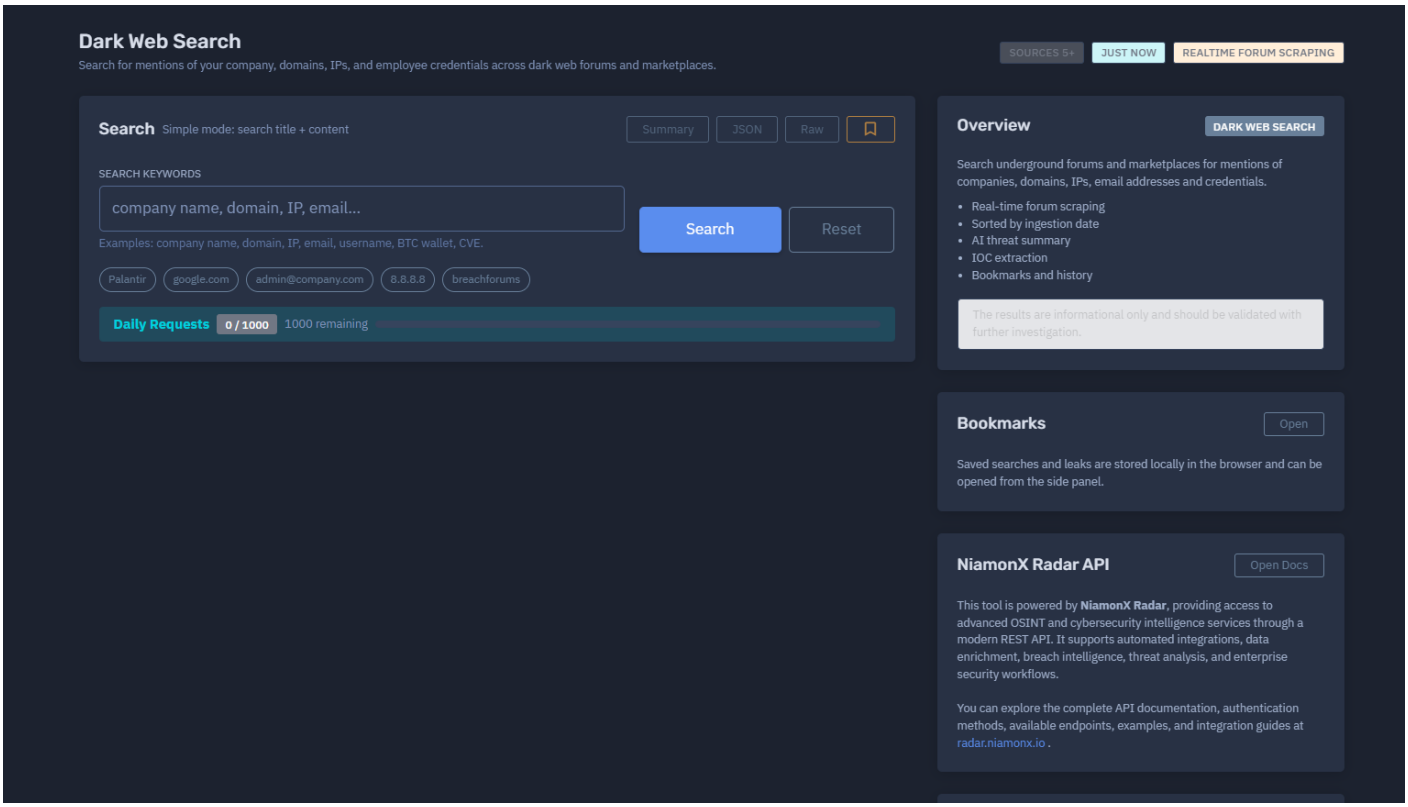
Dark Web Search | Underground Threat Intelligence Monitoring



The platform available at dash.niamonx.io/dark_web_search

Overview of the Service

Dark Web Search is a cybersecurity intelligence tool within the NiamonX platform designed to search for mentions of companies, domains, IP addresses, employee credentials, usernames, email addresses, cryptocurrency wallets, CVEs, and other security-relevant indicators across underground forums, dark web communities, and marketplace-related sources.

The tool helps organizations detect early signs of exposure, leaked credentials, threat actor discussions, infrastructure mentions, and possible compromise indicators.

It is designed for security teams, SOC analysts, threat intelligence researchers, compliance departments, and company owners who need to monitor whether their organization, assets, or employees are being discussed or exposed in underground environments.

The results are informational and should always be validated through further investigation before taking operational, legal, or security actions.

? How the Search Works

When a user submits a search query, such as a company name, domain, IP address, email address, username, BTC wallet, or CVE identifier, the system searches across indexed dark web and underground forum data.

In **Simple Mode**, the tool searches both:

- Post titles
- Post content

Results are sorted by ingestion date, meaning the newest collected items appear first.

The platform uses real-time forum scraping and NiamonX Radar intelligence capabilities to detect fresh mentions and newly ingested underground content.

Supported search examples include:

- Company name
- Domain
- IP address
- Email address
- Username
- Employee credential
- BTC wallet
- CVE identifier
- Product or project name
- Internal keyword
- Brand name

The system is intended to help users identify possible risks, not to provide final conclusions without manual validation.

? What Can Be Searched

Dark Web Search supports keyword-based searches related to organizational and technical exposure.

Common searchable values include:

- Company names
- Brand names
- Domains
- Subdomains
- IP addresses
- Corporate email addresses
- Employee usernames
- Credentials
- Cryptocurrency wallets
- CVE identifiers
- Internal project names
- Product names
- Infrastructure keywords
- Threat actor references
- Leak titles
- Forum post keywords

The tool is flexible and can be used for both broad monitoring and focused investigation.

For example:

- Searching a company name may reveal forum discussions or leak mentions.
- Searching a domain may reveal exposed credentials or infrastructure references.
- Searching an email may reveal account exposure or credential leaks.
- Searching a CVE may reveal underground discussions about exploitation.
- Searching a BTC wallet may reveal links to ransomware, scams, or threat actor activity.

? Key Features

Real-Time Forum Scraping

The tool continuously collects and processes data from monitored underground sources, allowing users to discover recently ingested mentions.

Search Across Dark Web Forums and Marketplaces

Dark Web Search helps identify mentions across underground communities, forums, marketplaces, and related intelligence sources.

5+ Source Groups

The platform currently provides access to more than five monitored source groups, with collected data updated through the NiamonX Radar intelligence infrastructure.

Simple Search Mode

Simple Mode searches across both post titles and post content, making it easier to find relevant mentions without advanced query syntax.

Ingestion Date Sorting

Results are sorted by ingestion date, allowing analysts to focus on the newest discovered content first.

AI Threat Summary

The platform can generate an AI-assisted threat summary to help users quickly understand the possible risk, context, and relevance of discovered mentions.

IOC Extraction

The system can extract Indicators of Compromise from discovered content.

Possible IOCs may include:

- IP addresses
- Domains
- URLs
- Email addresses
- Hashes
- Cryptocurrency wallets
- CVEs
- Usernames
- Infrastructure indicators

Risk Score

The risk score is calculated based on signals such as:

- Number of leak mentions
- Verified hits

- Credential presence
- IOC density
- Relevance of detected content
- Possible relationship to the searched entity

The score is intended as an analyst support metric and should not be treated as a final determination.

Bookmarks

Users can save searches and individual leak records as bookmarks.

Bookmarks are stored locally in the browser and can be opened from the side panel.

Search History

The tool keeps local browser-based history for easier access to previous searches.

Daily Request Limits

Daily request limits depend on the user’s current plan.

For example, a plan may include:

- 1000 daily requests
- Remaining request counter
- Usage tracking by plan limit

? Results and Threat Context

Dark Web Search results are designed to help analysts quickly understand what was found and why it may matter.

A result may include:

- Source name or source group
- Title
- Content snippet
- Ingestion date
- Detected indicators
- Risk score
- Related credentials

- Extracted IOCs
- AI-generated summary
- Bookmark option

The system helps users identify whether the discovered mention is likely related to:

- Credential exposure
- Company targeting
- Data sale or leak discussion
- Infrastructure reconnaissance
- Vulnerability exploitation
- Threat actor activity
- Brand abuse
- Fraud or phishing activity
- Ransomware-related intelligence

All findings should be reviewed manually and correlated with internal logs, SIEM data, EDR alerts, access history, and other trusted security sources.

? AI Threat Summary

The AI Threat Summary feature helps convert raw underground data into readable intelligence.

It may assist with:

- Explaining the context of the mention
- Highlighting possible risks
- Identifying exposed entities
- Summarizing credential-related findings
- Detecting relevant IOCs
- Suggesting defensive investigation steps
- Prioritizing high-risk results

AI-generated summaries are intended to support human analysts and should not replace professional review.

? IOC Extraction

Dark Web Search can automatically extract security indicators from discovered content.

Extracted indicators may include:

IOC Type	Description
IP address	Possible infrastructure, victim system, or attacker-controlled host
Domain	Mentioned corporate, phishing, malware, or infrastructure domain
Email	Exposed account, contact, or credential-related identifier
Hash	Malware, file, or credential-related hash
CVE	Vulnerability identifier discussed in underground content
Wallet	Cryptocurrency wallet connected to scams, ransomware, or illicit activity
Username	Forum handle, employee account, or leaked login
URL	Mentioned website, panel, leak page, or infrastructure reference

IOC extraction helps analysts move from raw search results to actionable threat intelligence.

? Bookmarks and Local Storage

The bookmark system allows users to save important findings for later review.

Bookmarks may include:

- Search queries
- Individual leak records
- Relevant dark web mentions
- Investigation leads
- High-risk findings

Saved searches and leaks are stored locally in the browser and can be opened from the side panel.

This allows analysts to keep track of investigations without relying on external notes or repeated manual searches.

? Daily Requests and Plan Limits

Dark Web Search uses daily request limits based on the user’s subscription plan.

The interface may show:

- Daily requests used
- Total daily request allowance
- Remaining requests

Example:

```
Daily Requests
0 / 1000
1000 remaining
```

These limits help control usage, protect infrastructure stability, and prevent abuse of the intelligence system.

? Risk Score Logic

The risk score is calculated using several intelligence signals.

Main scoring factors include:

- Number of leak mentions
- Number of verified hits
- Presence of credentials
- Density of extracted IOCs
- Recency of ingested content
- Relevance to the searched company, domain, or identifier
- Possible exposure severity
- Underground source context

A higher risk score may indicate stronger relevance, higher exposure, or more urgent investigation priority.

However, risk scores should be interpreted as guidance, not as absolute proof of compromise.

?? Security, Privacy & Ethics

Dark Web Search is intended for defensive cybersecurity, threat intelligence, brand monitoring, and lawful corporate security investigations.

Users must follow strict ethical and legal rules:

- Search only for assets, companies, domains, accounts, or indicators that you are authorized to investigate.
- Do not use the tool to stalk, harass, deanonymize, or target individuals.
- Do not attempt to purchase, trade, or distribute stolen data.
- Do not interact with threat actors based solely on search results.
- Do not redistribute leaked credentials, personal information, or sensitive material.
- Do not use discovered credentials for unauthorized access.
- Do not use dark web intelligence for fraud, phishing, extortion, or social engineering.
- Validate all findings before taking action.
- Follow applicable data protection, privacy, and cybersecurity laws.

Recommended defensive actions after discovering relevant mentions:

- Validate the finding using internal security logs.
- Check whether exposed credentials are active.
- Force password resets where appropriate.
- Enable or enforce multi-factor authentication.
- Review access logs for suspicious activity.
- Investigate affected systems or accounts.
- Notify internal security, legal, or compliance teams.
- Preserve evidence according to company procedures.
- Request takedown where legally applicable.
- Monitor for repeated mentions or escalation.

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

?? Technical Highlights

- Dark web and underground forum search
- Real-time forum scraping
- Search across 5+ monitored source groups
- Simple Mode search across titles and content
- Results sorted by ingestion date
- AI threat summary
- IOC extraction
- Risk score calculation
- Bookmarks for searches and individual leaks
- Local browser-based bookmark storage
- Search history
- Daily request limits based on plan
- Powered by NiamonX Radar API
- Suitable for SOC, threat intelligence, compliance, and security monitoring workflows

---

? NiamonX Radar API

Dark Web Search is powered by **NiamonX Radar**, an advanced OSINT and cybersecurity intelligence API.

NiamonX Radar provides access to modern intelligence services through a REST API and supports automated security workflows.

The API can be used for:

- Automated integrations
- Data enrichment
- Breach intelligence
- Threat intelligence analysis
- Dark web monitoring
- IOC enrichment
- Enterprise security workflows
- Internal SOC automation
- Risk monitoring
- Compliance support

Developers and security teams can explore the full API documentation, authentication methods, available endpoints, examples, and integration guides at:

□□ https://radar.niamonx.io/

? Usage Hints

- Simple Mode searches both title and content.
- Use company names, domains, IPs, emails, usernames, BTC wallets, or CVEs as search keywords.
- Risk score is calculated from leak counts, verified hits, credentials, and IOC density.
- Bookmarks can store both search queries and individual leaks.
- Saved searches and leaks are stored locally in the browser.
- Daily requests are based on the user’s plan limits.
- Results are informational and should be validated through further investigation.
- Newer results are prioritized by ingestion date.
- AI summaries help triage findings but do not replace analyst review.

? 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 Dark Web Search is a threat intelligence and monitoring tool that helps users detect mentions of companies, domains, IP addresses, employee credentials, wallets, CVEs, and other security indicators across underground forums and marketplace-related sources.

It provides real-time forum scraping, ingestion-date sorting, AI threat summaries, IOC extraction, bookmarks, local history, risk scoring, and integration support through the NiamonX Radar API.

The tool is designed for lawful defensive cybersecurity, corporate monitoring, incident response, threat intelligence, and exposure validation. All results should be treated as intelligence leads and confirmed through further investigation before taking action.

Revision #1
Created 17 June 2026 17:02:58 by NiamonX Team
Updated 17 June 2026 17:29:48 by NiamonX Team