

Student name : Chrisin Zacharia John

Date : 31-01-2026

SOC INCIDENT REPORT — PHISHING CAMPAIGN

1. Incident Title:

Phishing Attack

2. Date & Time Detected:

31-01-2026 — 03:46:11 UTC

3. Analyst Name:

Chrisin Zacharia John

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:

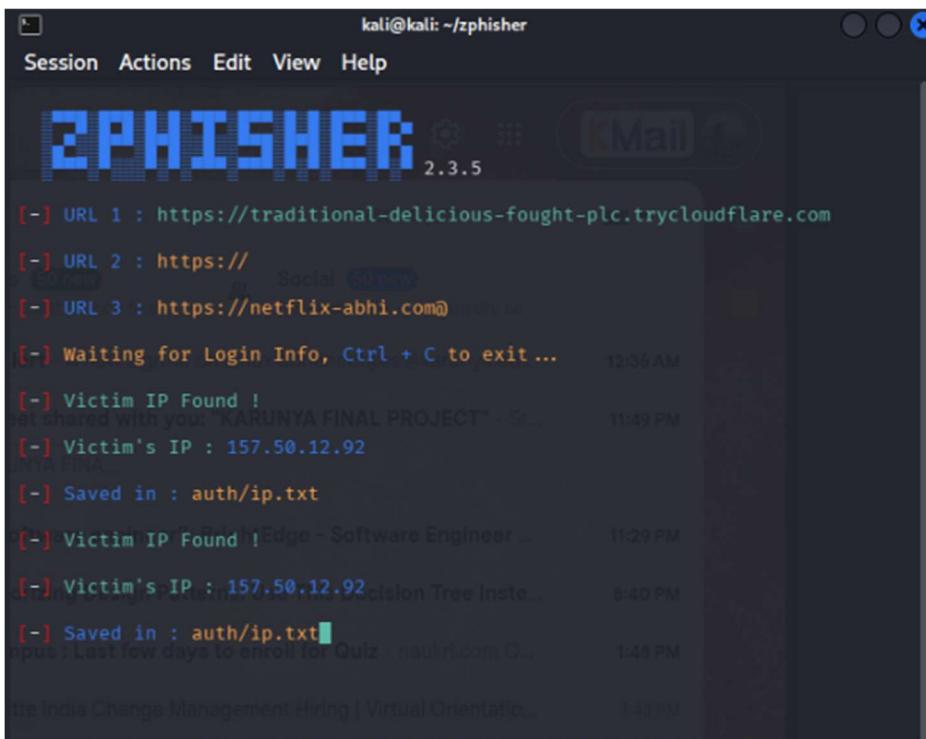
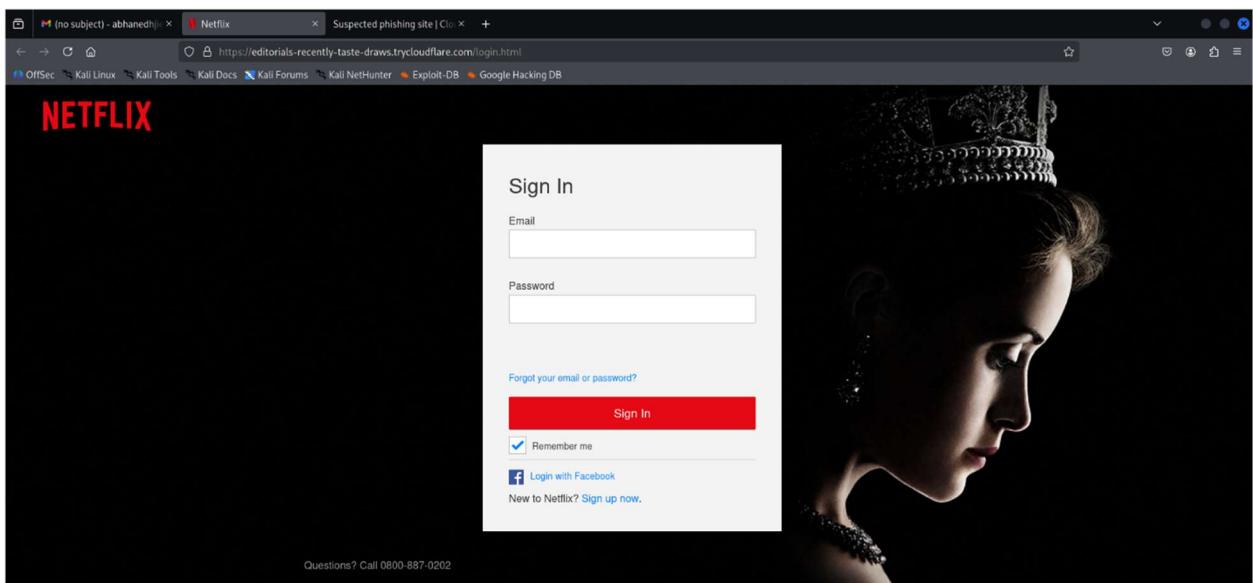
- Block *.trycloudflare.com domains where feasible
- Enable phishing URL sandboxing
- Enforce MFA
- Strengthen email gateway filtering
- Enable browser isolation

Strategic:

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

14. Final Status:

Contained



~/zphisher/auth/ip.txt - Mousepad

File Edit Search View Document Help

ip.txt usernames.dat

```
1 IP: 127.0.0.1
2 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101
  Firefox/140.0
3
4 IP: 157.50.12.92
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101
  Firefox/140.0
6
7 IP: 157.50.12.92
8 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101
  Firefox/140.0
9
10
```

kali-linux-2025.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox

VirusTotal - URL

File Machine View Input Devices Help

22:51

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

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

1/94 security vendor flagged this URL as malicious

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

Community Score

Detection Details Community

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Do you want to automate checks?

Security vendors' analysis	Malicious	Clean
Seclockup	Malicious	Clean
Acronis	Clean	Clean
AI Labs (MONITORAPP)	Clean	Clean
Anti-AVL	Clean	Clean
BitDefender	Clean	Clean
Blueliv	Clean	Clean
ChainPatrol	Clean	Clean
Abusix	Clean	Clean
ADMINUSLabs	Clean	Clean
AlienVault	Clean	Clean
benkow.cc	Clean	Clean
BlockList	Clean	Clean
Certego	Clean	Clean
Chong Lua Dao	Clean	Clean

