

## **Spam Act 2003 Review**

Submission from AusCERT

1 February 2006

### ***Executive Summary***

The Internet threat landscape has changed fundamentally since 2003 when the Spam Act was enacted with significantly increased incidence of online identity theft, a form of cyber crime. Looking forward, the concern is that this new form of criminally based activity poses the single greatest threat to trust and confidence on the Internet and, if left unchecked, will significantly harm the capacity of the Internet to be a suitable medium for e-commerce and e-government.

While the Spam Act 2003 remains and continues to be a useful piece of legislation for its specified purpose, the nature of the Internet threat environment has changed providing an opportunity for the Australian government to implement practical mechanisms that will help reduce the level of Internet based attacks emanating from or targeting Australian networks, particularly those motivated by illicit financial gain.

### ***Recommendations***

AusCERT recommends the use of appropriate mechanisms to facilitate:

- The identification of compromised hosts in Australia, particular ones engaged in active attacks such as phishing, distribution of online ID theft trojans, dissemination of viruses or worms, and denial of service attacks;
- The identification of compromised hosts in Australia that are being used to distribute any form of spam as defined in the Act; or which may be used in future to distribute spam by overseas based spammers;
- The use of mechanisms to compel ISPs to take appropriate steps in order to prevent further abuse by a compromised (or attacking) computer;
- Extending many of these same obligations on ISPs to include Australian based Domain Name Registrars to prevent the use of domain names as an alternate means of facilitating attacking or fraudulent web sites;
- The requirement by ISPs to implement technologies and policies to fight spam.

AusCERT also supports

- The internationalisation of the Australian Communication and Media Authority's (ACMA) Internet Security Initiative (ISI) through CERT network cooperation and through Australian and foreign government agreements to

help further reduce the volume and duration of Internet based attacks from compromised computers emanating from overseas; and

- The development of a 'safe harbour' computer security awareness and recovery web site as an adjunct to the ISI.

These mechanisms and initiatives may involve amendments to the Telecommunications Act, Spam Act 2003, regulatory powers of ACMA, industry codes and standards, or support for organisations such as AusCERT which is actively involved in reducing level of computer network attack activity in Australia and helping Australian organisations better protect their networks.

However, legislative mechanisms, by themselves, are unlikely to be sufficient to make a significant impact in curtailing the level of Internet based attacks directed against or emanating from Australian networks. Most attacks targeting Australian computers or networks are sourced from overseas, or if launched within Australia are undertaken from compromised computers making it difficult to identify or prosecute the attacker and beneficiary of such attacks.

Therefore, in addition to appropriate legislative support, AusCERT advocates the proposed mechanisms and initiatives to enable action to be taken by responsible and authoritative parties, including ACMA, ISPs, domain name registrars and AusCERT, as Australia's national CERT, to reduce the number of ongoing Internet based attacks emanating from Australian networks.

These actions, including increased support of ACMA and AusCERT, are likely to reduce the level of Internet based attacks sourced within Australia and provide benefit to Australian and overseas based organisations which are being harmed by such attacks. From AusCERT's perspective, it is more difficult to seek assistance and support from overseas counterparts to deal with off shore sourced attacks if Australia is not able to offer a timely reciprocated response.

## **AusCERT's role in preventing and mitigating Internet based attacks**

AusCERT is Australia's national Computer Emergency Response Team. AusCERT is an independent, not-for-profit, non-government organisation based within the University of Queensland.

In its capacity and role as the national CERT, AusCERT provides advice to Australian Internet community about computer threats and vulnerabilities and how to better secure their computers to prevent computer attacks.

AusCERT provides incident response assistance to Australian and overseas networks experiencing Internet based attacks emanating from Australia or being directed against Australian networks and/or their customers.

AusCERT, together with the Australian High Tech Crime Centre, has been at the forefront of monitoring, analysing and responding to incidents of online ID theft in Australia since March 2003. AusCERT is regarded as an expert in this field and has been asked to brief many local and overseas banking, government and law enforcement agencies about the nature of the threat.

## Nature of online identity theft and other Internet based attacks

Since March 2003, AusCERT has monitored and reported through various publications<sup>1</sup> the emergence and rapid escalation of online identity theft using computer technology and/or computer network attack techniques for the purposes of illicit financial gain. The majority of such incidents involve phishing attacks and trojan attacks. In the latter case, criminals motivated by illicit financial gain install trojan malware on compromised or purpose built web sites for the purposes of compromising and then capturing a large range of personal information of financial value from any computer that connects to the trojan hosting site.

Such attacks currently depend heavily on the dissemination of malicious spam as the initial attack vector to induce potential victims to disclose their personal information to the attacker controlled web site (phishing) or to click on a link to a web site established by the attacker to compromise the victim's computer. Compromise then occurs by the exploitation of vulnerabilities on the victim's computer and/or by downloading malware to facilitate subsequent stages of the malware attack.

The success of such attacks requires the attackers to gain access to a large supply of compromised hosts. Access to such hosts may be achieved by the attackers compromising the hosts themselves, or by purchasing networks of distributed compromised hosts (botnets) from a third party. The number of compromised hosts involved in a single phishing or trojan attack varies but AusCERT has seen about 100 compromised hosts involved in a single attack. Certainly attacks involving at least 20 or more compromised hosts are now common.<sup>2</sup> From an incident response and mitigation perspective, typically, the more hosts or sites involved, the longer it takes to identify all attacking hosts and contact the range of CERTs, ISPs and domain name registrars to request the closure of such sites. This is done to increase the time the attack is able to remain active and hence affect more victims.

It is commonplace for botnets involving many thousands of hosts to be involved in distributed denial of service attacks, which may or may not be illicitly financially

---

<sup>1</sup> AusCERT (2006), Case study – personalized phishing site

AusCERT (2005), e-government phishing attack was aided by poor coding on legitimate government web site

AusCERT (2005), Managing Risk Associated with Online ID Theft for Government and Providers of e-Government Services

AusCERT (2005), Trends and Developments in Online ID Theft – Update No. 2

AusCERT (2004), Trends and Developments in Online ID Theft, No. 1

AusCERT, Australian High Tech Crime Centre, AFP, NSW Police, Northern Territory Police, Queensland Police, South Australia Police, Tasmania Police, Victoria Police, Western Australia Police, 2005 *Australian Computer Crime and Security Survey*, page 24 - 26

AusCERT, Australian High Tech Crime Centre, AFP, NSW Police, Northern Territory Police, Queensland Police, South Australia Police, Tasmania Police, Victoria Police, Western Australia Police, 2004 *Australian Computer Crime and Security Survey*, page 24 - 25

AusCERT, AFP, Queensland Police, South Australia Police, Western Australia Police, 2003 *Australian Computer Crime and Security Survey*, page 19

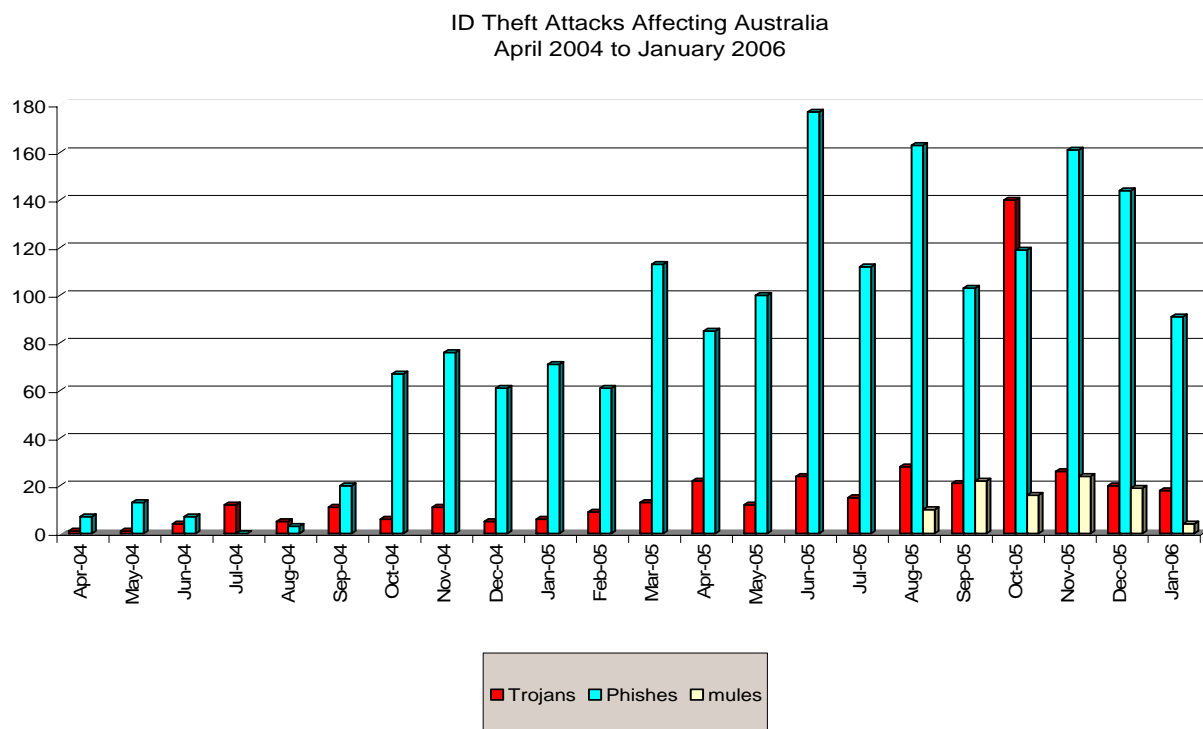
<sup>2</sup> Please note these figures refer to the number of hosts or sites which may be involved in undertaking or facilitating a cyber attack for the purposes of illicit financial gain. From an incident response perspective, AusCERT seeks to contact appropriate parties such as ISPs, domain name registrars and various overseas based computer emergency response teams to reduce the time the attacking hosts or sites are able to operate. These figures do not represent the number of potential computers which subsequently may become compromised as a result of this attack, or the number of users who are fooled into disclosing their personal information from phishing attacks.

motivated. DDOS extortion attacks along with online ID theft have become increasingly popular mechanism to derive illicit revenue. In 2005, 14% of respondents to the Australian Computer crime and Security Survey reported experiencing DOS attacks with losses of around \$8 million in one case.<sup>3</sup> Notably, large botnets in excess of one million hosts have been reported. Invariably the risk posed by DDOS attacks involving many thousands of hosts is that they can (potentially) deny service – not just to the end target – but to various ISPs and telecommunication carriers enroute.

In a single online identity theft attack, compromised hosts are typically required for the following functions:

- To distribute spam with anonymity, ie with the identity of the compromised host or a spoofed (false) IP address (may be many)
- To host the phishing or trojan site (may be many)
- To host decoy or redirect sites (may be many)
- To record the captured data (may be a web site, including with restricted access, or an email address)
- Control site which the attacker stores a range of tools, images, files etc for facilitating the current and further attacks of a similar nature.

The following diagram gives an indication of the increased number of attacks affecting Australian Internet users and/or Australian networks.

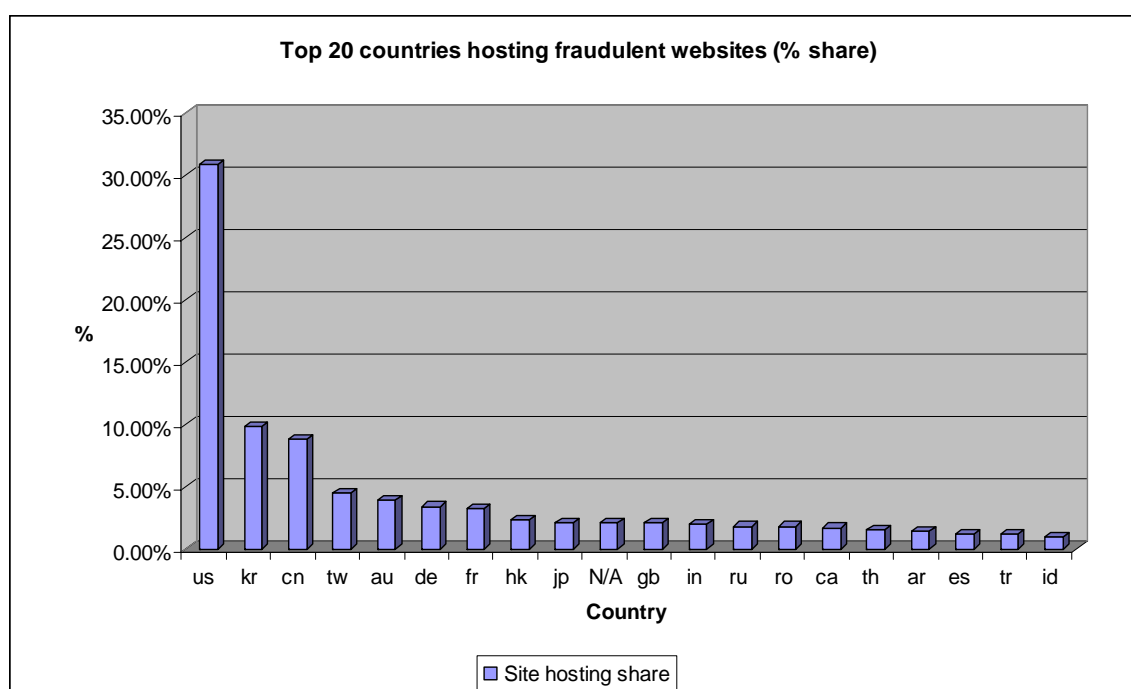


<sup>3</sup> AusCERT, Australian High Tech Crime Centre, AFP, NSW Police, Northern Territory Police, Queensland Police, South Australia Police, Tasmania Police, Victoria Police, Western Australia Police, 2004 Australian Computer Crime and Security Survey, page 26, <http://www.auscert.org.au/crimesurvey>

AusCERT assesses that the level of online ID theft will only continue to grow as:

- More Australians adopt broadband technology;
- More Australians and Australian organisations in the public and private sector provide services and information online with a financial value;
- Single factor authentication remains the primary means of authentication for e-government and e-commerce transactions;
- The underlying security of mainstream operating systems continue to be highly vulnerable to compromise;
- The level of skill required to effectively secure a remote client computer and to recognise common techniques attackers use to fool users into taking risks online increase; and
- Attackers succeed in generating illicit financial revenue from the attacks with a low level of risk of prosecution when they operate abroad from the countries and computer users which they target.

As the graph below shows, a proportion of these attacks are hosted in Australia. Typically attacks hosted in Australia target non-Australian interests and conversely, most attacks directed at Australian Internet users or Australian based networks are hosted abroad (often in the USA).



It is assessed that a key factor for the high volume of sites hosted in the US, is that the US offers a large supply of vulnerable hosts and that, on average, it takes longer to close a site in the US than it does in most other places. Such factors are important to attackers to optimise the duration of an attack.

Noteworthy is that Australia is currently ranked 5<sup>th</sup> highest compromised hosting site in the world, which may be attributed to the large number of broadband-connected computers available to attackers to compromise.

## Review

AusCERT believes that Australia legislation is sufficient to make it a criminal act to knowingly distribute spam, to compromise a computer, or to use an already compromised computer or compromise a computer in the commission of another crime such as fraud. However, we believe that legislation including the Spam Act 2003 could be strengthened to give greater protection to ISPs, including indemnify them against action taken to disconnect compromised hosts owned by their customers that are present on their network. ISPs should not need to rely solely on the provisions of acceptable use agreements to enable them to act quickly in good faith and to restrict liability for these actions.

Similarly, ACMA as the regulator for the telecommunications sector should also have the power and resources to ensure that ISPs and domain name registrars are taking action in a timely and effective manner against compromised computers on their network that are engaged in illegal activities, either at their own initiative, or in response to authorised third party requests such as from ACMA, Australian law enforcement or AusCERT.

This should ensure that ISPs have the authority to proactively identify such hosts within their network and act, or if lacking in skills or resources to identify such hosts, should be able to confidently take action based on the advice of a recognised independent authoritative third party, such as Australian law enforcement, ACMA or AusCERT.

Therefore, AusCERT supports practical mechanisms which complement existing legislation to enable the identification of compromised or attacking hosts or sites with domain names being used solely for fraudulent purposes within Australia and which enable or facilitate their timely closure or deregistration.<sup>4</sup>

Within the Act culpability rests with individuals within Australia who willingly and knowingly distribute spam. While AusCERT supports criminal culpability resting with such parties, it is a fact that the existence of many thousands of insecure and compromised computers on the Internet provide attackers and spammers with the computing resources needed to launch such attacks, often with a large degree of impunity. Individuals and organisations that allow their computers (either wittingly or unwittingly) to be used to facilitate such attacks by criminals are also contributing to the broader problem of Internet based illicit financial gain, and malicious attacks. However, AusCERT does not support criminal culpability being laid against computer owners whose computers are used unwittingly to facilitate such attacks.

Owners of compromised computers pay for the bandwidth and computer processing and storage capacity used by the criminals and may potentially face an increased risk of liability in civil or criminal proceedings.

Therefore, mechanisms which help identify insecure and compromised computers and help the owners of such computers to recover and secure their computers in Australia and elsewhere will reduce the computing resources available to attackers and cyber criminals to operate.

---

<sup>4</sup> AusCERT only supports deregistration when a domain has been established solely for fraudulent purposes. We would not support deregistration of domain names, where an attacker has compromised an existing legitimate domain for illicit financial gain.

Owners of compromised computers in Australia will also benefit from being notified of the use of their computer in the commission of various criminal acts and gaining access to services that facilitate their recovery.

AusCERT recommends that the provisions in the Spam Act 2003 and the Telecommunications Act be enhanced, either through changes to the legislation, or perhaps, more appropriately, through:

- the use of stringent codes of practice for ISPs and domain name registrars.
- Increased support for organisations such as ACMA and AusCERT which are actively involved in identifying, responding to reports of cyber attack and seeking assistance from CERTs, ISPs and domain name registrars to take mitigation action.

Mitigation options by ISPs may include disconnecting the attacking or compromised host (computer) from the Internet; or restricting the level of Internet access to the host until such time as the host is no longer compromised, etc. This could be similar to the “safe harbour” provisions that currently serve to protect the actions of certain Internet service providers when dealing with cases of alleged copyright infringements (Copyright Amendment Act 2004 (*Cth.*)).

In making this recommendation, it is noteworthy that most spam is disseminated from compromised hosts – not open mail relays as was often the case in the past.

Therefore, a key factor to prevent the dissemination of spam, whether sourced from overseas or within Australia, and other Internet based attacks is to identify and secure the compromised hosts that are used to facilitate such attacks.

ACMA’s Internet Security Initiative (ISI) provides an automated mechanism to accept data feeds to help Australian ISPs identify compromised hosts, including those involved in active Internet based attacks, on Australian networks. While ‘action’ by the ISP is ‘voluntary’ and the ISI is currently in early pilot stage, it would be worth monitoring and assessing the efficacy of the voluntary scheme to determine whether it is adequate to provide a noticeable reduction in longevity of compromised Australian hosts particularly when it is assessed that the number of compromised hosts in Australia is likely to rise in future.

The roles currently being played by both ACMA and AusCERT in reducing the capacity for, and duration of, Internet based cyber attacks and increasing the level of response from ISPs and domain name registrars complements the role of Law Enforcement Agencies which are grappling with the inherent problems of enforcing laws in a borderless virtual environment.

These initiatives, in turn, will enable the Australian government to more effectively lobby for similar initiatives to be introduced overseas in countries and jurisdictions which host the vast majority of compromised computers that harm Australian Internet users. Effective cross border detection, mitigation and response to malicious activity on the Internet can be founded on sound domestic response arrangements. The overall objective of any approach to dealing with the current generation of criminally motivated computer network attack activity must be the creation of an international matrix of response arrangements that link seamlessly across international borders.

Therefore, AusCERT also supports:

The internationalisation of the ISI through CERT network cooperation and through Australian and foreign government agreements to help further reduce the volume and duration of Internet based attacks from compromised computers emanating from overseas. This strategy will be particularly important to reduce the volume and impact of cyber attacks directed against Australian Internet users.

AusCERT assesses the Spam Act 2003 has had a positive influence on reducing the levels of spam originating in Australia, and therefore, has and continues to serve a useful purpose. However, the Act 2003 has limited capacity to deter or facilitate the prosecution of overseas based spammers and overseas based spammers continue to distribute large volumes of spam to Australian Internet users. AusCERT has not attempted to quantify or assess whether spam levels have increased since 2003, however, it is our view that spam levels have continued to increase significantly.

AusCERT supports the continuing efforts of the Australian government to lobby foreign governments to introduce similar spam legislation within their own countries and for those countries to seek the prosecution of spammers in an effort to reduce the volume of spam within Australia and as a deterrent to other spammers and cyber criminals.

AusCERT supports the requirement by ISPs to implement technologies and policies to fight spam. Please refer to Proposal of the Brazilian Internet Steering Committee's Task Force on Spam for examples, which is attached.<sup>5</sup>

AusCERT supports the requirement by ISPs to offer a premium service which includes malware and spam filtering, which may be offered to consumers in addition to existing services on a user-pays basis. Such mechanisms will not prevent all incidents of online identity theft or cybercrime but represents another measure which in combination with other mechanisms can help improve the overall quality of Internet security within Australia.

## **Other non-regulatory measures**

AusCERT as a small organisation has limited resources and is seeking to deal with a threat environment that is rapidly worsening. Better support and funding from the Australian government would allow AusCERT to provide increased levels of incident response to support the ISI and its existing role.

In Brazil, where cybercrime levels are significantly higher than Australia, CERT.br performs a similar role and function to AusCERT. Because the entire Internet using community in Brazil are the main beneficiaries of their work they receive funding from a portion of the domain registration fees levied in Brazil for the .br domain. Further information can be provided about CERT.br governance and funding models if required.

As an adjunct to the ISI, AusCERT supports ACMA's idea to establish a dedicated web site to provide protection and recovery advice, tools and resources to users whose computers have been quarantined from open Internet access until they take

---

<sup>5</sup> Hoepers, C. and Steding-Jessen, K, CERT.br, (13 May 2005) Proposal of the Brazilian Internet Steering Committee's Task Force on Spam



appropriate steps to clean their computers and/or remove files or programs that are contributing to attacks on third parties. Given AusCERT's role and function and computer security expertise, AusCERT is best place to develop, maintain and host such a site.