Malware Intelligence

KEY VALUE

- Support numerous security and intelligence use cases such as NOC/SOC support, threat hunting, campaign tracking, incident response and more
- Automatically operationalize high confidence, timely and contextual Indicators of Compromise (IOC's) within your environment
- Ability to monitor malware activity in near real-time and gain early insight and operational knowledge of the latest crimeware campaigns
- Ease of integration to consume through an online portal, RESTful API, and third-party integrations
- 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, command and control infrastructure
- Ability to submit malicious samples and correlate with historical data and establish ongoing monitoring

A Proactive Cyber Security Posture Demands External Visibility

Cybercriminals are continuously launching new attacks against organizations across the globe. Too often countering the threat of malware is reactive and limited to single point-in-time analysis. These analyses can become irrelevant as the adversary adapts and recalibrates to circumvent protection measures and avoid detection. Internal visibility is no longer enough to stay a step ahead of the adversary. Continuous monitoring and coverage of the adversary, their turf and their tools are a necessity. Without this external visibility, organizations are ill-equipped to deploy a proactive and intelligence led cyber security strategy.

24/7 Adversary Monitoring Delivers Timely Intelligence

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

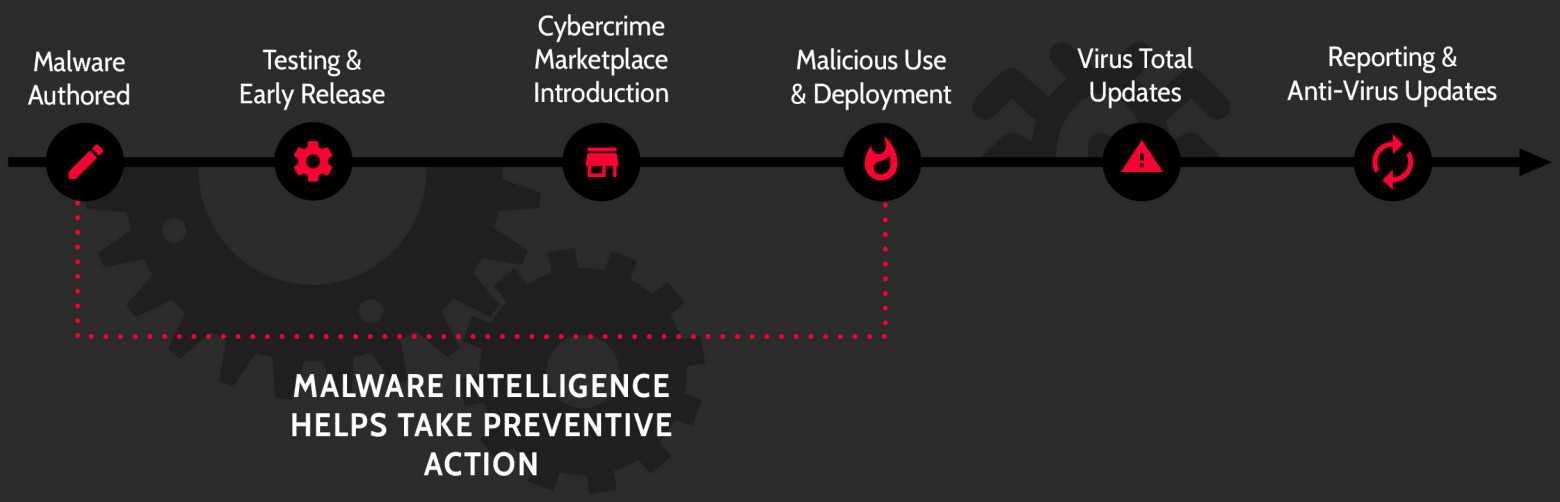
- Security Operations (NOC/SOC)
- Threat Hunting
- Incident Response
- Campaign Tracking
- 3rd-party Supplier and Vendor Risk

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

Operationalization Made Easy

Intel 471's TITAN platform and data model offers users to easily search, pivot and mine through a large dataset of threat intelligence and raw data. Our monitoring and alerting system can be used to alert on new activity in near real-time. The RESTful API and numerous integrations supports seamless ingestion into Threat Intelligence Platforms (TIPs), Security Information and Event Management (SIEM) systems, and other third-party platforms and security tooling.

sales@intel471.com



In-depth ***Malware Intelligence Reports*** providing 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.

In-depth ***Tactics, Techniques, Procedures 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 requirement(s).

Timely and high-fidelity ***File and Network Based Indicator*** feeds that can be automatically ingested and operationalized within security stacks to block and detect malicious activity from malware.

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

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

In depth ***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.

sales@intel471.com