ADVERSARY INTELLIGENCE

Data Sheet

KEY POINTS

- Finished intelligence and intelligence collection products that support the requirements of multiple areas of an organization
- Automatically aggregate relevant cybercriminal activity from numerous sources
- Gain insight and understanding of the latest malware, schemes and TTPs of cybercriminals
- Access and consume through an online portal, RESTful API and 3rd party integrations
- Intelligence requirements program to ensure our intelligence remains timely and relevant to your organization
- Automated alerting allowing for tracking and monitoring of threat actors proactively
- Request for information (RFI) support
- Receive your own dedicated and experienced intelligence collection manager

Do you really know who, what, when, where, why, and how cybercriminals are attacking your organization, sector and customers?

Financially motivated cybercriminals are continuously launching new attacks against your organization, sector and customers. Without timely and relevant adversary intelligence, these organizations remain in a reactive state with business critical events continuously occurring. Intelligence, fraud, risk, security and incident response teams need sophisticated and professional intelligence capabilities to help them respond faster, defend proactively, and protect efficiently.

Shining a light on top-tier cybercriminals

When it comes to the underground and tracking the most sophisticated and successful cybercriminals, it's all about placement and access. This is not a problem that can be solved with sophisticated technology or scraping but is a problem that requires experienced intelligence professionals. Our team is comprised of intelligence operators and native speakers located globally who are engaging with top-tier cybercriminals on an ongoing basis. They are also active in places where entry is highly guarded such as underground marketplaces, forums and chat rooms.

Intel 471’s Adversary Intelligence offering focuses on infiltrating and maintaining access to closed sources where threat actors collaborate, communicate and plan cyber attacks.

Benefits of the offering

Gain on-going and near real-time insight into the cybercriminal underground. This threat intelligence solution provides proactive and groundbreaking insights into the methodology of top-tier cybercriminals for targeting organizations, assets, and people as well as the enablers that support them.

Our field-based intelligence collection function and our headquarters-based intelligence analysis function is able to directly support the intelligence needs of your security, executive, vulnerability, risk, investigation and fraud teams.

Access the raw intelligence collection or the finished intelligence, it’s up to you! We provide deliverables for multiple teams and maturity levels. All finished intelligence is linked to the underlying intelligence collection that formed each assessment.

Deliverables

Deliverable	Scope	Objective	Frequency
Automated forum and marketplace collection	Regular and automated collection of cybercriminal forum/marketplace posts and discussions.	Expose clients to what cybercriminals are talking about, buying and selling.	Constant
Intelligence Bulletins	Detailed summary of notable event, activity, or theme observed in the underground.	Expose clients to significant events, activities, or themes that are beyond the scope of a single Information Report.	Weekly
Information Reports	Detailed intelligence collection report of notable event or actor update observed in the underground.	Expose clients to human intelligence collections derived from threat actors.	Multiple per day
Situation Reports (SITREP)	Brief summary of notable event/activity observed in the underground and/or open sources, including what action we're taking.	Alert/update clients to new/ongoing activity and inform them what action we're taking.	As needed
Underground Perspectives	Brief summaries of open source media topics, with related content observed in the underground.	Expose clients to underground activity that clarifies, confirms, or denies trending open source media articles.	Weekly
Profiles	Detailed summary of a notable or unique actor, service, or forum observed in the underground.	Highlight unique actors, services, and forums operating on the underground.	Weekly
Briefings	In-depth briefing of significant issue/event.	Provide client's intelligence teams with support for significant events.	As needed
Requests for Information (RFIs)	Targeted collection and research based on customer requests.	Provide client's intelligence teams with collection support for information gaps.	As needed
Underground Alerting	Keyword, actor or issue based alerting.	Provide client's intelligence teams with support for alerting of key terms, actors or issues from the underground.	As needed