

# Malware Detection Rates for Leading AV Solutions

A Cyveillance Analysis  
August 2010

## EXECUTIVE SUMMARY

With the ever evolving cyber-threat profile, traditional antivirus (AV) solutions can not adequately detect and protect against new and quickly changing malware threats on the Internet, leaving individuals exposed to many cyber dangers. In fact, based on Cyveillance's testing, AV solutions do not provide adequate protection even a month after new malware threats have been detected.

In this study, Cyveillance measures the effectiveness of the top AV solutions to protect against new threats as they are initially discovered in real-time and over the course of a thirty day period.

## APPROACH

To produce the cyber intelligence used in this report, Cyveillance has leveraged its patented Internet-monitoring technology platform. The technology continually sweeps the Internet, collecting information from more than 200 million unique domain names, 190 million unique websites, 80 million blogs, 90,000 message boards, thousands of IRC/chat channels, billions of spam emails, tiny urls and more.

Unless otherwise stated, it is also important to note that all figures and statistics included in this report are actual measurements as collected by Cyveillance Internet-monitoring technology rather than projections based upon sample datasets.

## CYBER INTELLIGENCE USED IN THIS STUDY

Cyveillance's proprietary threat analysis engines leverage text, images and behavior-based analyses to pinpoint online malicious websites and dangerous URLs "in the wild" that serve as malware infection and hosting points. Also, Cyveillance identifies URLs exhibiting malicious behavior such as URLs that take advantage of browser exploits but do not actually install an executable software package on the computer. This study focuses solely on installed binaries discovered "in the wild" and analyzed in real time as they were installed on our test machines.

On average, Cyveillance discovers thousands of unique malicious URLs per day, which normally provides hundreds to low thousands of unique malicious executables delivered "right now" on the live Web. The malware files used for this study include data collected and analyzed over a three-day period of April 20, 2010 through April 22, 2010, resulting in an overall total data set of approximately 1,708 confirmed malware files. To ensure the most conservative approach was applied, every malware file had to be confirmed as malware by at least three AV vendors used in this study. Any malware file that did not meet this criterion was not used in the testing.

## TESTING METHODOLOGY

The 1,708 confirmed malware files were run through the latest release of the top desktop anti-virus solutions upon initial detection and again every six hours for one month, allowing Cyveillance to track when malware files were detected by the AV solutions used in the testing. The approach provided the specific number of hours/days it took for each A/V company to recognize a malware file as a threat, if they ever did.

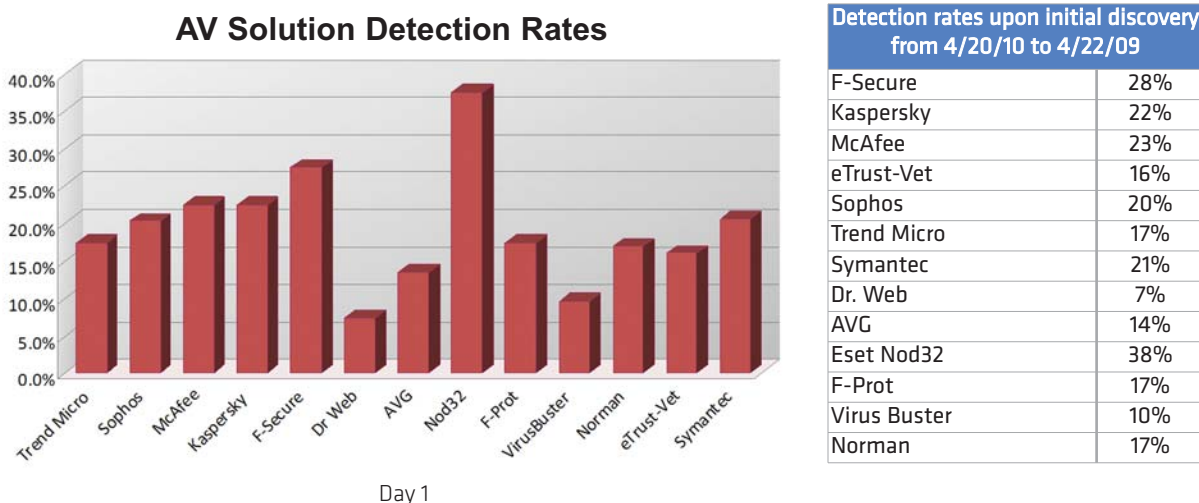
Aggregate statistics at the start of the study (upon initial detection), at numerous points throughout the month, and at the end of the month provide a clear trend line by vendor for how quickly they improved their solution to detect the latest threats being distributed “in the wild” on the Internet.

Finally, by taking each AV solution in isolation and eliminating all the samples never detected as a threat within the month long study period, Cyveillance determined for each individual solution, the approximate time in hours/days it takes each AV solution to recognize those samples it did eventually detect. The combination of detection rates upon discovery and the speed at which the detection of those malware files improved over time, provide an overall picture of each vendor’s performance with respect to Web-delivered malware threats.

### THE RESULTS

The table below (Figure 1) provides a measurement of the effectiveness of AV solutions upon initial detection of malware discovered by Cyveillance as it is installed in real time by malicious or infected websites. The samples were fed to the AV solutions in real time and only consisted of confirmed malicious files.

Figure 1 – AV Solution Detection Rates upon Initial Discovery



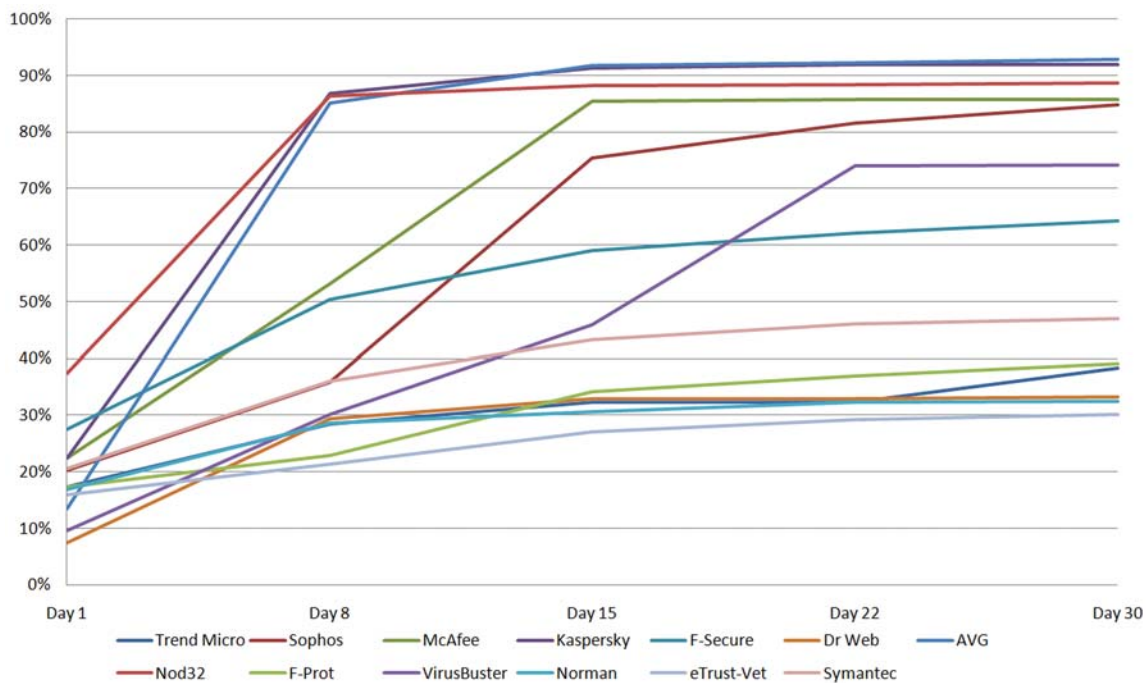
As the results show, even the most popular AV solutions detect less than half of the latest malware threats. It is well known within the industry that malware writers can either install these programs locally or use a number of websites to ensure their malware is *not* recognized as a threat at the time of release. If the malware writer can practically ensure the malware will go unrecognized upon release, then this means that a critical question of each security suite’s performance is the speed at which it “catches up” with the latest threats.

Over the course of the thirty day testing period, the speed and breadth of improvement realized by each of the AV solutions used is illustrated in the Figure 2 below:

Figure 2 – AV Test Results

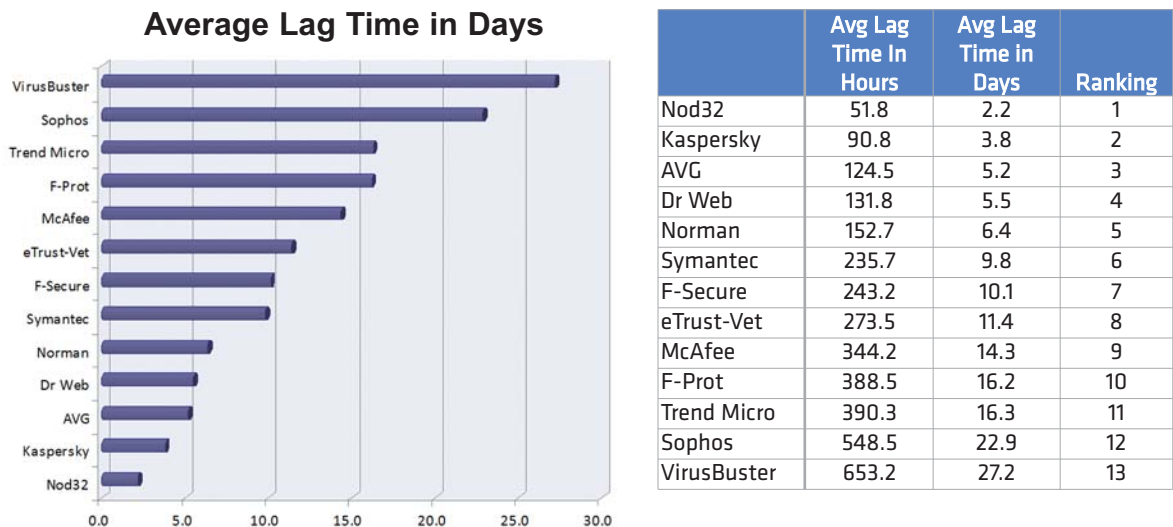
|        | Trend Micro | Sophos | McAfee | Kaspersky | F-Secure | Dr Web | AVG | Nod32 | F-Prot | Virus Buster | Norman | eTrust-Vet | Symantec |
|--------|-------------|--------|--------|-----------|----------|--------|-----|-------|--------|--------------|--------|------------|----------|
| Day 1  | 17%         | 20%    | 22%    | 22%       | 27%      | 7%     | 13% | 37%   | 17%    | 10%          | 17%    | 16%        | 21%      |
| Day 8  | 29%         | 36%    | 53%    | 87%       | 50%      | 29%    | 85% | 86%   | 23%    | 30%          | 29%    | 21%        | 36%      |
| Day 15 | 32%         | 75%    | 85%    | 91%       | 59%      | 33%    | 92% | 88%   | 34%    | 46%          | 31%    | 27%        | 43%      |
| Day 22 | 32%         | 81%    | 86%    | 92%       | 62%      | 33%    | 92% | 88%   | 37%    | 74%          | 32%    | 29%        | 46%      |
| Day 30 | 38%         | 85%    | 86%    | 92%       | 64%      | 33%    | 93% | 89%   | 39%    | 74%          | 32%    | 30%        | 47%      |

### Malware Detection Rates over 30 Days by AV Vendor



While the data used in the testing was limited to a thirty day period, the results provide the data needed to rank the AV solutions based on their ability to “catch up” to the numerous new threats discovered on the Internet daily.

Figure 3 – AV Test Results



**CONCLUSION**

As illustrated in the preceding section, the average time it takes for the top AV solutions to catch up to new malware threats ranges from 2 to 27 days. Given that this metric does not include malware files still undetected even after thirty days, the AV industry has much room for improvement.

Since AV solutions alone do not adequately protect individuals and enterprises from countless zero-day malware threats on the Internet, users should minimize the potential of infection through the following methods:

- Simply avoid going to unfamiliar, unknown or disreputable websites.
- Use more secure settings on your Web browser. This action may cause some inconvenience by requiring users to respond to security prompts when visiting feature rich websites, but it will reduce potential malware infections.
- Ensure all of your security software is up-to-date. Most security programs offer an automatic update feature. If this feature is enabled, then you are assured that your software is current with the latest malware protection offered by the manufacturer.
- Leverage supplemental malware block lists. Block lists can be used to help fill the protection gap from the time a new malware is released on the Internet to the time the signature is updated by the AV vendors.
- Educate employees how to avoid the ever evolving threat on the Internet.

## ABOUT CYVEILLANCE

Cyveillance, a world leader in cyber intelligence, provides an intelligence-led approach to security. Through continuous, comprehensive Internet monitoring and sophisticated intelligence analysis, Cyveillance proactively identifies and eliminates threats to information, infrastructure, individuals and their interactions, enabling its customers to preserve their reputation, revenues, and customer trust. Cyveillance serves the Global 2000 and OEM Data Partners – protecting the majority of the Fortune 50, regional financial institutions nationwide, and more than 30 million global consumers through its partnerships with security and service providers that include AOL and Microsoft. Cyveillance is a wholly owned subsidiary of QinetiQ North America. For more information, please visit [www.cyveillance.com](http://www.cyveillance.com) or [www.qinetiq-na.com](http://www.qinetiq-na.com).

Copyright © 2010 Cyveillance, Inc. All rights reserved. Cyveillance is a registered trademark of Cyveillance, Inc. All other names are trademarks or registered trademarks of their respective owners

Cyveillance, Inc.  
1555 Wilson Boulevard  
Suite 406  
Arlington, VA 22209-2405  
888.243.0097  
[www.cyveillance.com](http://www.cyveillance.com)  
[info@cyveillance.com](mailto:info@cyveillance.com)