ADVERSARY INTELLIGENCE

INTEL471

KEY VALUES

- Tailored (1 to 1) practitioner support dedicated to driving collection and analysis to satisfy customer intelligence requirements
- Industry leading Intelligence Requirements program to ensure intelligence is constantly focused on threats most relevant to your organization
- Finished Intelligence products to equip practitioners and leadership across multiple security disciplines within an organization
- 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 platform, RESTful API and 3rd party tools and platforms
- Request for information (RFI) support

intel@intel471.com

Become Proactive Against Cybercrime Threats

Financially motivated cybercriminals are committed to launching cyber attacks for monetary gain – this can have significant effects on business operations against 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 comprised 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.

Benefits of Adversary Intelligence

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 is able to directly support 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.

ADVERSARY INTELLIGENCE

Deliverables

Focused **Automated Collection** of cybercriminal forums and marketplace posts and discussions to reveal what cybercriminals are discussing, planning, buying and selling

Tactical **Information Reports** on notable cyber activity derived from Intel 471 human intelligence sources and engagement with threat actors in the underground

Situation Reports 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

Underground Pulse and **Underground Perspective** reporting curated from Intel 471 observations to provide customers insight of key underground cybercriminal trends and trending open source media topics

Finished **Intelligence Bulletins** providing contextual insight related to events, activities and themes observed in the underground

Targeted collection, research and reporting driven by customer **Request for information** (RFI)

In-depth I**ntelligence Briefings** on notable cybercriminal related events where "ground-truth" credibility and reliability assessments are provided

Detailed **Profile** summaries delivering intelligence to highlight unique actors, services, products, forums and marketplaces prolific within the cybercriminal underground

Team of dedicated **Linguistic Analysts** providing native language translation, cultural interpretation and knowledge of underground cyber-centric "slang"

A unified and highly curated **Alerting** capability providing near real-time detection and tracking of cybercrime threats spanning our linguistic coverage of the underground marketplace

Vulnerability Weaponization Monitoring capability to assist patch prioritization and vulnerability management by tracking significant vulnerabilities in the underground

intel@intel471.com