OSINT Report – BROTOTYPE

Date 09-12-2025
Name : ATHU: V A
Target : Brototype

OBJECTIVES

To conduct a comprehensive Open Source Intelligence (OSINT) investigation into **Brototype** (legally operating as **Packapeer Academy Pvt Ltd**) to verify its corporate legitimacy, map its digital infrastructure, and assess potential risks for students and stakeholders.

- **Corporate Verification:** To confirm the legal existence, registration status, and key decision - makers (Directors/CEO) of the entity "Packapeer Academy Pvt Ltd" using government databases (Zauba Corp, MCA).

- **Infrastructure Mapping:** To enumerate the company's digital footprint, including hidden subdomains, hosting providers, and third-party technologies (LMS, Tracking Pixels) to understand how they manage student data.

TOOLS USED

- Basic company information (Linkedin,Instagram,reddit,)
  > Linkedin
  > Instagram
  > reddit
  > google

- Domain and Website footprint(cmd ping,nslookup)
  > cmd(ping)
  >nslookup
  >DNS checker
  >whois.domaintools
  >SSL lab
  >who.is
  > DNS dumster
  >Maltigo

-

Company Overview

Name: Brototype/packapeer
Co Founder/CEO: Nikil Kilivayil
CO Founder/CTO:Faizal
Founded: 07-05-2019
Industry: Ed-Tech / Coding Bootcamp
Products: IT related course
Employees : 50-200
Website : https://www.brototype.com
Phone: 7034395811

Office Locations (with Google Maps Links)

> Kochi - https://maps.app.goo.gl/uYSF7iZ2EZS9rDDR8
> Kozikode - https://maps.app.goo.gl/kc94vyYG95WJBDsQ7
> Thrivandrum - https://maps.app.goo.gl/X2NSMFcbyb7eJbaU9
> Bengaluru - https://maps.app.goo.gl/kNBG2mwDnLmZ9aTk8

Social Media

Instagram : https://www.instagram.com/brototype.malayalam
youtube : https://www.youtube.com/@BrototypeMalayalam
Linkedin : https://www.linkedin.com/company/brototype
Facebook - https://www.facebook.com/brototypemalayalam

Domain Information

Main website - https://www.brototype.com
Domain Name - brototype.com
Registrar – GoDaddy.com,LLC
Expires-2030-11-10
ip - 157.245.98.112

DNSDumpster Results

Hosting Provider - DigitalOcean, LLC
Location – Bangaluru
ASN (Autonomous System Number) - **AS14061** (DigitalOcean Network)
Network Range (CIDR) - **157.245.0.0/16** → belongs entirely to DigitalOcean.

subdomain Enumeration

Subdomain	IP Address
api.brototype.com	64.227.181.76
app.brototype.com	139.59.31.160
brocamp.brototype.com	64.227.157.184
company.brototype.com	139.59.92.86
fa.brototype.com	128.199.25.250
grafana.brototype.com	139.59.32.172
graphql.brototype.com	167.71.229.243
practice.brototype.com	66.241.125.19
refer.brototype.com	139.59.92.86
reviewer.brototype.com	139.59.80.145
student.brototype.com	139.59.92.86
study.brototype.com	178.16.136.145
test-api.brototype.com	139.59.39.101
test-app.brototype.com	68.183.87.198
test-company.brototype.com	64.227.180.182
test-manifest.brototype.com	64.227.180.182
test-refer.brototype.com	64.227.180.182
test-student.brototype.com	64.227.180.182
test2-app.brototype.com	68.183.90.136
test3-app.brototype.com	157.245.108.47
test3-reviewer.brototype.com	157.245.108.47
v2-app.brototype.com	139.59.80.145
www.brototype.com	157.245.98.112

-

open services/ports

- SSH port 22 is open (dangerous if not secured).
    - ssh: SSH-2.0-OpenSSH_9.6p1 Ubuntu
- The website uses the **Nginx web server**(port 80,443)
    - http: nginx/1.24.0 (Ubuntu)
    - https: nginx/1.24.0 (Ubuntu)

Technologies detected

tech: Ubuntu - Operating system

tech: Nginx:1.24.0 - Web server

tech: PHP - Programming language used

tech: LiteSpeed - Monitoring tool

tech: Zabbix - Alternative web server

protection - cloudflare

MX Records (Email Servers)

Brototype emails are handled by Google.

POTENTIAL VULNERABILITIES FOUND FROM THE DNSDUMPSTER DATA

1. SSH Port (22) Open on Almost All Servers

Example from scan:

ssh: SSH-2.0-OpenSSH_9.x Ubuntu

Why this is risky:

- Attackers can attempt **brute-force attacks**

- If weak passwords exist, systems can be compromised
- SSH should ideally be restricted or accessible only via VPN

2. Multiple Nginx Versions Exposed

Versions seen:

- Nginx 1.18.0
- Nginx 1.24.0
- Nginx 1.26.0

Why this is risky:

- Attackers can search for **known vulnerabilities** in these versions
- Version disclosure helps attackers plan targeted exploits

Fix:

Disable version exposure in Nginx.

---

3. Many Test Subdomains Exposed Publicly

Examples:

- test-api.brototype.com
- test-app.brototype.com
- test-company.brototype.com
- test-student.brototype.com
- test3-app.brototype.com
- test3-reviewer.brototype.com
- test2-app.brototype.com

Why this is risky:

- Test environments usually have **weak security**
- May contain:
  - Debug info
  - Hardcoded credentials
  - Unprotected APIs
  - Old versions of software

4. Exposed Monitoring Tools

Detected:

- **Grafana**
- **Zabbix**

Why this is serious:

These tools:

- Contain sensitive system data
- If misconfigured, attackers can access dashboards
- Often have known default passwords

5. Multiple Subdomains Using Same IP

Example:
student.brototype.com
company.brototype.com
refer.brototype.com

All use the same IP: **139.59.92.86**

Why this is risky:

- One subdomain vulnerability can compromise ALL sites on the server
- Attackers can pivot inside the server

MOST CRITICAL RISKS (Summary)

Risk	Why Serious
SSH open everywhere	Brute-force attacks possible
Test subdomains	High chance of weak security & leaks
Monitoring tools exposed	Attackers gain system-level visibility
Old/default Nginx pages	Shows weak hardening
FTP running	Very outdated & insecure

Conclusion

The target (brototype.com) has **significant exposure** due to open SSH ports, publicly available test environments, and leaked version information. While the infrastructure is modern (DigitalOcean + Cloudflare + Ubuntu), the operational security is weak.