MALWARE INTELLIGENCE

Data Sheet

KEY POINTS

- Automatically operationalize high confidence and timely IOCs with context within your environment
- Reduce the number of incidents you are responding to by blocking IOCs before incidents happen
- Gain insight and understanding of the latest crimeware campaigns
- Access and consume through an online portal, RESTful API and 3rd party integrations
- Supports malware detection, incident response, threat hunting and intelligence use cases
- Everything mapped to MITRE's ATT&CK framework
- Malware intelligence reports
- IDS signatures and YARA rules
- TTP information
- Malware and botnet configuration information including web injects
- File and network based indicators

Moving to an intelligence-led security strategy

Financially motivated cybercriminals are continuously launching new attacks against your organization, sector and customers. Without high confidence, timely indicators with rich context and TTP information, organizations are unable to move from a reactive incident driven security posture to an intelligence lead security strategy.

Coverage and ability to operationalize within your organization

When it comes to malware and technical intelligence, it's all about coverage and how quickly you can operationalize it within your organization. Where was the data and information collected from? How fresh is it? Is it still being used by cybercriminals? When can I expire it from my environment? How do I automatically block badness?

Intel 471's Malware Intelligence offering leverages Intel 471's industry leading access in the cybercriminal underground to obtain early access to malware including trojans, RATs and stealers. This early access allows us to analyze and reverse engineer obtained malware to create signatures (IDS signatures and YARA rules), malware intelligence reports and criminal infrastructure monitoring. As soon as the observed malware families are observed in the wild, we will make you and your security systems aware of it for blocking and detection.

Future malware family support within Intel 471's Malware Intelligence product will be driven by customer feedback.

Benefits of the offering

Seamless and automatically ingested into your security tooling and infrastructure including Threat Intelligence Platforms (TIPs) and Splunk.

Near real-time visibility into the latest cybercriminal malware campaigns in the wild and the latest malware advertised and released by cybercriminals in the underground.

Block and detect malware faster, thereby reducing incidents.

Rich context into everything provided including associated malware family, version, malware intelligence reports, botnet configuration (including parsed web injects), linked indicators, IDS signatures, YARA rules and MITRE ATT&CK framework mapping.

Deliverables

Deliverable	Scope	Objective	Frequency
Malware Intelligence Reports	In-depth analysis of malware families and features, network traffic, how to identify and detect it and how to decode, extract and parse its configuration, control server(s), encryption key and campaign ID.	Expose clients to detailed technical information on malware families, how they work and how to analyze obtained samples.	As needed
YARA Rules and IDS Signatures	Rules and signatures that enable the identification and detection of malware families.	Enable clients to accurately identify specific malware families, malicious network traffic and improve malware detection systems.	As needed
TTP Information and Context	In-depth TTP information and context around everything we provide including but not limited to linked malware family name, malware version, encryption key, botnet ID, plugins used, expiration time and linked intelligence requirement(s).	Expose clients to a large amount of context around everything provided. Enables an enhanced contextual understanding when events are detected or blocked.	All the time
Malware and Botnet Configuration Information	Decoded, decrypted and/or parsed malware and botnet configuration information including but not limited to campaign ID, botnet ID, plugins used and web injects.	Expose clients to the content of malware and botnet configurations. Enables an understanding of the specific targets of banking trojans and the ability to pivot between two seemingly unconnected campaigns or samples from the same threat actor.	All the time
File and Network Based Indicators	An extremely timely and high fidelity file and network based indicator feed.	Expose clients to a file and network based indicator feed that can be automatically ingested and operationalized within a customer's security stack to block and detect malicious activity from malware.	All the time
Command and Control (C&C) Monitoring	In-depth monitoring of malware command and control (C&C) servers for actor initiated commands and updates.	Expose clients to commands received from malware C&C servers including threat actors looking for internal executables.	All the time