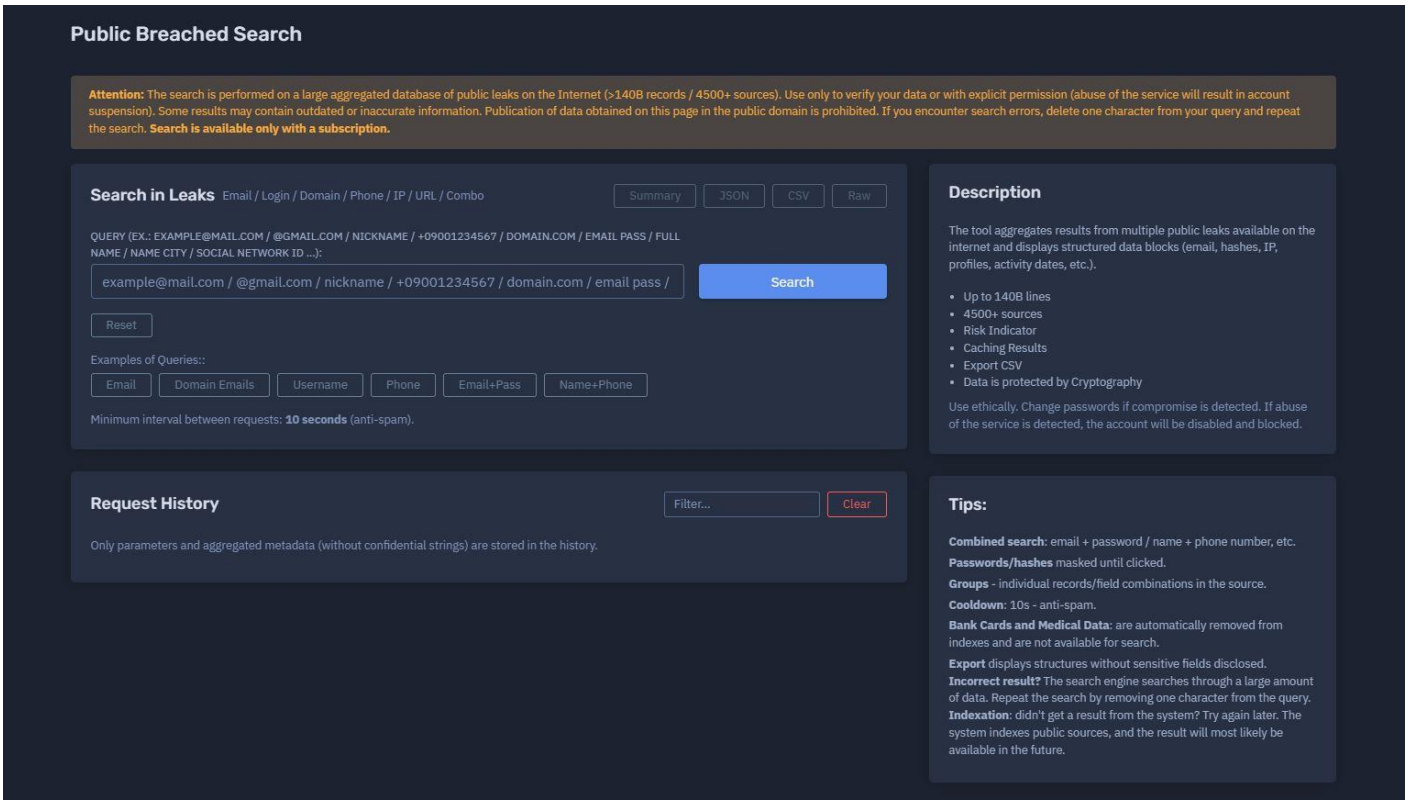
Data Breach Search

- Public Breached Search | Public Breaches (140+ Billion Records)
- ULP (Infostealer Logs) | Public Breached ULP Search
- PBS v2 (Beta Search) | Public Breached Search V2

Public Breached Search | Public Breaches (140+ Billion Records)



Overview of the Service

The platform available at dash.niamonx.io/breaches_search is a professional-grade **Public Breached Data Search System** designed for verifying whether specific personal identifiers have appeared in any known public data leaks across the Internet.
It operates on an **aggregated dataset exceeding 140 billion records** collected from **over 4,500 public breach sources**, making it one of the most extensive publicly searchable breach databases in existence.

? How the Search Works

When a user enters a query — such as an **email address, username, phone number, IP, or domain** — the system performs a real-time lookup across its encrypted, indexed data clusters. The query is normalized, tokenized, and securely matched against hashed or pseudonymized datasets to locate potential breach entries.

The search engine uses **multi-vector indexing** optimized for text, numeric, and composite keys (e.g., *email* + *password*, *name* + *city*), allowing flexible combined searches.

To maintain integrity and performance:

- Each user request is subject to a **10-second cooldown** (anti-spam policy).
- Partial queries can improve recall; deleting one character may trigger a broader match.
- Cached results are used for frequent queries to improve response time.

? What Can Be Searched

You can look up:

- **Emails and logins**
- **Phone numbers** (international format)
- **Domains or URLs**
- **IP addresses**
- **Full names or social network identifiers**
- **“Combo” lines** (e.g., *email + password* pairs from public leaks)

The system structures results into logical “groups” that may include:

- Email or login identifiers
- Hashed or masked passwords
- IP and domain references
- Profiles and related metadata
- First/last seen activity dates

Sensitive fields like passwords remain **masked** until explicitly revealed by the user.

?? Security & Ethics

All stored data and query logs are **encrypted using modern cryptographic algorithms**.
Only **aggregated metadata** — not full confidential strings — is retained in request history for transparency and analytics.

Additional safeguards:

- **Bank card and medical information** are automatically excluded from indexing.
- **Publication of retrieved data** is strictly forbidden.
- Detected abuse leads to **account suspension and IP blocking**.

The service is intended for **ethical use only** — such as checking whether your credentials or company assets appear in public leaks and taking appropriate security measures (e.g., password changes, MFA setup).

? Extra Features

- **Risk indicator:** assesses the exposure level of each result.
- **Result caching:** speeds up repeated lookups.
- **CSV export:** allows structured export without revealing sensitive fields.
- **Ongoing index updates:** new sources are continuously crawled and normalized.

In summary, **NiamonX Breach Search** acts as a secure, encrypted intelligence platform that enables professionals and individuals to verify their exposure in public breaches responsibly. It prioritizes **data protection, cryptographic integrity, and ethical transparency**, providing actionable insights while maintaining user and data privacy.

? Contact Information

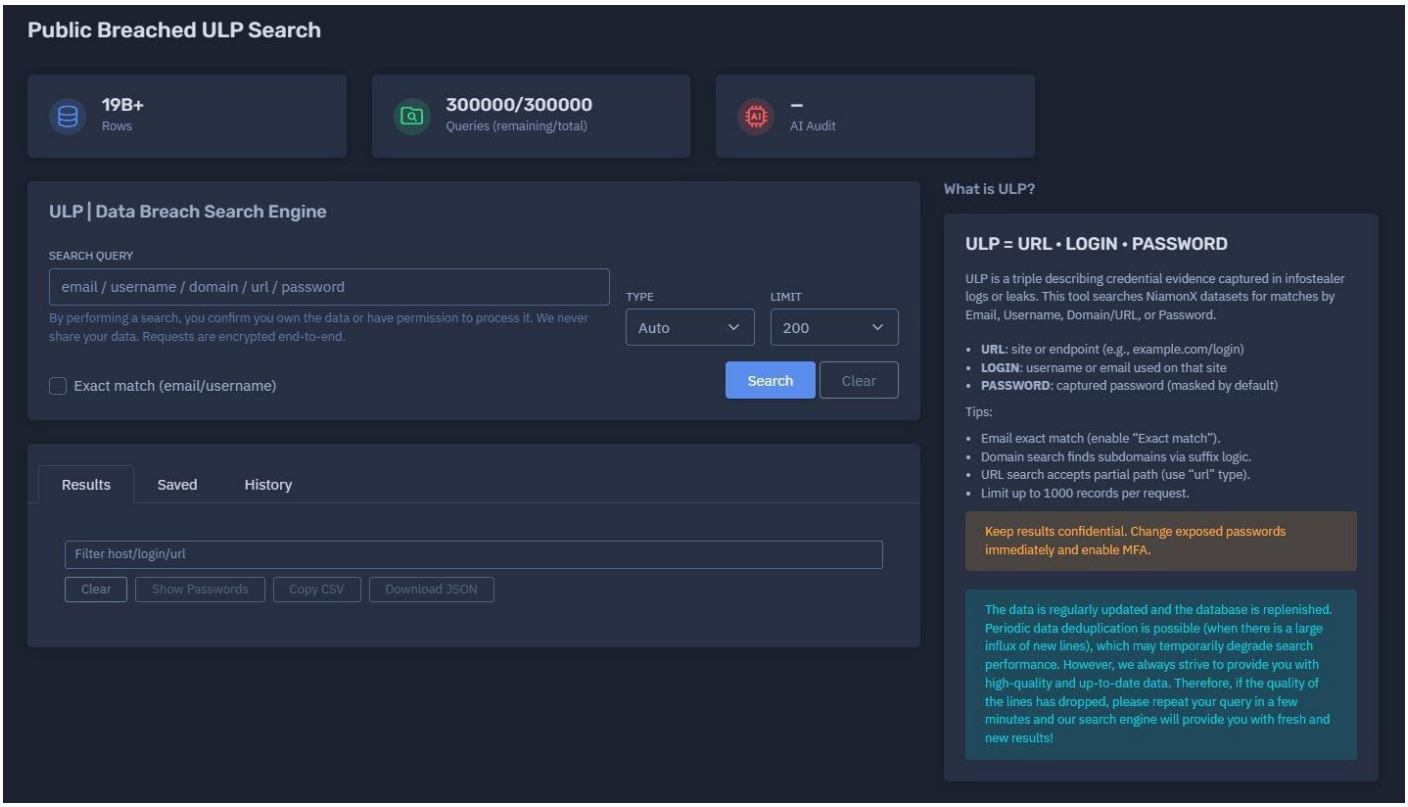
For any inquiries, users can contact the project team directly:

- **support @ niamonx.io** — Technical Support
- **other @ niamonx.io** — General Inquiries
- **takedown @ niamonx.io** — Requests for Data Removal / Privacy Takedowns
- **legal @ niamonx.io** — Legal Matters

An alternative contact channel is the official **Helpdesk**:

□□ https://support.niamonx.io/

ULP (Infostealer Logs) | Public Breached ULP Search



Overview of the Service

The platform available at **dash.niamonx.io/ulp_search** — known as **ULP Search** — is a specialized **Data Breach Search Engine** developed by **NiamonX** for identifying credential exposures in **public and infostealer leak datasets**.
It provides professionals and security researchers with a structured, secure, and ethical way to verify whether specific login credentials have been compromised online.

The ULP database currently indexes **over 19 billion credential records**, continuously updated and refined through automated pipelines, ensuring freshness, accuracy, and de-duplication.

? What is ULP?

ULP stands for **URL · LOGIN · PASSWORD**, representing a *credential triple* extracted from public or infostealer data sources.

Each record typically contains:

- **URL** — the website, endpoint, or domain where credentials were used (e.g., `example.com/login`)
- **LOGIN** — the associated username or email address
- **PASSWORD** — the captured or leaked password (masked by default for security)

This triplet allows correlation between breached accounts, reused passwords, and compromised domains, forming the foundation of forensic credential analysis within NiamonX's breach intelligence system.

? How the Search Works

Users can query the database using any of the following parameters:

- **Email address or username**
- **Domain or URL**
- **Password (masked matching supported)**

The system automatically detects the query type (`Auto` mode) or allows manual selection for more specific searches.
Searches are conducted in **real-time** against encrypted datasets, and results are filtered and ranked by confidence and relevance.

Key operational details:

- **Exact match** can be enabled for precise email or username lookups.
- **Domain-based searches** support suffix logic to detect subdomains (e.g., searching `example.com` will also include `mail.example.com`).
- **URL searches** accept partial paths, ideal for endpoint-level tracing.
- **Result limits:** up to 1,000 records per request.
- **Anti-abuse control:** all queries are encrypted and rate-limited.

If search performance temporarily decreases, it may indicate **active deduplication** or **dataset reindexing** — repeating the search after a few minutes ensures access to the freshest possible data.

? Key Features

- **AI Audit System:** enhances search precision and filters false positives through pattern-based validation and contextual AI analysis.
- **Result History & Filtering:** users can save searches, view historical queries, and filter by host, login, or URL.
- **Masked Passwords:** sensitive data remains hidden by default to prevent misuse.
- **Secure Export Options:** structured result exports with sensitive fields excluded.

- **Regular Updates:** continuous ingestion of verified breach data ensures up-to-date intelligence.

?? Security, Privacy & Ethics

Every search request is **fully encrypted end-to-end**, ensuring that user queries and results remain private.
The system never shares, resells, or exposes query data — even internally.

Ethical principles:

- Only perform searches for **data you own** or have **explicit authorization** to analyze.
- Keep results confidential and never redistribute them.
- Immediately **change any exposed passwords** and **enable multi-factor authentication (MFA)** if compromise is detected.
- Publication of retrieved data in open sources is strictly prohibited.

? Technical Highlights

- **19B+ credential records**
- **Real-time encrypted search**
- **Periodic deduplication & refresh cycles**
- **Adaptive caching for faster repeated queries**
- **Multi-type query engine (Email / Domain / URL / Password)**

? Contact Information

For support, inquiries, or privacy-related requests, the NiamonX team can be reached directly via:

- **support @ niamonx.io** — Technical Support
- **other @ niamonx.io** — General Inquiries
- **takedown @ niamonx.io** — Personal Data Removal Requests
- **legal @ niamonx.io** — Legal or Compliance Matters

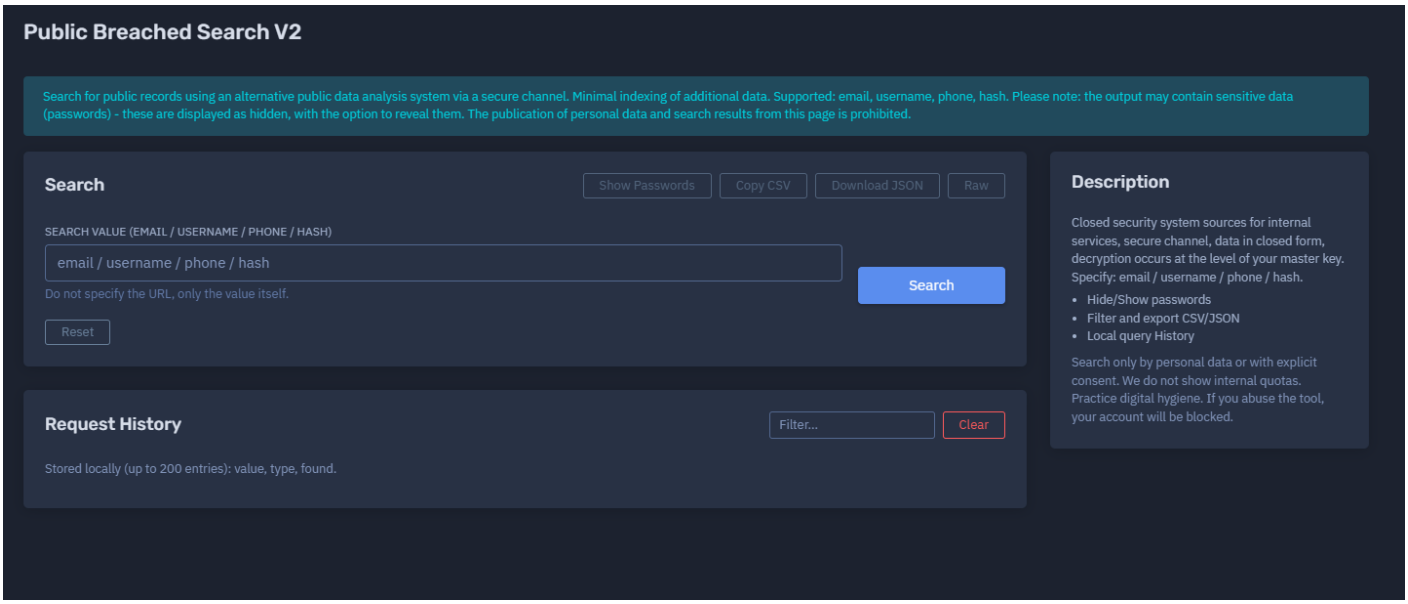
Alternative contact channel:

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

In summary, **NiamonX ULP Search** is a **cryptographically secure and ethically governed breach intelligence system** designed for professional credential analysis.

It provides deep visibility into compromised login data from billions of records — while maintaining the highest standards of **security, privacy, and responsible use**.

PBS v2 (Beta Search) | Public Breached Search V2



Overview of the Service

The platform available at dash.niamonx.io/breaches_s_v2 — known as **Public Breached Search V2** — is an advanced, security-focused version of the NiamonX breach intelligence engine. It enables users to safely and privately search for **publicly available leaked records** (emails, usernames, phone numbers, or hashes) through a **fully encrypted channel**, using an enhanced privacy-preserving architecture.

This system is designed for individuals, analysts, and cybersecurity teams who need to verify whether specific identifiers have been compromised — without exposing their search queries or retrieved data.

? How the Search Works

When a user submits a query — such as an **email address, username, phone number, or hash** — the system performs a real-time lookup across an **alternative, minimized index** of public breach data.
The search is executed through a **closed security network** using **end-to-end encryption** and a **master key–based decryption layer**. This ensures that:

- All transmitted data remains encrypted at every step.
- Decryption occurs **only on the client side**, not on NiamonX servers.

- The system never stores sensitive results or full identifiers in plain form.

This approach provides **maximum privacy**, ensuring that no third party — including NiamonX infrastructure — can access raw search data or results.

? What Can Be Searched

Supported input types:

- **Email address**
- **Username / Login**
- **Phone number** (international format)
- **Hash** (MD5 / SHA1 / SHA256 and similar)

Unlike the standard Breached Search engine, V2 does **not** support URLs, domains, or combined queries. It focuses exclusively on **personal identifiers and cryptographic hashes** to maintain precision and data hygiene.

Passwords found in results are **hidden (masked)** by default. Users may reveal them manually if needed for verification, but they must not redistribute or publicly display that information.

? Key Features

- **Encrypted Communication Channel:** every search request and response is transmitted securely.
- **Client-side Decryption:** sensitive content is decrypted locally using the user’s master key.
- **Minimal Indexing:** only essential metadata is stored to ensure fast lookups while reducing exposure.
- **Local Query History:** recent searches (up to 200 entries) are stored locally in the browser, not on the server.
- **Flexible Export:** results can be exported in **CSV** or **JSON** format, excluding confidential fields.
- **Password Visibility Control:** toggle to hide or show masked password fields.
- **Filtering System:** refine results by data type or source metadata.

?? Security, Privacy & Ethics

The service is built with **security-first architecture** and strict privacy guarantees:

- All communication is conducted through a **secure, encrypted channel**.

- Data is stored and processed in a **closed system** environment.
- **No internal quotas or usage metrics** are publicly displayed to prevent misuse.
- Searches must only be performed on **your own data** or with **explicit permission**.
- Abuse or attempts to deanonymize datasets will result in **account termination**.
- **Publication of personal or sensitive data retrieved from the system is strictly forbidden.**

Users are strongly encouraged to **practice digital hygiene** — for example, by changing passwords, enabling MFA, and avoiding credential reuse.

?? Technical Highlights

- **Alternative breach dataset with minimal indexing**
- **Closed internal security infrastructure**
- **End-to-end encryption with client-side decryption**
- **Local storage of query history (no server retention)**
- **Supports: email / username / phone / hash**
- **Output masking for passwords and sensitive fields**
- **CSV/JSON export with filtering tools**

? Contact Information

For any technical, legal, or privacy-related inquiries, users can reach the NiamonX team directly via:

- **support @ niamonx.io** — Technical Support
- **other @ niamonx.io** — General Inquiries
- **takedown @ niamonx.io** — Requests for Data Removal / Privacy Takedowns
- **legal @ niamonx.io** — Legal or Compliance Matters

Alternative contact channel:

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

In summary, **NiamonX Public Breached Search V2** is a **secure, privacy-preserving intelligence system** that enables safe and encrypted lookup of breach data.
It prioritizes **user confidentiality, cryptographic protection, and ethical operation**, ensuring that every search remains private, traceable only to the authorized user, and never exposed beyond their secure session.