



> DATASHEET

Cyble Darkweb & Cybercrime Monitoring

Actionable Intelligence from the Deepest Layers of the Internet

Introduction

The darkweb and cybercrime landscape spans a vast network of anonymized platforms, including TOR, I2P, illicit marketplaces, invite-only forums, paste sites, unindexed app stores, and encrypted communication channels such as Telegram and Discord. These environments serve as hubs for threat actor collaboration, data exfiltration, malware distribution, and monetization of stolen assets. Cyble's Darkweb & Cybercrime Monitoring service provides deep, continuous visibility into this fragmented ecosystem enabling organizations to proactively detect malicious intent, identify exposed data, and mitigate emerging threats before they impact operations or reputation.

| Threat Landscape



Over 350 billion darkweb records analyzed across forums, marketplaces, and ransomware leak sites.



\$10.2 billion in estimated annual losses due to identity theft and carding via dark marketplaces.



Ransomware leak sites have published **2500+** new victims in the last 12 months, exposing PII, source code, and internal documentation.



Telegram and other messaging platforms are increasingly used as alternate darkweb channels by **75%** of cybercrime groups.



Financial institutions, healthcare, and government agencies remain top targets for credential and data theft campaigns.

These figures underscore the need for continuous surveillance of illicit ecosystems to prevent reputational, financial, and legal damage.

| What is Cyble's Darkweb & Cybercrime Monitoring?

Cyble's Darkweb Monitoring service leverages advanced AI, NLP, and human intelligence to uncover real-time threats from closed cybercrime communities and underground networks. This intelligence helps security, fraud, and compliance teams take proactive actions to safeguard data, infrastructure, and brand integrity.

Component	Technical Description
Data Exposure	Correlation of organizational data artifacts (e.g., documents, email addresses, internal credentials, sensitive identifiers) with leaked datasets observed across deep and darknet ecosystems, including paste sites, breach forums, and illicit data dumps.
Leaked Credentials	Enumeration of credential pairs (username/password) harvested from stealer logs or breach datasets, indexed from darkweb forums, credential marketplaces, and Telegram drop sites. Includes verification against known breach corpora.
Ransomware Leaks	Continuous polling and monitoring of active ransomware group leak sites hosted on TOR/I2P, identifying exposed data sets and metadata (victim name, compromise date, file samples) linked to targeted organizations or industry verticals.
Compromised End-points	Identification of endpoint telemetry (hostnames, IPs, system metadata) linked to stealer logs or malware C2s, indexed in cybercrime infrastructure used for selling RDP access, infected machines, or initial access brokers (IABs).
Compromised Files & Potential Leaks	Deep search and extraction of proprietary documents, configuration files, code repositories, and business-sensitive assets exposed within darkweb archives, public P2P dumps, and encrypted messaging channels.
I2P & Tor Links	Active enumeration and scanning of hidden services (e.g., .onion and .i2p addresses) to detect references to organization-specific identifiers, credentials, or assets using deep search engines and darkweb crawlers.
Cybercrime Forum Mentions	Semantic and keyword-based analysis of threat actor discussions across closed and invite-only forums to identify targeted narratives, exploitation strategies, and data exposures referencing your organization.
Darkweb Marketplace Listings	Detection and indexing of underground marketplace items offering counterfeit goods, access credentials, financial data, phishing kits, or exploit tools associated with your brand, domain, or digital assets.
Telegram Channel Mentions	Monitoring of threat actor-operated Telegram channels and bots for chatter, leaks, or distribution of compromised organizational data, card dumps, stealer logs, and unauthorized access offers.
Discord Mentions	Monitoring of threat actor-operated Discord servers and channels to detect references to organizational assets, brand identifiers, credential leaks, or discussions of planned malicious activities including data dumps, access sales, and targeting directives
Compromised Cards	Detection of card data (BIN, PAN, CVV, expiry) associated with your ecosystem on fraud marketplaces, carding forums, or dump shops supporting fraud intelligence workflows.

How It Works

1

Data Collection:

Proprietary crawlers, partner APIs, and human reconnaissance collect intelligence across TOR, I2P, Telegram, IRC, paste sites, and underground forums.

2

AI-Powered Analysis:

NLP models and classifiers parse multilingual darkweb chatter and match content against your digital assets, domains, keywords, and identities.

3

Vetted Alerting:

Alerts are enriched and verified by Cyble's research team to reduce false positives and provide context (e.g., severity, source, recommended action).

4

Delivery & Integration:

Intelligence is delivered via Cyble Vision console or Access APIs to ingest in any relevant system. Also, reports are available for download in CSV and PDF formats.

| Key Benefits



Early Warning System:

Identify breaches before they become public incidents or affect customers.



Global Underground Visibility:

Coverage across 15K+ active darkweb and cybercrime sources, 250+ app stores, and 10+ threat actor forums.



Reduced Fraud & Financial Loss:

Prevent transaction fraud and unauthorized access through exposed card or login data detection.



Analyst-Ready Intelligence:

Receive high-context alerts with risk tags, source screenshots, and remediation recommendations.



Integration-Free Operation:

Delivered as a fully managed SaaS solution with no direct integration required, enabling rapid onboarding and threat visibility without impacting existing infrastructure.

| Use Cases

- 1 Early Threat Actor Targeting Insight:** Detect early indicators that your organization is being discussed or targeted in underground forums, ransomware groups, or data leak channels enabling proactive defense before attacks materialize.
- 2 Exposure-Based Risk Prioritization:** Gain clarity on which assets (e.g., credentials, IPs, endpoints, customer data) have been compromised or discussed by threat actors, allowing for prioritized remediation and incident response.
- 3 Brand and Identity Abuse Prevention:** Uncover the use of your brand in counterfeit product listings, phishing kit templates, scam pages, or fraud infrastructure sold across darknet markets helping mitigate reputational and financial damage.
- 4 Credential Leak Response:** Identify organization-specific email addresses or employee login pairs shared or sold on credential marketplaces, enabling you to pre-empt account takeover and internal compromise.
- 5 Darkweb Intel for Threat Attribution:** Leverage forum chatter, exploit trade, or leaked toolkits to trace back potential TTPs, affiliations, and motivations of adversaries discussing your digital environment.
- 6 Audit-Ready Threat Surveillance:** Strengthen compliance posture by maintaining documented surveillance of darkweb exposures supporting regulatory frameworks such as GDPR, PCI-DSS, and HIPAA with evidence of proactive monitoring.

| Conclusion

With Cyble's Darkweb & Cybercrime Monitoring, your organization gains unprecedented visibility into hidden threats, allowing you to act decisively against cybercriminals before they strike. From ransomware leaks to compromised credentials and forum chatter, Cyble delivers the intelligence you need to stay ahead in today's evolving threat landscape.



Scan the QR code to get a quick personalized demo of our AI-powered Threat Intelligence platform in action!

See Cyble in action

<https://cyble.com/request-demo/>
www.cyble.com

Get in touch with us today

contact@cyble.com | +1 888 673 2067

About Cyble

Cyble Inc. is a cybersecurity company specializing in dark web monitoring and threat intelligence services. Cyble leverages proprietary AI-based technology to help enterprises, federal bodies, and individuals stay ahead of cybercriminals. The company is known for its expertise in tracking cyber threats, data breaches, and other malicious activities.

© 2025 Cyble Inc. All rights reserved.

