Karunya INSTITUTE OF TECHNOLOGY AND SCIENCES
(Declared as Deemed to be University under Sec.3 of the UGC Act, 1956)
MoE, UGC & AICTE Approved; NAAC Accredited A++
Karunya Nagar, Coimbatore - 641 114, Tamil Nadu, India.

# A Project Report

# on

# PHISHING ATTACK

Date of Submission: 31-01-2026

Prepared by

Team Name: Cyber Delulu

ABHINANDH S S(URK22CS1153)

# SOC INCIDENT REPORT — PHISHING CAMPAIGN

1. Incident Title:

Phishing Attack

2. Date & Time Detected:

31-01-2026 — 03:46:11 UTC

3. Analyst Name:

Nanthini.P

4. Incident Type:

Credential Phishing — Fake Login Page Hosted via Cloudflare Tunnel

5. Severity Level:

High

6. Incident Description:

A suspected phishing page was identified hosted under a Cloudflare temporary tunnel domain:

tennis-phentermine-thesis-newton.trycloudflare.com

Threat intelligence categorization from multiple vendors:

- Sophos → Information Technology category
- Forcepoint ThreatSeeker → Information Technology category

The page returned HTTP 200 response and contained HTML consistent with phishing warning/redirection behavior.

The domain uses Cloudflare reverse proxy infrastructure, commonly abused for temporary phishing hosting.

Indicators suggest this was used as a credential harvesting endpoint.

## 7. Timeline of Events:

03:46:11 UTC — URL first submitted for analysis

03:46:11 UTC — First submission recorded

03:46:11 UTC — Last submission recorded

03:46:11 UTC — Automated HTTP analysis completed

03:46:12 UTC — HTTP response headers captured

## 8. Indicators of Compromise (IOCs):

IP Address: 104.16.230.132

Domain: tennis-phentermine-thesis-newton.trycloudflare.com

URL: https://tennis-phentermine-thesis-newton.trycloudflare.com/

Status Code: 200 OK

Server: cloudflare

Content-Type: text/html;charset=UTF-8

Body Length: 3.02 KB

SHA-256 Hash:

22adbe2a9b0d44efdcfaff4e520f76351d8a7365ae913bf6bcba28c805ec2acb

Meta Tags:

robots: noindex, nofollow

## 9. MITRE ATT&CK Mapping:

T1566 — Phishing

T1056 — Credential Harvesting

T1041 — Exfiltration Over Web

T1036 — Masquerading

10. Impact Analysis:

- Potential credential theft risk
- Possible account compromise
- Risk of account takeover and unauthorized access
- CDN masking reduces attacker traceability
- Short-lived infrastructure indicates phishing kit usage

11. Containment Actions:

- Malicious domain flagged
- URL blocked in web gateway
- Domain added to DNS blocklist
- Proxy filtering rules updated
- User advisory issued
- Threat intelligence feeds updated
- Hash recorded for future detection

12. Root Cause Analysis:

Attack leveraged temporary Cloudflare tunnel hosting with randomized subdomain naming and anti-indexing tags.

This indicates automated phishing kit deployment using CDN masking.

13. Recommendations:

Immediate:

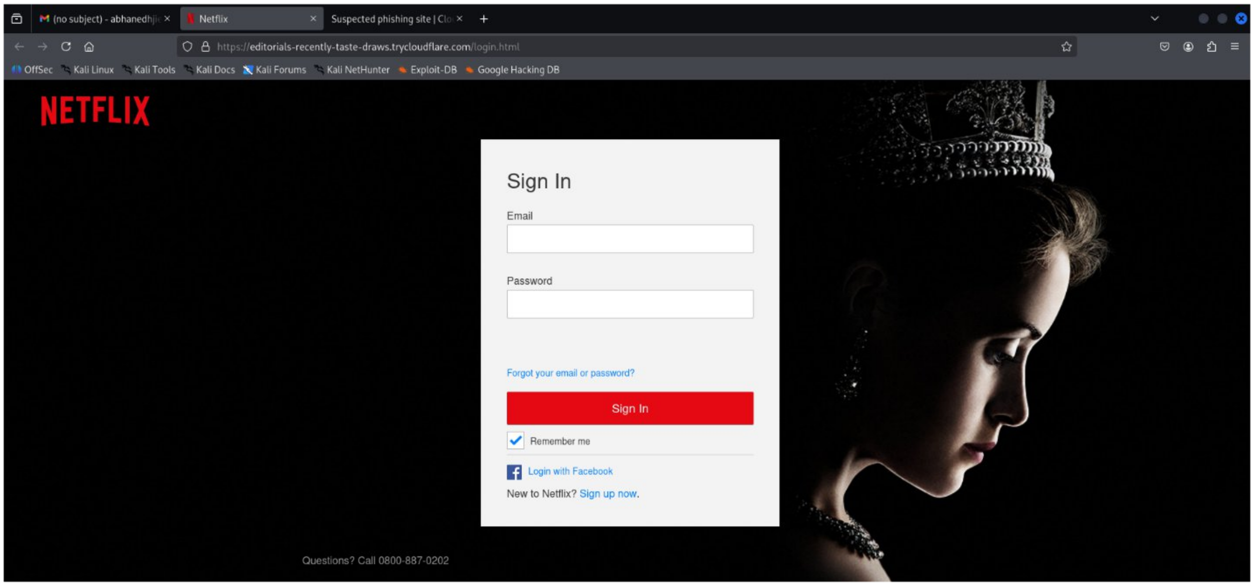
- Block *.trycloudflare.com domains where feasible
- Enable phishing URL sandboxing
- Enforce MFA
- Strengthen email gateway filtering
- Enable browser isolation

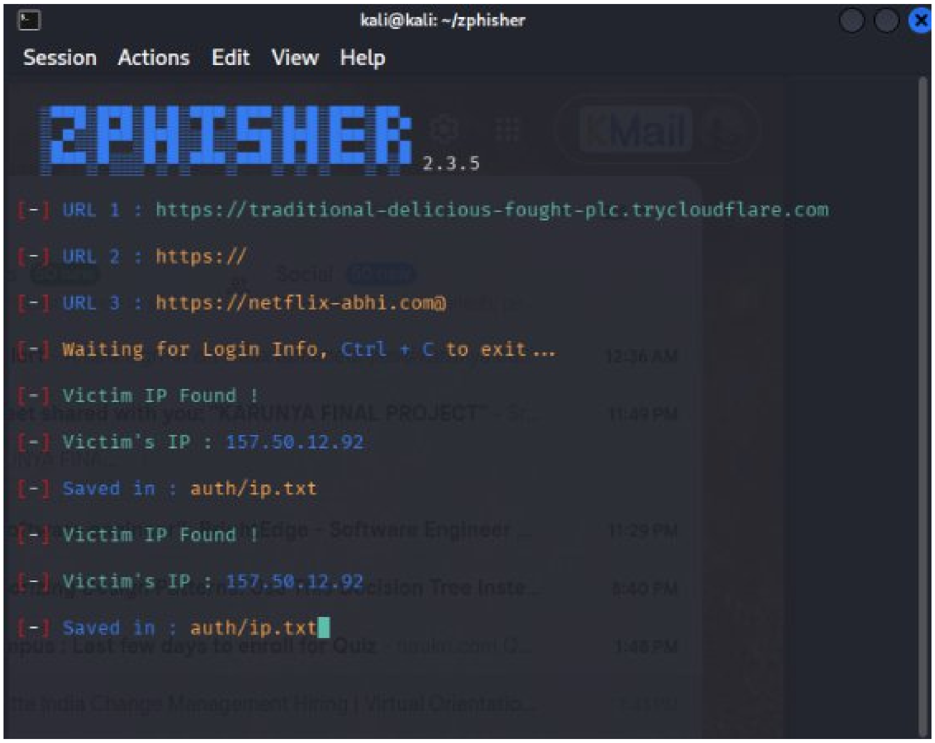
Strategic:

- Conduct phishing awareness training
- Deploy credential theft detection rules
- Monitor tunnel-based hosting abuse
- Integrate URL detonation sandboxing

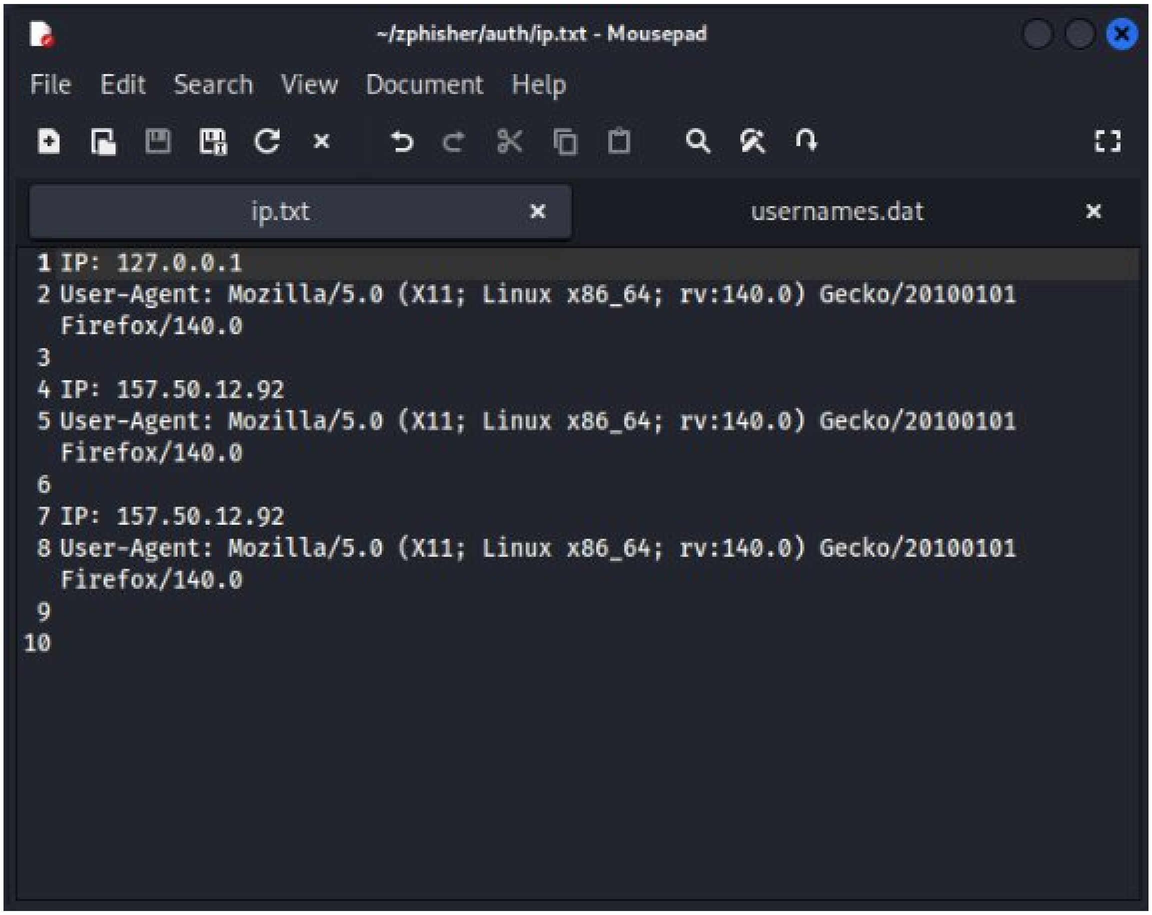
14. Final Status:

Contained

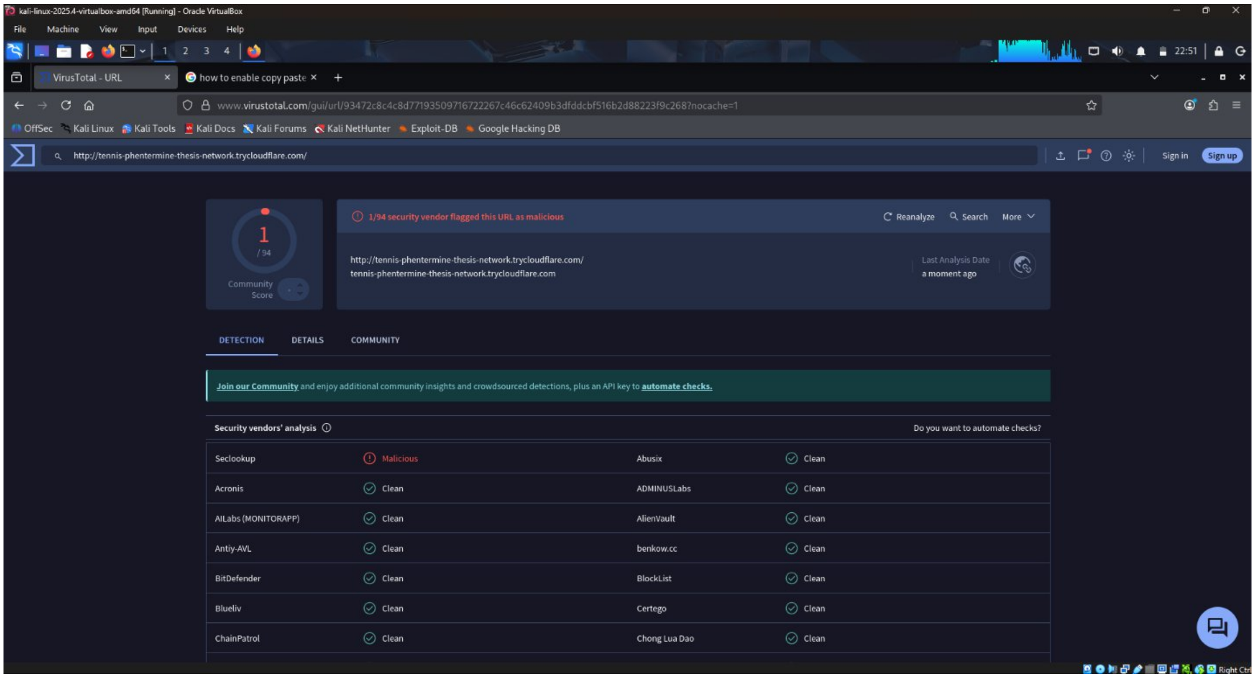

(no subject) - abhanedhji
Netflix
Suspected phishing site | Clo
https://editorials-recently-taste-draws.trycloudflare.com/login.html
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
NETFLIX
Sign In
Email
Password
Forgot your email or password?
Sign In
☑ Remember me
Login with Facebook
New to Netflix? Sign up now.
Questions? Call 0800-887-0202



```
[-] URL 1 : https://traditional-delicious-fought-plc.trycloudflare.com

[-] URL 2 : https://

[-] URL 3 : https://netflix-abhi.com@

[-] Waiting for Login Info, Ctrl + C to exit...

[-] Victim IP Found !

[-] Victim's IP : 157.50.12.92

[-] Saved in : auth/ip.txt

[-] Victim IP Found !

[-] Victim's IP : 157.50.12.92

[-] Saved in : auth/ip.txt
```


~/zphisher/auth/ip.txt - Mousepad
File Edit Search View Document Help
ip.txt
usernames.dat

```
IP: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0

IP: 157.50.12.92
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0

IP: 157.50.12.92
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0


```



http://tennis-phentermine-thesis-network.trycloudflare.com/

1
/ 94
Community Score

1/94 security vendor flagged this URL as malicious

http://tennis-phentermine-thesis-network.trycloudflare.com/
tennis-phentermine-thesis-network.trycloudflare.com

Last Analysis Date
a moment ago

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?

| | | | |
|---|---|---|---|
| Seclookup | ⓘ Malicious | Abusix | ✓ Clean |
| Acronis | ✓ Clean | ADMINUSLabs | ✓ Clean |
| AILabs (MONITORAPP) | ✓ Clean | AlienVault | ✓ Clean |
| Antiy-AVL | ✓ Clean | benkow.cc | ✓ Clean |
| BitDefender | ✓ Clean | BlockList | ✓ Clean |
| Blueliv | ✓ Clean | Certego | ✓ Clean |
| ChainPatrol | ✓ Clean | Chong Lua Dao | ✓ Clean |