

A Stitch in Time Prevents Cyber Crime

How many times have you received virus alert e-mails from your network administrator that warn you against opening certain e-mails? How many times has your system crashed due to some illegal SPAM that has infiltrated your system through a pirated movie CD? How many times have certain websites popped open on your computer screen that are unwanted and lewd? The answer is the same for the majority of us: very often.

NEW DELHI - We've all come across cyber crime in some form or the other, be it big or small. This has become a reality that one can't shy away from anymore. Companies, organisations, governments and most importantly, Special Forces have all come together to fight this potentially deadly offence. "*Bachche ke delivery ho gayi hai, maa khairiyat se hai,*" (The baby has been delivered, the mother is fine); "*Shaadi ki tarikh fix ho gai thi, magar usse postpone kar diya gaya hai,*" (The wedding date had been fixed, but has now been postponed).

According to a leading newspaper, that is an example of e-mails intercepted by the anti-terrorist squad (ATS) after the arrest of three alleged terrorists from Aurangabad in May this year. The police then recovered 13 kg of RDX and 10 AK-47 rifles from them. Police sources concluded that these emails, which perplexed investigators at first, might have referred to the delivery of ammunition to be used in the serial bomb blasts in Mumbai that week. An alleged member of the Lashkar-e-Taiba who was arrested in the Aurangabad arms haul even told the ATS that he kept in touch with prime suspect, Zabihuddin Ansari, via e-mail. The mail when decoded by the ATS meant that the consignment was delivered and the module was fine. The



**Vishak Raman, Country Manager
Fortinet, India**

second email when decoded meant that the date for the operation was fixed but was soon postponed. This is a horrid example of how felonious activities are being perpetrated using the Internet to their advantage. India is not alone, the world over methods such as these are used by terrorist groups endangering the lives of thousands of innocent people.

The Basic Definition

Any criminal activity that uses a computer as an instrument, target or a means for

furthering crimes comes under cyber crime. A more general definition of cyber crime would be "unlawful acts, where the computer is a tool, target or both."

As a tool, the computer can be used for financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, email spoofing, forgery, cyber defamation, harassment and even cyber stalking.

The computer can be a target for unlawful acts like unauthorised access to the computer or the system, computer networks, theft of information contained in the electronic form, email bombing, trojan attacks, Internet time thefts, theft of computer system and by physically damaging the computer system. Cyber crimes are mainly directed against individuals (in person or property), organisations (government or firms) or the society at large. Seeing the rise in such security threatening activities, companies have started to fret. Not only are they looking for better than ever options, they are also trying to nip the issue in the bud.

Vishak Raman, country manager, Fortinet, India, said: "More businesses are getting online now, and more critical business processes are being transacted over the Internet. This has led to a corresponding increase in criminal activity. Also, the

Physically damaging a computer system: This crime is committed by physically damaging a computer or its peripherals when no one is around. Its generally done for vengeance against some person professionally or personally.

“Bot-networks are being used more frequently to carry out criminal activities. In a bot-network, a criminal infiltrates hundreds or thousands of computers around the world, transforming each one into a sort of “zombie” client, and then uses the network to carry out denial of service (DoS) attacks,” said Vishak Raman of Fortinet.

Phishing: The act of sending an e-mail to any user falsely claiming to be an established or legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft later on. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organisation already has. The Web is, in turn bogus and is set up only to steal the user's information. By spamming large groups of people, the “phisher” counts on the e-mail being read by a percentage of people who would actually list legitimate edit card numbers. Phishing, also referred to as brand spoofing or carding, is a variation on “fishing,” the idea being that bait is thrown out with the hopes that while most will ignore the bait, some will be tempted into biting.

Sale of illegal articles: This would include sale of narcotics, weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or simply by using email for communication. Many of the auction sites in India for instance, are believed to be selling cocaine in the name of honey.

Online gambling: There are millions of websites that are hosted on servers all over the world, which offer online gambling. In fact, many of these websites are actually fronts for money laundering according to

some experts.

Intellectual property crimes: This type includes software piracy, copyright infringement, trademarks violations and theft of computer source code.

Email spoofing: A spoofed email is something that appears to originate from one source but actually has been sent from another source. Email spoofing also causes monetary damage.

Forgery: Counterfeit currency notes, postage and revenue stamps, mark sheets, etc., can be forged using sophisticated computers, printers and scanners. Fake mark sheets and certificates are made using computers, high quality scanners and printers. This particular market is believed to be booming in India.

Cyber Defamation: When defamation takes place with the help of computers and the Internet, its called cyber defamation. If someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends, it is cyber defamation

Cyber stalking: Cyber stalking involves following a person's movements across the Internet by posting message which can be threatening or obscene in nature on the bulletin boards frequented by the victim, constantly bombarding the victim with emails etc.

Financial crimes: This includes cheating, credit card frauds, money laundering etc.

Cyber pornography: This includes pornographic websites; pornographic magazines produced using computers to publish and print the material and the Internet to download and transmit pornographic pictures, photos, writings, etc., without warning.

Net Policing

To quote a cyber law ‘expert’ - “Orders like blocking various websites are bound to be observed more in breach than

observance.” The governments might feel that they have a right to block content that they find offensive but implementation is next to impossible. In a free society like ours, validity of net policing must certainly be questioned,” said Rajkumar Chandrashekar of ICS.

Section 79 of the Indian IT Act defines the liability of the network service providers. Under this, the network security provider is presumed to be guilty unless he proves that the offence or contravention was committed without his knowledge. However, net policing has only limited effect: “Threats originating from India itself may be subject to police action, but not attacks originating elsewhere, such as China or Eastern Europe,” said Raman of Fortinet.

“Net policing is a relatively new phenomenon in India. Many countries and independent bodies have organised law enforcement teams which track discussion boards and online forums, including chatrooms, to try and detect criminals at an early stage – to pre-empt cyber-crime. Mainly, these groups focus on software piracy, pornography targeting children, and individuals or groups selling personal details such as stolen credit card numbers or Paypal account information,” said Rion Dutta, management consultant (Information Risk Management) of MIEL eSecurity.

Are the Lawmakers Listening?

Cyber Crime Investigation Cell, Crime Branch, CID, Mumbai, recently registered a case against one accused in a case of Phishing attack on a financial institution site. The accused was charged under section 66 of IT Act, sec 419, 420, 465, 468, 471 of I.P.C. r/w Sections 51, 63 and 65 of Copyright Act, 1957 which attract the punishment of 3 years imprisonment and fine up to 2 lac rupees.

The IT Act of 2000 has a number of laws that can apply in the case of a server attack on a particular company or organisation. Though it has not yet come into the force as much as the many

effects of a successful hack into a company's systems can now, potentially, even put a company out of business."

"The biggest danger to businesses comes from the proliferation and growing sophistication of your traditional threats, such as Trojans, viruses and worms. Previously, these threats could be countered by detecting their signatures, but these signatures are becoming increasingly difficult to define because the threats are now combining attack methods and signatures from different categories, such as viruses that are delivered by worms, or spoofed websites containing malicious code," he added. He further explained that today's threats generally affect all businesses equally because the worms, viruses and Trojans do not discriminate - that is, the threats do not first see how big or successful your company is before deciding whether or not to infect your systems.

"More and more information is becoming available online. Compared to a couple of years back, the prevalence of online banking, bill payment and convenient services like online shopping and reservations in today's world have made the threat of identity and data theft a lot more realistic scenario," said Rajkumar Chandrashekar, VP- Technology, Infinite Computer Solutions (ICS).

Types of Attack

Unauthorised access to systems and electronic data theft: This activity is more commonly called hacking. Hacking in simpler terms means an illegal intrusion

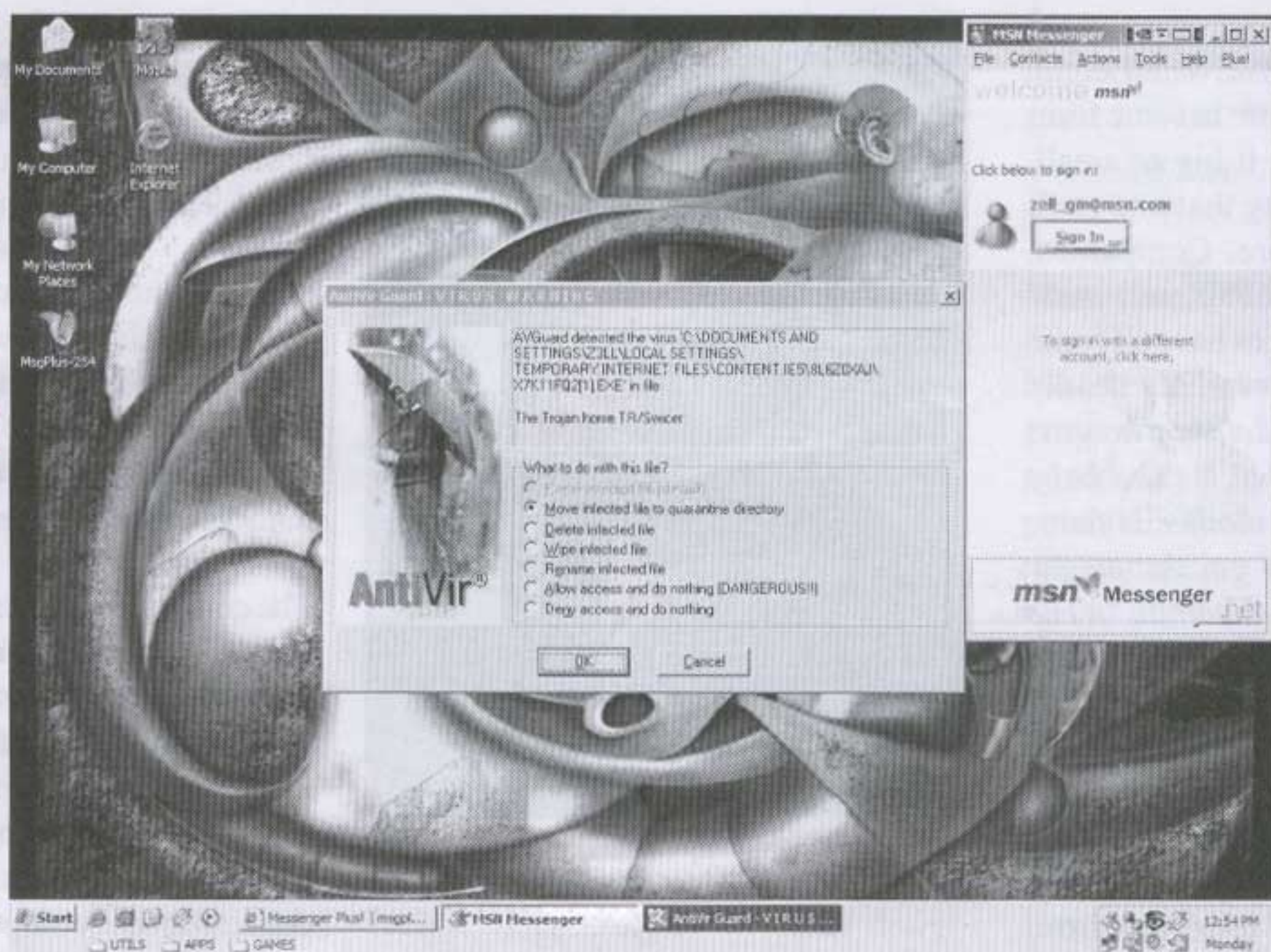
into a computer system and/or network. Every act committed towards breaking into a computer and/or network is hacking. Hackers write or use ready-made computer programs to attack the target computer. They possess the desire to destruct and they get a kick out of such destruction. Some hackers hack for personal monetary gains, like stealing credit card information, transferring money from various bank accounts to their own account. They are also capable of extorting money from any corporate giant by threatening to publish stolen information that is critical in nature.

Data diddling: This type of attack alters raw data just before it is processed by a

program into the bank's servers, that deducts a small amount of money from the account of every customer. No account holder will probably notice this unauthorised debit, but the rogue bank employee will make a considerable amount of money every month.

Virus / worm attacks: Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering it or deleting it. Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory.

There is another kind of threat that is emerging, which are targeted attacks. These are customised attack vectors, developed by organised criminal gangs that would target specific companies, typically to extract confidential or classified information. These attacks are a lot more difficult to detect and repel.



computer and then changes it back after the processing is completed. Electricity Boards in India have been victims to data diddling programs inserted when private parties were computerising their systems.

Salami attacks: These attacks are done for the commission of financial crimes. The key feature of this kind of attack is to make the alteration so insignificant that in a single case it would go completely unnoticed.

For example, if a bank employee inserts a

Logic bombs: These are event dependent programs that are created to do something only when a certain event (known as a trigger event) occurs. For instance, some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date (like the Chernobyl virus).

Trojan attacks: A Trojan as this program is aptly called, is an unauthorised program which functions within a seemingly authorised program, thereby concealing what it is actually doing.