Internet Industry Association

Jane Hearn
Inquiry Secretary
Standing Committee on Communications
House of Representatives
Suite R1-109, Parliament House, Canberra A.C.T. 2600
Tel: + 61 2 6277 2300; Fax: + 61 2 6277 4827
Via Email: jane.hearn.reps@aph.gov.au
Web site: http://www.aph.gov.au/house/committee/coms/index.htm

Submission to Standing Committee on Communications: Inquiry into Cyber Crime

As discussed last month, the Internet Industry Association welcomes your Committee's Inquiry into Cyber Crime and we are please to enclose our submission on this matter.

Peter Coroneos
Chief Executive
Internet Industry Association

Internet Industry Association

Since 1995 the Internet Industry Association has been Australia's national Internet industry organisation. Our members include telecommunications carriers, content creators and publishers, web developers, e-commerce traders and solutions providers, hardware vendors, systems integrators, banks, insurance underwriters, technology law firms, ISPs, educational institutions, research analysts, and professional and technical support services.

Increasingly, our members also include businesses hoping to establish an effective online presence for the purposes of e-commerce.

On behalf of its members, the IIA provides policy input to government and advocacy on a range of business and regulatory issues, to promote laws and initiatives which enhance access, equity, reliability and growth of the medium within Australia.

Cybercrime Act 2001

The IIA was pleased to make a submission on the then Cybercrime Bill in 2000.

The Cybercrime Act 2001 made a range of amendments to the Criminal Code Act 1995 to update the computer offences, based on the joint Commonwealth, State and Territory Model Criminal Code Damage and Computer Offences Report (January 2001), along with other changes to authorise certain intelligence activities.

The intention behind the legislation was to criminalise activities such as computer hacking, denial of service attacks, spreading computer viruses and interfering with websites.

The legislation covered the issues well. However our main concerns then were to ensure offences to be committed in the course of every day investigations carried out to determine the level of security or otherwise of a client's system did not get caught by the legislation.

We believe this was largely satisfied and that the Act formed a potentially important aspect of deterring criminal abuse of the Net.

Since then the nature of internet environment has developed beyond crude computer hacking and one-off mischief connected with computer viruses and fraud. This has highlighted more general weaknesses in the regime, the Association would like to comment on.

The new Net security environment

a) nature and prevalence of e-security risks including financial fraud and theft of personal information, including the impact of malicious software as viruses and trojans;

In the past most network attacks targeted large corporate, government and community networks. Attacking domestic premises via telecommunications carriers was less likely because dial-up access was the main means of communications.

Penetration of broadband access was minimal with the ABS less than 20% in 04/05[1]. However by 07/08 it was about 50% and continues to climb. Furthermore the internet access was distributed throughout various households by cable and wireless linkages.

Unlike dial-ups, broadband access distributed through a home could offer several different services at the same time. Furthermore it was typical to leave these broadband connections on all the time as the costs were capped at a monthly rate.

This meant that poorly secured home devices formed easy prey to deceptive downloads that could continue independent of the user and be programmed like a remote drone.

This offered an important distribution point for distributing unauthorised email such as spam and in turn circulating other unpalatable software such as spyware.

In the past few years, these drone systems have been organized in massive botnets or zombie bots that can be managed and leased internationally to perpetrate an increasing variety of cybercrimes.

A zombie botnet is a group of PCs infected with malicious software. These are called “zombies” or bots because they can be used remotely to carry out attacks against other computer systems. Zombies are compromised computers. Botnets are herds of Zombies.

They are often created by exploiting vulnerabilities in your PC and inserting malicious software or "malware" usually without the user knowing. Often it is hidden as part of some software or website that the user was interested in. It may occur also with unsecured wireless home networks.

Malware is used to create botnets, and botnets are used to further distribute spam and malware.

In association with National Consumer Fraud Week, the Internet Industry Association launched its first awareness campaign on the spectre of zombies[2]

At the heart of the issue is that malware infected systems are increasing. the vast number of 'zombies' continues to be largely responsible for the avalanche of spam suffered by users and companies.

Furthermore the threat is now compounded through infected – otherwise legitimate webs sites.

[1] 8146.0 - Household Use of Information Technology, Australia, 2007-08
http://www.abs.gov.au/ausstats/abs@.nsf/mf/8146.0

[2] http://www.iia.net.au/index.php/zombieweek.html

At a recently convened workshop on the issue on 10 June, IIA security expert, Paul Ducklin, of Sophos Australia estimated the number of newly affected URLs - 120,000 a month or about 4000/day.

In Australia, Ducklin puts the figure at 750 URLs a month. Ducklin estimates there are 20 million zombies in the world, with approximatedy 100,000 zombies in Australia. The average zombie device is capable of dispatching 10,000 spams a day.

Cyber-crooks send instructions to these computers, including commands to download malware onto the system, display advertising to the user, launch denial of service attacks, and above all, distribute spam.

In short, most cybercrime today is tougher to fix because:

- It is perpetrated by exploiting poorly secured devices to become botnets
- It is well funded and there are now organized layers that operate botnets
- Understanding of its scope and stealth is poorly understood
- Enforcement and judicial institutions do not appreciate that it is growing more pervasive
- It is a global phenomenon and perpetrators are hard to bring to the courts through international jurisdiction issues.

While there has been some success in arresting the growth of the botnets, it's clear that more needs to be done than mere preventive education.

b) The implications of these risks on the wider economy:
*** Including the growing economic and security impact of botnets.**

The IIA regards the spectre of increasing botnets as a leading cause in consumer frauds. Effectively trust, privacy and consumer confidence in the online economy will be undermined.

c) Level of understanding and awareness of e-security risks within the Australian community.

From the experience of our security and ISP members, the level of understanding and awareness is still very poor. The reasons for this are partly cultural, partly intergenerational and because technological risks tend to be under-estimated by many in the community, law enforcement and legislature.

This is exacerbated by the increasing sophistication of international perpetrators that fund and exploit security break-downs and mischief.

Currently most network routers are run within their default mode with generic log-ins and passwords. A substantial minority are not even secured for local access via "war driving" exploits from local interlopers.

Even if a breach of the Cybercrime Act occurs (say via theft of data or internet access) it is unclear how such breaches will ever come to light and the evidentiary issues that would need to be established.

The relative lack of prosecutions and statistics on the Cybercrime Act also undermines community awareness of the scope of the issues.

A compelling recent illustration was noted in some web commentaries on a remarkably light outcome of a clear breach of the Act.

Twenty two year old Brendan Roy Taylor was reportedly convicted of stealing 60,000 credit card users details (via phishing techniques) to sell online. An undercover policemen posed as a buyer and Taylor was arrested and charged.

One estimate suggests Brendan Taylor may have sent out a staggering 428,571 emails.

The magistrate convicted and sentenced Taylor, punishing him with a $150 fine and 12 month good behaviour bond.

Amazingly there appears to have been no mainstream media coverage of this story and the only source reportedly was a scan of a newspaper article from a WA paper.[3]

The industry is concerned that the apparently light sentence handed down in this case will undermine the deterrent effect of the legislated sanctions.

This certainly seems a case for more sentencing guidelines as we are concerned that lower courts may lack the technological expertise to appreciate the high tech offences on which they adjudicate.

d) Measures currently deployed to mitigate e-security risks faced by Australian consumers:

In general the challenge is not with the Cybercrime Act itself. The broader issue is that the entire system of cybercrime is too complex to handle by current institutions.

There have been worthy developments such as the Australian High Tech Crime Centre (AHTCC) launched in 2003.[4] However Government resourcing of cybercrime activities is a continuing weakness.

Qualified IT/cybercrime investigators require considerable forensic, technical and state of the art training to understand the dynamic programming and scripting developments that are around.

[3] http://ozsoapbox.com/rest-of-australia/cybercrime-penalties-in-australia-are-a-joke/

[4] http://www.ahtcc.gov.au/about_us/

The risk is that Federal bureaux such as AHTCC may recruit and develop their staff, only to see them attracted to private agencies at twice or three times their salaries.

The Federal Government must anticipate and respond to the fact that well qualified investigators and their units are thin on the ground and require far more resourcing than has been the case to date.

Yet, the IIA remains puzzled by the parsimonious budget outcome from E-Security Review 2008. A trifling $8.8 million was dedicated on e-security, to bring together Australia's existing computer emergency response arrangements under a new national Computer Emergency Response Team (CERT) and $2 million *over two years* for the national security public information campaign.[5]

When compared with the $43 billion NBN initiative that will open many more opportunities for cybercriminal organisations to compromise our systems, we support the e-security strategy but doubt whether it has been properly resourced to fulfil its mission.

To date the Internet Industry Association, through its own members' resources, has undertaken various e-security initiatives out of own interests.

In addition the IIA is pushing for a percentage of the NBN build budget to be allocated to building security into the infrastructure – as opposed to current efforts that are limited to retrofitting security measures into an inherently insecure medium. An *inherently secure* NBN will be a major step forward in overcoming current vulnerabilities.

Educational initiatives

The IIA would like to see more targeted funding at educational initiatives with clear behavioural benchmarks, so that the nature of our collective appreciation of cybercrime is appropriately managed, monitored and resourced.

The IIA has sponsored various campaigns on shoe-string budgets and the voluntary contributions of members. We'd welcome a re-appraisal of the wisdom of allowing this as an e-security strategy in the future.

* **Legislative and regulatory initiatives**

The IIA would welcome improved training of judicial and enforcement officers of the evolving spectre of cybercrime – and how it is beginning to become mainstream and yet below the radar of many State and Federal enforcement units.

* **Cross-portfolio and inter-jurisdictional coordination; International co-operation.**

[5] http://www.attorneygeneral.gov.au/www/ministers/robertmc.nsf/Page/MediaReleases_2009_SecondQuarter_StrengtheningourNationalSecurity

There is scope for improved consistency between States, Territories and International jurisdictions of cybercrime trends. A useful model has been the welcome broad international and cross border pursuit of cyberporn and pedophiles, for example.

As well we attach a recent case study from one of our member organisations that suggest the enforcement of cybercrime may have more general systemic issues.

The member has sought only that we withhold the name of his company and the local police station on this occasion. (See Attachment 1)

e) Future initiatives that will further mitigate the e-security risks to Australian internet users.

The IIA has moved to establish voluntary protocols to enable isps to alert their account users of potential cybercrime activity that their systems may be reflecting.

Our industry security member, McAfee's has estimated Australia per capita has risen to become the third most infected users[6]. The report noted, that China and the United States have been jostling for the top spot over the past three quarters and dominate in the number of zombie machines under the control of spammers. However Australia, which failed to make the top 10 in the third quarter of 2008 has rocketed up to the number three spot, accounting for six percent of all new zombies.

It predicts that the "Land Down Under" is proving to be fertile ground for zombie recruiting after China and India

These trends were noted back in 2005, when ACMA initiated a pilot Australian Internet Security Initiative[7] (AISI) drawing on the cooperation of six isps to alert them of zombie-like behaviour that be identified with one of their account holders.

The data sharing led to a more effective reduction in malware infected systems and the 2007 Budget allocated approximately $4.7 million (over four years) to enable the expansion of the AISI to all Australian ISPs who wish to participate.

So far some 62 isps are involved. However every time an ISP notifies one of their subscribers about the matter, it's like suggesting they have digital bad breath - and can they please attend to their infected device.

The total AISI program is responsible for 10,000 compromises reported every day.

[6] http://img.en25.com/Web/McAfee/5395rpt_avert_quarterly-threat_0409_v3.pdf

[7] http://www.acma.gov.au/WEB/STANDARD..PC/pc=PC_310317

Given the nature and frequency of the incidents some ISPs are more diplomatic than others. The larger ones have tried to automate it with a bland email suggesting not all is well with their system and they risk losing their net access until their system is less of a risk to the network.

Most affected users appreciate receiving this information. However there are privacy, consumer and technical issues along with education and equity to be dispensed.

On 10 June, the IIA in association with the Government, ISPs, security vendors and community representatives convened a meeting to explore the merits of a new voluntary esecurity code so that there will be a fair and sensible approach embraced with the aim of reducing malware infected systems.

It was agreed to develop a Draft Code Principles with representative from all stakeholders with the view to issuing the first draft by the end of July for broad consultation and review. A final version of the voluntary code should be available by 1 December 2009.

The Code should define the problem – what is a compromised computer and how do you know when you have one.

Likewise the IIA has convened meetings with network distributors to increase the security levels of the default configurations of their systems.

The IIA would welcome Government support to develop industry-branded schemes to promote improved security.

Attachment – Case Study of Enforcement of Cybercrime incident

[From email received August 06, 2009 10:42 AM]

Subject: Information about server attack - confidential

We have found that our main server cluster has attacked from the 23rd – 28th July and the attacker introduced some code which was to view orders that were being placed in real time and looking for address and credit card data. It was a very sophisticated method used in that the attacker gained access to our system and then created a temporary file that information was added to as it was found. Each day they then attempted to retrieve the information and delete the temporary file.

To some degree it was successful but due to some coding errors by the hacker this caused the websites to slow down and sometimes stop. So it was picked up and also interrupted the order process. They appear to have captured with 26 credit card numbers but we do not know if they successfully retrieved the file. If their code had worked as it was supposed to they could have many time more.

The attack came from a German IP address.

I contacted the Federal Police and was basically told it was a state matter, this is also the information on their website.

I contacted NSW Police headquarters and was put on to an analyst in their Internet Fraud area. He told me he could not do anything directly but that it had to be referred from a local police station.

I visited the local police and lodged an incident. They were somewhat confused as to how to handle the problem. The desk constable took a written report and tried to be very helpful. He did do his best and has since contacted me to follow up. We are trying to get them a list of credit cards and the IP address.

I guess I expected some better response at the national or state headquarters level. The local station struggle to handle this and I was also surprised that there was not some obvious escalation procedure.

I would be happy to discuss further.