Viruses and malicious software

UK plc focused on the virus threat

Recent research has shown that UK consumer uptake of broadband has been accompanied by high virus infection rates.

This survey shows that more UK businesses than ever (88%) have a broadband link to the Internet. As a result, the threat from malicious software (such as viruses, worms and Trojans) has never been greater.

The good news is that UK businesses have responded. Almost every company uses anti-virus software.

How do UK businesses protect themselves against malicious software?

- Anti-virus software
- Anti-spyware software
- New signature files updated within a day
- Software searches for probable viruses
- New operating system patches implemented within a week
- Intrusion detection or prevention software

Most UK businesses also realise that installing anti-virus software alone is not enough. Historically, it has always been vital to also keep signature files up to date; four-fifths of companies now do this within a day.

At a medium-sized property company, a virus infected several computers before the anti-virus software had been updated. Several days worth of work were lost.

Patching discipline has improved; nearly nine in ten UK businesses apply new operating system security updates within a week of their release. Large companies tend to be slower than smaller ones; testing new patches do not affect their critical applications often takes time.

Interestingly, some businesses automatically update their signature files but take more than a month to install critical patches. Others never update their signature files but install critical patches within a day. Both groups risk infection.

The effort is paying off

Despite the increased threat, fewer companies had viruses than in the last two surveys. Infection rates have dropped by roughly a third since two years ago.

How many UK businesses were infected by malicious software in the last year?

<table>
<thead>
<tr>
<th>Year</th>
<th>Large Businesses</th>
<th>Overall</th>
</tr>
</thead>
<tbody>
<tr>
<td>2004</td>
<td>35%</td>
<td>43%</td>
</tr>
<tr>
<td>2002</td>
<td>50%</td>
<td>41%</td>
</tr>
<tr>
<td>2000</td>
<td>43%</td>
<td>43%</td>
</tr>
</tbody>
</table>

Companies without anti-virus software did not report many infections. Organisations that suffer virus infection tend to install anti-virus software afterwards. In addition, the nature of the virus risk has changed. Virus outbreaks that blatantly disable the target’s network are less common. Today’s viruses are more subtle. Their stealth techniques mean that some businesses without anti-virus software may not realise that a virus has infected them.

Organisations that update their signature files immediately seem slightly less likely to have infections than those that do not. One might expect a bigger difference. However, anti-virus software is becoming more sophisticated. Some packages don’t just scan for viruses they know; they also try to spot probable virus activity (through so-called heuristic logic). Most UK businesses have this kind of software and so depend less on signature file updates.

Patching discipline also seems to help. Companies that install critical patches within a day report fewer virus infections than those that wait even a week.

Analysis by sector confirms this. Financial services, travel, leisure and entertainment companies patch most quickly (70% within a day) and are least likely to have had an infection. In contrast, telecommunications companies are the slowest to patch and most likely to have had an infection.

However, even those patching within a day had infections, so patching alone is not enough. A multi-layer defence of patching, anti-virus software and intrusion detection software offers the best protection.

DTI recommends

- Check your anti-virus software also protects against spyware.
- Make sure your anti-virus software is up to date.
- Ensure your computers have the latest security updates and patches installed.
- Put a monitoring or audit process in place to check this.

For more information, please see www.dti.gov.uk/industries/information_security and www.getsafeonline.org
Yesterday’s war?

One might be forgiven for thinking that the virus threat is over. This, however, is far from the truth.

Virus infection was the biggest single cause of respondents’ worst security incidents, accounting for roughly half of them. Two-fifths of these were described as having a serious business impact.

In addition, while the number of companies infected has fallen, the average number of infections each suffered has risen to roughly one a day. While the median was a few incidents in the whole year, several businesses reported hundreds of infections a day.

Virus infections were more likely to have caused service interruption than other incidents. Usually, the disruption was minor, affecting a small number of staff. However, roughly a quarter of companies reporting a virus as their worst incident had major disruption, with important services (such as e-mail) out for more than a day.

Virus infections tended to take more effort to resolve than other incidents. Fixing some took more than 50 person-days.

A manufacturer described how its staff were lured into installing a Trojan onto their PCs. The Trojan recorded their passwords and sent them to its author, who then offered to help the company for a fee. It took more than a week to fix the problem; in the meantime, the company’s Internet connection was restricted.

Changing virus tactics

Two years ago, a small number of viruses dominated. The Blaster worm, for example, single-handedly caused more than half the worst incidents in large businesses. Like strategic bombers, these viruses were designed to cause large amounts of indiscriminate damage. Virus writers measured their success by how much media coverage they scored.

In contrast, over the last year, no single virus has caused such widespread damage. Instead, a huge number of different viruses and variants have attacked. Individual viruses are less memorable: 60% of respondents could not recall which virus caused their worst incident. Among those that could, the range was very wide.

What caused the worst virus infections in 2005?

The nature of viruses, and the motivation of their writers, has changed. Today, virus writers are aware that publicity risks jail sentences with little or no personal gain. As a result, today’s viruses have become more insidious. Like guerrillas, these programmes lie hidden on infected machines, gather information and target their strikes at valuable data. Cyber-criminals now use virus infections to get in under the radar of businesses and steal confidential data.

Some malicious programmes (known as “bots”) take over infected computers, which can then be used for the bot writer’s purposes. For example, large numbers of bot-controlled computers (known as “bot networks”) can bombard web-sites with traffic, denying service. Separate research indicates bots have infected many UK household PCs; this indirectly puts UK businesses at risk.

A large telecommunications provider’s worst incident was when bots infected some of its PCs. Fortunately it had an effective contingency plan for this scenario. Even so, cleaning the network took several weeks of effort.

Infected computers are often used to send out spam (acting as so-called “spam relays”). Several companies reported having being used in this way.

Spyware – blurring the boundaries

Spyware represents a growing threat. This software typically downloads when a user visits an unscrupulous web-site. It then logs and transmits activity without the user’s knowledge. Some spyware programmes come bundled with legitimate shareware or free software. Some even have licence agreements, making them appear benign.

A quarter of UK businesses are not protected against this threat. As a result, roughly one in seven of the worst malicious software incidents involved spyware.

This report is printed on Mega Matt paper which is made from 50% recycled and 50% chlorine-free pulp from countries that operate strict reforestation policies.

Department of Trade and Industry. April 2006. URN 06/804.