BITSIGHT

WHITE PAPER

Identity Intelligence & Credentials Module

Detecting identity and credential compromises to understand priority leaks and triage risks for improved credential security management.

Challenge

Compromised credentials pose a significant threat to organizations as they can be used to impersonate users, escalate privileges, and carry out malicious activities such as data theft, fraud, or sabotage.

Organizations must be vigilant to understand and manage the access security of users in the face of rising credential and identity compromise. Identifying compromised credentials as quickly and early as possible empowers security teams to take preemptive measures to ensure organizational safety and integrity.

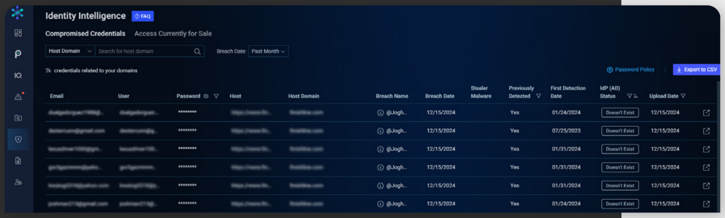
Unfortunately, the odds are against you as threat actors implement phishing and brute force tactics at scale to gain account access. Without identity and credential intelligence solutions, it can be near impossible to detect if a credential has been compromised and take action before disaster strikes.

Agenda

- Challenge
- Solution
- Use Cases
- Getting Started

Bitsight tracks over a billion credential appearances shared weekly across underground forums.

View of the Identity Intelligence module



Identity Intelligence

Compromised Credentials | Access Currently for Sale

Host Domain | Search for host domain | Breach Date: Past Month

2k credentials related to your domains

Email	User	Password	Host	Host Domain	Breach Name	Breach Date	Stealer Malware	Previously Detected	First Detection Date	IdP (AD) Status	Upload Date
[redacted]	[redacted]	********	[redacted]	[redacted]	@Jogh...	12/15/2024		Yes	01/24/2024	Doesn't Exist	12/15/2024
[redacted]	[redacted]	********	[redacted]	[redacted]	@Jogh...	12/15/2024		Yes	07/25/2023	Doesn't Exist	12/15/2024
[redacted]	[redacted]	********	[redacted]	[redacted]	@Jogh...	12/15/2024		Yes	01/31/2024	Doesn't Exist	12/15/2024
[redacted]	[redacted]	********	[redacted]	[redacted]	@Jogh...	12/15/2024		Yes	01/31/2024	Doesn't Exist	12/15/2024
[redacted]	[redacted]	********	[redacted]	[redacted]	@Jogh...	12/15/2024		Yes	01/31/2024	Doesn't Exist	12/15/2024
[redacted]	[redacted]	********	[redacted]	[redacted]	@Jogh...	12/15/2024		Yes	01/24/2024	Doesn't Exist	12/15/2024

Be the first to spot compromised credentials. Secure your assets. Protect your team.

Solution

Bitsight's Identity Intelligence Module helps you discover and manage compromised identity credentials, providing prioritization capabilities to help you safeguard priority assets and proactively remediate threats as they surface. From the onset of activation, the module provides immediate data on compromised accounts and continuously monitors organizational domains across the cybercriminal underground in real-time.

The module allows organizations to view the most updated information related to compromised credentials. It also informs you when malware has access to your domain and is for sale on the underground market, giving you an option to connect with Bitsight to purchase the access.

With Bitsight's Identity Intelligence module, you have access to the most pressing compromised credential information, optimally positioning you to take immediate action.

Use Cases

Primary use cases for the Identity Intelligence module include:

Early Detection of Compromised Credentials

Monitor underground sources to identify leaked or stolen credentials.

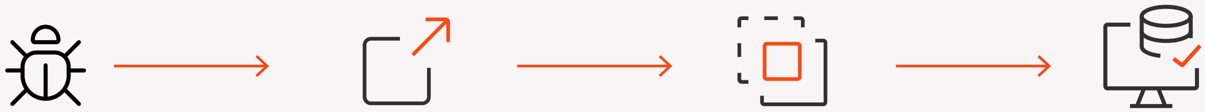
Incident Response to Known Breaches

Investigate identified breaches, assess risk and scope of breach, and respond before attackers can exploit the credentials.

Compliance and Risk Mitigation

Analysts can help support the upkeep of regulatory compliance standards by regularly checking for credential exposures to better protect sensitive customer and employee data.

COMPROMISED CREDENTIALS



COLLECTION
Bitsight gathers and classifies files as potential credential data.

PARSING
Our processor extracts emails, passwords, usernames, URLs, and more.

ASSET MATCHING
Extracted data is then matched with client assets.

DATABASE
Bitsight adds 1 billion compromised credentials weekly to its database.

Benefits

- Reduce the risk of unauthorized access to sensitive organizational information.
- Enhance security posture by quickly and efficiently addressing credential leaks.
- View and manage all credential exposure data from one module.

Features

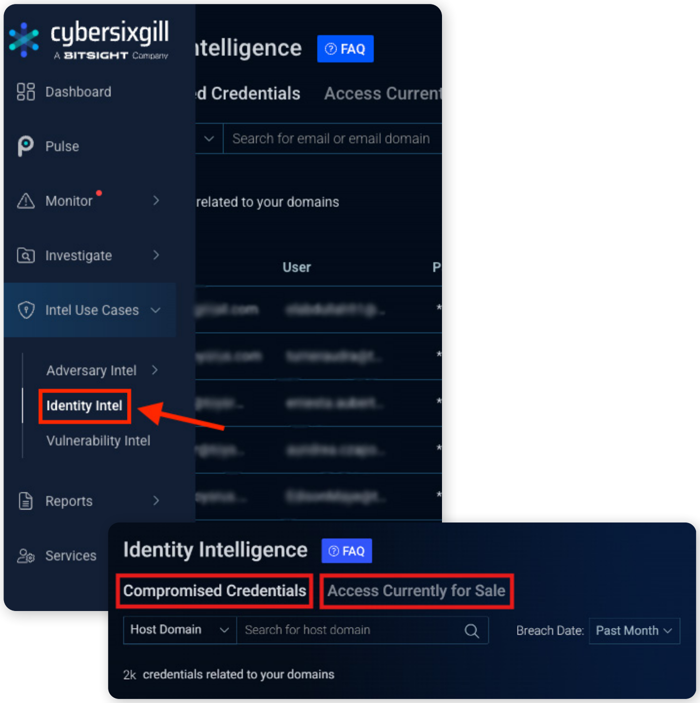
- View most updated compromised identity credentials for your domains.
- Advanced filtering capabilities, including identity provider integrations and password policies, enable precise credential leak detection.
- Capability to assign prioritization criteria for compromised credentials according to organizational needs.
- Access credential information, including Breach and Endpoint data collected by stealer malware (infostealers), for organizational risk analysis.
- Customizable alert setup according to organizational preferences.

Getting Started

Hover over the left-sided Navigation pane to reveal the Exposure tab and select the Identity Intelligence module.

Once the Module is open, there are two selectable viewing tabs at the top: Compromised Credentials and Access Currently for Sale.

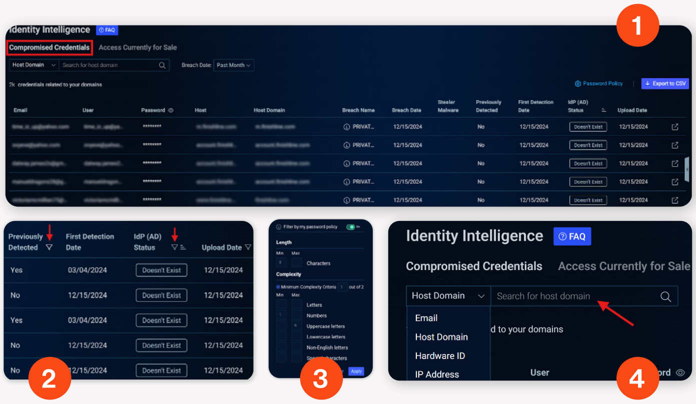
- **Compromised Credentials:**
  Identifies compromised credentials that are leaked or exposed.
- **Access Currently for Sale**
  Highlights access currently being sold across the underground and allows you to prevent compromises by "taking down" access to your systems.



Compromised Credentials

The Compromised Credentials tab focuses on account credentials that can be attributed to specific systems, e.g. your corporate portal, Jira instance, Netflix account and more. These primarily originate from logs of stealer malware. The tab also displays exposed or leaked email and password combinations. In most cases, these credentials belong to the email (i.e. the password is the email account's password). However, given the ambiguous nature of how these are shared in the underground, it is impossible to determine with certainty their true attribution.

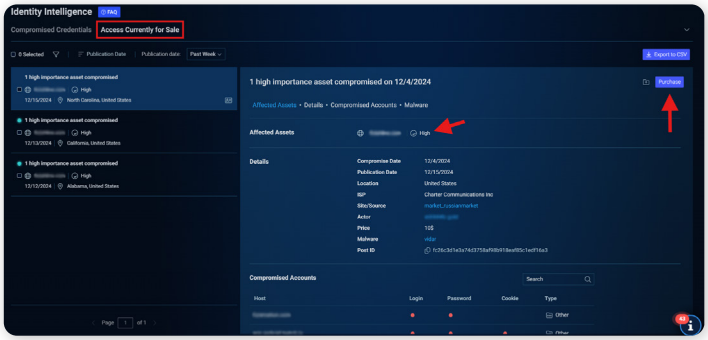
1. This view pivots off the Host information—i.e. the URL of the affected system—displaying accounts of systems matching your organization's domains that are listed in the "Attack Surface" page.
2. Previously detected credentials can be filtered, indicating they have been circulating in underground markets. IdP status filtering is also available, allowing security teams to determine if a user is still active and prioritize response efforts.
3. Users can also set a customizable password policy filter to view relevant compromised credentials that fit organizational password requirements as opposed to credentials that do not (aka fake credentials shared across the dark web).
4. Users are also able to search for specific Host and Email Domains as well as Hardware ID and IP Addresses for quick incident response.



Access Currently for Sale

The Access Currently for Sale tab displays information on compromised devices, typically via stealer malware, that is available for purchase across underground markets. This data is based on the assets (domains and IPs) that are listed in an organization's attack surface.

With Bitsight's elite threat intelligence services, we can infiltrate limited-access marketplaces to covertly take down and purchase stolen access being sold across the dark web. Contact our team to learn more.



☐ 0 Selected | Publication Date | Publication date: Past Week

1 high importance asset compromised
☐ [redacted] | High
12/15/2024 | North Carolina, United States

● 1 high importance asset compromised
☐ [redacted] | High
12/13/2024 | California, United States

● 1 high importance asset compromised
☐ [redacted] | High
12/12/2024 | Alabama, United States

Page 1 of 1

1 high importance asset compromised on 12/4/2024

Affected Assets • Details • Compromised Accounts • Malware

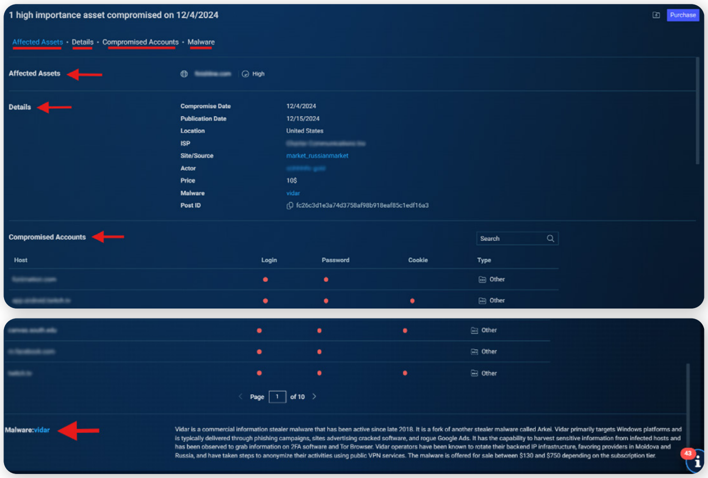
Affected Assets	[redacted] | High	
Details	Compromise Date	12/4/2024
	Publication Date	12/15/2024
	Location	United States
	ISP	Charter Communications Inc
	Site/Source	market_russianmarket
	Actor	[redacted]
	Price	10$
	Malware	vidar
	Post ID	fc26c3d1e3a74d3758af98b918eaf85c1edf16a3

Compromised Accounts

Search

Host	Login	Password	Cookie	Type
[redacted]	●	●		Other
[redacted]	●	●	●	Other

The asset details window allows users to view the Affected Assets, Details, Compromised Accounts, and Malware data related to the selected Asset.



1 high importance asset compromised on 12/4/2024

Affected Assets • Details • Compromised Accounts • Malware

Affected Assets	[redacted] | High	
Details	Compromise Date	12/4/2024
	Publication Date	12/15/2024
	Location	United States
	ISP	[redacted]
	Site/Source	market_russianmarket
	Actor	[redacted]
	Price	10$
	Malware	vidar
	Post ID	fc26c3d1e3a74d3758af98b918eaf85c1edf16a3

Compromised Accounts

Search

Host	Login	Password	Cookie	Type
[redacted]	●	●		Other
[redacted]	●	●	●	Other
[redacted]	●	●	●	Other
[redacted]	●	●		Other
[redacted]	●	●	●	Other

Page 1 of 10

Malware:vidar

Vidar is a commercial information stealer malware that has been active since late 2018. It is a fork of another stealer malware called Arkei. Vidar primarily targets Windows platforms and is typically delivered through phishing campaigns, sites advertising cracked software, and rogue Google Ads. It has the capability to harvest sensitive information from infected hosts and has been observed to grab information on 2FA software and Tor Browser. Vidar operators have been known to rotate their backend IP infrastructure, favoring providers in Moldova and Russia, and have taken steps to anonymize their activities using public VPN services. The malware is offered for sale between $130 and $750 depending on the subscription tier.

With our real-time collection and monitoring capabilities, security teams can quickly mitigate exposure from compromised accounts, deny threat actors access and limit damage to business operations.

Threat Intelligence Services

BI-WEEKLY CREDENTIALS REPORT

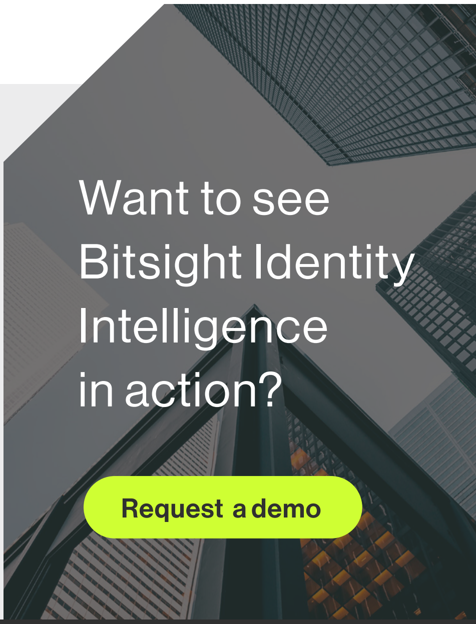
Statistics and analytics on compromised and leaked credentials providing visibility into threat exposure.

DEEP AND DARK WEB PURCHASES

Purchase compromised credentials listed for sale on underground marketplaces.

PURCHASE SUMMARY REPORT

High-level one-pager highlighting information about purchased data.



Want to see Bitsight Identity Intelligence in action?

Request a demo

sales@bitsight.com

BOSTON (HQ)
RALEIGH
NEW YORK
LISBON
SINGAPORE

Bitsight is a cyber risk management leader transforming how companies manage exposure, performance, and risk for themselves and their third parties. Companies rely on Bitsight to prioritize their cybersecurity investments, build greater trust within their ecosystem, and reduce their chances of financial loss. Built on over a decade of technological innovation, its integrated solutions deliver value across enterprise security performance, digital supply chains, cyber insurance, and data analysis.

BITSIGHT