Suggested Methods for the Validation of Samples

amtso™

Anti-Malware Testing Standards Organization

Notice and Disclaimer of Liability Concerning the Use of AMTSO Documents

This document is published with the understanding that AMTSO members are supplying this information for general educational purposes only. No professional engineering or any other professional services or advice is being offered hereby. Therefore, you must use your own skill and judgment when reviewing this document and not solely rely on the information provided herein.

AMTSO believes that the information in this document is accurate as of the date of publication although it has not verified its accuracy or determined if there are any errors. Further, such information is subject to change without notice and AMTSO is under no obligation to provide any updates or corrections.

You understand and agree that this document is provided to you exclusively on an as-is basis without any representations or warranties of any kind whether express, implied or statutory. Without limiting the foregoing, AMTSO expressly disclaims all warranties of merchantability, non-infringement, continuous operation, completeness, quality, accuracy and fitness for a particular purpose.

In no event shall AMTSO be liable for any damages or losses of any kind (including, without limitation, any lost profits, lost data or business interruption) arising directly or indirectly out of any use of this document including, without limitation, any direct, indirect, special, incidental, consequential, exemplary and punitive damages regardless of whether any person or entity was advised of the possibility of such damages.

This document is protected by AMTSO's intellectual property rights and may be additionally protected by the intellectual property rights of others.

Suggested Methods for the Validation of Samples

Introduction

The following represents a summary of tools available to validate anti-malware product testing samples, and may be used by testers, publications and vendors. This summary is not a comprehensive listing of all relevant tools or methodology, and does not endorse the use of any specific tools or methodology. Unless defined herein, all terms included in this document are used with their common meaning. The following should be read in conjunction of AMTSO's *Fundamental Principles of Testing*, *Best Practices for Dynamic Testing,* and other information available on www.amtso.org.

Steps to Validate Samples

Principle Five of AMTSO's *Fundamental Principles of Testing* states that "[t]esters must take reasonable care to validate whether test samples or test cases have been accurately classified as malicious, innocent or invalid." This principle requires the validation of samples in a sample set, which can be achieved in two steps:

Validate Viable Sample

Optimally the tester should ensure that the sample is "working", meaning that it is exhibiting malicious activity. The activity of a malware sample can be checked by active logging or passive comparison. In the active logging scenario, a set of any of the following monitoring tools* may be used to observe activity:

- HIPS tools
- Sandbox tools
- System tools
- Rootkit monitors
- Network monitoring tools

*Please note that this is a general, non-exclusive list of available monitoring tools.

Testers are advised to be cautious when utilizing monitoring tools, as some malware samples behave differently if they detect the presence of certain tools. This problem can be overcome by using custom-made tools with restricted access, so that malware authors are unable or less able to detect their presence.

In a passive comparison scenario the malware is executed in an environment, which is afterwards turned off and investigated offline for changes caused by the sample. The investigation includes:

- Mounting the file system
- Tracking differences in file system, registry, boot sectors
- Monitoring network activity outside the client

When processing logs, the tester should take into account that some of the seemingly malicious activity may be caused by the runtime packer used on the sample. For example, several activities considered malicious may be performed by the packer/protector (e.g. enumeration of processes, dropping of a driver file, detection of virtual machines). Once the packer has been identified, activity known to be attributable to the packer can be removed from the activity log, and remaining entries are likely to be attributable to the investigated sample.

Validate Loadable Executable

Sometimes it is not possible to check the viability of all samples. In this case the tester should at least ensure that each tested sample can be loaded by at least one version of a relevant operating environment. Note that in case of a script malware that operating environment consists of an operating system and an appropriate script interpreter; in case of a macro virus, the operating environment consists of an operating system and an appropriate application.

Validation of loadability can be approached both with static sample analysis, or by a more reliable dynamic examination such as hooking the PE loader of various target OS and examining whether or not the OS is able to run some executable code from the sample. PE format validation, in this case, becomes the equivalent of confirming thread creation and execution within the examined process.

Thus, for example, it is appropriate to verify the following minimal criteria for a Win32 executable, which currently is the class of executables that comprise the majority of test collections:

- It has a valid section table
- It has a valid entry point
- The file size is valid, being no shorter than the size calculated from the sum of the raw section sizes
- The section alignments are valid
- The section rights are valid (entry point section is executable)

This document was adopted by AMTSO on May 7, 2009