- Existe diferencias entre la URL original y la fraudulenta.
- La URL del sitio web fraudulento posee protocolo de seguridad de red (https)
- 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.**



17 / 92

17 proveedores de seguridad marcaron esta URL como maliciosa

Reanalizar Buscar Grafico API

Estado: 200 | Tipo de contenido: texto/html; juego de caracteres = utf-8 | Fecha del último análisis: hace 2 días

texto/html recursos externos modificación dom

Puntuación de la comunidad

DETECCIÓN DETALLES CONTENIDO COMUNIDAD 1

Únase a la comunidad VT y disfrute de información adicional de la comunidad y detecciones colaborativas, además de una clave API para automatizar las comprobaciones.

Análisis de proveedores de seguridad ¿Quieres automatizar chequeos?

alfaMontaña.ai	Suplantación de identidad	Avira	Suplantación de identidad
Bfore.Ai PreCrimen	Malicioso	BitDefender	Suplantación de identidad
CRDF	Malicioso	propiedad intelectual criminal	Suplantación de identidad
CyRadar	Malicioso	ESET	Suplantación de identidad
Fortinet	Suplantación de identidad	Datos G	Suplantación de identidad
Kaspersky	Suplantación de identidad	leonico	Suplantación de identidad

C. Indicadores de compromiso (IoC)

- Dominio : pages[.]dev
- SHA-256 : fd46536c016a0eca83b0deaea8867ebaf4bc7e9dc5a4059da1af04a89089015e
- IP : 172[.]66[.]44[.]143

D. 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, 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