

Malware Attribute Enumeration and Characterization - MAEC™

A Standardized Language for Attribute-Based Malware Characterization

MAEC IS A STANDARDIZED LANGUAGE for encoding and communicating high-fidelity information about malware based upon attributes such as behaviors, artifacts, and attack patterns.

By eliminating the ambiguity and inaccuracy that currently exists in malware descriptions and by reducing reliance on signatures, MAEC aims to:

- Improve human-to-human, human-to-tool, tool-to-tool, and tool-to-human communication about malware
- Reduce potential duplication of malware analysis efforts by researchers
- Allow for the faster development of countermeasures by enabling the ability to leverage responses to previously observed malware instances

Challenge

Modern methods for detecting and combating malware often rely on the characterization of malware attributes and behaviors. The use of static and dynamic analysis techniques allows for an encompassing profile of malware to be constructed based upon its disassembled binary and observed run-time behavior.

Yet, the lack of an accepted standard for unambiguously characterizing malware means that there is no clear method for communicating the specific malware attributes detected in malware by the analyses, nor for enumerating its fundamental makeup. The results are non-interoperable and disparate malware reporting between organizations, disjointed or inaccurate malware attribution, the duplication of malware analysis efforts, increased difficulty in determining the severity of a malware threat, and a greater period of time between malware infection and detection/response, among others.

Solution

MAEC solves these problems. The characterization of malware using abstract patterns offers a wide range of benefits over the usage of physical signatures, and allows for the accurate encoding of how malware operates and the specific actions that it performs. Such information can not only be used for malware detection, but also for assessing the end-goal the malware is pursuing and the corresponding threat that it represents.

Focusing on the attributes and behaviors of malware facilitates detection and analysis of emerging, sophisticated malware threats that circumvent the traditional signature-based and heuristic approaches. Characterizing malware in a standard way supports collaboration across organizations and the identification of common behavior, functionality, and code bases across instances of malware.

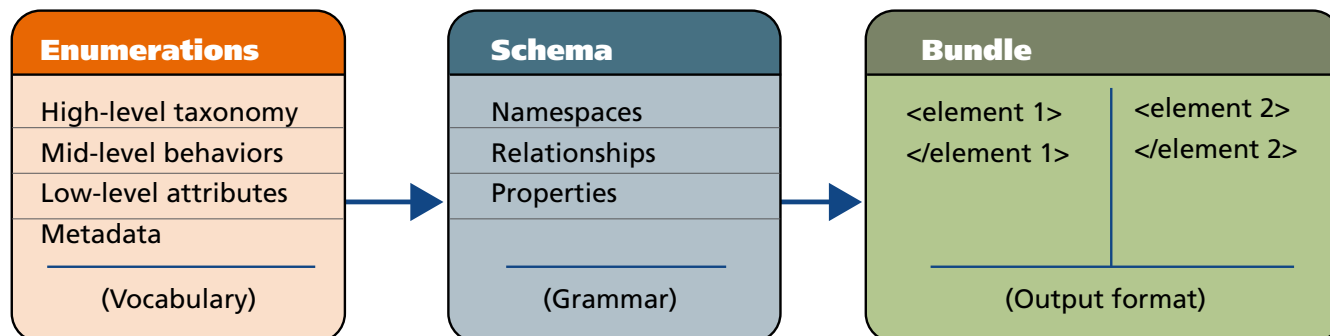
MAEC achieves this end result by utilizing three community-developed components to create the standardized MAEC Language:

- Vocabulary of attribute enumerations
- Schema for defining vocabulary syntax
- Standard output format based on schema

MAEC Language

MAEC is being developed as a formal language for characterizing attributes and behaviors of all types of malware. Initially MAEC will focus on characterizing the most common malware types, including Trojans, worms, and rootkits, but will

ultimately be applicable to more esoteric malware types. As a language, MAEC will have a grammar and vocabulary that provide a standard means of communicating information about malware attributes.



MAEC's core components include a vocabulary, grammar, and form of standardized output.

MAEC Enumerations – an enumerated vocabulary composed of three distinct levels of malware attributes at different levels of abstraction—low-level attributes, mid-level behaviors and high-level taxonomies—as well any metadata.

MAEC Schema – a syntax for the common vocabulary of attributes and behaviors, and an interchange format for structured information about these elements.

MAEC Bundle – a standard output format that can be used to describe a malware instance, malware components, or malware families in terms of MAEC's enumerations and schema.

MAEC Use Cases

As a domain-specific language for the characterization of malware, MAEC has a broad range of uses, especially with regards to malware analysis and anti-malware operations. The following are just a few of the use cases that MAEC will support:

Analysis-Oriented Use Cases

- Common Vocabulary for Malware Analysis
- Enhanced Data Sharing Between Malware Repositories
- Wrapper for Malware Analysis Tool Output
- Objective Criteria for Anti-malware Tool Assessment

Operations-Oriented Use Cases

- Uniform Malware Reporting Format
- Malware Detection
- Malware Threat Assessment
- Malware Response
- Malware/Attacker Correlation

Join the MAEC Community

MAEC is industry-endorsed through the MAEC Working Group, which includes members from industry, academia, and government.

Members of the antivirus and information security communities may contribute to the ongoing development of MAEC on the MAEC Discussion List at <http://maec.mitre.org/community/discussionlist.html>.

Member of
<http://measurablesecurity.mitre.org>



Learn More - <http://maec.mitre.org>