INTEL 471 FINISHED INTELLIGENCE — KNOW WHEN TO ACT

Organizations need actionable intelligence to protect themselves from ransomware and data extortion groups, hacktivists, fraud and third-party attack vectors. Intel 471's finished intelligence is a cornerstone of our portfolios, and provides unique threat insights built for stakeholder decision-making — from security operations to governance, risk and compliance teams.

Finished intelligence contains our subject-matter experts' analyses of actors, events and trends across the threat landscape and observables in Intel 471's field reporting. These reports draw on exclusive insights from human intelligence (HUMINT) sources and automated raw data collection from underground forums, marketplaces and restricted messaging groups. This combined approach provides exclusive and timely insights into the shifting motivations, methods and associations of high-impact adversaries.

A variety of analyst-curated tactical, operational and strategic finished intelligence help cyber threat intelligence programs, security teams and executives stay ahead of threats and proactively mitigate risk. To help decision-making, threats and activities in all reporting — available on our cyber intelligence platform Verity471 — are classified under our industry-recognized Cyber Underground General Intelligence Requirements (CU-GIRs), ensuring reporting is aligned with customer priority intelligence requirements.

The following is a snapshot of our weekly, monthly and quarterly finished intelligence reporting and analysis on the cyber underground, the growing cyber-geopolitical nexus and emerging advanced threats.

Finished Intelligence		
Report	**Description**	**Why it matters**
Breach Report	**Strategic** Analyzes compromised access advertised on underground forums and ransomware-as-a-service (RaaS) blogs in a reporting period.	• Gain a current view of the latest initial access claims and ransomware breach events to stay ahead of threats • Visibility of breach data observed by Intel 471, including impacted regions and sectors, to better prioritize resources • Track the evolution of common initial access tactics, techniques and procedures (TTPs) and adapt defenses accordingly • Actionable insights into new ransomware offerings, new underground name-and-shame extortion sites and shifting actor affiliations
Threat Brief	**Strategic** A detailed quarterly analysis of notable trends in ransomware programs, initial access brokers, shifting affiliations, CVE weaponization, malware, hacktivist targeting, technology, law enforcement operations and key observables.	• Strategic insights into the state of the underground, anticipate, prioritize and respond to threats effectively • Improve risk management, monitor threats to assets, and manage vulnerabilities • Stay on top of threat trends impacting regions and sectors • Gain deep insights into TTPs, and new affiliations among high-impact ransomware programs, access brokers and intrusion clusters • Enhance internal executive threat reporting • Aligned with MITRE ATT&CK and the Diamond Model of Intrusion Analysis
Malware Campaign Report	**Operational, Tactical** Deconstructs emerging malware distribution. Provide full malware campaign analysis contextualized with Adversary Intelligence underground insights. Identifies infection vectors, lures, post-infection behaviors, and indicators of compromise (IOCs). Provides C2 data, YARA rules, STIX Domain Objects (SDOs) leveraging our patented Malware Emulation and Tracking System (METS).	• Gain unique insights into active malware campaigns through METS bot emulation malware traffic interception, and gain early visibility into threats • Understand the full scope of a malware campaign to improve response and remediation • Gain in-depth insights into command-and-control infrastructure and the behaviors of top Windows and Android malware families for precise and proactive mitigation • Understand targeting of sectors and geographies to prioritize defensive measures • Analysis of malware TTPs, infection chains and payloads to improve detection rules and threat hunting for behaviors

Finished Intelligence		
Report	**Description**	**Why it matters**
Profile Report (Actor, Marketplace, Service)	A one-page report that highlights the key elements related to an actor, marketplace or service of interest. This report consists of a summary of the actor, marketplace or service, identifiers, TTPs, notable events and an assessment.	• A concise, "living" snapshot helps security teams understand threats to ensure defenses are aligned with real-world threat activity • Support attribution efforts with documentation of adversary infrastructure, aliases, CTI entities • Understand the nature and scope of threats for CTI-informed threat modelling and proactive risk management • Drive stakeholder awareness of specific threats
Emerging Threats Reports	**Tactical, Operational** Identifies threat hunt packages available for TTPs observed in new and trending cybercriminal and APT activity. Intel 471's hunt team releases Emerging Threat Collections within 24-72 hours of observing a major emerging threat. The collection provides: • Associated behavioral threat hunt packages • Threat profiles • A full synopsis of the threat.	• Benefits threat hunt, DFIR and intelligence teams • Visibility of new, advanced threats that evade detection • Quickly identify behavioral threat hunting packages for emerging threats • Contextualize and prioritize hunts with threat profiles and synopsis of threat • Saves critical time researching, developing and validating new behavioral hunts • Immediately execute pre-validated hunt packages for threats targeting a region or sector • Demonstrate coverage to leadership in targeted sectors • Drive new detections with behaviors and artifacts identified in hunts for emerging threats • DFIR team can use an associated hunt package to search and identify other areas of impact if a hunt identifies behaviors
Cyber Geopolitical Intelligence Bulletin	**Strategic** Provides a detailed look at notable events, threat activity and other trends related to the cyber geopolitical threat domain in our primary areas of interest (AOIs). This report gathers information from several sources to outline a single topic or theme with multiple variables at play.	• Lowers the noise floor and provides intelligence, security operations and executive teams with situational awareness • Key findings help users quickly assess emerging and ongoing geopolitical events that impact cyber risk • In-depth expert analyses of locally sourced information about regional events and cyber threats • Analyst-driven assessments and outlooks on the second or third order effects of observed activity on the overall threat environment • Helps monitor evolving threats that are likely to impact regional operations, supply chains and merger or acquisition targets

Adversary Intelligence provides a stream of Intel 471's field reporting in near-real time. Intel 471 analysts placed across the globe engage directly with threat actors in their own language in the restricted forums and marketplaces where they operate, providing unique insights to detect, anticipate and disrupt adversary plans.

Adversary Intelligence — Collection Stream		
Report	**Description**	**Why it matters**
Breach Alert	**Tactical** Tactical field reporting on observed breach events and actors who offer compromised victim access or data.	• Enables faster response by proactively monitoring breaches impacting your organization and third parties • Real-time insights into breach events and offers for compromised data or access by ransomware or data extortion groups and initial access brokers
Information Report	**Tactical, Operational** Intelligence on threat activity from HUMINT sources, engagement with threat actors, communication channels.	• First-hand insights into new activity, offers for weaponized CVEs, malware, compromised access, cybercrime products and services • Researcher notes on sourcing, context, information reliability assessment • Access raw data, including technical IOCs for detection, investigation and blocking
Spot Report	**Tactical** Concise reports on breaking news, events, malware and activity across the threat landscape.	• Situational awareness • Stay on top of trending topics with threat insights into notable events, actor activity, malware observations and offers for new malicious tools and services • Links to investigate actor claims in messaging platforms, forums and marketplaces

To learn more about Intel 471's extensive Finished Intelligence report offerings, please contact sales@intel471.com or reach out from our website.

ABOUT INTEL 471

Intel 471 equips enterprises and government agencies with intelligence-driven security offerings powered by real-time insights into cyber adversaries, threat patterns, and potential attacks relevant to their operations. By integrating human-sourced intelligence with advanced automation and curation, the company's platform enhances security measures and enables teams to bolster their security posture by prioritizing controls and detections based on real-time cyber threats. Organizations are empowered to neutralize and mitigate digital risks across dozens of use cases across our solution portfolios: Cyber Threat Exposure, Cyber Threat Intelligence, and Cyber Threat Hunting. Learn more at intel471.com.

Our customers' eyes and ears outside the wire.