AV

comparatives

Anti-Virus Comparative

Detection of widely spreading malware

Date: October 2006 (2006-10)

Last revision: 15th October 2006

Author: Andreas Clementi

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

1. Introduction

This is a detection test of widely spreading malware, which are also listed on the WildList of August 2006 (www.wildlist.org).
This test should not be called an ITW-Test, because AV-Comparatives does not have access to the WildCore collection and therefore can not guarantee that this test is 100% comparable to an ITW test, even if the test is based on samples listed on the WildList site.
In-the-Wild (ITW) tests are anti-virus tests done on the malware/viruses that have been reported by two or more WildList reporters (mainly Anti-Virus vendors) to the WildList Organisation International (WLO).
Official ITW-tests are provided and supported by various AV testing institutions, such as VirusBulletin (www.virusbtn.com), CheckVir (www.checkvir.com), ICSALabs (www.icsalabs.com), Checkmark (www.check-mark.com), and AV-Test (www.av-test.org), often bundled along with other test types.
ITW-Tests are important because for a globally distributed product it is the minimum of what you should expect an Anti-Virus program to do - protect you against well-known and spreading In-The-Wild samples (consisting of viruses, worms and some bots due to it limiting its reports to replicating malware).
Anyway, ITW-Tests alone are not enough for an user to evaluate an Anti-Virus product or to really know how much protection he can expect to get - even with an Anti-Virus which detects 100% of the WildList samples. Tests done on full sets of malware (like AV-Test.org and AV-Comparatives.org provides) offer users more information about which Anti-Virus offers wider and better detection rates.

Interesting quote[1] about „Tests and certifications based on the WildList“:

The WildList, established in the early 1990's by anti-virus researcher Joe Wells and now published monthly by the WildList Organization, aims to keep track of which viruses are spreading in the real world. Users are clearly most concerned about these threats [as opposed to those found only in the virus laboratory] and over the years detection of 'in the wild' viruses, as defined by the WildList, has become the de facto measure by which anti-virus products are judged. Fee-based anti-virus certification tests, most notably ICSA Labs [part of TrueSecure Corporation] and SC Magazine, are based on detection of WildList samples. In addition, as noted above, the Virus Bulletin 'VB100%' is awarded on the basis of a product's ability to detect WildList viruses. However, using WildList viruses as a yardstick to measure the detection capability of anti-virus products is not as clear-cut as it may at first seem.
To be included in the WildList, a virus must be reported by at least two separate WildList reporters [a group of 70 virus information professionals, many of whom work in the anti-virus industry]. However, there's no guarantee that what's reported provides an accurate picture of what's really out there. If a company's chosen anti-virus product finds and removes a virus without difficulty, will they bother to contact the vendor's support department to report the infection? It's much more likely that they will simply move on to the next job. So the WildList is more a measure of 'problem' viruses that required a support call than a reflection of all viruses found in the field.
Also, the WildList is compiled monthly, but it's a retrospective list of viruses reported. In other words, there's a time lag between receiving the reports and publishing the data. The WildList is always a month out-of-date, at best!
Today's threats spread faster than ever before and there's now a higher risk than ever before of being hit by a new piece of malicious code. More than 80% of new malicious programs are found in the field, on real machines, not just in so-called 'zoo' collections. So the term 'in the wild' is somewhat outmoded.

[1] Taken from the paper „Evaluating anti-virus tests Why some reviews are better than others“ written by David Emm and published on http://esac.kaspersky.fr/index.php?PageID=9

2. Tested products

The following 15 products (with last signature updates and versions of the 11th October 2006 and with default settings) were tested under Windows XP:

- Avast! Professional Edition 4.7
- AVG Professional 7.5
- AVIRA AntiVir Personal Edition Premium 7
- BitDefender Anti-Virus 10 Professional Plus
- Dr.Web Anti-Virus for Windows 95-XP 4.33.2
- ESET NOD32 Anti-Virus 2.5
- F-Prot Anti-Virus for Windows 3.16f
- F-Secure Anti-Virus 2007
- Gdata AntiVirusKit (AVK) 2007
- Kaspersky Anti-Virus 6.0
- McAfee VirusScan 2007
- Norman Virus Control 5.82
- Symantec Norton Anti-Virus 2007
- TrustPort Antivirus Workstation 1.4
- VBA32 Workstation 3.11.1

3. Test results

Below the test results of the tested products against widely spreading malware:

0 missed samples (**PASSED**)	**AVG** **AVIRA** **BitDefender** **Dr.Web** **ESET (NOD32)** **F-Prot** **F-Secure** **Gdata (AVK)** **Kaspersky** **Norman** **Symantec** **TrustPort**
1 missed sample (**FAILED**) - **W32/SdBot!ITW1764**	**McAfee**
2 missed samples (**FAILED**) - **W32/Detnat!ITW#2** - **W32/Detnat!ITW#3**	**Avast**
5 missed samples (**FAILED**) - **W32/Detnat!ITW#2** - **W32/Detnat!ITW#3** - **W32/Feebs!ITW#19** - **W32/Feebs!ITW#26** - **W32/Feebs!ITW#48**	**VBA32**

4. Final notes

AV-Comparatives (www.av-comparatives.org) will continue to provide tests with larger test-sets and also other more detailed new tests showing other aspects of Anti-Virus software on a regular basis.
This was the first and last attempt of AV-Comparatives to do a test similar to ITW-tests. For good and official ITW-tests done on a regular time-base by other independent testing bodies, please visit www.checkvir.com, www.virusbtn.com, www.av-test.org (results can be found in various computer magazines), www.icsalabs.com or www.westcoastlabs.org.

This report was edited the 15th October 2006: we apologize to all readers for the potentially misleading subjective comments or words that were contained in the first version of the 13th October. This version supercedes and replaces all earlier versions.
There were also some methodological errors in the first report and even if the results remain the same, the report was not qualified for being released in that form.
The first version was called ITW-Test, but ITW-Tests are done a bit differently. As AV-Comparatives does not have access to the WildCore collection and can not assure the readers that also other testers will use those samples for the test, the test can not be called ITW-Test – I renamed it now to 'Widely spreading malware test'.
I learned a lot from the errors and mistakes done in this type of testing, and will try to avoid such errors in future, and will also not perform any more of this type of test.

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 (October 2006)