Corporate computer networks suffer rash of viruses

By Kate Mackenzie and Jonathan Loades-Carter in London and Scott Morrison in San Francisco
Published: August 17 2005 00:43 | Last updated: August 17 2005 20:19

Businesses on Wednesday rushed to secure computer systems as a rash of competing viruses targeted corporate networks around the world running some versions of **Microsoft**'s software.

Companies affected included CNN, ABC News, the **New York Times** and the Financial Times. Computers at **DaimlerChrysler**, **Kraft** and **UPS** were also reported to have been infected by the worms, known by several names including Zotob and Rbot.

“We have grouped them into four main families,” said Mikko Hyppönen, chief research officer at Finnish security software company F-Secure. “They're even fighting with each other; some versions are removing earlier versions. It seems like some fighting is going on within rival virus writing gangs.”

By Wednesday night 12 variants of the worm had been identified and Mr Hyppönen said more strains would probably be released over the next few days. However, the threat was expected to recede as companies updated software.

The impact is thought, so far, to be less than from similar attacks by Blaster in 2003 and Sasser last year.

“As people patch their systems and start to take precautions, [the threat] will diminish,” said Les Fraser, security spokesman for the British Computing Society.

However, Ken Allan, partner at Ernst & Young, said the cost could run into millions of pounds.

The rash of worms was prompted by Microsoft's publication last week of details of a vulnerability in Windows 2000, Windows Server 2003 and some versions of Windows XP. Microsoft frequently publishes details of vulnerabilities in its software as soon as “patches” to fix the flaws become available. However, virus writers are increasingly taking advantage of the interval to computer network administrators have time to install the defences. The day after the vulnerability was publicised last week an anonymous computer programmer, believed to be based in Russia and using the name “houseofdabus”, published a computer code on the internet that made it easy for virus writers to exploit the flaw. The first virus to use the software was published on Sunday, and on Wednesday at least five more were released.

EDITOR'S CHOICE

FT briefing: The Zotob and Esbot worms
Lex: Computer viruses
Software menaces move with times
Microsoft escalates virus war
Computer worm Sasser hits 1m PCs
Windows won't be enough to keep out terrorists

“Houseofdabus” is thought to be responsible for a similar piece of code in early 2004 that led to the propagation of the Sasser virus. While viruses were traditionally used by hackers to assert their supremacy in “graphiti” style claims to fame, the past 18 months have seen worms such as the Zotob variant, which allows an intruder to control an infected computer, increasingly used by criminal groups for sending spam e-mail or for fraud.

The worms exploit a security hole in the plug-and-play feature in the Windows 2000 operating system. Microsoft offered a fix for the bug as part of its monthly patching cycle last week. The software maker deemed the issue “critical”, its most serious rating.

“Zotob has thus far had a low impact on customers and only targets Windows 2000. Customers running other versions such as Windows XP, or customers who have applied the MS05-039 update to Windows 2000 are not impacted by this attack,” the company announced on Wednesday.

The worms appeared just days after Microsoft’s patch release, leaving users very little time to protect their systems and adding to fears that virus writers are becoming more adept at exploiting vulnerabilities. Many Windows 2000 users are unlikely to have patched yet since they need time to test the fixes before installing them.

“Zero-Day Exploits - whereby virus writers and hackers exploit vulnerabilities within hours of their announcement - are on the rise, making vendors more and more cagey about announcing them,” said Graham Titterington, a security analyst at Ovum.

Experts said that fully-patched terminals should be able to resist Zotob but that corporations had been slow to apply the latest patches.

“If you are responsible for network security inside an organisation it’s time to wake up and smell the coffee: you need to patch your systems now against these security holes or not be surprised when hackers and worms blast their way through,” said Graham Cluley, senior technology consultant at IT security group Sophos.

A spokeswoman for the New York Times said the newsroom and other corporate areas of the newspaper had been affected but that the problem had been rectified. “We introduced some software patches and we don’t expect it will affect production of today’s newspaper,” she said.

A Royal Mail spokesman said some of the state-owned group’s offices, including its head office in Old Street, London, were hit by the worms but mail operations were unaffected.

“All the indications are that the mail operations are going ahead as it should be today,” the spokesman said.

A CNN spokeswoman said the worms caused disruptions to the New York and Atlanta offices for about one hour on Tuesday night, but that broadcasting continued as the offices used their London and Washington DC counterparts for backup.

The Wall Street Journal published a notice to readers in its European edition on Wednesday alerting them to production issues overnight, but a spokesperson said the newspaper did not use the software that was affected by the worms.

Mr Hartmann at Trend Micro said the outbreak at this point was still “controllable” because the malicious code targets older Windows 2000 software as opposed to newer Windows XP software. He said the number of machines vulnerable to this virus was much smaller than in previous

outbreaks from viruses such as Code Red or Nimda.

Symantec, the world's leading IT security company, on Wednesday morning raised its potential damage rating to "medium" and warned that if left unpatched the virus could allow a remote attacker full control over a compromised computer. However, it was already offering a downloadable tool for its removal.

Links

Security information from Microsoft about the Windows vulnerability

Information from anti-virus companies:

F-Secure

Mcafee/Network Associates

Symantec

Sophos