TRIBASTION TI

Know your breach exposure before attackers do.

Tribastion TI searches billions of leaked credentials, infostealer-log records and exposed secrets across your domains, emails and infrastructure. Results are deduplicated, risk-rated and mapped back to the machines they came from — in the console, or over a simple JSON API.

4	1	Masked	JSON
EXPOSURE SOURCES	CREDIT / SEARCH	BY DEFAULT	REST API

HOW IT WORKS

1

Search a term

A domain, email, username or keyword — from the console or one API call. Each search costs one prepaid credit.

2

Collect the footprint

The engine pulls matching stealer-log victims, breach records and leaked files, then offloads them to your own cloud storage.

3

Parse & enrich

Our parser recovers URL, username and password, extracts API keys and secrets, and links every identity across machines in an interlink graph.

4

Act on what's live

Validate whether a recovered key still works from your own position, force resets, and feed findings into your SOC or SIEM.

EVERYTHING THE EXPOSURE TOUCHES — ONE CONSOLE

Credential search
URL, username and password in one view — stealer credentials and parser-recovered ones, deduplicated.

Interlink graph
Pivot from any email, IP or username to every other machine it appears on. One lead opens the rest.

Dynamic reporting
Summary or comprehensive exposure reports across every module, delivered as encrypted PDFs.

Cloud offload
Every dumped file is moved off-platform to your own connected storage, replicated for backup.

Secrets & keys
API keys, cloud tokens and connection strings pulled from leaked files, risk-rated and validated live from your side.

Breach & stealer data
Breach corpora and stealer logs unified under one query, with phonebook and subdomain enrichment.

Client API
Self-service keys and prepaid credits — pull exposure straight into your own tooling.

Masked reveal
Passwords and secrets are masked by default. Full plaintext is a deliberate, per-account setting.

Compromised machines
Each infostealer victim categorised by IPs, emails, logins, cookies and files — the whole device, not one line.

Domain monitoring
Track a domain continuously; new exposure surfaces to the owning client automatically once approved.

Takedown workflow
Raise and track takedowns for malicious domains, hosts and fake accounts, with contact auto-discovery.

Audit log
Every search, validation and export is recorded with the actor and timestamp.

WHY TRIBASTION TI

Beyond the preview cap
Our own parser recovers URL, username and password from the raw dumped files — the exposure most feeds never surface.

Traced to the machine
Every credential links back to the infected device and the search it came from, in an interlink graph you pivot through.

Validate from your side
Test whether a leaked key or login still works from your authorized position — the platform never connects out for you.

Masked, and auditable
Safe to wire into a dashboard; full plaintext is a deliberate, per-account entitlement, and every action is logged.

WHO IT'S FOR

- **Enterprise security teams** — Continuously watch your domains, staff emails and infrastructure.
- **MSSPs & consultancies** — Onboard client domains, monitor them, hand each client scoped exposure.
- **Threat intel & IR** — Pivot from one leaked identity to every machine it touches.
- **Brand & fraud teams** — Catch fake accounts, phishing domains and impersonation early.

See your exposure in the next five minutes.

- ✓ Know your real exposure before attackers use it
- ✓ Prioritise by what is still live, not just what leaked
- ✓ Cut investigation time with one-click identity pivots
- ✓ Feed findings straight into your SOC, SIEM or ticketing

Get an API key **poc-ti.tribastiontechnologies.com/client/signup**

For volume, full-reveal and MSSP pricing, talk to your Tribastion account manager. ·