



On Demand Scan Test – Project 023

Contents:

Introduction	2
Security Applications Tested	2
Malware Samples used	2
Methodology used in the Test	3
Test Results	3
MRG Awards	4

Introduction:

Whilst Malware Research Group is focusing more and more on live infection testing (blocking and removal) using realistic infection vectors, we believe there is still value in on demand tests. Although on demand testing does not fully replicate how a security application may behave in preventing infections, it does give “an” indication as to its detection capabilities and is still the only way we can assess detection using a large sample size.

Security Applications Tested

1. A-Squared Anti-Malware 4.5.0.29
2. avast Antivirus Professional 5.0.462
3. AVG Anti-Virus Professional 9.0.801
4. Avira AntiVir Premium 10.0.0.597
5. BitDefender Antivirus 13.0.20.347
6. COMODO Internet Security 4.0.138377.779
7. ESET Nod32 Antivirus 4.0.474.0
8. F-Secure Antivirus 9.22 build 15450
9. G DATA Antivirus 20.2.4.1
10. Kaspersky Anti-Virus 9.0.0.736
11. McAfee AntiVrus Plus 14.0.306
12. Microsoft Security Essentials 1.0.1961.0
13. Norton AntiVirus 17.6.0.32
14. Online Armor++ 4.0.0.35
15. VIPRE Antivirus Premium 4.0.3248

Malware Samples used:

Trojans/Backdoors – 201,296

Worms – 25,811

Windows Viruses – 4,337

Rootkits/Exploits – 9,458

Adware/Spyware – 4,749

Other Malware – 14,043

Total Malware Samples – 259,694
















60% of the samples are < 3 months old, with the remaining 40% being between 3 – 6 months old.

Methodology used in the test:

1. Windows XP Professional Service Pack 3 is installed on 15 PCs (8 in Serbia & 7 in UK) and updated with all important updates.
2. An individual antimalware application is installed using default settings on each of the 15 systems.
3. Each of the 15 systems has a folder containing the 259,694 samples placed on the desktop (where the antimalware application in question has real time on access detection, this is disabled to allow the sample to be copied to the system without detection. Once copied, the real time detection is enabled again)
4. All the antimalware applications are fully updated.
5. The test is conducted by running a full system scan with each antimalware application.
6. Once the antimalware applications have completed the scan, the tester enabled them to remove or quarantine detected samples.
7. The scan is repeated again as in step 5.
8. Any remaining samples are counted then archived and stored in our labs. (*)
9. Testing is conducted with all systems having internet access.

Test Results:

The results of the test are detailed in the table below.

A-SQUARED		99.8
Online Armor++		99.8
G-DATA		99.4
Avira		98.9
Avast		98.7
McAfee		98.6
Norton		98.4
BitDefender		98.3
F-Secure		98.1
COMODO		97.8
Nod32		97.6
Kaspersky		97.5
VIPRE		97.3
AVG		95.1
MSE		94.8

A-SQUARED and Online Armor++ returned exactly the same result, which is to be expected in an on demand test as their respective Mamutu / Oasis components are not used in static scanning.

G-Data is to be comended on a great performance as well, with a good result in the mid 99% range.

(*) Missed samples will be supplied to vendors which have a support contract with MRG.

MRG Awards:

As with most competitive events, only the top three get “medals”. Given the top top three are so close, with indeed, two of them being the same, we have decided to give the MRG “Best Overall Detection” award to:

A-Squared Anti-Malware



Online Armor++



G DATA Antivirus

