New Strains of Viruses may Emerge from the Windows Source Code Leak

Submitted by: Marylebone Media Relations
Monday, 16 February 2004

16/02/04 - On 12th February, Microsoft Corporation announced that part of the source code for Windows 2000 and Windows NT 4.0 had been leaked and illegally published on the Internet. Kaspersky Labs believes that this will herald a new era for viruses.

Access to source code makes it far easier to identify previously unknown vulnerabilities in the Windows operating system. Virus writers and hackers can then use these breaches to attack computers. Having the source code makes it possible to integrate malicious programs into the heart of the operating system. Viruses are then an undetectable part of Windows. This is dangerous, as it opens the door to a new generation of stealth viruses, which mask their presence in the system by controlling the operation of anti-virus programs and firewalls.

“The leaking of the Windows source code is a historic event in computer virology; a new round of virus v.s anti-virus has begun. The Internet community may face new viruses attacking vulnerabilities in Windows for which no patches yet exist. The appearance of system-level viruses, which are almost impossible for traditional anti-virus software to detect, is another real danger,“ comments Eugene Kaspersky, Head of Anti-Virus Research at Kaspersky Labs, “Nevertheless, virus analysts are prepared for such contingencies and will rise to this new challenge from by the computer underground”.

The day before Microsoft announced the leak, several hundred megabytes of text files containing source code for Windows 2000 and Windows NT 4.0 were published on a number of hacker websites. The files included the code of key applications such as WINSOCK (the application which works with network resources), Internet Explorer, and Outlook. All the websites where the code was published have been closed down, but there is no guarantee that the information will not resurface.

The source code lays bare the internal workings of the operating system, exposing the nuts and bolts of the system. Access to source code makes it possible for users to modify programs, to adapt them to their own needs, and to independently correct errors without having to wait for the manufacturer’s response.
It should be remembered that a user needs to have substantial IT experience in order to take advantage of such an opportunity.

###

Media Contacts

Sarah Buttery

Kaspersky Lab UK

+44 870 011 3461

sarah@kasperskylab.co.uk

http://www.kaspersky.co.uk

Sara Claridge

Marylebone Media Relations

+44 1344 876558

sara@marylebone.co.uk

http://www.marylebone.co.uk

Distributed via Press Release Wire (https://pressreleases.responsesource.com/) on behalf of Marylebone Media Relations