Datasheet

ThreatVision

TEAMT5

Deep & Dark Web Risk Monitoring

Detect Leaked Data & Cybercrime Risks Earlier

Sensitive corporate data, account credentials, and credential-related compromised-device information may be sold, exchanged, or discussed across the deep & dark web, underground forums, Telegram channels, or cybercrime communities. ThreatVision Deep & Dark Web Risk Monitoring continuously tracks underground channels to identify highly relevant exposure risks and data leaks, while supporting impact assessment, scope analysis, and mitigation planning through regular alerts, tailored analysis reports, as well as consulting services.

Key Highlights

1.5B+ Leaked Data Records

Covers leaked credentials, accounts, and sensitive data across the deep & dark web and underground sources.

77M+ Compromised Devices

Tracks compromised devices that may involve credential theft, data leakage, or follow-up attacks.

1.4M+ Deep & Dark Web Sources

Covers deep & dark websites, underground forums, and sources related to criminal activity.

400+ Telegram Channels

Tracks underground communities, criminal discussions, and leaked-data circulation.

Chinese Underground Channels in APAC

Covers APAC cybercrime communities and underground channels, with over 50% in Chinese.

Financial and E-commerce Crime Risks

Focuses on criminal activity related to financial and e-commerce sectors.

Tailored Reports and Consulting Services

Provides analyst-led analysis, risk evaluation, mitigation suggestions, and consulting services.

Key Benefits

Proactive Risk Monitoring

Detect potential risks across the deep & dark webs earlier through regular monitoring, helping organizations take action before threats escalate.

Stronger Response Readiness

Regular monitoring and timely alerts help organizations detect leakage risks earlier, while tailored reports support response planning, communications preparation, and operational adjustments.

Reduced Reputational Damage

Earlier visibility into the potential scope and impact of leaked data helps organizations prioritize response actions and reduce further impact on brand reputation and stakeholder trust.

How ThreatVision Helps Organizations Address Deep & Dark Web Risks Earlier

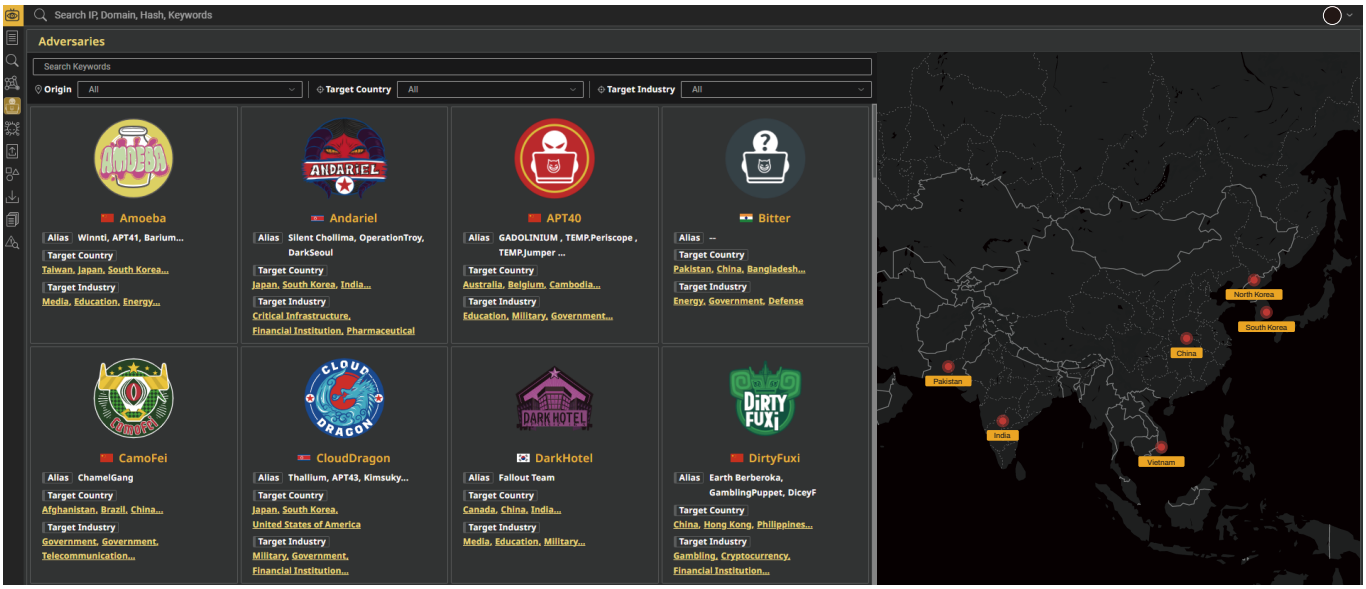
Business Concerns	How ThreatVision Helps
Have our accounts, credentials, or sensitive data been leaked?	Monitors the deep & dark web for enterprise domains, brands, credentials, and other keywords. Weekly monitoring results are delivered by email and automatically updated in ThreatVision.
Is the leaked data related to our business, customers, or internal systems?	Provides tailored monitoring reports to assess relevance, impact scope, and risk level.
Are underground forums or Telegram channels discussing or trading data related to us?	Tracks the Deep & Dark Web, hacker forums, Telegram, and Chinese underground channels for leaked-data circulation and criminal discussions.
How should we assess severity and priority after finding leaked signals?	Analysts provide DDW intelligence analysis, risk assessment, and mitigation recommendations to support follow-up decisions.
How are monitoring results delivered and used?	Weekly results are delivered by email and updated in ThreatVision. Leaked data can be exported as CSV for follow-up search and comparison.
Could a leak be connected to broader criminal activity?	When signals involve ransomware activity, cybercrime communities, or attack tools, ThreatVision Cybercrime Intelligence can help assess follow-up risks and defense priorities.

Service Package

Deep & Dark Web Risk Alert	Deep & Dark Web Tailored Report
• Monitor and scan deep and dark webs with weekly alert notifications. • Covers leaked credentials. • Weekly results delivered by email and updated in ThreatVision. • CSV export for leaked data.	• Dedicated monitoring report and professional consulting. • Analyst-written deep & dark web intelligence analysis, risk assessment, and mitigation recommendations. • Covers encrypted communities and various Chinese-speaking underground channels in APAC.

ThreatVision Platform Overview

ThreatVision's diverse intelligence supports various roles and tasks, helping organizations fully grasp the behavioral patterns of adversaries and proactively deploy defensive strategies. It is the optimal solution from strategic planning to frontline defense.



Get Started with ThreatVision

Please contact the TeamT5 sales team to request a 14-day trial account for ThreatVision. For further information, please email sales@teamt5.org. We look forward to helping protect your organization from cyber threats.

About TeamT5

v.202606

Widely trusted by more than 550 customers around the world, including government departments, technology, manufacturing, finance, medical care, military, telecommunications and other industries.

TeamT5 has more than 20 years of experiences in malware and advanced persistent penetration attacks (APT). With language and cultural advantages, we possess specific expertise in cyber espionage in the Asia-Pacific region, and are often invited to present the latest information at world-class cybersecurity conferences, including Black Hat in the United States, Code Blue / AVTokyo in Japan, Troopers in Germany, and Hack In The Box and FIRST. As a world-leading team in the field of threat intelligence research and advanced cybersecurity technology, we have also been interviewed by Bloomberg and CNN in the United States, Sankei Shimbun and Asahi Shimbun in Japan, and ET News in South Korea.

Tel +886-2-7706-1299
E-mail sales@teamt5.org

TEAMT5 | THREAT INTELLIGENCE PIONEER, BORN IN ASIA