MALWARE INTELLIGENCE

INTEL471

KEY VALUES

- Automatically operationalize high confidence, timely and contextual Indicators of Compromise (IOC's) within your environment
- Reduce the number of incidents you are responding to by blocking IOCs before incidents happen
- Gain early insight and operational knowledge of the latest crimeware campaigns
- Ease of integration to consume through an online portal, RESTful API and 3rd party integrations
- Defense in depth support for malware detection, incident response, threat hunting and intelligence use cases
- Intelligence and observables mapped to MITRE's ATT&CK framework
- Malware intelligence reports providing technical updates to malware families
- 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

Move to an Intelligence-Led Security Strategy

Financially motivated cybercriminals are continuously launching new attacks against organizations – often agnostic of sector and customers. Without high confident and timely indicators with deep context, organizations are unable to move from a reactive incident driven posture to an intelligence lead security strategy.

Coverage and Ability to Operationalize

When it comes to malware and technical intelligence, it is about coverage and how quickly you can operationalize it within your organization. Common but critical questions span from:

- Where was the threat data and information collected from?
- How "fresh" is the malware data, information and intelligence?
- Is the malware still being used by cybercriminals?
- When should the intelligence be expired?
- How do I automatically block badness with confidence?

Malware Intelligence leverages Intel 471's industry leading access within the cybercriminal underground to obtain early access to malware including Trojans, RATs and Stealers. This early access allows us to analyze and reverse engineer malware to create actionable signatures, malware intelligence reports and criminal infrastructure monitoring. As soon as observed malware families are seen in the wild, we will make you and your security systems aware to detect and mitigate.

Benefits of Malware Intelligence

Intel 471's Malware Intelligence was developed for seamless and automated ingestion into security tools and infrastructure, this includes Threat Intelligence Platforms (TIPs) and SIEMs (e.g., Splunk).

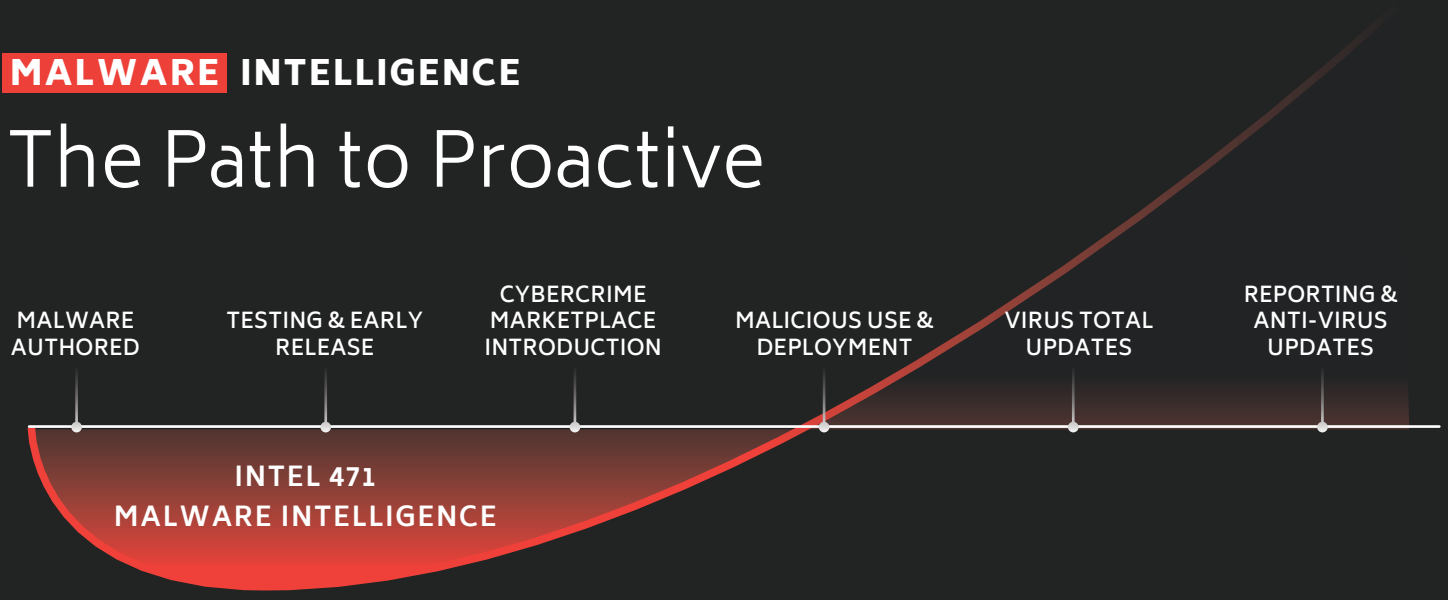
Security teams are equipped with early and near real-time visibility into the latest cybercriminal malware campaigns and latest malware advertised and released by cybercriminals in the underground. This enables security teams to confidently block and detect malware faster, thereby reducing incidents.

Organizations are able to implement a proactive driven security approach by using Intelligence on malware family, version, malware intelligence reports, botnet configuration (including parsed web injects), linked indicators, IDS signatures, YARA rules and MITRE ATT&CK framework mapping.

intel@intel471.com

MALWARE INTELLIGENCE

The Path to Proactive



DELIVERABLES

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

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

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)

Malware and Botnet Configuration Information providing decoded, decrypted and/or parsed configuration enabling insight on specific targets of banking trojans and the ability to pivot between seemingly unconnected campaigns or samples from the same threat actor

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

In depth **Monitoring of Command and Control (C&C)** servers to capture commands and updates initiated by threat actors to includes their reconnaissance looking for internal executables

intel@intel471.com