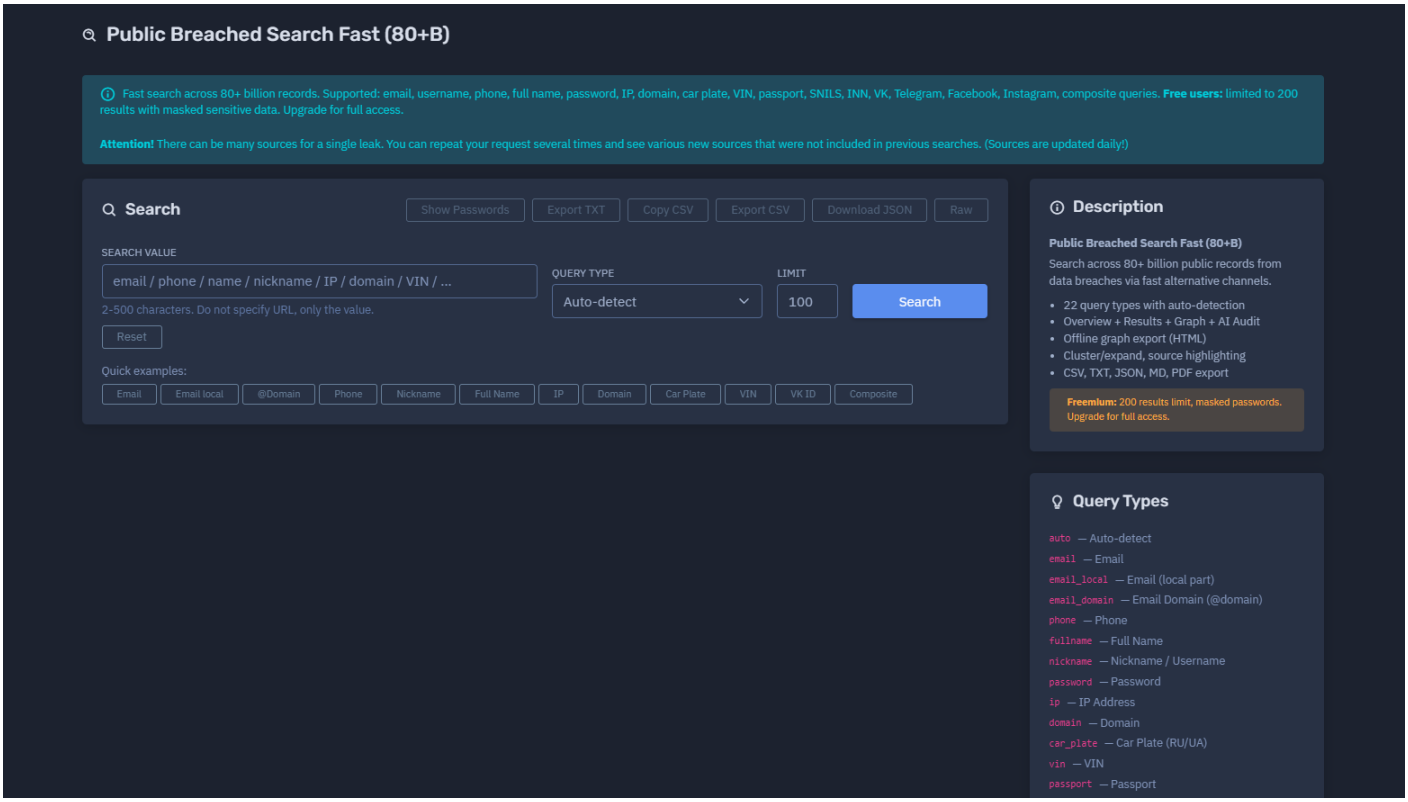
Public Breached Search Fast (80+B) | Fast Public Breach Intelligence Search



The platform available at dash.niamonx.io/breaches_search_fast

Overview of the Service

Public Breached Search Fast (80+B) is a high-speed breach intelligence tool available within the NiamonX platform. It enables users to search across **80+ billion public records** collected from publicly available breach datasets and alternative intelligence channels.

The system is designed for individuals, analysts, security researchers, compliance teams, and cybersecurity departments that need to quickly verify whether specific identifiers, accounts, or technical indicators appear in compromised public datasets.

Unlike the encrypted PBS v2 engine, **Public Breached Search Fast** focuses on speed, broad query coverage, source diversity, graph analysis, and flexible exports. It supports a wide range of

identifiers, including emails, usernames, phone numbers, names, domains, IP addresses, vehicle identifiers, social media IDs, and composite queries.

The service is intended strictly for lawful security analysis, personal data verification, incident response, and defensive investigations.

? How the Search Works

When a user enters a search value, the system performs a fast lookup across a large alternative breach index containing more than **80 billion public records**.

The user can either allow the system to automatically detect the query type or manually select a specific type, such as email, phone number, domain, VIN, passport, Telegram, VK, or composite query.

The platform then returns available matches, grouped and structured by source, data type, and related metadata.

Important behavior:

- The same leak may have multiple source references.
- A single query can return different source combinations across repeated searches.
- Sources are updated daily.
- Repeating a request may reveal additional sources that were not included in previous results.
- Free users are limited to **200 results**.
- Sensitive fields, including passwords, are masked for free users.
- Full access requires an upgraded account.

This approach allows the system to prioritize both speed and broad source discovery while keeping sensitive information controlled.

? What Can Be Searched

Public Breached Search Fast supports **22 query types** with automatic detection.

Supported query types:

- `auto` — Auto-detect
- `email` — Email address
- `email_local` — Email local part

- `email_domain` — Email domain
- `phone` — Phone number
- `fullname` — Full name
- `nickname` — Nickname or username
- `password` — Password
- `ip` — IP address
- `domain` — Domain
- `car_plate` — Car plate
- `vin` — Vehicle Identification Number
- `passport` — Passport
- `snils` — SNILS
- `inn` — INN
- `vk` — VKontakte identifier
- `telegram` — Telegram identifier
- `facebook` — Facebook identifier
- `instagram` — Instagram identifier
- `composite` — Multi-field composite query
- `fullname_dob` — Full name with date of birth
- `numeric_id` — Numeric identifier

The search input supports values from **2 to 500 characters**.

Users should enter only the value itself, not a full URL. For example, enter a domain name instead of a full website address.

?? Search Interface

The search interface includes the following main fields:

Search Value

The identifier or value to search for.

Examples of supported values:

- Email address
- Phone number
- Full name
- Nickname
- IP address
- Domain
- VIN
- Car plate

- Passport number
- Social media identifier
- Composite query

Query Type

The user may select a specific query type or use **Auto-detect**.

Auto-detection helps identify the most likely input type and route the search through the correct lookup logic.

Limit

The user can specify the maximum number of results to retrieve.

Free users are limited to **200 visible results** with sensitive information masked. Paid users may access higher result limits and full visibility depending on their subscription level and permissions.

? Key Features

Fast Search Across 80+ Billion Records

The system is optimized for quick lookups across a very large public breach index.

22 Query Types

Public Breached Search Fast supports a wide range of identifiers, including personal, technical, vehicle-related, and social media identifiers.

Auto-Detection

The platform can automatically detect the type of query entered by the user.

Overview Section

Search results include a structured overview of discovered matches, source distribution, and available metadata.

Results View

Matched records are displayed in a readable format with source highlighting and structured fields.

Graph View

The tool can visualize relationships between identifiers, sources, and connected records using graph-based analysis.

AI Audit

The AI Audit feature helps summarize and interpret the search results from a security and risk perspective.

Offline Graph Export

Users can export graph analysis as an offline HTML file for local review, reporting, or internal investigations.

Cluster and Expand

The system can cluster related records and expand connected entities to help analysts understand relationships between data points.

Source Highlighting

Sources are visually highlighted to make it easier to identify where specific records were found.

Flexible Export

Results can be exported in multiple formats:

- CSV
- TXT
- JSON
- Markdown
- PDF

Export functionality is intended for lawful internal use, incident response, compliance checks, and security reporting.

? Results, Graph, and AI Audit

Public Breached Search Fast provides multiple result analysis layers.

Overview

The overview section summarizes key information about the query, such as:

- Number of discovered records
- Related data categories
- Available source groups
- Detected query type
- Possible risk indicators

Results

The results section displays matching records from available public breach sources.

Depending on the user’s access level, some sensitive fields may be masked.

Graph

The graph view helps users analyze relationships between identifiers and sources.

This is useful for:

- Account compromise investigations
- Identity exposure analysis
- Infrastructure correlation
- Reused identifier detection
- Source relationship mapping

AI Audit

The AI Audit feature provides an automated interpretation of the findings.

It may help identify:

- Potential account compromise
- Reused credentials
- Risky exposure patterns
- Multiple-source appearances

- High-risk identifiers
- Recommended defensive actions

AI Audit is intended to support analyst decision-making and should not be treated as a final legal or forensic conclusion.

? Export Options

Public Breached Search Fast supports several export formats:

- **CSV** — for spreadsheets and structured analysis
- **TXT** — for simple plain-text review
- **JSON** — for technical workflows and integrations
- **MD** — for documentation and reporting
- **PDF** — for formal reports and sharing with authorized parties
- **HTML graph export** — for offline graph visualization

Sensitive fields may be masked or excluded depending on account permissions, subscription level, and platform security rules.

Users must not redistribute personal or sensitive data obtained from the system.

?? Important Notes About Sources

A single leak may have many different source references.

Because sources are updated daily, repeated searches may show different or additional sources that were not included in earlier results.

This behavior is normal and reflects the dynamic nature of the breach intelligence index.

Users should treat results as intelligence indicators and verify important findings through proper security, legal, or compliance workflows before taking action.

?? Security, Privacy & Ethics

Public Breached Search Fast is built for defensive cybersecurity, personal security verification, and lawful intelligence analysis.

Users must follow strict ethical rules:

- Search only your own data or data you are legally authorized to investigate.
- Do not use the system to stalk, harass, deanonymize, or target individuals.
- Do not publish personal or sensitive data retrieved from the platform.
- Do not redistribute passwords, identity documents, phone numbers, private addresses, or other confidential information.
- Do not use breach data for account takeover, credential stuffing, fraud, spam, phishing, or social engineering.
- Do not attempt to bypass masking, limits, access controls, or platform protections.
- Use discovered exposure only for remediation, reporting, and defensive security actions.

Recommended security actions after discovering exposed data:

- Change affected passwords immediately.
- Enable multi-factor authentication.
- Avoid credential reuse.
- Review account login history.
- Monitor suspicious activity.
- Notify affected users or internal teams when legally appropriate.
- Request takedown or removal where applicable.

Abuse of the system may result in account restriction, suspension, or termination.

?? Technical Highlights

- Search across **80+ billion public records**
- Fast alternative breach intelligence channels
- 22 supported query types
- Automatic query type detection
- Supports email, username, phone, name, password, IP, domain, VIN, car plate, passport, SNILS, INN, social media identifiers, and composite queries
- Overview, Results, Graph, and AI Audit modules
- Offline graph export in HTML format
- Cluster and expand functionality
- Source highlighting
- CSV, TXT, JSON, Markdown, PDF export
- Freemium access model
- Free users limited to 200 results
- Sensitive data masking for free users
- Daily source updates

? Query Types Reference

Query Type	Description
`auto`	Auto-detect
`email`	Email
`email_local`	Email local part
`email_domain`	Email domain
`phone`	Phone
`fullname`	Full name
`nickname`	Nickname / Username
`password`	Password
`ip`	IP address
`domain`	Domain
`car_plate`	Car plate
`vin`	VIN
`passport`	Passport
`snils`	SNILS
`inn`	INN
`vk`	VKontakte
`telegram`	Telegram
`facebook`	Facebook
`instagram`	Instagram
`composite`	Composite multi-field query
`fullname_dob`	Full name + date of birth
`numeric_id`	Numeric ID

? Contact Information

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

support@niamonx.io — Technical Support

other@niamonx.io — General Inquiries

takedown@niamonx.io — Data Removal / Privacy Takedown Requests

legal@niamonx.io — Legal and Compliance Matters

Alternative contact channel:

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

Summary

NiamonX Public Breached Search Fast (80+B) is a high-speed public breach intelligence tool designed for fast, broad, and structured searches across more than **80 billion public records**.

It supports 22 query types, automatic detection, source highlighting, graph analysis, AI-assisted audit, offline graph export, and multiple export formats.

The tool is intended for lawful cybersecurity investigations, personal exposure checks, compliance workflows, and defensive threat intelligence. It combines speed, large-scale coverage, and flexible analysis features while enforcing masking, access control, and ethical usage requirements.

Revision #2
Created 17 June 2026 16:58:28 by NiamonX Team
Updated 17 June 2026 17:00:50 by NiamonX Team