No longer just the 'Dirty Dozen'

As the quality and quantity of the malware threat evolves, Allan Dyer emphasises the importance of a comprehensive information security policy to protect your organisation from major malware-caused losses

The malware threat has changed enormously in the last quarter-century. In 1985, bulletin-board users found it useful to start a list of 'bad files' that were circulating. The original list had 12 entries, so it became known as the 'Dirty Dozen'. By 1989, there were over 50 entries, almost all destructive trojans, but the virus threat was rising.

A trojan could only harm your system if you chose to run the 'bad file', but a virus could copy itself and make previously-safe programs dangerous. Initially, the most successful viruses infected .com and .exe files, but boot sector viruses overtook them, partly because they can also spread on discs with no program files. In turn, they were overtaken by macro viruses, however, mostly infecting Microsoft Office documents, which were overtaken by e-mail viruses, notably 'Loveletter' in May 2000.

July the following year saw another outbreak become an international mainstream news story . . . and variants of the CodeRed worm were still successfully spreading 18 months later. Slammer, the fastest-spreading malware so far, was a worm that severely disrupted the internet and hit the headlines in January 2003.

***Allan Dyer** CISSP MHKCS MIAP AIMIS MSc (Tech) BSc is chief consultant of Yui Kee Computing Ltd in Hong Kong; with a background in microbiology and control engineering, he specialises in computer viruses, spam and promoting better information security. He is a founding member and President of Anti-Virus Asia Researchers (AVAR), Vice-Chairman of the HK Computer Society Information Security Specialist Group, and founding member of the Asia-Pacific chapter of the High Technology Crime Investigation Association. He contributes to Government consultations and public debate on information security issues*

Coming full circle

Now we are coming full circle: we are seeing large numbers of trojans and, although the internet is the main route of spread, spread on removable media, in the form of memory sticks instead of floppies, is common. An Autostart worm on a memory stick is today's equivalent of the boot sector virus that died out a dozen years ago. What we are not seeing is panicked mainstream media coverage. In February 1992, an anti-virus vendor excited the media claiming that "up to five million PCs worldwide" were infected by Michelangelo, but the number of PCs with overwritten hard drives on the activation day in March was tiny. In January 2009, a different anti-virus vendor produced a very conservative estimation, based on connections by infected machines to their servers, of 8.9 million Downadup infections, but media coverage was limited.

Security stories do get into the news: for example, the guilty verdict in the trial of David C Kernell, convicted at the end of April for breaking into Sarah Palin's Yahoo e-mail account was widely reported. To recap, breaking into one, poorly-secured webmail account results in worldwide news coverage, intensive investigation, and up to 20 years in jail . . . but you can get away with using a worm to break into 8.9 million PCs.

Three million types

It is not just that outbreaks of enormous size have become normal, the number of types of malware is staggering. One anti-virus vendor detected over three million types of malware in January 2009, but that grew to over seven million in May 2010.

The underlying driving force behind this growth is criminal gain. Michelangelo and Slammer caused serious damage, but their authors gained nothing. Today's trojans and botnets feature in a black economy where keyloggers gather on-line banking credentials, lists of credit card numbers are stolen from poorly-secured web sites, and these are sold to others to make the withdrawals. Botnets may be rented or sold for DDoS extortion or to send spam. The idea of causing a problem and demanding money to put it right is not new in the area of malware, the AIDS diskette was a real, but very badly executed, attempt in 1989. The typical extortion attack today targets a high-value site, such as on-line gambling, and threatens a DDoS attack, say on race night. The amount demanded is minor compared to the potential loss, and tracing the attacker is unlikely, so the victim pays.

So what is the future of the malware threat? Two things are certain: malware is not going to disappear, and the numbers will continue to grow. We can expect malware doing new things on new platforms. Social networking will be one area of development, already there have been rogue Facebook applications that trick users into spamming their friends and installing adware, and the possibilities for harvesting personal information to use for defeating 'security questions' are obvious.

Increasing criminal potential

Although malware on mobile phones has existed for the last six years, it has not been common, but there is increasing criminal potential. Two trends are on a collision course: on one hand, smartphones with internet browsing are becoming cheap and common; on the other hand, banks are desperate to counter on-line insecurities by using out-of-band transmission of a one-time password. How soon will it be before malware exists that collects your account details as you browse your bank web site, initiates a transaction and silently collects and uses the OTP sent by SMS?

Protection against malware requires defence in depth. Current anti-virus applications have changed a lot from the early days, in fact, they are probably called something like 'Client Security' or 'Total Protection', and include other security features, such as a host-based firewall, P2P control or content filtering. Their detection techniques have developed so much that talking about 'signature files' is misleading. However, malware developers have the advantage that they can continue modifying and testing until anti-virus software with the latest updates cannot detect them. Layering anti-virus with border protection and user education under the umbrella of a comprehensive information security policy will protect your organisation from major malware-caused losses.

When I think of league tables, it's usually more to do with the football results than anything else. But, if you're in business, in future, where you are in the league table is going to matter more about your carbon footprint than your goal difference.

The CRC Energy Efficiency Scheme (CRC) is a new regulatory incentive to improve energy efficiency in large public and private sector organisations. It is a mandatory scheme that aims to improve energy efficiency and reduce the amount of carbon dioxide (CO2) emitted in the UK. This is vital to achieving overall targets of reducing greenhouse gas emissions by 2050 by at least 80 per cent compared to the 1990 baseline.

CRC will affect large organisations in both the public and private sector. Organisations that meet the qualification criteria, which are based on how much electricity they were supplied in 2008, will be obliged to participate in CRC. Participating organisations will have to monitor their emissions and purchase allowances, initially sold by Government, for each tonne of CO2 they emit. The more CO2 an organisation emits, the more allowances it has to purchase.

By increasing energy efficiency the scheme will help organisations save money by reducing their energy bills. These savings should be well in excess of the costs of participating in the scheme. In addition, the better an organisation performs in terms of reducing its emissions, the higher it will appear in the annually-published league table, showing the comparative performance of all participants. This in turn provides a further benefit: all the revenue raised from selling allowances is 'recycled' back to participants, and the league table position affects how much of the revenue each organisation receives.

Greenpeace ranking system

Meanwhile, on the subject of league tables, Greenpeace has published a league table for familiar IT suppliers in terms of their ability to deliver Green IT. Greenpeace agrees with IT companies that technology has massive potential to cut carbon footprints, but it believes that they are dragging their feet in implementing effective solutions. Greenpeace's IT Leaderboard (see References) now offers a ranking system of technology companies, as a way to create 'friendly' competition and prod them