Scrapped paper
Results on cancer vaccine retracted after three years
p4

Under arrest
US scientists rally behind beleaguered plague researcher
p5

Ivory tower
Lion man carves a niche for itself as oldest statue
p7

An ill wind
Forest fires present hot prospect for fungus researchers
p8

Experts fear network paralysis as computer worms blast Internet

Declan Butler, Paris

Blaster, Welchia, SoBig — the late summer blitz of computer worms was the last thing the world's universities and researchers needed as they prepared for the start of term. And worse could be on the way, computer scientists say.

Universities were seriously disrupted by the SoBig.E worm in late July — which copied itself into reams of e-mails that it sent out from infected machines — and the Blaster worm, which struck on 11 August causing computers to restart constantly. Next came the Welchia worm, which tried to fix computers infected with Blaster but ended up causing its own problems. Then, on 18 August, came the SoBig.F variant, the most voluminous e-mail worm in Internet history.

"The volume of traffic created by the worms gorged many university networks, often grinding them to a halt," says Theresa Rowe, a security official at Oakland University in Rochester, Michigan.

Despite the widespread disruption, many computer professionals say that the attacks could have been far worse. SoBig's worm-laden messages may have accounted for one in every 17 e-mails worldwide at one point, but specialists say that far more disruptive worms could potentially be let loose.

Worms spread much faster than computer viruses — whereas viruses need to piggyback on other programs in order to propagate, worms simply self-replicate.

Computer departments in most universities and research laboratories had been on the alert since 16 July, when Microsoft announced a flaw in a connection protocol, called the remote procedure call (RPC), used by every Windows machine linked to the Internet. This flaw was quickly exploited by Blaster.

SoBig only spread when users opened the e-mail attachment in which it was hidden. Although the worm saturated networks and slowed down the Internet by creating huge volumes of e-mail traffic, it was widely spotted by antiviral filters and wary users, and only infected about 100,000 machines.

Far more worrying for computer experts is the potential trajectory for 'autonomous network worms' such as Blaster. Instead of arriving in e-mails, these worms crawl the Internet, scanning millions of computers for security weaknesses — such as that in the RPC. When they find one, they hack in and replicate themselves. Users are often unaware that their machines have been infected.

J. RAEDLE/GETTY IMAGES

Worm war: recent network attacks have seen users stocking up on computer-protection software.

In a paper published last year, scientists at the California-based Cooperative Association for Internet Data Analysis (CAIDA) predicted the emergence of high-speed worms that could hijack millions of Internet computers within minutes (S. Staniford, V. Paxson and N. Weaver "How to 0wn the Internet in Your Spare Time" in *Proc. 11th USENIX Security Symp.* 149–167; USENIX, Berkeley, 2002).

The paper's conclusions, based on mathematical models of existing worms, were partially borne out in January when a worm called Slammer infected almost all 75,000 vulnerable machines within minutes.

Relative to this potential, Blaster was something of a damp squib, says Nicholas Weaver, a researcher at the University of California, Berkeley, and a co-author of the CAIDA study. He points out that the RPC flaw was a "sitting target" for a very large Internet attack by a fast worm, given the huge number of vulnerable machines. Slammer, in contrast, could only hit the relatively small number of machines hosting Microsoft databases.

"What was remarkable about Blaster was how little damage it did," he says. "The lack of damage was mostly good luck in that Blaster was so poorly engineered." It was "glacially slow", he adds, which gave computer departments time to build defences against it. "A few tricks and it could have spread within minutes," Weaver warns, adding that, like most worms to date, it did not carry a particularly malicious payload. A properly engineered RPC-targeted worm carrying a destructive payload might have blacked-out computer systems worldwide, he claims.

Specialists in assessing that sort of risk will gather in Washington next month for the first Workshop on Rapid Malcode to discuss possible technical responses. But for Bruce Schneier, co-founder of Counterpane Internet Security of Cupertino, California, the problem is not so much technical as legal. He wants software suppliers to be held accountable in court for security problems. "When Firestone produces a tyre with a systemic flaw, they're liable," Schneier says. "When Microsoft produces an operating system with systemic flaws, they're not liable. That's crazy." ■