Feature Brief

VMRAY

AUTOMATED IOC GENERATION

Sandbox-generated IOCs are an under-utilized source of threat intelligence, due to the difficulty of extracting actionable and trusted IOCs in an efficient manner. VMRay Analyzer unlocks this potential by automating this process for security teams.

Addressed Challenges

Analysis Artifacts

A malware sandbox analyzing a threat collects pieces of forensics data which have been observed during the analysis runtime. This collected data, often referred to as "analysis artifacts", typically includes files, URLs, IPs, processes, and registry entries which were used, created, or modified as part of the malware execution.

While analysis artifacts may be used by security analysts to get a better understanding of what happened malware detonation, they usually cannot be used to characterize it. These artifacts are too generic and may be observed when executing benign samples.

For example, a malicious process accessing trivial Windows registry entries, or reading DLLs which belong to an execution environment such as .NET can generate artifacts identical to a benign process.

Indicators of Compromise (IOCs)

To characterize threats, security teams collect, aggregate, and monitor for IOCs. An IOC is essentially a piece of forensics data related to a given threat, that can identify the presence of this threat in a system or a network.

Distinguishing Artifacts from IOCs

In the context of a malware sandbox, IOCs are a subset of artifacts. In other words, while artifacts are all the observed forensics pieces of data, not every artifact can be considered an IOC. Detecting the presence of the DLL file in the above example doesn't mean this threat is present in your environment.

This fact makes it difficult for organizations to use a malware sandbox for effectively generating IOCs, since exporting them into **3**rd party systems, such as a TIP, may pollute their repositories. Misclassifying an artifact as an IOC can lead to false alerts, and potentially a direct negative impact on the production network.

Unfortunately, this is why malware analysts still use mostly manual, time-consuming methods to extract IOCs that are reliable and actionable.

VMRay Analyzer Feature Overview

Extracting Analysis Artifacts

When samples are analyzed using the VMRay Platform, analysis artifacts are extracted. Artifact types that are included in VMRay analysis reports are: Files, Filenames, URLs, Domains, IPs, Registries, Mutexes, Processes, Emails and Email Addresses.

Artifacts are extracted from analyses as follows:

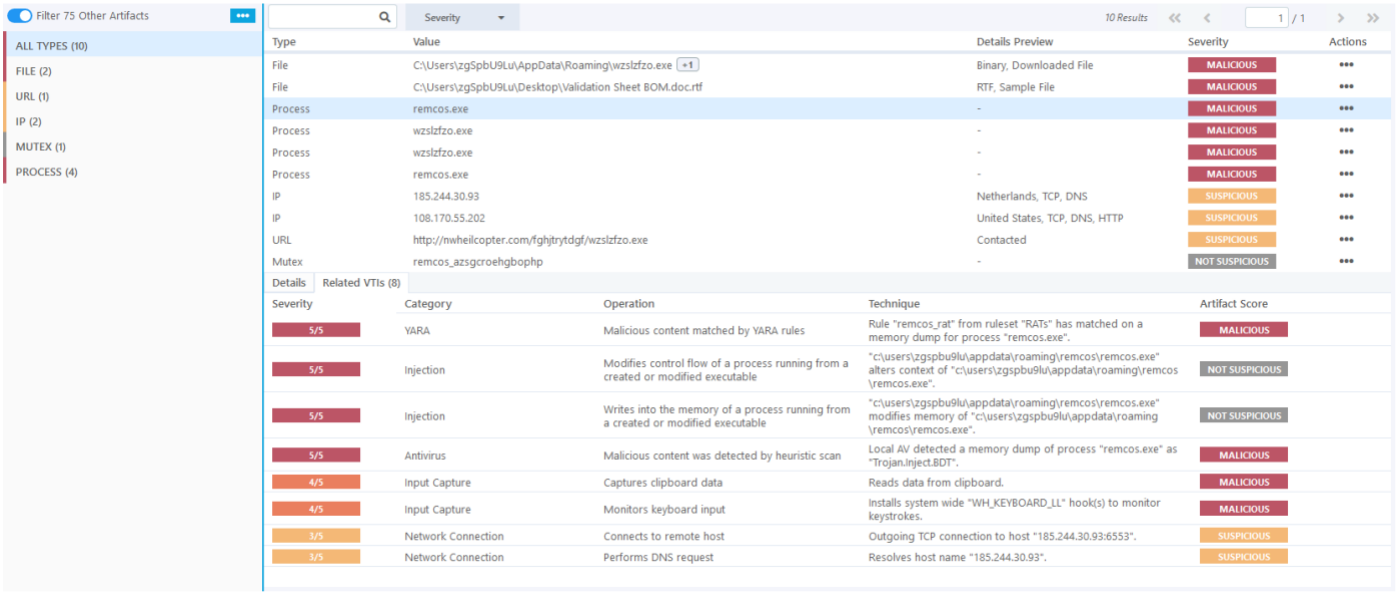
- Environment artifacts: artifacts such as files, processes, registry entries and mutexes which were used, created, or modified as part of the analysis runtime
- Network artifacts: URLs, domains and IPs extracted from network API calls as well as the PCAP
- Downloaded files: files that were downloaded during the analysis runtime
- Embedded links: URL links in documents and emails statically extracted
- Embedded artifacts: embedded files and network artifacts, statically extracted from the sample as well as other file artifacts such as scripts, macros and process command lines

IOCs Flagging and Scoring

VMRay Analyzer automates the process of extracting IOCs from analysis artifacts by flagging relevant artifacts as IOCs.

The key innovation is the use of VMRay Threat Identifier (VTI) rules to flag artifacts which are associated with an unusual behavior. For example, a URL used by a dropper to download the payload will be flagged as an IOC. This means that IOCs are now defined as a subset of artifacts, by adding to each artifact an "IOC" flag. To make this even more powerful, VTIs are now also used to better determine the maliciousness of an IOC.

In the following image, the Analysis Report IOCs tab presents an IOC with a malicious severity, together with the list of related VTIs which were used to determine its severity.



VMRay Analyzer Report - IOCs tab

Contextualizing and Exporting IOCs

Complementing IOCs flagging and scoring, other capabilities include:

- Exporting IOCs: supported formats are JSON, CSV and STIX 2.0, offering multiple ways to export IOCs to other security systems.
- Contextualizing: artifacts and IOCs are enriched with attributes extracted during the dynamic and static analysis, including geographic location, user agent, parent process, classifications, threat names, and others.
- The IOCs tab: an interactive tab provides detailed information on indicators, artifacts, and related VTIs. It allows team members to easily filter, navigate, explore and finally export IOCs.

Combined, these capabilities allow analysts to use IOCs generated by VMRay Analyzer with confidence, including as part of automated detection and protection workflows.