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

mi2g

news release - London, UK, 22 October 2002

Economic Damage from Digital Risk Stabilising

London, UK, 17:00 GMT 22 October 2002 – The estimate for the total economic damage arising from overt digital attacks has changed little in 2002 despite a doubling in the number of attacks year on year. This demonstrates a remarkable decline in the quality of targets chosen for digital attack. The projected estimate for overt digital attacks worldwide is $7 Billion for 2002 compared to $7.7 Billion for 2001. This stands in contrast to the projected 65,000 overt attacks for 2002 compared to 31,322 for 2001.

The principal targets for overt digital attacks in 2002 have been the US, Germany and UK amounting to half of all attacks across the world. October has been another record-breaking month for overt digital attacks with 11,730 attacks so far. The last quarter saw damage estimated at $2.5 Billion from overt digital attacks and October has already seen $700 Million worth of economic damages.

Economic damage through viruses, worms and hoaxes has been the worst in October for 2002 contributed in part by Bugbear, which alone caused in excess of $950 Million damage worldwide. The number of new viruses being discovered, however, is falling: 265 new viruses and worms have been discovered in 2002 in comparison to 273 in 2001 and 422 in 2000. The last quarter saw an estimated damage of $3.8 Billion from viruses and worms such as Klez, Yaha and Sircam.

When overt attacks, both recorded and unrecorded, are taken together with covert attacks, viruses and worms, the cumulative economic damage worldwide stands at between $32 and $39 Billion for 2002 so far. Although 2001 and 2002 have suffered similar economic damages and appear to be stabilising, previous years have shown exponential growth.

New vulnerabilities announced by software vendors in 2002 so far are 1,129 of which a record 276 were announced in October alone. Vulnerabilities pertain to the operating system, server software and third party applications and have a cumulative impact on digital attacks, for example, where blends of new and old vulnerabilities are exploited simultaneously. By comparison, there were 1,506 vulnerabilities announced in 2001, 990 in 2000, 861 in 1999 and just 245 in 1998.

"The proliferation of automatic digital attack tools and malicious code-writing kits on the internet coupled with the growth in software vulnerabilities has enabled larger numbers of computer systems to be compromised in a single attack," said DK Matai, Chairman and CEO of **mi2g**. *"This has meant that whilst the volume of security breaches in 2002 has risen significantly the quality of the targets selected and the consequent economic damage done has been more diffuse."*

[ENDS]

Editor's Notes:

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: $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 97,000 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