LeakMAP

Open-Source Intelligence Platform

LeakMAP differs from other leak database platforms in that it correlates the relationships between leaked content by profiling and mapping the content collected in our database.

Organizations can use LeakMAP to get background information on a potential employees, to prevent any misuse of work emails and to easily search for any potential leaks. And this way organizations can prevent hackers from orchestrating sophisticated phishing campaigns or crafting convincing social engineering attacks, or worse, compromising business emails or utilizng leaks.

Overview

- Breach Tracking
- Exposed Corporate Credentials Tracking
- Prevent Credential Stuffing Attacks
- Criminal Investigation Process
- Usernames & Passwords
- Credit Cards
- Company Documents
- Photos
- Audios
- ID Cards
- Passports
- Phone Numners
- Social Media Profiles

Features:

- LeakMAP seamlessly integratess with SMARTDECEPTIVE, providing you with timely alerts regarding targeted attacks. Moreover, it integrates with DARKMAP, to automatically bolster its leaked sources.
- Correlative Functional Search (for example, retrieve the information of individuals whose identification numner starts with 43, whose registered vehicle's license plate contains AB, or whose phone numner ends with 94).
- Full text search.
- GDPR-compliant data display.

FIND ECPOSED CREDENTIALS

GATHER INTELLIGENCE

PREVENT CREDENTIAL STUFFING ATTACKS

TRACK ,BREACHES

OTD BİLİŞİM
GLOBAL VAD

LEAKMAP: MAPPING THE DARK WEB'S LEAK LANDSCAPE

TYPES OF LEAKS

TYPE OF LEAKS

- Credentials
  - Emails
  - Usernames
  - Passwords
- Financial Data
  - Credit Card Numbers
  - Bank Info
- Personal Identifiable Information
  - Phone Numbers
  - ID Cards
  - Social Security Numbers
- Corporate Documents
  - Contracts
  - Trade Secrets
  - Strategic Plans

WHY IT MATTERS

WHY PROACTIVE LEAK DETECTION MATTERS

- Immediate Threat Mitigation
  Identifying and addressing leaked information before attacks occur
- Risk Profiling and Damage Control
  Building defensive strategies based on the nature of the leak
- Corporate Data Protection
  Ensuring that internal and customer data remains secure

HOW LEAKS OCCUR

HOW LEAKS OCCUR

- Phishing Attacks
- Weak Passwords & Poor Authentication Practices
- Third-Party Vendor Breaches
- Insider Threats
- Social Engineering
- Malware & Ransomware

POTENTIAL IMPACT

POTENTIAL IMPACT ON ORGANIZATIONS

- Financial Loss
  - Fraud
  - Fines
  - Legal Fees
- Reputation Damage
  - Loss of Customer Trust
- Compliance Violations
  - GDPR
  - HIPAA
  - PCI
  - DSS
- Operational Disruptions
  - Data Corruption
  - System Downtime
- Targeted Attacks
  - Future Exploitation Through Exposed Data

PREVENTATIVE MEASURES

PREVENTATIVE MEUSURES FOR ORGANIZATIONS

- Use of Advanced OSINT Tools like LeakMAP
- Integration of Decoy Systems to Deflect Targeted Attacks
- Regular Security Audits and Vulnerability Assessments
- Encryption of Sensitive Data
- Employee Cybersecurity Training

EMERGING TRENDS IN DATA LEAKS

EMERGING TRENDS IN DATA LEAKS

- Supply Chain Attacks: Attackers are increasingly targeting third-party vendors, service providers, or contractors to gain access to the larger organizations they serve. Recent breaches have shown how a single vendor compromise can lead to widespread exposure of sensitive information, highlighting the need for companies to not only secure their own systems but also monitor their partners.

- Double Extortion Attacks: In double extortion attacks, companies are hit with two simultaneous threats: first, encrypted data that disrupts operations, and second, the exposure of stolen information if a ransom isn't paid. Attackers use industries' vulnerability to disruption to increase the pressure to pay.

- Corporate Espionage and Insider Leaks: Insider threats remain a critical concern as employees with access to sensitive data may leak information either maliciously or accidentally. With remote work on the rise, these threats are even harder to detect.

- Leak Farming by Cybercrime Gangs: Some cybercrime groups, such as the infamous Maze ransomware group, systematically target multiple organizations to collect and release sensitive data over time.

LEAKMAP: Managing Data Breaches with Precision

CatchProbe LeakMAP is the largest. continuously expanding database for identifying and analyzing leaked data. providing organizations with real-time insights and alerts. Powered by a sophisticated mapping technology and integrating with SmartDECEPTIVE decoys. it enables deep profiling and proactive defense against targeted attacks.

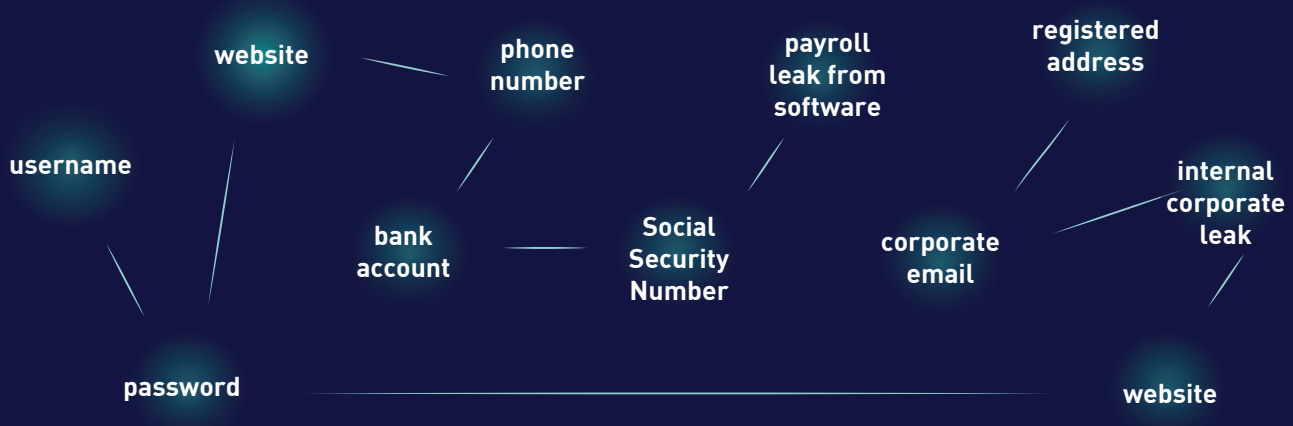
Key Differentiators

Comprehensive Leak Collection

Largest and continuously growing database of leaked credentials, financial data, PII, and corporate documents. Regular updates and expansions to ensure timely identification of newly leaked information.

Deep Profiling and Analysis

Advanced capability to correlate leaked content, enabling comprehensive profiling of leaks and potential targets.



Automated Credential Validation

LeakMAP can automatically test leaked usernames and passwords, identifying and deleting inactive or false credentials from its database, saving your team time and effort in verification while focusing on real threats.

OTD BİLİŞİM
GLOBAL VAD

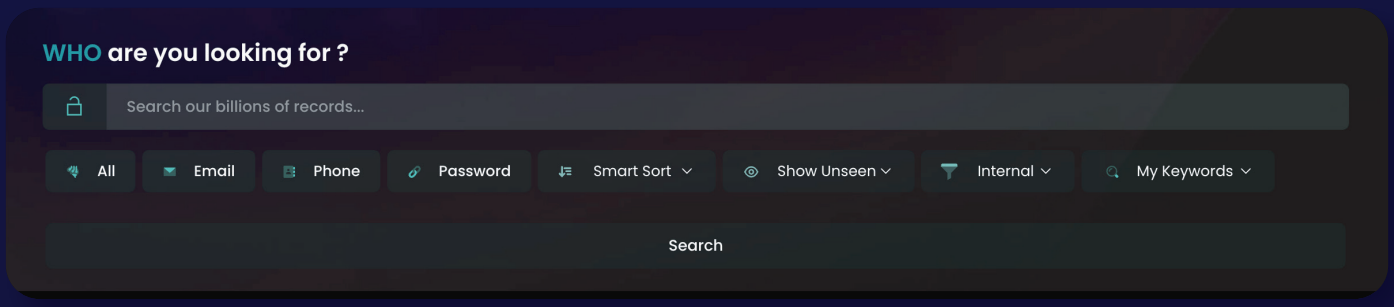
LeakMAP

Real-Time Alerts and Notifications

Besides real-time alerts, LeakMAP intelligently identities and filters out duplicate data leaks, ensuring that your organization is not alerted multiple times for the same leak, reducing unnecessary noise and response fatigue.

Easy-to-use interface with Advanced Filters

User-friendly interface with advanced filtering options, allowing you to swiftly search for specitic leaked data. Results can be filtered by date, status (seen/unseen), and domain type-whether external-facing corporate assets or internal systems and resources.



Privacy and Confidentiality Controls

Organizations can choose to mark certain tindings confidential, ensuring sensitive or strategic data is only accessible to authorized organizations or personnel.

Integration with SmartDECEPTIVE for Targeted Attack Detection

Integration with our decoy management module ensures that any attempt to use leaked data triggers an alert, giving organizations an early warning of targeted attacks.

OTD BİLİŞİM
GLOBAL VAD