	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°031	Fecha: 05-02-2024
		Página: 10 de 16

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.

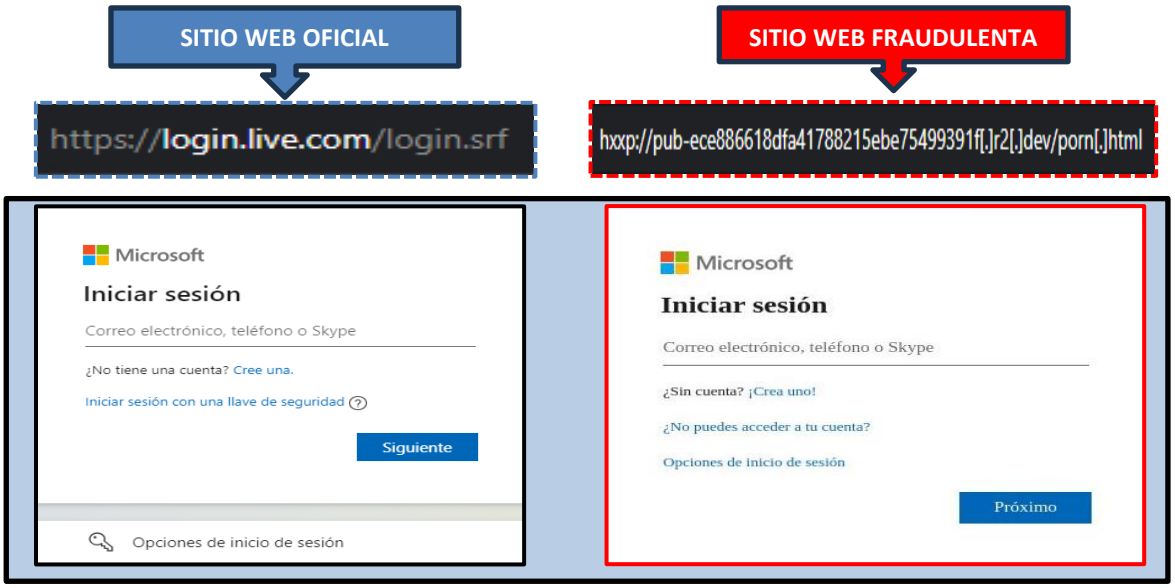
2. DETALLES:

El proceso del Phishing es el siguiente:

Solicita el correo electrónico de la víctima, para acceder al servicio en la web de la compañía Microsoft (Outlook, Hotmail, etc.)

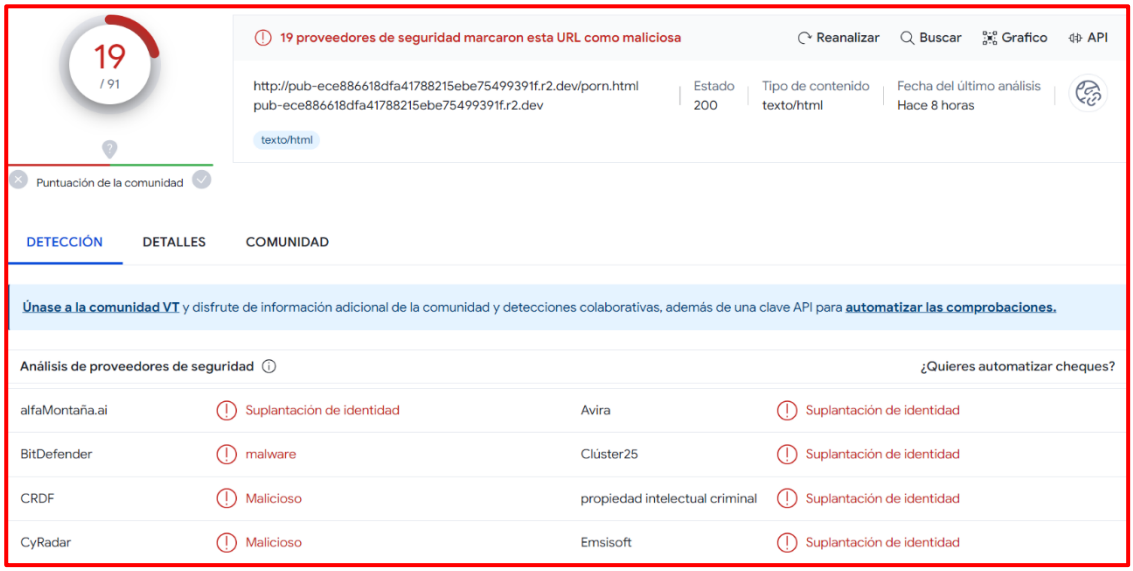
Requieren la contraseña de acceso para el servicio web de Microsoft, para luego dar clic en <**Iniciar sesión**>; sin embargo, después de unos segundos redirige al servicio del correo electrónico de la compañía Microsoft.

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 (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.



C. Indicadores de compromiso (IoC)

- Dominio : r2[.]dev
- Servidor : Cloudflare
- SHA-256 : 3d8fb7260795d81ad827183398e0c43f2bfec76a5e6cf85795b584ab68d798d7
- IP : 104[.]18[.]3[.]35

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.