ANTI-VIRUS OUTBREAK RESPONSE TESTING AND IMPACT

Andreas Marx
AV-Test GmbH, Klewitzstr. 7, 39112 Magdeburg, Germany

Tel +49 391 6075466 • Fax +49 391 6075469 • Email amarx@av-test.de

ABSTRACT

Often referred to as the 'window of vulnerability', the reaction time between when a new malware is discovered and when AV software updates are available can often make the difference as to whether a new threat gains a substantial foothold in-the-wild. To better understand the nature of this problem, *AV-Test.org* began monitoring 30 AV vendors, checking for updates every five minutes and comparing those updates to newly spreading malware.

The main idea of the project was described in the *Virus Bulletin* article 'Outbreak response times: Putting AV to the test' (*Virus Bulletin*, February 2004 p.4). A copy of this article is available at: http://www.virusbtn.com/magazine/archives/ or http://www.av-test.org/sites/references_papers.php3?lang=en.

The results of the tests thus far have revealed not only the reaction times for several high profile threats, including MyDoom, Bagle, and Netsky variants, but also sheds light on problems encountered during the update process. For example, detection may be incomplete initially, or the updates may fail to replicate across all vendor download servers in a timely manner, or the servers may not even be reachable – thus possibly resulting in missed detection or delay of the updates for some customers.

This paper takes an in-depth look at how the tests are conducted, what the results of these tests have demonstrated, and the possible impact of this.

The rather good or poor reaction times over a nine-month period, as well as the number of proactively detected malwares of the different AV companies will be presented.

In order to include the most recent threats in this paper, the full paper will be available at http://www.av-test.org after the close of the conference. The presentation (PPT) and all measured statistics (a large XLS) will be included as well.