

# Independent.co.uk

## Cyber crime stays one step ahead

**What started as the preserve of geeky hackers has become a multibillion-pound, international criminal industry, reports Sarah Arnott**

Saturday, 22 March 2008

Computer crime is not only exploding in volume but is mutating faster than it can be contained, a new report to be published next week will warn.

Some 2.5 million new types of malicious programme have been launched in the past two months alone – more than the previous 15 years put together, according to the latest data from the security firm Trend Micro. The UK now has around 1.25 million "infected" computers. And the average number of PCs across the world sending out spam emails every month shot up to 10 million last year, more than double the 4.2 million in 2006, which was double the 2.1 million in 2005.

What began as the preserve of geeky hackers showing off to their peers has become a multi-billion-pound, international criminal, industry including unsolicited email "phishing" campaigns to con people out of financial details and passwords, and complex extortion rackets.

In the age-old cat and mouse of the good guys against the bad, each side inspires the other to ever greater levels of sophistication. And as viruses evolve, taking root on everything from digital cameras to USB memory sticks, simply securing a corporate infrastructure may no longer be enough.

A key tool for the cyber-criminal is the botnet – an array of computers that are recruited by a virus and can then be controlled from one place, often without their owner's knowledge. Botnets can include tens of thousands of individual PCs, and have all manner of nefarious uses, including mass spamming, propagating yet more viruses, and crashing target websites by bombarding them with visitors.

The latest versions may even have automatic-recovery and self-healing features that parallel the most advanced corporate networks. And botnets are now rented out – for around \$1,000 (£504) for 10,000 computers.

"These criminals are clever, and there's lots of money to be made, so they are motivated to create more and more sophisticated infrastructures," Dave Rand, the chief technology officer at Trend Micro, said. "Part of the problem is that they no longer set out to take down the computer, but continue operating it without anyone's knowledge."

The current estimate is that there are 175 million infected computers live on the internet today. And cyber crime is worth billions of dollars. But incidences are so diverse, and the techniques are evolving so quickly, that it is almost impossible to gauge the true scale of the problem.

In value terms, the biggest scam at the moment is "click fraud", where scurrilous websites that are being paid by advertisers on a per-click basis use botnets to bombard the site with apparent interest. Second is good, old-fashioned, fraud – using credit-card details, online accounts or electronic transfers – based on information stolen either from individuals' computers or from insecure company databases. Third is extortion – often against gambling sites in the run-up to major sporting events – where botnets are used to prove the site can be knocked down unless payment is received.

The criminals' techniques are continually developing. This month, for example, saw the first botnet involving both humans and machines. To circumvent security measures in signing up free email accounts, a criminal group set up a high-tech sweat shop in India to process the part of the application that cannot be done automatically.

And hardware is starting to become infected in the manufacturing process, before it has even left the factory. Though the numbers are small so far, there have been recorded problems with Apple iPods, TomTom satnavs and, most recently, digital picture frames. "Anything which has storage

capacity and can be plugged into a computer could now be carrying a virus," Graham Cluley, the senior technology consultant at Sophos, said.

### How to enforce the law in the new Wild West

\*The problem with cyber crime is that it is ahead of the game. It is ill-defined, international and difficult to trace. And it is often not even clear which laws are being broken.

However, it is possible to have an impact. International comparisons show that developed economies – with stricter copyright laws, higher awareness levels and more modern technology – have lower virus levels. Turkey, for example, has 2.5 million infected computers, double the number in the UK and five times that of the Netherlands.

But even in countries with a sense of the problem, there are no easy answers as to who takes responsibility for what.

Some point the finger at the internet service providers (ISPs). "If the top 10 ISPs in the world spam league did anything, we would all be getting two orders of magnitude less," Dave Rand, chief technology officer at Trend Micro, said.

But the internet industry says legitimate providers already have complex and effective anti-spam measures.

"For any measures to be truly effective, every network operator in the world has to do likewise because there is no discrimination in terms of where an infected computer is," a spokesman for BT said. "And consumers also have a role to play in ensuring they protect their system appropriately."

Any success in tackling the problem will rely on a co-ordinated approach – including the internet industry, the Government, and end users. It will also mean finding ways to frame laws that are sufficiently loose to keep up with technological change, but sufficiently strict to be enforceable.

"Online crime is on the rise, and there is a growing awareness that it can only be addressed collectively," Jeremy Beale, head of ebusiness at the CBI, said.

Critics say the Government needs to put its money where its mouth is.

Lord Broers – who chairs the House of Lords committee that branded the internet as the new Wild West – says online law enforcement should be a priority.

"The Government should do a better job in gathering data on internet crime and fraud," Lord Broers said. "And we have to shift resources into this sort of policing."

---

[Independent.co.uk](#)[The Web](#)[Advanced Search](#)