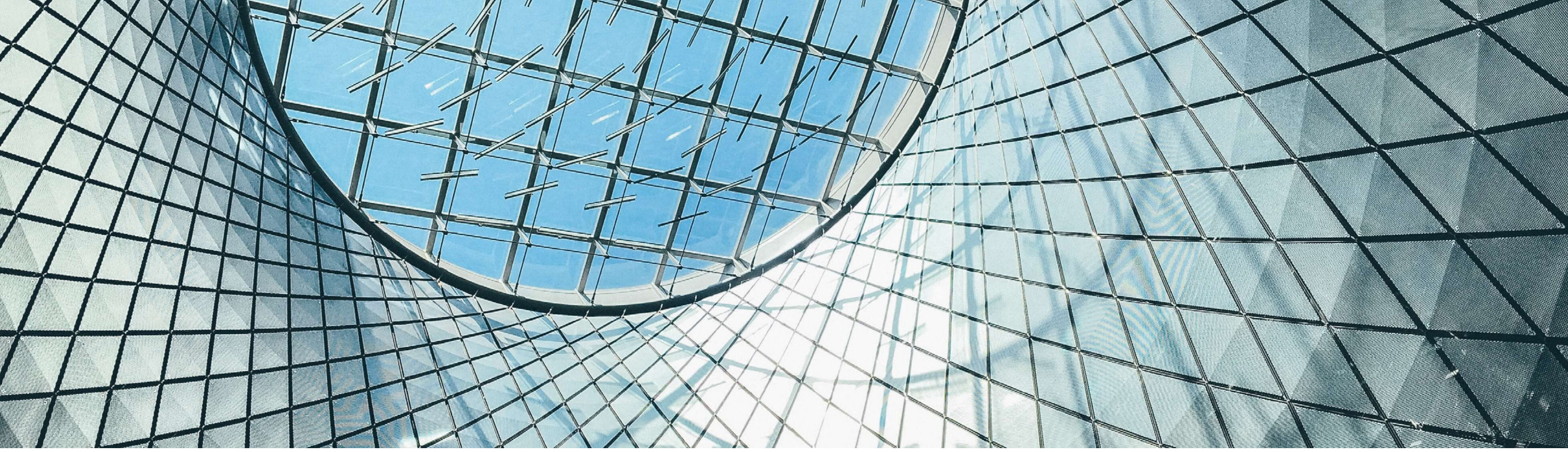

Market Insight Report Reprint

Coverage Initiation: Intel 471 counters cyberthreats with intelligence expertise and innovation

March 29 2021

Scott Crawford, Matthew Utter

In a busy market, threat intelligence is differentiated by more than insight into the nature of threat actor motives and methods. Intel 471 seeks to shine not only in the expertise of its 'boots on the ground,' but in the way it scales the gathering and delivery of actionable content.

451 Research

S&P Global
Market Intelligence

Introduction

The stakes in cybercrime today are high. On a broad scale, malware and attacks such as ransomware plague organizations worldwide, while adversaries leverage tools and techniques that may be as advanced as any legitimate approach to IT. The potential for substantial material gain motivates this activity – forcing adversaries to leverage stealth and sophistication to avoid detection and penalties.

In order to reveal this landscape, organizations must take advantage of human expertise as well as technology that can counter the adversary directly. Intel 471 leverages both. Capitalizing on experienced knowledge of the threat landscape and intelligence operations, technology that yields actionable findings from emulating the adversary's own techniques and a platform that delivers insight in readily consumable ways, Intel 471 seeks to make the most of the threat intelligence opportunity.

THE 451 TAKE

Intel 471's focus is on optimizing the gathering of high-quality observations and technical evidence of cybercriminal activity. The company emphasizes 'boots on the ground' expertise, fluent in cultural nuance combined with technology for gathering actionable evidence of threat activity and delivering it to its clientele. Its systematic approach to defining a framework for intelligence objectives, optimizing the gathering of human insight as observations are made and a sophisticated malware emulation architecture for collecting fine-grained technical evidence, are among the features differentiating Intel 471 in a crowded and competitive threat intelligence landscape.

This means that Intel 471's offering likely has greatest appeal to a mature threat analysis operation that can employ this insight directly in adapting strategies and tools. Less-advanced organizations may have greater reliance on more commodity defenses or on service providers. But for those that can capitalize on its capabilities, Intel 471 offers a wealth of information and analysis valuable to understanding in detail the nature of cybercriminals, their motivations and the specifics of fast-changing attacker tools and tactics of high concern to many organizations.

Context

Intel 471 was founded in 2014. The company of about 140 employees has headquarters in Dallas, with additional locations around the world. Founded by CEO Mark Arena and COO Jason Passwaters, the company, since its founding, has been self-funded. Before Intel 471, Arena worked as a software engineer for Telstra and ERG Transit Systems, as a technical specialist for the Australian Federal Police and as the chief researcher for iSIGHT Partners, which is now part of FireEye. Passwaters worked in military counterintelligence/human intelligence (HUMINT) and was the group leader of digital analysis and forensic analysis at Crucial Security. He also worked as the senior director of global research for iSIGHT Partners.

Technology

Intel 471 has built its offering on the basis of two key pillars. The first is technology to make the most of the gathering, management and delivery of observables across its customer base at a high level of detail. The second, as with any threat research organization, is human expertise, and in Intel 471's case this means analysts with familiarity and fluency not only in the tradecraft of threat intelligence, but in their cultures, languages, locales and venues of operation.

Experience is reflected first and foremost in an approach to defining and prioritizing intelligence objectives based on the precedent of so-called ‘general intelligence requirements,’ or GIRs, a framework Intel 471 has developed in the spirit of traditional methodology that comes from the military and US intelligence communities. Intel 471’s definition of Cyber Underground GIRs (CU-GIRs) allows intelligence experts to define the attributes of cybercrime intelligence of most value to a given organization and its priorities. Such an approach allows Intel 471 to systematically define relevance, synchronize and prioritize the intelligence effort and report observables that map to clients’ specific requirements and needs.

Human expertise enters not only into the cultural and linguistic fluency necessary to recognize and understand adversary activity in a variety of locales, but also to recognize the most valuable sources of information. Simply ‘scraping the dark web’ across thousands of venues and forums only adds to an overwhelming volume of data and can significantly decrease the signal-to-noise ratio of intelligence. Intel 471 analysis identifies the most useful among forums and venues of greatest relevance to cyberthreats affecting its clients.

Through a combination of automated collection and personas cultivated over time, Intel 471 provides coverage of cybercriminals in chatrooms, marketplaces and other forums. Cybercriminals often turn to these venues to facilitate the exchange of stolen credentials, access to compromised targets, malware and ransomware. Through its automated collection framework, Intel 471 takes in data on key actors, threats, issues and organizations within marketplaces and chat rooms, gathering intelligence and reducing the time between observation and action for its clients. These automation efforts help Intel 471 to scale its data collection initiatives. Analyst personas build rapport with the users of these marketplaces to guide engagements and retrieve information on these actors and their next steps. This process allows them to map out different entities along with closely tracing the flow of activity and information within these channels.

Intel 471 also focuses on malware intelligence, largely through the development and deployment of its Malware Emulation and Tracking System (METS). This system emulates the behavior of various elements of malware architecture to gather intelligence directly from cybercriminal malware systems that often leverage a high degree of automation and scale of their own. Details obtainable from malware is tracked as ‘state changes,’ which may be as fine-grained as noting the delivery of new modules of functionality or changes in the nature of command-and-control (C2) instructions. An example of this level of granularity enabled Intel 471 to recognize and differentiate, for instance, legitimate efforts to thwart Trickbot attacks in advance of the 2020 US elections in near real time. Through its emulation framework, the company can track different versions of malware and capture controller events while remaining undetected. Intel 471 also collects secondary payloads and tools to understand the end goal of certain malware. For example, a capability of the Cutwail malware that often targets a broad range of industries enables METS to capture malicious attachments and templates associated with an attack attempt, as well as targets and senders, all in near real time.

In addition to this information, the company provides YARA Rules and IDS signatures, indicators of compromise (IOCs), evidence of tactics, techniques and procedures (TTPs), malware and botnet configuration information and C2 monitoring. These efforts aim to help clients ingest the required data to identify, understand, connect and react to events that may threaten their organizations.

Products

All of these processes result in insights that are provided within Intel 471's Titan platform. Users can access this information through a web-based UI or ingest data through available APIs, which enable consumption through a customer's own assets such as a security information and event management (SIEM) system. Within the platform, users can access not only Intel 471's intelligence stream but also research on vulnerabilities, stolen credentials, malware and translations of content. It also centralizes intelligence alerts and provides a platform for managing requests for intelligence (RFIs), which describe needs for specific intelligence findings. Users can search for intelligence, including finished intelligence, historical and spot reports on particular actors and events to understand activity over time. The company also provides executive summaries of findings along with comments, IOCs, sourcing information and evidence of where different attacks were found.

The vulnerability dashboard provides a list of common vulnerabilities and exposures (CVEs) along with risk levels, affected vendors, patch availability, location (private, underground or open source), and level of interest by cybercriminals. In addition to these insights, the company provides information on exploit status (code available, weaponized, productized or not observed). Users can set up alerts based on specific watch groups that track ransomware, network or system access and insider threats.

Strategy

Intel 471 is not itself a 'threat intelligence platform' or TIP in the sense of an Anomali, EclecticIQ, ThreatConnect or ThreatQuotient because it does not integrate third-party content into its platform. It does, however, integrate its content into these and other platforms that extend intelligence capability such as Maltego, QuoLab, Siemplify and Silobreaker, as well as with the open source MISP (Malware Information Sharing Platform), security information and event management tools such as Splunk, security orchestration and automation, and a number of other intelligence-driven security and enrichment technologies.

The product is bundled into tiers with different levels of features from raw data to full access. Top-tier customers have access to a collections manager and specialist team that serves as a direct link to the global intelligence team and the broader effort. Customers can define priorities and requirements that drive their intelligence initiatives and participate in monthly calls to further identify relevant intelligence. The company hopes that this process will help organizations develop their own programs and extend capabilities.

Intel 471 also offers Club 471, which is a community of customers, senior intelligence analysts and intelligence operators. The community acts as a forum to share insights.

Competition

Threat intelligence is an active field where Intel 471 may both compete with and complement other cyberthreat intelligence vendors such as CrowdStrike, Cybersixgill, Digital Shadows, FireEye (through acquisitions such as iSIGHT Partners and Mandiant), Flashpoint and Group-IB, among others. Broader intelligence vendors such as LookingGlass Cyber, SecureWorks or Team Cymru do not compete as directly against the specific capabilities of Intel 471, but they may be contenders for threat intelligence spending. Other threat research organizations aggregate data in different ways through their own analysis to identify potential threats to organizations, but here again, these may not compete directly against Intel 471's specific capabilities. Recorded Future, for example, also produces its own expert analysis within its Insikt Group, but the company's technology is known for its ability to automate the recognition and gathering of intelligence primarily from unstructured data across many sources. In addition to these, broader security vendors such as Cisco and its Talos group, IBM's X-Force, Kaspersky's threat intelligence business and Palo Alto Networks' Unit 42 among many others also provide threat intelligence in addition to their security technology offerings.

SWOT Analysis

STRENGTHS

Intel 471 leverages experience and expertise in threat intelligence, including the cultural nuance necessary to be credible in adversary venues, combined with technological differentiation in the multiple automated collection capabilities to deliver, via its Titan platform, a differentiated offering in the marketplace.

WEAKNESSES

The level of capability and packaging options Intel 471 offers should appeal to organizations with a threat intelligence function or strategy that ranges from newly established to mature. Regardless, the advanced nature of Intel 471's offering could limit its appeal to a broader field of prospects with no objective to have a threat intelligence capability, but this limitation is likely offset by the advantages and tools it offers to those with the resources and desire to build that capability.

OPPORTUNITIES

A profusion of cybercriminals, venues and attack tools and methods coupled with high stakes for successful attacks, continues to drive innovation and investment in the field. Intel 471's differentiation gives it advantages for organizations that value the quality of its offering.

THREATS

Threat intelligence is a highly crowded and competitive field, with many recognized names including those who have combined with strategic security and IT vendors.

CONTACTS

The Americas
+1 877 863 1306
market.intelligence@spglobal.com

Europe, Middle East & Africa
+44 20 7176 1234
market.intelligence@spglobal.com

Asia-Pacific
+852 2533 3565
market.intelligence@spglobal.com

www.spglobal.com/marketintelligence

These materials have been prepared solely for information purposes based upon information generally available to the public and from sources believed to be reliable. No content (including index data, ratings, credit-related analyses and data, research, model, software or other application or output therefrom) or any part thereof (Content) may be modified, reverse engineered, reproduced or distributed in any form by any means, or stored in a database or retrieval system, without the prior written permission of S&P Global Market Intelligence or its affiliates (collectively, S&P Global). The Content shall not be used for any unlawful or unauthorized purposes. S&P Global and any third-party providers, (collectively S&P Global Parties) do not guarantee the accuracy, completeness, timeliness or availability of the Content. S&P Global Parties are not responsible for any errors or omissions, regardless of the cause, for the results obtained from the use of the Content. THE CONTENT IS PROVIDED ON "AS IS" BASIS. S&P GLOBAL PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, FREEDOM FROM BUGS, SOFTWARE ERRORS OR DEFECTS, THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED OR THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION. In no event shall S&P Global Parties be liable to any party for any direct, indirect, incidental, exemplary, compensatory, punitive, special or consequential damages, costs, expenses, legal fees, or losses (including, without limitation, lost income or lost profits and opportunity costs or losses caused by negligence) in connection with any use of the Content even if advised of the possibility of such damages.

S&P Global Market Intelligence's opinions, quotes and credit-related and other analyses are statements of opinion as of the date they are expressed and not statements of fact or recommendations to purchase, hold, or sell any securities or to make any investment decisions, and do not address the suitability of any security. S&P Global Market Intelligence may provide index data. Direct investment in an index is not possible. Exposure to an asset class represented by an index is available through investable instruments based on that index. S&P Global Market Intelligence assumes no obligation to update the Content following publication in any form or format. The Content should not be relied on and is not a substitute for the skill, judgment and experience of the user, its management, employees, advisors and/or clients when making investment and other business decisions. S&P Global Market Intelligence does not endorse companies, technologies, products, services, or solutions.

S&P Global keeps certain activities of its divisions separate from each other in order to preserve the independence and objectivity of their respective activities. As a result, certain divisions of S&P Global may have information that is not available to other S&P Global divisions. S&P Global has established policies and procedures to maintain the confidentiality of certain non-public information received in connection with each analytical process.

S&P Global may receive compensation for its ratings and certain analyses, normally from issuers or underwriters of securities or from obligors. S&P Global reserves the right to disseminate its opinions and analyses. S&P Global's public ratings and analyses are made available on its Web sites, www.standardandpoors.com (free of charge) and www.ratingsdirect.com (subscription), and may be distributed through other means, including via S&P Global publications and third-party redistributors. Additional information about our ratings fees is available at www.standardandpoors.com/usratingsfees.