	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°211	Fecha: 07-09-2023
		Página: 8 de 11

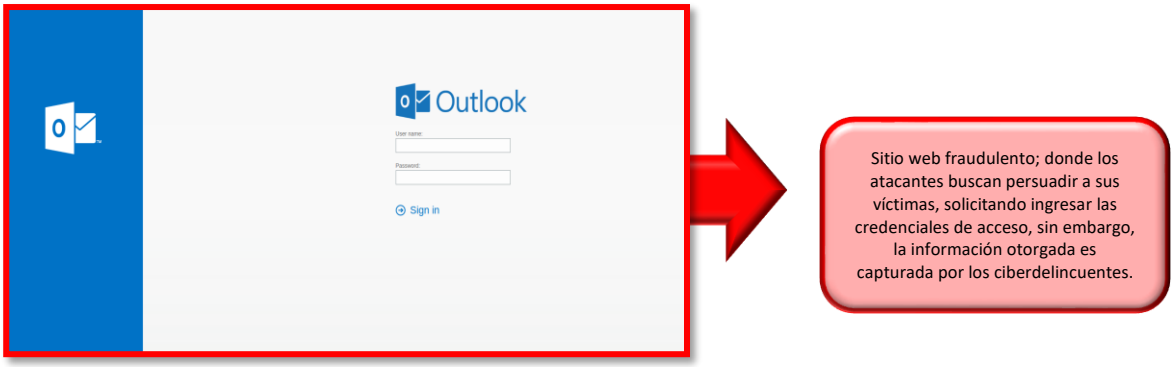
Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Nueva campaña de Phishing que suplanta la identidad de Outlook		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre 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, los ciberdelincuentes se encuentran desarrollando una campaña de Phishing, a través de los diferentes navegadores web, quienes vienen suplantando la identidad del sitio oficial de "Outlook"; con el objetivo de acceder u obtener credenciales de inicio de sesión de las posibles víctimas.

2. DETALLES:

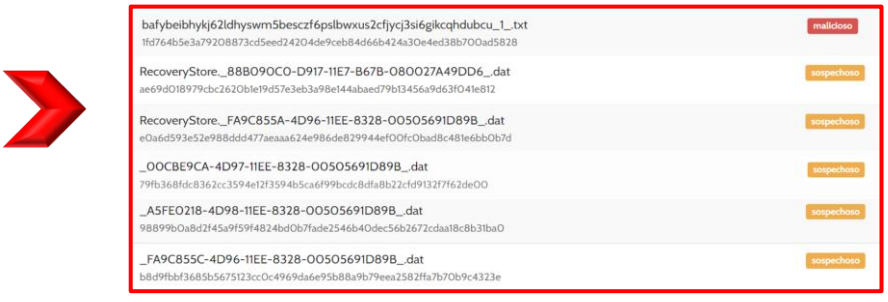


A. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD:**

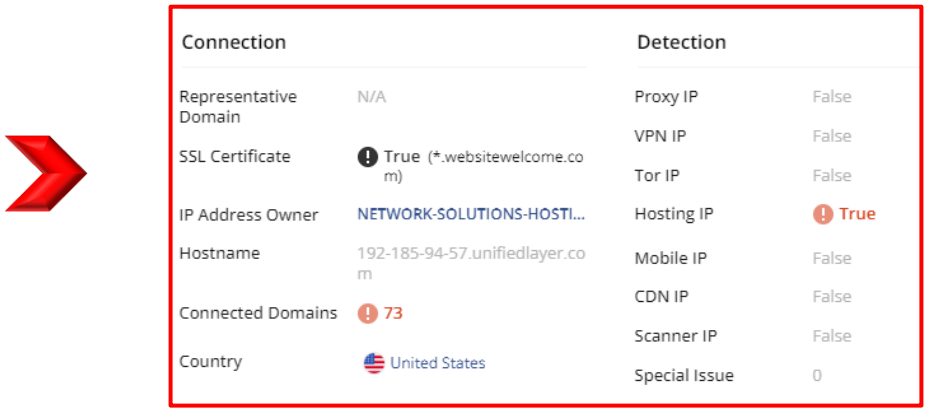
a) Indicadores de compromisos:

I. URL:
hxxps[:]//pub-749b686f620d4a78877b378ce1e6fbb2[.]r2[.]dev/outlook-owa-skjuehenje[.]html

II. SHA-256: f652ca05a9336ae9931cbc7634bd98a19495cb356ab2f4de0d20bb0644d90472



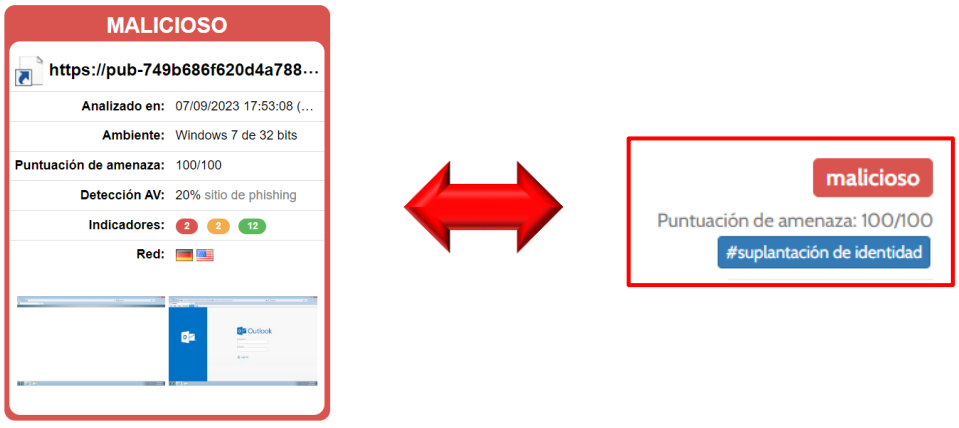
III. IP: 104[.]18[.]3[.]35



B. Se hallaron **18 proveedores** de seguridad que marcaron este dominio como malicioso.

alphaMountain.ai	Phishing	Avira	Phishing
BitDefender	Phishing	Cluster25	Phishing
CRDF	Malicious	CyRadar	Malicious
Emsisoft	Phishing	ESET	Phishing
Forcepoint ThreatSeeker	Phishing	Fortinet	Phishing
G-Data	Phishing	Kaspersky	Phishing
Lionic	Phishing	Netcraft	Malicious
Phishtank	Phishing	Sophos	Phishing
Trustwave	Phishing	VIPRE	Malicious

C. Otras detecciones:



D. Cómo funciona el Phishing:

- Los correos electrónicos incluyen enlaces a sitios web preparados por los ciberdelincuentes en los que solicitan información personal.
- Medios de propagación del Phishing: WhatsApp, Telegram, redes sociales, SMS entre otros.
- Los ciberdelincuentes intentan suplantar a una entidad legitima (organismo público o privado, entidad financiera, servicio técnico, etc.)

E. Referencia:

- Phishing o suplantación de identidad: Es un método que los ciberdelincuentes, utilizan para engañar a los usuarios para conseguir que revele información personal, como contraseñas, datos de tarjetas de créditos, números de cuentas bancarias, entre otros.

3. RECOMENDACIONES:

- Evitar acceder a enlaces que llegan inesperadamente por correo electrónico u otros medios.
- No proporcionar datos personales (contraseñas, tarjetas, cuentas bancarias, etc.) por correo, teléfono o SMS.
- No introducir datos confidenciales en sitios web sospechosas o de dudosa procedencia.
- Verificar la fuente de información de tus correos entrantes.
- Introducir tus datos únicamente en webs seguras.
- Tener siempre actualizado el sistema operativo y el antivirus. En el caso del antivirus, comprobar que está activo.

Fuente de Información:	Análisis propio de redes sociales y fuente abierta