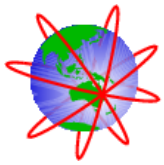

AusCERT

Australia's National Computer Emergency Response Team

Review of .au domain name policy framework

Submission to .auDA

15 June 2007

Background

AusCERT is the national Computer Emergency Response Team (CERT) for Australia and a leading CERT in the Asia/Pacific region and the world.

As the national CERT, AusCERT is an independent, not-for-profit organisation that supports Australian interests by helping to protect the security of the Australian Internet using community, primarily by:

- Monitoring, analysing and providing advice about computer network threats and vulnerabilities;
- Providing assistance to Australian networks facing attack sourced from within Australia, or more often, overseas;
- Providing advice on how to protect against and recover from computer security attacks.

In providing incident response assistance for a high volume of Internet based attacks on a weekly basis, AusCERT often deals with computer network attacks involving the misuse of domain names in all domain spaces, including .au.

In making this submission, AusCERT refers the Review Panel to a previous submission made by AusCERT on this matter in 2006. AusCERT's submission to the 2006 review and structure of the .au Internet Domain is available from:

http://www.auscert.org.au/7019

The points raised in the earlier submission remain just as relevant today as they were in 2006 with no discernible reduction in the registration of domain names for fraudulent or criminal purposes.

1. Should .au be opened up to direct registrations (eg. domainname.au)? If yes, should there be any policy rules, and if so what rules?

In reviewing .auDA's discussion paper on this issue, AusCERT notes that .auDA has identified more compelling issues to oppose the direct registration of .au domains than it has identified in favour.

Of most concern to AusCERT are the security and fraud related issues which are likely to arise in a situation which allows directname registration, regardless of whether option 1 (exclusive directname registration) or option 2 (combination or directname and 3LD) is chosen. As noted under 7.9 of the paper:

> *Introducing direct registrations may lead to increased disputes about rights to a domain name. … ultimately only one entity can secure the .au version of a domain name, which is particularly problematic where the same domain name is held by different registrants in different 2LDs.*
>
> *Regardless of which implementation option is adopted, introducing direct registrations is likely to cause user confusion, at least in the short to medium term … and may lead to an increased risk in phishing and scams.*

AusCERT assesses this confusion is likely to persist in the long term and be used to the advantage of criminal elements for fraudulent purposes by compromising the security of Internet users' computers and/or data. This assessment is based on extensive experience monitoring and responding to cyber crimes which rely on the use of specially registered domains over several years.

Since 2003, AusCERT has been actively involved in monitoring and responding to various forms of cybercrime (including but not limited to phishing and malware designed to stealing access credentials and personal information; soliciting mules for money laundering and launching denial of service attacks). Many of these attacks rely on the use of specially registered domains. Sometimes domains are chosen because they bear a similarity to well known domain names or entities or attempt to sound legitimate in their own right by describing a legitimate service but many do not appear to have any particular significance or meaning. Therefore, it is difficult to assess by the domain name itself whether it will be used for fraudulent purposes. In this regard it is important that the registration process be as thorough as possible, including adequate identification of the domain owner, to assess the likely legitimacy of the domain.

By allowing direct registrations (under option 1), criminals could potentially register domains such as :

> ato.au
> tax.au
> yourtax.au

to fool users into thinking they are communicating with the Australian Taxation Office or some other commercial taxation advisory service. Whereas maintaining the use of 2LDs

within the .au space provides the added identifier of whether the site is a government (.gov.au) or commercial (.com.au) domain or other type of entity etc. Under current guidelines it is more difficult to register a fraudulent .com.au domain.

Another reason to oppose option 1 in particular, is that it would preclude the ability to subsequently allow the introduction of new 2LDs in the .au space, such as .bank.au, which is a very useful initiative which can help prevent consumers falling victim to phishing related attacks.[1]

Alternatively (under option 2) as noted above, it is possible for criminals to register auda.au to imply that auda.au is a trustworthy domain and for all intents and purposes identical to the well known domain auda.org.au and then use it to compromise the security of those that are fooled into clicking on an auda.au link or typing it directly into the web browser address bar.

If direct name registrations are to be permitted then the same stringent policies and procedures which currently govern the registration of domains under each of the existing 2LDs must be extended to the direct domains to ensure as much as possible they are being used for legitimate purposes and there is a nexus between the domain name and the person or entity.

In addition, if direct name registrations are to be permitted, the existing policies and procedures should be *tightened to enable the speedy deregistration* of the domain by the registrar and reseller in the event the domain is being used solely for fraudulent or criminal purposes, as discussed below.

2. Should the policy rules for asn.au, com.au, id.au, net.au and org.au be changed? If yes, what changes should be made?

AusCERT is opposed to any relaxation of the rules which currently pertain to the registration of each of the 2LDs within the .au namespace.

Given the difficulties, AusCERT (and others) continue to have in seeking the timely deregistration of domain names – most of which are currently registered overseas – being used for fraudulent/criminal purposes, AusCERT recommends policies and procedures be implemented in Australia for this purpose. Such policies and procedures are necessary precisely because deregistration requests for the most part do not originate from law enforcement.

AusCERT supports the suggestion outlined in 7.14 of the discussion paper, where the policies and procedures apply *only to the deregistration of domains that are registered solely for fraudulent or criminal purposes*. Such procedures should *not* apply to those cases where the web site of a *legitimate domain is compromised* and is being used by criminals to attack or compromise other computers. For example, the recent case of the

[1] http://www.dnc.org.nz/story/30272-29-1.html

Sydney Opera House web site (www.sydneyoperahouse.com) attack is an example of a legitimate domain name that is being used for legitimate purposes but the web site was compromised to deliver a trojan to the computers that connected to the web site.[2]

Moreover, the procedures must allow for *speedy* deregistration. AusCERT considers within 24 hours (regardless of whether it is a working day or not) once a registrar or reseller is notified of alleged criminal activity and the advice is based on the advice of an expert party is an appropriate time frame for a registrar or reseller to respond to requests from AusCERT or law enforcement (or other expert parties), that the domain is being used solely for fraudulent or criminal purposes.

The response in these cases must be speedy if they are to be at all effective. As noted by the APWG,[3] every minute these fraudulent sites are live increases the number of potential victims. A single attack involving a fraudulent domain that is serving malware that is up for longer than 24 hours is likely to infect or compromise many hundreds or thousands of computers and their users' data.

Some registrars and resellers have argued that they face liability risks if they deregister a domain based on a false claim, even if the advice or request to deregister the domain comes from a party with expertise in the area. To reduce their risks they argue they will only respond to a court order or law enforcement request. If policies and procedures to allow timely deregistration of specially registered fraudulent domains are to be effective, then the policies and procedures must address the registrars' concerns about liability, without simply shifting liability concerns to other parties who are attempting to mitigate the attack. This is probably a matter that requires further discussion and is an area of debate within the APWG about how this may best be achieved.

Contrary to popular belief, the vast majority of requests for deregistration of fraudulent domains, are not initiated by law enforcement. Nor does law enforcement necessarily have the expertise to identify fraudulent sites that are hosting malware. Therefore, such processes should not make law enforcement the *only* 'authority' for requesting that action is taken.

The importance of establishing appropriate policies and procedures for timely (accelerated) deregistration of domains that have been specially registered solely for criminal and fraudulent purposes is also being addressed by the Anti-Phishing Working Group.[4]

In particular, the APWG has confirmed AusCERT's own experiences that in the "vast majority of cases phishing [and malware] sites are not removed by law enforcement". It

---

2 http://www.smh.com.au/news/security/operahousehack/2007/06/11/1181414219766.html

3 APWG, Issues in Using DNS Whois Data for Phishing Site Take Down, http://www.antiphishing.org/reports/APWG_MemoOnDomainWhoisTake-Downs.pdf, page 4

4 Ibid.

is therefore, essential that the policies and procedures developed do not rely on registrars/resellers acting solely on the advice of law enforcement.

Given the volume of attacks of this nature that occur globally, including directed at Australian interests, it is unlikely law enforcement would be willing to add such requests to their current work loads. Therefore as a strategy for the timely removal of fraudulent domains, relying upon law enforcement alone is not practical. It is likely to overburden law enforcement and substantially increase the time that fraudulent domains remain active – further increasing the number of victims for each attack and compromising the integrity of the .au domain.

In some countries where domain registration rules are more relaxed, such as the ccTLDs of .hk, .cn and kr and also for the gTLDs, these domains include a far higher proportion of specially registered fraudulent domains. For example, the vast majority of cyber attacks against Australian interests which involve the use of a .hk domain are specially registered fraudulent domains. Typically, it is difficult to get such domains deregistered in Hong Kong[5] in a timely manner as registrars there will only respond to a local law enforcement request. As a consequence .hk domains are popular among cyber criminals. The impact is global – and can be used to attack people and systems in Hong Kong and around the world.

For example for the period between 1 January 2007 and 15 June 2007, AusCERT identified about 100 fraudulent domains registered within the .hk domain being used by criminals to compromise Australian computer systems and data. This is compared to about 70 fraudulent domains in the .hk space for the whole of 2006.

Around the world, however, the number of fraudulent domains registered at any one time is difficult to quantify but is assessed to be many thousands.

AusCERT also recommends that

1) resellers with termination authority for a domain are listed in WHOIS data; and

2) the same policy rules that apply to registrars also apply to resellers and that registrars should have more control over and accountability for the action of resellers.

3. Should registrants be allowed to sell their .au domain names?

AusCERT has no opinion on whether registrants should be allowed to sell their .au domains.

However, if this is permitted then, policies and procedures should be put in place to ensure that before the sale proceeds that the registrar/reseller has ensured that the proposed buyer has complied with all requirements to ensure they are entitled to purchase the domain according to the existing rules that apply to the sale of a new 3LD .au domain.

---

[5] Note that Hong Kong is only one example and is not the only problem area in this regard.