WHITEPAPER

Actionable Cyber Threat Intelligence:

Making Accuracy and Relevance a Priority

A Perspective for Public Sector Organizations,
Defense and Critical National Infrastructures

Abstract

Infrastructure-targeting cyber attacks using advanced malware pose a constant threat to national and military installations. Cyber attacks on these critical networks and facilities are intended to disrupt services, cause damage, exfiltrate confidential information, or interfere with operations, with potentially devastating ramifications if successful. Defending against these threats requires a protection strategy that matches the sophistication of the attacks the organizations are facing:

Cyber threat intelligence (CTI) has long been recognized as a crucial element of cyber risk management and cyber defense strategies. Yet, CTI effectiveness and usability can be limited by the quality, reliability, and relevance of the information, or by concerns related to data privacy and confidentiality. These challenges must be addressed to unlock the full potential of CTI programs. The accepted best-practice is to utilize threat information from multiple external and internal sources, e.g., commercial and open-source threat intelligence, in combination with self-generated intelligence based on own data.

This paper examines the generation of internal threat intelligence from malware- and phishing-related alerts.

Problem Statement

Most security teams routinely leverage external threat intelligence, such as open-source feeds and commercial threat information from CTI providers. The value and usability of external threat intelligence varies depending on the source, and it is essential for security teams to evaluate their external threat feeds before making decisions based on them. External threat intelligence, even if accurate, may not be applicable in the organization's specific environment, since the intelligence source may not align with the organization's own threat model. Open-source feeds can be vulnerable to manipulation by malicious actors, who can use the data to launch targeted attacks or spread false information.

To adequately protect against zero-day and custom-developed, highly targeted malware, security teams need to look beyond secondary threat data. To obtain a more accurate picture of malicious activities on their networks, they also require threat intelligence that has been extracted from data collected in their own environments – intelligence that is not available from external sources. Security teams must understand the limitations of external CTI and create their own internal threat information to bridge the gaps.

Malware and phishing alerts originating from internal security controls are inexhaustible and often underestimated sources for in-house CTI generation. However, the challenge lies in the ability to sort through the vast number of alerts, remove false positives, analyze the remaining ones in-depth to provide context and detailed behavioral insights and extract Indicators of Compromise (IoC). Manual malware analysis is not scalable, even if the organization's cybersecurity team has the necessary skills. Security teams require a more efficient approach for developing internal threat intelligence that can support their decisions and actions.

Definition:
Cyber Threat Intelligence (CTI)

Threat intelligence provides organizations with evidence-based information needed to develop effective defense strategies and make informed decisions.

Threat intelligence (CTI) typically falls in three categories:

Strategic CTI enables the assessment of the cyber threat landscape and informs the high-level cybersecurity strategy of the organization, including investments in additional security measures.

Tactical CTI provides details on the modus operandi of threat actors (i.e., their tactics, techniques, procedures, TTP) and helps to remove weaknesses in the existing defense setup.

Operational CTI is about the artifacts that are relevant for real-time investigation. It focuses on knowledge about specific attacks and helps to prioritize immediate threats.

Guidance Framework

To be effective, a CTI program must be tailored to the specific organization; otherwise, it is merely a collection of information that may or may not be relevant. The CTI value proposition to an organization comes explicitly from its ability to reliably enhance the organization's security operations and cyber risk management practices. The combination of externally sourced and self-generated threat intelligence provides a "best-of-both-worlds" approach, giving the organization a more comprehensive view of their threat landscape. A CTI program should always include threat intelligence consumption as well as threat intelligence production elements.

Since advanced malware plays a part in many, if not most, cyber attacks, it is good practice to utilize the never-ending stream of malware and phishing alerts as source material for internal intelligence generation. Although manual analysis of a malware sample by expert threat researchers can yield excellent output, it is no viable option for analyzing the large volume of samples required for the generation of threat intelligence.

Organizations should leverage automated malware analysis to speed up the process, ideally with the help of a technology that combines different static and dynamic analysis methods. The inclusion of state-of-the-art sandboxing technology is critical to expose and analyze yet unseen advanced malware.

Criteria to keep in mind when selecting a tool for the faster creation of threat intelligence from malware and phishing alerts:

- **Automation is essential to scalability:** To this effect, the tool must be able to easily connect with the wider security environment to automatically ingest alerts from sources such as EDR, XDR, SIEM, or SOAR systems. Equally, the solution must be able to automatically extract highly reliable, actionable Indicators of Compromise (IOCs) and behavioral insights from the analysis and present them in human-readable and machine-readable form to support the dissemination of the self-generated intelligence.
- **Compliance with confidentiality requirements:** The tool must support the compliance regulations of highly security-sensitive organizations, offering a range of deployment options, including on-premise and air-gapped deployments, to ensure the analyses can be conducted without any data leaving the organization's network. Cloud-based deployments for analyzing less sensitive data can be a viable option if the data centers meet confidentiality requirements.
- **Resistance against malware evasion techniques:** Advanced malware has been designed to thwart analysis. The tool must be highly resistant to evasion and avoidance attempts, as any overlooked malware behavior will compromise the generation of reliable CTI.

How VMRay Can Help

VMRay offers cutting-edge technologies for automated analysis and investigation of advanced malware and phishing threats, providing solutions tailored to the specific requirements of threat intelligence, incident response, and security operations teams. VMRay unites reputation analysis, static analysis, next-generation sandboxing, and machine learning into one single platform – the foundation of the solution portfolio.

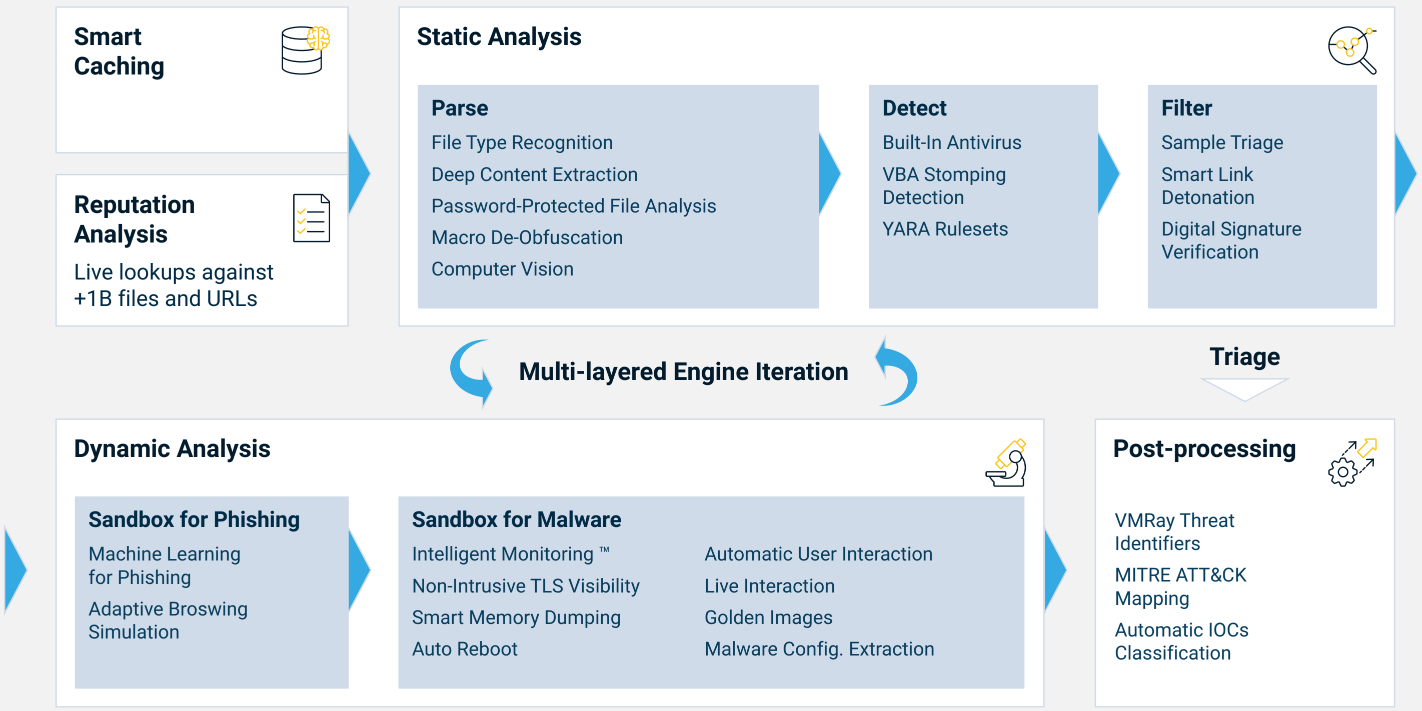
Definition:
Threat Data
Threat Information
Threat Intelligence

Threat Data:
Data with limited contextual information gathered from multiple sources, such as events or logs.

Threat Information:
The threat data has been structured and contextualized to yield more meaningful information.

Threat Intelligence:
The threat information has been further processed, analyzed, enriched with additional context, and compiled into actionable threat intelligence.

VMRay Platform Architecture



Smart Caching

Reputation Analysis

Live lookups against +1B files and URLs

Static Analysis

Parse

File Type Recognition

Deep Content Extraction

Password-Protected File Analysis

Macro De-Obfuscation

Computer Vision

Detect

Built-In Antivirus

VBA Stomping Detection

YARA Rulesets

Filter

Sample Triage

Smart Link Detonation

Digital Signature Verification

Multi-layered Engine Iteration

Triage

Dynamic Analysis

Sandbox for Phishing

Machine Learning for Phishing

Adaptive Broswing Simulation

Sandbox for Malware

Intelligent Monitoring ™

Non-Intrusive TLS Visibility

Smart Memory Dumping

Auto Reboot

Automatic User Interaction

Live Interaction

Golden Images

Malware Config. Extraction

Post-processing

VMRay Threat Identifiers

MITRE ATT&CK Mapping

Automatic IOCs Classification

The following table maps the VMRay technology to the five key characteristics required for effective threat intelligence:

Timely: Threat intelligence must be provided in near real-time with as little delay as possible, within the timeframe where it has operational relevance.	Threat intelligence teams often lack the tools necessary to quickly provide information for events that involve advanced malware and sophisticated phishing attacks. VMRay provides the necessary capabilities: • **Fully automated sample analysis:** VMRay delivers fully automated workflows, with no human interaction required during the analysis process, e.g., automated simulation of user behavior such as mouse clicks or system reboots to trigger malware behavior. VMRay weeds out false positives and triages valid alerts according to severity, enabling CTI teams to focus on high-priority events. • **Mitigate staff shortage and skill gaps:** VMRay acts as a force multiplier to ease the strain on CTI teams, allowing less experienced team members to take on tasks that usually require more advanced skills. This places even low-staffed teams in a position to efficiently generate high-quality internal threat intelligence for incident response, threat hunting, and security policy development.
Relevant: Threat intelligence must be tailored to the specific environment.	Externally sourced CTI gives broad visibility into the global threat landscape but is often too generic and may not capture the unique threats to a particular organization. VMRay helps to close this gap by providing the means to generate highly relevant CTI from in-house sources: • **Technology stack integration:** VMRay enables high-volume alert ingress from sources like EDR, XDR, SOAR, and SIEM through out-of-the-box connectors for leading vendor solutions or REST-API for custom-integrations.

Accurate: Threat intelligence must be correct, complete, and explicit.	Advanced malware is highly evasive, and designed to escape analysis and detection. VMRay enables organizations to reliably identify and catch threats that have bypassed other security controls. • **Highly resistant against sandbox evasion:** VMRay's monitoring approach ("looking from the outside in") makes the analysis environment virtually invisible, even to sophisticated, context-aware malware. Samples are encouraged to expose their true intentions. • **Designed to catch custom-developed malware:** The VMRay analysis environment is highly customizable to resemble the organization's production environment as closely as possible. Customization includes the use of Golden Images and Geolocation settings to uncover targeted attacks.
Specific: More detailed and more specific insights allow defenders to determine the best countermeasures.	The speed and effectiveness of CTI generation is closely linked to the quality of the analysis and the quality of the reports that are subsequently generated from the analysis results. Low-quality analysis can miss important details, while low-quality reporting can contain up to 90% irrelevant noise. Both undermine the ability to identify and address a complex threat quickly. • **Full visibility into malware behavior:** VMRay captures and categorizes every interaction between the suspicious files / URLs and the analysis environment, down to the granular level of function logs and memory dumps. No critical details get missed during analysis. • **Noise-free reporting:** VMRay's in-depth analysis reports present detailed information relevant to understanding the analyzed threat. Irrelevant information is filtered out so that important signals are not lost in the background noise.
Actionable: Threat intelligence must be usable in a practical sense and translate into actionable steps that can be taken.	Output from malware analysis is an underutilized source of threat intelligence due to the difficulty of extracting actionable IOCs in a time-efficient manner. VMRay automates the extraction of high-fidelity IOCs for CTI teams. • **Automated generation of actionable IOCs:** VMRay extracts highly reliable Indicators of Compromise from data gathered during threat analysis, distinguishing generic artifacts from IOCs and removing irrelevant information from the report while flagging and scoring relevant IOCs. The result is powerful, actionable threat intelligence that can be shared with the security environment.

VMRay supports confidentiality and privacy requirements in regulated sectors:

On-premise deployments

Including air-gapped environments. Samples and analysis data never leave the organization's network. This is the preferred deployment option of organizations that are required to keep all data within their own environment for compliance reasons.

Cloud-based deployments

Hosted in GDPR-conform, ISO/IEC 27001-certified data centers in Europe and the USA. All samples uploaded to VMRay Cloud products are only accessible by the organization's own users. VMRay does not share any files or customer data with external parties. Reputation lookups and VirusTotal integration are optional, and can be controlled site-wide, or enabled and disabled with each sample submission.

Multi-Factor Authentication

Organizations can enable Multi-Factor Authentication (MFA) and use a Time-based One-Time Password (TOTP) token generated from another device to access their VMRay account. Popular authentication apps can be used to scan and generate codes required for authentication. In addition, VMRay's SSO support can be leveraged to use the identity provider's MFA support.

Regulatory compliance

VMRay is ISO/IEC 27001-certified.

Additional Information:

VMRay Technology Glossary
vmray.com/detection-analysis-technologies

VMRay Analysis Reports
vmray.com/resources/malware-analysis-reports

VMRay Threat Feeds
threatfeed.vmray.com

About VMRay

VMRay has **pioneered the Malware Analysis industry** since its founding in 2013. Today, VMRay has earned an excellent reputation in the government and defense sector, and is trusted by the world's largest organizations, industrial and technology corporations, international financial services institutions, and leading consulting and accounting firms.

VMRay GmbH
Suttner-Nobel-Allee 7
44803 Bochum • Germany

VMRay Inc.
75 State Street, Ste 100
Boston, MA 02109 • USA

VMRAY