



Metascan™ Performance Analysis

About Metascan™

Metascan enables IT professionals and software engineers to develop advanced scanning solutions using Metascan's built-in antivirus engines as well as integrating with preinstalled antivirus engines. Metascan currently has CA eTrust, Norman, ClamAV, Eset, Microworld and VirusBuster as its built-in antivirus engines, but in the future more engines will be added. The integration of the pre-installed engines along with using the built-in engines into a single multi-scanning solution improves the likelihood of malware detection as well as increase in performance.

The goal of the Metascan performance analysis was to simply observe the multiple built-in engines ability to scan various types and various sizes of files.

This report is to help an end-user or a software developer understand what Metascan™ can do as well as the performance of Metascan™.

Performance Analysis – Test I

The performance analysis was done in order to see how the different engines handled various types of files.

Metascan was installed on a Microsoft Windows XP Professional Version 2002 Service Pack 2 machine with the following specifications:

Intel® Core™2 CPU
6300 @ 1.86GHz
1.86 GHz, 2.00 GB of RAM

The following files were scanned:

File Name	Size (bytes)	Type
*Eicar.com	68	MSDOS application
*melt.exe	29184	MSDOS application
Test.pdf	314748	PDF document v1.4

Cleanfile.txt	18	Text file
testdoc.doc	24064	Microsoft Office Document (Word)
*test1.zip	2501440	Zip archive with one recursive archive
*test2.zip	266660	Zip archive with six recursive archives
*testrar.rar	165	Rar archive
*testzip.zip	347	Zip archive

* indicates that files were infected

Metascan scanned the first file using each individual built-in engine and then scanned that same file again with all six engines. A time stamp was taken from when the file was put into scan queue to when Metascan received a call-back from the engine(s) reporting whether the file was clean or if threats were found. With all six engines the time stamp ends when Metascan reports its last callback.

The second file was then scanned in the same way, the third, the fourth, and so on. Once the list of files was completed, this whole process was repeated. It was run a total of ten times. In order to get an accurate analysis of the performance of each engine as well as the performance of all six engines, the average of the ten runs per file were taken (removing the minimum and maximum times).

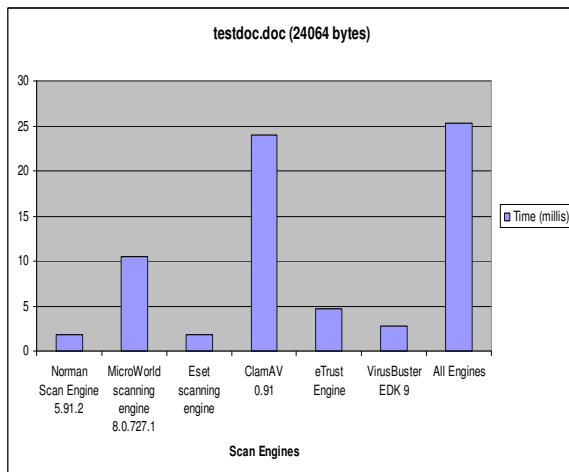
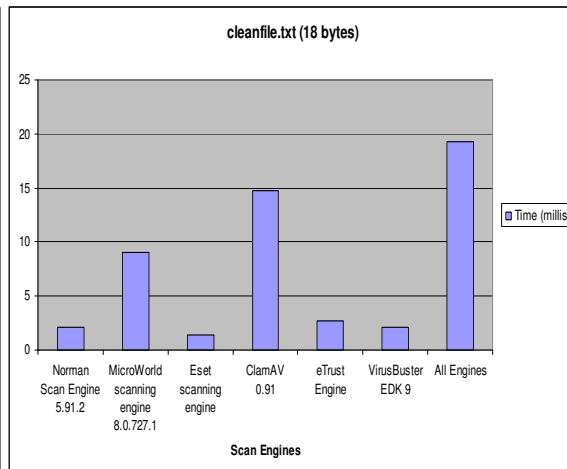
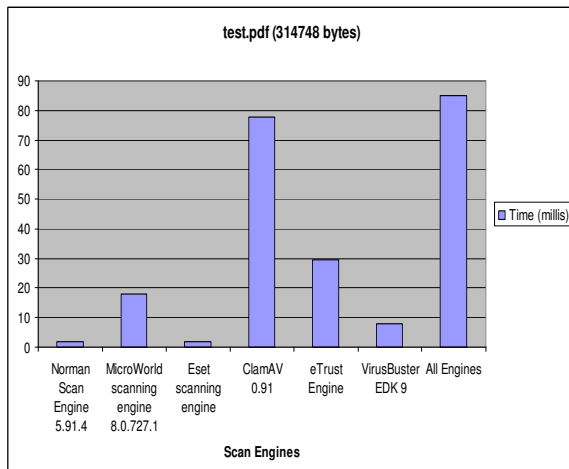
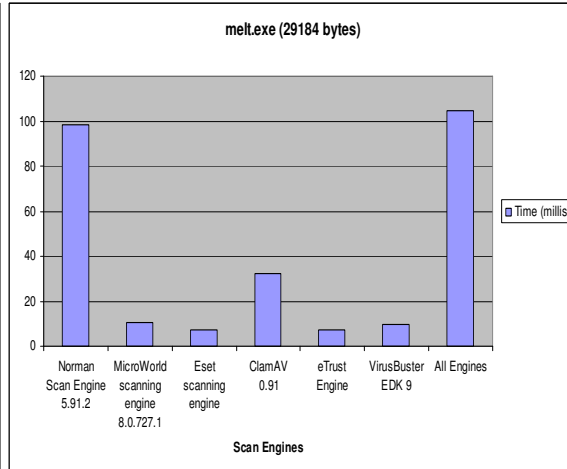
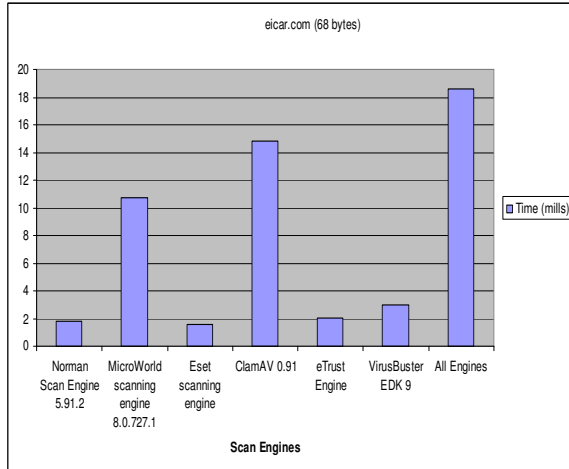
The infected files that were used in this particular test were files that all six engines reported as infected. Note that in many situations at least one engine would detect a particular file as infected while the others reported it clean.

Performance Analysis – Test II

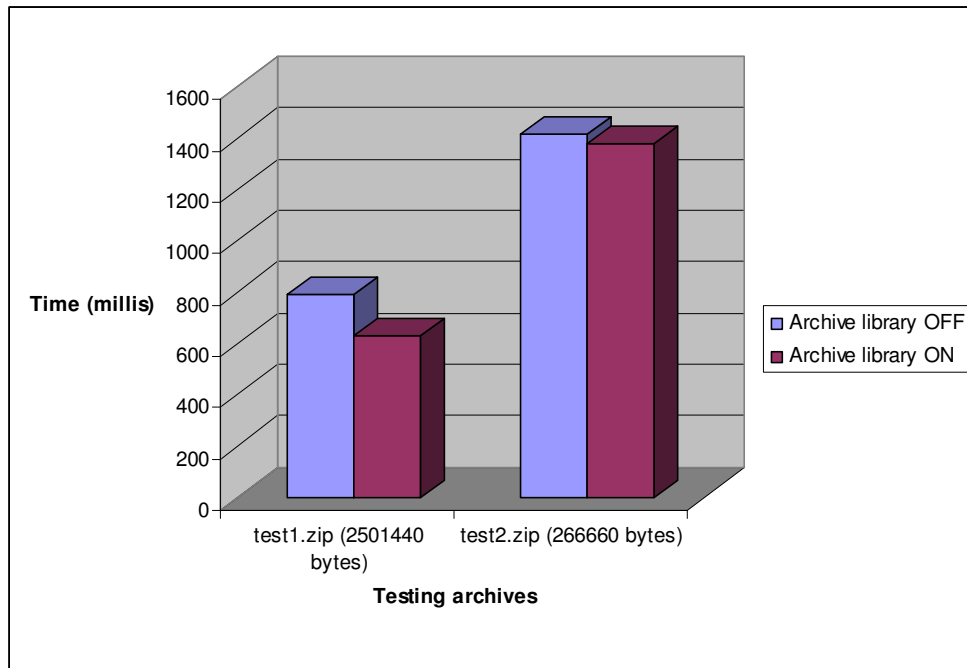
The second analysis performed was to compare the efficiency and ability of Metascan™ to scan files on the optional RAM drive. The same files that were scanned in the first analysis (see Table 1) were now placed on the optional RAM drive that is installed with Metascan™. The files then went through the same procedure.

Performance Analysis Results – Test I

The first set of graphs shows the average time (in milliseconds) it takes Metascan™ to scan each file with each individual engine as well as all six engines.



The second chart shown below compares the performance of Metascan using the Archive library versus not using the Archive library with all six scan engines. Archives are being extracted to specified temporary path and then handed off to each scan engine. Many scan engines available in the market are not capable of scanning archive contents.

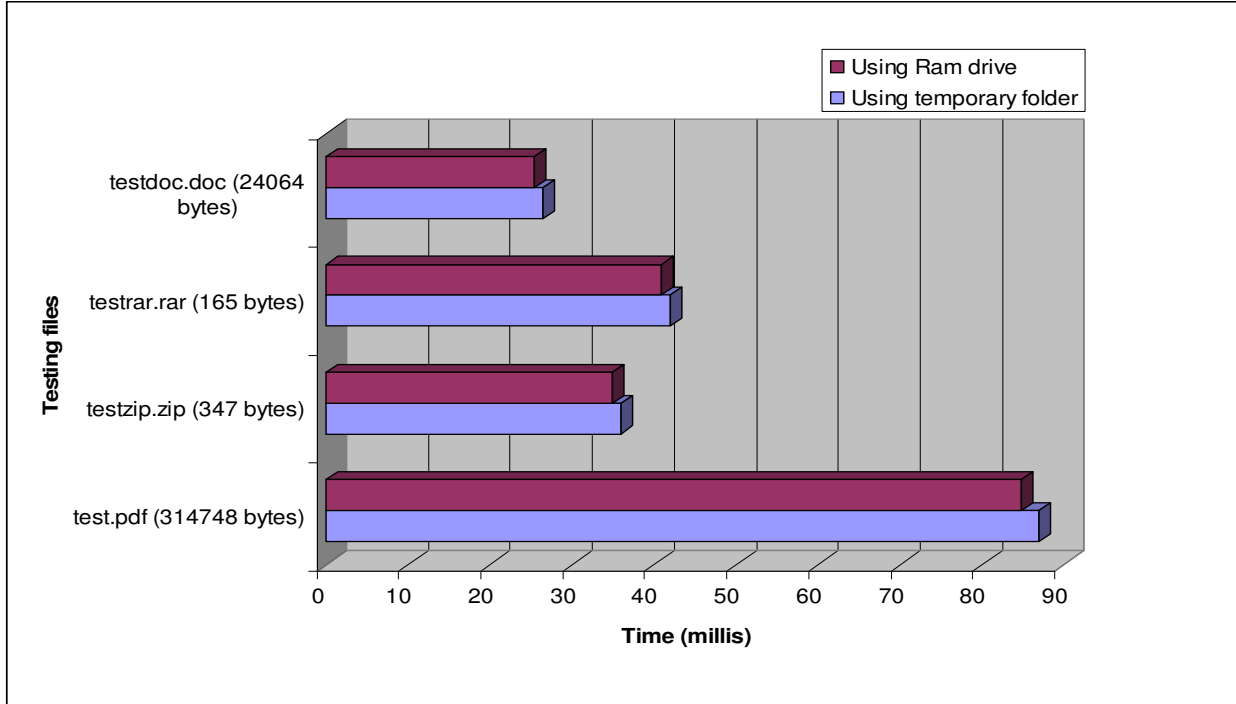


From this test you can see that Metascan delivers high scanning performance with the highest chances of threat detection combining forces of six scan engines and the advantage of archive library.

Performance Analysis Results – Test II

The graph shows the average time (in milliseconds) of all six engines scanning a particular file using a temporary folder on hard drive and on the optional RAM drive. The purpose of the graph is to illustrate how, for some particular files, Metascan has the ability to scan faster when the file is located on the optional RAM drive.

Chart 2.1 Performance testing of OPSWAT RAM disk vs. Temporary Folder



Using RAM drive will help boost performance of scanning archives and simultaneous requests. RAM drive size can be adjusted to best fit the needs of the particular configuration.