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

news release - London, UK, 15 November 2002

Hacker attacks against Russia rising fast in November

London, UK, 13:30 GMT 15 November 2002 – Hacker attacks against Russia are rising fast in November making it the 10th most attacked country this month although it was not even in the top 20 previously. Russia has suffered 87 overt digital attacks in the first half of November already. In comparison, Russia suffers an average of 30 attacks per month typically.

Traditionally, Russia has been one of the most secure countries in dealing with the threat from digital risk because it has very strong digital defence and counter-attack capabilities amongst its native hacker community, military and government agencies.

The Islamic hacking groups originating in the Arab world, Pakistan and Indonesia, including: El-Batar, Medan hacking, USG, have all been active against Russian online systems since late October. In comparison, the larger surrounding former Soviet Republics, such as Ukraine, Kazakhstan, Uzbekistan and Belarus, have not shown a rising trend in digital attacks throughout 2002.

Russia has been the victim of Chechen rebels led terrorism in a Moscow theatre in late October.

The other top G-8 victims of digital attacks in November are the US (3,412), Canada (247), France (221), UK (193), Japan (180), Germany (128) and Italy (122).

The worldwide economic damage caused during November so far by overt and covert digital attacks including viruses is estimated at between $3.1 and $3.8 Billion.

[ENDS]

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

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: $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).

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

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.