	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 142	Fecha: 17-06-2023
		Página 25 de 28

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Nueva campaña de Phishing suplanta la identidad de la red social Twitter		
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	G02
Clasificación temática familia	Fraude		

Descripción

1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes vienen llevando a cabo una nueva campaña de Phishing que suplanta la identidad de la red social Twitter, con el objetivo robar las credenciales de acceso de la cuenta de las potenciales víctimas.

2. Proceso de estafa de Phishing:

Imagen 1: Sitio web falso usado por los ciberdelincuentes solicita a la víctima, ingresar sus credenciales de acceso tales como (dirección de correo electrónico y contraseña).

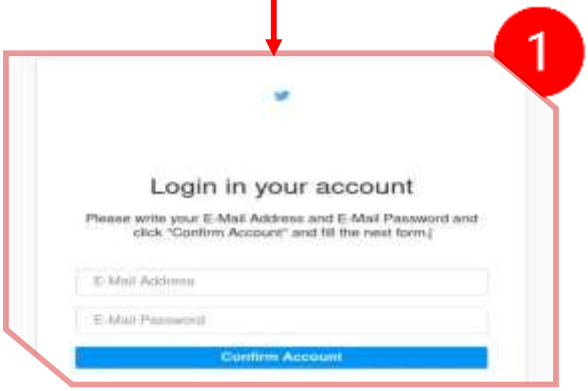
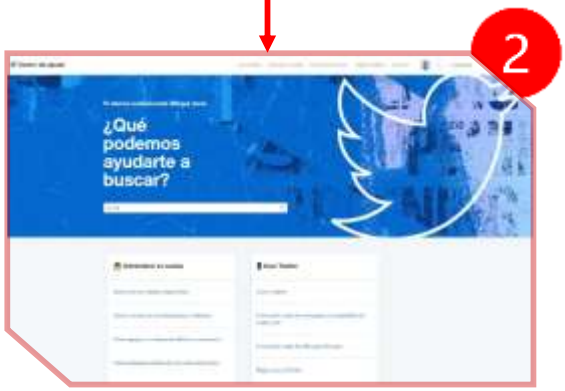


Imagen 2: Una vez ingresado las credenciales de acceso, es redirigido al centro de ayuda del sitio web legítimo de Twitter, aludiendo un aparente error; sin embargo, los datos fueron capturados.



3. Diferencias del sitio web legítimo de Twitter y sitio web Fraudulento:

SITIO WEB LEGÍTIMO
URL: https://twitter.com/

SITIO WEB FRAUDULENTO
URL: hxxp:// twitter-verify.alfelaijwatches.com

DIFERENCIAS

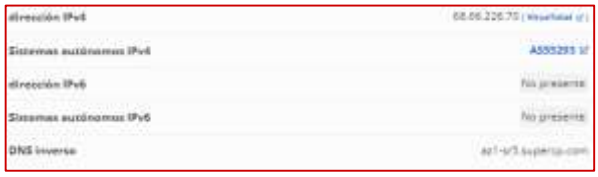
- **Existe una diferencia debido a que el URL y el dominio de sitio web fraudulento no coincide con el oficial.**
- **Ambos sitios webs, presentan diferencias en la tipografía y el color de diseño del sitio web.**

4. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, obteniendo la siguiente información:

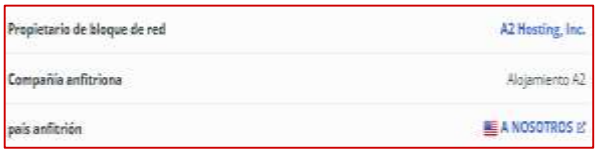
- **URL:** hxxp:// twitter-verify.alfelaijwatches.com

- **Dominio:** sui-drop[.]net

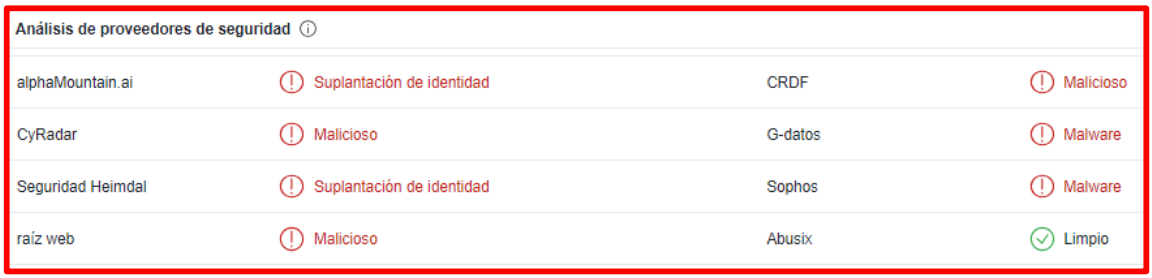
- **Direcciones IP:** 68[.]66[.]226[.]70



- **Proveedor de alojamiento:** A2 Hosting, Inc. .



5. Se hallaron **siete (07) proveedores** de seguridad que marcaron este dominio como malicioso.



6. Concepto de Twitter: Esta plataforma de red social, es un servicio que permite que los grupos de amigos, familiares y compañeros de trabajo se comuniquen y estén en contacto a través de mensajes rápidos y frecuentes. Las personas publican Tweets, que pueden contener fotos, videos, enlaces y texto.

7. **Otras detecciones**:

8. **Recomendaciones:**

- No dar clic a sitios que tengan enlaces de dudosa procedencia.
- Verificar detenidamente la redacción y ortografía de la dirección URL, que coincidan con el sitio web oficial (hppts:www.twitter.com).
- Evitar compartir la información con terceras personas, amigos o familiares (usuario y contraseña).
- Utilizar una firma de antivirus actualizado, ya que es la primera barrera ante posibles ataques cibernéticos (instala antivirus con licencia original).
- Evitar responder a mensajes enviados desde (correo electrónico, Whatsapp, SMS y otros), que contengan enlaces de dudosa procedencia.

Fuentes de información	Análisis propio de redes sociales y fuente abierta