Testing of antivirus software for the detection of Zero-day threats (test I)

Thu, 11/26/2009 - 15:48 — Ilya Shabanov

Many antivirus malware protection tests performed round the world were criticized by professionals as they considered them synthetic and far from reality. The first and the main claim was that only some antivirus protection components (such as classical signature detect or heuristics) are tested during the file collection test launch. At the same time, no contribution of other technologies (such as behavioral analysis, HIPS or reputation services, firewall/IDS, HTTP on-the-fly traffic, etc.) is taken into consideration.

The second sound reason is that a real user does not store and launch any old malware on its hard drive. As a rule, only Zero-day samples penetrate there and no antivirus can protect against them.

The work efficiency can also to some extent depend on the penetration method as some antivirus software can eliminate the infection threat at the stage of malware script launch at the web-page, others do that during loaders activation downloaded with exploit, and the third ones do it even later, with the installed malware start.

In this test we analyzed the complex antivirus protection effectiveness to Zero-day malware spread via websites.

We collected links to infected websites from different sources. As a rule, everyone can come across such links in search engines, E-mail, ICQ, Skype and other instant messengers or social networks.

Key results of the testing

Award	Products
 **Platinum Zero-day Protection Award**	DefenseWall 2.56
 **Gold Zero-day**	Kaspersky Internet Security 2010 Comodo Internet Security 3.9 Trend Micro Internet Security 2009

Protection Award	
 **Silver Zero-day Protection Award**	Sophos Anti-Virus 7.6 Safe'n'Sec Personal 3.5 Avira Premium Security Suite 9.0 Norton Internet Security 2009 Avast Antivirus Professional 4.8
 **Bronze Zero-day Protection Award**	Eset Smart Security 4.0 AVG Internet Security 8.5 Microsoft Security Essential 1.0 G-DATA Internet Security 2010
Failed	F-Secure Internet Security 2009 McAfee Internet Security Suite 13 Outpost Security Suite 2009 Panda Internet Security 2010 BitDefender Internet Security 2009 Dr.Web Security Space 5.0

Eighteen antivirus popular antivirus programs participating in this testing included:

1. Avast Antivirus Professional 4.8-1335
2. AVG Internet Security 8.5.386
3. Avira Premium Security Suite 9.0.0.377
4. BitDefender Internet Security 2009 (12.0.12)
5. Comodo Internet Security 3.9.95478.509
6. Dr.Web Security Space 5.0.1.06018
7. Eset Smart Security 4.0.437
8. F-Secure Internet Security 2009 (9.00 build 149)
9. G DATA Internet Security 2010 (20.0.2)
10. Kaspersky Internet Security 2010 (9.0.0.459)
11. McAfee Internet Security Suite 13.11
12. Microsoft Security Essential 1.0.2140.0
13. Norton Internet Security 2009 (16.5.0.135)
14. Outpost Security Suite 2009 (6.5.5.2535.385.0692)
15. Panda Internet Security 2010 (15.00.00)
16. Sophos Anti-Virus 7.6.9
17. Trend Micro Internet Security 2009 (17.1.1250/8.913.1006)
18. * VBA32 Workstation 3.12.10.10

* VBA32 Workstation Antivirus was disqualified as some technical problems arose during the testing process and thus a part of the results was lost.

Also in the test participated two specialized HIPS (Hosted Intrusion Prevention System):

1. DefenseWall HIPS 2.56
2. Safe'n'Sec Personal 3.5.0.490

According to the testing methodology we selected 36 working URL to the websites with Zero-day infection which were used to measure the protection efficiency.

Evaluating the effectiveness of antivirus protection to Zero-day malware

The final results of antivirus software and HIPS comparative testing are given below in Diagram and Table 1.

Diagram 1: Different protection software efficiency against Zero-day threats

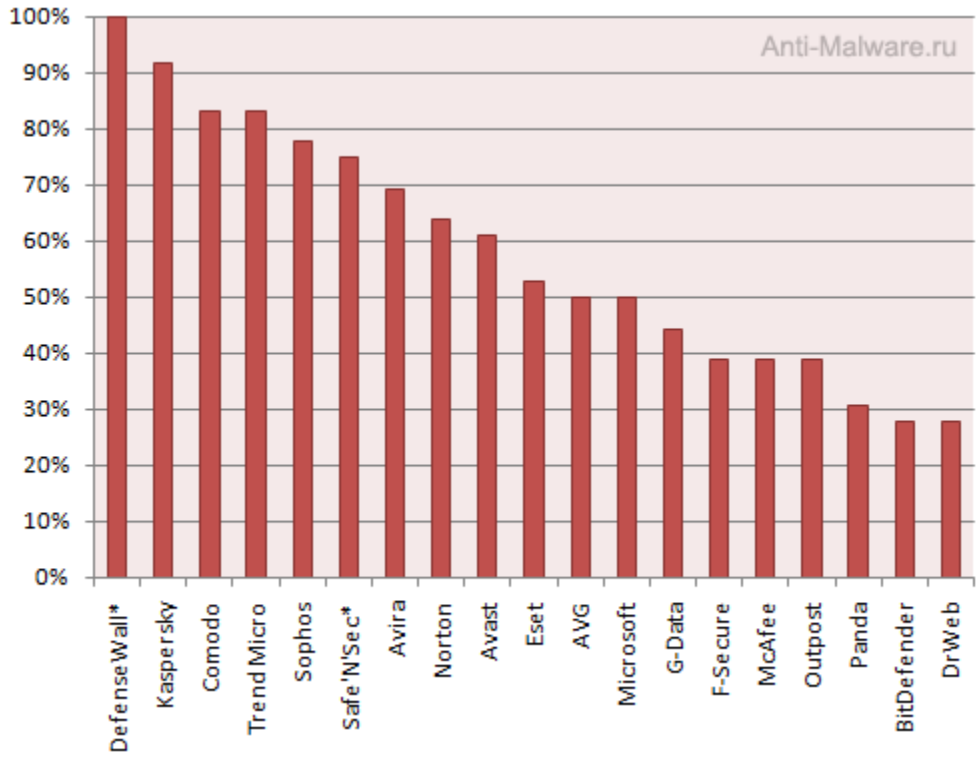

Table 1: Antivirus software efficiency against Zero-day threats

Antivirus	Points	% of maximum	Award
DefenseWall*	36	100%	Platinum Zero-Day Protection Award

			Platinum Zero-day Protection Award
Kaspersky	33	92%	
Comodo	30	83%	
Trend Micro	30	83%	 Gold Zero-day Protection Award
Sophos	28	78%	
Safe'N'Sec*	27	75%	
Avira	25	69%	
Norton	23	64%	
Avast	22	61%	 Silver Zero-day Protection Award
Eset	19	53%	
AVG	18	50%	
Microsoft	18	50%	
G-Data	16	44%	 Bronze Zero-day Protection Award
F-Secure	14	39%	
McAfee	14	39%	
Outpost	14	39%	
Panda	11	31%	
BitDefender	10	28%	
Dr.Web	10	28%	Не прошли тест

According to the test results, DefenseWall HIPS turned to be the most effective protection against malware as it managed to prevent 100% of infections. So, it is the only one that won **Platinum Zero-day Protection Award**.

The antivirus products showed very good results: Kaspersky Internet Security, Comodo Internet Security and Trend Micro Internet Security, that prevented 80% of infections and won **Gold Zero-day Protection Award**. If the results for the first of them were quite expected after the analogous test last year, the results for other two were quite unexpected.

Sophos Anti-Virus, Safe'n'Sec Personal, Avira Premium Security Suite, Norton Internet Security and Avast Antivirus Professional were quite effective against Zero-day malware and won **Silver Zero-day Protection Award**. Norton and Avast showed considerable progress in Zero-day threats protection as compared to our previous preliminary testing.

Eset Smart Security, AVG Internet Security, Microsoft Security Essential and G-DATA Internet Security turned to be a little bit worse and overcame a 40% level, so they won **Bronze Zero-day Protection Award**. It is worth mentioning that a new free Microsoft antivirus has quite a good debut and outscored many paid competitors.

All the other antiviruses such as F-Secure Internet Security, McAfee Internet Security Suite, Outpost Security Suite, Panda Internet Security, BitDefender Internet Security and Dr.Web Security Space failed the test. Unfortunately, they can be considered as effective protection against malware. The results for BitDefender and Dr.Web wend down as compared to the preliminary testing.

Ilya Shabanov, Managing Partner at Anti-Malware Test Lab:

"This dynamic antivirus and HIPS software testing for protection against Zero-day threats demonstrated a great technological gap between the leaders in this industry and the players that lag behind. It is just impossible to notice this gap by the old, outdated tests checking millions of ancient malware samples the essential part of which has passed into history. They do not reflect the reality and we can clearly see that by this test results."

"Multi-layered protection and developing proactive and reputation technologies – these are the attributes of reliable antivirus protection. The vendors that understand the importance of these technologies are now the leaders of this test and showed a considerable progress in that area. And we hope the losers will come to certain conclusions and we will see progress in protection effectiveness next year."

Vasiliy Berdnikov, Head of testing department at Anti-Malware Test Lab:

"Currently the most cases of the users' infection with malware take place during web-surfing. It can be an infected site link sent via e-mail, ICQ, social network messages or visiting a potentially dangerous site as well as via legitimate sites cracked or infected by cybercriminals. In this case infection comes through vulnerability in browser, its components and plugins such as Adobe Acrobat Reader, Flash Player, etc.

An antivirus can stop infection at the earliest stages starting from blocking the site that is on the blacklists, signature or heuristic detecting of script-exploit or downloader. Further infection can be stopped through blocking shell-code, detecting malware files, suspicious behavior or using sandbox technology when the browser and all the generated processes are launched in a limited environment that does not allow a malware code to infect the core system. We can find all these technologies in tested products. The results prove that sandbox technology, behavioral analysis and other attack early detecting technologies are the most effective and reliable web-threats protection."