Glossary – SIPS & EVEDA – v1.01

A Priori

A Predictor of Radical Insurgence; an early warning pilot launched by **mi2g** in early 2003 for estimating the risk of future militant activity based on patterns of politically motivated overt digital attacks.

Bespoke Security Architecture

mi2g tools provide a comprehensive and Bespoke Security Architecture™, which marries traditional security components, configuration management and automated intelligence techniques with a legal framework, human resource training and company policies. **mi2g** has an innovative approach to safety and security based on the pioneering Digital Risk Management methodology. See also *Digital Risk Management.*

Black hat

A "Black Hat" hacker is an individual that perpetrates cyber-crime for financial gain or intellectual challenge. See also *White Hat*.

Business Interruption

The stoppage of normal business processes often due to a virus outbreak or denial of service attack. See also *Economic Damage* and *EVEDA.*

Command and Control Attack

A form of digital attack, which could be covert or overt. Essentially an attack where 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. See also *Data Attack.*

Covert Digital Attack

A digital attack that cannot be directly validated. The SIPS database and EVEDA do not contain any comprehensive information on covert attacks, but estimates are made of the damage they are likely to have caused based on extrapolations made from specific sample data. See also *Overt Digital Attack.*

D2 Banking

D2 Banking ('digital and data banking') is the next generation of electronic banking and utilises **mi2g**'s bespoke security architecture to deliver combined digital and data banking services securely. See *eDFi.*

Data Attack

A premeditated violation of the confidentiality, integrity, authentication or non-repudiation of transactions based on the underlying databases. Such attacked databases may include confidential credit card numbers, identity information, customer and supplier profiles and transaction histories. See also *Command and Control Attack.*

Denial of Service Attack

Activity directed towards an online system or service with the objective of making it inaccessible to legitimate users. This is often perpetrated by generating a very large number of requests for the target website or sending a very large number of emails. See also *Distributed Denial of Service Attack.*

Digital Risk Management

Digital Risk Management resolves the complexity associated with implementing digital solutions and measuring their performance through Service Level Management. It includes selecting the optimum technology set, managing external partners and alliances, linking payments to targets, defining rigorous quality control procedures, managing system availability, achieving the expected return on investment, and bringing about changes in corporate culture required for successful business.

Distributed Denial of Service Attack

A denial of service attack that is carried out on a large scale by taking remotely control of a large number of computers (See *Zombie)* and then directing them to simultaneously carry out a denial of service attack on a single target. See also *Denial of Service Attack.*

Economic Damage

Value of damage done by digital attacks or malware due to resultant 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 market capitalisation decline. See also *EVEDA* and *Business Interruption.*

eDFi

The electronic Data Fort Initiative™ (eDFi) is a secure data vaulting service which allows users to access their critical personal and business information anywhere and at anytime via hand held devices, the internet and interactive digital television. See *D2 Banking.*

Equivalent Person Day (EPD)

The EVEDA economic damage estimates are based on the number of Equivalent Person Days (EPDs) that are lost following a disruptive incident such as an overt digital attack or malware attack. An EPD is defined as any day one person works for eight hours. **mi2g**'s Economic Valuation Engine for Damage Analysis (EVEDA) equalises each EPD at US $1,500.

EVEDA

EVEDA (Economic Valuation Engine for Damage Analysis) is a component of SIPS and estimates economic damage from hacking, viruses, worms and spam as loss of business, productivity, management time, cost of recovery, Intellectual Property Rights (IPR) violations, customer and supplier liabilities and share price decline where applicable. See also *Economic Damage.*

Hacker

Originally a term simply used to refer to computer enthusiasts the word “hacker” now refers to individuals who gain unauthorised access to computer systems for the purpose of stealing and corrupting data, ie who carry out overt and covert digital attacks. See also *Black Hat.*

Identity Theft

The illegitimate usage of information about an individual by a criminal to successfully impersonate them, either online, by mail, over the telephone, or in person. Hacking activity is increasingly carried out for the purpose of stealing identities and using them to commit credit card fraud. Although the gathering of the personal data may not be illegitimate, it often involves illegitimate access to online computer systems. See also *Phishing.*

Macro-Hacking Groups

Macro-hacking groups form when individual hacking groups coalesce and become interconnected through common agendas. The individual hacking groups from which a macro-group is constructed will carry out digital attacks under a common banner.

Malware

Malware is short for “Malicious Software” and is the collection of Viruses, Worms and Trojan Horses. See also *Virus*, *Worm* and *Trojan Horse.*

Overt Digital Attack

Overt Digital Attacks are incidents where a hacker group has gained unauthorized access to a computer network and has made modifications to any of its publicly visible components (such as a broadcast, service routine, payment / data collection or print out). See also *Data Attack* and *Command and Control Attack.*

Phishing

Phishing involves the distribution of fraudulent email messages that appear to come from banks, insurance agencies, retailers, branded goods manufacturers or credit card companies. These messages are designed to persuade the recipients to divulge personal authentication data such as account usernames and passwords, credit card numbers, social security numbers, etc. See also *Identity Theft.*

Politically Motivated Hacking

Any form of digital attack carried out for the purpose of furthering political goals. This can range from simply leaving propaganda messages behind on attacked online systems and websites to carrying out identity theft and credit card fraud in order to carry out terrorist attacks or otherwise fund the fulfilment of political objectives.

Publicly visible components

Many systems connected to the internet have some form of publicly visible components. This can be anything from a website in the case of an online web server to a TV or phone signal in the case of a satellite. See also *Overt Digital Attacks.*

Scans / Attempts

Any computer system connected to the internet can expect to log some form of digital “attack attempt” roughly once every 30 seconds. Most of these are just automated scanning tools looking for system vulnerabilities or random attempts to exploit old vulnerabilities. Having a properly configured firewall in place will render most of these attempts unsuccessful. See also *Overt Digital Attacks* and *Covert Digital Attacks.*

SIPS

SIPS stands for “Security Intelligence Products and Systems”. It is a proprietary database containing details of overt and covert digital attacks, viruses, worms, Trojan horses, spam, phishing and denial of service attacks. See also *EVEDA.*

Spam

Unsolicited commercial email sent in bulk, often anonymously, to promote various products and services. Spam is responsible for causing substantial economic damage through business interruptions as bandwidth is consumed by semi-automated systems and time is wasted by employees deleting unwanted spam email messages.

In recent years, spam has also become more closely associated with other forms of cyber crime as spammers resort to increasingly criminal methods – attacking customer information databases to find email addresses as well as launching viruses and Trojan horses that target anti-spam websites in spam denominated distributed denial of service attacks. See also *Spam Relays.*

Spam Relays

Once spammers have masked their messages through open proxies, they have to use other programs to find "open relays," the messages' intermittent stops before reaching a recipient.

Relay servers exist on all e-mail systems, and they route messages to the proper address within a company. But some insecure relays are left "open," enabling anyone from the outside to send messages through them to any other outside address. Companies soon shut down open relays, but so many exist that the software rotates them quickly. Users of personal computers at home are often unknowingly victimized as their computer broadband connections often leave open relays through which spam is sent. See also *Spam.*

Trojan Horse

Seemingly innocuous software containing additional hidden code carrying out unauthorized activity on the victim computer. A Trojan horse will often be some form of key-logging software enabling the hacker that planted it to gain access to passwords.

Distributed denial of services attacks use Trojan horse software to carry out ordinary denial of service attacks on thousands of innocent computers and then activating them to launch a larger attack simultaneously. See also *Distributed Denial of Service Attacks.*

Virus

Viruses are malicious software, often spreading by email and often causing damage to (remote) computer systems. They can also reproduce by modifying other programs to include a copy of themselves. See also *Worms.*

White hat

A White hat hacker is an individual working to counter the activities of Black Hat hackers. They often have identical capabilities as Black hat hackers but work as computer security professionals. See also *Black Hat.*

Worm

A worm is a special type of virus that can replicate itself, proliferate through networks and use memory, but cannot attach itself to other programs. See also *Virus.*

Zombie

A computer system commandeered by a hacker to participate in a distributed denial of service attack. See also *Trojan horse* and *Distributed Denial of Service.*