



PCSL-Testing No.1 Report

(Date: July 3rd, 2008)

Author: Jeffrey Wu

Sample Material: 200805 "Malware-List"

Testing Method: PCSL manual (200806)

English website:

<http://www.pcsl.info/index.php>

Chinese website:

<http://www.pcsl.info/cn/index.php>

1. Testing Products

[IKARUS virus.utilities T3 \(W32 Command Line Scanner\)](#) [IKARUS Security Software GmbH](#)
[Kaspersky Internet Security 2009](#) [Kaspersky Lab](#)
[Kingsoft Internet Security 2008](#) [Kingsoft, International.](#)
[Trend Micro AntiVirus plus AntiSpyware 2008](#) [Trend Micro Incorporated.](#)
[Twister Anti-TrojanVirus V7 R3](#) [Fileseclab](#)

All the anti virus vendors mentioned above had agreed to join PCSL-Testing and PC Security Labs has the right to test their products and publish its final report in PC Security Labs' homepage.

We strongly suggest our readers not only focus on the "on demand" detection of antivirus products. Some products may offer some amazing functions such as hips, anti-leak and other additional protection modules. Also, false alarm rate is an important area we should pay attention to, we will gather as large number as clean files to hold a testing based on them. We will regularly release single product testing report to provide a comprehensive view of security products. The first single product testing will be Kingsoft Internet Security 2009.

2. Testing Method

- 1) Prepare the "Malware-List" package collected during the month before last. The malware will be divided into three main parts: Trojan horse, virus and worm. That means all the samples will be put into three individual file folders.
- 2) Testing platform: Windows XP Pro SP3 updated. The OS will be installed in VMware Workstation 6.0.3 and update. Then we create several copies of current virtual machine using the clone function.
- 3) Install every scanner in an individual virtual machine, or use command line scanner.
- 4) Set every scanner to the highest detection rate configuration (e.g. deep/redundant scan, highest heuristic, suspicious function and so

on).

- 5) Every scanner's last update time: 18:00(GMT+08:00) on first Thursday of each Month.
- 6) Copy "Malware-List" package into each virtual machine and start the on demand scanning by each scanner, and the processing mode is to delete or quarantine the samples. After finishing the scanning, we will check the samples left in the file folder and then calculate the samples' number each scanner can detect. **Detection number=Total sample number – sample number left in the original file folder.**
- 7) For "Malware-List" , we have a judging system, that is: For detecting one Trojan horse sample, each scanner can get 2 points; for detecting one worm sample, each scanner can get 1.5 points; for detecting one virus sample, each scanner can get 1 point. So each scanner can get **score=2* Trojan horse detection number+1.5* worm detection number+1* virus detection number.**
- 8) For maximum detection, the max score should be **2* Trojan horse sample number+1.5* worm sample number+1* virus sample number.**
- 9) So each scanner' s final result = **(actual score/maximum score)*100.**
- 10) Analyze and make the report pdf.

3.Testing Results

200805 "Malware-List"

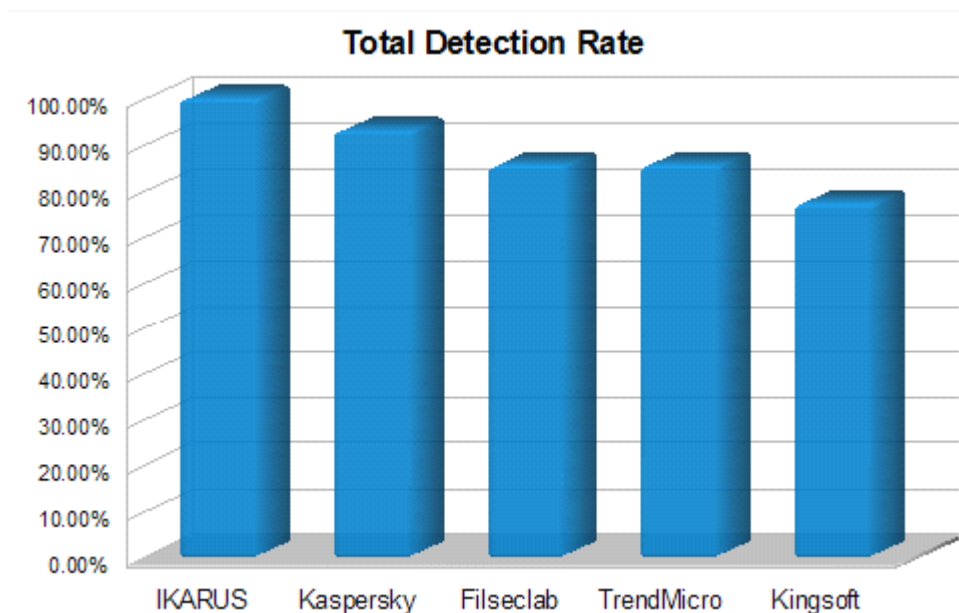
Total: 1040 Trojan: 980 Virus: 7 Worm: 53

Product detailed information

AV Product	Engine	Signature
IKARUS virus.utilities T3	1001026	71027
Kaspersky Internet Security 2009	8.0.0.357	902057
Kingsoft Internet Security 2008	N/A	2008.7.3.17
Trend Micro AntiVirus plus AntiSpyware 2008	8.710.1002	5.380.60
Twister Anti-TrojanVirus V7 R3	7.3.1.23211	8.44.24336

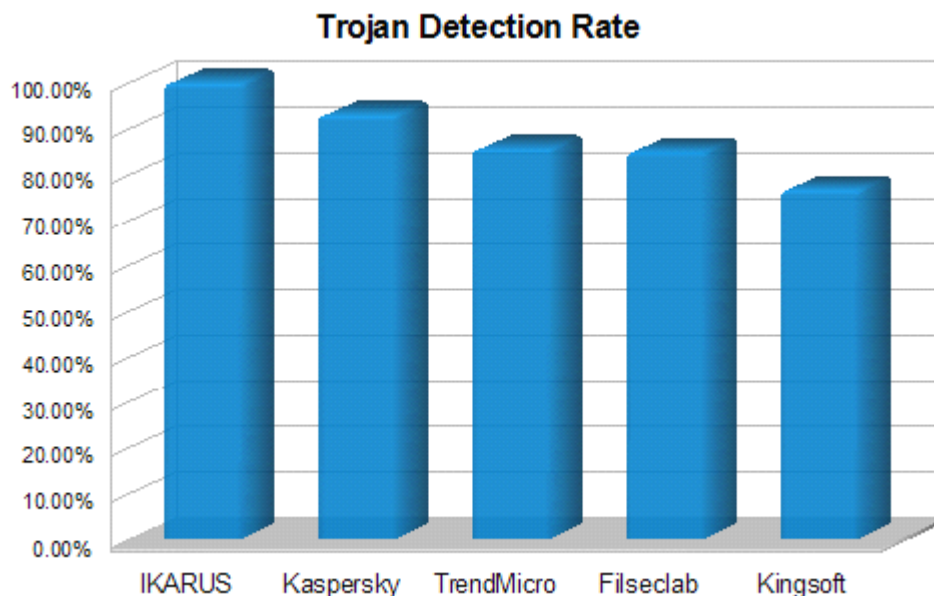
Total Detection Summary 1040 samples

AV Product	Total detection	Rate
IKARUS virus.utilities T3	1037	99.71%
Kaspersky Internet Security 2009	965	92.79%
Kingsoft Internet Security 2008	799	76.83%
Trend Micro AntiVirus plus AntiSpyware 2008	885	85.10%
Twister Anti-TrojanVirus V7 R3	886	85.19%



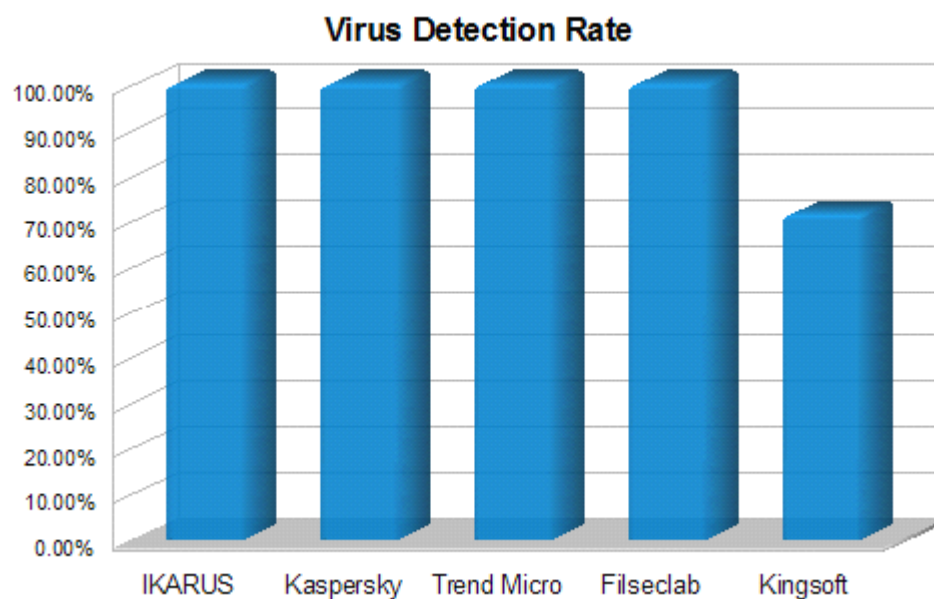
Trojan Detection Summary 980 trojan samples

AV Product	Trojan detection	Rate
IKARUS virus.utilities T3	977	99.69%
Kaspersky Internet Security 2009	909	92.76%
Kingsoft Internet Security 2008	751	76.63%
Trend Micro AntiVirus plus AntiSpyware 2008	838	85.51%
Twister Anti-TrojanVirus V7 R3	831	84.80%



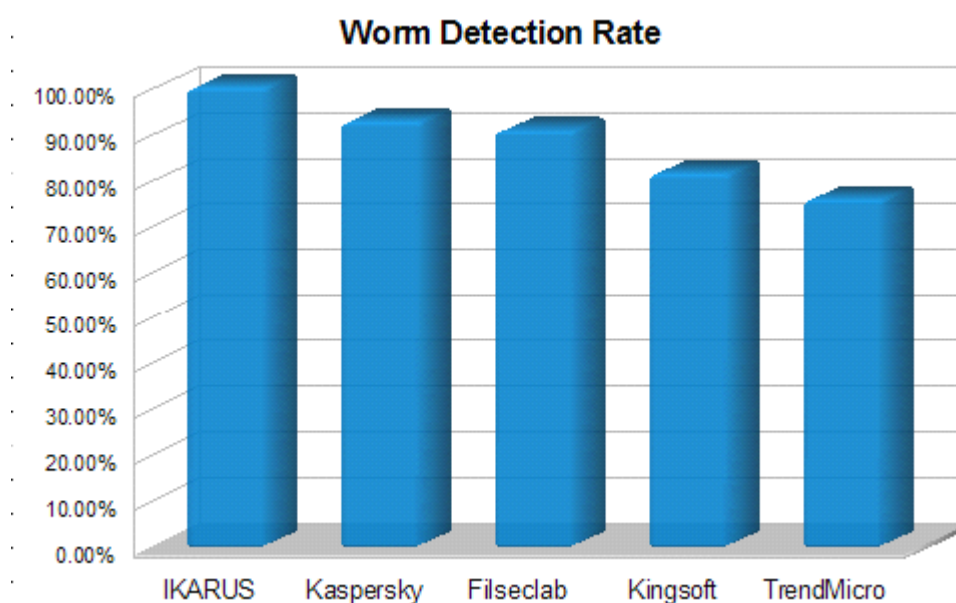
Virus Detection Summary 7 virus samples

AV Product	Virus detection	Rate
IKARUS virus.utilities T3	7	100%
Kaspersky Internet Security 2009	7	100%
Kingsoft Internet Security 2008	5	71.43%
Trend Micro AntiVirus plus AntiSpyware 2008	7	100%
Twister Anti-TrojanVirus V7 R3	7	100%



Worm Detection Summary 53 Worm samples

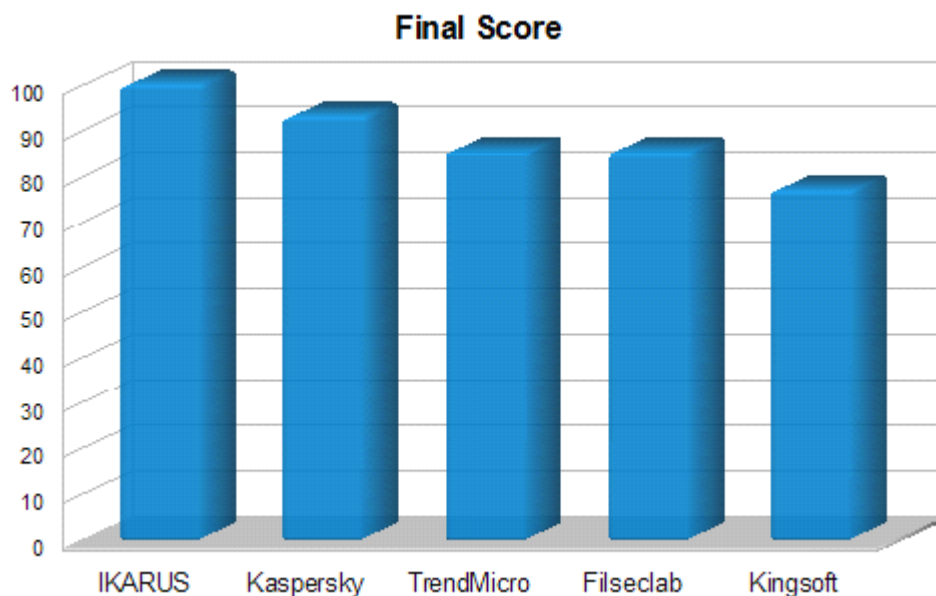
AV Product	Worm detection	Rate
IKARUS virus.utilities T3	53	100%
Kaspersky Internet Security 2009	49	92.45%
Kingsoft Internet Security 2008	43	81.13%
Trend Micro AntiVirus plus AntiSpyware 2008	40	75.47%
Twister Anti-TrojanVirus V7 R3	48	90.57%



Final Score Summary

AV Product	Trojan score	Virus score	Worm score	Total	Final Score
IKARUS virus.utilities T3	1954	7	79.5	2040.5	99.71
Kaspersky Internet Security 2009	1818	7	73.5	1898.5	92.77
Trend Micro AntiVirus plus AntiSpyware 2008	1676	7	60	1743	85.17
Twister Anti-TrojanVirus V7 R3	1662	7	72	1741	85.07
Kingsoft Internet Security 2008	1502	5	64.5	1571.5	76.79

Maximum Score = 980*2+7*1+53*1.5=2046.5



4. Copyright & Disclaimer

We focus on computer security and we try our best to protect the PC security. All the samples are from the Internet and we are not responsible for the malware samples. The research is taken in an internal network environment and we all edit the samples' extension in order to prevent incorrect manipulation by the user. And the samples are for research only and we suggest normal users not download the packages and we are not responsible for the damage they cause by themselves. In addition, we are also not responsible for the behavior taken by the outlaws.

And also, the testing report from PCSL is for reference only and our report result is free for use without modification by the AV vendor who joins our testing project. Any commercial activity wants to cite our report result please contact Jeffrey Wu through his email address (jeffrey@pcsl.info). We are not responsible for the behavior to cite, use, publish our testing report or related words without our permission. This report belongs to Jeffrey Wu (PC Security Labs).

Licensing

Copyright (c) 2008 by Jeffrey Wu

All rights reserved.

Using the materials of this testing report without mentioning the source is prohibited.