Tribastion

BREACH EXPOSURE, MAPPED TO YOUR ESTATE

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

INSIDE THIS BROCHURE

● THE PROBLEM

Your next breach has probably already leaked

Most intrusions start with a credential that is already public. Infostealer malware harvests the saved passwords, session cookies and API keys off employee and supplier machines; breach corpora pile up the rest. The material is out there for weeks or months before anyone uses it — the only question is whether you see it first.

Why now.
Infostealer logs have turned credential theft into a commodity market. A single infected laptop can expose dozens of corporate logins, live cloud keys and active sessions at once — and none of it shows up in a vulnerability scan.

What most teams see

A vulnerability list, an alert queue, and a breach-notification feed that arrives after the fact — with no link back to the machine, the person, or whether the exposure is still live.

What Tribastion TI shows

The actual leaked credentials and secrets for your estate, deduplicated and risk-rated, each traced to the device it came from, with a way to check what still works — before an attacker does.

● WHAT YOU GET OUT OF IT

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

FROM A SINGLE SEARCH TO ACTION

Search, collect, enrich, act

One search covers every source we hold. Our own parsers turn raw dumps into structured exposure you can investigate — and act on — in the console or over the API.

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.

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.

ONE INVESTIGATION CONSOLE

Everything the exposure touches, in one place

Every module below is a working page in the platform today. They share one collected dataset, so a credential always traces back to the machine and the search it came from — no swivel-chairing between tools.

Credential search

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

Secrets & keys

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

Compromised machines

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

Interlink graph

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

Breach & stealer data

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

Domain monitoring

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

Dynamic reporting

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

Client API

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

Takedown workflow

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

Cloud offload

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

Masked reveal

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

Audit log

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

Masked by default.

Every result hides the password and secret values unless an account is explicitly entitled to full plaintext — so the whole console is safe to open in front of a client or wire into a dashboard.

● FOR CLIENTS & MSSPS

Your exposure, over an API you can rely on

Create an account, get a key instantly, and pull your exposure straight into your own tooling. One credit per search, results masked by default, rate-limited per account.

● ENDPOINTS

METHOD	PATH	PURPOSE
POST	/api/v1/search	Search a domain, email, username or keyword — 1 credit
GET	/api/v1/account	Balance, entitlements and usage
POST	/api/v1/takedown	Raise a takedown for a malicious domain, host or account

● ONE CALL

```
curl -X POST https://ti.tribastiontechnologies.com/api/v1/search
  -H "Authorization: Bearer tik_your_api_key"
  -H "Content-Type: application/json"
  -d '{"q":"example.com","limit":100}'
```

Prepaid credits, no surprises

One credit per search. Start with free credits, top up when you need to, and track balance and usage from your dashboard — no sales call required to evaluate it.

Built for MSSPs

Onboard client domains, monitor them continuously, and hand each client their own scoped exposure and reports. Suspend or rotate any key at any time.

Domain monitoring & reporting.
Add a domain once; new exposure surfaces automatically as it is collected, and every finding can be turned into a summary or comprehensive report — delivered as an encrypted PDF whose open password is the recipient's email.

HANDLED THE WAY SENSITIVE DATA SHOULD BE

Powerful, and built to be used responsibly

The controls that limit how exposure is shared are enforced in the platform itself, not only in the interface.

Masked by default
Passwords and secrets are hidden in every response unless an account is explicitly entitled to reveal them.

Validation stays with you
Checks on a leaked key run from your authorized position. The platform never uses a recovered credential itself.

Encrypted at rest
Connected storage and integration credentials are encrypted and never returned by any page or API response.

Scoped, rate-limited keys
Every API key is per-account, credit-metered and rate-limited. Suspend or rotate at any time.

Every action logged
Searches, validations and exports are recorded with actor and timestamp for a full audit trail.

WHO IT IS 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.

Create an account, claim free credits and run your first search over the API or the console.

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

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