Tel +44 (0)20 7924 3010 Fax +44 (0)20 7924 3310
solutions@**mi2g**.com http://www.**mi2g**.net

mi2g

news release - London, UK, 8 October 2002

UK & Australia Fresh Targets in Hack Attacks

London, UK, 17:00 GMT 8 October 2002 – Digital attacks on the UK and Australia in particular and the US at large continue to mount as tension over the Iraq issue and further violence between Israel and Palestine remains entrenched.

The preliminary estimate of Economic Damage for the first week in October based on initial calculations puts the total damage caused worldwide by all hacker groups at between US $51m (£33m) and $63m (£40m). [Source: EVEDA (Economic Value Engine for Damage Analysis) component of SIPS] EVEDA defines economic damage as loss of productivity, management time, Intellectual Property Rights (IPR) violations, customer and supplier liabilities and share price decline where applicable.

The overt digital attacks have included several high profile breaches such as the online systems of the US State Department, the California Energy Commission and the World Health Organisation's South East Asia Regional Office (WHO SEARO).

The Unix Security Guards (USG), a Pro-Islamic hacking group, was responsible for 1,417 of the attacks in October so far: 1,142 on USA, 124 on UK and 99 on Australia. USG was first formed in May 2002 and so far it has carried out 1,772 anti-Israel and anti-US/UK attacks. Every time there has been an incursion of Israeli forces into Palestinian controlled territories, including 7th October's raid on Khan Younis in which 14 Palestinians were killed, USG has launched a relentless series of attacks against the US, UK and Israel. Australia and Ireland are also victims.

Rank	Country (top 5)		Code	Attacks
1	🇺🇸	United States	US	1979
2	🇬🇧	United Kingdom	GB	595
3	🇮🇹	Italy	IT	173
4	🇧🇷	Brazil	BR	109
5	🇦🇺	Australia	AU	103

USG have been responsible for 21% of the 595 attacks on the UK so far in October, always leaving highly politicised messages which are anti-Israel, US and UK.

Although it is too early to say, the initial estimate of economic damage worldwide from overt digital attacks in September has been calculated at between 270 and 325 Million US Dollars [£170m and £210m].

"It is clear that these digital attacks are having an impact on business productivity, confidence levels, brand names as well as compromising trust and integrity," said DK Matai, Chairman and CEO of **mi2g**. *"Board level executives are only now beginning to recognize that protecting critical infrastructure is a priority and it requires a long term strategic approach."*

[ENDS]

Editor's Notes:

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). There are two types of overt digital attacks: Data attacks and Command and Control attacks. **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.

What is the economic impact of "overt digital attacks"?

The economic impact is different for the two types of overt digital attacks: Data attacks and Command and Control attacks. For the victims of data attacks the fallout is likely to be in the area of business interruption, denial of service, identity or corporate information theft, copying or deletion of vital business information, loss of sensitive intelligence or intellectual property, loss of reputation and / or share price decline. Command and control attacks are more sophisticated and have invariably required insider help to perform and sustain. The possible consequences are either the slow down or disruption of critical infrastructure, such as, transport, telecommunications, financial payment systems and utilities.

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 90,000 overt digital attacks and 6,090 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