



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:

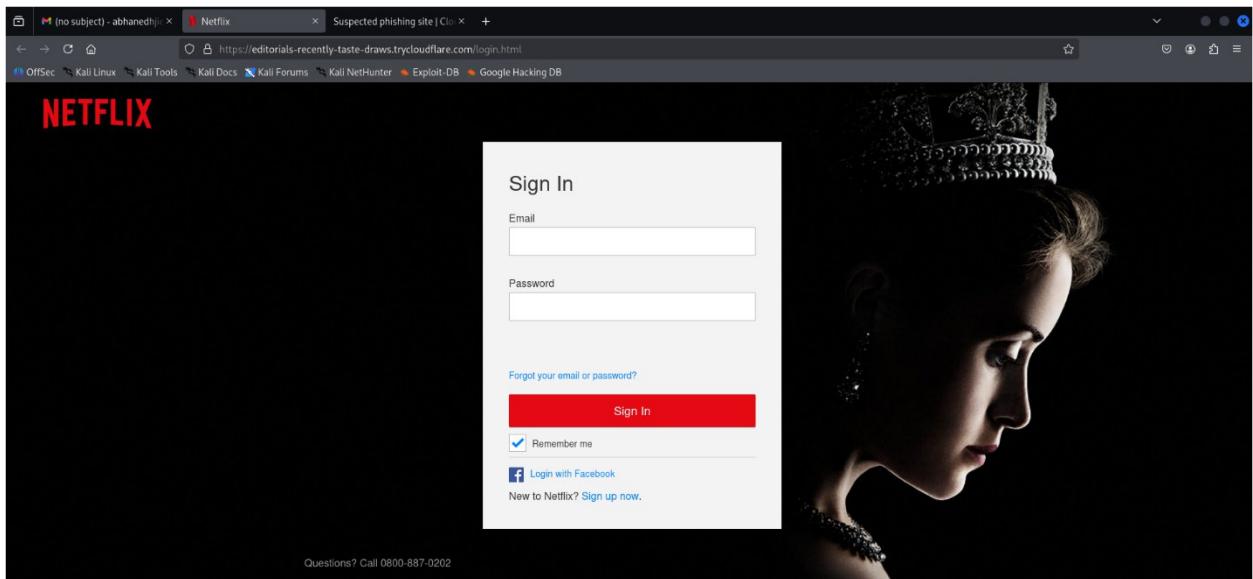
- Block *.trycloudflare.com domains where feasible
- Enable phishing URL sandboxing
- Enforce MFA
- Strengthen email gateway filtering
- Enable browser isolation

Strategic:

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

14. Final Status:

Contained



kali@kali: ~/zphisher

Session Actions Edit View Help

ZPHISHER 2.3.5

```
[+] 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... 12:36 AM
[+] Victim IP Found !
[+] shared with you "KARUNYA FINAL PROJECT" - 11:49 PM
[+] Victim's IP : 157.50.12.92
[+] Saved in : auth/ip.txt
[+] Victim IP Found ! Edge - Software Engineer ... 11:29 PM
[+] Victim's IP : 157.50.12.92 cision Tree Inste... 8:40 PM
[+] Saved in : auth/ip.txt
[+] Last few days to enroll for Quiz - quizku.com (2... 1:48 PM
[+] India Change Management Hiring | Virtual Orientatio...
```

~/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

File Machine View Input Devices Help

VirusTotal - URL how to enable copy paste +

www.virustotal.com/gui/url/93472c8c4c8d77193509716722267c46c62409b3dfddcbf516b2d88223f9c268?nocache=1

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

Σ http://tennis-phentermine-thesis-network.trycloudflare.com/ Sign in Sign up

1/94 security vendor flagged this URL as malicious

Community Score

REANALYZE Search More

Last Analysis Date a moment ago

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 vendor's analysis	
Seclookup	Malicious
Acronis	Clean
AI Labs (MONITORAPP)	Clean
Anti-AVL	Clean
BitDefender	Clean
Bluediv	Clean
ChainPatrol	Clean
Abusix	Clean
ADMINUSLabs	Clean
AllerVault	Clean
benkow.cc	Clean
BlockList	Clean
Certego	Clean
Chong Lua Dao	Clean

Right Click

Detailed description: This screenshot shows a Kali Linux desktop environment running in Oracle VM VirtualBox. A Firefox browser window is open to the VirusTotal URL analysis page. The main content area displays a summary that 1 out of 94 security vendors flagged the URL as malicious. Below this is a 'Community Score' section with a large red '1' and '94'. A table lists the results from various security vendors, with most showing 'Clean' status except for Seclookup which flagged it as 'Malicious'. There are tabs for 'DETECTION', 'DETAILS', and 'COMMUNITY'. A green bar at the bottom encourages joining the community. On the right side of the browser window, there are 'Reanalyze', 'Search', and 'More' buttons, along with a note about the last analysis date. At the bottom of the browser, there's a link to 'Join our Community' and an 'Automate checks' button. The desktop background shows a dark blue gradient with a small white icon in the bottom right corner. The taskbar at the bottom has several icons, including a terminal and file manager.