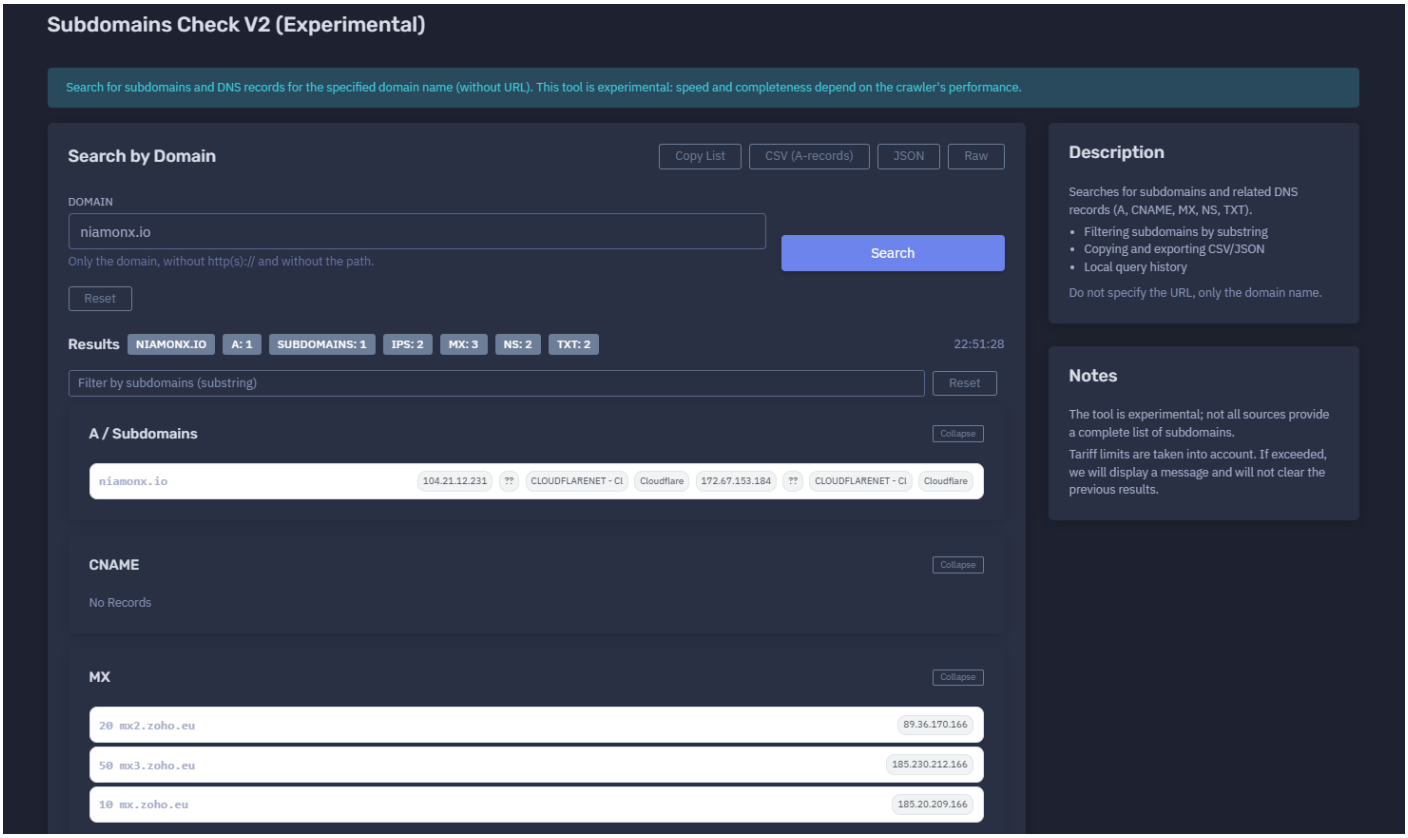
Subdomains Check V2 | Experimental Subdomain & DNS Records Discovery Tool



The platform available at **https://dash.niamonx.io/subdomains_v2** — known as **Subdomains Check V2** — is an experimental domain intelligence tool within the NiamonX platform. It searches for subdomains and related DNS records for a specified domain name, including A records, CNAME records, MX records, NS records, TXT records, resolved IP addresses, and basic network/provider information.

This tool is designed for fast domain reconnaissance, DNS inventory, infrastructure mapping, attack surface review, OSINT analysis, SOC workflows, incident response, and technical asset discovery.

Because the module is experimental, the speed, coverage, and completeness of results may depend on crawler performance, available sources, DNS response behavior, and tariff limits.

Overview of the Service

Subdomains Check V2 helps users discover subdomains and associated DNS records for a target domain. The tool accepts a domain name, performs discovery and DNS resolution, then organizes the results into clear sections.

The module can return:

- A records
- Discovered subdomains
- Resolved IP addresses
- CNAME records
- MX records
- NS records
- TXT records
- Basic IP/network provider information
- Local request history
- Exportable CSV and JSON data

Subdomains Check V2 is useful when users need to quickly understand which public DNS records and subdomains are associated with a domain.

The tool is especially helpful for:

- OSINT analysts
- SOC teams
- Incident response teams
- Threat intelligence researchers
- Attack surface management teams
- Bug bounty researchers
- DNS administrators
- DevOps engineers
- Security auditors
- Brand protection teams
- Compliance teams
- Infrastructure owners

? How the Tool Works

When a user enters a domain name, Subdomains Check V2 searches for subdomains and related DNS records. The tool then resolves available records and presents the results in grouped sections.

Example input:

```
Domain: niamonx.io
```

Example result summary:

```
niamonx.io
A: 1
Subdomains: 1
IPs: 2
MX: 3
NS: 2
TXT: 2
22:51:28
```

Example resolved A / subdomain result:

```
niamonx.io
104.21.12.231
CLOUDFLARENET
Cloudflare

172.67.153.184
CLOUDFLARENET
Cloudflare
```

Example DNS records:

```
MX:
20 mx2.zoho.eu
50 mx3.zoho.eu
10 mx.zoho.eu

NS:
abdullah.ns.cloudflare.com
ashley.ns.cloudflare.com

TXT:
"google-site-verification=MQNH6Yoh9hKD1hgzeQtEb9VN5_ikdspHYQxlxGS6Y-4"
"v=spf1 include:zohomail.eu -all"
```

The tool provides a practical overview of both discovered subdomains and domain-level DNS configuration.

? Supported Input

Subdomains Check V2 accepts only a domain name.

Correct input examples:

```
niamonx.io
```

```
example.com
```

```
sub.example.com
```

```
company.org
```

Incorrect input examples:

```
https://niamonx.io
```

```
http://example.com
```

```
https://example.com/page
```

```
example.com/path
```

```
*.example.com
```

```
user@example.com
```

```
192.168.1.1
```

```
localhost
```

The interface guidance is:

```
Only the domain, without http(s):// and without the path.
```

Users should enter the domain only, without protocol, path, query parameters, fragments, wildcard prefixes, or URL formatting.

Recommended input format:

```
domain.tld
```

?? Main Function: Search by Domain

The main search field starts the domain discovery and DNS record collection process.

Example:

```
Search by Domain
Domain: niamonx.io
```

After the query is processed, the tool displays a result summary and grouped DNS sections.

The tool may collect and display:

- root domain A records;
- discovered subdomains;
- resolved IP addresses;
- CNAME records;
- MX records;
- NS records;
- TXT records;
- IP ownership/provider hints;
- local request history.

Because this version is experimental, results may vary depending on crawler performance and available data sources.

? Experimental Status

Subdomains Check V2 is marked as experimental.

Interface note:

```
This tool is experimental: speed and completeness depend on the crawler's performance.
```

This means:

- not all sources may return complete data;
- some subdomains may be missed;
- some records may be temporarily unavailable;
- crawler speed may vary;
- large domains may take longer;
- results may differ between repeated checks;
- DNS changes may affect output;
- tariff limits may affect whether a new query can be completed.

The tool should be treated as a fast discovery and enrichment layer, not as a guaranteed complete DNS inventory.

For critical security work, results should be validated with additional tools and repeated over time.

? Results Summary

The Results section provides a compact overview of the discovered records.

Example:

```
niamonx.io
A: 1
Subdomains: 1
IPs: 2
MX: 3
NS: 2
TXT: 2
22:51:28
```

Typical fields include:

Field	Description
Domain	The domain that was searched
A	Number of A-record hostnames or A-record groups found
Subdomains	Number of discovered subdomain entries
IPs	Number of resolved IP addresses
MX	Number of mail exchanger records
NS	Number of name server records
TXT	Number of text records

Field	Description
Time	Query time or result timestamp

The summary is useful for quick triage and comparison between multiple domain checks.

? A Records and Subdomains Section

The **A / Subdomains** section shows hostnames and their resolved IPv4 addresses.

Example:

```
A / Subdomains


niamonx.io
104.21.12.231
CLOUDFLARENET
Cloudflare

172.67.153.184
CLOUDFLARENET
Cloudflare
```

A records are used to map hostnames to IPv4 addresses.

This section helps users identify:

- public-facing hosts;
- CDN-backed services;
- cloud-hosted infrastructure;
- shared hosting or provider networks;
- exposed root-domain records;
- resolved subdomain infrastructure;
- IPs that should be enriched with WHOIS or ASN data.

A single hostname may resolve to multiple IP addresses because of:

- CDN usage;
- load balancing;
- high availability;
- geo-distributed infrastructure;
- provider-managed routing;
- DNS round-robin behavior.

? Network and Provider Information

Subdomains Check V2 may show basic provider or network hints next to resolved IP addresses.

Example:

```
CLOUDFLARENET - Cl
Cloudflare
```

This helps users quickly identify whether a hostname appears to be associated with:

- CDN providers;
- cloud providers;
- hosting companies;
- ISP infrastructure;
- security proxy services;
- managed DNS or edge networks.

Provider information is useful for triage, but it should not be treated as final attribution. For accurate infrastructure ownership analysis, users should also check IP WHOIS, ASN data, BGP routes, passive DNS, HTTP headers, and TLS certificates.

? Filtering by Subdomains

The tool provides filtering by subdomain substring.

Example:

```
Filter by subdomains (substring)
```

Filtering is useful when working with large result sets.

Users can search for terms such as:

```
api
```

```
admin
```

```
dev
```

```
stage
```

```
support
```

```
mail
```

This helps analysts quickly locate interesting, risky, or business-relevant hostnames.

? CNAME Records

The CNAME section displays canonical name records.

Example:

```
CNAME
No Records
```

A CNAME record points one hostname to another canonical hostname.

Example:

```
app.example.com → example.hosting-provider.com
```

CNAME records are useful for identifying:

- third-party services;
- cloud applications;
- SaaS integrations;
- CDN aliases;
- managed landing pages;
- verification targets;
- external dependencies;
- possible subdomain takeover risks.

If the tool shows:

```
No Records
```

it means no CNAME records were returned for the current result set.

Important security note: CNAME records pointing to third-party services should be reviewed carefully. Abandoned or misconfigured CNAME records may indicate potential subdomain takeover

risk, but this must be validated responsibly.

? MX Records

The MX section shows mail exchanger records for the domain.

Example:

```
MX
20 mx2.zoho.eu
50 mx3.zoho.eu
10 mx.zoho.eu
```

MX records define where e-mail for the domain should be delivered.

The number before the mail server is the MX priority.

Example:

```
10 mx.zoho.eu
```

Lower priority numbers are preferred first.

In the example above:

```
10 mx.zoho.eu
20 mx2.zoho.eu
50 mx3.zoho.eu
```

the mail server with priority `10` is preferred before `20` and `50`.

MX records are useful for:

- identifying mail providers;
- reviewing e-mail infrastructure;
- checking business mail routing;
- validating domain configuration;
- supporting phishing and spoofing investigations;
- preparing e-mail security reviews.

? MX IP Resolution

Subdomains Check V2 may also resolve MX hostnames to IP addresses.

Example:

```
20 mx2.zoho.eu
89.36.170.166

50 mx3.zoho.eu
185.230.212.166

10 mx.zoho.eu
185.20.209.166
```

This helps users understand not only which mail servers are configured, but also which IP addresses they resolve to.

MX IP resolution is useful for:

- mail infrastructure mapping;
- provider verification;
- allowlist planning;
- e-mail security review;
- incident response;
- troubleshooting mail delivery;
- comparing DNS results across time.

? NS Records

The NS section shows authoritative name servers for the domain.

Example:

```
NS
abdullah.ns.cloudflare.com
162.159.44.203

ashley.ns.cloudflare.com
172.64.32.71
```

NS records indicate which name servers are responsible for the domain’s DNS zone.

Name server data helps identify:

- DNS provider;
- authoritative DNS infrastructure;
- delegated DNS management;
- provider dependencies;
- DNS hosting configuration;
- security and availability posture.

The tool may also resolve name server hostnames to IP addresses.

Example:

```
abdullah.ns.cloudflare.com → 162.159.44.203
ashley.ns.cloudflare.com → 172.64.32.71
```

NS records are important during security audits because DNS provider compromise or misconfiguration can affect the entire domain.

? TXT Records

The TXT section displays text records associated with the domain.

Example:

```
TXT
"google-site-verification=MQNH6Yoh9hKD1hgzeQtEb9VN5_ikdspHYQxlxGS6Y-4"
"v=spf1 include:zohomail.eu -all"
```

TXT records may contain:

- SPF policies;
- DMARC records;
- DKIM records;
- domain ownership verification tokens;
- third-party service verification;
- security policy metadata;
- mail provider configuration;
- platform integration records.

TXT records are useful for identifying how a domain is connected to external services and how e-mail authentication is configured.

? SPF Records

TXT records may include SPF configuration.

Example:

```
v=spf1 include:zohomail.eu -all
```

SPF defines which mail servers are allowed to send e-mail on behalf of the domain.

In this example:

```
include:zohomail.eu
```

allows Zoho Mail infrastructure to send mail for the domain.

The ending:

```
-all
```

means mail from unauthorized senders should fail SPF validation.

SPF records are important for:

- preventing spoofing;
- e-mail authentication;
- phishing resistance;
- mail delivery reliability;
- domain security posture.

? Domain Verification Records

TXT records may also include verification tokens.

Example:

```
google-site-verification=MQNH6Yoh9hKD1hgzeQtEb9VN5_ikdspHYQxlxGS6Y-4
```

Verification records are commonly used by services such as:

- Google;
- Microsoft;
- Zoho;
- cloud providers;
- SaaS platforms;
- CDN services;
- mail providers;
- analytics platforms;
- search console tools.

These records prove domain ownership to third-party services.

Security teams should review TXT records to identify outdated, unused, or unexpected third-party integrations.

? Local Request History

Subdomains Check V2 stores a local request history in the browser.

Example interface note:

```
Request history (local)
Filter...
We keep the domain and a brief summary (up to 200 entries).
```

Example history item:

```
niamonx.io
A:1
Subs:1
IPs:2
17.06.2026, 22:51:28
```

Other examples:

```
itstep.org
A:50
Subs:50
IPs:2
```

```
16.05.2026, 22:37:48
```

```
haveibeenpwned.com
A:13
Subs:13
IPs:3
10.12.2025, 00:46:07
```

The local history helps users:

- repeat previous checks;
- compare domain summaries over time;
- continue investigation sessions;
- filter previous requests;
- quickly revisit recently analyzed domains.

Because history is stored locally in the browser, it may be removed when browser data is cleared or when the user changes browser profiles, devices, or private browsing sessions.

On shared or untrusted devices, users should clear local history after checking sensitive domains, client assets, or incident-related infrastructure.

? Tariff Limits

Subdomains Check V2 respects user tariff limits.

Interface note:

```
Tariff limits are taken into account. If exceeded, we will display a message and will not clear the previous results.
```

Important points:

- Each query may consume plan quota.
- Limits depend on the user’s active plan.
- Large or repeated searches may reach the limit faster.
- If the limit is exceeded, the tool displays a warning.
- Previous results remain visible when the limit is exceeded.
- The interface does not clear previous results after a limit error.

This behavior helps prevent users from losing their last successful result when a new query cannot be completed.

? Copying and Exporting Results

Subdomains Check V2 supports copying and exporting data.

Available actions may include:

- copy results;
- export CSV;
- export JSON;
- copy DNS records;
- preserve local history summaries.

Export features are useful for:

- security reports;
- SOC tickets;
- incident response notes;
- compliance evidence;
- asset inventory;
- attack surface documentation;
- spreadsheet analysis;
- automation workflows;
- historical comparison.

? CSV Export

CSV export allows users to work with results in spreadsheet tools or reporting systems.

CSV data may include:

- domain;
- hostname;
- record type;
- record value;
- resolved IP;
- provider information;
- priority for MX records;
- timestamp.

Example CSV-style structure:

```
Domain,Record Type,Hostname,Value,IP,Provider
niamonx.io,A,niamonx.io,104.21.12.231,104.21.12.231,Cloudflare
niamonx.io,A,niamonx.io,172.67.153.184,172.67.153.184,Cloudflare
niamonx.io,MX,niamonx.io,10 mx.zoho.eu,185.20.209.166,Zoho
niamonx.io,NS,niamonx.io,abdullah.ns.cloudflare.com,162.159.44.203,Cloudflare
niamonx.io,TXT,niamonx.io,"v=spf1 include:zohomail.eu -all",,
```

CSV export is useful when results need to be shared with technical teams, compliance departments, management, or auditors.

? JSON Export

JSON export provides structured machine-readable output.

JSON data may include:

- searched domain;
- A records;
- subdomains;
- IP addresses;
- CNAME records;
- MX records;
- NS records;
- TXT records;
- resolved IP details;
- timestamp;
- summary counts.

JSON is useful for:

- automation;
- API-style processing;
- custom scripts;
- evidence preservation;
- technical validation;
- integration with asset inventory systems;
- comparing results over time.

? Why This Tool Matters

Subdomains and DNS records are a major part of an organization’s public attack surface. A domain may appear simple from the outside, but DNS records can reveal mail providers, name servers, cloud services, CDN usage, verification tokens, third-party dependencies, and public application endpoints.

Subdomains Check V2 helps users identify:

- public hostnames;
- exposed services;
- CDN-backed infrastructure;
- mail infrastructure;
- DNS providers;
- TXT-based service integrations;
- SPF configuration;
- name server dependencies;
- resolved IP addresses;
- possible third-party exposure;
- unexpected or forgotten records.

This information supports both defensive security and operational infrastructure management.

? Common Use Cases

DNS Inventory

Create a structured overview of DNS records associated with a domain.

Subdomain Discovery

Find discovered subdomains and review how they resolve.

Attack Surface Mapping

Identify public hostnames, IP addresses, DNS providers, and mail systems.

SOC Triage

Enrich alerts involving domains, hostnames, or suspicious DNS records.

Incident Response

Check whether a suspicious domain or subdomain is related to known infrastructure.

Phishing Investigation

Review DNS records, mail configuration, and provider information for suspicious domains.

Brand Protection

Inspect domains and subdomains related to impersonation, fraud, or unauthorized brand usage.

Mail Security Review

Review MX and TXT records, including SPF-related configuration.

DNS Provider Review

Check NS records and identify authoritative DNS providers.

Cloud and CDN Mapping

Identify whether hostnames resolve to CDN or cloud provider infrastructure.

Compliance Documentation

Document DNS records and public exposure for audits, reports, and risk reviews.

Asset Inventory

Add discovered hostnames, IPs, and records to an asset management workflow.

? Recommended Workflow

A practical Subdomains Check V2 workflow should follow these steps.

1. Enter the Domain

Use only the domain name.

Example:

```
niamonx.io
```

Do not include:

```
https://
http://
/path
?query=value
#fragment
*
```

---

2. Run the Search

Start the query and wait for the result.

Example:

```
Search by Domain
```

The tool will search for subdomains and related DNS records.

---

3. Review the Summary

Check the high-level result counts.

Example:

```
A: 1
Subdomains: 1
IPs: 2
MX: 3
NS: 2
TXT: 2
```

This gives a quick overview of how much data was found.

---

4. Review A / Subdomains

Inspect discovered hostnames and IP addresses.

Example:

```
niamonx.io
104.21.12.231
172.67.153.184
```

Follow up with IP WHOIS, ASN lookup, HTTP checks, TLS inspection, or screenshot capture when needed.

---

5. Check CNAME Records

Review whether the domain or subdomains point to external services.

Example:

```
CNAME: No Records
```

If CNAME records exist, validate whether the targets are expected and still active.

---

6. Review MX Records

Check mail routing and provider configuration.

Example:

```
10 mx.zoho.eu
20 mx2.zoho.eu
50 mx3.zoho.eu
```

Confirm that the mail provider is expected and that MX priorities are correct.

---

7. Review NS Records

Check authoritative name servers.

Example:

```
abdullah.ns.cloudflare.com
ashley.ns.cloudflare.com
```

Verify that the DNS provider is expected and properly managed.

---

8. Review TXT Records

Inspect TXT records for SPF, verification tokens, and third-party integrations.

Example:

```
v=spf1 include:zohomail.eu -all
```

Check for outdated, unexpected, or overly permissive records.

---

9. Filter Subdomains

Use substring filtering to locate interesting names.

Examples:

```
api
admin
dev
stage
mail
support
```

Filtering is useful for large domains with many discovered subdomains.

---

10. Export Results

Use CSV or JSON export for reporting and follow-up analysis.

Recommended exports:

```
CSV
JSON
```

---

11. Validate With Additional Tools

Because the tool is experimental, validate important findings with additional sources.

Recommended follow-up checks:

- DNS resolver checks;
- Subdomains Extended;
- IP WHOIS;
- ASN lookup;
- HTTP status checks;
- TLS certificate inspection;
- website screenshot capture;
- passive DNS;
- historical DNS;
- technology fingerprinting;
- authorized vulnerability scanning.

? Security Review Checklist

When reviewing results, pay special attention to the following areas.

Unexpected IP Addresses

Check whether resolved IPs belong to expected providers.

Questions:

- Is this IP expected?
- Does it belong to the correct provider?
- Is it shared CDN infrastructure?
- Is it an origin server?
- Should this hostname be publicly exposed?

Third-Party Dependencies

Review CNAME, NS, MX, and TXT records for third-party services.

Potential dependencies:

- CDN providers;
- DNS providers;
- mail providers;
- SaaS platforms;
- cloud hosting services;
- verification platforms;
- analytics or marketing tools.

Mail Security

Review MX and TXT records.

Important checks:

- Is the mail provider expected?
- Does SPF exist?
- Is SPF too broad?
- Is DMARC present in related records?
- Are DKIM records configured elsewhere?
- Are old verification records still needed?

Name Server Control

Review NS records.

Questions:

- Are the name servers expected?
- Who controls the DNS provider account?
- Is MFA enabled on the DNS provider?
- Are there stale delegations?
- Is DNS change monitoring enabled?

Subdomain Exposure

Review discovered subdomains and search for sensitive patterns.

Examples:

```
admin
dev
test
stage
staging
internal
portal
dashboard
api
backup
old
legacy
```

These names may indicate systems that need closer review.

TXT Record Hygiene

TXT records can expose operational information.

Review for:

- outdated verification tokens;
- unused provider integrations;
- old SPF includes;
- sensitive metadata;
- abandoned service records;
- unclear ownership.

?? Limitations and Important Notes

Subdomains Check V2 should be interpreted carefully.

Important limitations:

- The tool is experimental.
- Results may not be complete.
- Crawler performance affects speed and coverage.
- Some sources may not provide all subdomains.

- DNS records may change frequently.
- Some records may be cached.
- Some subdomains may not resolve.
- Provider information may be approximate.
- A record count does not necessarily mean the number of active applications.
- CDN IPs may be shared by many unrelated customers.
- Missing CNAME records do not prove there are no external dependencies.
- Missing TXT records do not prove that no verification records exist elsewhere.
- Tariff limits may prevent new queries.
- If tariff limits are exceeded, previous results remain visible.

Interface note:

```
The tool is experimental; not all sources provide a complete list of subdomains.
```

For high-confidence analysis, combine results with multiple discovery and DNS validation methods.

? Interpreting Results Correctly

Subdomains Check V2 provides point-in-time DNS and subdomain intelligence.

Important interpretation notes:

- A discovered hostname does not automatically indicate risk.
- A missing record does not always prove absence.
- DNS data can vary by resolver, region, cache, and time.
- CDN and cloud records may hide origin infrastructure.
- Mail records show routing, not necessarily account ownership.
- TXT records may represent active or historical integrations.
- NS records show authoritative DNS providers, but not full security posture.
- IP provider names help with triage but should be validated.
- Experimental discovery may miss subdomains.
- Repeated checks over time may produce different results.

The tool should be used as part of a broader investigation workflow.

? Recommended Reporting Format

When documenting results, use a consistent format.

Example:

```
Domain: niamonx.io
Query time: 17.06.2026, 22:51:28

Summary:
A records: 1
Subdomains: 1
Resolved IPs: 2
MX records: 3
NS records: 2
TXT records: 2

A / Subdomains:
niamonx.io
- 104.21.12.231
- 172.67.153.184

MX:
- 10 mx.zoho.eu → 185.20.209.166
- 20 mx2.zoho.eu → 89.36.170.166
- 50 mx3.zoho.eu → 185.230.212.166

NS:
- abdullah.ns.cloudflare.com → 162.159.44.203
- ashley.ns.cloudflare.com → 172.64.32.71

TXT:
- "google-site-verification=MQNH6Yoh9hKD1hgzeQtEb9VN5_ikdspHYQxlxGS6Y-4"
- "v=spf1 include:zohomail.eu -all"
```

For security reports, add analyst notes:

```
Observation:
The domain resolves through Cloudflare infrastructure and uses Zoho mail exchangers. TXT
records include Google site verification and SPF authorization for Zoho Mail.

Recommended next step:
Validate DMARC and DKIM configuration, confirm that the listed providers are expected, review
DNS provider account security, and enrich resolved IPs with WHOIS / ASN data.
```

?? Security, Privacy & Responsible Use

Subdomains Check V2 is intended for lawful DNS analysis, OSINT research, security review, compliance, infrastructure mapping, and defensive cybersecurity workflows.

Acceptable use cases include:

- auditing domains you own or are authorized to assess;
- reviewing public DNS configuration;
- discovering subdomains;
- mapping public infrastructure;
- supporting incident response;
- enriching SOC investigations;
- reviewing mail and DNS security;
- checking provider dependencies;
- documenting public exposure;
- preparing asset inventories;
- supporting authorized bug bounty reconnaissance.

Users should follow responsible use principles:

- Do not use the tool for unauthorized targeting or harassment.
- Do not attempt to exploit discovered systems.
- Do not assume that DNS discovery equals vulnerability.
- Validate important findings with additional evidence.
- Follow authorization boundaries.
- Store exported results securely.
- Avoid exposing sensitive investigation results publicly.
- Report issues through proper disclosure channels.

Subdomain and DNS discovery is a legitimate defensive and OSINT technique, but it should be used responsibly and legally.

?? Technical Highlights

- Experimental subdomain and DNS discovery tool
- Available at `dash.niamonx.io/subdomains_v2`
- Searches by domain name
- Accepts domains without protocol or path
- Searches for subdomains
- Collects A records
- Collects CNAME records
- Collects MX records

- Collects NS records
- Collects TXT records
- Resolves IP addresses
- Shows basic provider/network hints
- Displays result summary counts
- Supports filtering by subdomain substring
- Supports copying results
- Supports CSV export
- Supports JSON export
- Maintains local request history
- Stores up to 200 local history entries
- Preserves previous results if tariff limit is exceeded
- Suitable for OSINT, SOC, incident response, attack surface management, DNS review, mail security analysis, and infrastructure mapping

---

? Usage Hints

- Enter only the domain name, such as `example.com`.
- Do not include `http://` or `https://`.
- Do not include paths, query strings, fragments, or wildcards.
- Review the summary counts first.
- Check A records and resolved IPs.
- Review provider hints, but validate them with IP WHOIS and ASN tools.
- Use subdomain filtering to find interesting names.
- Check CNAME records for third-party dependencies.
- Review MX records to understand mail routing.
- Review NS records to confirm DNS provider configuration.
- Review TXT records for SPF and verification tokens.
- Export CSV for reporting and spreadsheet review.
- Export JSON for automation and technical validation.
- Repeat checks over time because DNS data changes.
- Treat results as experimental and validate important findings.
- Keep local history in mind when using shared devices.
- Use the tool only within authorized and lawful workflows.

? Contact Information

For technical, legal, abuse, privacy, or support-related inquiries, users can contact the NiamonX team directly:

support@niamonx.io — Technical Support

other@niamonx.io — General Inquiries

takedown@niamonx.io — Privacy or Data Removal Requests

legal@niamonx.io — Legal and Compliance Matters

Alternative contact channel:

Helpdesk: https://support.niamonx.io/

Summary

NiamonX Subdomains Check V2 is an experimental subdomain and DNS records discovery tool for domain-based reconnaissance. It searches for subdomains and related DNS records, including A, CNAME, MX, NS, and TXT records, resolves IP addresses, shows basic provider information, supports substring filtering, provides CSV and JSON export, and stores local request history with brief summaries.

The tool is designed for OSINT research, DNS inventory, SOC workflows, incident response, attack surface mapping, mail security review, provider dependency analysis, brand protection, compliance documentation, and authorized security assessments. Because it is experimental, results should be treated as point-in-time discovery intelligence and validated with additional DNS, WHOIS, ASN, HTTP, TLS, screenshot, passive DNS, and asset inventory sources before drawing final conclusions.

Revision #1
Created 17 June 2026 20:52:21 by NiamonX Team
Updated 17 June 2026 20:55:47 by NiamonX Team