news release - London, UK, 13 November 2002

Hacker attacks on Government systems declining year-on-year

London, UK, 16:30 GMT 13 November 2002 – Australia has been the worst hit victim of overt digital attacks on its military and government computer systems in November, with 32 so far. 9th November saw the compromise of 13 computer servers on a New South Wales state government network in a synchronised assault on a single day. The other big military and government digital attack victims this month have been the US (18) and China (10).

The worst hit military and government attack victims in 2002 have been China (173), USA (162), Turkey (109), Brazil (108) and Australia (66). Overt digital attacks on government and military systems worldwide are falling and comprise less than 2% of all overt attacks in 2002. However, 18% of all overt attacks on China in 2002 were targeted at government and military systems. The proportion of attacks focused on the military and government systems for the US was less than 1%, Turkey was 20%, Brazil was 2% and Australia was 6%. The rest of the attacks were targeted mostly at small to medium size businesses, some large businesses, educational establishments and not-for-profit organisations.

In 2002, the most notable examples of overt digital attack on military and government computers were: The US Government House of Representatives, US Department of Agriculture, New York State Department of Education, US National Park Service, Goddard & Marshall Space Flight Centers, Washington State Library, the US National Institute of Aging and the US State Department's International Information Programs.

The overall trend for overt digital attacks on military and government online computers is declining since April and May 2001, which had marked the worst period of attacks on US and China government and military computer systems because of the spy plane incident. There were 2,031 overt attacks on government and military targets recorded worldwide in 2001 by the **mi2g** SIPS database. For 2002, the **mi2g** Intelligence Unit is projecting a total of 1,400 such attacks, ie, a decline of a third year on year.

The overall trend for digital attacks is on an upward curve with 31,322 overt digital attacks recorded in 2001 and 64,408 - more than double - recorded in 2002 already. The revised projection for 2002 is for over 70,000 such attacks mostly targeted at small to medium size businesses.

"The major challenge for the nation states in the coming decade is to be able to respond adequately to the digital attacks taking place not just on government systems but also on small to medium size businesses. This is where governments and the defence forces will have to concentrate their cyber-security efforts so that adequate safety and protection can be provided to the civilian components of our online society that are incapable of defending themselves against concerted international attacks," said DK Matai, Chairman and CEO of **mi2g**

In 2001, in terms of military and government victims, the top five overtly attacked countries were China (394), USA (386), Brazil (164), Taiwan (110) and Mexico (67). 2001 had also seen the continuation of the ongoing cyberspace tensions between China and Taiwan, which started in Q3 1999.

1999 was the first year for which cyber warfare was predicted and recorded by **mi2g**. 1999 included the NATO-Serbia conflict and China-Taiwan standoff and it was the worst period for worldwide economic damage attributable to government and military computer systems as well as loss of digital performance and degradation in capability as a result. The estimated worldwide damage through attacks on government and military computer systems has been calculated at between $1.5 and $1.8 Billion for 1999; $740 and $ 900 Million for 2000; $960 Million and $1.2 Billion for 2001; and $560 and $690 Million for 2002 so far.

[ENDS]

Editor's Notes:

In a speech delivered last year in London which was introduced by Andrew Pinder, the UK Government eEnvoy, **mi2g**'s Chairman and CEO, DK Matai had predicted that the damaging situation from digital attacks would arise in the future based on the trends observed between 1995 and 2001. A concrete way forward to solve this unfolding problem was suggested in the speech, which is available at:

http://www.mi2g.net/cgi/mi2g/reports/int_briefings/221001.pdf

Also note the **mi2g** release titled: “Government backed counter-attack-forces necessary in future”

http://www.mi2g.com/cgi/mi2g/press/111102.php

What is EVEDA?

EVEDA stands for Economic Value Engine for Damage Analysis. EVEDA is a component of the SIPS (Security Intelligence Products & Systems) database, which estimates economic damage as loss of productivity, management time, Intellectual Property Rights (IPR) violations, customer and supplier liabilities and share price decline where applicable. EVEDA collects its information from a variety of open sources and measures the economic value associated with a particular brand or publicly listed company based on a unique set of algorithms developed by the **mi2g** SIPS team in conjunction with risk analysts.

Over the last six years, the worldwide economic damage estimate for all forms of digital attack has been estimated via EVEDA at between: $36 and $44 Billion (2002 so far); $35 and $43 Billion (2001); $22 and $27 Billion (2000); $18 and $22 Billion (1999); $3.6 and $4.4 Billion (1998); $2.9 and $3.7 Billion (1997); $800 and $970 Million (1996).

What is an “overt digital attack”?

Hacker attacks on digital systems, such as computers and digitally controlled machines, can be either covert or overt. Covert attacks are not reported, validated or witnessed by a reliable third party source, whereas overt attacks are either public knowledge or known to an entity other than the attacker(s) and the victim(s).

mi2g defines an overt digital attack as being an incident when a hacker group has gained unauthorized access to an online system and has made modifications to any of its publicly visible components (such as a broadcast, service routine, payment / data collection or print out) whilst executing:

1. Data Attacks: The confidentiality, integrity, authentication or non-repudiation of transactions based on the underlying databases is violated. Such attacked databases may include confidential credit card numbers, identity information, customer and supplier profiles and transaction histories;

2. Command and Control Attacks: SNMP (Simple Network Management Protocol) controlled computers, routers and switches, networks of ATMs (Automated Teller Machines), DCS (Distributed Control Systems), SCADA (Supervisory Control And Data Acquisition) systems or PLCs (Programmable Logic Controllers) have been compromised.

What are the motives for "overt digital attacks"?

The principal motives for digital attacks have been political tension, protest and digital warfare; espionage, surveillance and reconnaissance; destruction of competitive advantage or share price; disgruntled or misdirected workforce issues; anti-globalisation and anti-capitalism protest; environmental and animal rights activism; intellectual challenge and recreational hacking; financial gain.

SIPS Background

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 108,000 overt digital attacks and 6,100 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.

First contact: Tel: +44 (0) 20 7924 3010 Fax: +44 (0) 20 7924 3310   eMail: intelligence.unit@**mi2g**.com