Antivirus update reaction times of major antivirus vendors

Based on independent data from AV-Test.org
Speed of response is the key!

- Everyone can protect against old viruses and threats.
- Heuristic solutions do not catch 100% of viruses and they generate a very high number of false positives. In addition, virus writers test their malware against proactive solutions as long as they succeed in getting through the system.
- The difference comes in reacting to new threats with signature updates.
- It is the new threats that do most of the widely publicized damage.
Any antivirus solution is only as good as the latest update

- Major differences in speed between antivirus companies
- F-Secure consistently ahead of the major competitors
- F-Secure updates several times each day, some major competitors only once per week
Patching window gets smaller

Time to exploitation of vulnerability


Vulnerability discovered  Advisory Released
Recent viruses emerge only days after vulnerability is discovered.
Response delays of just hours have a big impact

- In major outbreaks the amount of infected messages or machines typically follows a roughly exponential curve.
- The time from outbreak until the antivirus update is received is critical.
- Antivirus response delays of just a few hours can have a major impact on the amount of damage the outbreak can do in an organization.
Average response times for the 12 major outbreaks in the first half of 2005

Source: AV-Test.org
Number of updates / month
January 2005

Source: AV-Test.org
A note on the data source

AV-Test.org, an independent antivirus testing lab, provides response time testing during virus outbreaks in addition to their detection testing for a wide range of antivirus products. AV-Test.org testing and results are used in major publications and IT security magazines worldwide such as PC-World, PC-WELT, Virus Bulletin, ComputerBild, CHIP and c't. (www.av-test.org)