

Adversary Intelligence

KEY VALUE

- Dedicated and experienced intelligence collection manager
- Industry-leading Intelligence Requirements program to ensure intelligence is constantly focused on the threats most relevant to your organization
- Finished Intelligence products to equip practitioners and leadership across multiple security disciplines
- Time-sensitive insight and operational knowledge of the tactics, techniques and methodology of cybercriminals
- Automated aggregation of relevant cybercriminal activity to support risk management and prioritization
- Comprehensive and proactive monitoring and alerting system to track threat actors and their malicious tools and tactics
- Ease of integration to consume intelligence through an online portal, RESTful API and third-party tools and platforms
- Request for information (RFI) support

Become Proactive Against Cybercrime Impact

Cybercriminals are committed to launching cyber attacks for monetary gain – this can have significant effects on business operations across your sector, organization and customers. Without timely and relevant intelligence exposing these adversaries and their TTPs, organizations remain in a reactive state with business-critical operations continuously at risk of being impacted. Intelligence, fraud, risk, security and incident response teams need sophisticated and professional intelligence capabilities to help them respond faster, defend proactively, and protect efficiently.

Reveal Top-Tier Cybercriminals and Their Operations

Tracking the most sophisticated and successful cybercriminals requires placement and access within the cybercriminal underground and local outreach contacts where they operate. Unfortunately, this is a problem that cannot be solved solely with technology, data scraping or any other feature that does not include experienced intelligence professionals.

Our team is composed of globally dispersed intelligence operators and native speakers who engage with top-tier cybercriminals on an ongoing basis. We have a long-standing and active presence within underground marketplaces, forums and chat rooms where entry is highly guarded.

Intel 471's Adversary Intelligence is produced from a focused collection, analysis and exploitation capability and curated from where threat actors collaborate, communicate and plan cyber attacks.

Adversary Intelligence Benefits

Obtain on-going and near real-time insight into the cybercriminal underground. Adversary Intelligence provides proactive and groundbreaking insights into the methodology of top-tier cybercriminals – target selection, assets and tools used, associates and other enablers that support them.

Intel 471's field driven collection and headquarters-based analysis directly supports the intelligence needs across an organization spanning your security, executive, vulnerability, risk, investigation and fraud teams.

Access finished intelligence or leverage the underlying and raw collection, it's up to you! We provide deliverables for multiple teams and maturity levels.



Focused and ongoing Automated Collection of cybercriminal forums and instant messaging platforms where adversaries plan and operate



Human Intelligence Reports by Intel 471 “boots on the ground” experts covering adversaries targeting customer organizations, industry verticals, geographies and third parties.

Includes:

- Daily tactical **Information Reports** on notable cyber activity derived from Intel 471 human intelligence sources and engagement with threat actors in the underground.
- Event-driven **Situation** and **Spot Reports** to relay raw and timely intelligence for current or emerging events observed in the cybercriminal underground along with action Intel 471 is taking.
- Weekly **Underground Pulse Reports** curated from Intel 471 observations to provide customers insight of key underground cybercriminal trends.



Finished Intelligence Analysis Reports of key Intel 471 insights of current and future cybercriminal activities observed in the underground including prolific adversaries, new and emerging threats, and recommended courses of action for customers to protect themselves.

Includes:

- Finished **Intelligence Bulletins** providing contextual insight related to interconnected events, activities and themes observed in the underground.
- Detailed **Profile** “baseball card” summaries to highlight prolific and emerging actors, services, products, forums and marketplaces within the cybercriminal underground.
- Monthly **Breach Analysis Report** to outline key insights into breach related activity based on geographic and industry-specific observations, breach types and future outlook.
- **Quarterly Threat Briefing** provides a published report and corresponding webinar summarizing key trends, major incidents, top adversaries, significant tactics, General Intelligence Requirements insights, and future outlook.
- **Whitepaper Reports** to provide long form intelligence of trends, statistics and forecasting of emerging underground themes or threats impacting industry verticals and geographies.



Additional **Adversary Intelligence** capabilities at your fingertips:

- All Intel 471 collection and reporting is steered by Intel 471 customer priorities using **General Intelligence Requirements**, which are integrated into the Titan platform and API.
- A unified and highly curated **Alerting** capability providing near real-time detection of cybercrime threats spanning Intel 471 linguistic coverage from the underground most relevant to customers.
- An Intel **471-shared knowledgebase** of categorized high-fidelity alerting curated by native speaking linguists and subject matter experts covering adversaries within the cybercrime underground from fraud schemes to malware.
- Targeted collection, research and tactical reporting driven by customer **Request for information** (RFI).