

# Cybercrime Intelligence

#### **KEY VALUE**

- Gain broad coverage over the spaces where cybercriminals communicate, buy, sell and plan attacks
- Unique and ongoing visibility into bot communications, in depth malware analysis, deep technical reporting and high fidelity indicators of compromise (IOC) all in near real-time
- Comprehensive monitoring and alerting system to track malware and threat actor activity, vulnerability exploit statuses and compromised credentials
- Early warnings of compromise related to your third-party vendors and suppliers and other malicious activity
- Request for information (RFI) and other analyst support
- Industry leading Intelligence Requirements program to ensure intelligence is constantly focused on threats most relevant to your organization
- Ease of integration to consume intelligence through an online portal; RESTful API and thirdparty tools and platforms

#### **Proactively Address Cybercrime**

The impact of cybercrime across nearly every aspect of the business is a reality that today's security and intelligence practitioners battle daily. Not only are we fighting sophisticated adversaries probing our networks, but we're now faced with a plethora of threats such as account takeover, constantly evolving malware, sophisticated intrusions, the scourge of ransomware, massive data leaks, third-party supplier and vendor compromises, a seemingly endless surplus of critical vulnerabilities being released to the wild and the list goes on. Reactive to the next incident is no longer an acceptable or effective approach.

### Coverage and Ability to Operationalize

Intel 471's unparalleled global intelligence capability consists of automated collection systems and human intelligence teams that sit across 14 countries to provide near real-time coverage of threat actor and malware activity. Our Cybercrime Intelligence offers broad coverage across four core focus areas:

Adversary Intelligence: ongoing automated collection, human intelligence reporting, and high-fidelity alerting of top-tier cybercriminals targeting and affecting nearly every industry and geography across the globe.

Malware Intelligence: analysis and near real-time monitoring of malware activity and command & control infrastructure providing a steady stream of technical indicators, campaign reporting and deep technical insights on the top malware families deployed by threat actors.

Vulnerability Intelligence: regular vulnerability reporting and ongoing monitoring of the precursors of exploitation such as actor interest, exploit status, weaponization, productization and much more.

Credential Intelligence: ongoing monitoring and alerting of compromised credentials associated with your employees, VIPs, customers and third-party suppliers and vendors.

#### Benefits of Cybercrime Intelligence

Obtain ongoing and near real-time insight into the cybercriminal underground. Cybercrime 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.



## Malware Intelligence

- Constant stream of high-fidelity technical Indicators, malicious infrastructure and indicators of compromise (IOCs) that can be used for proactive alerting and blocking
- Deep technical reporting detailing all aspects of the malware such as complete functionality, targeting, detection, who wrote it, who is using it and more
- Timely field reporting related to updates, newly added functionality, malware campaigns, related adversary activity and other significant events associated with the malware
- Malicious file and sample analysis results that include configuration extraction, indications of targeting through file/url triggers, spam campaign templates, secondary payloads, modules/ plugins, and much more



## **Vulnerability** Intelligence

- Live vulnerability dashboard that tracks current threat levels as it relates to patch status, exploit status, adversary interest, weaponization and productization so you can drive patch priorities
- Weekly CVE Weaponization Report that provides a weekly snapshot of vulnerabilities of interest to cybercriminals and all associated details
- Individual vulnerability reports with full context that includes references to source reporting, POC code and open source info



## **Adversary Intelligence**

- Focused and ongoing Automated **Collection** of cybercriminal forums and instant messaging platforms where adversaries plan and operate
- Human Intelligence and Field Reports by Intel 471 "boots on the ground" experts covering adversaries targeting customer organizations, industry verticals, geographies and third parties
- Finished Intelligence Analysis Reports of key Intel 471 insights of current and forecasted cybercriminal activities observed in the underground including new and emerging threats and trends
- Team of dedicated Linguistic Analysts providing proactive and on-demand native language translation, cultural interpretation and knowledge of underground cyber-centric "slang"



## **Credential Intelligence**

- Dashboard that provides the ability to monitor and alert to *compromised* credentials found across the underground or offered by threat actors directly
- Full details of your employee's compromised credentials to include contextual information such as date ranges, occurrence across other data sets, links to threat actors and more
- Indications of credential compromise related to your key *third-party vendors* and suppliers and customers
- Raw data sourced from compromised data sets, malware/stealer logs and other private sources found within the underground marketplace