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**.com

mi2g

press release - London, UK, 8 January 2002

Escalation in Politically Motivated Hacking

London, UK, 2:00pm GMT 8th January 2002 – The latest figures compiled by the **mi2g** Intelligence Unit have shown that politically motivated hacking has increased in 2001. The principal reasons cited for the overt hacking attacks include intellectual challenge, disgruntled personnel, political motivation (including ideological differences) and criminal activity.

Global Hot Spots

The China-Taiwan standoffs and the US-China spy plane incident in 2001 made the .cn China domain and .tw Taiwan domain, two of the most defaced domains after .com and together they accounted for just under 9% (2,653) of total defacements for 2001. The domain .tw rose by 1,178% to 1,355 from 106 and the .cn domain rose similarly by 1,326% to 1,298 from 91.

The number of Israeli domain (.il) defacements rose by 220% to 413 in 2001. As the Palestinian Intifada continued many hack attacks on the Israeli domain came from sympathetic hackers including attacks originating from predominantly Islamic countries such as Egypt and Pakistan.

The number of web site defacements of Indian domains (.in) rose by 205% to 250 and 300% for Pakistan (.pk) to 72 in 2001.

UK

The UK Government domain .gov.uk experienced a 378% increase in web site defacements to 43 from 9 in 2000. The UK organisations domain .org.uk rose to 25 from 5 and the UK commercial domain .co.uk increased by 181% to 385 from 137. Many UK companies use the global .com domain and those statistics are not specific to geography. Anti-capitalist protest, criminal activities and anti-NATO sentiment were principally behind the attacks.

USA

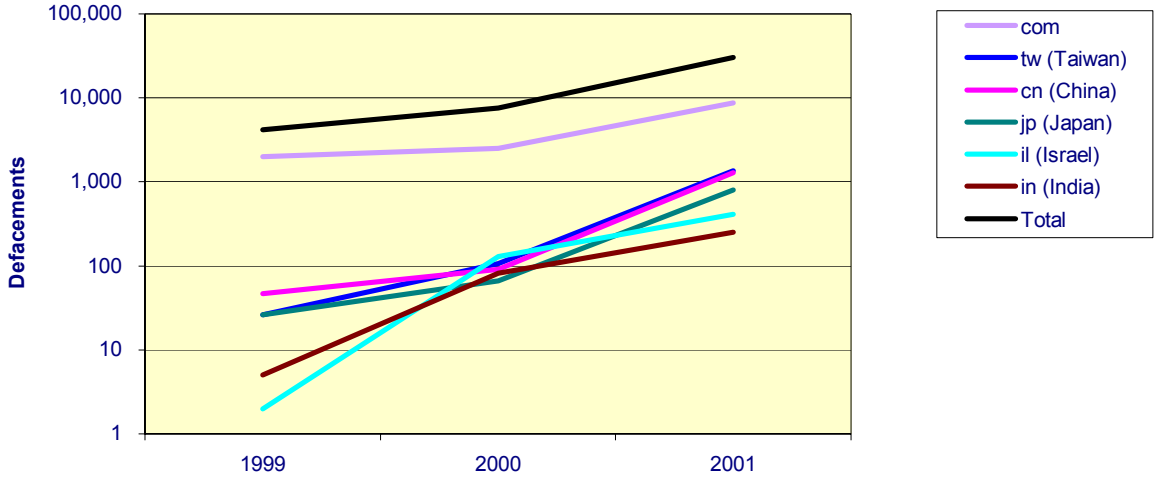
Dotcom (.com) domains accounted for nearly 30% (8,736) of all web defacements (30,388) in 2001. They include both US and non-geography specific global entities. The US government domain .gov experienced a 37% increase in web site defacements to 248 from 181 in 2000. The US military domain .mil experienced a 128% increase in web site defacements.

> *"Global web site defacement is indicative of the general conflicts prevalent in the physical world. 2002 may be a year in which politically motivated attacks, both physical and electronic, could complement strikes from disgruntled employees and organised crime,"* said DK Matai, Chairman and CEO, **mi2g**.

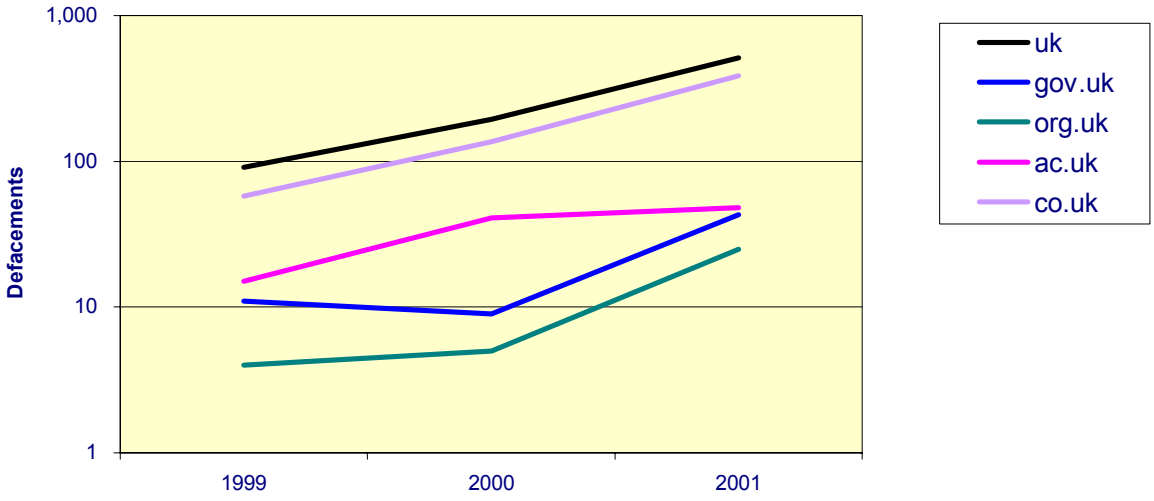
R&D, The Glassmill, 1 Battersea Bridge Road, London SW11 3BZ
Tel +44 (0)20 7924 3010 Fax +44 (0)20 7924 3310
solutions@**mi2g**.com http://www.**mi2g**.com

mi2g

Global Hot Spots - Defacements by Domain (1999 - 2001)

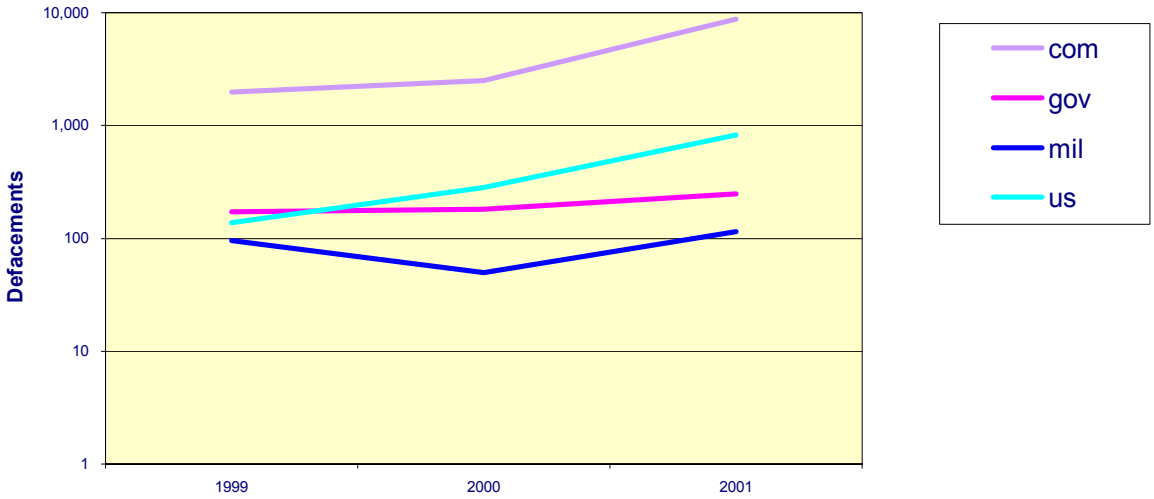


UK Sites - Defacements by Domain (1999 - 2001)



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**.com

US Sites - Defacements by Domain (1999 - 2001)



Editor's Notes:

More statistics can be obtained from www.mi2g.com/status

About mi2g:

mi2g Digital Solutions Engineering pays particular regard to security. **mi2g** advises on the management of eRisk and incorporates Bespoke Security Architecture in its SMART sourcing solutions.

mi2g builds highly secure intranets and extranets, digital communities and data warehouses that are specifically constructed for data mining, customer relationship management and enhancing the network effect.

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

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 eRisk Management?

eRisk 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 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**
Telephone: +44 (0) 20 7924 3010 Facsimile: +44 (0) 20 7924 3310 eMail: intelligence.unit@mi2g.com