PDI Dark Web Monitoring

Proactively detect and respond to dark web threats

Organizations face a growing risk of credential theft, data leaks, and brand impersonation as cybercriminals increasingly exploit dark web marketplaces and private forums. Many businesses lack visibility into these hidden threats, leaving them vulnerable to breaches, compliance violations, and reputational damage. Traditional security tools often miss post-exfiltration activity, and automated alerts can overwhelm teams with false positives, delaying response and increasing risk.

Gain early warning and actionable insights from verified dark web intelligence

PDI's Dark Web Monitoring service delivers continuous surveillance of dark web sources to identify exposed credentials, stolen data, and brand threats before they're weaponized. Backed by expert analyst validation, the service filters out noise and delivers only relevant, contextual alerts empowering your team to act swiftly and decisively. With tailored intelligence, real-time breach notifications, and quarterly threat reports, you gain a proactive edge in defending your digital assets and maintaining customer trust.

Real-time alerts

Human-verified intelligence

Tailored threat detection

Actionable reporting

Detect stolen credentials before they're used against you

pditechnologies.com

PDI TECHNOLOGIES

Enhance your security posture with integrated, analyst-verified threat intelligence

PDI's Dark Web Monitoring service is designed for high-risk, regulated industries such as retail, healthcare, and finance. It integrates seamlessly with existing security operations, including SIEMs and ticketing systems, and supports compliance with frameworks like NIST and CIS Controls. By attributing threats to malware like Lumma Stealer and tracking dark web chatter trends, the service provides deep context and early indicators of attack campaigns.

Today's threat landscape

- **1.35M** dark web listings in Q1 2025
- **38%** drop in early Q1 activity followed by a sharp rebound
- Lumma Stealer responsible for nearly **1M** listings
- Retail ransomware extortion surged **74%** in Q1

Infostealer attribution

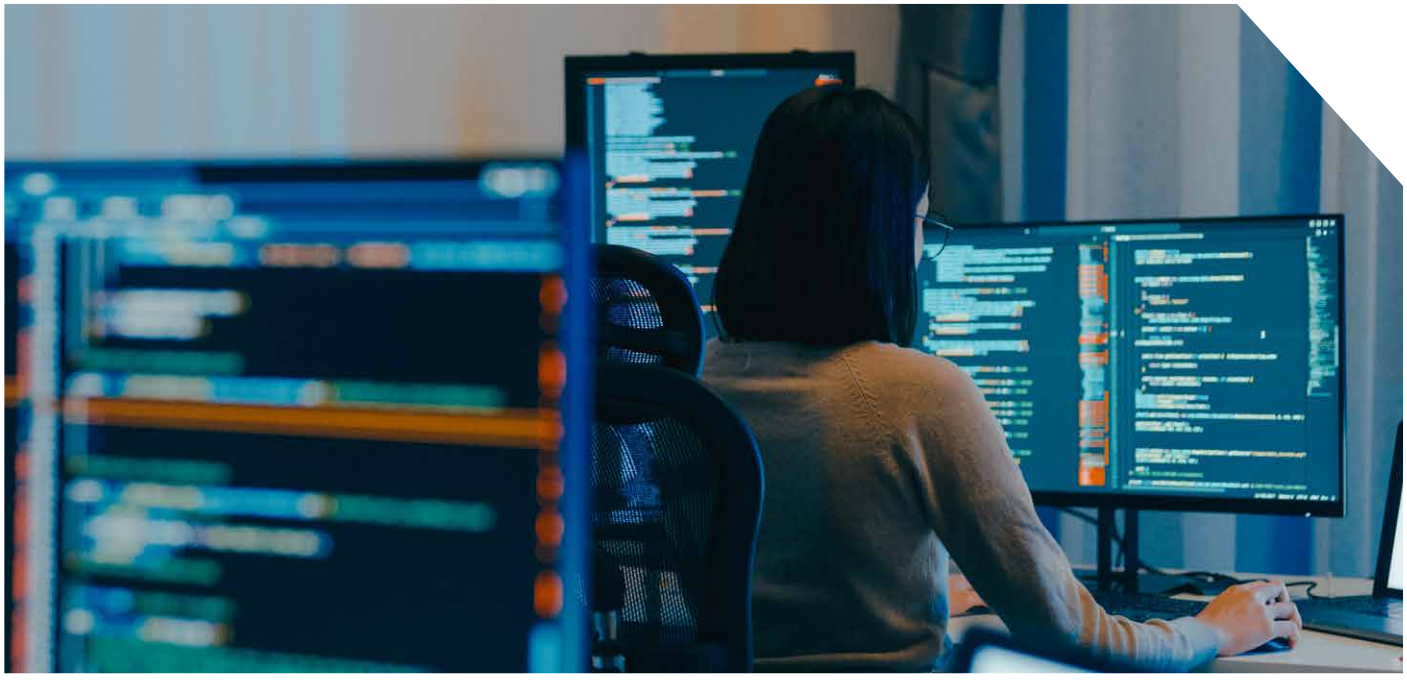
Understand how and where your data was compromised

SOC integration

Streamlined workflows with 24/7 monitoring and response

Credential risk reduction

Prevent fraud, account takeovers, and compliance violations



pditechnologies.com

PDI TECHNOLOGIES

Take a proactive approach to safeguarding your digital presence

PDI's team scours dark web marketplaces, forums, select threat actor communication channels, ransomware blackmail sites, credential exposure points, and pastebins to locate compromised data from your organization. Our service continuously tracks threats such as the following.

01 Compromised accounts

Monitor the dark web for any signs of compromised account credentials, whether they're being sold, shared, or accessed.

02 Data leak

Track the dark web for any signs of your organizational data being exposed.

03 Defacement

Guard against defacement attacks aimed at tarnishing your online presence.

04 Fraud

Detect compromised credit card details, even when paired with identity information.

05 Hacktivism

Keep watch for hacktivists targeting your domains.

06 Phishing

Identify rogue apps impersonating your brand and active phishing pages aimed at your organization.

07 Typosquatting

Detect threat actors impersonating your domain to harvest credentials or spread malware.

08 General mentions

Scan for mentions of your organization, domains, and products on underground sites, social media and messaging platforms.

Get a free report of your credential leaks

Learn how PDI Dark Web Monitoring can uncover threats before they hit your inbox or the headlines.

Talk with an Expert

pditechnologies.com

PDI TECHNOLOGIES