Rich pickings for hi-tech thieves

Viruses, trojans and other malicious programs sent on to the net to catch you out are undergoing a subtle change.

The shift is happening as tech savvy criminals turn to technology to help them con people out of cash, steal valuable data or take over home PCs. Viruses written to make headlines by infecting millions are getting rarer. Instead programs are now crafted for directly criminal ends and firms are tightening up networks with defences to combat the new wave of malicious code.

The growing criminal use of malware has meant the end of the neat categorisation of different sorts of viruses and malicious programs. Before now it has been broadly possible to name and categorise viruses by the method they use to spread and how they infect machines. But many of the viruses written by criminals roll lots of technical tricks together into one nasty package.

"You cannot put them in to the neat little box that you used to," said Pete Simpson, head of the threat laboratory at security firm Clearswift. Now viruses are just as likely to spread by themselves like worms, or to exploit loopholes in browsers or hide in e-mail message attachments. "It's about outright criminality now," said Mr Simpson, explaining why this change has come about. He said many of the criminal programs came from Eastern Europe where cash-rich organised gangs can find a ready supply of technical experts that will crank out code to order. Former virus writer Marek Strihavka, aka Benny from the 29A virus writing group, recently quit the malware scene partly because it was being taken over by spyware writers, phishing gangs, and spammers who are more interested in money rather than the technology. No longer do virus writers produce programs to show off their technical prowess to rivals in the underground world of malware authors. Not least, said Paul King, principal security consultant at Cisco, because the defences against such attacks are so common. "In many ways the least likely way to do it is e-mail because most of us have got anti-virus and firewalls now," he said. Few of the malicious programs written by hi-tech thieves are cleverly written, many are much more pragmatic and use tried and tested techniques to infect machines or to trick users into installing a program or handing over important data. "If you think of criminals they do not do clever," said Mr King, "they just do what works."

As the tactics used by malicious programs change, said Mr King, so many firms were changing the way they defend themselves. Now many scan machines that connect to the corporate networks to ensure they have not been compromised while off the core network.

Many will not let a machine connect and a worker get on with their job before the latest patches and settings have been uploaded. As well as using different tactics, criminals also use technology for reasons that are much more transparent. "The main motivation now is money," said Gary Stowell, spokesman for St Bernard software. Mr Stowell said organised crime gangs were turning to computer crime because the risks of being caught were low and the rates of return were very high. With almost any phishing or spyware attack, criminals are guaranteed to catch some people out and have the contacts to exploit what they recover. So-called spyware was proving very popular with criminals because it allowed them to take over machines for their own ends, to steal key data from users or to hijack web browsing sessions to point people at particular sites. In some cases spyware was being written that searched for rival malicious programs on PCs it infects and then trying to erase them so it has sole ownership of that machine.