The Parliament of the Commonwealth of Australia

Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime

The Report of the Inquiry into Cyber Crime

House of Representatives
Standing Committee on Communications

June 2010
Canberra

ISBN 978-0-642-79313-3 (Printed version)

ISBN 978-0-642-79314-0 (HTML version)

Contents

LIST OF TABLES

LIST OF FIGURES

Foreword

In the past decade, cyber crime has grown from the nuisance of the cyber smart hacker into an organised transnational crime committed for vast profit and often with devastating consequences for its victims. A sophisticated underground economy provides the IT tools to commit these crimes and the market for stolen identities and financial information.

In the technological world of cyber crime it can be easy to forget the human cost of the theft and deception inflicted on innocent people. We are reminded of the human cost by our constituents who face the emotional devastation and lasting financial consequences of the crimes perpetrated against them.

There has been an exponential growth in the volume of malicious software and the sophistication and adaptability of cyber crime techniques. In the face of these trends, the Committee believes the expectation that end users should or can bear the sole responsibility for their own personal online security is no longer a tenable proposition. We need to apply the same energy and commitment given to national security and the protection of critical infrastructure to the cyber crime threats that impact on society more generally.

A key message throughout this inquiry was that a more integrated, coordinated and concerted effort is required to combat the cyber crime that victimises ordinary consumers and private businesses. This requires a commitment to cooperation, strategic thinking and a cyber space perspective to overcome the silos of traditional institutions.

The Committee does not accept that the Internet is a kind of unpoliced 'wild west' − the Internet is a global communication medium that is subject to the same laws as the offline environment. It is true that technology enables criminals to obscure their identity and victimise people in different countries. It is equally true that technology allows us to trace perpetrators, to preserve, aggregate and analyse digital evidence, and to coordinate global enforcement action.

Through a nationally led and coordinated policy, as well as regulatory and law enforcement effort, Australia can deliver a more effective and strategic response to this problem. By necessity this has to be a joint public-private effort because the architecture of the Internet and the IT technology is in private hands. While the capacity to negotiate and create international agreements between nations is in the hands of the State.

The private sector, especially IT manufacturers, Internet Service Providers and web hosting companies, and the Domain Name Registrars and Resellers, all bear some corporate social responsibility to promote the integrity of the Internet. There is also a vast quantity of intelligence data that can be better shared between the public and private sector.

To this end the Committee has recommended that the interests and needs of consumers and business generally be elevated in the national *Cyber Security Strategy*. Some of the concrete steps that can be taken immediately include:

- a national coordination point to oversee this broader strategy;
- a national cyber crime reporting centre;
- better coordination and training for law enforcement agencies;
- public-private information sharing on a wider range of cyber crime types.

These new institutional arrangements should be supported by a stronger commitment to detect botnets, remediate infected computers and deal with compromised and fraudulent websites. This will require additional funding to support the Australian Communications and Media Authority.

The current strategy puts an emphasis on education and community awareness but seems to lack the coherence or clear benchmarks for success that might be expected for such an important priority. A clearly articulated national community education e-security strategy, including broader public campaigns, will help to promote more e-security awareness among the general public.

The private sector must also play its part. The Internet industry has to accept that commercial gains also carry social responsibilities. IT manufacturers also need to give a higher priority to security through better product testing, design and the provision of information to support informed consumer choices.

The reality of modern life is that information and communications technologies are a part of our everyday existence – the complexity and global reach of the Internet age can seem overwhelming but we should not lessen our commitment to protecting personal privacy or ensuring that informed consent and choice remain the central principles when transacting online.

Online businesses and public agencies must observe Australia's prohibitions against the over collection of personal information. The public also has a right to know if their personal information has been compromised because of a security breach.

On behalf of the Committee, I wish to thank the agencies, IT companies, peak bodies and the consumer groups who gave us substantial and well considered evidence. We also thank the State Governments who recognise this is an important national and international issue and are seeking ways to cooperate across jurisdictions to deal with this problem.

Finally, I also wish to thank my Committee colleagues who participated in this inquiry with enthusiasm for a difficult subject and with a commitment to bipartisanship. Members regularly hear the stories of their constituents seeking advice on where to take their complaints or how to protect themselves in the future. This first-hand experience and the cases we heard about during the inquiry served to remind us of the importance of tackling this insidious problem.

Ms Belinda Neal MP

Chair

Membership of the Committee

Chair	Ms Belinda Neal MP
Deputy Chair	The Hon Mark Vaile MP (until 26/8/08)
	Mrs Kay Hull MP (from 26/8/08)
Members	The Hon Bruce Billson MP (until 3/2/10)
	Mr David Bradbury MP
	Ms Julie Collins MP
	Mr Steve Georganas MP
	Mr Steve Irons MP (until 4/6/09)
	Ms Nola Marino MP (from 4/6/09)
	The Hon Peter Lindsay MP
	Ms Kerry Rea MP
	Ms Amanda Rishworth MP
	The Hon Tony Smith MP (from 3/2/10)

Committee Secretariat

Secretary	Jerome Brown
Inquiry Secretary	Jane Hearn
Research Officers	Dr Narelle McGlusky (until 4/11/09)
	Geoff Wells (from 12/11/09)
Administrative Officers	Heidi Luschtinetz
	Dorota Cooley

Terms of reference

The House of Representatives Standing Committee on Communications shall inquire into and report on the incidence of cybercrime on consumers:

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

b) the implications of these risks on the wider economy, including the growing economic and security impact of botnets;

c) level of understanding and awareness of e-security risks within the Australian community;

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

   i) education initiatives

   ii) legislative and regulatory initiatives

   iii) cross-portfolio and inter-jurisdictional coordination

   iv) international co-operation;

e) future initiatives that will further mitigate the e-security risks to Australian internet users; and

f) emerging technologies to combat these risks.

Glossary and abbreviations

.auDA	.au Domain Administration
419 scam	See ‘Advance-fee fraud’
ABA	Australian Banking Association
ABS	Australian Bureau of Statistics
ACC	Australian Crime Commission
ACCAN	Australian Communications Consumers Action Network
ACCC	Australian Competition and Consumer Commission
ACFT	Australian Consumer Fraud Task Force
ACMA	Australian Communications and Media Authority
Advance-fee fraud	A scam where the victim hands over money in the hope of realising a significantly larger gain
Adware	A type of software which directs advertisements at users and in some cases gathers personal information
AFP	Australian Federal Police
AGD	Attorney General’s Department
AHTCC	Australian High Tech Crime Centre
AIC	Australian Institute of Criminology
AIIA	Australian Information Industry Association
AISI	Australia Internet Security Initiative

ALRC	Australian Law Reform Commission
Anti-virus software	Software to prevent, detect and remove malware
APCA	Australian Payments Clearing Association
APWG	Anti-Phishing Working Group
ASCCA	Australian Seniors Computer Clubs Associations
ASIC	Australian Securities and Investment Commission
ASIO	Australian Security Intelligence Organisation
ATO	Australian Taxation Office
AusCERT	Australian Computer Emergency Response Team
Backdoor	A hidden access point which permits a computer to be remotely accessed by another computer
Blacklist	A list or register of persons or computers who are denied access to a network or computer system
Bot	A malware-infected computer that can be remotely controlled over a network
Botherder	See 'botmaster'
Botmaster	The controller of a botnet
Botnet	A network of bot computers that can be simultaneously controlled from a central point
ccTLD	Country Code Top Level Domain, a domain name denoting where a website is registered (such as '.au')
CERT Australia	Computer Emergency Response Team Australia
Cloud computing	Computing where users can access programs, processes and information on-demand over the Internet, without such resources being installed on their own computer
CLPC	Cyber Space Law and Policy Centre
CNP Fraud	Card Not Present Fraud, online credit card fraud committed with stolen information only without the need for the physical credit card
Computer offences	Criminal acts of a technical nature such as hacking, DDoS attacks and malware intrusions

CTN	Consumer Telecommunications Network
Cyber attack	An attempt to undermine or compromise a computer system or the user of such a system
Cyber crime	A range of crime types including computer offences, online banking and credit card fraud, and online scams
Data breach	The unauthorised disclosure, release or loss of secure information to an insecure environment
DBCDE	Department of Broadband, Communications and the Digital Economy
DDoS	Distributed Denial of Service, a method by which botnets flood a computer system with information thus damaging or shutting down the system
DNS	Domain Name System, the system that translates user-friendly web addresses into IP addresses
DNS hijacking	The act of subverting a computer to contact a fake DNS server instead of a legitimate DNS server
DNS spoofing	The act of replacing a genuine IP address in the DNS with a fake IP address
DNSSEC	Domain Name System Security Extensions
Domain	See 'Domain names'
Domain hijacking	The act of taking control of a domain name by stealing the identity of a domain name owner
Domain Owner	The registrant of a particular domain name
Domain Registrar	An accredited organisation that manages the registration of particular domain names
Domain Reseller	An organisation that on-sells the rights to use particular domain names
Domain names	A hierarchical series of codes that combine to form unique web addresses (See 'gTLD' and 'ccTLD')
DSD	Defence Signals Directorate
E-security	The protection of computer systems from technical threats

ESPaC	E-Security Policy and Coordination Committee
FBI	US Federal Bureau of Investigation
FCCG	Queensland Police Fraud and Corporate Crime Group
Firewall	A part of a computer system or network that blocks unauthorised access
gTLD	Generic Top Level Domain, a domain name generally denoting the nature of a website's owner (such as '.gov')
Hacker	A person who illegally accesses, controls or damages other computer systems
Honeypot	A dummy computer, program or email account set up to attract and deflect cyber attacks on a system
HTCOC	High Tech Crime Operations Centre
HTTP	Hypertext Transfer Protocol, a protocol that enables computers to exchange data with web page hosts
ICANN	Internet Corporation for Assigned Names and Number
ICPEN	International Consumer Protection and Enforcement Network
ICT	Information and communications technology
Identity crime	The theft or misuse of another person's identity
Identity fraud	The illegal assumption of another person's identity for purposes of fraud
Identity theft	The theft of personal information
IIA	Internet Industry Association
IP Address	Internet Protocol Address, a number that identifies a device on a network
ISP	Internet Service Provider, a company that provides access to the Internet
IT	Information technology
ITU	International Telecommunication Union
JBFSIT	Joint Banking and Finance Sector Investigations Team
Keystroke logger	A hidden program which illegally records each key that

	is pressed on a computer's keyboard
LEA	Law enforcement agency
Malware	A generic term for software designed to damage or subvert a system
Money mule	A person who launders money via internet banking and wire transfers to online criminals
NBN	National Broadband Network
Nigerian scams	See 'Advance-fee fraud'
NSW	New South Wales
NT	Northern Territory
OECD	Organisation for Economic Co-operation and Development
Banking fraud	Fraud committed to illegally remove money from another person's bank account
Credit card fraud	Fraud committed using stolen credit card information
OPC	Office of the Privacy Commissioner
OVPC	Office of the Victorian Privacy Commissioner
Peer-to-peer	A form of decentralised network where computers can exchange information directly with any other computer
Phishing	The act of assuming the online identity of a legitimate organisation to trick users into divulging information or to commit fraud
PM & C	Department of the Prime Minister and Cabinet
QPS	Queensland Police Service
Romance scam	A scam where victims hand over money to fraudulent participants on online dating websites
Rootkit	A set of programs designed to hide malware infections on a computer
SA	South Australia
SME	Small or medium sized enterprise
SOCA	UK Serious and Organised Crime Agency

Spam	Unsolicited bulk email messages
Spamtrap	A dummy email address used to attract spam (See ‘Honeypot’)
Spyware	A program that illegally records data such as computer screen images, stored data and details on internet browsing activity
TISN	Trusted Information Sharing Network for Critical Infrastructure Protection
Toolkit	Off-the-shelf style, user-friendly malware packages
Trojan	Malware which appears legitimate but in fact contains hidden malicious functions
UK	United Kingdom
US	United States of America
Virus	Malware contained within a ‘host’ program which spreads by inserting a copy of itself into other programs
WA	Western Australia
Walled garden	Restricted network access to isolate infected computers from other computers on a network
Whitelist	A list or register of persons or computers who are permitted access to a network or computer system, to the exclusion of those not on the list
Worm	Self-replicating malware which transmits across a network without a host program
WPISP	OECD Working Party for Information Security and Privacy
Zombie	See ‘Bot’

List of recommendations

3 Research and Data Collection

Recommendation 1

That the Australian Government nominate an appropriate agency(s) to:

- conduct a stock take of current sources of data and research on cyber crime;
- develop clear national definitions and procedures for the collection of data on cyber crime; and
- negotiate clear agreements between government agencies and industry on the sharing and protection of information for research purposes.

Recommendation 2

That the Australian Government nominate an appropriate agency(s) to collect and analyse data, and to publish an annual or bi-annual report on cyber crime in Australia.

5 Domestic and International Coordination

Recommendation 3

That the Australian Government establish an Office of Online Security headed by a Cyber Security Coordinator with expertise in cyber crime and e-security located in the Department of Prime Minster and Cabinet, with responsibility for whole of Government coordination. The Office is to take a national perspective and work with State and Territory governments, as well as federal regulators, departments, industry and consumers.

That the Australian Government establish a National Cyber Crime Advisory Committee with representation from both the public and private sector to provide expert advice to Government.

Recommendation 4

That the Australian Government, in consultation with the State and Territory governments and key IT, banking and other industry and consumer stakeholders, develop a national online cyber crime reporting facility geared toward consumers and small and medium sized businesses.

This model should include the following features:

- a single portal for standardised online receipt of cyber crime reports across a wide range of cyber crime types (e.g. malware, spam, phishing, scams, identity theft and fraud);
- a 24/7 reporting and helpline;
- no financial minimum to be applied to cyber crime reports;
- systematic data collection that allows data to be aggregated;
- referral to appropriate authorities and cooperation on the disruption of cyber crime and targeted prosecutions;
- free access to scanning software to detect malware;
- public information about cyber crime types and preventative measures to increase online personal security;
- e-security alerts tailored to the needs of ordinary consumers and small and medium sized businesses; and
- analysis of cyber crime methodologies and trends or cooperation with another body to perform that analysis.

Recommendation 5

That the Federal, State and Territory police forces establish an E Crime Managers Group to facilitate the sharing of information and cross jurisdiction cooperation.

Recommendation 6

That the Australian Government, in consultation with the State and Territory governments, industry and consumer organisations, develop a national law enforcement training facility for the investigation of cyber crime.

Recommendation 7

That the Australian Government consult with major IT security vendors, academia and key industry stakeholders to develop:

- options for establishing a coordinated public-private capacity to provide real time operational information on a wider range of cyber crime types that impact on Australian consumers;
- an 'intelligence hub' that facilitates information sharing within and across industry sectors and provides:
  - ⇒ longer term analysis on cyber crime methodologies across a range of cyber crime types;
  - ⇒ education on the preservation of digital evidence; and
  - ⇒ support to law enforcement agencies for targeted prosecutions in Australia and overseas.

6 Criminal and Law Enforcement Framework

Recommendation 8

That the Federal, State and Territory Attorneys-General review the existing computer and identity fraud provisions and, if necessary, introduce or amend provisions to ensure consistency across all Australian jurisdictions.

Recommendation 9

That the Federal Attorney-General, in consultation with State and Territory counterparts, give priority to the review of Australian law and practice and move expeditiously to accede to the Council of Europe Convention on Cybercrime.

Recommendation 10

That Australia's cyber crime policy strategically target the underground economy in malicious IT tools and personal financial information; the disruption of botnets and the identification and prosecution of botherders.

Recommendation 11

That the Commonwealth, State and Territory governments establish a national working group on cyber crime to maintain an ongoing, dedicated mechanism for the review and development of legislative responses to cyber crime.

That the working group take a whole of cyberspace perspective and consider relevant IT industry, consumer protection and privacy issues as well as the criminal law.

7 Protecting the Integrity of the Internet

Recommendation 12

That the Australian Communications and Media Authority further increase its access to network data for the purpose of detecting malware compromised computers. This should include active consideration of how to increase access to network data held by global IT security companies and, in consultation with relevant departments, whether legal protections to address commercial, regulatory and privacy concerns are desirable.

Recommendation 13

That the Australian Communications and Media Authority consider how best the Australian Internet Security Initiative network data might be used to support the threat assessment and emergency response functions of government.

Recommendation 14

That the Australian Communications and Media Authority take the lead role and work with the Internet Industry Association to immediately elaborate a detailed e-security code of practice to be registered under the *Telecommunications Act 1997* (Cth).

That the code of practice include:

- an obligation that the Internet Service Provider provides basic security advice when an account is set up to assist the end user to protect themselves from hacking and malware infections;
- a mandatory obligation to inform end users when their IP address has been identified as linked to an infected machine(s);
- a clear policy on graduated access restrictions and, if necessary, disconnection until the infected machine is remediated;
- the provision of basic advice and referral for technical assistance for remediation; and

- a requirement that acceptable use policies include contractual obligations that require a subscriber to:
  - ⇒ install anti-virus software and firewalls before the Internet connection is activated;
  - ⇒ endeavour to keep e-security software protections up to date; and
  - ⇒ take reasonable steps to remediate their computer(s) when notified of suspected malware compromise.

Recommendation 15

That the Australian Government, in consultation with the Internet industry, review the scope and adequacy of s.313 of the *Telecommunications Act 1997* (Cth) to promote Internet Service Provider action to combat the problem of malware infected machines operating across the Internet.

Recommendation 16

That a more integrated model for the detection and removal of malware, built on the Australian Internet Security Initiative, be implemented. The new scheme should involve the Australian Communications and Media Authority, Internet Service Providers, IT security specialists, and end users in a more tightly coordinated scheme to detect and clean malware infected computers.

Recommendation 17

That the Australian Communications and Media Authority be funded to develop a system that can obtain data on compromised web pages from various sources (including developing an internal capability). This data be collated and provided as daily aggregated reports to Internet Service Providers identifying infected web pages residing on their networks.

That in addition to Internet Service Providers, domain owners and hosting companies also be included in the new scheme.

Recommendation 18

That the system for reporting and detecting compromised web pages proposed in recommendation 17 be supported by a registered industry code that outlines industry procedures for dealing with infected websites.

That the Australian Communications and Media Authority be empowered to enforce the provisions of the registered code, including, for example, where there is a need to direct a service provider to remove malicious content.

That Internet Service Providers and hosting companies who act on reports of infected websites be indemnified against claims for losses.

Recommendation 19

That the Australian Communications and Media Authority and the Internet Industry Association review the *Spam Code of Practice* to assess the effectiveness of current industry standards for the reporting of spam.

That serious consideration be given to obliging Internet Service Providers to include the Australian Communications and Media Authority's *SpamMatters* program as part of their email service to subscribers.

Recommendation 20

That the Australian domain name registration industry be subject to a code of conduct that is consistent with the Anti-Phishing Working Group *Best Practices Recommendations for Registrars*.

The code of conduct should:

- enumerate the type of information that should be collected during the domain name registration process by the registrar, that would help to preserve evidence and assist law enforcement authorities;
- identify processes that should be put in place to identify fraudulent activity before the domain name registration takes effect; and
- provide clear procedures for responding to requests for rapid take down of fraudulent sites and sites that host malware.

Recommendation 21

That the Minister for Broadband, Communications and the Digital Economy make a reference to the House of Representatives Standing Committee on Communications to inquire into the regulation, standards and practices of the domain name registration industry in Australia.

8 Consumer Protection

Recommendation 22

That the Australian Government ensure that:

- remedies available under the new Australian Consumer Law can be effectively asserted against perpetrators outside Australia; and

- the *Foreign Judgments Act 1991* (Cth) be amended to allow for the reciprocal registration and enforcement of non-money judgments made under the Australian Consumer Law.

Recommendation 23

That the Treasurer amend the Australian Consumer Law to include specific protections against the unauthorised installation of software programs:

- the reform should target the unauthorised installation of programs that monitor, collect, and disclose information about end users' Internet purchasing and Internet browsing activity;
- the authority to install a software program must be based on informed consent; and
- to obtain informed consent the licence/agreement must require clear accessible and unambiguous language.

Recommendation 24

That the Australian Competition and Consumer Commission, in consultation with manufacturers and distributors of personal computers, mobile phones and related IT devices such as modems and routers, develop information standards to:

- address the e-security vulnerabilities of these products and the provision of e-security information to consumers at the point of sale; and
- require that the information is presented in a manner that is clear and accessible to a non-IT literate person.

Recommendation 25

That the Treasurer direct the Productivity Commission to conduct an in depth investigation and analysis of the economic and social costs of the lack of security in the IT hardware and software products market, and its impact on the efficient functioning of the Australian economy.

That, as part of its inquiry, the Productivity Commission address the merits of an industry specific regulation under the Australian Consumer Law, including a scheme for the compulsory independent testing and evaluation of IT products and a product labelling scheme.

Recommendation 26

That the Treasurer consult with State and Territory counterparts with a view to amending the Australian Consumer Law to provide a cause of action for compensation against a manufacturer who releases an IT product onto the Australian market with known vulnerabilities that causes losses that could not have reasonably been avoided.

Recommendation 27

That the manufacturers of IT products adopt a best practice approach that ensures products are designed to prompt and guide end users to adopt more secure settings.

That the Australian Government monitor industry practice in this regard, and promote international standards that put a higher priority on security through product design.

9 Privacy Measures to Combat Cyber Crime

Recommendation 28

That the Office of the Privacy Commissioner use the full extent of its powers to ensure that overseas organisations that handle the personal information of Australian citizens and residents are aware of, and adhere to, their obligations under the *Privacy Act 1988* (Cth).

Recommendation 29

That the Office of the Privacy Commissioner expedite the adoption of an approved privacy code of practice for members of the Australian Internet industry, including smaller Internet Service Providers.

Recommendation 30

That the Office of the Privacy Commissioner encourage government agencies and commercial organisations to undertake regular audits to identify risks to personal information in both new and existing projects and policies.

10 Community Awareness and Education Initiatives

Recommendation 31

That the Department of Broadband, Communications and the Digital Economy, in consultation with relevant agencies, industry and community organisations, develop a nationally coordinated strategy for the education of consumers:

- that the strategy cover all aspects of cyber crime including malware, identity theft, identity fraud and scams; and

- includes clear benchmarks against which the effectiveness of education initiatives can be clearly evaluated and publicly reported on to Parliament.

Recommendation 32

That the Stay Smart Online and SCAMwatch websites be linked to the national cyber crime reporting centre referred to in recommendation 4.

Recommendation 33

That the Department of Broadband, Communications and the Digital Economy implement a public health style campaign that uses a wide range of media to deliver messages on cyber security issues, technical precautions and appropriate user behaviours.

Recommendation 34

That the Department of Broadband, Communications and the Digital Economy support the development of IT literacy training that includes cyber security and is available to the community as a whole.