R&D, The Glassmill, 1 Battersea Bridge Road, London SW11 3BZ
Tel +44 (0)20 7924 3010 Fax +44 (0)20 7924 3310
solutions@**mi2g**.com http://www.**mi2g**.net

mi2g

news release - London, UK, 14 August 2002

Windows regains mantle of most vulnerable OS

London, UK, 11:30 GMT 14 August 2002 – The latest figures compiled by the Intelligence Unit at **mi2g** indicate that Windows has once again regained the position of most vulnerable online operating system.

Although overt attacks on Microsoft Windows based systems had been broadly falling in the first quarter of 2002, the rate at which Windows systems are being compromised is outpacing Linux again, having increased by 5% in June followed by a further 12% rise in July. In comparison, attacks on Linux systems decreased by 39% in June.

In April and May this year, Linux systems were successfully attacked worldwide in far greater numbers (2192 / 2057) than Windows systems (1677 / 1991). In June and July however, the trend reversed and more Windows systems (2082 / 2338) were compromised than Linux systems (1260 / 1711).

The sudden rise in attacks on systems running Linux earlier this year was due to several easily exploitable vulnerabilities being uncovered in open source third party applications such as PHP scripts and bulletin boards. Bad or default configuration of Linux and the applications running on it were also determining factors for the success of the overt attacks.

A total of 27,273 successful overt digital attacks have taken place so far in 2002, 47% were on systems running Windows, 36% on Linux based systems and 17% on various operating systems including Unix, BSD, Solaris, AIX and others.

"The recent Apache vulnerabilities have affected both Windows and Linux systems. Online administration is about overall configuration management. At one level it is about patching the known vulnerabilities of the OS and the server software that runs on top. At another level it is about selecting reliable third party applications so as to stop them from being used as a launch pad for deeper penetration," said DK Matai, Chief Executive of **mi2g**.

The top ten domains that have been the biggest victims of digital attack so far in 2002 are: *.com* (Commercial), *.de* (Germany), *.br* (Brazil), *.net* (Network), *.org* (Organization), *.it* (Italy), *.uk* (UK), *.kr* (Korea), *.tw* (Taiwan) and *.ch* (Switzerland) in that order.

Executive Summary of the July 2002 SIPS Report – July was the second most intense month on record for overt digital attacks with 4,879 incidents, the peak being May 2002 with 4,897. The most prominent hacker group in July was *hax0rs lab*. The operating system most susceptible to attack was Microsoft Windows followed by Linux reversing the April/May one off blip in which Linux overtook Windows temporarily. The most attacked domain after *.com* was *.it* (Italy) followed by *.br* (Brazil) and then *.net* and *.org*. The principal motives for digital attacks have been political tension and protest; anti-globalisation, environmental and animal rights protest; disgruntled or misdirected workforce; intellectual challenge; commercial gain.

[ENDS]

R&D, The Glassmill, 1 Battersea Bridge Road, London SW11 3BZ
Tel +44 (0)20 7924 3010 Fax +44 (0)20 7924 3310
solutions@**mi2g**.com http://www.**mi2g**.net

mi2g

Editor's Notes:

mi2g has been collecting data on overt digital attacks going back to 1995 via the SIPS (Security Intelligence Products and Systems) database. The SIPS database has information on over 70,000 overt digital attacks and over 6,000 hacker groups. The **SIPS** intelligence citations include the 2002 Computer Security Institute (CSI) / Federal Bureau of Investigation (FBI) Computer Security Issues and Trends Survey [Vol. VIII, No. 1 – Spring 2002].

Detailed copies of the **SIPS** reports for each month, including back issues can be ordered from the intelligence.unit@**mi2g**.com. A vetting process may be carried out prior to the release of the **SIPS** reports to individuals and for overseas orders.

mi2g solutions engineering pays particular regard to security. **mi2g** advises on the management of Digital Risk and incorporates Bespoke Security Architecture in its SMART sourcing solutions. **mi2g** has pioneered the Contingency Capability Radar to assist in rigorous business continuity planning based on ISO 17799.

For further information – www.**mi2g**.net

What are Asymmetric Threats?

Any threat, which is disproportionate, such as the risk of a small group attacking a large country or a few individuals harming thousands is described as asymmetric. Chemical, biological, radiological, nuclear and digital (CBRN-D) attacks can all manifest asymmetrically.

What is Bespoke Security Architecture?

Bespoke Security Architecture brings together firewall layers, intrusion detection and other defensive structures, as well as automated intelligence techniques with legal, human resource and company policies.

What is Digital Risk Management?

Digital Risk Management deals with a variety of issues associated with implementing digital solutions and integrating Service Level Management. It includes selecting the optimum technology set, managing external partners and alliances, linking payments to targets, defining rigorous quality control procedures, managing the growth in online traffic post launch, achieving the expected return on investment, and bringing about the changes in the corporate culture required for successful eBusiness.

What is the Contingency Capability Radar?

The Contingency Capability Radar is an ISO 17799 based platform, containing tools and templates to assess and visualise risk exposure of an entire global enterprise.

What is SMART Sourcing?

mi2g SMART Sourcing is the careful selection of cost effective and trustworthy suppliers from around the world for building and maintaining highly secure digital platforms on a 24 by 7 basis.

First contact for additional information – Intelligence Unit, **mi2g**
Tel: +44 (0) 20 7924 3010 Fax: +44 (0) 20 7924 3310 eMail: intelligence.unit@**mi2g**.com