

## Latest Tool for Cyber-Terrorists.

A new, bolder breed of cyber-attacker has arrived, blending computer break-ins with virus infections. These sophisticated attacks are known as "hybrid threats" or "blended threats." Examples (so far) are "Nimda" and "Code Red," each of which caused massive damage. And have the potential of taking down large computer networks in a matter of minutes.

Anonymous coding on remote networks called "Zoos," attackers are creating viruses that are introduced into "the wild" (Internet), and infect computer systems more speedily than ever by attacking from a blend of directions. They can do significant damage to computer systems and data, or they can give outsiders the ability to track keystrokes or gain passwords and other information on computer systems connected to the Internet.

### Simple virus vs. hybrid threats

Simple: "Melissa" (1999). A destructive Word document that was uploaded to an Internet news group. Anyone who downloaded and opened the document triggered the virus. Melissa sent the document (including itself) in an e-mail message to the first 50 address book contacts. The virus then created 50 new messages from each recipient's machine, etc...

At the time, Melissa was the fastest-spreading virus ever seen, forcing a number of large companies to shut down their e-mail systems. The ripple effect across the Internet was staggering, and the damage incalculable.

**Protecting against hybrid threats is crucial.**

**Updated, multi-layer, anti-virus programs combined with firewalls provide the best protection against both viruses and hybrids.**

**Call for a review and update of your security protection.**

Hybrid threats, in contrast, might start with a simple virus, such as a replicating e-mail that sends copies to an address book. Then they use open shares to spread throughout the network. ("Open shares" are the default Windows setting for folder access, which – if not modified - give viruses a transmission method.) They also invisibly infect vulnerable Web servers and start flooding local networks with traffic. It's a powerful blend that can wreak havoc quickly.

"Nimda" and "Code Red" are examples. The economic cost of Code Red and Code Red II exceeded \$2 billion, (Computer Economics) and ballooned to about \$200 million per day at its peak.

Because they attack from different directions, hybrid threats spread through PCs and corporate networks, and cause problems for individuals as well as corporations. During past blended-threat attacks, Internet service providers experienced soaring traffic that caused slow service. Lost productivity and personal privacy violations are imminent.

### The problem isn't going away

A large percentage of consumers still don't have virus software — or, if they do have it, don't update it regularly. Viruses are a long-term problem with no easy answers. They are becoming more sophisticated and for many "cyber-punks", shutting down a major site or causing millions of dollars in damage is the ultimate power trip.

### Fight hybrid threats with blended action

"The solution starts with individuals keeping virus software updated," says Tracy Hulver, McAfee. "To combat hybrid threats, people need a security window into their machine with tools that monitor incoming & outgoing traffic...constantly know the status of their machine and be alerted when it is vulnerable to attack, and they need to be able to shut down a blended attack quickly."

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

239.337.2667