Cybersecurity Incident Report

Incident Title:

Investigation of Suspected Cryptocurrency Phishing Scam via TikTok Private Message

Date of Incident:

02/01/2026

Reported By:

Samsudeen Olapade
Cybersecurity Analyst

---

1. Executive Summary

This report documents the investigation of a suspicious private message received via TikTok, which appeared to be an attempted cryptocurrency phishing scam. The message claimed that the sender intended to commit suicide and had left a large sum of cryptocurrency (USDT) for the recipient, providing login credentials to an external website.

Due to the unusual nature of the message and the high likelihood of fraud, a controlled technical investigation was conducted using a secure virtual home lab environment. Open-source threat intelligence tools were used to assess the legitimacy of the website and associated indicators. The investigation confirmed that the website was malicious and had been flagged as a phishing site by multiple cybersecurity vendors.

---

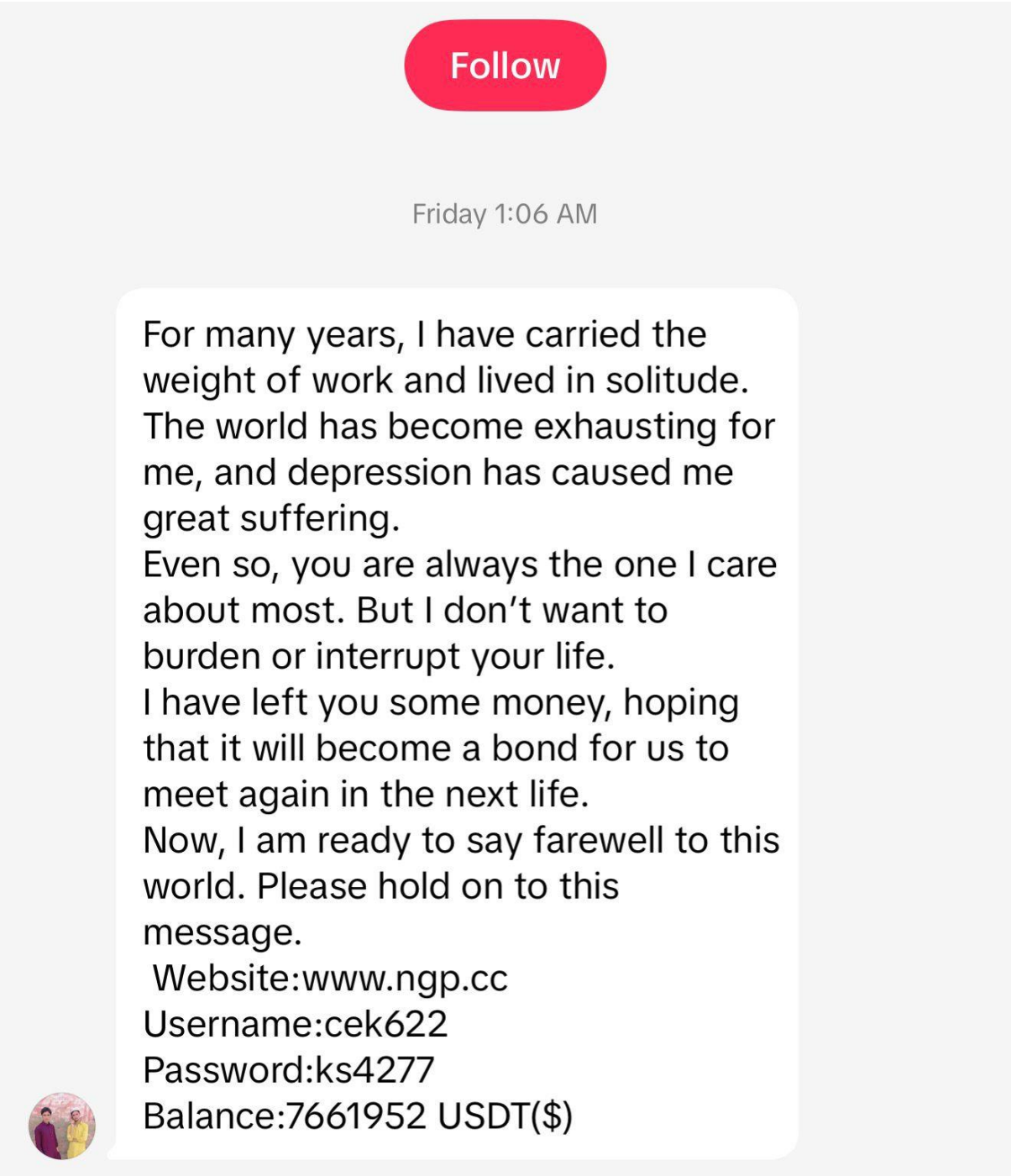
2. Incident Description

On 2nd of January 2026, I received a private message in my TikTok inbox from an unknown sender. A screenshot of the message has been retained and will be attached to this report as evidence.

The message contained emotionally manipulative content suggesting depression and suicidal intent, followed by a claim that the sender had left their life savings for me. The sender provided:

- A website URL: www.ngp.cc
- A username: cek622
- A password: ks4277
- A claimed balance of **77661952 USDT**

The message requested that I “hold on to this message” and implied access to the funds.



---

3. Initial Assessment

The message raised multiple red flags commonly associated with social engineering and phishing scams, including:

- Emotional manipulation (suicide and loneliness narrative)
- Unsolicited financial offer from a stranger
- Disclosure of login credentials

- Promise of unusually large cryptocurrency funds
- Request to interact with an external website

While no immediate concern for personal safety was identified, the scenario strongly indicated a potential scam.

---

4. Investigation Methodology

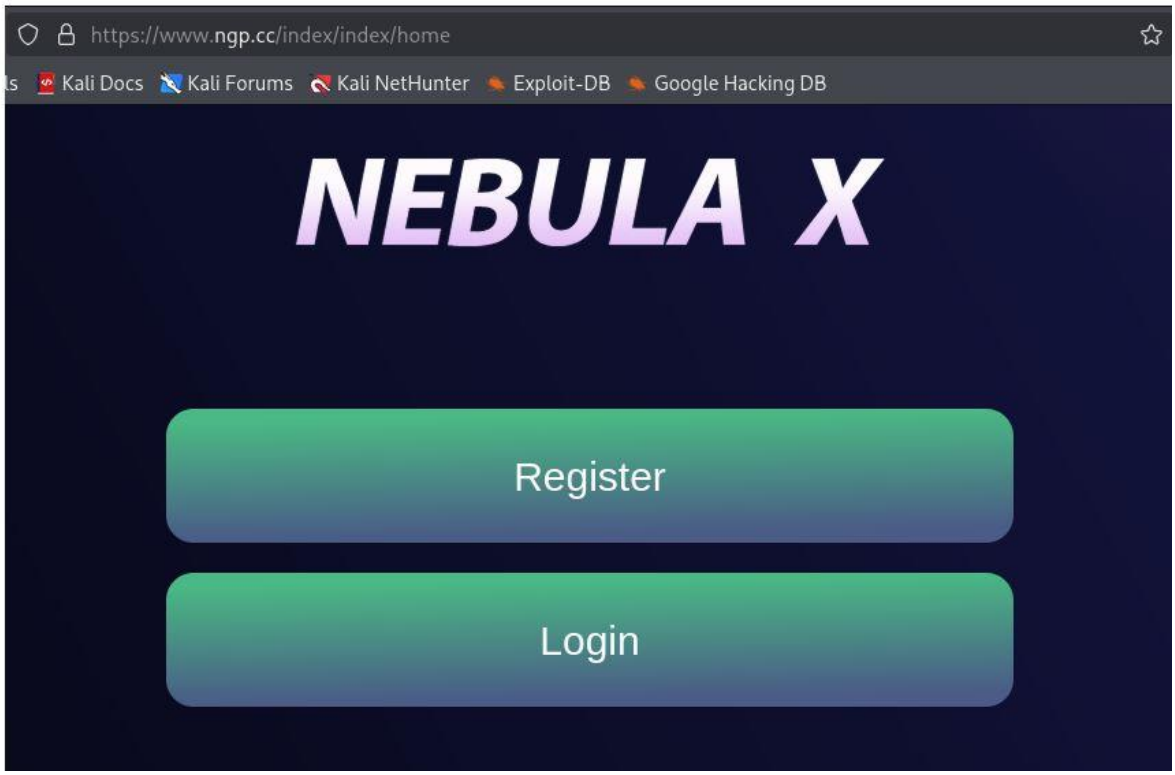
As a cybersecurity professional, I conducted a **controlled investigation** strictly within a **virtualized home lab environment** to avoid any risk to personal systems or data.

Environment Used

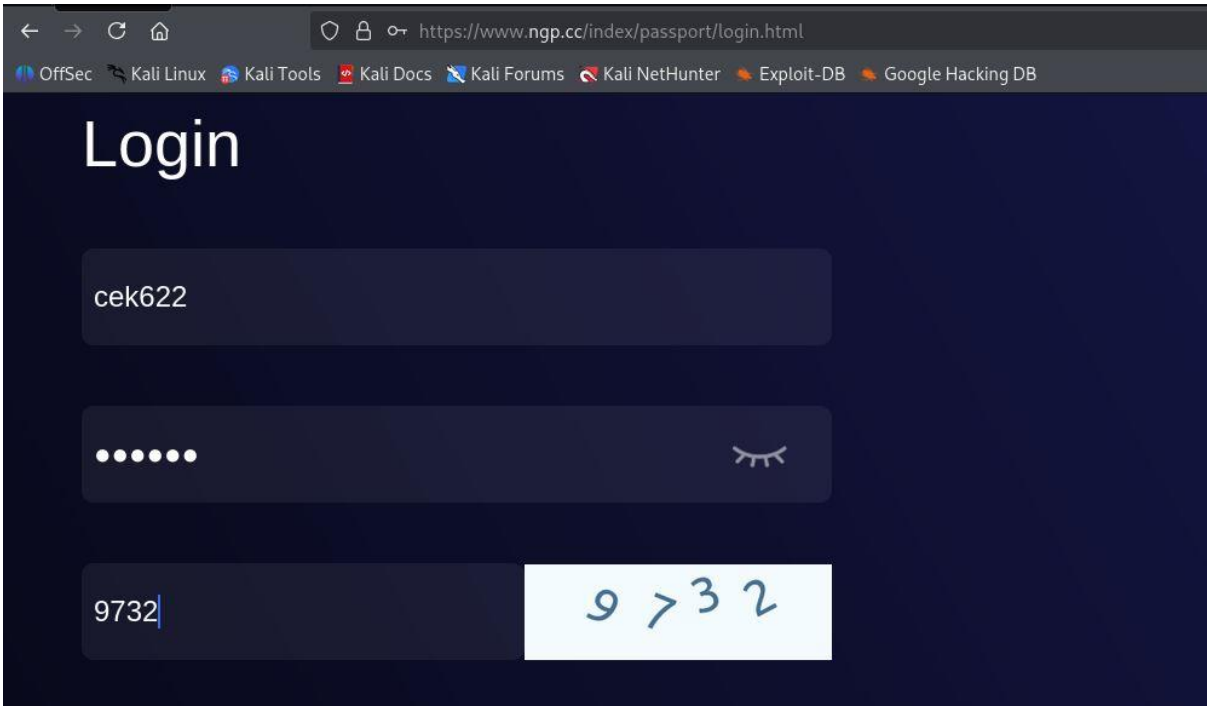
- Isolated virtual machine (VM)
- No personal credentials or wallets used
- Newly generated USDT wallet address for testing
- Network isolation enabled

Actions Taken

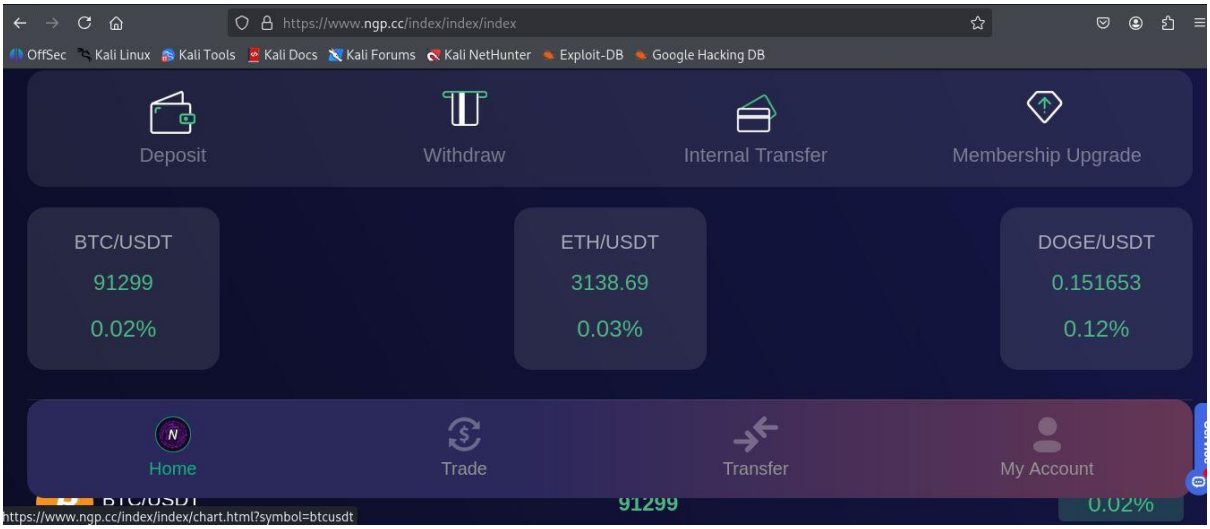
1. Visited the provided URL using the browser in the virtual machine.

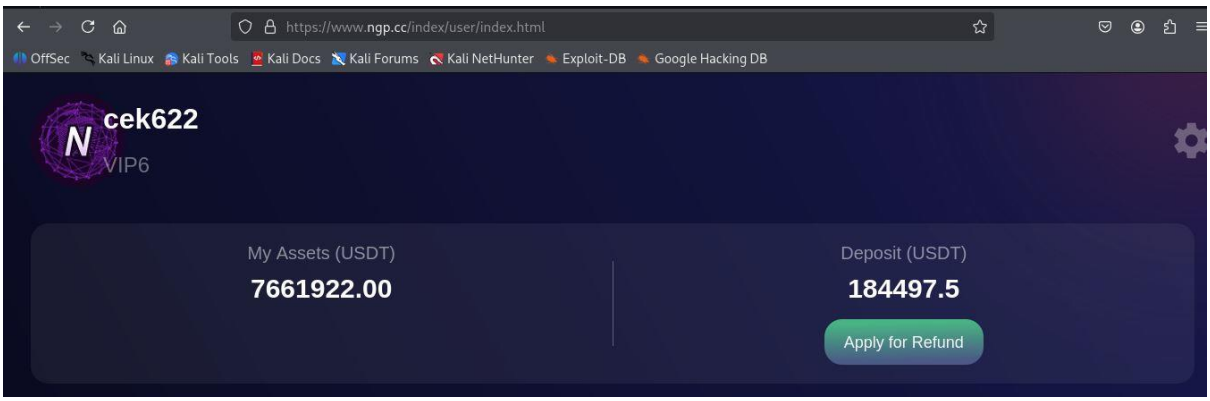


2. Logged into the website using the supplied credentials solely to observe behaviour.

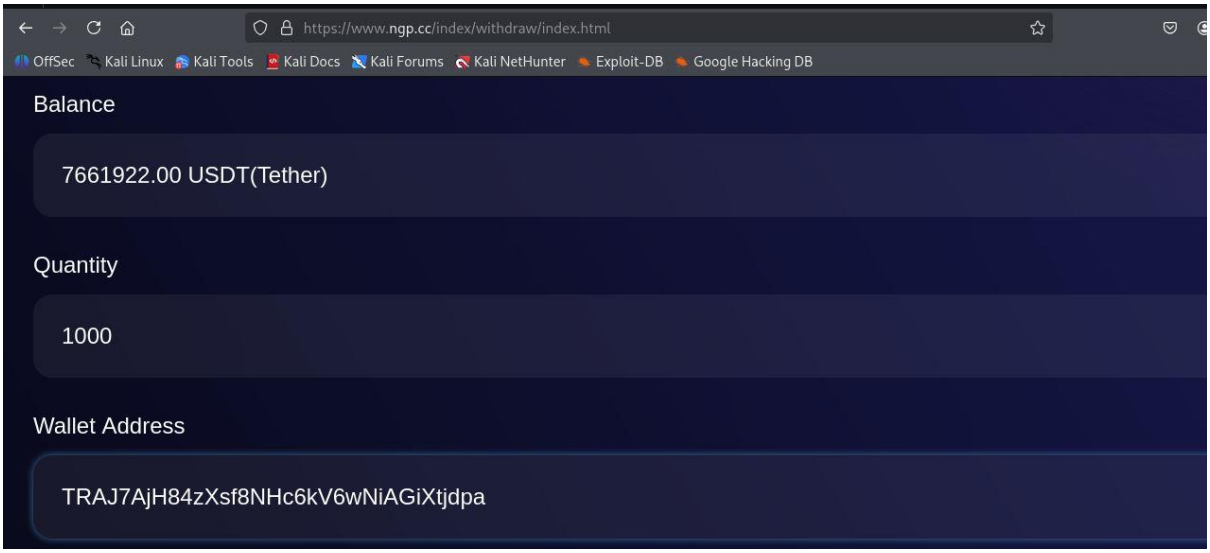


3. Confirmed that a balance was displayed on the account.





4. Attempted to withdraw funds to a newly generated test USDT wallet address.
5. Observed that the withdrawal process did not proceed beyond a certain point.



6. Conducted reputation and threat analysis using open-source intelligence tools.

---

5. Technical Findings

Website Analysis

- The website did not use a genuine or secure configuration.
- The URL showed characteristics consistent with malicious or fraudulent platforms.
- The withdrawal process appeared intentionally blocked, a common tactic used to encourage victims to pay “fees” or provide further sensitive information.

Threat Intelligence Results

The URL was analysed using the following open-source tools:

- **VirusTotal**
- **URLScan.io**
- **PhishTank**

Results indicated that **at least three cybersecurity vendors** had flagged the URL as a **phishing site**.

---

6. Indicators of Compromise (IOCs)

- Suspicious domain: www.ngp.cc
- TikTok private message delivery vector
- Emotional social engineering content
- Fake cryptocurrency balance display

- Blocked withdrawal functionality

---

7. Impact Assessment

- No financial loss occurred.
- No personal or sensitive information was compromised.
- No personal systems were affected due to the use of an isolated lab environment.

---

8. Conclusion

The investigation confirms that the TikTok message was part of a **cryptocurrency phishing and social engineering scam**. The attacker leveraged emotional manipulation combined with fake crypto account access to lure victims into interacting with a malicious website.

The website was confirmed as malicious through independent open-source threat intelligence platforms. The inability to withdraw funds aligns with known scam patterns designed to extract fees, credentials, or wallet information from victims.

---

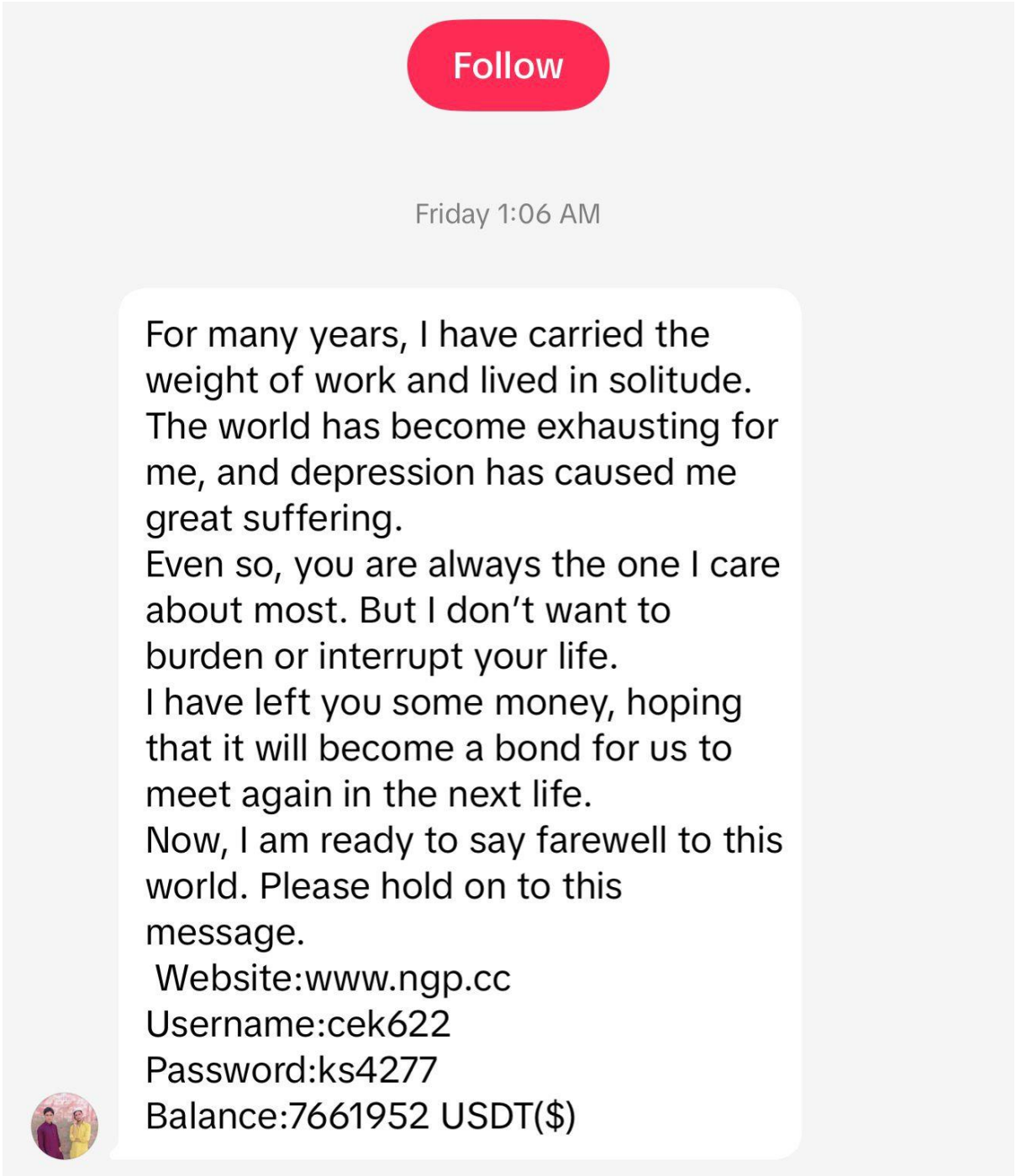
9. Recommendations

- Do not engage with unsolicited financial offers received via social media.
- Avoid logging into unknown websites using provided credentials.
- Report the account and message to TikTok.
- Share indicators of compromise with relevant cybersecurity communities.
- Continue using isolated environments for investigating suspicious content.

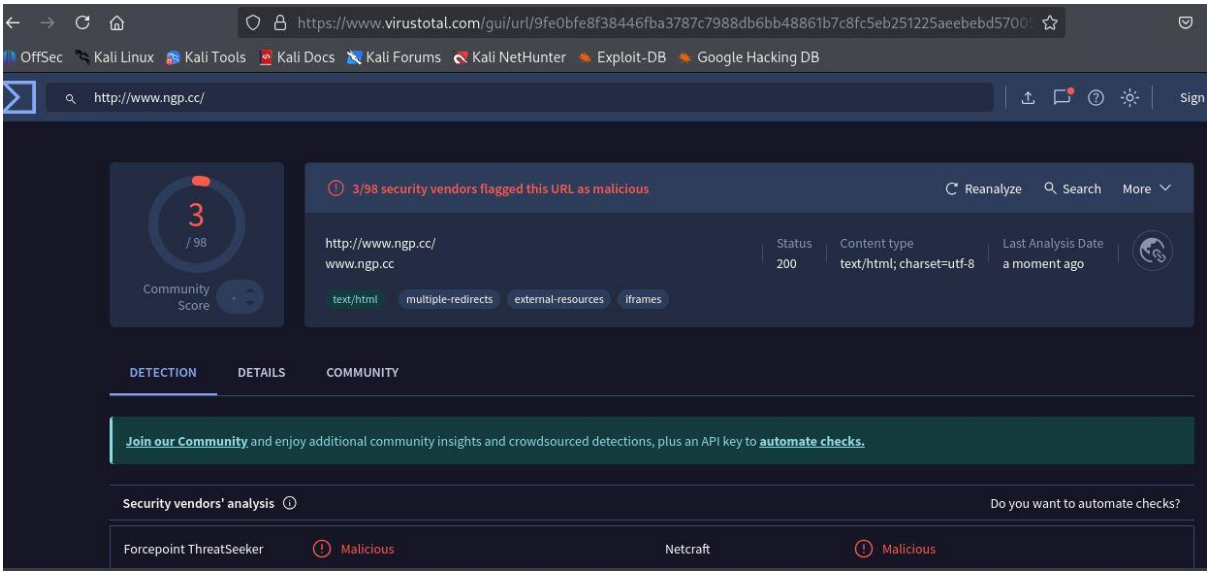
---

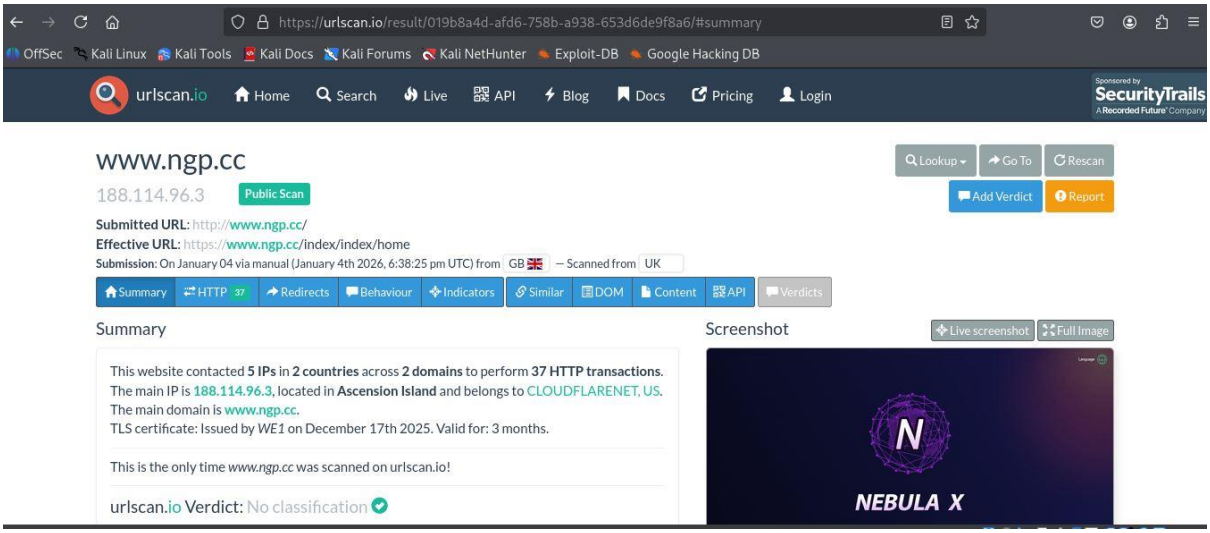
10. Evidence Attached

- Screenshot of the TikTok private message



- OSINT scan results (VirusTotal, URLScan.io, PhishTank)


https://www.virustotal.com/gui/url/9fe0bfe8f38446fba3787c7988db6bb48861b7c8fc5eb251225aeebebd5700
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
http://www.ngp.cc/
Sign
3
/ 98
Community Score
3/98 security vendors flagged this URL as malicious
Reanalyze
Search
More
http://www.ngp.cc/
www.ngp.cc
Status
200
Content type
text/html; charset=utf-8
Last Analysis Date
a moment ago
text/html
multiple-redirects
external-resources
iframes
DETECTION
DETAILS
COMMUNITY
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Security vendors' analysis
Do you want to automate checks?
Forcepoint ThreatSeeker
Malicious
Netcraft
Malicious


https://urlscan.io/result/019b8a4d-afd6-758b-a938-653d6de9f8a6/#summary
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
urlscan.io
Home
Search
Live
API
Blog
Docs
Pricing
Login
Sponsored by SecurityTrails
A Recorded Future Company
www.ngp.cc
188.114.96.3
Public Scan
Lookup
Go To
Rescan
Add Verdict
Report
Submitted URL: http://www.ngp.cc/
Effective URL: https://www.ngp.cc/index/index/home
Submission: On January 04 via manual (January 4th 2026, 6:38:25 pm UTC) from GB — Scanned from UK
Summary
HTTP 37
Redirects
Behaviour
Indicators
Similar
DOM
Content
API
Verdicts
Summary
This website contacted 5 IPs in 2 countries across 2 domains to perform 37 HTTP transactions.
The main IP is 188.114.96.3, located in Ascension Island and belongs to CLOUDFLARENET, US.
The main domain is www.ngp.cc.
TLS certificate: Issued by WE1 on December 17th 2025. Valid for: 3 months.
This is the only time www.ngp.cc was scanned on urlscan.io!
urlscan.io Verdict: No classification
Screenshot
Live screenshot
Full Image
N
NEBULA X