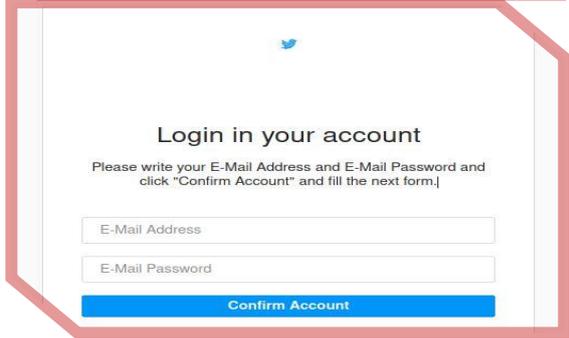


	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 086		Fecha: 12-04-2023
			Página 12 de 14
Componente que reporta	DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ		
Nombre de la alerta	Nueva campaña de phishing suplanta la identidad de la red social Twitter		
Tipo de ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de subfamilia	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 la víctima.
2. Como parte de la simulación se obtuvo la siguiente información:

1

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).



2

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:



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

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

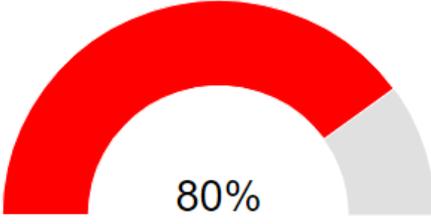
- **URL:** hxxp://twitterdoge[.]info/
- **Dominio:** twitterdoge[.]info
- **Direcciones IP:** 188[.]114[.]97[.]3
- **Tamaño:** 48B
- **Proveedor de alojamiento:** Cloudflarenet

Avira	🚫 Phishing	CRDF	🚫 Malicious
CyRadar	🚫 Malicious	ESTsecurity	🚫 Phishing
Heimdal Security	🚫 Phishing	Kaspersky	🚫 Phishing
Netcraft	🚫 Malicious	ESET	🚫 Suspicious

5. **Concepto de :** 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.

6. **Otras detecciones:**

Asesor de estafa



80%

Puntaje de estafa de dominio

Última actualización: 11/04/2023 14:05:09 (UTC)

Ver detalles: [🔗](#)

Visite al proveedor: [🔗](#)

malicioso

Puntaje de amenaza: 100/100
Detección AV: 62%

#suplantación de identidad

Detalles

- Última comprobación (UTC): 2023-04-11 03:37
- Visto por primera vez (UTC): 2023-04-08 14:06
- IP: [188.114.97.3](#)
- País: [Países Bajos](#)
- Proveedor de alojamiento: [CLOUDFLARENET](#)
- ASN: [AS13335](#)
- Certificado TLS: [GTS CA 1P5](#)

7. **Recomendaciones:**

- Acceder al sitio web a través de fuentes oficiales
- Verificar la información en la entidad correspondiente.
- Evitar responder a mensajes enviados desde (correo electrónico, Whatsapp, SMS y otros), que contengan enlaces de dudosa procedencia.
- Verificar detenidamente la redacción y ortografía de la dirección URL, que coincidan con el sitio web oficial.
- Evitar compartir la información con terceras personas, amigos o familiares.
- Utilizar una firma de antivirus actualizado, ya que es la primera barrera ante posibles ataques cibernéticos.

Fuentes de información

- Análisis propio de redes sociales y fuente abierta