Science & Technology

Computer viruses

Fighting fire with fire

Dec 8th 2005

From *The Economist* print edition

A new idea for immunising computers against viruses

COMPUTER viruses, the self-replicating programs that infect workstations a networks, are a hazard to business. The “I love you” worm, which wreaked May 4th 2000, spread by sending a copy of itself in an e-mail to everyone address book it encountered. It took just a few mugs in each company to attached “love letter” to generate thousands upon thousands of messages overwhelmed systems round the world. The cost to business was estimate billion.

The “I love you” worm was exceptional, but run-of-the-mill viruses are a c nuisance. However, a paper published in this month's *Nature Physics*, by E Tel-Aviv University in Israel and his colleagues, has suggested a new way with them.

A virus spreads by infecting its host, reproducing itself and moving on. Firewalls and other sorts of anti-virus software—computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious bits of code such as spyware—are one line of defence. These programs search files for known viruses and monitor what is running for suspicious behaviour. If a known virus is encountered, it can be stopped.

But new viruses are continually being created. As soon as a new virus is detected, a second line of defence would be to pass information about it between computers quickly, before they become infected. And that is what Mr Shir is proposing. Moreover, the researchers believe it takes a virus to stop a virus. They would like to propagate the vaccine as an epidemic.

FINANCE & ECONOMICS
Economics Focus
Economics A-Z

SCIENCE & TECHNOLOGY
Technology Quarterly

PEOPLE
Obituary

BOOKS & ARTS
Catch if you can
Style Guide

MARKETS & DATA
Weekly Indicators
Currencies
Big Mac Index

DIVERSIONS

RESEARCH TOOLS

CLASSIFIEDS

DELIVERY OPTIONS
E-mail Newsletters
Mobile Edition
RSS Feeds

The Economist Group
Economist Intelligence Unit
Economist Conferences
The World In
Intelligent Life
CFO
Roll Call
European Voice
Economist Diaries and
Business Gifts

As in the biological world, a big problem with vaccines is that they cannot until the virus they seek to stop spreading has emerged. Vaccines are thus one step behind. What Mr Shir and his colleagues outline is a plan to accel spread of a vaccine in a way that allows it to overtake the virus.

Their strategy uses a series of “honey pots”. These pieces of software attra and are employed by anti-virus firms to pick new threats up quickly. The r idea is to embed these honey pots within a network so that any virus spre through the network would be likely to reach them promptly. The honey p then be linked to each other in a separate, overlying network that allowed vaccines to pass across it.

This separate network would act as a by-pass, enabling the vaccine to ove virus and reach uninfected computers first. A honey pot would automatical a new virus, extract its signature and pass this information—the vaccine— honey pots using the overlying network. The honey pots would share this i with other computers on the network. All uninfected computers would ther recognise the new virus as dangerous, and refuse it entry.

The strategy would become more effective as the size of the network grew example, for a network of 50,000 computers, if 0.4% of them were honey 5% of computers would become infected by a virus before they were immu there were 200,000 computers, the infection rate would fall to about 1%. I computers (about the number now in America), less than a thousandth of would be infected. The savings to business could be great indeed.

Back to top »