Frequently Asked Questions – SIPS & EVEDA – v1.00

What do SIPS and EVEDA stand for?

SIPS stands for Security Intelligence Products and Systems. EVEDA stands for Economic Valuation Engine for Damage Analysis and is a component of SIPS.

What is the purpose of SIPS and EVEDA?

SIPS and EVEDA are employed by the **mi2g** Intelligence Unit to produce statistics and estimates of digital damage worldwide for use by our clients and in our Intelligence Briefings and News Alerts. **mi2g**'s Intelligence Briefings and News Alerts are distributed to a variety of government agencies, banks, insurance and reinsurance companies and professional services groups for keeping track of digital, legal, insurance, reinsurance, political, operational and systemic risks.

From where does the data in the SIPS and EVEDA originate?

mi2g is principally reliant on data for SIPS and EVEDA from a number of sources:

1. Personal relationships at CEO, CFO, CIO, CISO level within the banking, insurance and reinsurance industry in Europe, North America and Asia. We have been involved in pioneering cyber liability insurance cover for Lloyd's of London syndicates which has given us access to case histories since the mid 1990s.

2. Monitoring hacker bulletin boards and hacker activity. We have several white hat hackers who we use for penetration testing and developing our Bespoke Security Architecture that feed digital risk information through to us on a continuous basis including vulnerabilities, exploits and the latest serious attacks they are aware of.

3. We maintain anonymous communication channels with a large number of black hat hacker groups.

Cases of systems attacked are systematically screened by Intelligence Unit personnel to ascertain hacker motivation and country of origin. Domain specific knowledge such as hacker contact details and the relationships between hacker groups are extracted automatically.

EVEDA collects its information from a variety of open sources and calculates the economic damage associated with a particular digital attack based on a unique set of algorithms developed by the **mi2g** SIPS team in conjunction with risk analysts and economists.

What is an "overt digital attack"?

Successful hacker attacks on digital systems, such as computers and digitally controlled machines, can be either covert or overt – as opposed to scans or attempts.

Covert attacks are not validated 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 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) 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 identity theft, political tension, protest and digital warfare; criminal syndicate activity; extortion; 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.

An emerging motive is related to sending spam. While harvesting email addresses from newsgroups and web pages is a well-known method, many members of the spamming and hacking communities have begun to use more sophisticated methods such as hacking into customer databases used by companies selling products online and converting compromised computers into open spam relays that can send out hundreds of thousands of emails per minute.

What are the motives for malware – virus and worm – writers?

The ready availability of malware-writing toolkits on the Internet and the ease with which viruses and worms can be released anonymously means that any mal-intentioned person who wants to release another more vicious version can do so without having to rely on any specialist technical knowledge.

Email-based viruses and worms can also be written for the purpose of surveillance and reconnaissance including identity theft and sending spam.

A fairly low labour-intensive method for garnering working email addresses is one of releasing an email virus that implants or downloads a "Send Mail" Trojan that either copies and sends all email addresses found on infected computers to machines controlled by the virus author or creates a huge traffic of email bombardment to check which email addresses are still valid whilst spoofing the origin.

Malware-writers may also seek to maintain control over infected computers for use as anonymous denial of service or spam-relays, or as servers of illegal material such as stolen credit-card numbers, pirated image, audio and video libraries as well as child pornography. The financial gain involved is increasingly becoming a motive for transnational cybercrime-gangs.

What are SIPS and EVEDA?

SIPS is an engine that collects and reports on overt hacking activity around the globe. The **mi2g** SIPS database has information on over 8,500 hacker groups and maintains a record of over 380,000 individual hacking events (as per March 2004) going back to 1995. It also contains extensive incident data on companies, government agencies and Non-Government Organizations (NGOs) worldwide so that an attack on individual online systems can be linked to a specific organisation. The SIPS Database also has records of viruses and vulnerabilities that are updated automatically, on a daily basis, as new incidents, infections and alerts become known.

EVEDA is a component of SIPS and estimates economic damage from hacking, phishing, viruses, worms and spam as helpdesk support costs, overtime payments, contingency outsourcing, loss of business, bandwidth clogging, productivity erosion, management time reallocation, cost of recovery, software upgrades, Intellectual Property Rights (IPR) violations, customer and supplier liabilities and share price decline where applicable.

Over the last seven years, the worldwide economic damage estimate for all forms of digital attack including hacking, malware and spam has been estimated via EVEDA at between: $186 and $228 billion (2004 so far); $225 and $275 billion (2003); $107 and $130 billion (2002); $33 and $40 billion (2001); $25 and $30 billion (2000); $19 and $23 billion (1999); $3.8 and $4.7 billion (1998); $1.7 and $2.0 billion (1997); $800 and $980 Million (1996).

What kind of economic impact do "overt digital attacks" have?

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. This is what EVEDA estimates.

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. **mi2g** continues to develop algorithms and rehearsals to be able to measure the economic damage from these type of attacks.

Why are economic damage estimates expressed in US Dollars?

mi2g's economic damage estimates are expressed in US Dollars because the US dollar is a universally traded currency and serves as a reserve for most governments and central banks across the globe. Estimates offered in US dollars can therefore be more readily and intuitively understood by the vast majority of people in comparison to estimates made in British Pounds Sterling or other local currencies.

What is an Equivalent Person Day (EPD)?

The EVEDA economic damage estimates are based on the number of Equivalent Person Days 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.

How is the SIPS and EVEDA information verified?

The sources used for gathering the SIPS data store mirrors of the systems attacked. They are retrieved automatically using various tools, such as GNU Wget, as soon as an attack is reported, either by the perpetrator, the victim or another reliable source.

EVEDA is checked to a +/- 10% accuracy. General economic damage information is verified by sampling specific cases and extrapolating the damage done to a range of similar domains and computer environments. We continue to cross check the EVEDA estimates against other studies by leading international authorities.

What about statistics on unreported or covert attacks?

The SIPS database and EVEDA do not contain any specific information on attacks that are covert, not reported, validated or witnessed by any reliable source. We do, however, often receive notification on individual security breaches from our partners and clients across the globe, which are included.

Where has data from SIPS been quoted?

Citations of aggregate data from SIPS include the annual eCommerce and Development Report 2003 published by the United Nations Conference on Trade and Development (UNCTAD), the 2002 CSI/FBI Computer Crime and Security Survey, CNN, BBC World Service, Financial Times, Washington Post, New York Times, Time, Newsweek and Fortune Magazines.

mi2g Intelligence Briefings, as well as a selection of articles from various online news sources, are available on www.mi2g.net under the "Latest News" section.

What about other forms of digital attack?

SIPS and EVEDA contain only partial information on the activities of all viruses, worms or all Distributed Denial of Service (DDoS) attacks as these can be difficult to track, quantify and validate meaningfully. Sometimes a perceived DDoS attack may be down to load balancing or inappropriate bandwidth allocation because of too many users. The SIPS database does contain detail on individual viruses and vulnerabilities by name, date, type and risk level and some validated Denial of Service attacks.

Economic damage for malware and spam is calculated on the basis of sampled productivity loss data combined with estimates of the number of machines infected. We prefer to limit our model for such damage to productivity loss even though actual losses could be higher due to data deletion and modification, Trojans, brand loss and other factors, since some malware does not directly cause damage in this way.

Which Operating Systems are most vulnerable to digital attacks?

Based on the information garnered through SIPS in March 2004 for twelve trailing months, Linux is the most breached operating system followed by Microsoft Windows.

For the twelve trailing months as of March 2004, 68.0% of all overt digital attacks were on systems running Linux and 17.2% were on systems running Windows.

A known difficulty with administering a Windows based system is the effort that has to be expended in 24/7 configuration management, reboot-patch-reboot, in comparison to that required for open source solutions such as Linux and OpenBSD, which may be patched without the reboot drill most of the time. This is particularly valuable where computers are in need of having zero downtime. On the other hand, poorly configured or updated third party applications and server running on a Linux system are often a bigger threat to online server security than up-to-date Microsoft applications and server running on a Microsoft Windows platform.

Many hacker groups, in anonymous interviews with **mi2g**, have said that they prefer attacking Linux systems because they will find more configuration errors within those systems and that makes mounting the attack simpler. Hacker groups with political motivation target country or content specific online systems regardless of operating systems. Those hacking for intellectual gain or fun will generally be attracted to the perceived greater challenge associated with hacking well-configured BSD, Linux, Solaris and Unix systems or the online systems of high-profile organisations.

Although the relative market share of different operating systems ought to be reflected in the proportion of digital attack suffered by each of them, the precise proportions do fluctuate considerably - generally in a way that is coupled with the preferences of the hackers and the announced vulnerabilities that have still not been patched.

There are several motivations and issues involved behind targeting Windows over Linux or vice-versa, ranging from the reasons for an attack down to number of vulnerabilities being announced for Operating Systems, Servers, Applications and Libraries at a given moment in time and the ease with which the patches can be applied across a large scale deployment.

Do multiple website attacks resulting from a single system breach count as one attack or many?

Mass website attacks are counted as multiple attacks because although there is a single action on the part of the attacker, economic damage is always done to multiple victims.

When insurance cover for cyber liability was pioneered it was originally conceived around single IP addresses. Later on, technology allowed multiple domain hosting to be achieved with the same IP address, to the point that "1000's" of sites can all now be located on the same IP.

An insurance company has to pay those "1000" companies when a denial of service, business interruption, customer or supplier liability insurance claim is invoked as a direct result of vandalism or other criminal activities.

These days insurance policies are structured around profit centres and domains rather than just on IP addresses. Each attack incident, if verified, is classed as a unique attack regardless of whether it

occurred repeatedly, ie, once every two days or once every month and regardless of whether it was part of a mass attack or not.

The liabilities for each of the “1000” attacks will tend to spread across the customers and suppliers of each profit centre entity. So, it is inconceivable that it can be treated as one single attack from an insurance customer perspective.