



CYBER THREAT INTELLIGENCE PRODUCT BROCHURE



business benefits, product capabilities
and operational use cases

2026 EDITION

EXECUTIVE SUMMARY

Identity-first exposure intelligence for business risk reduction

HackedList.io helps organizations identify stolen credentials, infostealer logs, exposed sessions and dark-web mentions before they become account takeover, fraud, ransomware or supplier-risk incidents.

The product is designed for decision-makers and security teams that need actionable visibility into the criminal data economy without building a full threat-intelligence collection program internally.

4.5B+

stolen credentials indexed
continuous global collection

55M+

compromised users tracked
domain and email exposure

183

countries covered
global visibility

- **Prevent account takeover:** detect exposed employee, customer and supplier credentials tied to your domains and services.
- **Prioritize what matters:** combine URL, username, dataset, device and timing context to decide which records require immediate action.
- **Reduce incident-response time:** turn alerts into reset, revoke-session, reimage, investigation and reporting workflows.
- **Protect executives and high-value users:** monitor VIP emails outside corporate domains where private-device exposure can create business impact.
- **Operationalize intelligence:** deliver records through the portal, PDF reporting, CSV/API exports and AI/MCP-enabled workflows.

Core promise

HackedList.io turns identity exposure intelligence into clear remediation decisions - not just another raw breach-data feed.



WHY THIS MATTERS NOW

Attackers increasingly log in instead of breaking in

Infostealer malware quietly steals browser passwords, session cookies, authentication tokens, autofill data, screenshots, device metadata and documents from infected computers. These logs are quickly traded and validated by access brokers, fraud actors and ransomware affiliates.

The operational risk is no longer limited to leaked passwords. A single fresh log can include enough context to bypass weak controls, impersonate a trusted user and move into SaaS, email, VPN, cloud or supplier environments.

Market reality

What it means for leadership

Credential exposure is measurable before impact

Exposed credentials and session artifacts often appear in criminal sources before fraud, ransomware or data theft is visible internally.

The hand-off window has collapsed

Logs can move quickly from infection to validation and resale, reducing the time available for manual discovery.

SaaS and session tokens are high-value targets

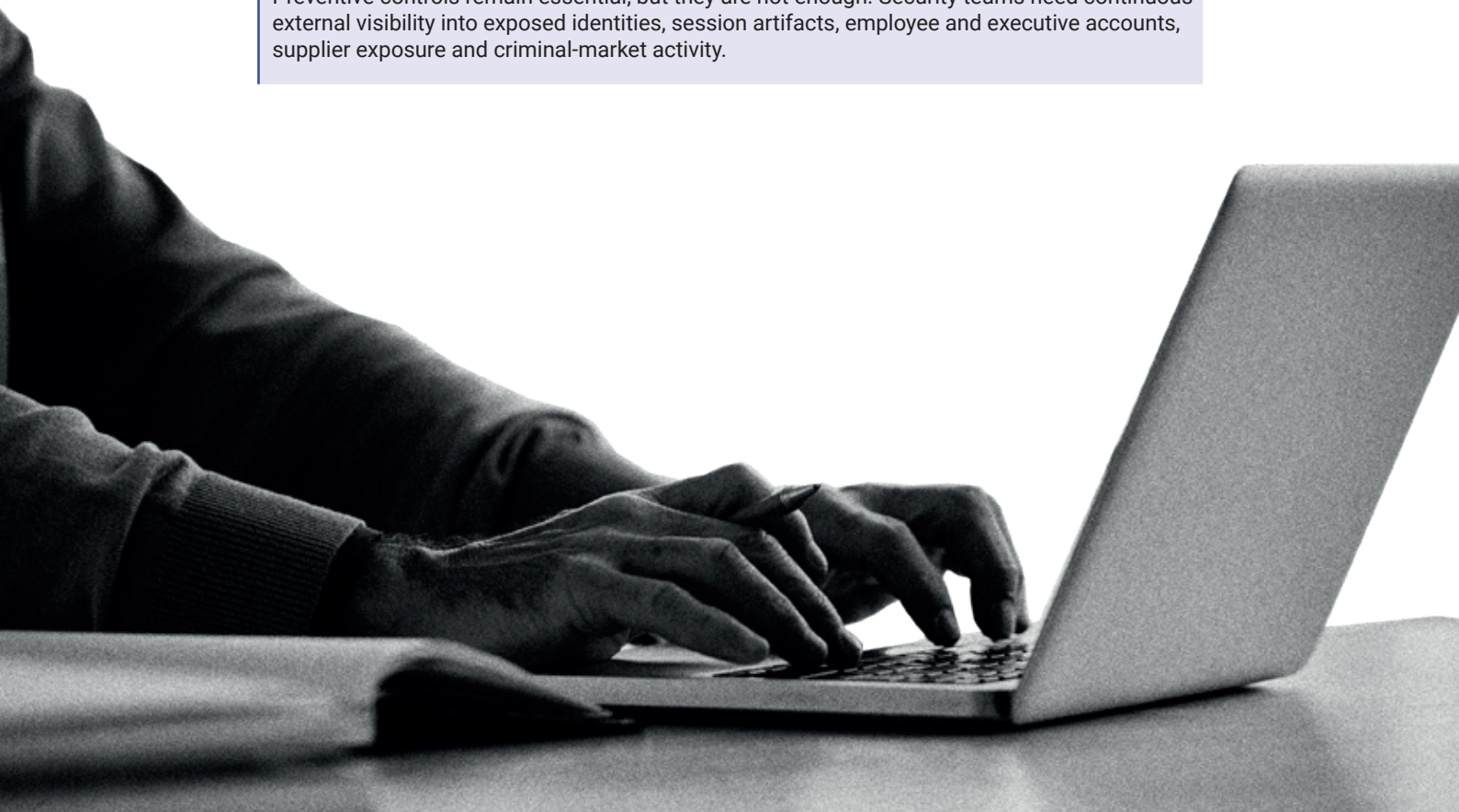
Cookies and tokens can let attackers enter cloud and collaboration platforms as an already-authenticated user.

AI increases identity exposure

AI tools, browser extensions and developer workflows add new places where credentials and tokens can be stored and stolen.

Business implication

Preventive controls remain essential, but they are not enough. Security teams need continuous external visibility into exposed identities, session artifacts, employee and executive accounts, supplier exposure and criminal-market activity.



HOW INFOSTEALER LOGS BECOME ATTACK CHAINS

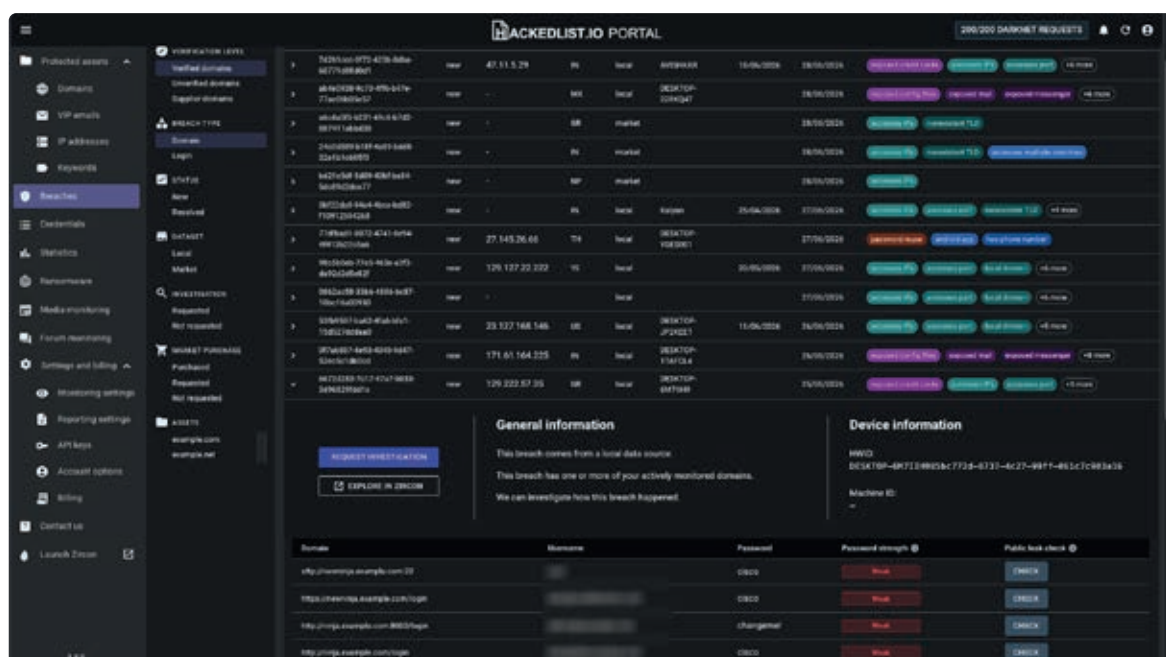
From stolen identity data to downstream impact

A stealer log is a ready-made access package. It can combine passwords, service URLs, cookies, tokens, autofill data, browser history, screenshots, device fingerprints and local files. Attackers treat this package as a starting point for fraud or intrusion, not as static breach data.

Stage	Attacker objective
01 Infect	A work or personal device is infected through phishing, fake installers, cracked software, malicious ads or poisoned downloads.
02 Harvest	The stealer captures saved passwords, cookies, tokens, browser artifacts, files and device metadata.
03 Package & trade	The stolen bundle is organized as a log and shared through marketplaces, Telegram channels or private criminal communities.
04 Validate & pivot	Access brokers or operators test what still works, prioritize valuable services and pivot into corporate systems.
05 Monetize	The same log can feed account takeover, BEC, fraud, supplier abuse, ransomware access or cloud compromise.

Where the stolen artifacts are abused

Stolen artifact	How attackers use it	Typical downstream impact
Passwords + exact service URLs	Test access against VPN, SSO, email, CRM, banking, admin consoles and third-party portals.	Account takeover, unauthorized access, targeted fraud and escalation to incident response.
Session cookies / OAuth tokens	Reuse an authenticated session instead of triggering a normal login challenge.	SaaS or cloud compromise that may bypass MFA and look like legitimate user activity.
Browser history + autofill	Build credible phishing pretexts and identify business workflows, vendors and payment relationships.	BEC, payment redirection, extortion and highly personalized social engineering.
Device fingerprints / meta-data	Mimic the infected user device and reduce anomaly signals.	Lower detection rate during fraud or intrusion attempts.
Local documents and screenshots	Validate the victim, harvest documents and discover business context.	Identity fraud, supplier abuse, extortion and data-theft preparation.



UNDERSTANDING THE BREACH LANDSCAPE

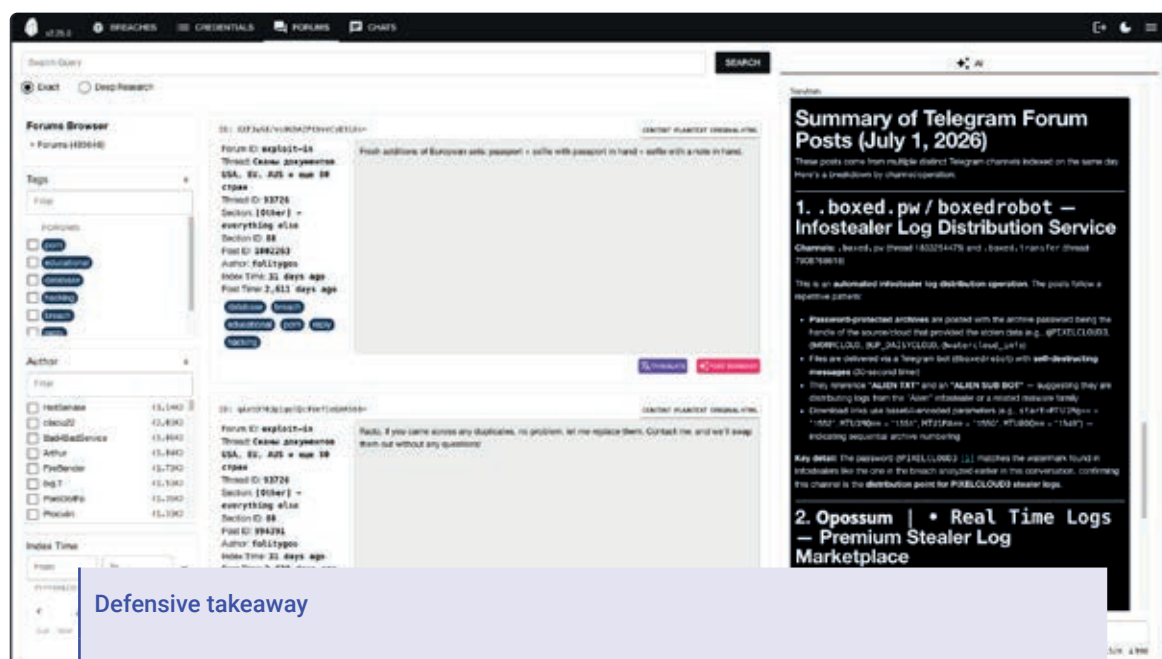
What a breach actually means

A breach in this context indicates that a computer has been infected by infostealer malware. The risk is active and operational: attackers may have obtained credentials, cookies, tokens, device information and documents from the compromised endpoint.

Breach Component	Security Implication	Business Risk
Active Malware	Infostealer running on a system	Data exfiltration in near real time.
Compromised Cookies	Session hijacking and impersonation	Unauthorized access to business and personal services.
Stolen Tokens	Authentication bypass or persistence	Persistent access to cloud and SaaS environments.
Browser Data	Saved passwords, forms and history	Lateral movement and credible social engineering.
Device Fingerprints	Ability to mimic identity context	Potential bypass of weak anomaly-based controls.
Downloaded files	Documents, configs or secrets copied from disk	Disclosure of IP, contracts, network details and personal data.

Why traditional security can miss the risk

- MFA can be weakened by stolen session cookies or tokens.
- Firewalls and endpoint tools may not detect a legitimate login from a stolen identity.
- Private-device infections can expose corporate accounts used outside managed environments.
- Supplier and contractor devices can become indirect access points into your organization.



Defensive takeaway

The first useful signal may appear outside your perimeter, in a criminal marketplace or underground forum. HackedList.io is built to turn that signal into a practical response.

A GLOBAL PROBLEM

Continuous visibility across stolen-identity ecosystems

Stolen credentials are not a local issue. Infections happen everywhere, and the stolen data is traded across borders. HackedList.io continuously collects and indexes this data from around the world, giving visibility across employees, customers and suppliers.

4.5B+

stolen credentials

current website counter

55M+

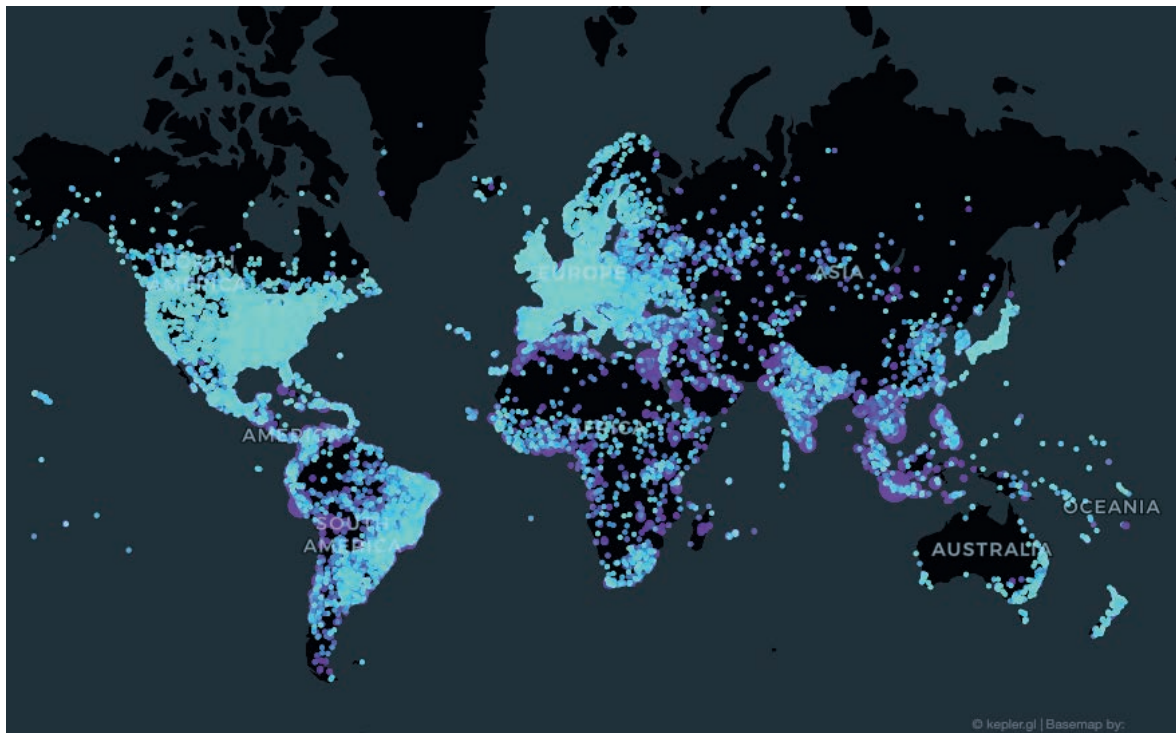
compromised users

tracked globally

183

countries

exposure distribution



The live statistics and map turn a worldwide stream of stolen data into a clear, board-readable picture of exposure concentration and global identity risk.

01 Collect

Stealer logs, markets, forums and Telegram

02 Normalize

Domains, usernames, URLs, timestamps and device context

03 Prioritize

Risk by asset, person, supplier, market status and freshness

04 Act

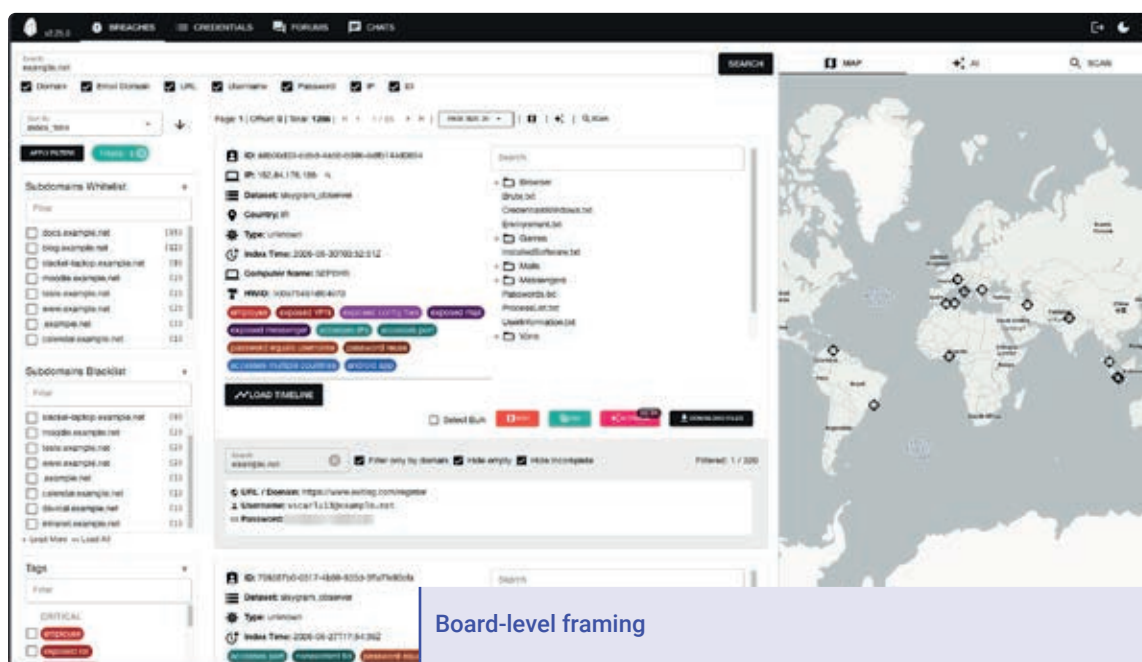
Reset, revoke, investigate, notify, export and report

BUSINESS BENEFITS

What buyers get out of the platform

HackedList.io is positioned for organizations that need actionable credential and dark-web intelligence without building a dedicated collection operation. It connects CTI, ITDR, exposure management and executive-risk workflows.

Business outcome	How HackedList.io helps	Operational value
Reduce time-to-know	Detect credentials tied to domains, executives or suppliers in infostealer and breach sources.	Faster containment: reset passwords, revoke sessions, review device health and check access logs.
Prioritize what matters	Use URL, username, dataset type, infection/index time, market status and device context.	Less alert fatigue; act first on VPN, SSO, admin consoles, cloud and payment systems.
Support ransomware readiness	Monitor ransomware leak activity and connect identity exposure to early-warning signals.	Better sector posture and vendor-risk awareness.
Strengthen executive protection	Monitor VIP emails and private-account exposure around leaders and high-value users.	Reduce takeover, impersonation and extortion risk.
Improve third-party visibility	Monitor supplier and partner domains where allowed by plan and policy.	Identify downstream risk before a vendor exposure becomes an incident.
Automate response	Use portal workflows, PDF reports, CSV/API and MCP-ready integrations.	Actionable intelligence moves into security operations, GRC and leadership reporting.



Board-level framing

Going beyond dark-web monitoring, this is an identity exposure control: a way to prove that stolen access is being watched, triaged and remediated before it becomes a larger business incident.

PRACTICAL MISUSE SCENARIOS

How stolen logs become fraud and cyberattacks

An infostealer log can contain saved credentials, session cookies, autofill data, browser history, local files and device metadata. These artifacts allow criminals to convert an infection into account takeover, payment fraud, supplier abuse or intrusion.

Abuse scenario	How stolen log data is used	Business impact
Account takeover and credential stuffing	Reused username-password pairs are tested against customer portals, e-shops, loyalty programs and internal apps.	Fraudulent purchases, refunds, loyalty-point theft, chargebacks, account lockouts and support costs.
BEC and payment redirection	Mailbox credentials or cookies give access to real threads, invoices, vendors and payment relationships.	Invoice manipulation, fake bank-detail changes, payroll diversion and high-trust financial loss.
SaaS/session hijacking	Cookies, OAuth tokens or browser sessions are reused for email, CRM, collaboration, file storage and helpdesk access.	Data theft, shadow admin activity and access that may avoid normal login alerts.
Ransomware initial access	VPN, SSO, RDP and admin-panel credentials from stealer logs are validated and sold to access brokers.	Fast intrusion path, lateral movement and ransomware preparation.
Cloud, DevOps and AI-tool compromise	Logs may expose cloud consoles, CI/CD, GitHub accounts, API keys, AI prompts, browser extensions and developer platforms.	Source-code theft, malicious code injection and leakage of prompts, secrets or customer data.
Identity and financial fraud	Autofill data, personal documents, screenshots, private-account access and banking portals can be combined into identity profiles.	Account opening, loan or credit-card fraud, extortion and reputational damage.



Where HackedList.io adds value

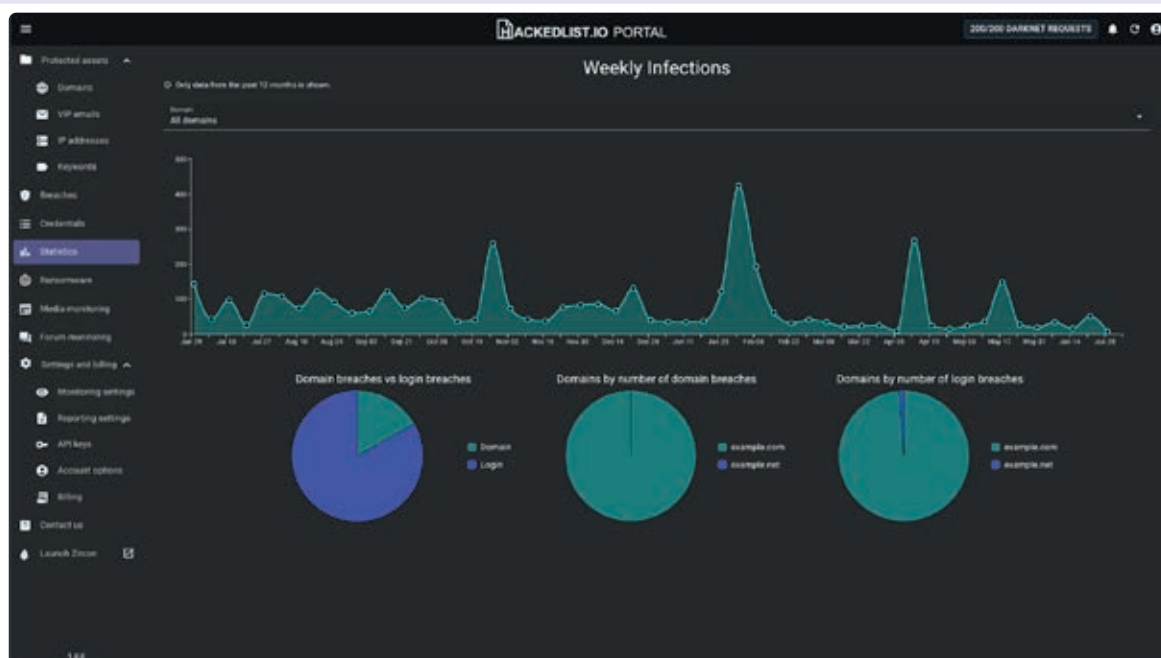
The platform helps turn these scenarios into response queues: identify affected domains, VIPs, suppliers and high-risk URLs; prioritize records involving VPN, SSO, admin consoles, cloud or payment systems; then send the findings into remediation workflows.

PRODUCT CAPABILITIES

Business benefit plus concrete function

The product combines automated source collection, domain monitoring, investigation context, reporting and integration features into a repeatable exposure-management workflow.

Capability	What it does	Business benefit
Domain asset monitoring	Add domains, verify ownership by DNS TXT, HTML tag or manual verification, and monitor related breach records.	Know where employee, customer or service credentials are exposed.
Investigation-ready breach records	Records can include URL/domain, username, password, IP, country, dataset, infection/index time, computer name and hardware ID when available.	Give analysts context to validate risk, scope impact and document response.
Local and market breach discovery	Local records are directly held in HackedList.io datasets; market leads indicate records observed for sale and can be reviewed by plan/request.	Separate immediately actionable records from deeper-investigation leads.
Filtering and workflow tracking	Filter by time, type, domain, status, verification level and investigation state.	Turn breach data into a manageable remediation queue.
Automatic reports	Configure email reports, PDF delivery, schedules and summary views.	Keep executives and operational stakeholders informed without manual reporting.
API, CSV and MCP access	Export records and connect intelligence to internal systems and AI workflows.	Support SIEM, SOAR, ITSM, GRC and analyst automation.
VIP email monitoring	Monitor executive or high-risk private emails when consent and policy requirements are met.	Protect high-risk people who may have exposure outside company domains.
Combolist and supplier coverage	Monitor credential combinations and supplier domains where plan and policy allow.	Detect reused or legacy credentials and third-party identity exposure.



PORTAL WORKFLOW

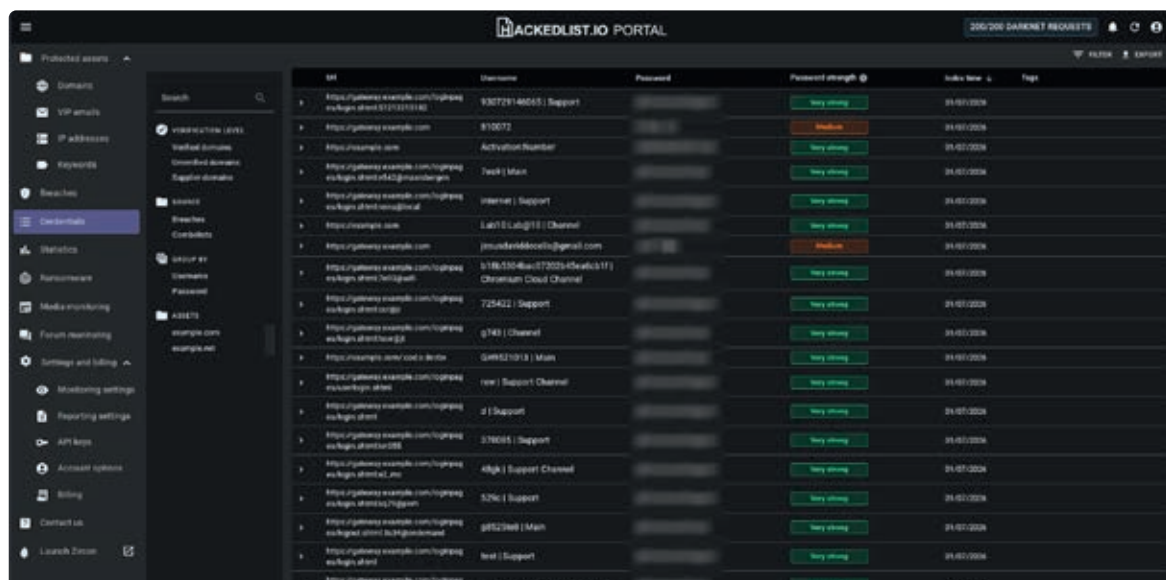
Make breach data usable by humans and systems

The Portal is the operational layer for fast breach triage. It turns criminal-source records into a clean, reliable dashboard with structured records, review status and investigation options.

Step	What happens	Output
01 Add assets	Add monitored domains, supplier domains or VIP emails based on entitlement and policy.	Defined scope for exposure monitoring.
02 Verify / consent	Use DNS/HTML/manual verification or VIP email confirmation where required.	Governed monitoring and auditability.
03 Receive records	View local records and market leads linked to monitored assets.	Prioritized exposure queue.
04 Triage	Filter by time, type, status, dataset and investigation state.	Faster decisions and reduced noise.
05 Act	Reset, revoke, reimage, request investigation or market purchase where applicable.	Concrete remediation action.
06 Report	Create PDF reports, CSV exports, API feeds and executive summaries.	Stakeholder-ready evidence.

Designed for multiple stakeholders

Role	How they use it
IT managers	Plain-language records and reports reduce dependency on specialist tooling while keeping ownership clear.
SOC / CSIRT	Structured fields, CSV, API and investigation requests support containment, case management and repeatable response.
Identity teams	Exposure context helps decide when to reset passwords, revoke sessions, reimagine endpoints or review conditional access.
Risk and leadership	Trend reports and third-party exposure indicators translate technical findings into business risk language.



RANSOMWARE, SUPPLIERS AND EXECUTIVES

Use cases that matter to leadership

Credential and infostealer exposure is valuable because it often appears before larger incidents. The most actionable program is a feedback loop: monitor stolen identity exposure, remove risky access, identify infected devices, and validate whether suppliers or executives are exposed.

Use case	Signal monitored	Business action
Ransomware monitoring	Ongoing and recent ransomware activity, victim listings, sectors, countries and group behavior.	Prepare before a sector-specific spike reaches your organization; validate backups, access controls and vendor plans.
Supplier domains	Partner and supplier exposure where allowed by plan and policy; sensitive data is handled according to entitlement and rules.	Detect downstream exposure before a vendor incident becomes your operational risk.
VIP emails	Executive or private-account exposure that can feed impersonation or targeted fraud.	Reduce business-email-compromise, extortion and reputational risk around leadership.
Customer and public portals	Credentials exposed for customer-facing, e-commerce, loyalty and service portals.	Prevent account takeover, fraud, helpdesk overload and charge-backs.
Dark-web mentions	Forum and marketplace mentions of brand, executives, products, domains and leaked context.	Prioritize investigation before leaked data becomes a campaign.

Why this belongs in third-party risk

A supplier breach is no longer only a compliance issue. Stolen supplier access can create customer impersonation exposure, billing manipulation, shared-credential risk and downstream service interruption.

Why this belongs in identity security

MFA, EDR and password policy do not automatically neutralize stolen cookies, OAuth tokens, unmanaged-device credentials or personal-account exposure around employees, partners and executives.



AI-ASSISTED INVESTIGATION AND ZIRCON

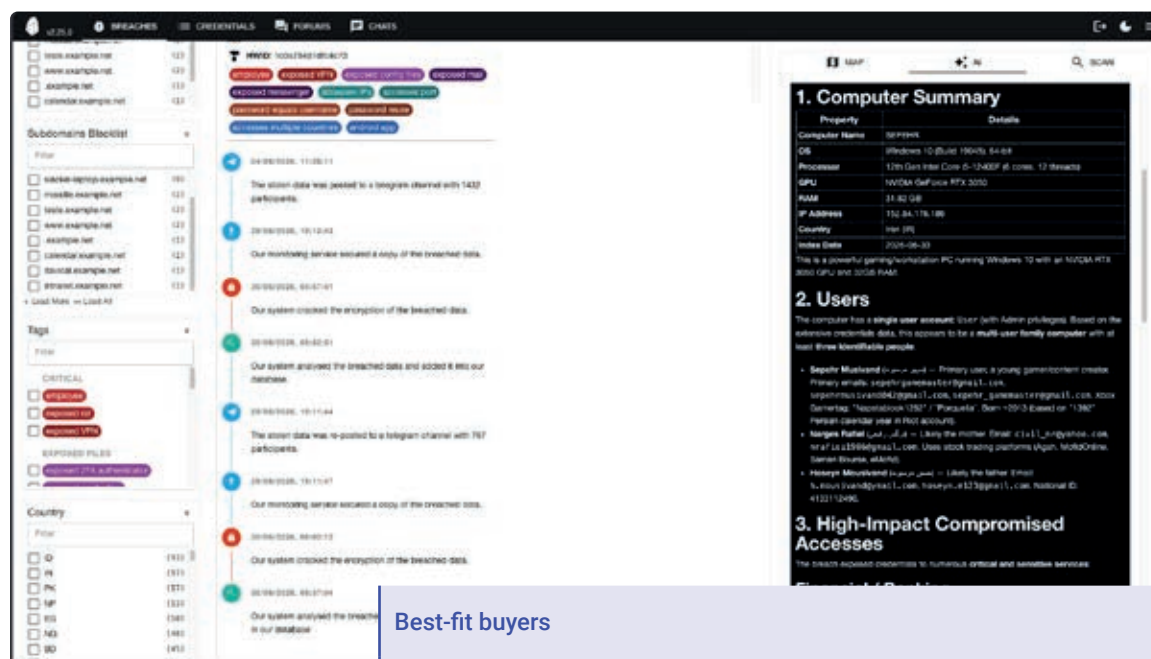
For deeper cases and analyst workflows

The standard Portal is designed for fast triage. Zircon is positioned as HackedList.io analytical engine for deeper investigations where teams need to review full infostealer logs, correlate records and run case-driven scans.

Zircon capability	What it lets you do
Full infostealer-log access	Review the full stolen package, not only a summarized alert, so analysts understand exactly what is exposed.
Duplicate and repeat-infection tracking	Spot when the same victim, device or email appears repeatedly, which may indicate unresolved compromise.
Custom dark-web scans	Run targeted scans for a case, brand, executive, product or supplier across selected sources.
AI-assisted triage	Summarize, rank and navigate large sets of text files and artifacts inside stealer logs and forum datasets.
On-premise option	Deploy advanced analysis inside a customer-controlled environment when data-residency or sensitivity requirements apply.
Investigation support	Request support on local records to identify infection path, business impact, affected credentials and recommended actions.

AI-searchable malicious forums

HackedList.io can turn indexed underground forum, marketplace and Telegram content into searchable intelligence. Analysts can ask natural-language questions such as whether a brand, executive, domain, supplier or product is being mentioned.



The screenshot displays the Zircon interface. On the left, there's a sidebar with filters for domains, subdomains, tags, and country. The main area shows a timeline of events with colored markers and text descriptions. On the right, a detailed report is visible, titled '1. Computer Summary', which includes hardware details like OS, Processor, GPU, RAM, IP Address, and Country. Below this, there's a section for '2. Users' listing email addresses and names. The bottom right corner of the interface features a 'Best-fit buyers' section.

Best-fit buyers

Zircon is most valuable for CSIRT, SOC, threat-hunting, MSSP, law-enforcement support, forensic teams and regulated industries that need deeper evidence, repeatable case work and controlled data handling.

INTEGRATIONS, AI WORKFLOWS AND DEPLOYMENT

Automation is a product feature, not a custom project

Security teams are under pressure to move faster while attackers automate reconnaissance, vulnerability discovery and identity abuse. HackedList.io supports integration through API access, CSV exports, reporting, MCP and privacy-aware deployment options.

Integration / control	What it enables	Business value
API and CSV	Fetch breach data, export records and enrich alerts in internal systems.	SIEM, SOAR, ITSM, GRC, identity governance and custom analyst workbenches.
MCP server	Expose governed HackedList.io intelligence to AI assistants and automated workflows through a standardized interface.	Ask exposure questions in plain language and trigger controlled follow-up actions.
Automatic reports	Send PDF reports by email, current schedules and reporting preferences.	Board-ready reporting without manual spreadsheet work.
VIP account controls	Private-account exposure monitoring with consent and verification.	Reduce executive-account take-over risk.
EU-operated infrastructure	Infrastructure controlled by HackedList.io in the EU.	Supports security, sovereignty and governance requirements.
Privacy-aware B2B model	VIP email monitoring requires user confirmation; supplier sensitive data can be handled according to entitlement and rules.	Balances exposure protection with contractual and legal boundaries.

Buyer checklist: what good infostealer intelligence must answer

Evaluation area	What the sales conversation should prove
Source proximity and freshness	Show visibility into stealer logs, log clouds, markets, forums and Telegram; show index vs infection timing.
Context for prioritization	Show URL, username, timestamps, IP/country/device context when available, investigation status and purchase indicators.
Remediation workflow	Demonstrate reset/revoke/reimage workflows, status exports, triage queues, request-market-purchase and stakeholder reports.
Automation and AI-readiness	Show CSV/API exports, MCP/AI integration and controlled downstream use.
Governance and privacy	Explain domain verification, VIP consent, password masking, EU-operated infrastructure and plan-specific limits.

WHY HACKEDLIST.IO?

Actionable dark-web intelligence without enterprise friction

HackedList.io delivers breach intelligence through data collection, cleaning, enrichment and investigation workflows that turn criminal-source signals into operational response.

- Comprehensive coverage: passive and active surveillance across hacker forums, Telegram channels, darknet marketplaces and breach datasets.
- Always evolving: new sources and detection logic are added as threat actors change how they trade and validate stolen data.
- Actionable intelligence: records are structured so teams can validate risk, identify the exposed service and take the next remediation step.
- Accessible darknet research: dark-web intelligence becomes understandable for executives, IT managers, SOC teams and smaller organizations.
- Top-notch security: HackedList.io operates on its own hardware in the European Union, in environments under its control rather than relying on public cloud providers.

Typical deployment path

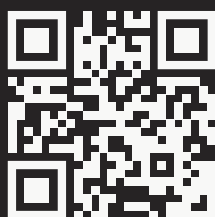
Phase	Focus	Outcome
1. Exposure review	Scan core domains, VIP emails and high-risk service patterns.	Initial risk picture and quick wins.
2. Operational monitoring	Enable recurring reports, portal workflows and response ownership.	Continuous detection and remediation cadence.
3. Automation	Add CSV/API, SIEM/SOAR/ITSM enrichment and MCP/AI workflows.	Scalable integration with existing security stack.
4. Deep investigation	Use Zircon or investigation support for high-risk cases and forensic context.	Complete picture for major incidents and regulated environments.



Strategic value

The platform closes the gap between external criminal activity and internal security operations: it shows where stolen access exists, what it likely affects and what to do next.

HACKEDLIST.IO



operations@hackedlist.io

Trusted by

mafra

 **RadioFreeEurope**
Radioliberty

AGROFERT

 **VEOLIA**

T Mobile



MINISTRY
OF REGIONAL
DEVELOPMENT CZ

 **orange™**


**Charles
University**

PRUSA
RESEARCH
by JOSEF PRUSA




FIOCCHI

CSG)