

CYBER THREAT INTELLIGENCE PRODUKTBROSCHÜRE



**Geschäftlicher Nutzen, Produktfunktionen
und operative Anwendungsfälle**

AUSGABE 2026

EXECUTIVE SUMMARY

Identitätszentrierte Exposure-Intelligence zur Reduzierung von Geschäftsrisiken

HackedList.io unterstützt Organisationen dabei, gestohlene Zugangsdaten, Infostealer-Logs, offengelegte Sitzungen und Erwähnungen im Dark Web zu erkennen, bevor daraus Vorfälle wie Account-Übernahme (ATO), Betrug, Ransomware oder Lieferantenrisiken entstehen.

Das Produkt richtet sich an Entscheidungsträger und Sicherheitsteams, die umsetzbare Transparenz über die kriminelle Datenökonomie benötigen, ohne intern ein vollständiges Programm zur Threat-Intelligence-Erfassung aufbauen zu müssen.

4,5 Mrd.+

indexierte gestohlene Zugangsdaten

kontinuierliche globale Erfassung

55 Mio.+

überwachte kompromittierte Nutzer

Domain- und E-Mail-Exposure

183

abgedeckte Länder

globale Sichtbarkeit

- **Account-Übernahme verhindern:** Erkennen Sie offengelegte Zugangsdaten von Mitarbeitenden, Kunden und Lieferanten, die mit Ihren Domains und Diensten verknüpft sind.
- **Prioritäten richtig setzen:** Kombinieren Sie URL-, Benutzernamen-, Datensatz-, Geräte- und Zeitkontext, um zu entscheiden, welche Datensätze sofortiges Handeln erfordern.
- **Incident-Response-Zeit verkürzen:** Überführen Sie Warnmeldungen in Workflows für Passwort-Reset, Sitzungswiderruf, Neuaufsetzen, Untersuchung und Reporting.
- **Führungskräfte und schützenswerte Nutzer absichern:** Überwachen Sie VIP-E-Mail-Adressen außerhalb von Unternehmensdomains, bei denen die Gefährdung privater Geräte geschäftliche Auswirkungen haben kann.
- **Intelligence operationalisieren:** Stellen Sie Datensätze über das Portal, PDF-Reporting, CSV-/API-Exporte und KI-/MCP-fähige Workflows bereit.

Kernversprechen

HackedList.io verwandelt Intelligence über Identitätsgefährdung in klare Entscheidungen für Gegenmaßnahmen – und ist nicht nur ein weiterer roher Datenfeed zu Datenlecks.

WARUM DAS JETZT WICHTIG IST

Angreifer melden sich zunehmend an, statt einzubrechen

Infostealer-Malware stiehlt unbemerkt Browser-Passwörter, Session-Cookies, Authentifizierungs-Token, Autofill-Daten, Screenshots, Gerätemetadaten und Dokumente von infizierten Computern. Diese Logs werden von Access Brokern, Betrugsakteuren und Ransomware-Affiliates schnell gehandelt und validiert.

Das operative Risiko beschränkt sich nicht mehr auf geleakte Passwörter. Ein einziges frisches Log kann genügend Kontext enthalten, um schwache Kontrollen zu umgehen, sich als vertrauenswürdiger Nutzer auszugeben und in SaaS-, E-Mail-, VPN-, Cloud- oder Lieferantenumgebungen vorzudringen.

Marktrealität	Was das für die Führungsebene bedeutet
Die Offenlegung von Zugangsdaten ist bereits vor dem Schaden messbar	Offengelegte Zugangsdaten und Sitzungsartefakte erscheinen häufig in kriminellen Quellen, bevor Betrug, Ransomware oder Datendiebstahl intern sichtbar werden.
Das Zeitfenster bis zur Weitergabe ist geschrumpft	Logs gelangen schnell von der Infektion über die Validierung bis zum Weiterverkauf und verkürzen so die Zeit für die manuelle Entdeckung.
SaaS- und Sitzungs-Token sind hochwertige Ziele	Cookies und Token ermöglichen es Angreifern, als bereits authentifizierter Nutzer in Cloud- und Kollaborationsplattformen einzudringen.
KI erhöht die Identitätsgefährdung	KI-Tools, Browser-Erweiterungen und Entwickler-Workflows schaffen neue Orte, an denen Zugangsdaten und Token gespeichert und gestohlen werden können.

Geschäftliche Konsequenz

Präventive Kontrollen bleiben unverzichtbar, reichen allein aber nicht aus. Sicherheitsteams benötigen kontinuierliche externe Transparenz über offengelegte Identitäten, Sitzungsartefakte, Mitarbeiter- und Führungskräftekonten, Lieferantengefährdung und Aktivitäten auf kriminellen Marktplätzen.

WIE AUS INFOSTEALER-LOGS ANGRIFFSKETTEN WERDEN

Von gestohlenen Identitätsdaten zu Folgeschäden

Ein Stealer-Log ist ein fertiges Zugangspaket. Es kann Passwörter, Dienst-URLs, Cookies, Token, Autofill-Daten, Browserverlauf, Screenshots, Geräte-Fingerprints und lokale Dateien vereinen. Angreifer nutzen dieses Paket als Ausgangspunkt für Betrug oder Eindringen – nicht als statische Leak-Daten.

Phase	Ziel des Angreifers
01 Infizieren	Ein dienstliches oder privates Gerät wird über Phishing, gefälschte Installer, Raubkopien, schädliche Werbung oder manipulierte Downloads infiziert.
02 Sammeln	Der Stealer erfasst gespeicherte Passwörter, Cookies, Token, Browserartefakte, Dateien und Gerätemetadaten.
03 Bündeln & Handeln	Das gestohlene Bündel wird als Log organisiert und über Marktplätze, Telegram-Kanäle oder private kriminelle Communities verbreitet.
04 Validieren & Ausbreiten	Access Broker oder Betreiber prüfen, was noch funktioniert, priorisieren wertvolle Dienste und dringen in Unternehmenssysteme vor.
05 Monetarisieren	Dasselbe Log kann Account-Übernahme, BEC, Betrug, Lieferantenmissbrauch, Ransomware-Zugang oder Cloud-Kompromittierung speisen.

Wo die gestohlenen Artefakte missbraucht werden

Gestohlenes Artefakt	Wie Angreifer es nutzen	Typische Folgeschäden
Passwörter + exakte Dienst-URLs	Zugriff auf VPN, SSO, E-Mail, CRM, Banking, Admin-Konsolen und Drittanbieter-Portale testen.	Account-Übernahme, unbefugter Zugriff, gezielter Betrug und Eskalation zur Incident Response.
Session-Cookies / OAuth-Token	Eine authentifizierte Sitzung wiederverwenden, statt eine normale Login-Abfrage auszulösen.	SaaS- oder Cloud-Kompromittierung, die MFA umgehen und wie legitime Nutzeraktivität aussehen kann.
Browserverlauf + Autofill	Glaubwürdige Phishing-Vorwände erstellen und Geschäftsabläufe, Lieferanten und Zahlungsbeziehungen identifizieren.	BEC, Umleitung von Zahlungen, Erpressung und hochgradig personalisiertes Social Engineering.
Geräte-Fingerprints / Metadaten	Das infizierte Nutzergerät nachahmen und Anomaliesignale reduzieren.	Geringere Erkennungsrate bei Betrugs- oder Eindringversuchen.
Lokale Dokumente und Screenshots	Das Opfer validieren, Dokumente abgreifen und den Geschäftskontext erschließen.	Identitätsbetrug, Lieferantenmissbrauch, Erpressung und Vorbereitung von Datendiebstahl.

DIE LANDSCHAFT DER DATENKOMPROMITTIERUNG VERSTEHEN

Was eine Kompromittierung tatsächlich bedeutet

Eine Kompromittierung bedeutet in diesem Kontext, dass ein Computer mit Infostealer-Malware infiziert wurde. Das Risiko ist aktiv und operativ: Angreifer haben möglicherweise Zugangsdaten, Cookies, Token, Geräteinformationen und Dokumente vom kompromittierten Endpunkt erlangt.

Komponente	Sicherheitsrelevanz	Geschäftsrisiko
Aktive Malware	Auf einem System laufender Infostealer	Datenexfiltration nahezu in Echtzeit.
Kompromitierte Cookies	Session-Hijacking und Identitätsvortäuschung	Unbefugter Zugriff auf geschäftliche und private Dienste.
Gestohlene Token	Umgehung der Authentifizierung oder Persistenz	Dauerhafter Zugriff auf Cloud- und SaaS-Umgebungen.
Browserdaten	Gespeicherte Passwörter, Formulare und Verlauf	Laterale Bewegung und glaubwürdiges Social Engineering.
Geräte-Fingerprints	Möglichkeit, den Identitätskontext nachzuahmen	Mögliche Umgehung schwacher anomaliebasierter Kontrollen.
Heruntergeladene Dateien	Von der Festplatte kopierte Dokumente, Konfigurationen oder Secrets	Offenlegung von geistigem Eigentum, Verträgen, Netzwerkdetails und personenbezogenen Daten.

Warum klassische Sicherheit das Risiko übersehen kann

- MFA kann durch gestohlene Session-Cookies oder Token ausgehebelt werden.
- Firewalls und Endpunkt-Tools erkennen einen legitimen Login mit gestohlener Identität möglicherweise nicht.
- Infektionen privater Geräte können Unternehmenskonten offenlegen, die außerhalb verwalteter Umgebungen genutzt werden.
- Geräte von Lieferanten und Auftragnehmern können zu indirekten Zugangspunkten in Ihre Organisation werden.

Fazit für die Verteidigung

Das erste brauchbare Signal erscheint möglicherweise außerhalb Ihres Perimeters – auf einem kriminellen Marktplatz oder in einem Untergrundforum. HackedList.io ist darauf ausgelegt, dieses Signal in eine praktische Reaktion zu überführen.

EIN GLOBALES PROBLEM

Kontinuierliche Sichtbarkeit über Ökosysteme gestohlener Identitäten

Gestohlene Zugangsdaten sind kein lokales Problem. Infektionen geschehen überall, und die gestohlenen Daten werden grenzüberschreitend gehandelt. HackedList.io erfasst und indexiert diese Daten kontinuierlich weltweit und schafft so Sichtbarkeit über Mitarbeitende, Kunden und Lieferanten hinweg.

4,5 Mrd.+

gestohlene Zugangsdaten

aktueller Website-Zähler

55 Mio.+

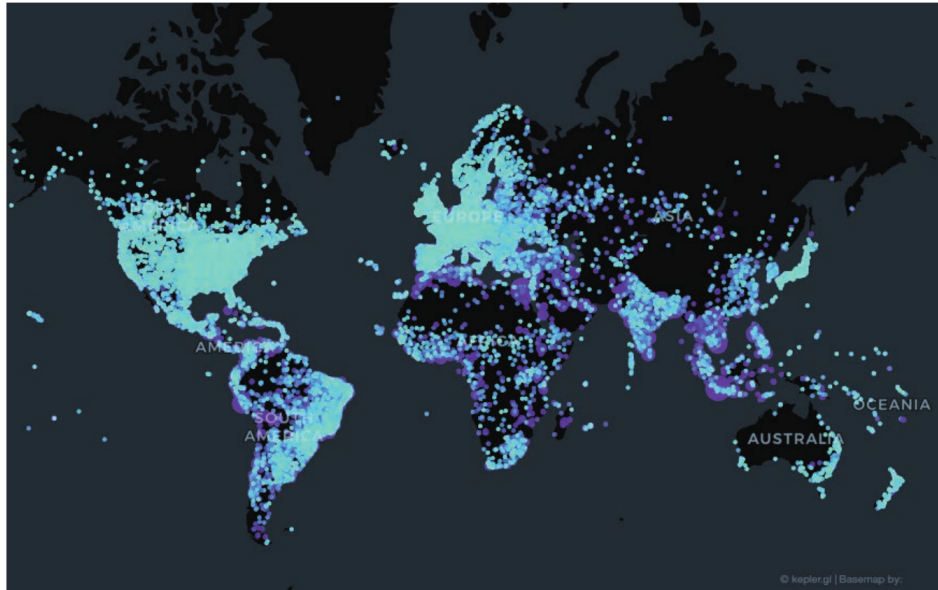
kompromittierte Nutzer

weltweit erfasst

183

Länder

Verteilung der Gefährdung



Die Live-Statistiken und die Karte verwandeln einen weltweiten Strom gestohlener Daten in ein klares, für die Führungsebene verständliches Bild der Gefährdungskonzentration und des globalen Identitätsrisikos.

01 Erfassen

Stealer-Logs, Marktplätze,
Foren und Telegram

02 Normalisieren

Domains, Benutzernamen,
URLs, Zeitstempel und
Gerätekontext

03 Priorisieren

Risiko nach Asset, Person,
Lieferant, Marktstatus und
Aktualität

04 Handeln

Zurücksetzen, widerrufen,
untersuchen, benachrichtigen,
exportieren und berichten

GESCHÄFTLICHER NUTZEN

Was Kunden aus der Plattform gewinnen

HackedList.io ist für Organisationen konzipiert, die umsetzbare Intelligence zu Zugangsdaten und Dark Web benötigen, ohne einen eigenen Erfassungsbetrieb aufzubauen. Die Plattform verbindet Workflows für CTI, ITDR, Exposure-Management und das Risiko von Führungskräften.

Geschäftsergebnis	Wie HackedList.io hilft	Operativer Nutzen
Zeit bis zur Kenntnis verkürzen	Zugangsdaten erkennen, die in Infostealer- und Leak-Quellen mit Domains, Führungskräften oder Lieferanten verknüpft sind.	Schnellere Eindämmung: Passwörter zurücksetzen, Sitzungen widerrufen, Gerätezustand prüfen und Zugriffsprotokolle kontrollieren.
Prioritäten richtig setzen	URL, Benutzername, Datensatztyp, Infektions-/Indexzeit, Marktstatus und Gerätekontext nutzen.	Weniger Alarmmüdigkeit; zuerst bei VPN, SSO, Admin-Konsolen, Cloud- und Zahlungssystemen handeln.
Ransomware-Bereitschaft unterstützen	Ransomware-Leak-Aktivität überwachen und Identitätsgefährdung mit Frühwarnsignalen verknüpfen.	Bessere Sicherheitslage der Branche und Bewusstsein für Lieferantenrisiken.
Schutz von Führungskräften stärken	VIP-E-Mail-Adressen und die Gefährdung privater Konten von Führungskräften und schützenswerten Nutzern überwachen.	Risiko von Übernahme, Identitätsvortäuschung und Erpressung reduzieren.
Transparenz über Dritte verbessern	Lieferanten- und Partnerdomains überwachen, soweit Tarif und Richtlinie dies zulassen.	Folgerisiken erkennen, bevor die Gefährdung eines Lieferanten zum Vorfall wird.
Reaktion automatisieren	Portal-Workflows, PDF-Berichte, CSV/API und MCP-fähige Integrationen nutzen.	Umsetzbare Intelligence fließt in Security Operations, GRC und das Reporting für die Führungsebene.

Einordnung für den Vorstand

Dies geht über Dark-Web-Monitoring hinaus und ist eine Kontrolle der Identitätsgefährdung: ein Weg, nachzuweisen, dass gestohlene Zugänge überwacht, triagiert und behoben werden, bevor daraus ein größerer Geschäftsvorfall wird.

PRAKTISCHE MISSBRAUCHSSZENARIEN

Wie gestohlene Logs zu Betrug und Cyberangriffen werden

Ein Infostealer-Log kann gespeicherte Zugangsdaten, Session-Cookies, Autofill-Daten, Browserverlauf, lokale Dateien und Gerätemetadaten enthalten. Mit diesen Artefakten können Kriminelle eine Infektion in Account-Übernahme, Zahlungsbetrug, Lieferantenmissbrauch oder Eindringen umwandeln.

Missbrauchsszenario	Wie gestohlene Log-Daten genutzt werden	Geschäftliche Auswirkung
Account-Übernahme und Credential Stuffing	Wiederverwendete Benutzernamen-Passwort-Paare werden gegen Kundenportale, Online-Shops, Bonusprogramme und interne Anwendungen getestet.	Betrügerische Käufe, Rückerstattungen, Diebstahl von Bonuspunkten, Rückbuchungen, Kontosperrungen und Supportkosten.
BEC und Umleitung von Zahlungen	Postfach-Zugangsdaten oder Cookies ermöglichen den Zugriff auf echte Konversationen, Rechnungen, Lieferanten und Zahlungsbeziehungen.	Rechnungsmanipulation, gefälschte Änderungen von Bankdaten, Umleitung von Gehaltszahlungen und Vertrauensbetrug mit hohem finanziellem Schaden.
SaaS-/Session-Hijacking	Cookies, OAuth-Token oder Browsersitzungen werden für Zugriff auf E-Mail, CRM, Kollaboration, Dateispeicher und Helpdesk wiederverwendet.	Datendiebstahl, verdeckte Admin-Aktivität und Zugriff, der normale Login-Warnungen umgehen kann.
Ransomware-Erstzugang	VPN-, SSO-, RDP- und Admin-Panel-Zugangsdaten aus Stealer-Logs werden validiert und an Access Broker verkauft.	Schneller Angriffspfad, laterale Bewegung und Vorbereitung von Ransomware.
Kompromittierung von Cloud, DevOps und KI-Tools	Logs können Cloud-Konsolen, CI/CD, GitHub-Konten, API-Schlüssel, KI-Prompts, Browser-Erweiterungen und Entwicklerplattformen offenlegen.	Diebstahl von Quellcode, Einschleusen von Schadcode und Leaks von Prompts, Secrets oder Kundendaten.
Identitäts- und Finanzbetrug	Autofill-Daten, persönliche Dokumente, Screenshots, Zugriff auf private Konten und Banking-Portale lassen sich zu Identitätsprofilen kombinieren.	Kontoeröffnungen, Kredit- oder Kreditkartenbetrug, Erpressung und Reputationsschäden.

Wo HackedList.io Mehrwert schafft

Die Plattform hilft, diese Szenarien in Reaktions-Warteschlangen zu überführen: betroffene Domains, VIPs, Lieferanten und risikoreiche URLs identifizieren; Datensätze zu VPN, SSO, Admin-Konsolen, Cloud oder Zahlungssystemen priorisieren; und die Ergebnisse anschließend in Workflows für Gegenmaßnahmen leiten.

PRODUKTFUNKTIONEN

Geschäftlicher Nutzen plus konkrete Funktion

Das Produkt vereint automatisierte Quellenerfassung, Domain-Überwachung, Untersuchungskontext, Reporting und Integrationsfunktionen zu einem wiederholbaren Workflow für Exposure-Management.

Funktion	Was sie leistet	Geschäftlicher Nutzen
Überwachung von Domain-Assets	Domains hinzufügen, den Besitz per DNS-TXT, HTML-Tag oder manueller Prüfung verifizieren und zugehörige Leak-Datensätze überwachen.	Wissen, wo Zugangsdaten von Mitarbeitenden, Kunden oder Diensten offengelegt sind.
Untersuchungsbereite Leak-Datensätze	Datensätze können URL/Domain, Benutzername, Passwort, IP, Land, Datensatz, Infektions-/Indexzeit, Computernamen und Hardware-ID enthalten, sofern verfügbar.	Analysten Kontext geben, um Risiken zu validieren, Auswirkungen einzugrenzen und die Reaktion zu dokumentieren.
Lokale und marktbasierte Leak-Erkennung	Lokale Datensätze werden direkt in den HackedList.io-Datenbeständen gehalten; Markt-Leads verweisen auf zum Verkauf angebotene Datensätze und können je nach Tarif/Anfrage geprüft werden.	Sofort umsetzbare Datensätze von Leads für tiefergehende Untersuchungen trennen.
Filterung und Workflow-Verfolgung	Nach Zeit, Typ, Domain, Status, Verifizierungsstufe und Untersuchungsstand filtern.	Leak-Daten in eine handhabbare Warteschlange für Gegenmaßnahmen verwandeln.
Automatische Berichte	E-Mail-Berichte, PDF-Zustellung, Zeitpläne und Übersichtsansichten konfigurieren.	Führungskräfte und operative Stakeholder ohne manuelles Reporting informiert halten.
API-, CSV- und MCP-Zugang	Datensätze exportieren und Intelligence mit internen Systemen und KI-Workflows verbinden.	SIEM, SOAR, ITSM, GRC und Analysten-Automatisierung unterstützen.
VIP-E-Mail-Überwachung	Private E-Mail-Adressen von Führungskräften oder Hochrisikopersonen überwachen, sofern Einwilligung und Richtlinien erfüllt sind.	Hochrisikopersonen schützen, die außerhalb der Unternehmensdomains gefährdet sein können.
Combolist- und Lieferantenabdeckung	Zugangsdaten-Kombinationen und Lieferantendomains überwachen, soweit Tarif und Richtlinie es zulassen.	Wiederverwendete oder veraltete Zugangsdaten und die Identitätsgefährdung Dritter erkennen.

PORTAL-WORKFLOW

Leak-Daten für Menschen und Systeme nutzbar machen

Das Portal ist die operative Ebene für die schnelle Triage von Datenlecks. Es verwandelt Datensätze aus kriminellen Quellen in ein übersichtliches, zuverlässiges Dashboard mit strukturierten Datensätzen, Prüfstatus und Untersuchungsoptionen.

Schritt	Was geschieht	Ergebnis
01 Assets hinzufügen	Überwachte Domains, Lieferantendomains oder VIP-E-Mail-Adressen gemäß Berechtigung und Richtlinie hinzufügen.	Definierter Umfang für die Gefährdungsüberwachung.
02 Verifizieren / Einwilligung	DNS-/HTML-/manuelle Verifizierung oder VIP-E-Mail-Bestätigung nutzen, sofern erforderlich.	Regelkonforme Überwachung und Nachvollziehbarkeit.
03 Datensätze empfangen	Lokale Datensätze und Markt-Leads einsehen, die mit überwachten Assets verknüpft sind.	Priorisierte Gefährdungs-Warteschlange.
04 Triage	Nach Zeit, Typ, Status, Datensatz und Untersuchungsstand filtern.	Schnellere Entscheidungen und weniger Rauschen.
05 Handeln	Zurücksetzen, widerrufen, neu aufsetzen, Untersuchung oder Marktkauf anfordern, sofern zutreffend.	Konkrete Gegenmaßnahme.
06 Berichten	PDF-Berichte, CSV-Exporte, API-Feeds und Management-Zusammenfassungen erstellen.	Für Stakeholder aufbereitete Nachweise.

Für unterschiedliche Stakeholder konzipiert

Rolle	Wie sie es nutzen
IT-Verantwortliche	Verständlich formulierte Datensätze und Berichte reduzieren die Abhängigkeit von Spezialwerkzeugen und halten Verantwortlichkeiten klar.
SOC / CSIRT	Strukturierte Felder, CSV, API und Untersuchungsanfragen unterstützen Eindämmung, Fallmanagement und wiederholbare Reaktion.
Identity-Teams	Der Gefährdungskontext hilft bei der Entscheidung, wann Passwörter zurückgesetzt, Sitzungen widerrufen, Endpunkte neu aufgesetzt oder Conditional-Access-Regeln überprüft werden sollten.
Risiko und Führung	Trendberichte und Indikatoren zur Gefährdung Dritter übersetzen technische Erkenntnisse in die Sprache des Geschäftsrisikos.

RANSOMWARE, LIEFERANTEN UND FÜHRUNGSKRÄFTE

Anwendungsfälle, die für die Führungsebene zählen

Die Gefährdung durch Zugangsdaten und Infostealer ist wertvoll, weil sie oft vor größeren Vorfällen sichtbar wird. Das wirkungsvollste Programm ist ein Regelkreis: Gefährdung gestohlener Identitäten überwachen, riskante Zugänge entfernen, infizierte Geräte identifizieren und prüfen, ob Lieferanten oder Führungskräfte betroffen sind.

Anwendungsfall	Überwachtes Signal	Geschäftliche Maßnahme
Ransomware-Überwachung	Laufende und jüngste Ransomware-Aktivität, Opferlisten, Branchen, Länder und Gruppenverhalten.	Vorbereiten, bevor ein branchenspezifischer Anstieg Ihre Organisation erreicht; Backups, Zugriffskontrollen und Lieferantenpläne prüfen.
Lieferantendomains	Gefährdung von Partnern und Lieferanten, soweit Tarif und Richtlinie es zulassen; sensible Daten werden gemäß Berechtigung und Regeln behandelt.	Folgegefährdung erkennen, bevor ein Lieferantenvorfall zu Ihrem operativen Risiko wird.
VIP-E-Mail-Adressen	Gefährdung von Führungskräften oder privaten Konten, die Identitätsvortäuschung oder gezielten Betrug ermöglichen kann.	Risiko von Business E-Mail Compromise, Erpressung und Reputationsschäden im Umfeld der Führung reduzieren.
Kunden- und öffentliche Portale	Offengelegte Zugangsdaten für Kunden-, E-Commerce-, Bonus- und Serviceportale.	Account-Übernahme, Betrug, Helpdesk-Überlastung und Rückbuchungen verhindern.
Dark-Web-Erwähnungen	Erwähnungen von Marke, Führungskräften, Produkten, Domains und geleaktem Kontext in Foren und auf Marktplätzen.	Untersuchung priorisieren, bevor geleakte Daten zu einer Kampagne werden.

Warum dies zum Lieferantenrisiko gehört

Eine Kompromittierung bei einem Lieferanten ist längst nicht mehr nur ein Compliance-Thema. Gestohlene Lieferantenzugänge können Risiken durch Kundenvortäuschung, Manipulation der Abrechnung, gemeinsam genutzte Zugangsdaten und Betriebsunterbrechungen in der Lieferkette schaffen.

Warum dies zur Identitätssicherheit gehört

MFA, EDR und Passwortrichtlinien neutralisieren gestohlene Cookies, OAuth-Token, Zugangsdaten nicht verwalteter Geräte oder die Gefährdung privater Konten von Mitarbeitenden, Partnern und Führungskräften nicht automatisch.

KI-GESTÜTZTE UNTERSUCHUNG UND ZIRCON

Für tiefergehende Fälle und Analysten-Workflows

Das Standard-Portal ist auf schnelle Triage ausgelegt. Zircon ist die analytische Engine von HackedList.io für tiefergehende Untersuchungen, bei denen Teams vollständige Infostealer-Logs prüfen, Datensätze korrelieren und fallbezogene Scans durchführen müssen.

Zircon-Funktion	Was sie ermöglicht
Vollständiger Zugriff auf Infostealer-Logs	Das gesamte gestohlene Paket prüfen, nicht nur eine zusammengefasste Warnung, damit Analysten genau verstehen, was offengelegt ist.
Verfolgung von Duplikaten und Reinfektionen	Erkennen, wenn dasselbe Opfer, Gerät oder dieselbe E-Mail wiederholt auftaucht – ein möglicher Hinweis auf eine ungelöste Kompromittierung.
Individuelle Dark-Web-Scans	Gezielte Scans für einen Fall, eine Marke, eine Führungskraft, ein Produkt oder einen Lieferanten über ausgewählte Quellen durchführen.
KI-gestützte Triage	Große Mengen an Textdateien und Artefakten in Stealer-Logs und Forendatensätzen zusammenfassen, priorisieren und durchsuchen.
On-Premise-Option	Fortgeschrittene Analysen in einer kundengesteuerten Umgebung bereitstellen, wenn Anforderungen an Datenresidenz oder Sensibilität bestehen.
Untersuchungsunterstützung	Unterstützung zu lokalen Datensätzen anfordern, um Infektionsweg, geschäftliche Auswirkungen, betroffene Zugangsdaten und empfohlene Maßnahmen zu bestimmen.

KI-durchsuchbare kriminelle Foren

HackedList.io kann indexierte Inhalte aus Untergrundforen, Marktplätzen und Telegram in durchsuchbare Intelligence verwandeln. Analysten können Fragen in natürlicher Sprache stellen – etwa, ob eine Marke, Führungskraft, Domain, ein Lieferant oder Produkt erwähnt wird.

Ideale Zielgruppen

Zircon ist besonders wertvoll für CSIRT, SOC, Threat Hunting, MSSP, die Unterstützung von Strafverfolgungsbehörden, forensische Teams und regulierte Branchen, die tiefergehende Nachweise, wiederholbare Fallarbeit und kontrollierte Datenhandhabung benötigen.

INTEGRATIONEN, KI-WORKFLOWS UND BEREITSTELLUNG

Automatisierung ist eine Produktfunktion, kein individuelles Projekt

Sicherheitsteams stehen unter Druck, schneller zu handeln, während Angreifer Aufklärung, Schwachstellensuche und Identitätsmissbrauch automatisieren. HackedList.io unterstützt die Integration über API-Zugang, CSV-Exporte, Reporting, MCP und datenschutzbewusste Bereitstellungsoptionen.

Integration / Steuerung	Was sie ermöglicht	Geschäftlicher Wert
API und CSV	Leak-Daten abrufen, Datensätze exportieren und Warnungen in internen Systemen anreichern.	SIEM, SOAR, ITSM, GRC, Identity Governance und individuelle Analysten-Arbeitsplätze.
MCP-Server	Regelkonform bereitgestellte HackedList.io-Intelligence über eine standardisierte Schnittstelle für KI-Assistenten und automatisierte Workflows verfügbar machen.	Gefährdungsfragen in natürlicher Sprache stellen und kontrollierte Folgeaktionen auslösen.
Automatische Berichte	PDF-Berichte per E-Mail gemäß aktuellen Zeitplänen und Reporting-Präferenzen versenden.	Vorstandsreifes Reporting ohne manuelle Tabellenarbeit.
VIP-Kontosteuerung	Überwachung der Gefährdung privater Konten mit Einwilligung und Verifizierung.	Risiko der Übernahme von Führungskräftekonten reduzieren.
In der EU betriebene Infrastruktur	Von HackedList.io in der EU kontrollierte Infrastruktur.	Unterstützt Anforderungen an Sicherheit, Souveränität und Governance.
Datenschutzbewusstes B2B-Modell	Die VIP-E-Mail-Überwachung erfordert die Bestätigung des Nutzers; sensible Lieferantendaten können gemäß Berechtigung und Regeln behandelt werden.	Bringt Gefährdungsschutz mit vertraglichen und rechtlichen Grenzen in Einklang.

Einkäufer-Checkliste: Was gute Infostealer-Intelligence beantworten muss

Bewertungsbereich	Was das Verkaufsgespräch belegen sollte
Quellennähe und Aktualität	Sichtbarkeit in Stealer-Logs, Log-Clouds, Marktplätze, Foren und Telegram nachweisen; Index- vs. Infektionszeitpunkt zeigen.
Kontext für die Priorisierung	URL, Benutzername, Zeitstempel, IP-/Land-/Gerätekontext (sofern verfügbar), Untersuchungsstatus und Kaufindikatoren zeigen.
Workflow für Gegenmaßnahmen	Workflows für Zurücksetzen/Widerrufen/Neuaufsetzen, Statusexporte, Triage-Warteschlangen, Marktkaufanfragen und Stakeholder-Berichte demonstrieren.
Automatisierung und KI-Bereitschaft	CSV-/API-Exporte, MCP-/KI-Integration und kontrollierte Weiterverwendung zeigen.
Governance und Datenschutz	Domain-Verifizierung, VIP-Einwilligung, Passwortmaskierung, in der EU betriebene Infrastruktur und tarifspezifische Grenzen erläutern.

WARUM HACKEDLIST.IO?

Umsetzbare Dark-Web-Intelligence ohne Enterprise-Reibungsverluste

HackedList.io liefert Leak-Intelligence durch Datenerfassung, -bereinigung, -anreicherung und Untersuchungs-Workflows, die Signale aus kriminellen Quellen in operative Reaktionen überführen.

- **Umfassende Abdeckung:** passive und aktive Überwachung von Hackerforen, Telegram-Kanälen, Darknet-Marktplätzen und Leak-Datensätzen.
- **Ständige Weiterentwicklung:** Neue Quellen und Erkennungslogik werden ergänzt, sobald Bedrohungsakteure ihre Art zu handeln und gestohlene Daten zu validieren ändern.
- **Umsetzbare Intelligence:** Datensätze sind so strukturiert, dass Teams Risiken validieren, den offengelegten Dienst identifizieren und den nächsten Schritt zur Behebung gehen können.
- **Zugängliche Darknet-Recherche:** Dark-Web-Intelligence wird für Führungskräfte, IT-Verantwortliche, SOC-Teams und kleinere Organisationen verständlich.
- **Erstklassige Sicherheit:** HackedList.io betreibt eigene Hardware in der Europäischen Union – in selbst kontrollierten Umgebungen, anstatt sich auf öffentliche Cloud-Anbieter zu verlassen.

Typischer Einführungspfad

Phase	Fokus	Ergebnis
1. Gefährdungsprüfung	Kern-Domains, VIP-E-Mail-Adressen und risikoreiche Dienstmuster scannen.	Erstes Risikobild und schnelle Erfolge.
2. Operative Überwachung	Wiederkehrende Berichte, Portal-Workflows und klare Reaktionsverantwortung aktivieren.	Kontinuierlicher Rhythmus aus Erkennung und Behebung.
3. Automatisierung	CSV/API, SIEM-/SOAR-/ITSM-Anreicherung und MCP-/KI-Workflows ergänzen.	Skalierbare Integration in den bestehenden Security-Stack.
4. Tiefgehende Untersuchung	Zircon oder Untersuchungsunterstützung für Hochrisikofälle und forensischen Kontext nutzen.	Vollständiges Bild für große Vorfälle und regulierte Umgebungen.

Strategischer Wert

Die Plattform schließt die Lücke zwischen externer krimineller Aktivität und internen Security Operations: Sie zeigt, wo gestohlene Zugänge existieren, was davon wahrscheinlich betroffen ist und was als Nächstes zu tun ist.

HACKEDLIST.IO



operations@hackedlist.io

Vertraut von

mafra

 RadioFreeEurope
RadioLiberty

AGROFERT

 **VEOLIA**

T-Mobile



MINISTRY
OF REGIONAL
DEVELOPMENT CZ

 **orange™**


**Charles
University**

PRUSA
RESEARCH
by JOSEF PRUSA




FIOCCHI

CSG)