



Anti-Trojan Comparative 2006

On-demand detection of malicious software

Date: March 2006

Last revision of this report: 22th March 2006

Author: Andreas Clementi

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

1. Tested products

All products were updated the 14th March 2006 and set to use the best possible settings. The Malware Test-beds were frozen the 2nd February 2006. We will show the on-demand test results from 7 of the best and most well-known dedicated Anti-Trojan products:

Product name and version	Website
a-squared Anti-Malware Personal 1.6.5	http://www.emsisoft.com
Anti-Trojan Shield 2.1	http://www.atshield.com
Digital Patrol 5.0	http://www.proantivirus.com
Ewido Anti-Malware Plus 3.5	http://www.ewido.net
PC DoorGuard 4.2	http://www.trojanclinic.com/pdg.html
Tauscan 1.7	http://www.agnitum.com/products/tauscan
Trojan Remover 6.4.8	http://www.simplysup.com/tremover

Even if the results of some products may look low, keep in mind that most of those had relatively high scores (compared to others) and that those Anti-Trojan vendors were fair enough to allow us to show their results publicly - probably because they know that maybe their product has low on demand detection rates but is good at e.g. removing malware or at detecting malware while execution.

2. Comments

Only the 'backdoors' (including Bots), 'trojans' and 'other malware' test-sets of February 2006 were used in this test¹ (~153.000 samples). Please note that our test-sets do usually not contain files like editors, clients, harmless tools, old DOS trojans, etc.

Some Anti-Trojan products have a higher number of signatures in their databases than samples detected in this test, maybe because they detect also other things like dialers, worms, viruses or files like backdoor clients, editors, tools etc. not included in this test². This test focuses mainly only on dangerous backdoor servers and bots (~78.000), trojans (~69.000) and other malware (~6.000). Anti-Trojans are intended to use in addition to Anti-Virus software and not as replacement of an Anti-Virus product. Also dedicated Anti-Trojan products that have lower malware detection rates than Anti-Virus products make sense to use as additional layer of defense against malicious software, esp. for high risk users.

Please try Anti-Trojan products on your own system. Some products may offer additional options/features targeted to identify and remove malware (which are probably the main factors for the use of Anti-Trojan products, as the on-demand detection rate of malware does in general not look very good). There are also many other program features and important factors (e.g. compatibility, system resource usage, price, update frequency, spyware and dialer detection, etc.) to consider.

The detection rates of 25 various Anti-Virus products show that the best ones are able to detect ~99% of the used test-sets and the worst ones around ~30%. The average Anti-Virus product detects around ~75% of the used malware test-sets.

¹ In this document, with 'malware' we mean non-replicating malware like backdoors, trojans and other malware. 'Other malware' contains e.g. Flooders, Nukers, DDoS, Exploits, ActiveX and IRC malware, Rootkits, etc.

² On the other hand, it could be also just high numbers for 'marketing purposes'. Once again an example that the number of claimed signatures/records says nothing about the detection capabilities or quality of a product.

3. Summary results

As the results are in general not that high in all three categories, we will show here only the total detection rate over the three used test-sets:

Total on-demand detection rate of malware (backdoors, trojans & othermalware):

1. Ewido	73%
2. a-squared	47%
3. Digital Patrol	46%
4. Tauscan	18%
5. Anti-Trojan Shield	17%
6. PC DoorGuard	15%
7. Trojan Remover	9%

No other tested³ Anti-Trojan product detected on demand more than 20% of the used test-sets (except the first three listed).

This test demonstrates which from the Anti-Trojan products detected more or less malware (in our malware test-sets) than other Anti-Trojan products.

Anti-Trojan products have to be understood as a complement to your Anti-Virus product. As such, it is an additional security improvement/layer, because the Anti-Trojan product may offer additional protection features/tools targeted to identify and remove malware, which some Anti-Virus products may currently not have.

Due the other features that most Anti-Trojan products offer to protect the system against malware, readers should not be much concerned about the low on-demand detection rates reached by the Anti-Trojan products in this on-demand test.

We did this test (like always) for free. Due the low participation of Anti-Trojan vendors, we do not know yet if we will provide an Anti-Trojan test also next year.

We will not comment this test further and concentrate more on our on-going Anti-Virus comparatives, due that you can find below some answers to possible questions.

4. Some questions and answers

Question 1: *If dedicated Anti-Trojan products have lower on-demand detection rates than common Anti-Virus products, why it still makes sense to use them?*

Answer: Anti-Trojan products may not have the best on-demand detection rates, but usually they offer additional tools to identify active malware or to remove the malware from the system.

Some products have Intrusion Detection Systems to block the malware while execution based on its behaviour (behaviour blockers) or are very good at detecting dialers or spyware (not included in this test). Other Anti-Trojans products may for example have a memory scanner, monitor and clean the registry and/or have tools to monitor start-up programs, current connections, running processes, etc.

In addition, also the support they could give in case of new malware has to be considered: e.g. some single trojans may get added sooner by a specific Anti-Trojan vendor than by other vendors. However, this could be reached also by using a second on-demand anti-virus scanner.

³ We tested some more products, but we do not show their results here.

Question 2: Based on the results in this test, which Anti-Trojan do you suggest to use in addition to Anti-Virus software?

Answer: AV-Comparatives do only provide detection rates data and does usually not suggest the use of specific software. You have to try the software on your own system and take the decision by yourself.

Nevertheless, in this Anti-Trojan software test, Ewido has with 73% clearly a higher on-demand detection rate than the other tested Anti-Trojan products. Due that, we would probably suggest to use Ewido in addition to your Anti-Virus software.

A-squared has - based on our internal testing - an excellent on-demand detection rate of dialers, which makes it interesting to use especially for peoples which Anti-Virus product does not have a good on-demand detection rate of dialers. A-squared comes for example also with an Intrusion Detection System, that analyzes in realtime the behaviour of all running applications, which allows the software to detect new or modified Malware without the need of daily signature updates. Especially for Malware that was written for single attacks this is a good addition to any Antivirus software.

Also most other Anti-Trojan products offer various good protection methods, just try them to see how they work. Basically we suggest the use of any Anti-Trojan product (e.g. DigitalPatrol, TrojanHunter, Tauscan, Anti-Trojan Shield, PC Doorguard, TrojanRemover, TheCleaner, Anti-Trojan Elite, etc.), especially to experienced⁴ high-risk users, as all of the tested products offer various protection tools/methods, which may show their effectiveness to identify malware only after executing the malware and not in an on-demand test. But keep in mind that every additional program running in the background takes system resources.

Anti-Trojan products make sense to use in addition to Anti-Virus products if the Anti-Virus product⁵ used does not have a good detection rate of malware. If you use an Anti-Trojan, it is preferable if you use it with activated guards/protection and not only as on-demand scanner.

Question 3: I use an Anti-Virus product and an Anti-Trojan product. Do I still need a dedicated Anti-Spyware product? Which Anti-Spyware products exist?

Answer: Yes, in our opinion you anyway need also a dedicated Anti-Spyware product. Some of the most well-known Anti-Spyware products are Ad-Aware (<http://www.lavasoftusa.com>), Spybot Search&Destroy (<http://www.safer-networking.org>), SpySweeper (<http://www.webroot.com/consumer/products/spysweeper>) and Windows Defender⁶ (<http://www.microsoft.com/athome/security/spyware/software>).

Question 4: I use an Anti-Virus product, an Anti-Trojan product, an Anti-Spyware product and a Personal Firewall. Do I still need anything else?

Answer: Maybe you could think about using a backup solution just to ensure you will not lost data if your security programs fails. The two most known image backup solutions are probably Acronis TrueImage (<http://www.acronis.com>) and Norton Ghost (http://www.symantec.com/sabu/ghost/ghost_personal).

⁴ Some features require a bit knowledge from the user side in order to be able to use them properly and efficient

⁵ note that Anti-Virus products included in our tests are already a selection of very good scanners with usually high on-demand detection rates of malware

⁶ Currently in Beta2 release

Question 5: Why the Anti-Trojan product is not included in this test?

Answer: Some possible answers are:

- TrojanHunter asked us to remove its name from the tested products after they saw its results to be lower than they probably expected and probably due that they do not believe in the results they reached against our test-sets
- BOClean (<http://www.nsclean.com/boclean.html>) does currently not have an on-demand scanner
- TheCleaner (<http://www.moosoft.com>) did not reply to our invitation in time, so we will not publish their results in this report.

5. Copyright and Disclaimer

This publication is Copyright (c) 2006 by AV-Comparatives. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of Andreas Clementi, prior to any publication. AV-Comparatives and its testers cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data.

Andreas Clementi, AV-Comparatives (March 2006)