	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°209	Fecha: 05-09-2023
		Página: 8 de 11

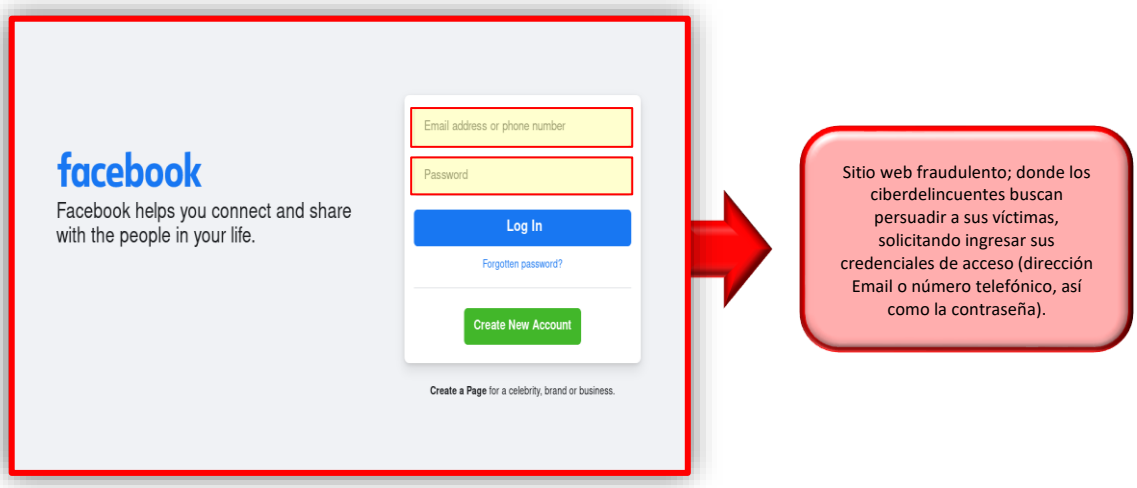
Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Campaña de Phishing, suplantando la identidad de la Red Social Facebook		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, 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 de la Red Social Facebook; con el objetivo de acceder u obtener credenciales de inicio de sesión de las posibles víctimas.

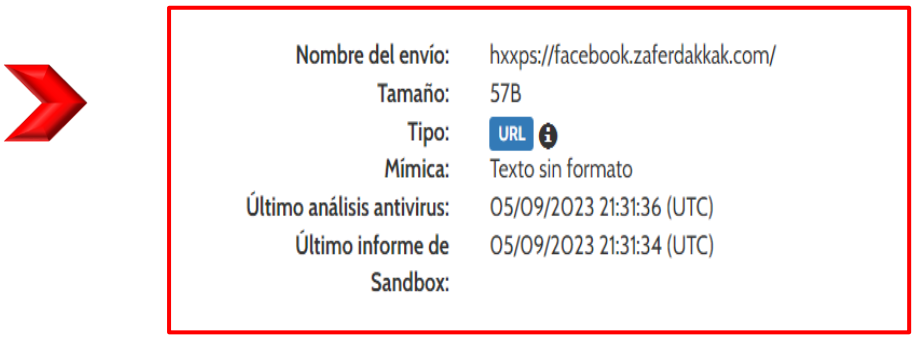
2. DETALLES:



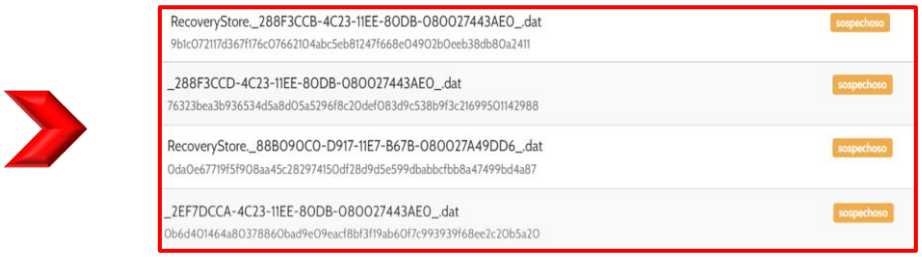
A. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD:**

a) Indicadores de compromisos:

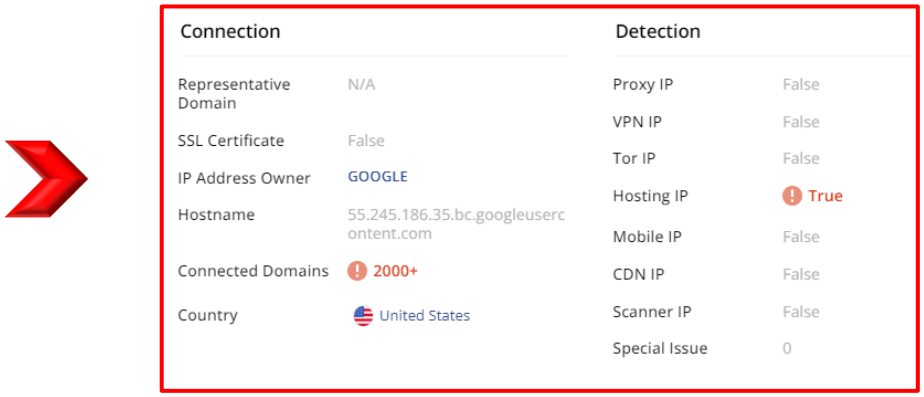
I. URL: hxxps[:]//Facebook[.]zaferdakkak[.]com/



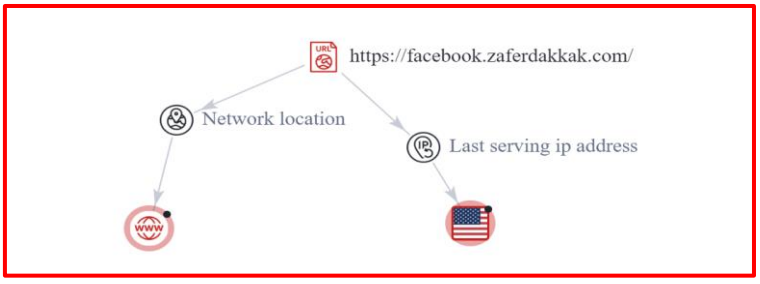
II. SHA-256: 894c1681cc8a13ac84fd2ae3ce17aabda3e403ac43290d01b7bec11a1764a9f5



III. IP: 35[.]186[.]245[.]55



IV. TIPOLOGÍA:

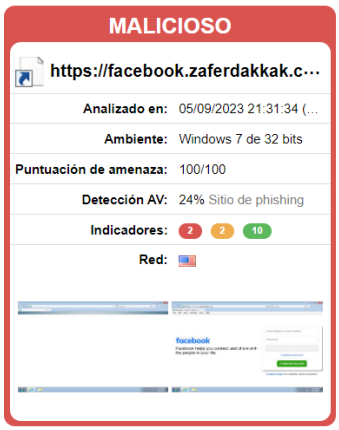


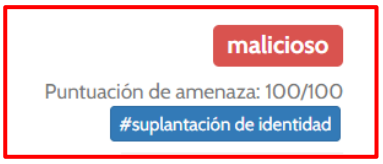
Se puede aprecia como la URL, esta alojada en un servidor ubicado en EE.UU.

B. Se hallaron **22 proveedores** de seguridad que marcaron este dominio como malicioso.

Avira	Phishing	BitDefender	Phishing
Certego	Phishing	Cluster25	Phishing
CRDF	Malicious	CyRadar	Malicious
Emsisoft	Phishing	ESET	Phishing
Forcepoint ThreatSeeker	Phishing	Fortinet	Phishing
G-Data	Phishing	Google Safebrowsing	Phishing
Kaspersky	Phishing	Lionic	Phishing
Netcraft	Malicious	Phishing Database	Phishing
PhishLabs	Phishing	Phishtank	Phishing
Segasec	Phishing	Sophos	Phishing
VIPRE	Malicious	Webroot	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.)

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