Passive Reconnaissance Report

Target Domain

Domain: [REDACTED]

1. WHOIS Lookup

- Registrar: NameCheap, Inc. (IANA ID: 1068)
- WHOIS Server: whois.namecheap.com
- Created: August 31, 2019 | Expires: August 31, 2025
- Last Updated: August 1, 2024
- Domain Status: clientTransferProhibited
- Nameservers:
  - dns1.registrar-servers.com
  - dns2.registrar-servers.com
- DNSSEC: Not enabled
- Abuse Contact: abuse@namecheap.com | +1.661.310.2107

2. DNS Records Summary (via dig & nslookup)

A Record:

- [REDACTED] -> xxx.xxx.xxx.xxx

AAAA Record:

- No AAAA record returned (IPv6 not configured)

CNAME Record:

- No CNAME found for root domain

MX Record:

- mailserver.purelymail.com (priority 10)
- IP: xxx.xxx.xxx.xxx

SOA Record:

- Server: dns1.registrar-servers.com
- Admin: hostmaster.registrar-servers.com
- Serial: 1747782390 | Refresh: 43200 | Retry: 3600 | Expire: 604800

TXT Records:

Passive Reconnaissance Report

- google-site-verification=[REDACTED]
- purelymail_ownership_proof=[REDACTED]
- SPF: v=spf1 include:_spf.purelymail.com ~all

3. DNSDumpster Findings

Subdomain Identified:
- ip.[REDACTED] -> xxx.xxx.xxx.xxx

Mail Server:
- mailserver.purelymail.com -> xxx.xxx.xxx.xxx

Nameservers:
- dns1.registrar-servers.com -> xxx.xxx.xxx.xxx
- dns2.registrar-servers.com -> xxx.xxx.xxx.xxx

TXT Records:
- Matched dig/lookup results

4. Shodan Enumeration

Initial search using the domain [REDACTED] yielded no results.

However, querying its resolved IP (xxx.xxx.xxx.xxx) allowed Shodan enumeration:

- ISP: Comcast Cable Communications
- Geo: United States

Open Ports:
- Port 80 (HTTP): 301 redirect using OpenResty (NGINX-based)
- Port 443 (HTTPS): TLS handshake error: TLSV1_UNRECOGNIZED_NAME
- Port 3478 (UDP): STUN service detected, likely used for NAT traversal or real-time communication. Returned different IP in response, suggesting relay infrastructure.

5. Technical Observations

- [OK] WHOIS and DNS records appear standard.
- [!] No IPv6 address available (missing AAAA record).
- [!] SSL/TLS handshake issue on port 443 (potential misconfiguration).

Passive Reconnaissance Report

- [OK] SPF and TXT records present and valid.
- [OK] STUN on 3478 suggests VoIP or RTC functionality in backend.

6. Additional Notes

- Shodan scan worked only after manual resolution of domain to IP.
- DNS and email systems use third-party providers (Namecheap, PurelyMail).
- DNSSEC not configured - security can be improved.
- TXT records show integrations such as Google verification.

7. Recommendations

1. Resolve TLS/SSL certificate errors (port 443).
2. Review STUN server exposure and limit to necessary services.
3. Enable IPv6 where possible.
4. Add DNSSEC to increase trust and security posture.
5. Monitor software like OpenResty for known vulnerabilities.

Analyst

Prepared by: Paul Harrison
Cybersecurity Intern