Comparative of various technologies to protect systems against malware

incl. Behavior Blockers,
Host Based Intrusion Prevention Systems,
Sandboxing and Virtualization Technologies

Date: October 2006 (2006-10)

Last revision: 31th October 2006

Author: Andreas Clementi

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

1. Introduction

Besides traditional Anti-Virus products, there are also products with different approaches when it comes to protect your system against harmful known and unknown malware. This test report will introduce you a little bit in these systems and will try to show you how effective they are. The following 9 products[1] were tested:

❖ **BufferZone Home Pro**	http://www.trustware.com
❖ **CyberHawk 1.2**	http://www.novatix.com
❖ **DefenseWall HIPS 1.7.1**	http://www.softsphere.com
❖ **GeSWall PE 2.5**	http://www.gentlesecurity.com
❖ **Kaspersky Internet Security 6.0**	http://www.kaspersky.com
❖ **PrevX1 2.0**	http://www.prevx.com
❖ **Safe'n'Sec Personal 2.5**	http://www.safensoft.com
❖ **Sandboxie 2.62**	http://www.sandboxie.com
❖ **ViGUARD Platinium 12**	http://www.viguard.com

In contrast to traditional Anti-Virus software, where malware gets detected on-access or on-demand (before you execute the malicious file), those systems work in real-time, i.e. while you execute the malicious file.

a) Behavior blockers / Host-based intrusion prevention systems: a behavior blocker monitors the activity of programs and operating system. If a program tries to do a potentially harmful activity, the behavior blocker will stop the program before it affects the system and ask you what to do: let the program continue to execute or blocking the program. The decision about blocking/allowing will in most cases be taken by yourself, so you need to know what and when an action is malicious or benign, otherwise it could even happen that you compromise your system or legitimate programs functionality. Depending on how sophisticated the rules of the behavior blocker are, you will get few or many prompts from the program when you e.g. try to run a legitimate application. Behavior blockers have to find a deal between security and false alarms: if they block anything, the false alarms might be high – if they block only few actions, the false alarms / user prompts are reduced. Traditional behavior blockers only warn you about suspicious activities, they do not “detect” malware.

b) Sandboxing / Virtualization systems: a virtualization system protects your system by running software in a simulated system – a sandbox. Every harmful action that a malware does is done in the simulated system and does not affect the real host system files. They do not tell if an application is malicious or not. Some of those virtualization tools will also ask you if you want to let a program run in the sandbox or to add it to the trusted applications list.

c) Access control policy: the difference between sandboxing and an access control policy is that an access control policy does not focus on the separation between sandbox and the host system, but rather on the damage prevention, keeping as much links as possible for usability reasons.

In any case, you will have to check those various systems on your PC in order to evaluate if you like them or not.

[1] ISS Proventia Desktop was also invited - but unfortuantly, the invitations remained unreplied.

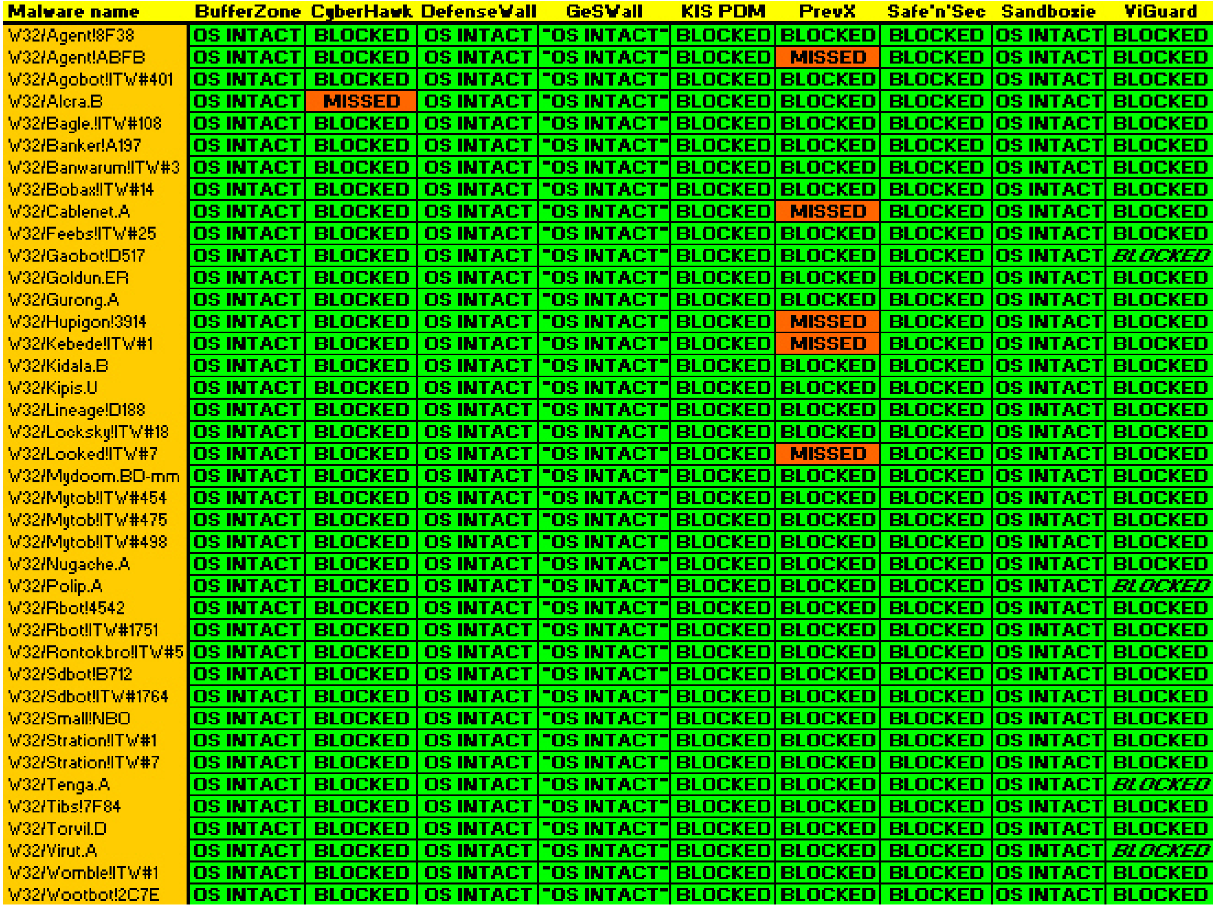
2. Test-set

For testing those products, we executed the following malware and looked if their malicious actions were blocked and/or if any system was compromised. The following 40 actual spreading or new samples were used for this test:

W32/Agent!8F38, W32/Agent!ABFB, W32/Agobot!ITW#401, W32/Alcra.B, W32/Bagle!ITW#108, W32/Banker!A197, W32/Banwarum!ITW#3, W32/Bobax!ITW#14, W32/Cablenet.A, W32/Feebs!ITW#25, W32/Gaobot!D517, W32/Goldun.ER, W32/Gurong.A, W32/Hupigon!3914, W32/Kebede!ITW#1, W32/Kidala.B, W32/Kipis.U, W32/Lineage!D188, W32/Locksky!ITW#18, W32/Looked!ITW#7, W32/Mydoom.BD-mm, W32/Mytob!ITW#454, W32/Mytob!ITW#475, W32/Mytob!ITW#498, W32/Nugache.A, W32/Polip.A, W32/Rbot!4542, W32/Rbot!ITW#1751, W32/Rontokbro!ITW#5, W32/Sdbot!B712, W32/Sdbot!ITW#1764, W32/Small!NBO, W32/Stration!ITW#1, W32/Stration!ITW#7, W32/Tenga.A, W32/Tibs!7F84, W32/Torvil.D, W32/Virut.A, W32/Womble!ITW#1, W32/Wootbot!2C7E.

3. Test results

Below the test results of the tested products:



Malware name	BufferZone	CyberHawk	DefenseWall	GeSWall	KIS PDM	PrevX	Safe'n'Sec	Sandboxie	ViGuard
W32/Agent!8F38	OS INTACT	BLOCKED	OS INTACT	"OS INTACT"	BLOCKED	BLOCKED	BLOCKED	OS INTACT	BLOCKED
W32/Agent!ABFB	OS INTACT	BLOCKED	OS INTACT	"OS INTACT"	BLOCKED	MISSED	BLOCKED	OS INTACT	BLOCKED
W32/Agobot!ITW#401	OS INTACT	BLOCKED	OS INTACT	"OS INTACT"	BLOCKED	BLOCKED	BLOCKED	OS INTACT	BLOCKED
W32/Alcra.B	OS INTACT	MISSED	OS INTACT	"OS INTACT"	BLOCKED	BLOCKED	BLOCKED	OS INTACT	BLOCKED
W32/Bagle.!ITW#108	OS INTACT	BLOCKED	OS INTACT	"OS INTACT"	BLOCKED	BLOCKED	BLOCKED	OS INTACT	BLOCKED
W32/Banker!A197	OS INTACT	BLOCKED	OS INTACT	"OS INTACT"	BLOCKED	BLOCKED	BLOCKED	OS INTACT	BLOCKED
W32/Banwarum!ITW#3	OS INTACT	BLOCKED	OS INTACT	"OS INTACT"	BLOCKED	BLOCKED	BLOCKED	OS INTACT	BLOCKED
W32/Bobax!ITW#14	OS INTACT	BLOCKED	OS INTACT	"OS INTACT"	BLOCKED	BLOCKED	BLOCKED	OS INTACT	BLOCKED
W32/Cablenet.A	OS INTACT	BLOCKED	OS INTACT	"OS INTACT"	BLOCKED	MISSED	BLOCKED	OS INTACT	BLOCKED
W32/Feebs!ITW#25	OS INTACT	BLOCKED	OS INTACT	"OS INTACT"	BLOCKED	BLOCKED	BLOCKED	OS INTACT	BLOCKED
W32/Gaobot!D517	OS INTACT	BLOCKED	OS INTACT	"OS INTACT"	BLOCKED	BLOCKED	BLOCKED	OS INTACT	*BLOCKED*
W32/Goldun.ER	OS INTACT	BLOCKED	OS INTACT	"OS INTACT"	BLOCKED	BLOCKED	BLOCKED	OS INTACT	BLOCKED
W32/Gurong.A	OS INTACT	BLOCKED	OS INTACT	"OS INTACT"	BLOCKED	BLOCKED	BLOCKED	OS INTACT	BLOCKED
W32/Hupigon!3914	OS INTACT	BLOCKED	OS INTACT	"OS INTACT"	BLOCKED	MISSED	BLOCKED	OS INTACT	BLOCKED
W32/Kebede!ITW#1	OS INTACT	BLOCKED	OS INTACT	"OS INTACT"	BLOCKED	MISSED	BLOCKED	OS INTACT	BLOCKED
W32/Kidala.B	OS INTACT	BLOCKED	OS INTACT	"OS INTACT"	BLOCKED	BLOCKED	BLOCKED	OS INTACT	BLOCKED
W32/Kipis.U	OS INTACT	BLOCKED	OS INTACT	"OS INTACT"	BLOCKED	BLOCKED	BLOCKED	OS INTACT	BLOCKED
W32/Lineage!D188	OS INTACT	BLOCKED	OS INTACT	"OS INTACT"	BLOCKED	BLOCKED	BLOCKED	OS INTACT	BLOCKED
W32/Locksky!ITW#18	OS INTACT	BLOCKED	OS INTACT	"OS INTACT"	BLOCKED	BLOCKED	BLOCKED	OS INTACT	BLOCKED
W32/Looked!ITW#7	OS INTACT	BLOCKED	OS INTACT	"OS INTACT"	BLOCKED	MISSED	BLOCKED	OS INTACT	BLOCKED
W32/Mydoom.BD-mm	OS INTACT	BLOCKED	OS INTACT	"OS INTACT"	BLOCKED	BLOCKED	BLOCKED	OS INTACT	BLOCKED
W32/Mytob!ITW#454	OS INTACT	BLOCKED	OS INTACT	"OS INTACT"	BLOCKED	BLOCKED	BLOCKED	OS INTACT	BLOCKED
W32/Mytob!ITW#475	OS INTACT	BLOCKED	OS INTACT	"OS INTACT"	BLOCKED	BLOCKED	BLOCKED	OS INTACT	BLOCKED
W32/Mytob!ITW#498	OS INTACT	BLOCKED	OS INTACT	"OS INTACT"	BLOCKED	BLOCKED	BLOCKED	OS INTACT	BLOCKED
W32/Nugache.A	OS INTACT	BLOCKED	OS INTACT	"OS INTACT"	BLOCKED	BLOCKED	BLOCKED	OS INTACT	BLOCKED
W32/Polip.A	OS INTACT	BLOCKED	OS INTACT	"OS INTACT"	BLOCKED	BLOCKED	BLOCKED	OS INTACT	*BLOCKED*
W32/Rbot!4542	OS INTACT	BLOCKED	OS INTACT	"OS INTACT"	BLOCKED	BLOCKED	BLOCKED	OS INTACT	BLOCKED
W32/Rbot!ITW#1751	OS INTACT	BLOCKED	OS INTACT	"OS INTACT"	BLOCKED	BLOCKED	BLOCKED	OS INTACT	BLOCKED
W32/Rontokbro!ITW#5	OS INTACT	BLOCKED	OS INTACT	"OS INTACT"	BLOCKED	BLOCKED	BLOCKED	OS INTACT	BLOCKED
W32/Sdbot!B712	OS INTACT	BLOCKED	OS INTACT	"OS INTACT"	BLOCKED	BLOCKED	BLOCKED	OS INTACT	BLOCKED
W32/Sdbot!ITW#1764	OS INTACT	BLOCKED	OS INTACT	"OS INTACT"	BLOCKED	BLOCKED	BLOCKED	OS INTACT	BLOCKED
W32/Small!NBO	OS INTACT	BLOCKED	OS INTACT	"OS INTACT"	BLOCKED	BLOCKED	BLOCKED	OS INTACT	BLOCKED
W32/Stration!ITW#1	OS INTACT	BLOCKED	OS INTACT	"OS INTACT"	BLOCKED	BLOCKED	BLOCKED	OS INTACT	BLOCKED
W32/Stration!ITW#7	OS INTACT	BLOCKED	OS INTACT	"OS INTACT"	BLOCKED	BLOCKED	BLOCKED	OS INTACT	BLOCKED
W32/Tenga.A	OS INTACT	BLOCKED	OS INTACT	"OS INTACT"	BLOCKED	BLOCKED	BLOCKED	OS INTACT	*BLOCKED*
W32/Tibs!7F84	OS INTACT	BLOCKED	OS INTACT	"OS INTACT"	BLOCKED	BLOCKED	BLOCKED	OS INTACT	BLOCKED
W32/Torvil.D	OS INTACT	BLOCKED	OS INTACT	"OS INTACT"	BLOCKED	BLOCKED	BLOCKED	OS INTACT	BLOCKED
W32/Virut.A	OS INTACT	BLOCKED	OS INTACT	"OS INTACT"	BLOCKED	BLOCKED	BLOCKED	OS INTACT	*BLOCKED*
W32/Womble!ITW#1	OS INTACT	BLOCKED	OS INTACT	"OS INTACT"	BLOCKED	BLOCKED	BLOCKED	OS INTACT	BLOCKED
W32/Wootbot!2C7E	OS INTACT	BLOCKED	OS INTACT	"OS INTACT"	BLOCKED	BLOCKED	BLOCKED	OS INTACT	BLOCKED

BLOCKED: malicious behavior of the malware was blocked.
OS INTACT: the sandboxes prevented that the malware modified/accessed the real system.
"OS INTACT": the access control policy prevented that the malware modified/accessed the real system, but the isolated malware processes were not terminated.
MISSED: the program was not able to recognize the malicious activity and/or to protect the system by blocking the malware.
BLOCKED: malware blocked in interactive mode but not in automatic mode.

4. Comments

(!) Please note the version numbers of the tested AV products: most of those product versions were released very recently and are able to detect more malicious activities than the previous versions. You are urged to update to the newest program versions and to keep them updated (updates to cover the misses in this test are in the meantime already released).

BufferZone: All unknown programs are executed in the virtual environment of BufferZone. Any malicious action is done within it, leaving the real OS intact. With some few clicks, all programs that are currently running within the BufferZone can be terminated and the files inside the BufferZone removed. The interface is intuitive also for non-experienced users. From BufferZone's website (which applies also to most other sandbox programs): *„BufferZone does not try to detect/block suspicious behavior. What it does is run Internet programs (Web browsers, P2P, Instant Messaging) in an environment where these programs (and their downloads + child processes) do not affect the real file-system + registry. "*

CyberHawk: is easy to install and to use, does not require configuration and blocks/warns about potentially dangerous activities, protecting the system by most threats. It had 1 missed sample. Detection of that kind of samples will be added in next release of CyberHawk.

DefenseWall: is a sandbox HIPS which categories the files in trusted/untrusted. Unknown files should be executed as untrusted. DefenseWall allows to terminate the process and shows all files that e.g. a malicious application created or added registry entries – they can be removed from the system by using the Rollback function. DefenseWall does not tell you if a file is malicious or not.

GeSWall: is an access control policy. Depending on which security level is used, an action like e.g. isolation is done automatically without pop-up's. As there is no option to terminate processes of isolated programs, they have to be killed manually, which could have affect to the system performance if a user does not do it. Due that, the user could receive tray notifications about which actions were denied, but can not terminate isolated processes. Anyway, due to the protection of auto-run settings and prevention of services/drivers installation, those processes are alive until user logoff as the system forces termination at this stage anyway and there are no settings to schedule an execution. GeSWall can be used to isolate critical applications, which may serve as entry points for the attacks. These applications are browsers, e-mail, chat, P2P, IRC, multimedia, viewers, etc. GeSWall isolates the "entry points" and tracks down the files coming through these entry points, in order to prevent damage. Actually, GeSWall is aware and can identify about 50 "entry point" applications for which it applies an isolation policy with respect to their particular requirements. GeSWall consider all present resources (files/registry/processes/etc.) as trusted and prevents their modifications. The rules grant access for particular resources required by individual applications. GeSWall protects against modification of system resources, reading confidential files, keylogging, prevents auto-run settings, etc.

KIS PDM: blocked all harmful actions and categorized them correctly (e.g. Trojan.generic, Invader, etc.) and is able to rollback changes made by the malware.

Prevx1: blocks malware based on its behavior and/or based on a list of known malicious files. If an user runs a malicious file that is not recognized based on its behavior or is not already included e.g. in the user community database (for which you need to be online to access it and use that capability), it will prompt the user what to do with the file: if the user knows that the file is safe he can run it, otherwise he is suggested to block the execution. Some users may not be able to be 100% sure that a file is clean and therefore they have to rely on software decision for that. Prevx contains also e.g. nice monitoring tools to see how a program behaves and what it does. PrevX has now fixed the detection for the 5 misses.

Safe'n'Sec: tells in detail what is going to happen if a suspicious behavior is detected and lets in most cases the user decide what to do further with the file (block it or execute it), but usually with the strong suggest to block the actions and details about why (which helps the user to take the correct decision.

Sandboxie: malicious applications executed in the sandbox remain in the sandbox leaving the real system intact. As it does not tell to a user whether a file run within the sandbox is doing something malicious or not, it is maybe not ideal for every user, but a useful tool to protect against malware that comes thru downloaded files and email clients, browsers, file sharing clients, etc.

ViGuard: is a simple little program, which does it jobs: it alerts you about dangerous programs based on their activities and blocks them as such. Does not have any noticeable system impact. ViGuard had a serious bug in the automatic mode (in which ViGuard was not able to find 5 samples, but blocked them all in the interactive mode), which has been patched in the meantime.

Note: *the above comments are based on the opinions of the tester. The tester strongly suggests to readers to try the above products in order to build up their own opinion over the various tools.*

5. Final notes

The technologies (behavior-blocker, HIPS, sandboxes, etc.) tested in this comparative showed that most of them are able to protect very well a system against malware, even if only a small set of various actual malware was used for this test. Keep in mind that even those products may not always be 100% foolproof (e.g. due bugs, „non-monitored“ functions etc.) - or, if they would be, its use could be time-consuming/annoying for the user.

The tested products should not be considered as a replacement to Anti-Virus software – they should be used in addition to Anti-Virus software. Many well-known AV products already include or will in future include modules like behavior-blockers or similar technologies, which will by the very last attempt/chance to detect malware (as it works while the file is already being executed) if all other detection mechanism in the AV software failed.

Results of Behavior-blockers / Sandboxes (which work on-execution) can not be applied to results reached e.g. thru signature / heuristic detection (which work usually on-demand and on-access).

While Anti-Virus products usually take the decision for the user about the malignity of a file, behavior-blockers may warn the user about suspicious activity and e.g. let the user take the verdict if a file is malicious or if a file is benign/legitimate and does only flag a false alert of the behavior-blocker. Even if nowadays most behavior-blockers try to minimize the number of required user interactivity, it will probably always remain target for false alerts and possible user’s wrong decisions.

Beside that, we suggest readers to try those various products on their PC’s, in order to evaluate the number of alerts they get during their work, the additional system impact due the products and if they like to work with such tools on their PC.

6. 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 (October 2006)