

By Julian Rogers

As the web has become more sophisticated, so have the cyber criminals that lurk on its information super highways – the most sinister being those that use Mafioso-style tactics to extort money from firms by crippling their websites and demanding thousands of dollars to prevent future attacks. Russia and Eastern Europe is a known hotbed for these on-line protection rackets but, more recently, cyber gangs have been unearthed in Asia, in particular China and India.

The most popular form of attack is distributed denial of service (DDoS). It works by using 'zombie computers', PCs containing a hidden software programme that can be controlled remotely without the user's knowledge to flood the firm's website with useless data and requests for information. This malicious traffic slows the site until it buckles under the pressure and, in many cases, is forced offline. The criminals then demand that the companies pay up or pay the consequences.

DDoS attacks have risen sharply over the past few years and cost industries billions of dollars in lost business every year. However, exact figures are hard to gauge as many firms are reluctant to draw attention to the fact that their sites have been hit. Modest estimates suggest at least 2000 sites a week are affected by a denial-of-service, with large multinational companies the preferred target.

"Many large commercial organisations throughout the Asia Pacific region have been affected but, understandably, they want to remain anonymous," says Bernie Trudel, Principal Security Consultant, Asia Pacific, at network technology firm Cisco Systems. "Many companies do initially give into hackers' demands but invariably they look for technology solutions, especially as the ransom keeps escalating.

"After investigation, some of these organisations came to realise that their traditional security defences were only effective up to a point and now understand the importance of updating security policies, processes and tech-

nologies to protect themselves against these new types of threats. Unfortunately, some companies do not understand that many attacks over the internet are indiscriminate about who becomes a victim. In the best case, they become unwitting participants in attacks against other companies. In the worst case, they realise too late that their IT infrastructure has been compromised and they face significant costs in recovering their data and services."

The real threat of DDoS came to prominence two years ago when hackers targeted dozens of major international sports betting firms, deliberately timing their attacks to coincide with lucrative sporting events – one wave was launched during the run up to the US Super Bowl and another on the eve of the Cheltenham Festival, the highlight of the British horseracing calendar. Knowing the amount of lost revenue companies would face if their sites failed, the culprits then demanded up to US\$50,000 to stop further sabotage. Some are believed to have given into the criminals' demands until, eventually, investigators traced the attack back to Russia and arrests were made.

More recently, in January the Million Dollar Homepage site, created by a UK student selling pixels as advertising space, grabbed the headlines when it was struck down by a denial-of-service. Hackers threatened more bombardments unless they were paid a ransom of US\$5000, but their demands proved futile. The 21-year-old founder refused to give in, even when the site went down and the ransom was upped to US\$50,000.

President and Director of Mumbai-based web services provider Directi, Divyank Turakhia, is adamant that firms should not bow to the criminals' demands. "Do not pay the ransom," he insists. "There is no reason why they shouldn't ask for more once you pay the initial amounts." His company experienced first-hand the disruption 'denial of service' can cause after hackers launched a damaging offensive on its websites. The firm now has sophisticated software protection in place but still experiences at least two or three unsuccessful attacks by hackers every week.

H E L D T O R A N S O M

Are you safe from the cyber extortionists?





"By protecting your own systems you reduce the risk of a successful attack against your own business, but you also help the next firm by reducing the risk of your systems being used as a jumping off point for an attack against others"
Paul Ducklin

"Denial-of-service is undoubtedly the top source of financial loss caused to online businesses due to cyber crime. The typical motives behind such attacks are extortion, bragging rights, political statements, damaging competition and so on. As more businesses have started making a good amount of money because of their internet presence, groups of hackers have seen this as an opportunity to make a fast buck. These groups have started getting smarter and are attacking the mid-sized segment as the companies within it do not always have much technical expertise and rarely have protection against DDoS attacks," he says.

"The typical *modus-operandi* that I have seen is that a ransom note is sent between four and 72 hours after the DDoS attack has brought down a particular website or web application. The note asks for a sum of money and states that the group will protect you against further DDoS attacks for one year if you pay the ransom. However, they can't really 'protect' you from anyone else launching

MILESTONE FOR PC VIRUSES

This year marks the 20th anniversary of one of the first PC viruses, Brain. It was unleashed in early 1986 but due to the constraints of technology, could only spread through 360k floppy disks. It was created in Pakistan and designed as a 'boot sector virus', which described the area of the disk where it lurked. Brain was also the first 'stealth' virus, meaning it could try to hide itself from detection. If a computer user tried to view the infected disk space, Brain would display the original, unaffected boot space. It also meant that the virus could be spread between computers when users swapped floppy disks.

It is believed that the creator of Brain was a software firm that wanted to protect the products it developed and sold, but viruses then were seen as more of a hindrance than a threat. It's a very different story 20 years on. Currently, there are more than 150,000 known malicious programmes circulating and infecting PCs, causing serious threats to corporate and private security.

VIRUSES DOWN THE YEARS

1982 – Elk Cloner

Elk's creator, Richard Skrenta – a 15-year-old high school student – designed it to infect Apple II home computers. The virus spread through floppy disks and infected the machine's operating system, subjecting irritated users to a short and smug online poem to boot.

1986 – Brain

Infected PCs when floppy disks were swapped between users. Created in Pakistan, the virus was harmless compared to today's malicious programmes.

1992 – Michelangelo

Media hype surrounding Michelangelo led to panic amongst computer users worldwide. Experts predicted that the virus would infect five million machines on March 6th. It in fact turned out to far less deadly.

1999 – Melissa

Melissa was unique in the way that it combined a macro virus with one that plundered the user's address book to e-mail itself to new victims.

2000 – The Love Bug

Love turned to hate when this particularly nasty virus caused an estimated US\$10 billion worth of damage. Disguised as a message saying 'I love you', curious victims opened the infected e-mail and the bug spread rapidly throughout the world.

2004 – My Doom

A worm spread through e-mail. It is still considered to be the fastest growing malicious programme ever created.

an attack. If you pay once, in all probability they will just keep coming back for more. Worse still, if others realise that you have paid up, they will start extorting money from you too."

Dark side of the boom

Despite a whole range of businesses now utilising the web and security breaches becoming more commonplace, Turakhia highlights the fact that he has seen even tech-savvy organisations fail to take preventative action until they are actually hit, putting their livelihoods at serious risk. "Solutions are available today for protection against all kinds of DDoS attacks. Directi receives threats every week but they haven't affected us in a very long time because of the systems that we have in place," he points out.

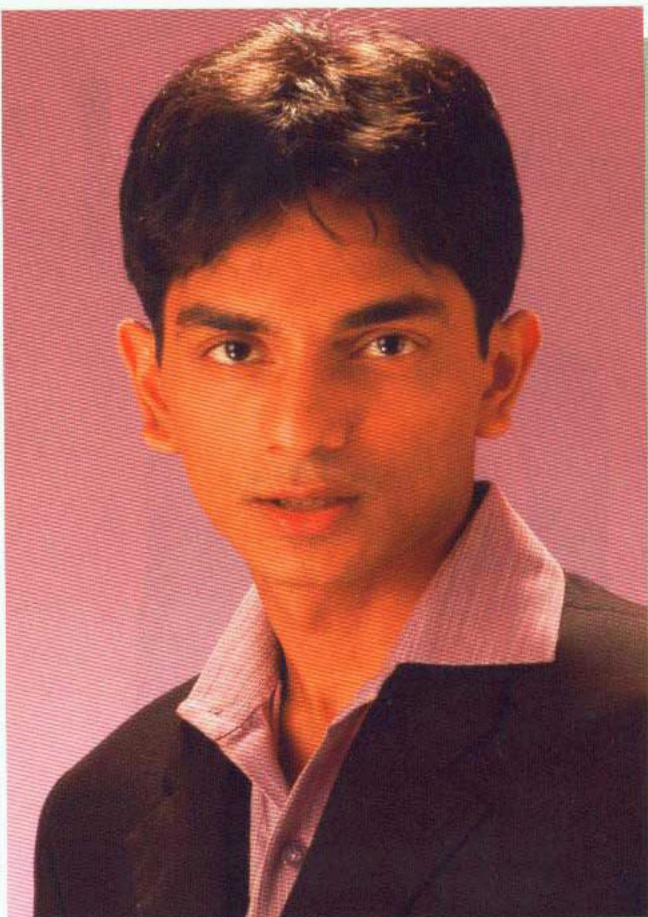
"The hardware and other resources required to defend oneself against large DDoS attacks is prohibitively expensive, although, some data centres and hosting companies are now giving this service for free by amortising this cost across a large set of customers."

And Paul Ducklin, Head of Technology at IT security provider Sophos' Asia Pacific division, believes the recent spate of DDoS attacks have forced businesses to wise up. "When it comes to computer security, I don't think the ostrich technique of burying your head in the sand is very widely used anymore, simply because it is so clear that it doesn't work," he explains.

"Computer security is a two-way street. By protecting your own systems you reduce the risk of a successful attack against your own business. But you also help the next firm by reducing the risk of your systems being used as a jumping off point for an attack against others." He also agrees with Turakhia that giving in to demands will only make things worse. "A technical concern over giving in and paying up the money – ignoring morality and business ethics for the moment – is that you are treating the symptom and not the cause. If you pay up now, are you prepared to pay up again, and again and again? What makes you think that paying up now will protect you, rather than marking you out as a long-term victim to be milked of money?"

Tracking down the criminals can take months and, even then, securing a conviction may be difficult. Different laws for different countries can mean a judicial headache for investigators. But Turakhia says the real problem comes down to tracking down the perpetrators in the first place as DDoS attacks come from several thousands computers and the owners do not even know that their machine is compromised. "Tracking attacks can be an impossible task," he adds. "Many times, the attacks are initiated from a different country altogether and the coordination of authorities between two or more countries is a long drawn process. It's going to take a long time before the legal system would be able to cause a decline in such activity. The only solutions are the technology solutions that you can deploy

to protect yourself against such attacks. If everyone started deploying these solutions by default, then such activity would decline by itself."



"If you pay once, in all probability the hackers will just keep coming back for more. Worse still, if others realise that you have paid up, they will start extorting money from you too"
Divyank Turakhia

to protect yourself against such attacks. If everyone started deploying these solutions by default, then such activity would decline by itself."

Ducklin also more practically gives a reason why jurisdiction is a tricky aspect for law enforcement. "How do you investigate and prosecute a crime which, for example, seems to have started out of Venezuela using a zombie PC in Israel to start a DDoS attack against a server in Finland, which hosts content for a company registered in the UK for business it conducts with customers in Thailand?"

Unfortunately, as long as the web is still around and widely used, it will always provide a hunting ground for hackers hell bent on launching malicious viruses and disruptive attacks. But there are those that argue that it's businesses themselves that CIOs needs to keep their eye closest on. Extortionists know that the majority of firms will not pay the ransom but thanks to the few that feel paying off the hackers is a small price to pay compared to a massive loss of revenue and negative publicity, the cycle continues and puts even more companies at risk. ■