Результаты теста антивирусов на защиту от новейших (Zero-day) вредоносных программ (ноябрь 2009)

В данном тестировании была изучена **комплексная эффективность** антивирусов по противодействию новейшим образцам вредоносных программ, передаваемых пользователям **наиболее распространенным сейчас способом** - через зараженные веб-сайты.
Были собраны ссылки на зараженные сайты из различных источников. Как правило, на такие ссылки каждый из нас натыкается в поисковиках, получает по e-mail, ICQ или другие средства интернет коммуникации, включая социальные сети.
Тест проводился в период с 7 июля по 22 октября 2009 года. Перед началом теста производилась подготовка среды тестирования. Для этого под управлением VMware Workstation 6.0 был создан набор чистых виртуальных машин, на которые была установлена операционная система Microsoft Windows XP Pro SP3 (последние обновления намеренно не ставились). На каждую машину по отдельности была установлена своя программа защиты из числа приведенных ниже.

В сравнении участвовали:

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, он же СТРИМ.Антивирус)
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 Antivirus 7.6.9
17. Trend Micro Internet Security 2009 (17.1.1250/8.913.1006)
18. VBA32 Workstation 3.12.10.10

Также в тесте участвовали две специальные программы для проактивной защиты от новейших видов угроз класса HIPS (Hosted Intrusion Prevention System):

1. DefenceWall HIPS 2.56
2. **Safe'n'Sec Personal 3.5.0.490**

Отбор вредоносных программ
Для теста выбирались ссылки на сайты, зараженные только новейшими образцами вредоносных программ. Что означает «новейшие»? Это означает, что эти загружаемые по ссылкам образцы вредоносных программ не должны были детектироваться файловыми антивирусами более чем 20% из списка тестируемых продуктов, что проверялось через сервис VirusTotal (всего на этом сервисе подключено 41 различный антивирусный движок). Если отобранные самплы и детектировались кем-то, то вердикты, как правило, были неточными (подозрение на заражение или упакованный объект).
Количество образов, удовлетворяющих таким требованиям, было очень небольшим, что существенно отразилось на размере итоговой выборки и сроках тестирования. Всего более за несколько месяцев тестирования было отобрано 36 рабочих ссылок на новейшие вредоносные программы, которые и использовались в тесте.

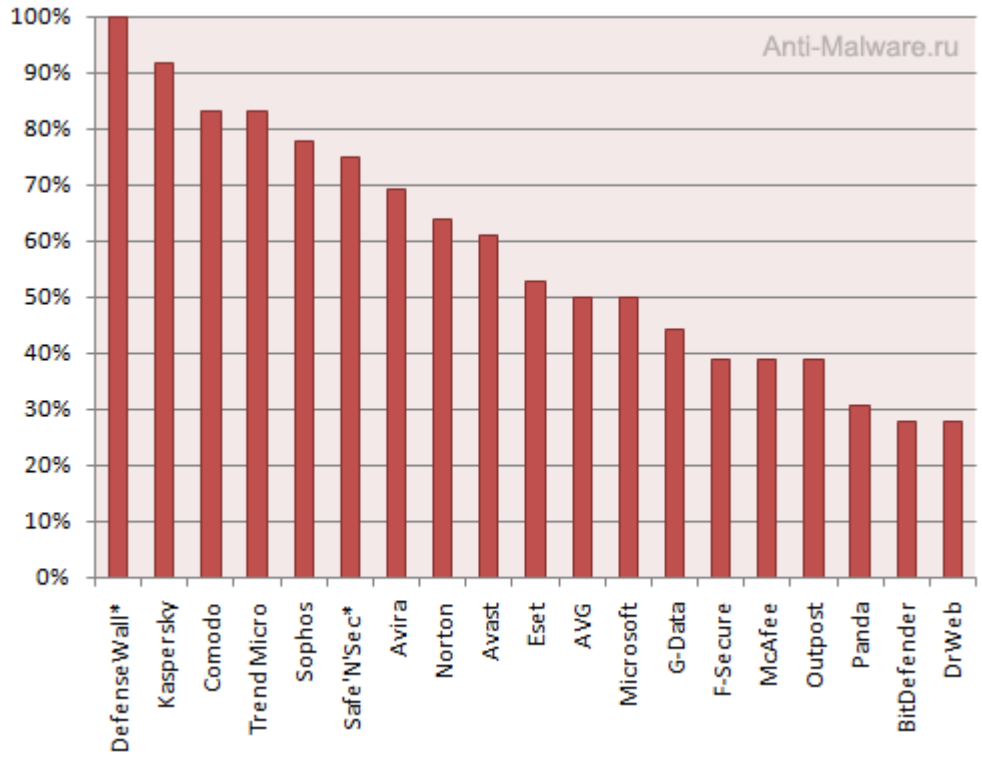
Итоговые результаты теста

Итоговые результаты сравнительного тестирования антивирусных программ и HIPS представлены ниже в таблице и на рисунке 1.

Таблица 1: Эффективность антивирусных программ против новейших угроз (Zero-day)

Антивирус	Баллы	% от макс.	Награда
DefenseWall*	36	100%	 Platinum Zero-day Protection Award
Kaspersky	33	92%	 Gold Zero-day Protection Award
Comodo	30	83%	
Trend Micro	30	83%	
Sophos	28	78%	 Silver Zero-day Protection Award
Safe'N'Sec*	27	75%	
Avira	25	69%	
Norton	23	64%	
Avast	22	61%	
Eset	19	53%	 Bronze Zero-day Protection Award
AVG	18	50%	
Microsoft	18	50%	
G-Data	16	44%	
F-Secure	14	39%	**Не прошли тест**
McAfee	14	39%	
Outpost	14	39%	
Panda	11	31%	
BitDefender	10	28%	
Dr.Web	10	28%	

Рисунок 1: Эффективность различных программ защиты против новейших угроз (Zero-day)



***** - программы класса HIPS