

Threat Detector Platform



**Protect Your
Privacy** secure your
data!

Platform Overview	3
Platform Features	5
Dashboard	6
Tracking Threats	7
Email Breach Intelligence	8
Employees Malware Logs	10
Customers Malware Logs	12
Device Breach Tracker	13
Path Breach Detector	15
Customers Malware Logs	17
Task	19
Contact Us	21

Platform Overview

The Threat Detector platform is a comprehensive and advanced solution exclusively designed for companies and organizations to proactively detect and analyze cyber threats. It enables continuous monitoring of digital activities, offering precise analyses of leaked data and potential risks. The Threat Detector platform aims to protect sensitive information and reduce security risks through advanced technological tools, empowering organizations to strengthen digital defenses and make informed security decisions.

Platform Features

1 - Real-time Proactive Monitoring

- The platform offers continuous monitoring of digital activities to detect potential cyber threats instantly. Organizations receive immediate alerts on any suspicious activity or heightened risks, enabling them to take preventive actions at the right time.

2 - Comprehensive and Customized Leaked Data Analysis

- Threat Detector provides detailed analysis of leaked data from various sources, including confidential logs, compromised sites, and leaked databases. Analyses can be customized to align with the organization's specific needs, focusing on data type and risk nature.

3 - Customizable Reporting Interface

- The platform offers flexible, customizable reports, allowing organizations to create detailed reports on threats and risks tailored to their requirements. These reports include clear summaries and recommendations to enhance cybersecurity measures.

Platform Features

4 - Easy Integration and Security Management

- The platform integrates seamlessly with existing security systems within organizations, offering centralized security management tools. This enables organizations to track vulnerabilities and manage threats through a single, user-friendly interface.

5 - Advanced Sector-specific Analysis

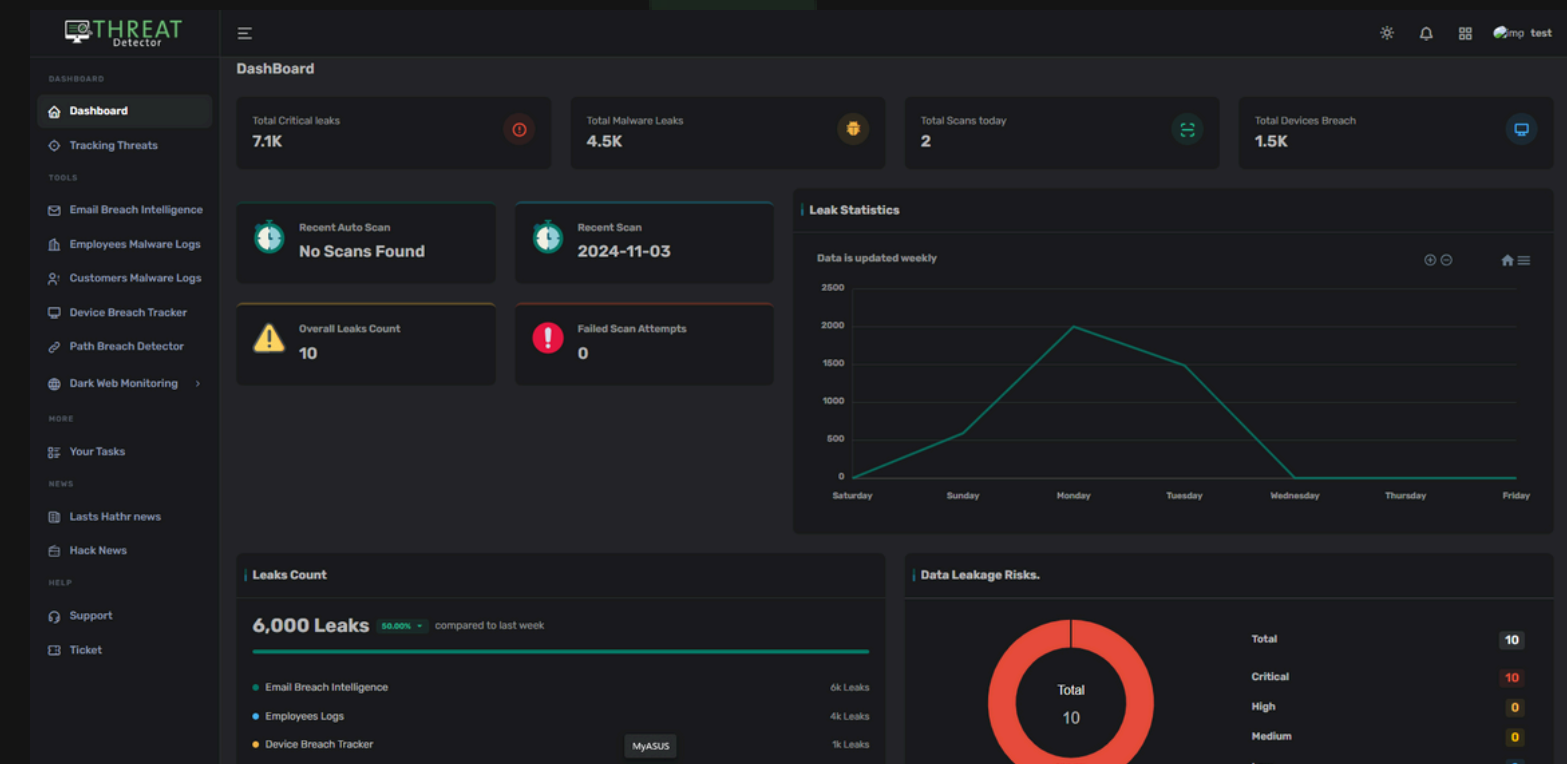
- The Threat Detector platform provides tailored analyses for various industries, including financial, healthcare, and retail sectors, helping organizations understand common threats in their field and take necessary precautions to safeguard data.

6 - Continuous Support and Innovative Security Solutions

- Users benefit from ongoing technical support by a specialized cybersecurity team, along with advanced solutions to counter evolving threats. The platform is regularly updated to stay ahead of new challenges in cybersecurity.

Dashboard

The Dashboard section is designed to provide an overview of key statistics and metrics across all sections of the system. It offers a comprehensive summary that helps users quickly understand the current state of various activities and data within the platform. For example, users can view the total number of data breaches detected, the number of alerts generated, and other critical information related to security incidents and system performance. This section is essential for monitoring the overall security posture, enabling users to identify trends, spot potential issues, and make informed decisions based on real-time data.

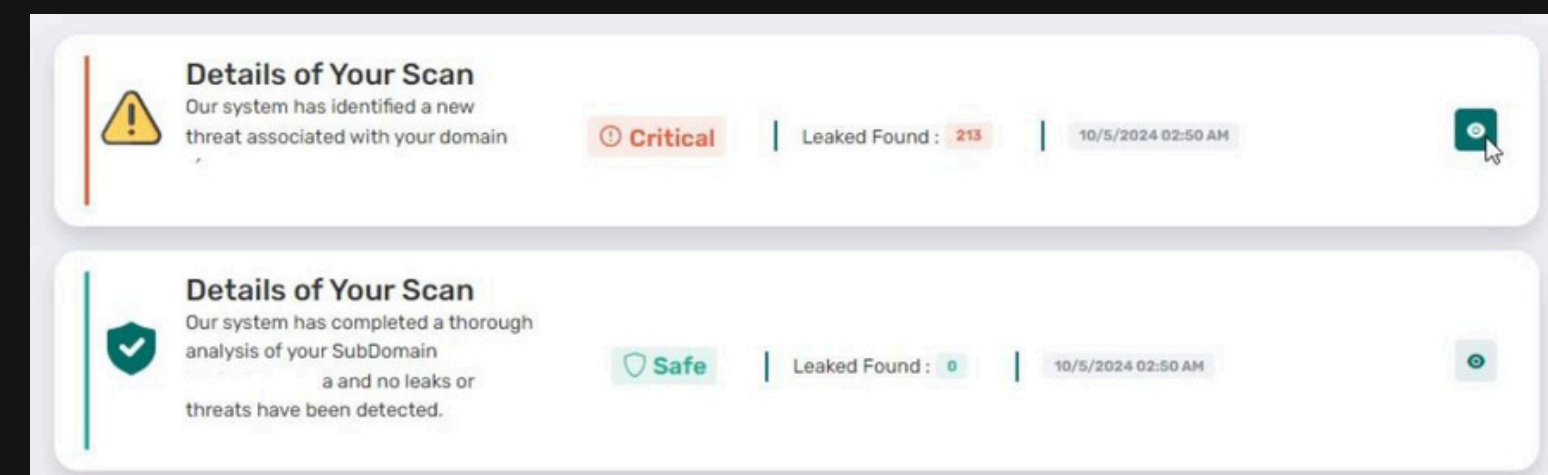
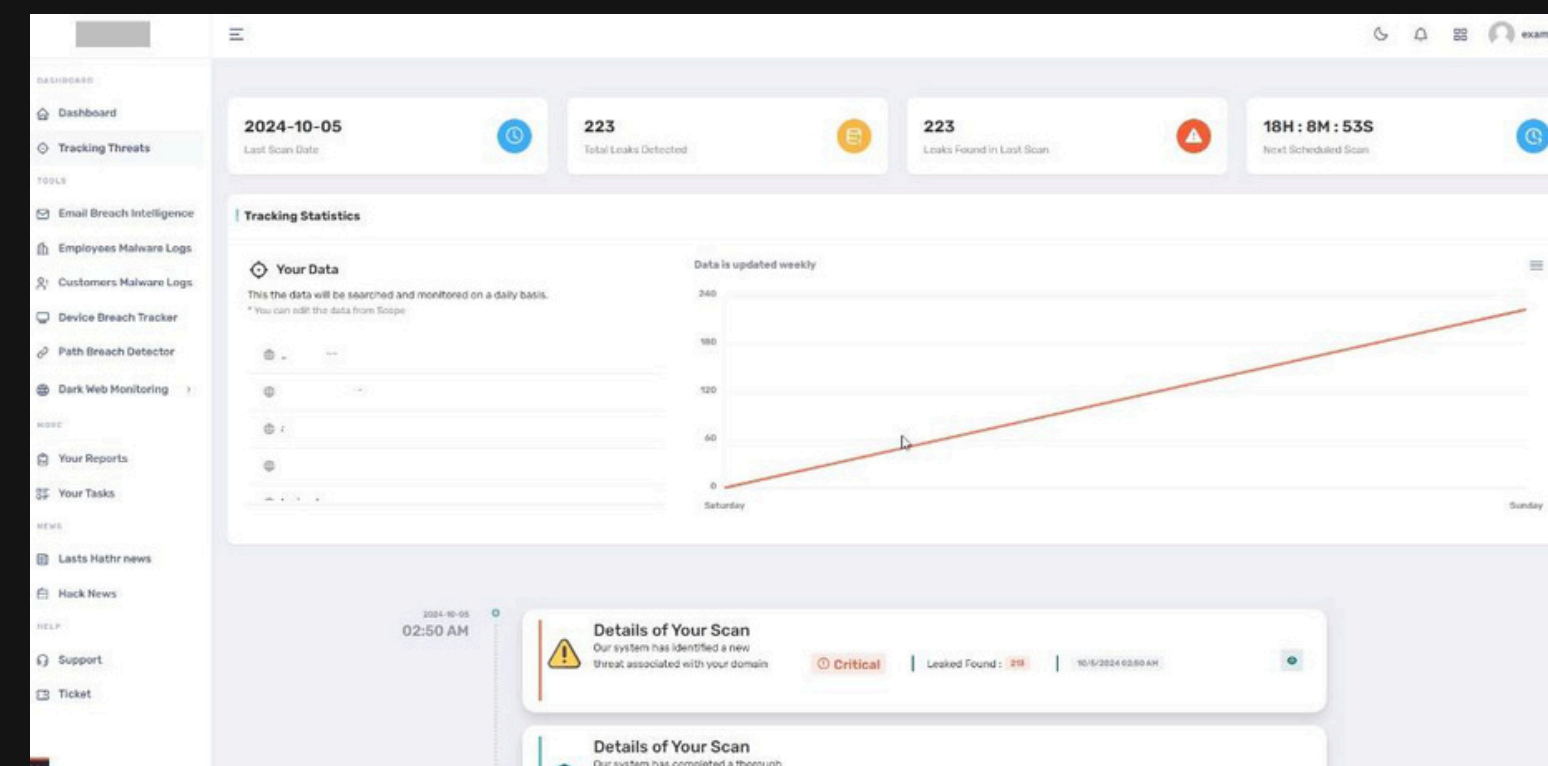
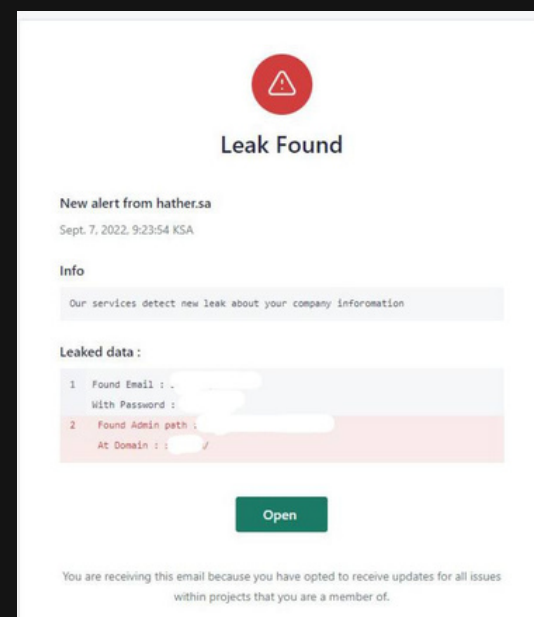


Tracking Threats

This section is dedicated to tracking the company's emails or IP addresses. When any new data leak occurs, an immediate and urgent alert is issued. The section includes the following tasks:

- Monitoring the company's emails and IP addresses.
- Detecting new data leaks as soon as they occur.
- Issuing immediate and urgent alerts to the relevant departments within the company about new leaks.
- Providing detailed reports on the discovered incidents.

This section aims to enhance the company's immediate protection by continuously monitoring for new leaks and issuing necessary alerts for prompt action.

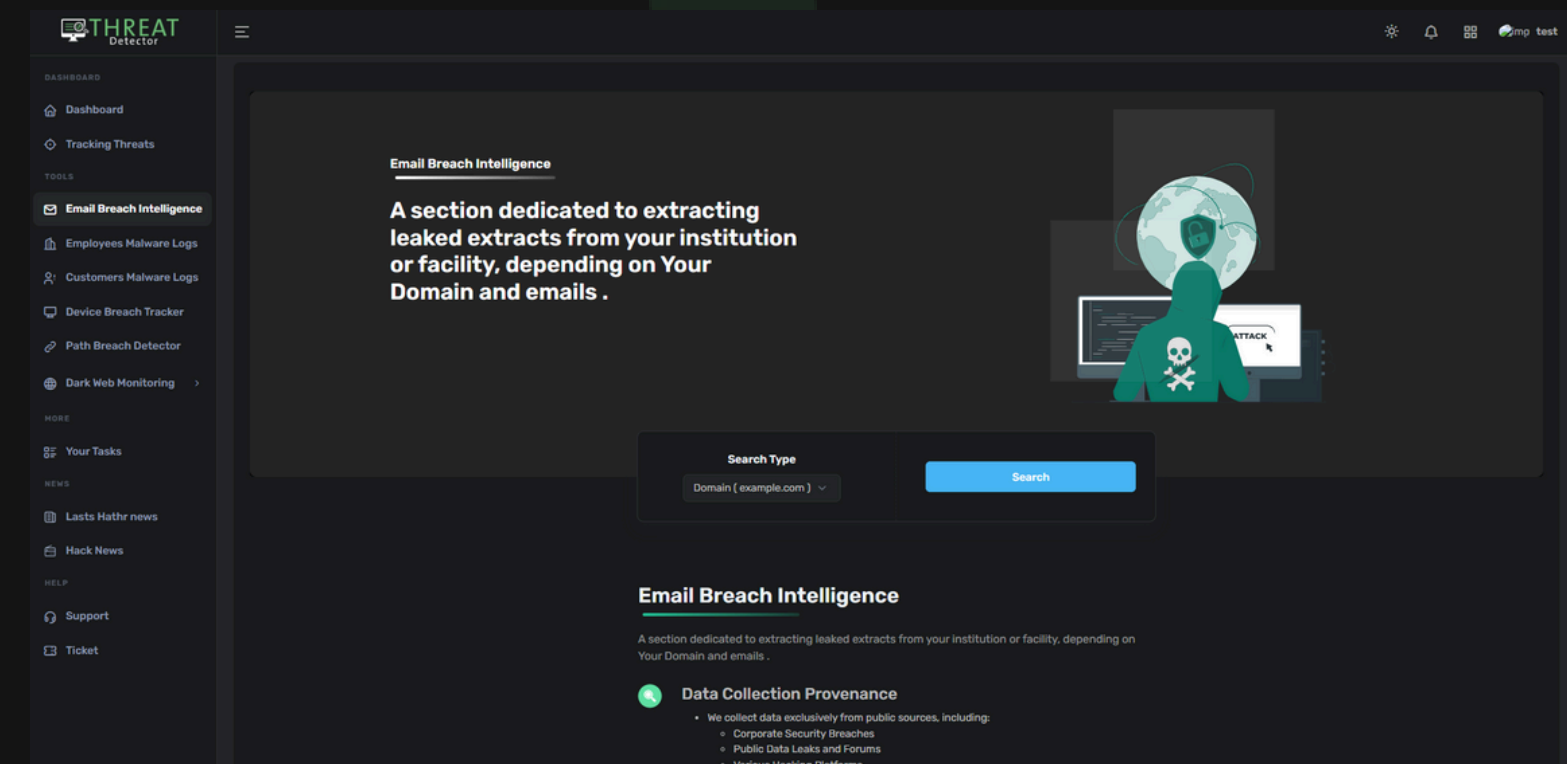


Email Breach Intelligence

This section specializes in extracting leaked data for companies based on the type of breach. It gathers information related to

- Email Address
- Passwords
- Cookies
- Other details such as phone numbers and country, among others.

The section aims to provide detailed and accurate analysis of leaked data to enhance companies' cybersecurity and improve strategies for preventing future breaches.



Email Breach Intelligence

The screenshot displays the THREAT Detector interface. The main section, 'Your Task info', shows the 'Result of scanning the domain example.com' with an overall risk level of 'Critical' (7.2k). It breaks down the risk into four categories: Critical Risk (7.2k), High Risk (3.4k), Medium Risk (2k), and Low Risk (1.7k). Below this, a 'Leaked Information #0' section provides a 'Leaked Description' and 'Leaked From' details (school.mos.ru). A 'Social Media Platforms' donut chart shows 397 leaks from Twitter, with other platforms like LinkedIn, Facebook, and GitHub also represented. The 'Scan Statistics' section shows 7250 logs, 14350 data leaks, and 14000 emails found. A 'More Info About The Leaked Passwords' table lists various passwords with their strengths and crack times. A 'More Info About The Emails' table lists specific email addresses and domains.

Strength	Attempts Needed	Complexity	Crack Time (N/A)	Crack Time (Slow Offline)
Very Weak	6398.8 billion Times	Very Low	centuries	20 years
Weak	10.0 million Times	Low	12 days	17 minutes
Good	12 Times	Medium	1 second	less than a second
Good	2 Times	Low	less than a second	less than a second
Good	2 Times	Low	less than a second	less than a second
Good	227 Times	Low	23 seconds	less than a second
Weak	100.0 million Times	Very Low	4 months	3 hours
Average	93.2 thousand Times	Low	3 hours	7 seconds

ID	Email	Domain	Action
0	marshenkodo@example.com	example.com	Get Info
1	me@example.com	example.com	Get Info
2	me@example.com	example.com	Get Info
3	me@example.com	example.com	Get Info
4	me@example.com	example.com	Get Info
5	me@example.com	example.com	Get Info
6	me@example.com	example.com	Get Info
7	me@example.com	example.com	Get Info

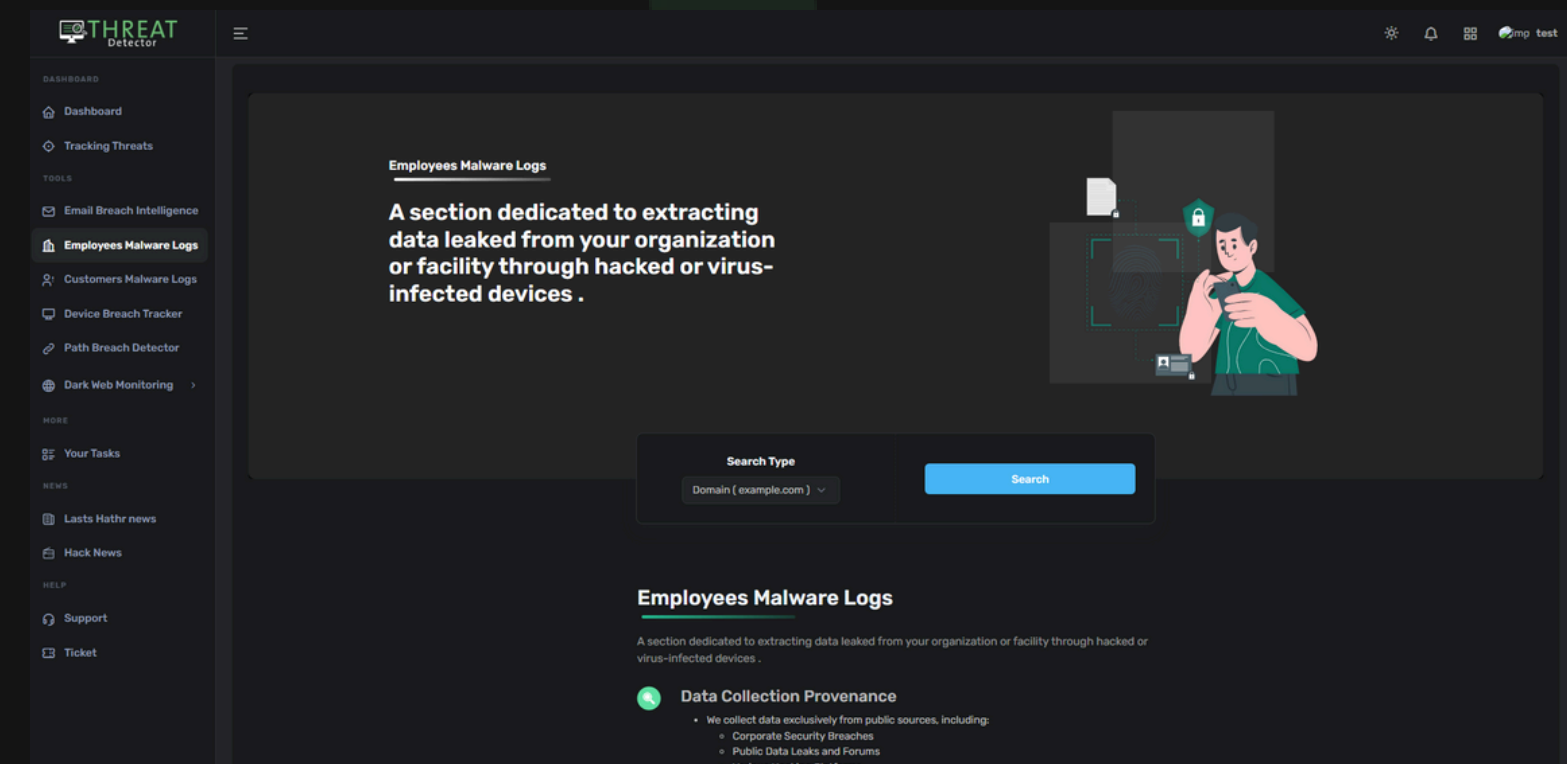
The section aims to provide detailed and accurate analysis of leaked data to enhance companies' cybersecurity and improve strategies for preventing future breaches.

Employees Malware Logs

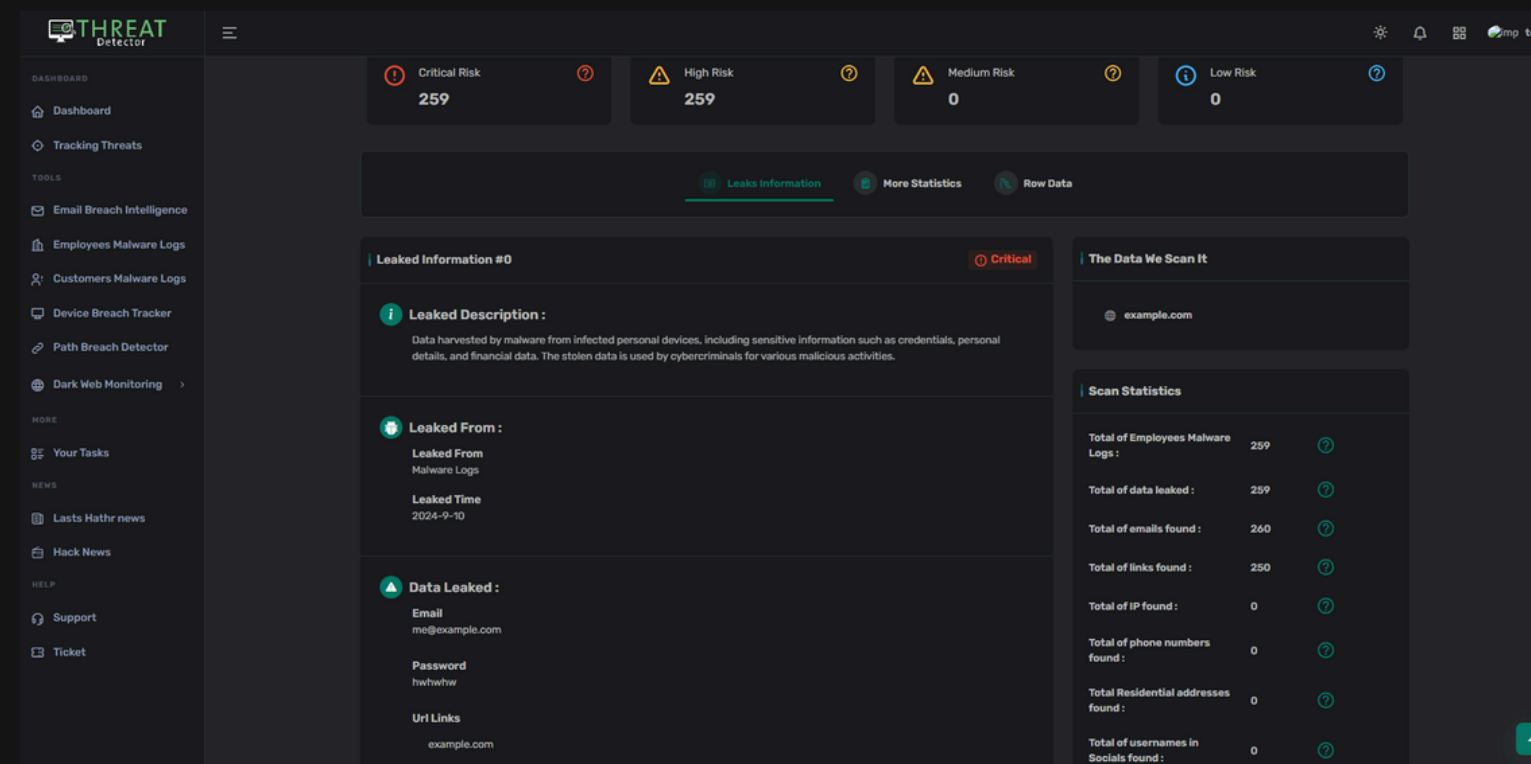
This section specializes in extracting data from employees affected by malware. It offers the following services

- Collecting and Documenting Incidents: Detailed recording of email and credential compromise incidents related to malware.
- Analyzing Compromised Data: Conducting in-depth analysis of data extracted from compromised employee devices.
- Comprehensive Reporting: Providing detailed reports on breaches and compromised credentials.
- Categorizing Breach Information: Organizing data by breach type, source, and affected employee.

The aim of this section is to provide clear insights into malware-related incidents, helping organizations strengthen their defenses and protect sensitive employee information.



Employees Malware Logs



Employees Malware Logs

A section dedicated to extracting data leaked from your organization or facility through hacked or virus-infected devices .

- Data Collection Provenance**

 - We collect data exclusively from public sources, including:
 - Corporate Security Breaches
 - Public Data Leaks and Forums
 - Various Hacking Platforms
- Data Search and Utilization**

 - You can search about your information, including:
 - Email Addresses
 - Main Domain
- Expected outputs and results**

 - The data cannot be uniform in the output, but the following data is monitored.
 - Email Address
 - Password
 - Origin links as domains and host ip

This section provides essential advice and guidelines for securing your accounts and data, along with detailed statistics to help you understand potential threats. We offer recommendations to enhance the protection of your information, including guidance on changing passwords and setting up multi-factor authentication. Additionally, the section includes statistical data showing the percentage of incidents related to malware logs, supporting you in making informed decisions to strengthen your company's security.


Advice

Theft Logs Leak Discovered in Your Company We would like to inform you that after thorough investigations, a theft logs leak has been discovered within your company. This leak includes sensitive information such as usernames, passwords, and email addresses belonging to your clients or employees. Such data may be at risk of exploitation by unauthorized parties, posing a threat to information security and individual privacy.

Advice

We have detected password leaks associated with your accounts. Immediate action is required to protect your security. We strongly recommend changing your passwords and reviewing your account security settings to address these vulnerabilities. Additionally, consider enabling multi-factor authentication for enhanced protection.

Leaked Statistics



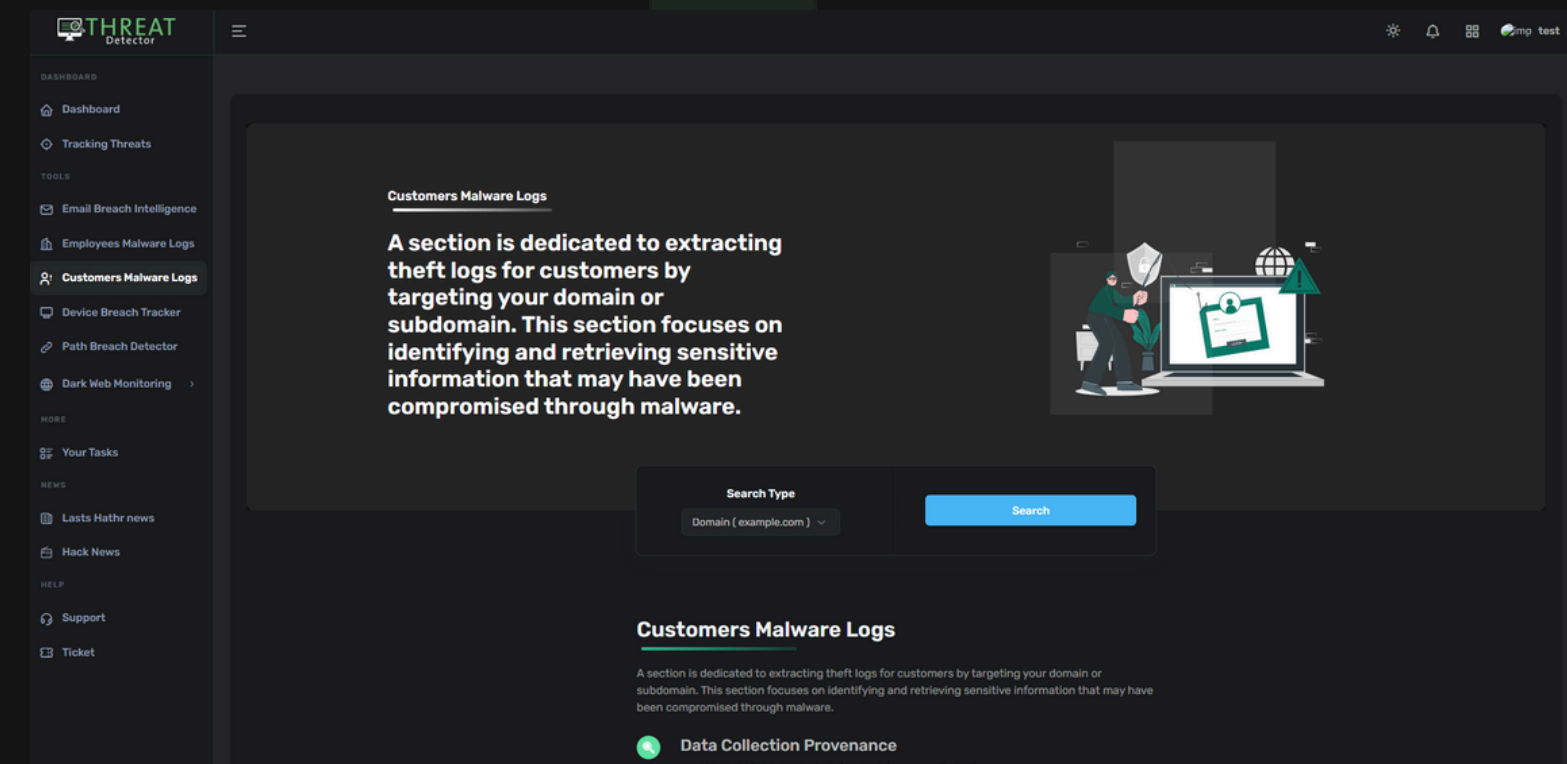
● Malware Logs

Customers Malware Logs

This section focuses on identifying and analyzing data from customers affected by malware. It includes:

- **Incident Documentation:** Recording detailed cases of malware-related data compromises involving customers.
- **Data Analysis:** Conducting in-depth analysis of compromised data to understand the extent of the breach and potential impacts on customers.
- **Comprehensive Reporting:** Providing detailed reports on discovered breaches, including recommendations for risk mitigation.
- **Data Categorization:** Organizing compromised data by breach type, source, and affected customer details.

The goal of this section is to provide insights into customer-focused malware incidents, assisting organizations in safeguarding their clients' sensitive information and enhancing overall security measures.

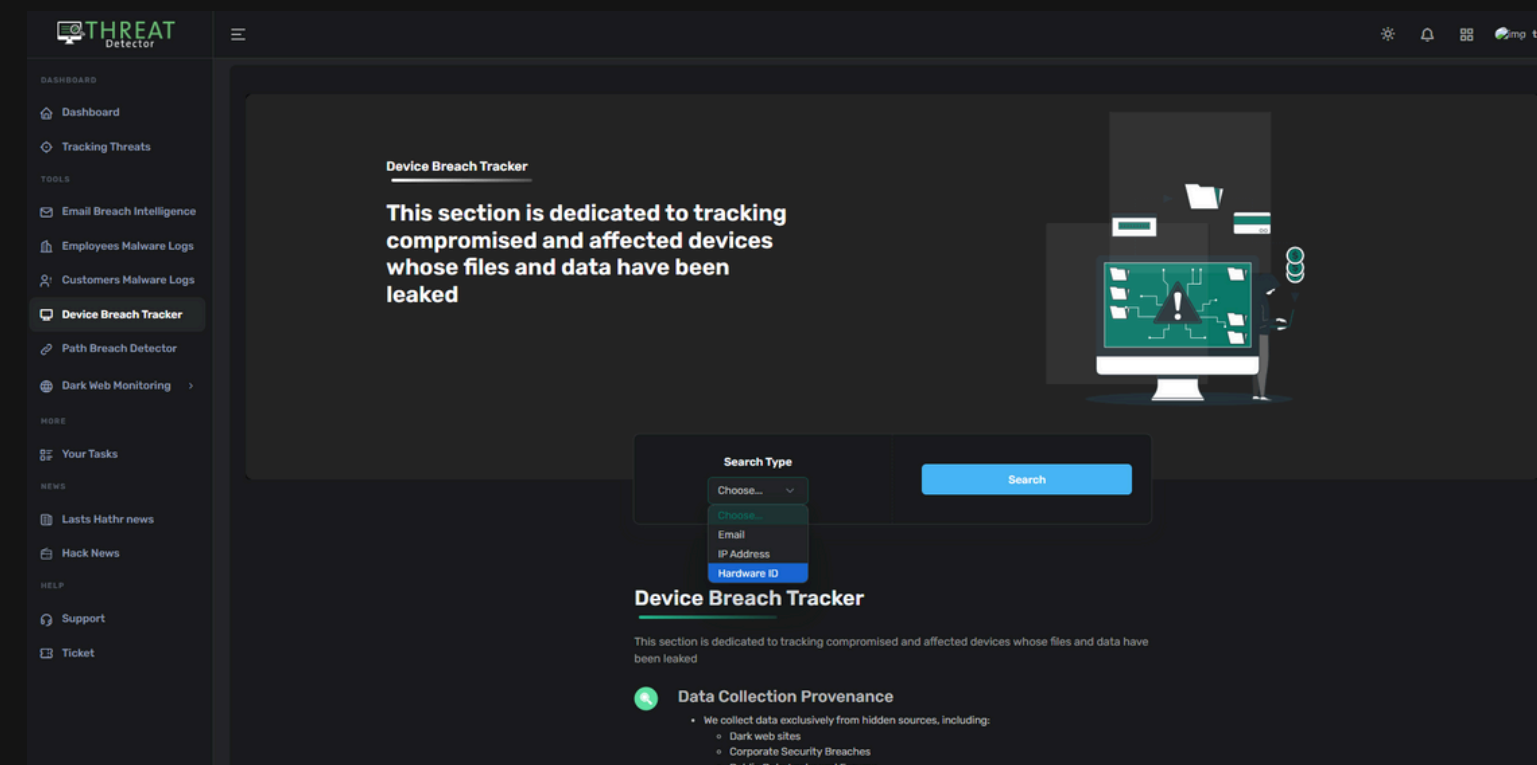


Device Breach Tracker

This section is dedicated to tracking compromised and affected devices impacted by stealer logs, where files and data have been leaked. It provides a detailed analysis, including:

- **Compromised Device Name:** Identifying the name of each affected device.
- **Device IP Address:** Recording the IP address associated with the compromised device.
- **Device HWID:** Documenting the unique hardware ID (HWID) of the device.
- **Extracted Files:** Listing files extracted from the device, along with the path for each leaked file.
- **Affected Files Display:** Showing details of the files impacted by the breach.
- **Breach Date:** Indicating the date when the device was compromised.

The section aims to provide comprehensive and precise information on device breach incidents related to stealer logs, supporting investigations and enhancing security measures.



Device Breach Tracker

```

REDLINE
Telegram: https://t.me/REDLIN[REDACTED]

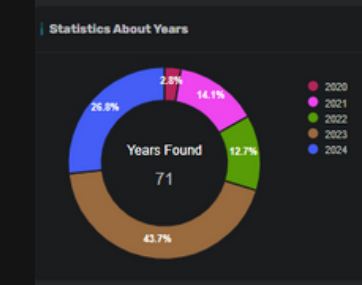
URL: android://wctkUkAl[REDACTED]AbZVxmFvWkN8yHs6TuGuEfxswkThq5qxOWi0
RFB155t1j2td7DaRC_cF8R3q1UQ--@com.waze/
Username: Chri[REDACTED]
Password: ql[REDACTED]
Application: Google_[Chrome]_Default

URL: android://pBoWdSL[REDACTED]rcr9vsiPPHGed3xcXJ5ZJccRGvbP7pPFSq
eQ8IHooDFe29iIwzU_fETWE2UpQ--@com.linkedin.android/
Username: chri[REDACTED]
Password: chr[REDACTED]
Application: Google_[Chrome]_Default

URL: https://login.live.com/login.srf
Username: chr[REDACTED]
Password: chr[REDACTED]
Application: Google_[Chrome]_Default

URL: https://accounts.google.com/signin/v2/s1/pwd
Username: chr[REDACTED]
Password: chr[REDACTED]
Application: Google_[Chrome]_Default

URL: https://www.niagara-community.com/_ui/system/security/ChangePassword
Username: U[REDACTED]
Password: B[REDACTED]
Application: Google_[Chrome]_Default
    
```



This section is designed to extract all leaked data from compromised devices. It provides comprehensive details, including:

- **Leaked File Paths and Affected Data:** Lists all the files and data affected by the breach, with the exact path for each leaked file.
- **Device Access Date:** Indicates the date when the device was accessed.
- **Compromised Device Information:** Provides detailed information about the device that was compromised.
- **Infected File Path:** Shows the path to the infected file that led to the compromise.

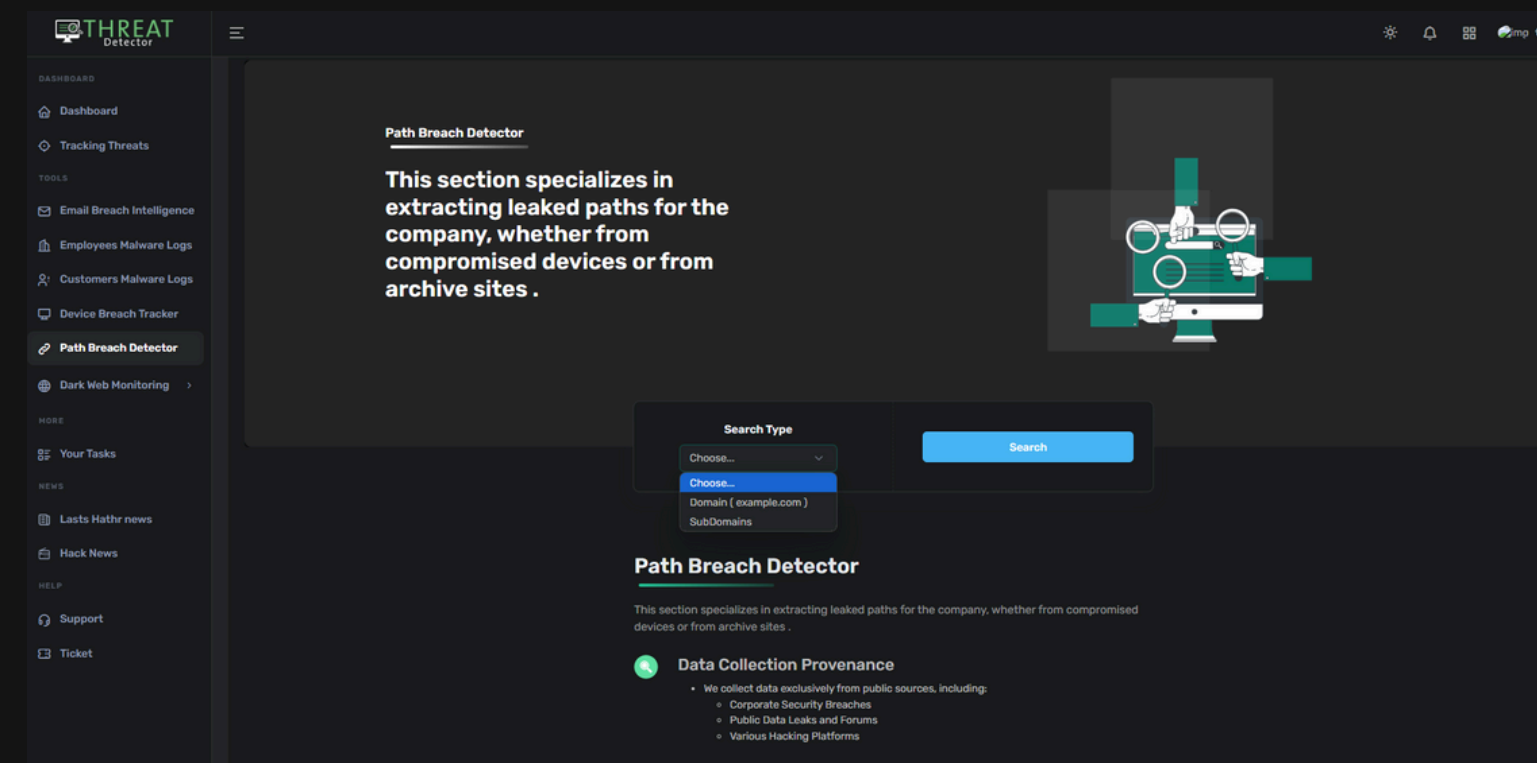
The importance of this section lies in its ability to deliver accurate and exhaustive insights into device breaches. By documenting all aspects of the compromised data, this section supports thorough investigations and enables the organization to take targeted actions to protect against similar breaches in the future.

Path Breach Detector

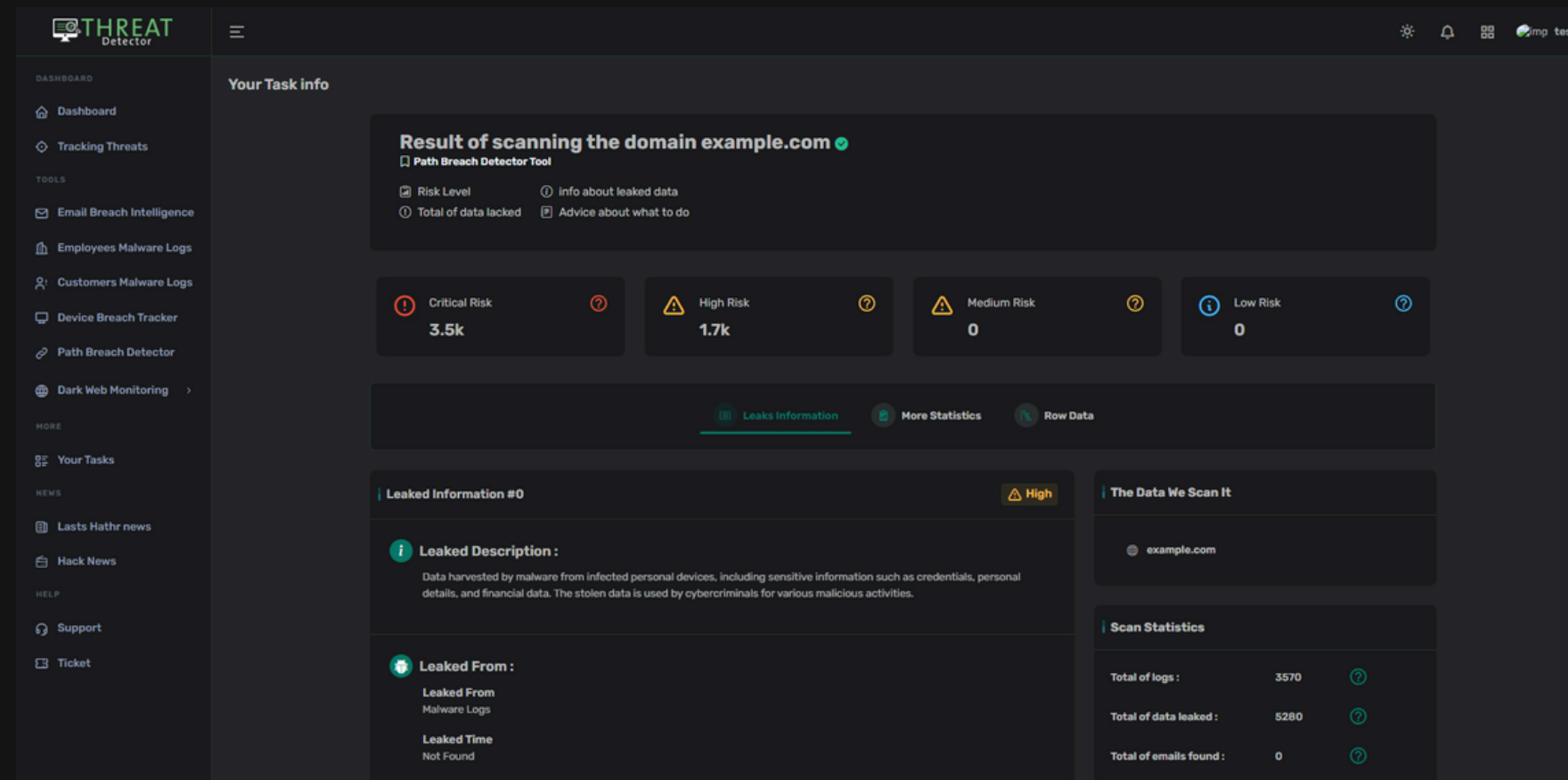
This section specializes in identifying and extracting all leaked paths related to the company, whether they stem from compromised devices, archive sites, or WHOIS records. The section's activities include:

- **Collection and Documentation:** Gathering and thoroughly documenting all leaked paths associated with the company's domains, subdomains, or IP addresses.
- **Path Analysis:** Analyzing each path to identify its source and intended target.
- **Detailed Reporting:** Providing a comprehensive list of compromised paths, including sensitive information such as usernames, passwords, and any other critical data contained within the leaks.

The purpose of this section is to offer companies a full overview of their leaked paths, allowing them to strengthen their digital security measures and develop effective preventive strategies against future leaks.



Path Breach Detector



THREAT Detector

Your Task info

Result of scanning the domain example.com

Path Breach Detector Tool

- Risk Level
- Total of data leaked
- Info about leaked data
- Advice about what to do

Critical Risk: 3.5k
High Risk: 1.7k
Medium Risk: 0
Low Risk: 0

[Leaks Information](#)
[More Statistics](#)
[Row Data](#)

Leaked Information #0 High

Leaked Description :
Data harvested by malware from infected personal devices, including sensitive information such as credentials, personal details, and financial data. The stolen data is used by cybercriminals for various malicious activities.

Leaked From :
Leaked From: Malware Logs
Leaked Time: Not Found

The Data We Scan It
example.com

Scan Statistics

Total of logs :	3570
Total of data leaked :	5280
Total of emails found :	0

Leaked Information #126 High

Leaked Description :
Data harvested by malware from infected personal devices, including sensitive information such as credentials, personal details, and financial data. The stolen data is used by cybercriminals for various malicious activities.

Leaked From :
Leaked From: Malware Logs
Leaked Time: Not Found

Data Leaked :
Link: <http://example.com/my-login>

Leaked Information #29 Critical

Leaked Description :
Data harvested by malware from infected personal devices, including sensitive information such as credentials, personal details, and financial data. The stolen data is used by cybercriminals for various malicious activities.

Leaked From :
Leaked From: Malware Logs
Leaked Time: Not Found

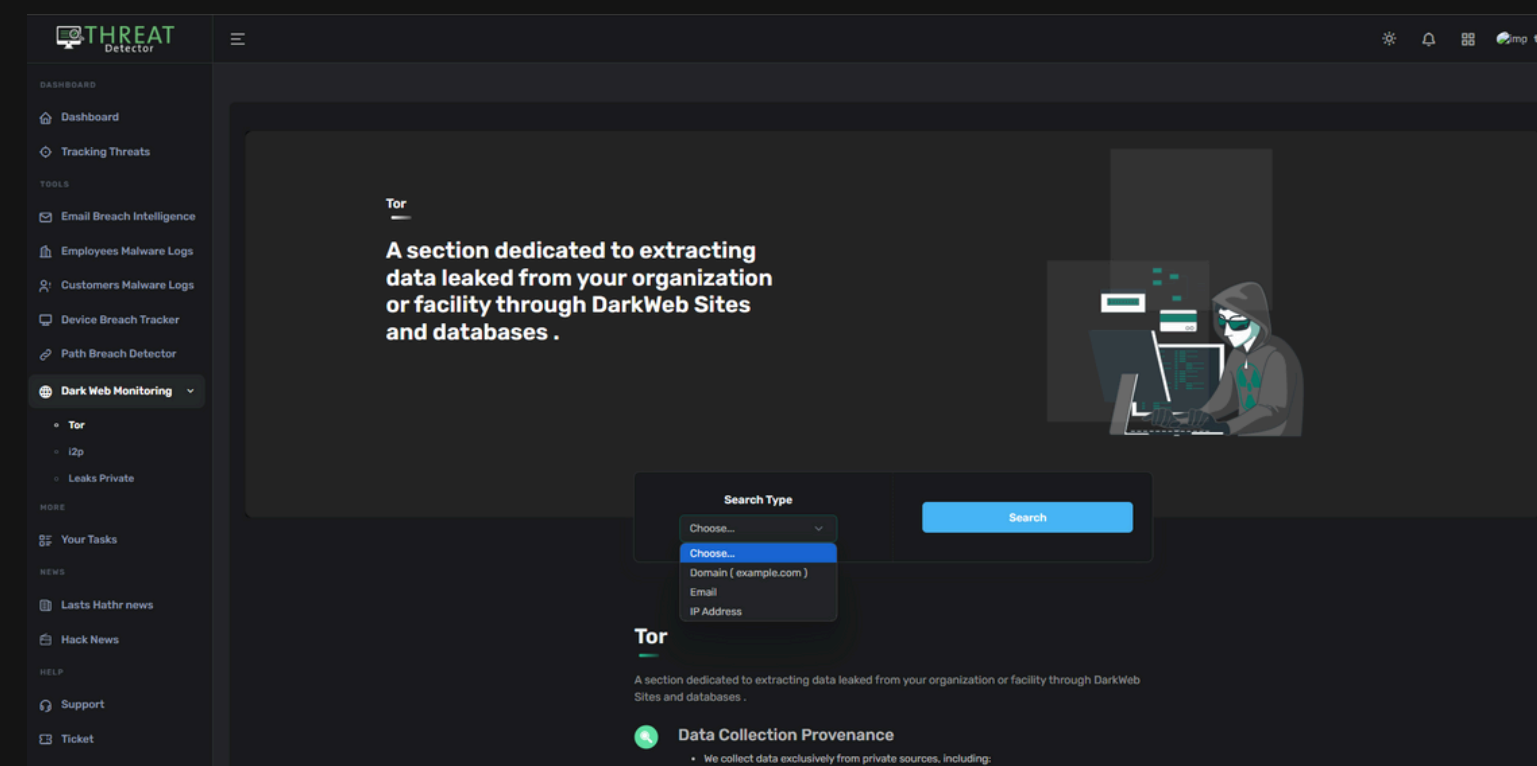
Data Leaked :
Link: <http://example.com/admin/admin/index/index/key/ad9cd4bd6cf3328febe38bcb53e651af7617bc781f774c09082798a086876843admin:admin1234>

The purpose of this section is to offer companies a full overview of their leaked paths, allowing them to strengthen their digital security measures and develop effective preventive strategies against future leaks.

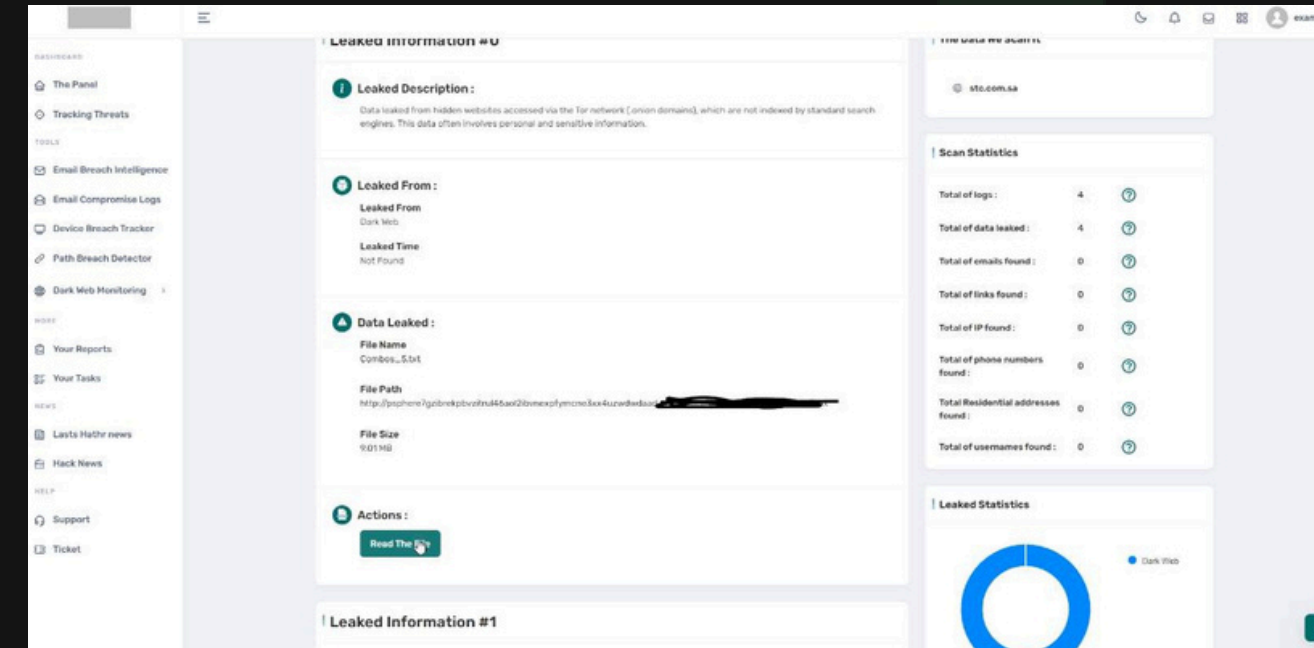
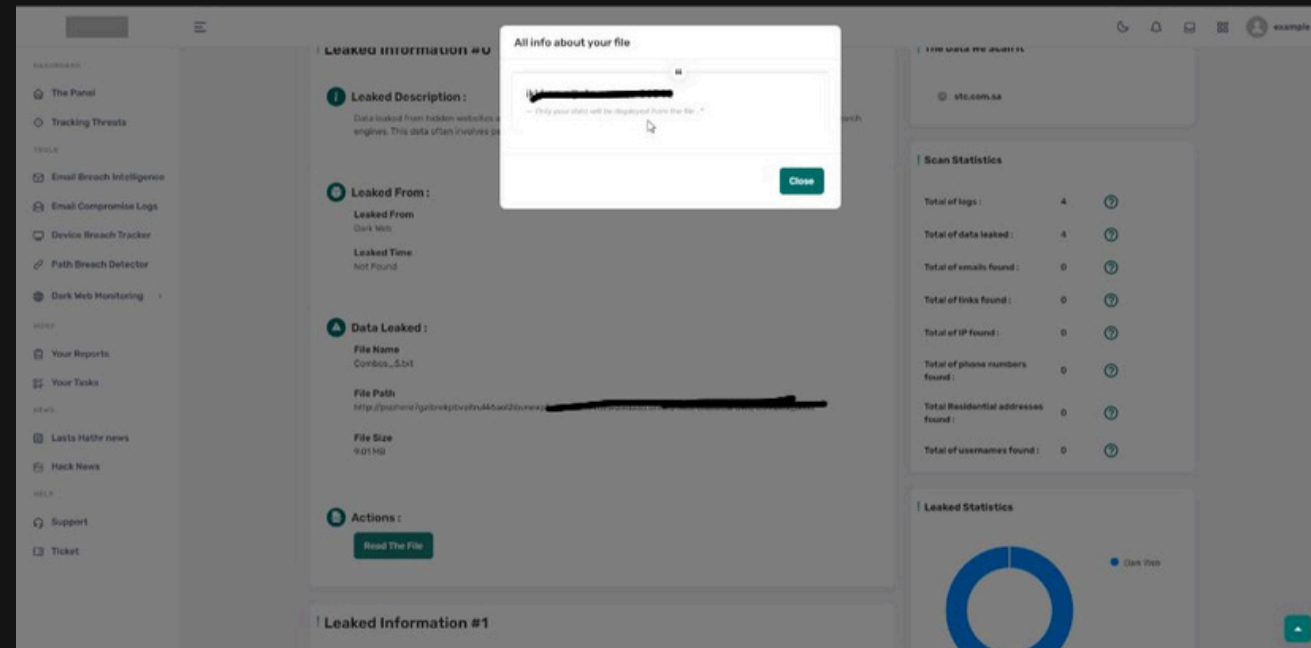
Dark Web Monitoring

This section is dedicated to extracting leaked data from all branches of the dark web, including

- Tor : Focuses on tracking and extracting leaked data from the Tor network within the dark web.
- I2P : Monitors and extracts leaked data from the I2P network.
- Leaks Private : Specializes in monitoring and extracting private data from the dark web, including stealer logs, text files, and other sensitive data from hacker sites, forums, Telegram channels, Discord servers, and other platforms.

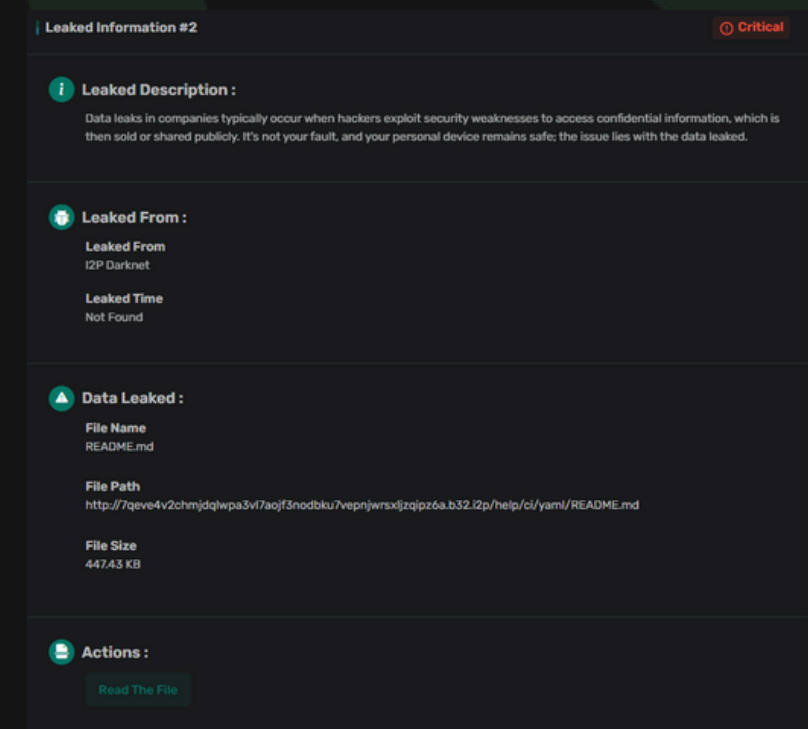
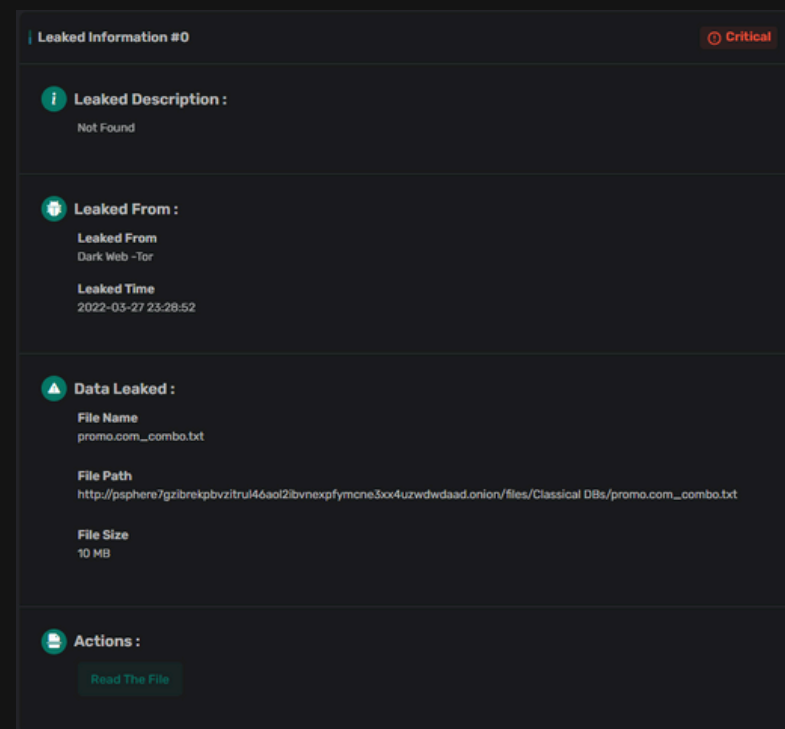


Dark Web Monitoring



Key Tasks of the Section

- Continuous monitoring of activities across all branches of the dark web (Tor, I2P, and Leaks Private).
- Extracting leaked data, identifying leak sources, and analyzing the details of compromised data.
- Providing comprehensive reports on leaked data and potential sources, helping companies take preventive actions and protect their sensitive information.



Tasks

The Tasks section of the Cyber Sentinel Dashboard is a comprehensive repository of detailed reports from all sections within the dashboard. This section includes

1 Risk Analysis

An assessment of the risks associated with each section.

2 Leak Statistics

The number of leaks recorded in each section.

3 Potential Risks


Identification and evaluation of potential risks to the company.

4 Mitigation Strategies

Recommendations and strategies for dealing with the leaks and mitigating their impact on the company.

This section is essential for maintaining an overview of the company's cybersecurity posture and ensuring that all potential threats are systematically addressed.

Tasks



DASHBOARD

- Dashboard
- Tracking Threats

TOOLS

- Email Breach Intelligence
- Employees Malware Logs
- Customers Malware Logs
- Device Breach Tracker
- Path Breach Detector
- Dark Web Monitoring

MORE

- Your Tasks**

NEWS

- Lasts Hathr news
- Hack News

HELP

- Support
- Ticket

☰
⚙️ 🔔 🗄️ imp test

Your Tasks

Total of tasks
14

Critical Leaks
9

High Leaks
3

Total of completed tasks
14


Medium Leaks
2

Low Leaks
0

Total of pending tasks
0

Total of error tasks
0

Total Number of Leaks Found
15.1K



Track your Scans from here

All Tasks History

🗄️
All sections are here

✉️
Email Breach Intelligence

🏢
Employees Malware Logs

🖥️
Device Breach Tracker

🔗
Path Breach Detector

🌐
Tor

🌐
i2p

👤
Customers Malware Logs

🔒
Leaks Private


ID.	Scan Tool	Search For	Risk Level	Total Data Found	Total leaked Found	Status	Created At	Actions
470	Employees Malware Logs	example.com	Critical	3200	+ 3200	Completed	2024-11-03 21:09:32	👁️ 🗑️
469	Email Breach Intelligence	example.com	Critical	10433	+ 10433	Completed	2024-11-03 19:47:36	👁️ 🗑️
468	Device Breach Tracker	example.com	Critical	270	+ 270	Completed	2024-11-03 19:32:41	👁️ 🗑️

Platform Hathr

Your Security Choice in Your Digital World



Contact us:

 29th floor, Al-Alya Towers, Tower B
intersection of Al Tahlia and Alya St
Riyadh, KSA

 www.hathr.sa  +966 552 300 849
 info@hathr.sa  +966 112 978 246

 [hathr_sa](#)
 [hathrr_sa](#)

 Home