

Solve Cybercrime Faster.

Turn an alias into an arrest.

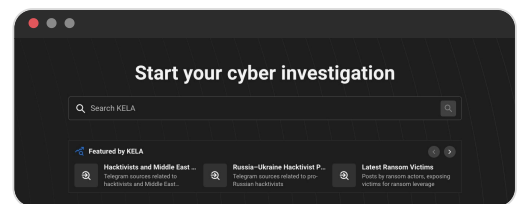
Unmask the threat actor behind dark web identities and build the case that convicts them, backed by **11+ years of proprietary cybercrime data**. Search the underground anonymously, in 130+ languages, and pivot from alias to real-world identity before evidence disappears.



Suspects hide behind aliases in closed forums and marketplaces investigators cannot safely reach; cases stall without original source evidence.



Search the underground anonymously from one interface, in 130+ languages, and pivot from alias to real-world identity.



11+ Years of Data
Anonymous Research
Original Source Evidence
130+ Languages

Anonymous by Design

Research without exposing the investigating authority or the direction of the inquiry to the source.

11+ Years, One Data Lake

A proprietary cybercrime archive: forums, markets, Telegram and Discord, leaked credentials, infostealer accounts, breached servers.

Evidence That Survives Scrutiny

Content held in-platform, so posts deleted at source stay reviewable with metadata intact.

What investigators get

From alias to identity

Trace a handle across 11+ years of forums, markets and chats, through every earlier moniker, to the person behind it: the same work that unmasked USDOD and named TeamPCP operators.

In their language, not yours

Search and auto-translate raw data in more than 130 languages, and read text inside screenshots through OCR, so leaked documents, price lists and panels are searchable.

Analyst context on every lead

Link raw data to KELA finished intelligence (actor profiles, events and insights), each with references back to the original sources.

A line of inquiry stays open

Save any query, share it with your unit and set alerts on new results, so a case continues across shifts and hand-overs without being rebuilt.

How it Works

Alias in, evidence out. The same four steps, whatever the offense.

1

Start from what you hold

A handle, domain, email, subnet or card range; the query type is detected automatically.

The query builder blocks malformed queries before they run.

2

Search everything collected

One query across raw sources and analyst-written intelligence, in 130+ languages, without exposing the inquiry.

Narrow by source, seller, service or date.

3

Pivot to the person

Follow the handle through full threads, chat histories and earlier monikers to the real-world identity behind it.

Finished intelligence links back to raw posts.

4

Preserve and continue

Content stays in the platform after deletion at source, with metadata and provenance intact.

Save the query, alert your unit, or pull it by API.

Use cases

Unmasking an alias

From one handle in a tip-off, to that actor's posts, sales threads and chat messages across KELA's forum and messaging sources.

Fraud and carding cases

From a card BIN tied to fraud losses, to the underground listings and chats carrying cards from that issuer.

Initial access sales

From a reported intrusion, to remote access market listings for the breached server and the seller's handle.

Leak and extortion claims

From an extortion claim, to the leaked records themselves, searchable by victim domain with breach source context.

11+ years of proprietary cybercrime data, one search

Every alias leaves a trail. KELA's data lake holds more than a decade of it, so earlier monikers, old posts and deleted threads are still there to find. Six data types:



Hacking Discussions

Forums, illicit markets and dark net communities.



Instant Messaging

Telegram and Discord, with full chat history.



Leaked Credentials

Third-party breaches and database dumps.



Compromised Accounts

Infostealer logs and botnet markets.



Breached Servers

Remote access market listings and sellers.



Finished Intelligence

Reports, events and insights by KELA analysts.

Features

✓ Anonymous Research

Research without exposing the identity of the investigating authority or the direction of the inquiry to the source.

✓ 130+ Languages

Raw data is searchable and auto-translated in more than 130 languages; analyst-written intelligence is produced in 15+.

✓ Source Retention

Content is held in the platform rather than linked, so a post removed at source stays reviewable with its metadata and provenance intact.

✓ Purpose-Built Query Types

Domain (includes subdomains), exact email, subnet in CIDR notation, 6-digit card BIN and free text, each tuned for more accurate matches.

✓ Boolean and Metadata Search

AND, OR, NOT, exact phrase, proximity and wildcards, plus fields: author handle, source, title, username, shared file name, country, sector, category.

✓ Image Text Search

OCR-extracted text from images in forums and chats is searchable by default, or on its own with the image operator.

✓ Source and Bot Enrichment

Hover a source, chat, bot ID or seller for context: source type, geography, description and infected machine details.

✓ Finished Intelligence

Reports, events and insights from KELA analysts, filterable by country, sector and category, linked to raw references, related intelligence and IOCs.

✓ AssetsLens

Filter any result set to the approved assets in your inventory and jump between every match inside posts, chats and reports.

✓ Saved Queries and Alerts

Daily or weekly email notifications, a new-results-only view, and group saved queries shared across your team.

✓ Featured Queries

Pre-built queries from KELA's threat intelligence analysts open real-time views of trending activity across KELA's sources.

✓ API and Licensing

RESTful JSON API for search, saved queries and full records with entity extraction. Licensed by search tokens.

From alias to arrest: the record

The same search KELA's analysts run on live cases.

BRAZIL

Operation Medici Umbra

KELA provided intelligence to the operation led by the Civil Police of Rio Grande do Sul, which mapped and dismantled a three-tier fraud pipeline and reached "Jota", the hacker supplying the sensitive government data behind it.

INFRAGARD AND AIRBUS LEAKS

USDOD

KELA unmasked the actor behind the InfraGard and Airbus leaks, tracing the alias through earlier monikers including NetSec and Scarfac33 to a named individual in Belo Horizonte, after the actor targeted the Brazilian Federal Police.

AUSTRALIA AND UNITED STATES

TeamPCP

KELA briefed the Australian Federal Police, the Western Australia Police Force and the FBI in March 2026. On 27 August 2026, two alleged members were charged in Western Australia; one was named in the threat actor profile KELA supplied in April 2026.

BREACHFORUMS

IntelBroker

KELA published its in-depth analysis of the actor before the arrest.

RESEARCH BEHIND THE HEADLINES

Scattered Spider, ShinyHunters, JLR

KELA research underpinned public reporting on Scattered Spider, ShinyHunters and the Jaguar Land Rover intrusion.

Trusted by Federal Authorities and Law Enforcement Worldwide

Actionable intelligence for government organizations across:

- ✓ National Police and Federal LEAs
- ✓ Ministries of Defense (MOD)
- ✓ National Security and Intelligence Directorates
- ✓ National CERTs and CSIRT Organizations
- ✓ Military Intelligence Commands
- ✓ Financial Crime and Investigative Units
- ✓ Public Safety and Border Security Agencies

