Anti-Virus Comparative

Technology Preview Report

McAfee Artemis

Date: February 2008

Last revision: 3rd June 2008

Author: Andreas Clementi

Website: http://www.av-comparatives.org

1. Introduction

In the last 2 years the detection rates of McAfee went a bit down (from ADVANCED+ to ADVANCED), but later this year McAfee will be releasing a new technology (currently code named Project Artemis) which will improve its detection rates considerably.

This new technology, having recently completed private beta and going to public beta later this month, will provide an effective and rapid reaction to new threats or threats for which no daily signature update (DATs) have been released yet.

McAfee plans to have the technology fully ready for consumer and enterprise deployment later this year. For more details you can check out http://www.mcafee.com/us/threat_center/projectartemis.html link.

2. Tested product

We tested exactly the same product version (McAfee VirusScan Plus) with the same updates (DATs from 4th February 2008) like in the comparative of February 2008 (http://www.av-comparatives.org/seiten/ergebnisse/report17.pdf) – with the only difference of one little special EXTRA.DAT (still in closed beta at the time of our testing) which activates this new functionality (can be applied to any McAfee Anti-Malware products for Microsoft Windows operating systems). As this technology requires a communication with the servers of McAfee AVERT Labs, a live internet connection is needed during the scan to take full advantage of this advanced detection, as well as having the "program heuristic" enabled in the product.

3. How it works

This new technology (Artemis) looks for suspicious PE[1] files, and when found it sends some kind of checksum (with no personal/sensitive data) to a central database server hosted by McAfee AVERT Labs. The central database server is constantly updated with new discovered malware, and is McAfee's malware queue for which no official DATs have been created so far. If a match is found in the central database, the scanner will report and handle the malware detection. The files in McAfee's queue have not been undergone any analysis, but they are crosschecked by McAfee's huge whitelists to avoid false alarms.

[1] *file format for executables, object code and DLLs, used in modern Microsoft Windows operating systems.*

By having a remotely mantained blacklist it may be able to provide faster protection to new malware than vendors which release signature updates many times at day to cover the high amounts of new malware appearing every hour.

4. Test results

Below the detection rates of McAfee (without and with Artemis):

Company		McAfee		McAfee	
Product		**McAfee VirusScan+**		**McAfee VirusScan+**	
Program version		12.0.176		12.0.176	
Engine / signature version		5200.2160 / 5222		5200.2160 / 5222	
Number of virus records		371.817		371.817	
				with Artemis	
Windows viruses	149.202	147.115	98,6%	148.326	**99,4%**
Macro viruses	95.059	95.056	~100%	95.056	~100%
Script viruses	14.284	12.855	90,0%	12.855	90,0%
Worms	190.952	188.318	98,6%	190.816	**99,9%**
Backdoors/Bots	400.986	383.059	95,5%	398.850	**99,5%**
Trojans	817.043	757.305	92,7%	808.359	**98,9%**
other malware	15.838	14.370	90,7%	15.412	**97,3%**
TOTAL	**1.683.364**	1.598.078	**94,9%**	1.669.674	**99,2%**

As it can be seen, with Artemis the detection rates over PE malware are very high.

During our tests over our clean set of files we found Artemis producing very many false alarms (over 500), but it has to be considered that this technology is still not fully tested and was an internal beta at time of testing.

Update (May 2008): we re-tested Artemis over our clean-set in May 2008 and now that McAfee has expanded its Whitelists, Artemis still produces relativly many false alarms, but at least no longer on very important/critical files.

It is to expect that the false alarm rate caused by Artemis will decrease over the next months (by keeping the high malware detection rates), as McAfee is currently activly working on expanding its Whitelists and introducing better Blacklist filtering (with separate levels for workstations and gateways).

5. Copyright and Disclaimer

Andreas Clementi, AV-Comparatives (March 2008)