


ADVERTISEMENT



**IT KNOWLEDGE EXCHANGE**

Sign up for your free blog today!



Your online connection to

[HOME](#) :: [NEWS](#) :: [MAGAZINE](#) :: [WEBCASTS](#) :: [WHITE PAPERS](#) :: [LEARNING](#) :: [ADVICE](#) :: [TOPICS](#) :: [EVENTS](#) :: [ABOUT US](#)SEARCH : [Advanced Search](#) | [Site Index](#)Powered by: 

ADVERTISEMENT

[Home](#) > [Security News](#) > AV upstarts tout need for speed in zero-day fight

## Security News:

[EMAIL THIS](#) [LICENSING & REPRINTS](#)

### AV upstarts tout need for speed in zero-day fight

By Jon Boroshok, Contributor  
02 Feb 2006 | SearchSecurity.com

The recent frenzy from the [Windows Meta File \(WMF\) worm](#) has created a growing concern and confusion about [zero-day](#) and [zero-hour threats](#).

There's a great deal of uncertainty about how real the threat is from exploits that immediately take advantage of new vulnerabilities, and about how organizations should determine which vendors can best protect them.

"Zero-day is, to some degree, a marketing concept," said Ron Moritz, senior vice president and chief security strategist of Islandia, N.Y.-based software giant Computer Associates International Inc. "When you actually consider the area of malicious code, all viruses and worms can probably be considered as zero-day exploits."

Yet malicious hackers are constantly learning how to react more quickly, and that threat has created a business climate among enterprise security managers in which speed of response -- how quickly an AV vendor can protect vulnerable customers via a software update or other means -- has become critically important.

#### Time or trust?

AV-Test.org of Magdeburg, Germany tests antivirus, antispyware and personal firewall software on behalf of vendors and trade magazines. The test results, available on [its site](#), offer an interesting contrast between U.S. antivirus giants and smaller European competitors.



**Building a company to shave three hours off response time is much easier to do than to shave three hours off response time if you already have millions of deployments.**

Patrick Peterson, IronPort Systems

While the time-trial-like tests seem to indicate that a number of the upstart European firms typically issue software updates more quickly than their more widely known U.S. counterparts, opinions differ about whether speed alone is the most important criteria when choosing a vendor.

AV vendors' researchers play a dominant role in how quickly each can respond to the evolving skill set of the "bad guys." Moritz, whose company produces AV software, said a key differentiator is how quickly an AV vendor gets access to the virus, worm or malicious code sample, and how well its back-office automation infrastructure supports rapid analysis and inoculation prototyping. He feels response rates will vary from test to test, and from signature to signature. In choosing a vendor, Moritz said, companies must decide, "who do you trust and have confidence in."



"Our experience does not indicate a specific advantage of any region," said Yuval Ben-Itzhak, CTO for San Jose, Calif.-based security vendor Finjan Software Ltd. "A reliable AV vendor keeps its leadership in the global market."

Herbert H. Thompson, chief security strategist for Wilmington, Mass.-based application testing firm Security Innovation Inc., calls zero-day threats, "an escalation of arms -- you vs. malicious code." He said that if somebody really launched a zero-day worm, there's no way a patch could catch up, regardless of the time trial results.

"Do the test numbers reflect the effectiveness of the signature? No," he said. "Which is the bigger risk -- no patch or the unproven, untested patch?" Thompson feels that the solution vendor decision comes down to brand trust.

#### Multiple vendors, multiple layers

Richi Jennings, lead analyst for San Francisco-based Ferris Research, said the

zero-hour threat is very real, but is not convinced it boils down to Europe vs. U.S. when it comes to picking a solution provider.

"However, it's clear from several sets of AV-Test.org results that some smaller AV vendors are quite consistently doing a better job at pushing new AV signatures than the well-known U.S. vendors, such as McAfee and Symantec. Three notable examples are Kaspersky Lab and BitDefender (both based in Eastern Europe) and Sophos (Canada)," said Jennings.

Jennings said that to effectively protect against viruses, worms and other malware, organizations should implement a multi-layered strategy that includes products from several vendors and implementing protection at several points in the network.

Patrick Peterson, vice president of technology for San Bruno, Calif.-based e-mail security provider IronPort Systems, Inc., said that the speed of smaller European companies is not the only factor to consider and agrees that a multi-layered, multi-vendor defense in depth is critical.

He explained that while the European AV firms tout their rapid responses, their products tend to be much less complex. Symantec Corp. and McAfee Inc. have rich desktop suites with considerable enterprise integration capabilities. They also have many more customers with far more platforms and configurations. The Europeans have relied almost exclusively on price and response time to enter the market.

#### More on zero-day threats

[Network safety relies on reaction time to Patch Tuesday](#)

[VeriSign raises stakes in battle for threat intelligence](#)

[Report: Zero-day exploits are nearing](#)

"Building a company to shave three hours off response time is much easier to do than to shave three hours off response time if you already have millions of deployments," said Peterson. "The smaller European players are faster and more aggressive, but this can result in less accuracy and more updates."

Peterson said that companies should have a rapid response-oriented vendor with a different business model than the giants. This can correlate with the European firms, but it doesn't have to.

"We have seen enterprises stick with 'the bigs' on the desktop where management and suite integration is king. I don't think the smaller players have the solution to compete with Symantec and McAfee here," Peterson said. "We have seen customers moving aggressively to Sophos and other European vendors at the gateway where management and integration complexity is less and updates can be deployed in real-time 100%."

Vincent Weafer, senior director for Symantec's Security Response research group,


echoed the belief in a layered defense, recommending the use of different technologies, but not necessarily different vendors. "Variety is the key," said Weafer. "The threats are different." The right tool for the right problem is important, he added, and AV is not the only answer. Weafer recommended looking at security architecture segmentation, with layers of security at the gateway, application server, and desktop/endpoint level.

Weafer said the key to look for is response time and quality. The time trials offered by AV-test.org still have holes and don't cover everything, including quality and false positives. Whether speedy Europeans or tried and tested U.S. veteran vendors, all seem to agree that a layered defensive strategy is the best way to stay safe.

"The days when reactive technology would protect you are gone," said Patrick Hinojosa, CTO of Bilbao, Spain-based Panda Software. He said that an effective zero-day defensive system must be proactive, manageable, self-contained and make its own decisions with few false positives.

He called the time trails a snapshot. "Response time means reactive. Someone has to be hit first."

*Jon Boroshok is a Massachusetts-based freelance writer who can be reached at [jb@JournalistForHire.com](mailto:jb@JournalistForHire.com).*

**Sound Off!** -  [Be the first to post a message to Sound Off!](#)

**Share - Digg This!**

 [Bookmark with Del.icio.us](#)

## **SECURITY RELATED LINKS**

### **Ads by Google**

#### **Protect Against Zero Day**

Get Free App Firewall Security Kit. Defend Against 0 Day & Many More.

[www.citrix.com/websecurity](http://www.citrix.com/websecurity)

#### **Spyware Remover Download**

PC Magazine Editor's Choice Winner Best Anti-Spyware. Secure Your PC!

[www.PCTools.com](http://www.PCTools.com)

#### **Security Software**

Top 5 Sites for Security Software Compare, choose, buy!

[www.genieseecker.com](http://www.genieseecker.com)

#### **Antivirus Free Downloads**

Free Antivirus, Spyware and Registry Cleaners! Read reviews.

[www.PCPerformanceTools.com](http://www.PCPerformanceTools.com)