



## Comparative test of Microsoft Security Essentials - June 2010

### Contents:

Introduction	2
Security Applications Tested	2
Test Samples used	2
Methodology used in the Test	2
Test Results	3
Conclusions	3

## **Introduction:**

The launch of Microsoft Security Essentials promised the opportunity of robust, free security for all home users. MSE uses the same engine as Forefront, Microsoft's commercial, enterprise product and so should in theory offer protection on par with that provided by the top vendors.

MRG has tested MSE regularly since its release and have found that generally, its performance is below that of the main commercial product and indeed, inferior to several of the better known free products offered by these vendors.

## **Security Applications Tested:**

- Avast Home Edition 5.0.594
- Avira AntiVir Personal 10.0.0.567
- Microsoft Security Essentials 1.0.1963.0

## **Samples and Test Tools used:**

- Trojan (Alureon)
- Trojan.Downloader (Renos)
- Rogue (Security Master AV)
- Trojan.Downloader (FakeAlert)
- Trojan.Spy (Zbot)
- Rugue (FakeAV)
- Worm (Kolab)
- Trojan (Monder)
- Trojan (FraudPack)
- Email.Worm (VB)
- Trojan.Downloader (Small)
- Trojan (Pincav)
- Trojan (Start Page)
- Trojan.Downloader (Banload)
- Trojan (Starter)
- Trojan.Downloader (JS Agent)
- Backdoor (Bredolab)
- Trojan (IRCbot)
- Trojan (Buzus)
- Trojan.Downloader (Delf)
- Self Protection Tool
- MRG FM Simulator V1.0

## **Methodology used in the Test:**

1. Windows XP Professional Service Pack 3 is installed and updated with all important updates.
2. An image of the Operating System is created.
3. A clone of the Imaged system is made for each of the 3 security applications to be used in the test.
4. An individual security application is installed using default settings on each of the Cloned systems and then updated.
5. Twenty two fresh clones of the clone created in 4 are created.
6. The testing is conducted by:

- a. Downloading one of the test samples / tools using Internet Explorer to the desktop and executing it.
7. A test is deemed to have been passed by the following criteria:
  - a. The security application blocked the execution of the malware.
  - b. The security application was not terminated by the self protection tool
  - c. The security application prevented the MRG FM Simulator functioning.
8. A test is deemed to have been passed by the following criteria:
  - a. The security application failed to block the execution of the malware.
  - b. The security application was terminated by the self protection tool
  - c. The security application failed to prevent the MRG FM Simulator functioning.
9. Testing is conducted with all systems having internet access.
10. Each individual test for each security application is conducted from a unique IP address.
11. All security applications are fully functional unregistered versions or versions registered anonymously, with no connection to MRG.

**Test Results:**

The results of the test were as follows:

Application Name	Trojan (Alureon)	Trojan.Downloader (Renos)	Rogue (Security Master AV)	Trojan.Downloader (FakeAlert)	Trojan.Spy (Zbot)	Rogue (FakeAV)	Worm (Kolab)	Trojan (Monder)	Trojan (FraudPack)	Email.Worm (VB)	Trojan.Downloader (small)	Trojan (Pincav)	Trojan (Start Page)	Trojan.Downloader (Banload)	Trojan (Starter)	Trojan.Downloader (JS Agent)	Backdoor (Bredolab)	Trojan (IRCb0t)	Trojan (Buzus)	Trojan.Downloader (Delf)	Self Protection	MRG FM Simulator V1.0
Avast Home Edition 5.0.594	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✗	✓	✗	✓	✗	✓	✗
Avira AntiVir Personal 10.0.0.567	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓	✗
Microsoft Security Essentials 1.0.1963.0	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✗	✓	✓	✗	✗	✓	✗	✗

**Conclusions:**

These results fit with those we see from our in house testing. It is notable that MSE fails the self protection test. Whilst we understand it is an ongoing battle to keep up with the huge numbers of malware samples in the wild, we feel that it should be a simple task for a developer such as Microsoft to ensure their application has adequate self protection.

Microsoft has recently released MSE 2.0 Beta. We will be testing this shortly to see if it offers any improvement over V1.X.