

Anti-Virus Comparative



On-demand Detection of Malicious Software

Chinese Vendors

including false alarms

Language: English

August 2011

Last Revision: 27th September 2011

www.av-comparatives.org

Preface

Major players such as international brand names etc. have had research centers in China for many years. Now, a growing number of Chinese software companies and individual programmers are marketing their applications to users in Europe and Northern America. Even without travelling to China, many computer users worldwide benefit from the work of Chinese programmers. Many Apps “Made in China” are very popular among foreign users.

Especially smaller and medium sized foreign invested businesses in mainland often have a heterogeneous IT infrastructure. Their expat managers often face requests from Chinese employees and colleagues to utilize local software which is often less expensive than “foreign” products. For foreign IT decision makers, who often have a limited command of Chinese, it is next to impossible to judge software applications for which almost no non-Chinese third-party information is available.

As an independent nonprofit organization, we are in contact with many companies and institutions with offices in mainland China. The IT decision makers of two foreign-invested companies asked us to check the ability of security software developed in China to detect international malware.

The two foreign clients commissioned this study are long time users of China-made non-security applications. They are both willing to switch to local software whenever the price is competitive and quality and service can be relied upon.

As the companies of both clients are both bound by even stricter liability and privacy regulations from their home country on top of local laws and regulations, they need an independent verification of the international detection capability of the security software they protect their company with.

Why “international detection capability”?

Chinese companies are important players in the global market. The Chinese SANY Group, e.g., invested one hundred million Euros into a factory in Germany. The group has a total of over 30 daughter companies outside of China. Many other Chinese groups now have daughter companies and offices around the world.

China is a major trading partner for many countries. Almost 10% of all German imports worth a total of 76.5 billion Euros originate from the People’s Republic of China. For the United States of America, China ranks second in imports and third in exports.

In 2010, 57.39million Chinese tourists have travelled abroad, up 20.4% from the previous year. In 2011, 32 million Chinese tourists have already travelled abroad spending USD 28 billion.

Chinese companies running business or offices outside of mainland China, Chinese companies buying from or selling to partners outside of China and Chinese tourist visiting other countries and regions all need security software with a reliable ability to detect international malware.

There is a limited number of threats, which is only targeted at the users in a specific country. For the majority of the malware, the location of your computer is not important.

Tested Product Versions

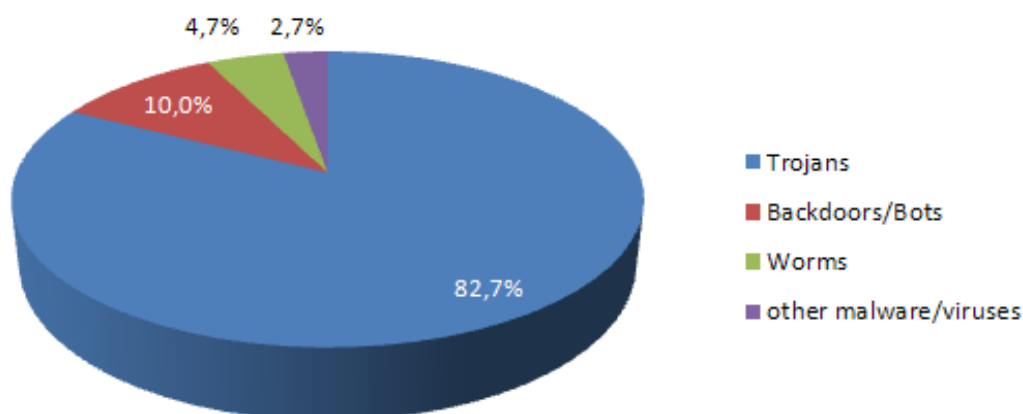
Four products of Chinese vendors have been included in this test.

Our clients want to stay anonymous and to keep the tested vendors confidential. The only thing we can reveal is that all of these vendors are from mainland China and are not listed in our comparative report of August 2011.

Malware

The Malware sets have been frozen on 1st of August, 2011. The system sets and the products were updated and frozen on the 12th of August 2011.

The used test-set contains about 200-thousands recent/prevalent malware samples from last months and consists of:



Test setting

AV-Comparatives prefers to test with default settings. As most products run with highest settings by default (or switch to highest automatically when malware is found, making it impossible to test against various malware with “default” settings), in order to get comparable results we set also the few remaining products to highest settings (or leave them to lower settings) in accordance with the respective vendors.

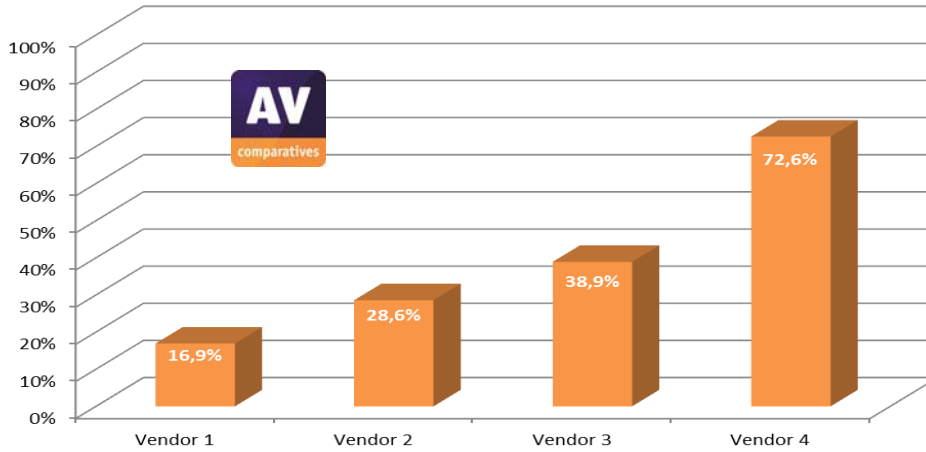
Several products make use of cloud technologies, which require an active internet connection. Our test is performed using an active internet connection.

Telemetry data has been consulted to include prevalent malware samples which are/were hitting users in the last six months. Due the focus on prevalent/widespread and recent samples (majority is from last three months), the size of the test-set is much smaller than in previous years.

Test Results

Below are the test results tables containing the detection rate details of the various products over the used test-set.

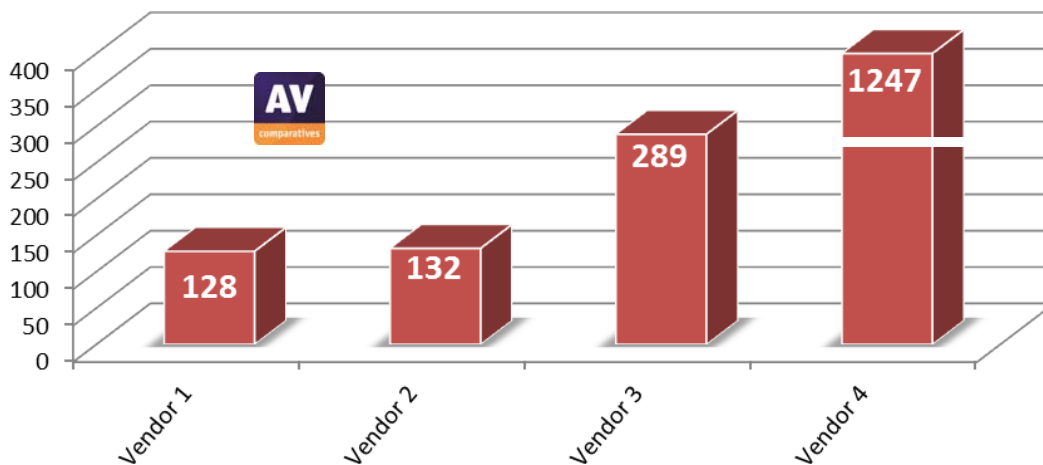
Graph of missed samples (lower is better)



Percentages refer to the used test-set only. Even if it is just a subset of malware, it is important to look at the number of missed malware.

False positive/alarm test

In order to better evaluate the quality of the detection capabilities (distinguish good files from malicious files) of anti-virus products, we provide a false alarm test. False alarms can sometimes cause as much troubles as a real infection. Please consider the false alarm rate when looking at the detection rates, as a product which is prone to cause false alarms achieves higher scores easier.



Copyright and Disclaimer

This publication is Copyright © 2011 by AV-Comparatives e.V. ®. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of the management board of AV-Comparatives e.V., prior to any publication. AV-Comparatives e.V. 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 e.V. 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. AV-Comparatives e.V. is a registered Austrian Non-Profit-Organization.

For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives e.V. (September 2011)

**Every second counts.
Who is attacking you? And how?**

**Even the best AV solution leaves you exposed
to zero-day and custom malware attacks.**

**Get real-time analysis.
No waiting for signature updates.**



validEDGE
www.validedge.com

*ValidEdge Malware Analysis Appliances
Free 30-day evaluation.*

DETECT

ANALYZE

HEAL