

IT

WEEK

The newsweekly for the connected enterprise

Stealth worms lie in wait

EAMONN SULLIVAN

Security experts warned last week that firms should prepare for a new breed of virus that operates autonomously.

A report dismissed the recent Love Letter attack as crude and demonstrated how it is possible to create a far more sophisticated virus that would work across platforms, do its work with stealth and disappear before it could be stopped.

Michal Zalewski, a Warsaw-based security specialist, worked on a project to develop such a worm. All work stopped on the project last year, but the group created

a working model and believe others may have done so too. "That makes us scared," said Zalewski.

The most dangerous viruses will be targeted at particular firms, he said, making antivirus products much less effective. "I've been asked twice to develop such spy software," Zalewski said.

Nick Galea, director of security firm GFI, said, "Hackers will use email to hack into databases without firms knowing."

Analyst firm the Gartner Group said firms should implement content firewalls, quarantining executables, scripts and macros at the email server or firewall level.

THE WORM TURNS

Seven attributes of a new deadly virus

- **Portability** works across platforms
- **Invisibility** stays undetected
- **Independence** spreads itself without user intervention
- **Learning** learns new techniques
- **Integrity** hard to trace, alter or kill
- **Polymorphism** changes frequently
- **Usability** does its job and vanishes

"But if you encrypt email, those scanners will have trouble," warned Andreas Junes-tam, a consultant with Defcom Security.

▼ [News, p25](#) ▼ [Comment, p26](#) ▼ [Briefing, p45](#)

▼ [Analysis, p67](#) ▼ www.zdnet.com/zdnet/stories/news/0,4586,2567745,00.html

▼ <http://lcamtuf.na.export.pl/worm.txt>