

## Declare war on



## Worms

Emerging worms and viruses are outslugging antivirus technologies.

By Chee Sing Chan

Our blissful IT existence is routinely interrupted by yet another worm or virus variant—an obnoxious intruder anxious to spread havoc within our hardworking computer systems. Yet as these threats morph and mutate into ever-more virulent forms, our defenses seem rooted to the spot.

Four of the five worst outbreaks in history [MyDoom, NetSky, Bagle and Sasser] took place in 2004, demonstrating the rising speed and severity of the threats spawned by modern day virus writers. Such blended threats are evading perimeter defenses, catching end-users by surprise as they rapidly exploit software vulnerabilities. The time from announcement to outbreak has fallen dramatically: from 26 days for the Blaster worm in 2003 to “zero-day” exploits.

The dominant antivirus technologies today are those that filter out infections based on signatures, noted Eric Litt, chief information security officer at General Motors. “This approach only works with known vulnerabilities and code,” he added. “Given the [diminishing] time between vulnerability disclosures and exploit availabilities, that simply isn’t enough.”

### Secured layers

Traditional antivirus technologies are signature-based scanners that filter out worms and viruses by matching patterns in their files. Users and vendors acknowledge that while such technologies still have a role, they will fade from prominence. “In future, big companies will not be able to count on antivirus vendors to win the race,” said Litt. To some degree, security vendors agree.

The effectiveness of anti-virus software relies on users being diligent in applying patches, updating virus signatures and doing scans, said Tommy Tam, managing director for Hong Kong and South East Asia, Fortinet. “The problem is, this anti-virus software frequently represents the first, last and only line of defence against malware.”

“I expect the core antivirus engine to remain the same for some time,” said David Sykes, senior director for enterprise sales, Asia Pacific, Symantec. “It will continue to be a critical component of security, but not the answer by itself.”

Hong Kong-based security provider Network Box takes the view is that the role of standalone antivirus tools is changing and being questioned.

“It’s frustrating that many people do not appreci-

ate that just having standard anti-virus tools on [the] desktop and at gateways is simply not going to cut it any more,” said Michael Gazeley, managing director at Network Box. Gazeley notes that while many viruses and worms arrive via e-mail, worms like Sasser infect via web browsers, bypassing antivirus tools that only guard the e-mail gateways.

Unfortunately, many end-users remain unaware of the wide range of threats, and the means required for protection. “From individuals to SMEs to the largest organizations including government departments,” declared Gazeley, “the ignorance of the security situation is pretty universal.”

Both Gazeley and Sykes endorse the need for a firewall, intrusion detection and prevention systems (IDS and IPS), plus antivirus, antispyware, con-



**Network Box's Gazeley:** From individuals to SMEs to the largest organizations, the ignorance of the security situation is pretty universal.

tent monitoring/filtering solutions and company policy management, all configured to function in unison, for effective multilayered security.

Vendors like Network Box and Symantec have led the way towards integrated security offerings. “The march towards integration is relentless,” said

### Bottom Line:

- New worms and viruses are beating traditional anti-virus tools.
- Antivirus alone is insufficient and must be part of a multilayer defense.
- Newer antivirus technologies are still unproven.

Sykes. “Antivirus will follow the path of past IT [and] naturally evolve into integrated solutions.” Vendors clinging to non-integrated products “will have to wake up and smell the coffee,” Gazeley insisted.

### Gates wide open

For many companies, particularly SMEs, security at the network gateway has yet to be addressed properly, said vendors. Graham Cluley, senior technology consultant at antivirus vendor Sophos, noted that simple application of generic rules and policies on top of antivirus tools will remove the bulk of incoming threats.

“Sometimes there is a battle between those looking after security at the desktops and those at the email gateways,” said Cluley. “The result is a lack of communication between the two functions and a disjointed security posture.”

Many organizations maintain separate security groups for desktop versus network, observed Allan Bell, marketing director for Asia Pacific at McAfee. “Having these groups working together should be a key part of a firm’s security policy,” he added. “Unfortunately many organizations write their security policy, then leave it to gather dust in the cupboard.”

“This is still a major problem, many companies have set internal policies that start at the gateway and should also be applied down to desktop level, but in many cases, that simply doesn’t get enforced,” said Addie Luk, general manager at Trend Micro Hong Kong.

### Virus-whackers of the Future

The need for more proactive antivirus technologies has led to development of alternative methods of protection. Instead of signature-based systems, emerging offerings include memory firewalls that use application memory scanning to detect and block known and unknown threats. Other variations include technology that throttle or block network traffic based on deviations from normal traffic patterns. Such new technologies are still in a maturing phase and traditional vendors believe will take some time before becoming as effective as traditional signature-based antivirus.

—IDG staff contributed to this report