MALWARE INTELLIGENCE

DOMAIN BRIEF

THE MOVE FROM REACTIVE TO PROACTIVE

Cyber threat actors are continuously launching malware attacks against organizations across the globe. Too often, countering these threats is reactive and limited to single point-in-time analysis. These analyses become irrelevant quickly as the adversary adapts and recalibrates to circumvent protection measures and avoid detection. This means your organization is always playing catch up.

Intel 471's Malware Intelligence releases organizations from a reactive security posture by providing continuous monitoring and coverage of malware infrastructure and tools. Without this external visibility, organizations are ill-equipped to deploy a proactive and intelligence led cybersecurity strategy.

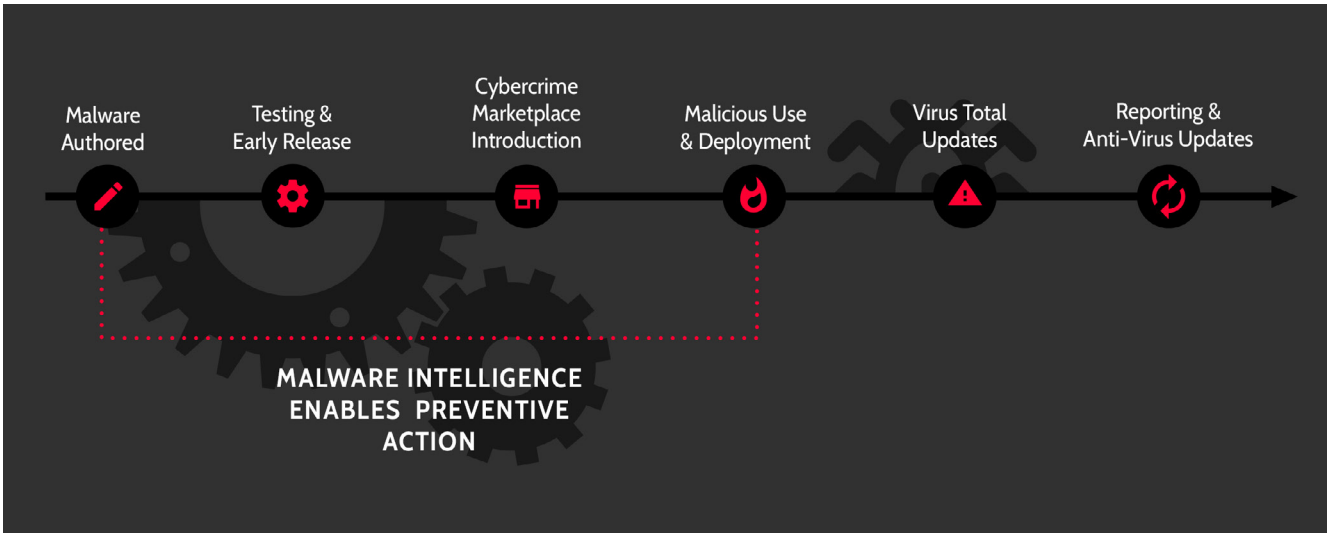
REAL-TIME INSIGHTS INTO ADVERSARY INFRASTRUCTURE WITH INTEL 471

Whether you need high-fidelity Indicators of Compromise (IOCs) streaming to your SIEM and firewalls, to track individual spam campaigns as they are executed, or to hunt for the precursors of a ransomware scenario, Malware Intelligence empowers you to start the shift towards a proactive and intelligence-led security system.

At the core of our Malware Intelligence is our unique and patented Malware Emulation & Tracking System (METS). METS provides ongoing surveillance of malware activity at the command-and-control level, delivering near real-time insights and deep context in support of numerous use-cases, such as:

- Malicious threat detection
- Breach and data leak monitoring
- Threat hunting
- Incident response investigative support
- Ransomware disruption
- Third-party exposure

SEE INSIDE TO STAY AHEAD:
WHAT DOES MALWARE INTELLIGENCE DELIVER?



Intel 471's Malware Intelligence is at the front end of malicious software development, enabling more effective understanding and mitigation of potential issues.

KEY BENEFITS:

- Support numerous security and intelligence use cases such as threat hunting, incident response investigative support, data breach and leak detection, and more
- Operationalize high-confidence, timely, and contextual Indicators of Compromise (IOCs) within your environment
- Monitor malware activity in near real-time, and gain early insight and operational knowledge of the latest crimeware campaigns
- Easy integration to consume through an online portal, RESTful API, and third-party integrations for fast operationalization
- Finished malware intelligence reports providing deep technical analysis and tactical updates to Tactics, Techniques, and Procedures (TTPs)
- Intrusion Detection System (IDS) signatures and YARA rules to reveal attack patterns and malware families and strains
- Malicious file and network-based indicators and associated tactics and techniques
- Malware and botnet configuration information, including web injects, and command and control infrastructure
- Ability to submit malicious samples and correlate with historical data and establish ongoing monitoring

KEY FEATURES:

Malware Intelligence Reports provide analysis of malware families and features, network traffic, how to identify, detect and decode it, extract and parse its configuration, control server(s) encryption key and campaign ID.

YARA Rules and IDS Signatures to accurately identify the identification and detection of malware families, malicious network traffic, and improve detection systems.

Malware Configuration Information provides decoded, decrypted and/or parsed configuration information, enabling insight on specific targets of banking trojans, spam campaigns, or other secondary malware payloads.

TTPs and Context to enable a detailed understanding when events are detected and blocked — including but not limited to linked malware family and version, encryption key, botnet ID, plugins used, expiration time, and associated intelligence requirements.

Continuous ***tracking and monitoring of over 350+ malware families*** which provides a timely and high-fidelity stream of indicators designed to be automatically ingested and operationalized within security stacks to block and detect malicious activity from malware.

Monitoring of ***Command and Control (C&C)*** servers to capture commands and updates initiated by threat actors to include secondary payloads, plugins, modules, and anything delivered to the "bot" from the adversary. All data is available for download for local processing and analysis.

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 **www.intel471.com**.