

Hacking has assumed more varied and subtle forms. But they remain as dangerous, say **Darlington Jose Hector** and **R Raghavendra**

HACKERS

innovate to douse firewalls

Hacking isn't what it used to be. New-age hackers have evolved new strategies, launching quiet, focused attacks rather than releasing massive viruses or denial-of-service outbreaks that were evident some time ago. Instead of accessing a network and disabling multiple computers, hackers today seek to break into a network, stay there, and either collect personal information or use an organisation's computing resources.

More effective firewalls and available for taking these machines under your control and it is estimated that nearly 10,000 PCs are added to botnets everyday. So, the next time you have to complete this big project, you have options on the internet to rent out some botnets.

More effective firewalls and

HACKING THROUGH INSTANT MESSAGING

which increased more than 500% to over 100 unique threats in 2005 compared to less than 20 in 2004.

BLENDED THREATS

cracked down on these websites, they have shut down for obvious reasons. But Eastern Europe is still active on this front," says Niraj.

Hackers of this generation, in fact, are spoilt for choice. A CEO of a company in the US was nabbed last year for committing a "denial of service attack" on his competitor. You can hire some third party organisation whose job it is to bombard your competitor's website with millions of hits. Obviously, the website would throw up a denial of service and in turn, you benefit.

RANSOMWARE

And how about paying a ransom on the Net? Recently an internet subscriber in the US received an e-mail saying that the webserver was encrypted and has been locked by a password. He was told that the website had been taken over which shall be unlocked on paying a certain amount through his credit card. He paid the the money and the website was back.

CHANGING PROFILE

The typical picture of a hacker has often been one of an introverted, misunderstood teen with a great deal of repressed anger. However, one can now forget the stereo-

types, as virus writers raise in age and outlook. A popular perception of the writer as a dysfunctional is not accurate anymore. Most virus coders are well-justed youths who have normal relationships with their family.

FINANCIAL GAINS

The difference is that they are now being lured by the promise of financial gain. Online fraud is a growing international business. Since internet penetration in India leapt 54% last year to 38.5 million users, we are increasingly exposed to this global scourge. Basic security solutions and static passwords longer provide adequate protection.

A recent survey of enterprises in India shows that 54% of respondents become the victims of economic crime in the two years to 2005 — compared with in the previous survey. These victims, 15% had hit by incidents of 'false pretences' — a category of economic crime that includes crimes such as phishing, and other online frauds. Most alarmingly, nearly one third of these were detected by char-



tighter controls have made older forms of hacking difficult. Thus, the number of viruses housed within e-mail messages dropped by more than 50% in 2005.

But the newer forms of attacks are as troubling. First, a company often does not know that a hacker has broken the network and is tinkering with its resources. Second, these at-

INSTANT MESSAGING

One of the simplest and most effective ways so far has been that of viruses spreading through instant messaging applications. Typically, a message pops up on a user's screen asking him/her to accept a file. The message often comes from the buddy list so the user thinks that it is authentic, and accepts the file.

Explaining the new-age hacking phenomenon, **Freddy Magnum**, VP for product marketing, Fortinet (US), says, "The case in point is the rise of 'blended threats' which make use of a combination of attack vectors, such as web, email or instant messaging application to propagate viruses that infect computers with the intent to spam users. The public is often not aware that these attack vectors exist, but most network administrators are aware of the dangers."

BUYING VIRUSES

According to Niraj Kaushik, country manager, Trend Micro India and SAARC, people are also buying viruses off the Net. "Check this site called anti-detection.com, from where you can buy viruses. Organisations are willing to pay any amount of money to buy these viruses and snake into a rival company's data base," Kaushik says.

"Everytime people have

Websites with the addresses co.in and gov.in mostly fall prey to targets...about 1,400 Indian websites have been attacked in the first half of this year alone. The intrusion originates both from within and outside the country.

- Dayanidhi Maran at a Nasscom meet earlier this month.

tacks are difficult to trace. Many security programmes were designed to monitor network anomalies, but when a fraud is committed without it being detected as an anomaly, it becomes difficult to spot.

BOTNET

Take this method called botnet, which is essentially a huge network of computers across the world that is under one's control. Commands are

The virus then sends messages to all of the users' buddies. This method of attack is particularly effective if it is a senior manager's computer that gets infected, because most, if not all, employees would feel compelled to accept the file.

In the last few months there have been some obvious trends here, such as the rise of mobile viruses and Trojans,

TIPS TO AVOID THE TRAPS

Enterprises should look to building as many lines of defence as they can. That is, instead of relying solely on the firewall, businesses should be deploying gateway antivirus and malware solutions in addition to the firewall to screen traffic as it enters the corporate network. Personal firewalls and antivirus software should be installed on all employee PCs and laptops and the signatures should be kept up-to-date.

For bigger businesses, experts say there should be at least one engineer dedicated to looking at the security of systems and data. Close monitoring and patch management are often overlooked in companies. Security education for employees should be mandatory. Users sometimes disable the antivirus on their computers to make it "work faster", and then forget to turn it back on. The risks of turning off security should be made clear to users.

The most important thing to note, however, is that there is no silver bullet that will stop all threats to a company's network or data. The threats cannot be completely avoided. The best that companies can hope for is the management of these threats.