



AusCERT

Australia's National Computer Emergency Response Team

Review of structure and operation of the .au Internet domain

AusCERT Submission

28 November 2006

AusCERT background

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

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 regularly deals with computer network attacks involving the misuse of domain names in all domain spaces, including .au. AusCERT would like to respond to DCITA's discussion paper in this context.

Attack modus operandi involving domain names

Since March 2003, AusCERT has been at the forefront of monitoring, analysing and responding to incidents of online ID theft in Australia. The majority of such incidents involve phishing attacks and trojan attacks. In both cases, it is common practice for attackers to either host such attacks on compromised web domains or to specifically register a fraudulent domain on a compromised computer to support the attack. A significant proportion of these attacks use specially registered domains in order to conduct the attack and typically these are registered with false or stolen identity

information or credit card details. Using a specially registered domain is seen as beneficial by attackers to increase the longevity of their attacks, as the attacker can redirect victims to new malicious hosts as needed by updating their domain name records. So, in such an attack, the registrar becomes the ultimate point at which the attack can be disabled.

A compounding problem is that when domains are registered for the purpose of hosting malware, the web site may appear innocuous and unrelated to organisations or topics that could be associated with illicit financial gain or other forms of information theft. Unless registrars or resellers have experience in identifying malware and malicious web code – and most do not (particularly when anti-virus signatures may not yet have been produced and disseminated for the particular malware sample), it is often not readily apparent to registrars or resellers that the site is being used for fraudulent and illegal purposes. Consequently it can be extremely difficult to deregister the domain in a timely manner. In these situations, every minute a fraudulent domain is up, the more damage that occurs.

In these circumstances it would be useful to make provision in the policies and procedures to enable a registrar or reseller to deregister a domain in response to a request from an authoritative and independent third party with experience in malware detection and analysis.

So, any strategies, policies and procedures that can be adopted to prevent the registration of domains other than for demonstrably legitimate purposes would reduce the opportunity for Internet based attacks that are designed to steal a range of personal information and compromise computers on corporate, government and home networks.

While to date, some .au administration policies and practices are superior to domain administration in some other countries, unfortunately poor practices elsewhere impacts negatively on Australian Internet users. Therefore, it is incumbent on Australian policy makers to ensure that Australia administers its .au space as well as possible in order to provide an example to others. It is difficult to argue for changes elsewhere in order to protect Australian Internet users without adopting sound policies and procedures here.

3.1 .au administration

3a. In the broadest context, is the 'domain operator/registry/registrar/reseller' model the most appropriate for .au in delivering the most efficient and effective administrative structures? If not, what structural changes could provide greater efficiencies?

In AusCERT's experience, the accountability between registrars and resellers can sometimes be unclear and poorly managed. The policies which guide a registrar's actions do not always appear to be applied to resellers. For example, one of the few fraudulent registrations of domain names AusCERT has experienced in the .au space was accepted by a reseller.

AusCERT regularly requests assistance from registrars and resellers in disabling domains registered for purely fraudulent purposes. Often, it is a registrar who is listed in the WHOIS contact information for a domain, but a reseller who is delegated

responsibility for disabling the domain itself. Even if a registrar shows excellent response times when disabling domains that they control, AusCERT has often found that their resellers may not.

AusCERT recommends that:

- 1) resellers with termination authority for a domain are listed in WHOIS data; and
- 2) registrars should have more control over and accountability for the policies of resellers.

6.5 Domain name eligibility and allocation

6j. Could a relaxation of these rules facilitate meaningful growth in .au, or could it lead to inappropriate name registration and hoarding practices?

AusCERT believes that the current practices of domain allocation are working well, and should not be changed. A relaxation of these rules would almost certainly result in a substantial increase in the number of fraudulent domains registered in the .au space. AusCERT has observed this behaviour repeatedly in handling many thousands of fraudulent domain registrations elsewhere in the world.

The .au space is currently seen by many as being reputable. A domain existing in the .au space is highly likely to belong to the organisation whose name appears in the domain name. This has been of great value to Australian consumers and organisations to quickly and reliably establish the ownership of an .au domain name, since they know from experience that it has a reasonable level of trust.

A commonly-used technique by fraudsters is to register a domain name that is a slight variation of a legitimate domain name. For example, a criminal may register 0lb.com.au as an attack against a legitimate online bank that uses the olb.com.au domain. This makes it more difficult for consumers to verify the correct owner of the domain, which enhances the credibility of the attempt to steal personal information.

Continuing to verify the identity of the registrant and preventing reselling of domains will limit the opportunity to register fraudulent domain registrations in the .au space. In the past two years, AusCERT has observed only two domain names used for identity theft in the .au space as opposed to thousands in the .com, .net, .biz, .info and some other ccTLD spaces which are less tightly controlled. Relaxation of the rules on eligibility and allocation will facilitate such attacks within the Australian namespace.

AusCERT strongly recommends that auDA's current policy for domain name eligibility and allocation is maintained to preserve high consumer confidence in the .au namespace, specifically to ensure the verification of:

- the identity of the registrant and
- the nature of the business or proposed use of the domain is legitimate and bears a resemblance to the requested domain.

Conclusion

Overall, the majority of the questions posed by the review of the .au namespace do not have a significant impact on the security and confidence of the Australian Internet space. However, the items highlighted by AusCERT above are of critical impact and should be considered in the most serious possible light. AusCERT deals with the issues discussed above day-in day-out as a course of business. Therefore, AusCERT is an authoritative source of information on this topic in the global context. Please feel free to contact us should you require any further information or should you wish to discuss these issues more fully.