



Media Contact:

Tony Welz
Welz & Weisel Communications
703-218-3555
tony@w2comm.com

Cyveillance Test Reveals Majority of Active Malware Attacks Go Undetected

According to Company's Latest Fraud Report: Leading Anti-Virus Solutions on Average Detect Less than Fifty Percent of Active Malware Found on Internet

ARLINGTON, Va., August 11, 2008-- [Cyveillance](#), the world leader in cyber intelligence, today announced that a recent test of best-of-breed anti-virus vendors over a thirty-day period revealed that more than half of all malware threats on the Internet go undetected. Data for the test was compiled from the thousands of active malware threats Cyveillance detects daily¹, which was then fed through each of the vendors' anti-virus solutions in real-time. This data was captured as part of Cyveillance's recent "1H 2008 Online Fraud Report," which was issued today.

Cyveillance identifies a malware threat as a file or application downloaded from a Web site or server that exhibits properties that are both involuntary and malicious in nature. An active malware threat is one that has been located on a live Web site within the last 30 days.

Given the reactive nature of today's malware and anti-virus detection technology, even leading anti-virus solutions are inherently at a disadvantage to keep up with the dynamic nature of growing malware threats. Because anti-virus solutions primarily detect previously identified malware threats, perpetrators quickly replace recently discovered malware threats with modified versions and exploit this discovery lag-time to evade detection and infect unsuspecting machines. As such, the Cyveillance test which took place from June 20 – July 19, 2008, looked at five best-of-breed anti-virus vendor solutions², deployed in their default settings with auto-update features enabled to ensure all malware signatures were within vendor parameters.

A full description of Cyveillance's anti-virus malware detection data is included in the company's "[1H 2008 Online Fraud Report](#)." In addition to a detailed evaluation of the effectiveness of leading anti-virus malware solutions, the report also tracks the online "fraud chain" comprised of malware components that store and serve malware executables, distribute malware to consumers, and receive and store the confidential information collected from infected computers. Other key report findings include:

- Data tracked during first half of 2008 shows that the United States not only continued to extend its lead as the top malware distributor, but is now distributing more malware than all other countries combined.
- 367 unique new brands were phished in the first half of 2008, which represents a 80% increase over the second half of 2007.
- Phishers continue to expand attacks worldwide. In the first half of 2008, Cyveillance identified phishing attacks in 30 different countries, with numerous new targets in the Middle East and Latin America.

"Security technologies such as anti-virus and anti-spyware solutions are effective once malicious code has been identified and confirmed as a mainstream threat, and these vendors are doing their best to keep up with the rapid onslaught of new threats," said Panos Anastassiadis, CEO and Chairman of Cyveillance. "However, because they are predominantly reactive in nature, they will continue to fall short when it comes to protecting against real-time and zero-day threats. No solution will ever be 100 percent effective, but by adding proactive intelligence gathering techniques to these defensive anti-virus technologies, the gap between infection and protection can be greatly reduced."

All figures and statistics in the Cyveillance "1H 2008 Online Fraud Report" report are actual measurements rather than projections based upon sample datasets. The cyber intelligence included in this report includes data collected and analyzed between January 1 and June 30, 2008. It represents aggregate cyber intelligence findings that Cyveillance has delivered to its OEM data partners, except where otherwise noted. A member of the NAFCU Services Corporation [Preferred Partner Program](#), Cyveillance also provides this data through easy and affordable solutions designed specifically for credit unions without the internal bandwidth or resources to combat the problem on their

own. For more information about Cyveillance's research findings, please visit:

<http://www.cyveillance.com/web/forms/request.asp?getFile=111>

About Cyveillance

Cyveillance, the 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. For more information, visit www.cyveillance.com.

¹*Cyveillance's comprehensive monitoring technology continuously sweeps the Internet – monitoring and collecting information from over 200 million unique domain name servers, 150 million unique Web sites, 80 million blogs, 90,000 message boards, thousands of IRC/Chat channels, billions of spam emails, auction sites, bot networks and more. This approach yields the discovery of more than 100,000 new sites each day.*

²*Vendors tested included F-Secure, Kaspersky, McAfee, Sophos and Trend Micro. Symantec data was inconclusive at time of publication and was not included in the test results.*