

Cybercrime watch

detect and block malware before it can enter the corporate networks.”

Peter Wood, ceo of security tester First Base, agrees: “The problem of viruses has really morphed into the problem of sophisticated malware, especially trojan horse programs combined with worm-like behaviour. Blended malware programs are now the biggest threat and are usually linked with spam e-mail, infected web sites, free software and other social engineering vectors.”

More openings for attack

Web 2.0 and the rise in mobile offices are giving cybercriminals more openings for attack.

“Malware is now also more than just a Windows problem,” says Vanja Svajcer, principal virus researcher at SophosLabs. “Although the sheer number of Windows threats continues to far outweigh attacks against other platforms, we’ve seen cybercriminals begin to turn their attention to other operating systems such as Apple OSX and Linux and vulnerable cross-platform software. This trend only looks set to continue with the increasing popularity of portable devices such as the iPhone, iPod Touch, Google Android phone and ultra-mobile netbooks.

“With many organisations encouraging mobile working, devices like the iPhone have become commonplace among firms, but they can in fact pose a real threat,” he continues. “As an iPhone is constantly on-line ~ and so vulnerable to attack ~ whenever it is switched on, it becomes worth far more to a hacker than a compromised Mac or even PC. Add to this

the limited security options for the iPhone ~ no firewall and a slow uptake of third-party security software in favour of quirky extras ~ and from a hacker’s perspective, every iPhone is the same. Quite simply, to hack one iPhone means to hack them all, making it the cheaper option for cyber crooks and, no doubt, the weapon of choice in the not-too-distant future.”

The problem is that, while we’re seeing a number of new mobile devices being introduced into the market, mobile security is not yet receiving the same level of attention as PC security.

“This creates a serious vulnerability in the mobile market and makes it easy for hackers to target mobile users . . . which will lead to an increase in threats this year,” notes Guy Bunker, chief scientist, security solution provider Symantec.

So who are these cyber criminals and what are they trying to achieve?

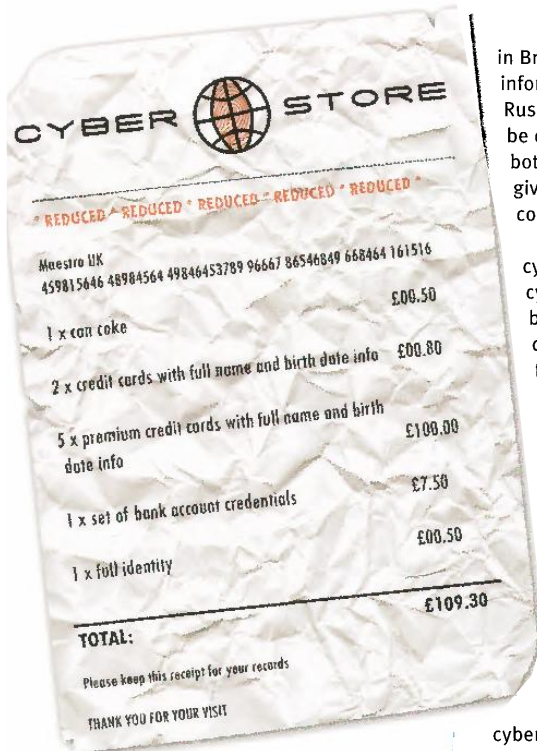
In the past, most malware was written by ‘kids’ who wanted to test their skills. Now, however, the majority of malware is written by professional and

. . . the English speaking world tends to have the best protection in place

talented programmers who are seeking commercial returns. They write innovative programs to penetrate computers and networks; they research vulnerabilities and use social engineering to ensure that their malware spreads widely.

“Virus writing has steadily been shifting away from the preserve of the mischievous nerdy teenager towards becoming a tool of the trade for international crime gangs, often based in Asia, Russia and South America. These gangs use hacking techniques and malware to steal information, distribute

To kick off our in-depth look at Security, Keri Allan concentrates on cybercrime, which has developed from a small-time irritation which was fairly easy to block into a major, and sometimes profitable, arm of organised crime



spam to sell illicit goods and use viruses to recruit home and work computers into botnets so that they can demand extortion money from web site owners who will be targeted with distributed denial-of-service (DDoS) attacks if they refuse to pay up," highlights Svajcer.

The US hosts more malware

According to Svajcer, the United States hosts more malware than any other country ~ at the end of 2008, the figure stood at 37 per cent. However, with regard to where malware is actually created, 24.5 per cent came from the English-speaking world, while 11.6 per cent originated in China. Much of the Chinese malware takes the form of backdoor trojans, but there is also a proportion that is designed to steal passwords from on-line gamers.

"Although the US is responsible for the largest proportion of malware, it's worth noting that the English-speaking world tends to have the best protection in place, particularly when compared to countries like China, Russia or Brazil," says Svajcer. "Here, user awareness is lower, meaning that infected systems and web sites in these countries typically stay on-line longer, representing a significant proportion of the overall threat.

"The majority of malicious code written

in Brazil is trojans designed to steal information from on-line banks. Russian hackers meanwhile appear to be concentrating largely on creating botnets and opening backdoors to give cybercriminals remote access to compromised computers," he notes.

Whatever route these cybercriminals take, all forms of cybercrime can cause problems for business. Sophisticated malware can locate passwords and try brute force attacks against other network resources, and it is very difficult ~ and costly ~ for most organisations to locate and disinfect these worms and trojans. The recent global problem with the Conficker worm is a classic example. One version of the worm infected 3.5m Windows computers worldwide in just four days.

According to Ben-Itzhak, data-stealing crimeware makes up about 95 per cent of current cybercrime, which is a big concern for businesses: "They are stealing confidential documents, e-mail content and addresses, login credentials to corporate systems, customer data and credit card data. As cyber gangs can later auction the stolen data and cash out, they are focusing on stealing this data."

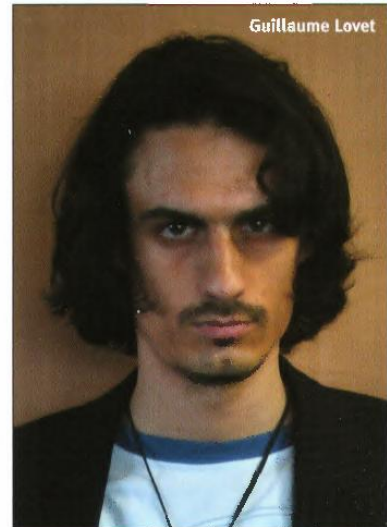
The biggest threats

Guillaume Lovet, senior manager, Threat Response Team, EMEA at Fortinet Technologies, highlights the biggest threats of which IS and IT managers should be aware.

"At the enterprise level, there are two main kinds of virus risks. These include theft to intellectual property and denial of service attacks (DoS) ~ preventing access to databases and applications.

"The loss or theft of intellectual property is an essential part of industrial spying or specific targeted attacks. These vary according to the profile of the cybercriminal. Experienced cybercriminals will try to penetrate the enterprise network by exploiting its weaknesses. A less-experienced cybercriminal will target the user by distributing trojans to employees. It's important to note that the e-mail is not the only major virus vector: in 2005 a big industrial spying attack occurred in Israel where the cybercriminal sent trojans to employees via mail through a demo software CD.

... user education is paramount, to help minimise infection from e-mails



Guillaume Lovet



Guy Bunker



Keri Allan has been writing about business and technology issues for the last eight years, covering a huge number of areas from CRM and ERP to consumer electronics and video games. She has an honours degree in Journalism and Sociology
web site www.keriallan.com



Yuval Ben-Itzhak

"A DoS attack aims to prevent access to the IT service by saturating it with a high volume of requests. The success of this relies on the volume of requests instead of their nature, so it is very difficult to prevent it. This kind of attack can focus directly on an individual organisation or distributed globally through a botnet.

"The motivation behind these attacks can be sabotage ~ a competitor wanting to destroy any competition ~ or cybercriminals practising the digital extortion racket," he continues. "In the case of cybercriminals, a ransom will be demanded and, if the enterprise does not pay up, the attack goes on and the service remains inaccessible. For on-line businesses, this threat can have a huge impact and, as a result, many companies unofficially pay the ransom (in a balance



Vanja Svajcer

sheet, it appears under security consulting services).

"Finally, an attack by a genetic virus can also lead to a *de facto* DoS attack. For instance, some spam-dedicated viruses can rapidly saturate an enterprise network's bandwidth; therefore blocking internal and business critical requests."

Now you know how you might be attacked, and by whom, the next step is to know how best to protect your organisation.

Sophisticated malware requires a sophisticated response. Of course anti-virus software with hourly updates is essential, as is a personal firewall on every desktop and laptop. However, user education is paramount, to help minimise infection from e-mails, infected web sites, peer-to-peer networking and countless other vectors criminals employ.

Issues to consider

There are all manner of issues to consider, and specialists offer their own advice to specific issues.

For example, Kevin Moreau, general manager at data back-up and disaster recovery specialist Acronis UK and Ireland, advises how to deal with zero-day attacks.

"The increasing strength of zero-day attacks (essentially when an unknown or unpatched vulnerability is exploited in the window between a vendor identifying a virus and when the vendor patch is issued) means that security vendors are not offering adequate protection to companies leaving business critical applications wide open to downtime," he says.

"Many presume that their chosen security vendor will protect them, but by the time the company has provided a patch for a security breach, it is often too late. Such threats jeopardise the security of both consumers and businesses' systems, but they also take a huge amount of time to fix and patch, even when a solution to an attack has been found. The fastest and most secure way to solve a zero-day attack is to simply travel back in time to a healthy state. As such, we strongly advise companies to consider how they back up and recover their systems in tandem with their security policies. Having the ability to roll back to an uninfected state guarantees security even when systems fail against threats such as the 'Conficker' worm. Plus, if you already have a back-up and recovery system in place, this form of protection is essentially free, something

to consider in IT budget crunch times."

Patrick Walsh, director of Product Management & Marketing at network security company eSoft, focuses on the importance of protecting yourself from Web 2.0 security 'holes': "To keep free of viruses, companies must have security-focused web filtering with up-to-the-minute updates. They must ask questions such as: how soon can a new malicious web site be discovered? How quickly are updates deployed? How often are pages revisited? How are new or changed web pages discovered? What are the criteria for marking a web page as malicious?"

... cyber gangs can later auction the stolen data and cash out

"Web 2.0 threats require Web 2.0+ security solutions and this requires a new way of viewing the world. Taking random walks around the web or waiting for anti-virus signatures is not an effective way of finding and stopping the spread of new threats. Security buyers need to insist on real-time updates and live crawling of new and dynamic content. Until buyers are asking the right questions of their web filtering vendor, they will remain stuck in the dark ages of the web filtering evolution."

Svajcer leaves you with this advice: "Never under-estimate the importance of properly configuring systems and keeping patches up to date. When a new security hole is found in an application or operating system, and a patch is available, organisations should have an infrastructure for testing the patch works properly and rolling that patch out across their user base. There is limited need for most users to have access to much of the IT system ~ ensuring minimal system privileges will help IT and IS managers better do their jobs and ensure their systems are able to deal with the very latest threats."