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

news release - London, UK, 11 November 2002

Government backed counter-attack-forces necessary in future

London, UK, 11:30 GMT 11 November 2002 – As the damage done by radical, criminal and intellectually motivated hackers continues to rise, about six Billions Dollars of economic value was destroyed worldwide by overt and covert digital attacks including viruses and worms in October alone. As a result, the **mi2g** Intelligence Unit predicts there will be a growing requirement for Governments to intervene and to mobilise counter-attack-forces that protect economic targets and critical national infrastructure constituents on a 24/7 basis.

In a study to be released later this month, **mi2g** will reveal a new trend developing with far more damaging economic consequences. The near doubling of hacking incidents every two months in late 2002 will be shown to have shifted away from targeting government departments and agencies towards focusing principally on Small to Medium size Enterprises (SMEs) and large corporations where opportunity allows.

The SMEs are incapable of sheltering themselves or having the budget and expertise to be able to ward off sustained digital mass attacks, which have now become a daily occurrence with widely available, automated and easy-to-use sophisticated digital attack tools. The mounting collective losses to businesses might impact on governments' revenue streams through reduced tax collection, so in the future, it will be prudent to look after the SME growth engines and not just large businesses, who on the whole have the budgets and manpower resources to look after themselves.

National Interest

In the not too distant future, there is a likelihood that command and control attacks, which blend cyber terrorism with physical terrorism, simultaneously seek to disrupt transport or telecommunication hubs; financial services or commerce; water or energy distribution; could also be manifest as hackers organise themselves more rigorously along the lines of criminally financed terrorist syndicates with specific ideological agendas and become more adept at social engineering to procure insider help locally.

Historically, politicians in civilised Western democracies have challenged their defence forces to provide adequate defence capability within limited resources. The focus has been on the four physical dimensions – land, sea, air and outer space – and not on the new 5th Dimension, which is cyberspace. There is no real digital defence capability deployed so far - other than occasional simulations and exercises which are to uncover gaps in the national critical infrastructure's digital defences. The redressal lies primarily in developing counter-attack-forces, which would begin to arrest the imbalance of power between ill-motivated hackers on the one hand and little-prepared businesses on the other.

It is unrealistic to expect that any defence department can provide 'counter-attack-forces' against digital attacks for an entire nation's economic targets immediately and, in any case, the

expertise needed is relatively fast moving and cannot be 'trained' into would be combatants in a short period of time.

Human intelligence

Most complex attacks take place through insider knowledge and assistance. Just one motivated individual cannot usually perpetrate complex cross-boundary physical or digital terrorism. Disgruntled employees in sensitive places are suborned, coerced or indeed volunteer their services to support a cause. This is seen in financial services when complex fraud or deeply damaging hack attacks take place. It is also seen in large multi-nationals, in the breach of government services security and even in the planning of the 11th September co-ordinated attacks. More attention needs to be given to the value of human intelligence collected by local agencies, where the information is collected in situ at the grass roots level.

In the future, when seeking to protect the critical infrastructure constituents and business digital systems at a national level, the economically prudent way forward would be to combine knowledge management, analysis and counter-attack tools with on-the-ground human intelligence sources. Surveillance and reconnaissance dashboards of digital systems would need to be managed by experienced counter-attack-forces on a 24/7 basis.

Next Steps

mi2g believes that this war on digital terrorism can be won decisively and effectively. As in all wars, our collective national defences must excel enemy aggression. We will therefore need to understand that:

1. **Defence** has always been about securing trade routes and markets. Given that several Trillion Dollars of trade is routed digitally, counter-attack-forces with electronic weapons that can disable attacking systems from various parts of the world will ultimately need to be deployed with Governments' backing as part of their 5th dimension defence shield. Counter-attack-forces will save businesses a lot of lost time and money in dealing with rogue, politically motivated, electronic attacks from radical and criminal groups scattered across the world and within the nation.

2. **Laws** will have to be passed throughout the civilised world that will declare cyber attacks that spark fear and cause damage to life and assets as equivalent to physical-world terrorism at an international level. The perpetrators of such attacks will have to be dealt with as terrorists.

    a. This process has already begun with the US Senate and House of Representatives passing the *"Uniting and Strengthening America Act by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001"* in October last year and the *"Cyber Security Enhancement Act (CSEA) of 2001"* in July this year. The CSEA seeks life imprisonment for anyone putting lives at risk by electronic means. In the UK, under the Terrorism Act 2000, enacted into law in February 2001, people who endanger lives through the manipulation of public computer systems are to be considered under the anti-terrorism law as would any other terrorist.

b. All business operations could also be required, by law, to possess a sufficiently layered and tranched security architecture so that even if one layer or tranche of defence were to be breached the entire set of valuable databases or command and control capabilities would not be immediately compromised.

3. **Mobilisation of resources** including new investment will become necessary on interoperable distributed knowledge management and analysis systems, which allow data to be shared easily from and between different sources and agencies collecting intelligence. Also, investment in more local human intelligence across the globe will be essential. The expertise of the very few available people who are proficient in the technologies of the 5th dimension would need to be utilised to train the counter-attack-forces through the establishment of a national centre of excellence for digital defence. Nothing significant can be achieved without this cohesive sharing capability being made available to the future counter-attack-forces, who would be able to ensure reliability, availability, maintainability and scalability of SME business systems in the event of hacker attacks.

Conclusion

"After four successive record breaking months in the number of overt digital attacks this year, ***mi2g*** *believes that we have entered an era of sustained attacks from radicals, criminals and intellectual power zealots, who will be difficult to contain and to deal with at the consumer and small to medium size corporate level in the 21st Century. The roll out of 'always on' full broadband and wireless connectivity tilts the balance against the innocent citizens and corporations. In the years to come, government intervention to deal with 5th dimension warfare could become imperative. It is no longer a question of if but when,"* said DK Matai, Chairman and CEO, **mi2g**.

"*It is unlikely that governments will choose to remain oblivious to the challenge of daily digital attacks on their citizens and their livelihoods given the Billions of Dollars of damage being caused to digital commerce, productivity, intellectual property and employed capital. Organized crime syndicates embarking on identity theft, elaborate scams and financial fraud have now become rampant. As knowledge management based authentication systems proliferate both at airports and digital commerce sites, digital identity theft levers are going to be exercised by future criminals."*

[ENDS]

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

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 this 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

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 (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 107,000 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