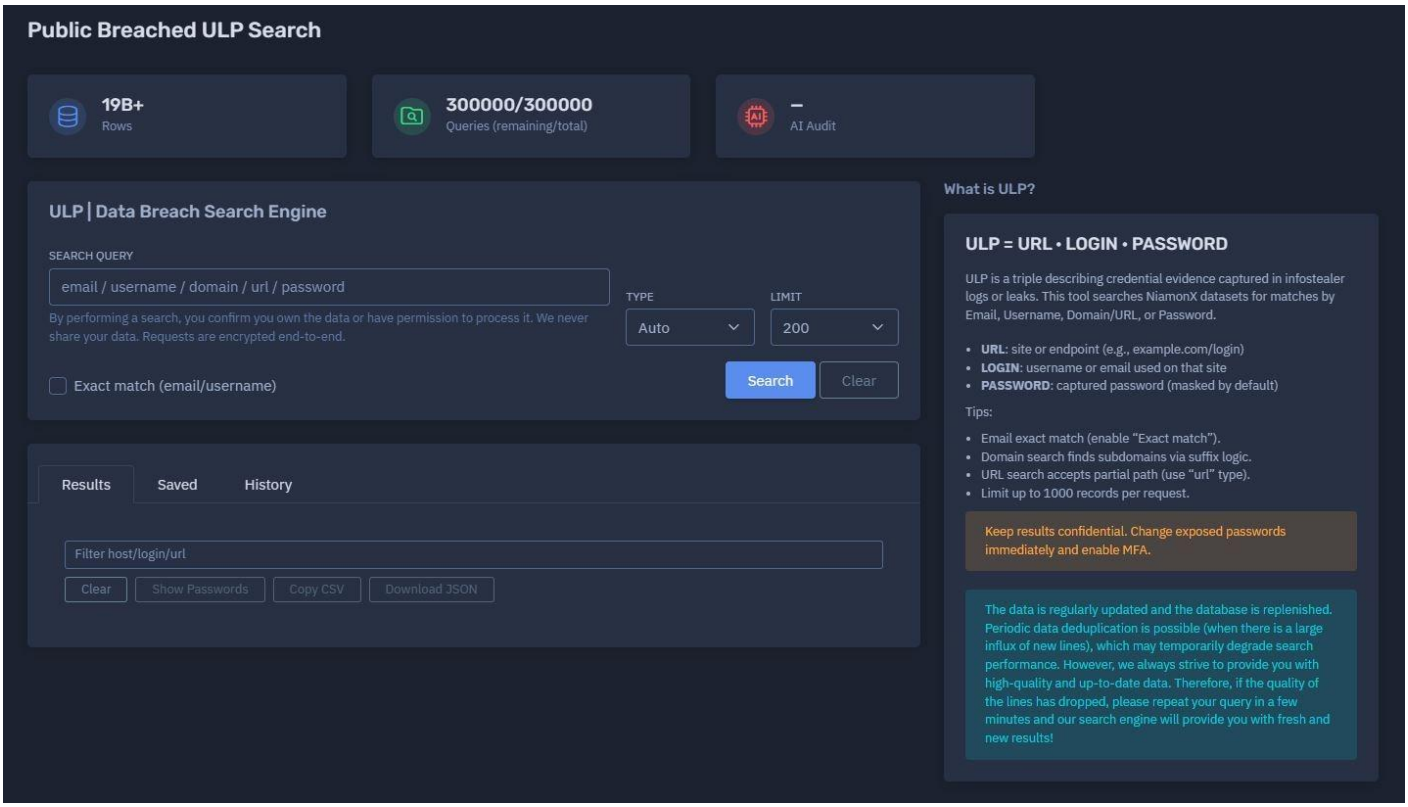
ULP (Infostealer Logs) | Public Breached ULP Search



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**.

Revision #1
Created 9 November 2025 05:35:16 by NiamonX Team
Updated 9 November 2025 05:38:35 by NiamonX Team