ausregistry

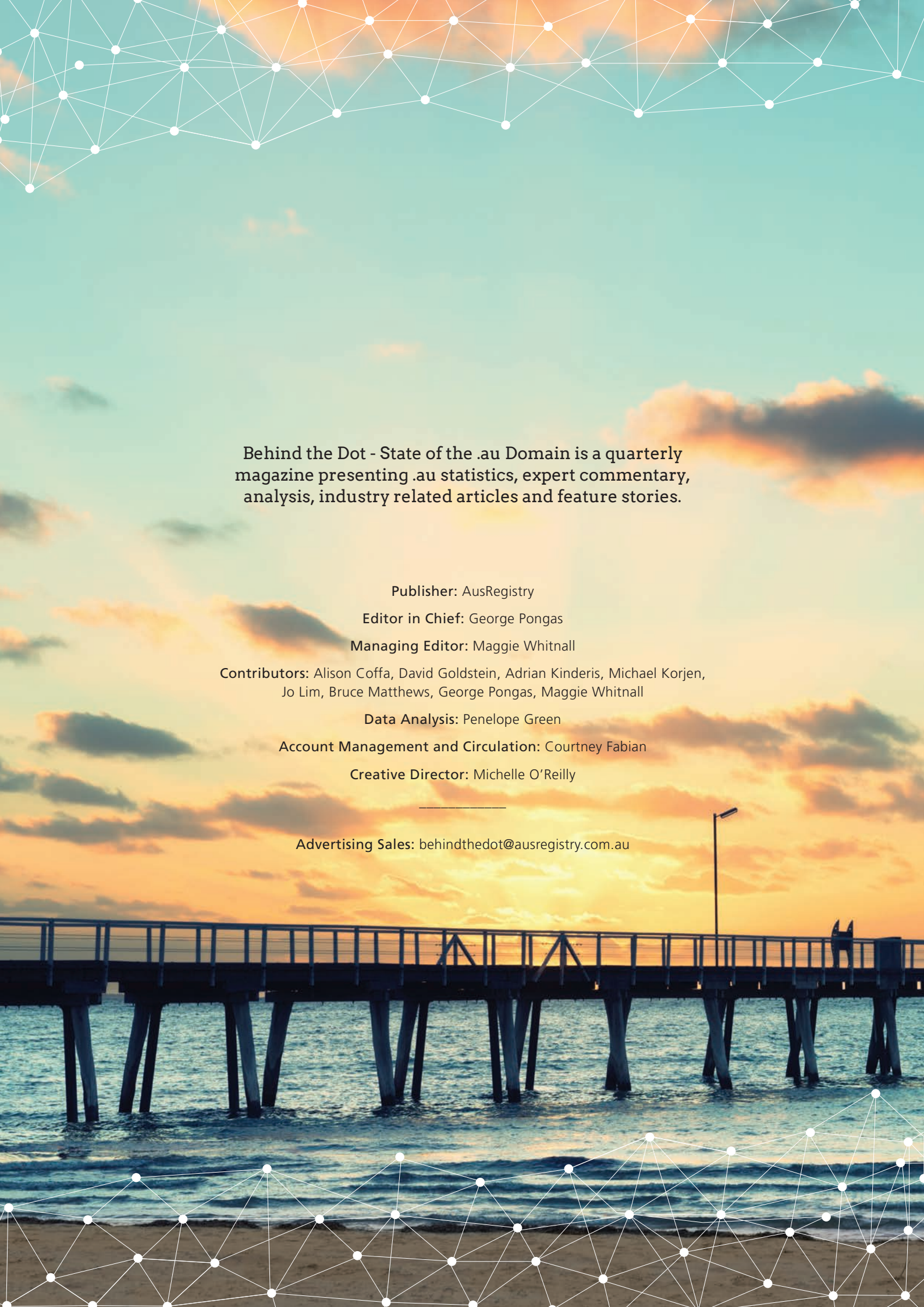
Edition 6, Feb 2016

BEHIND THE DOT

state of the .au domain

CYBER SECURITY & THREATS

tips and insights to protect your business and stay safe online



Behind the Dot - State of the .au Domain is a quarterly magazine presenting .au statistics, expert commentary, analysis, industry related articles and feature stories.

Publisher: AusRegistry

Editor in Chief: George Pongas

Managing Editor: Maggie Whitnall

Contributors: Alison Coffa, David Goldstein, Adrian Kinderis, Michael Korjen, Jo Lim, Bruce Matthews, George Pongas, Maggie Whitnall

Data Analysis: Penelope Green

Account Management and Circulation: Courtney Fabian

Creative Director: Michelle O'Reilly

Advertising Sales: behindthedot@ausregistry.com.au

Contents

DEPARTMENTS

Visit our new website to view more reports
ausregistry.com.au/research-au

FEATURE

CHARTS & TABLES


3,000,766
.au domain names
currently registered
31 December 2015

Foreword

Welcome to the sixth edition of AusRegistry's industry report, *Behind the Dot: State of the .au Domain.*

Trust is an integral aspect of the .au namespace. Our .au survey has consistently shown that Australian Internet users are more likely to trust a website that ends in .au and that they associate .au domain names with Australian entities.

Maintaining this trust is of vital importance to us at AusRegistry; not only to ensure the continued growth of the .au namespace but also to fulfil our commitment to Australia's Internet community and establish .au as a global leader.

It is for this reason we've dedicated this edition of *Behind the Dot* to the important theme of security.

A significant tool for protecting our country's online ecosystem has been the implementation of DNS Security Extensions, otherwise known as DNSSEC. In this edition, we've examined DNSSEC in detail to outline how it works and who should consider implementing it.

Online security is not however, an issue solely for Registries. Major brands and individuals alike can and should take essential steps to ensure their data, assets and reputations are protected from online attacks. This edition of *Behind the Dot* contains a close look at some of the major global brands that have been threatened by digital hijackers; as well as some of the risks to individual domain name registrants and some tactics for addressing them.

We've also called upon some of Australia's leading security experts for their tips and insights on staying safe online. CERT Australia Technical Director, Dr Jason Smith gives us his views on cyber security issues affecting critical infrastructure, while Bruce Matthews, Cyber Security Manager at the Australian Communications and Media Authority (ACMA) provides an overview of the Australian Internet Security Initiative. Finally, Robert Schischka of nic.at, the Registry for the Austrian country code Top-Level Domain (ccTLD), offers an international perspective on DNSSEC.

In addition, we're delighted to have the contribution of a number of our .au Registrars in this edition, to give their predictions for the year ahead in .au and the domain name industry abroad. We look forward to continuing this inclusion of Registrars in future editions.

Finally, February also marks the release of AusRegistry's newly refurbished website. The website will provide a smoother, intuitive source of information on the .au namespace for the Australian Internet community at large. Please visit the website (www.ausregistry.com.au) and let us know what you think.

It is my pleasure to present the sixth edition of *Behind the Dot: State of the .au Domain*. As always, we welcome your feedback and input on the magazine and thank you for reading.

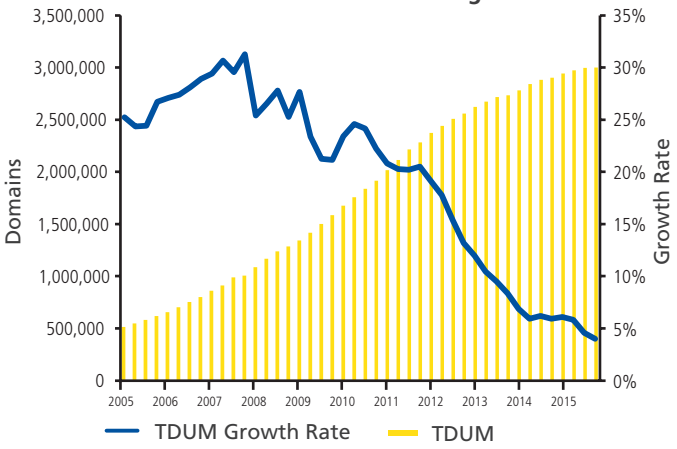
Adrian Kinderis
CEO, AusRegistry

Under the microscope

The .au namespace grew marginally in the last quarter, as expected. This is caused by an imbalance between creations and drops, as new registrations traditionally slow with the onset of the holidays, while drops remain steady until the New Year.

This imbalance occurs due to the natural registration and drop cycle. The 30-day grace period means high creates are not mirrored in high drops exactly two years later, but are instead mirrored two years and a number of weeks later. Thus the low creates experienced in December will likely not be reflected in low drops until January two years later.

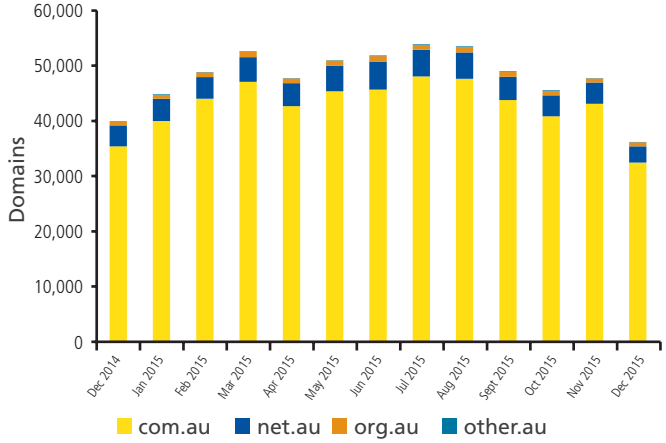
.au Domains Under Management



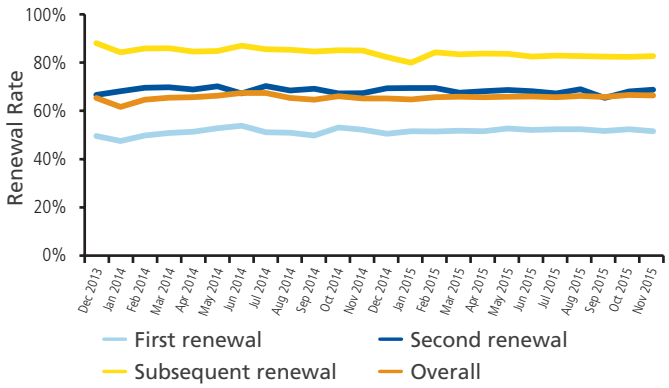
Quarterly and annualised growth remains positive with com.au growing by over four percent year-on-year and org.au growing by nearly three percent. Not all 2LD zones expanded however - net.au contracted for the fifth consecutive quarter and the small namespaces of id.au and asn.au struggled similarly. Overall, .au domains under management in the open zones rose to a total of 3,000,766 as of 31st December 2015.

These weaker growth figures are due to lower registrations – December 2015 had the lowest number of new creates since December 2009, when the namespace was just embracing policy updates that opened up commercial opportunities.

.au Monthly Creates



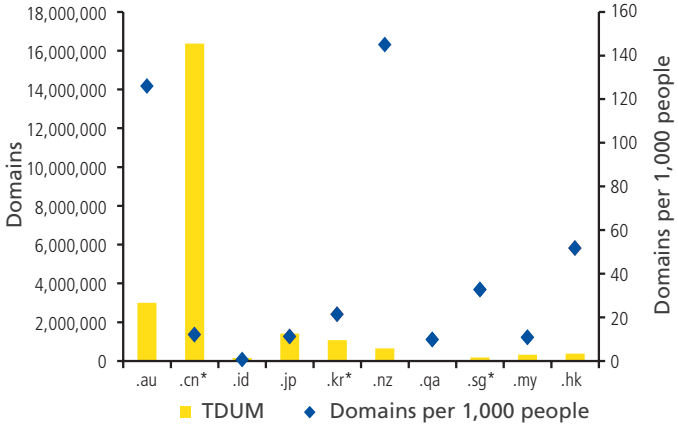
Renewal Rates by Domain Age



October 2015 was also relatively low, possibly reflecting the mature market and static policy conditions or as a result of new gTLDs entering the market. This trend will bear careful watching in the months and years to come.

Despite this, the namespace is fundamentally healthy with the renewal rate holding at over 66 percent and marginally higher than a year ago. This is being driven by an increasing proportion of solid, long-term domain names that have been held for four years or more and whose registrants remain content and committed to their .au names. The age of a domain remains the key indicator of propensity to renew.

Domain Numbers in the APTLD Region



** as at 30 November*

.au belongs to the APTLD, the organization for country code Top-Level domains in the Asia-Pacific. Comparing Australia to a selection of other countries in the region (chosen on the basis of data availability and to represent a range of APTLD country codes). In the December quarter, the major movements in the region came from .cn and .hk who both had over 30% growth – primarily from investors seeking new places to invest following the China stockmarket crash. Comparing .au to the country codes of our neighbours shows that Australia has a high per capita ownership rate and remains a significant ccTLD by volume.

.au research and surveys

Edition 5 of *Behind the Dot* featured a number of findings from the first .au zone file scans, conducted in June and August 2015. The .au zone file contains every domain registered in .au and reveals a large amount of information about domain name usage and website ownership.

Analysis of the .au zone file revealed 110 data elements, each of varying application to the Australian market. Many of the findings, when combined with Registry data and in isolation, provide important insights and guidelines for a top-performing website.

Of the 2,880,831 .au domains scanned (under com.au, net.au, org.au, id.au and asn.au), 1,878,767 or just over 65% returned a response of either 'Available' or 'Redirect' indicating that they pointed to a website or webpage. The remaining domains returned a 'Host not found' or 'Access denied' response.

AusRegistry will continue to report on the zone file findings of this and subsequent zone file analyses in future editions of *Behind the Dot*.

Incoming links

An incoming link (also referred to as a backlink or inbound link) is a hyperlink on a third-party web page that points to a web page on your website. The number of incoming links is an indication of the popularity or importance of that website or page and is one of the factors considered by Google to determine the PageRank of a webpage.

Only a small proportion of .au websites, 4.6%, had ten or more incoming links with the majority of websites, 63.6%, having none.

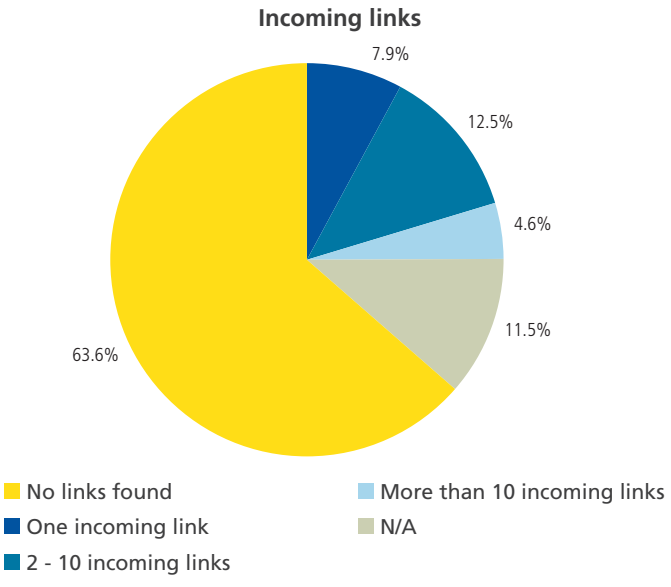


Chart 1: Incoming links. Total 1,878,767 .au domains (open 2LDs returning a 'Available' or 'Redirect' response)

Outgoing links

An outgoing (or external) link is a hyperlink that points to a destination outside the website. The number of outgoing links refers to the number of unique external links found on the website during indexation. If a link to www.example.com.au is found seven times on three different pages, it will be counted as one unique external link.

Nearly 60% of .au websites have between 2-10 outgoing links.

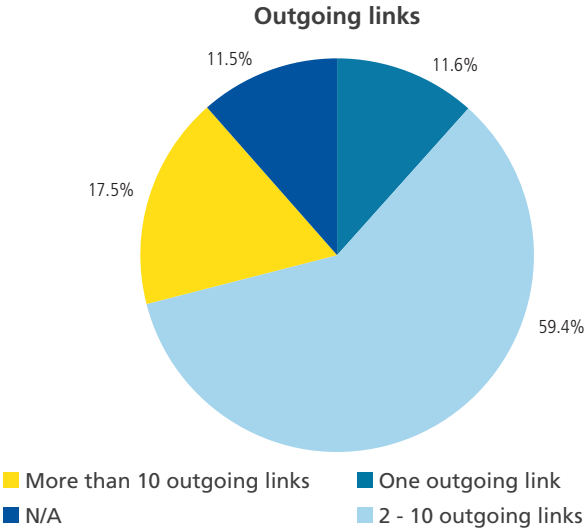


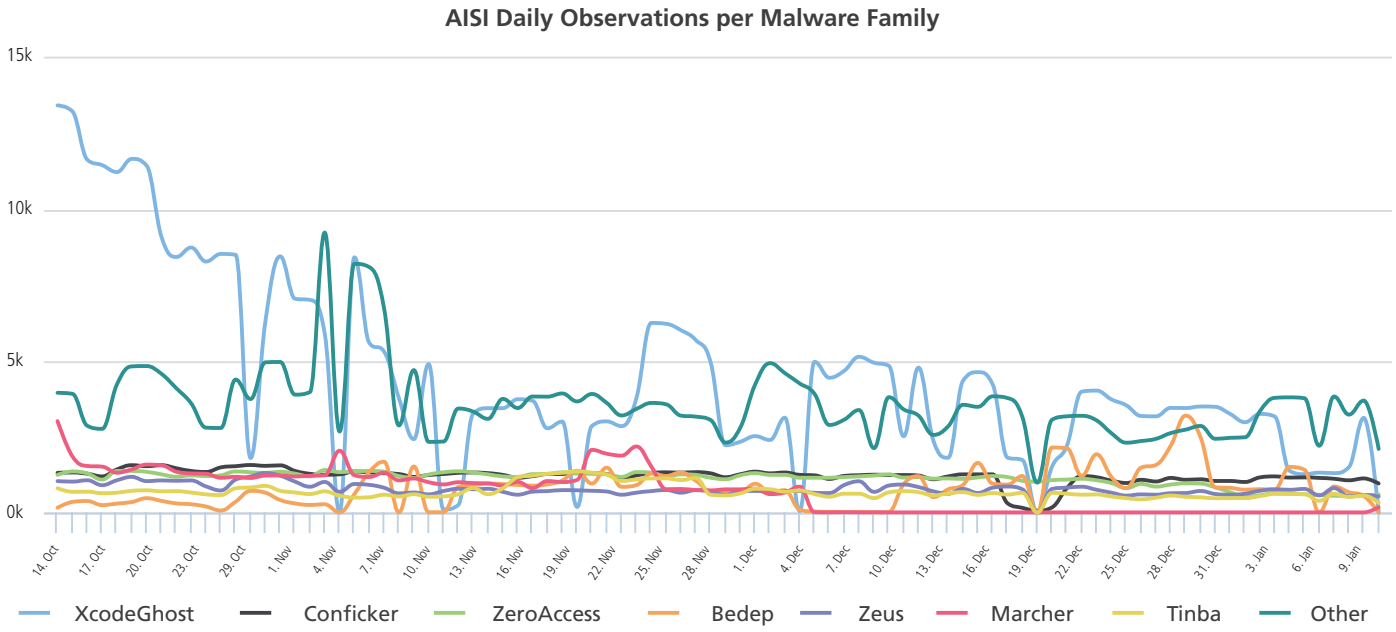
Chart 2: Outgoing links. Total 1,878,767 .au domains (open 2LDs returning a 'Available' or 'Redirect' response)

Conclusion

Quality incoming links from well ranked websites are seen by many SEO experts as a key objective to help achieve high search rankings. These external links are difficult to manipulate, thereby proving to be a strong leading indicator for search engines to determine the popularity and quality score of your website. Some time spent developing relationships and partnerships with trustworthy and popular websites may help you to outperform your business competitors.

AISI: keeping Australian Internet services healthy

By Bruce Matthews
Cyber Security Manager, Australian Communications and Media Authority



Source: Australian Communications and Media Authority. © Commonwealth of Australia (Australian Communications and Media Authority) 2014.

Have you ever wondered how vulnerable your internet-facing services—such as websites, routers and network accessible storage devices—are to being exploited or infiltrated? Or how many vulnerable Australian internet services there currently are? This article discusses an initiative run by the Australian Communications and Media Authority (ACMA) that processes data every minute of every day to report this information to Australian internet providers.

The ACMA has now operated the Australian Internet Security Initiative (AISI) for 10 years. For most of this period the focus of the AISI has been on identifying and reporting malware infected computing devices on Australian IP ranges, whereby daily reports identifying infected computing devices are sent each day to the 140+ participating Australian internet providers. Using the information contained in the reports, these providers can identify which of their customers are infected and give them advice to assist the removal of the infection.

The AISI is a voluntary program, so it is up to each internet provider to identify when, how and if they will contact their customers and what advice they will provide. A variety of approaches are adopted, as is described in a research report[1] (*The Australian Internet Security Initiative: Interviews with industry participants* – based on interviews with AISI participants) released by the ACMA in October 2015. It is encouraging to see there is strong support for the AISI, with participating providers—including all major ISPs—estimated to cover more than 95 per cent of Australian residential internet users.

In March 2015 the ACMA began reporting Australian internet services that are either 'vulnerable' to known malicious exploits or misconfigured so that the service can cause harm to other internet users. This added a preventative feature to the AISI, enabling action to be taken by the service owner before any harm has been caused.

The range and types of vulnerable services reported through the AISI continue to expand. Some of the types reported (such as POODLE and FREAK) are SSL services that, due to outdated configurations, are potentially open to 'man in the middle' attacks. The AISI is also currently reporting a large number of UDP (User Datagram Protocol) services configured in a manner that enables them to be inadvertent participants in Distributed Denial of Service (DDoS) attacks—known as 'DDoS amplifier' services. These misconfigured services are not a theoretical problem, as the ACMA has evidence that some of these services are being used in DDoS attacks.

Of perhaps even greater concern, the ACMA is also reporting a relatively small number of 'open' services –internet accessible database type services that either have no authentication or have a default setup without authentication. Such a setup obviously places any data they contain at risk to capture or manipulation by cybercriminals.

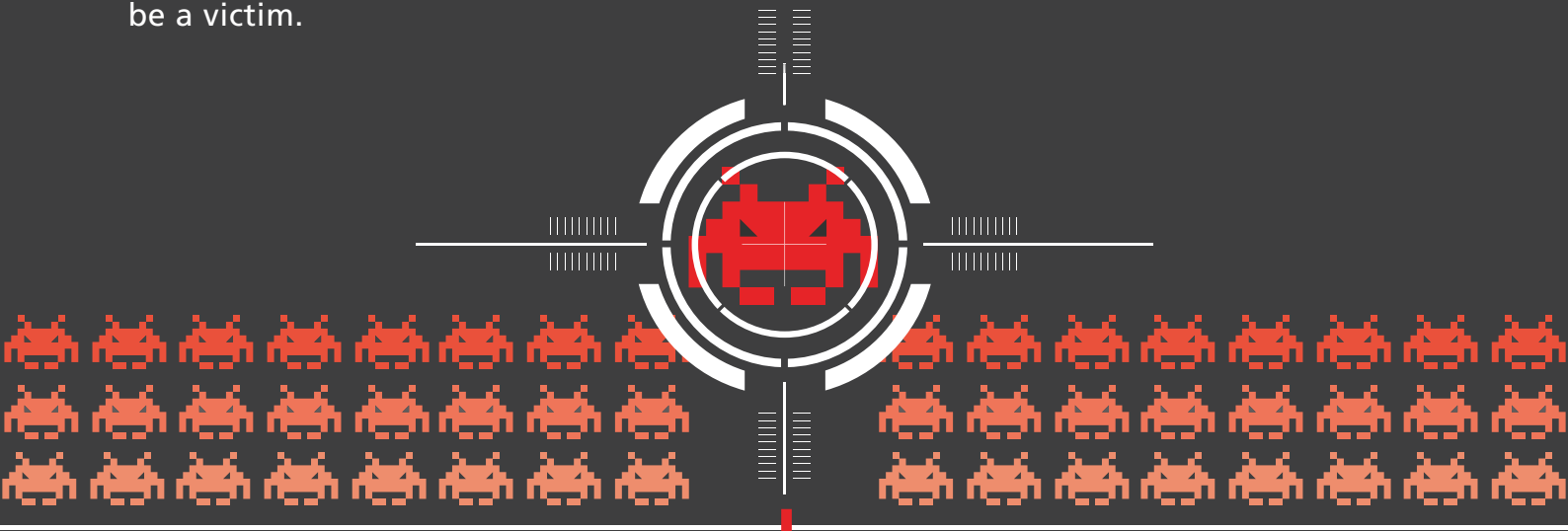
The ACMA considers there is considerable scope to make Australian internet services safer and less exploitable. Over the last three months approximately 300,000 vulnerable services per day have been reported through the AISI, compared with between 10-15,000 reports per day of AISI malware infections. Charts detailing trends with these reports are updated daily at www.acma.gov.au/aisi-stats. If you are interested in further information about the AISI, please send an email to aisi@acma.gov.au.

This feature article was authored exclusively for Behind the Dot by the ACMA's Cyber Security Manager, Bruce Matthews.

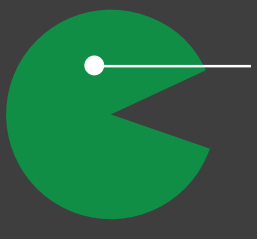
1 Australian Communications and Media Authority 2015, The AISI: interviews with industry. Available from: < http://acma.gov.au/theACMA/Newsroom/Newsroom/Media-releases/the-aisi-interviews-with-industry >. [1 December 2015].

Stop the malware invasion!

Malware (malicious software) is used by online criminals to steal personal or financial information from your computer. But a whopping 49% of us* don't believe we'll ever be a victim.



We're on the front line



88%

of us give personal or financial info online

What we do online:

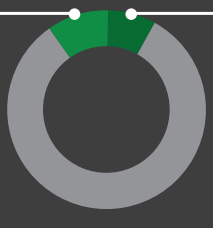
But we're not properly armed

18%

Nearly one-fifth of Aussie internet users don't have sufficient protective software on their home computer

10%

1.46 million users have none at all



8%

1.12 million users don't regularly update their software

So, fortify your defences

It's easy to secure your computer and protect yourself from malware:

1. Install security software and update it regularly
2. Turn on automatic updates so all your software receives the latest fixes
3. Set strong passwords

The ACMA operates the Australian Internet Security Initiative (AISI) to help alert internet service providers about malware and viruses on their customers' computers.

Source: ACMA, Malware and harmful software—Consumer views on software threats and use of protections, September 2013.

*Adult Australians who use the internet for personal purposes.

A DDOS ATTACK JUST ATE $16M IN REVENUE. ALONG WITH HIS ANNUAL BONUS.

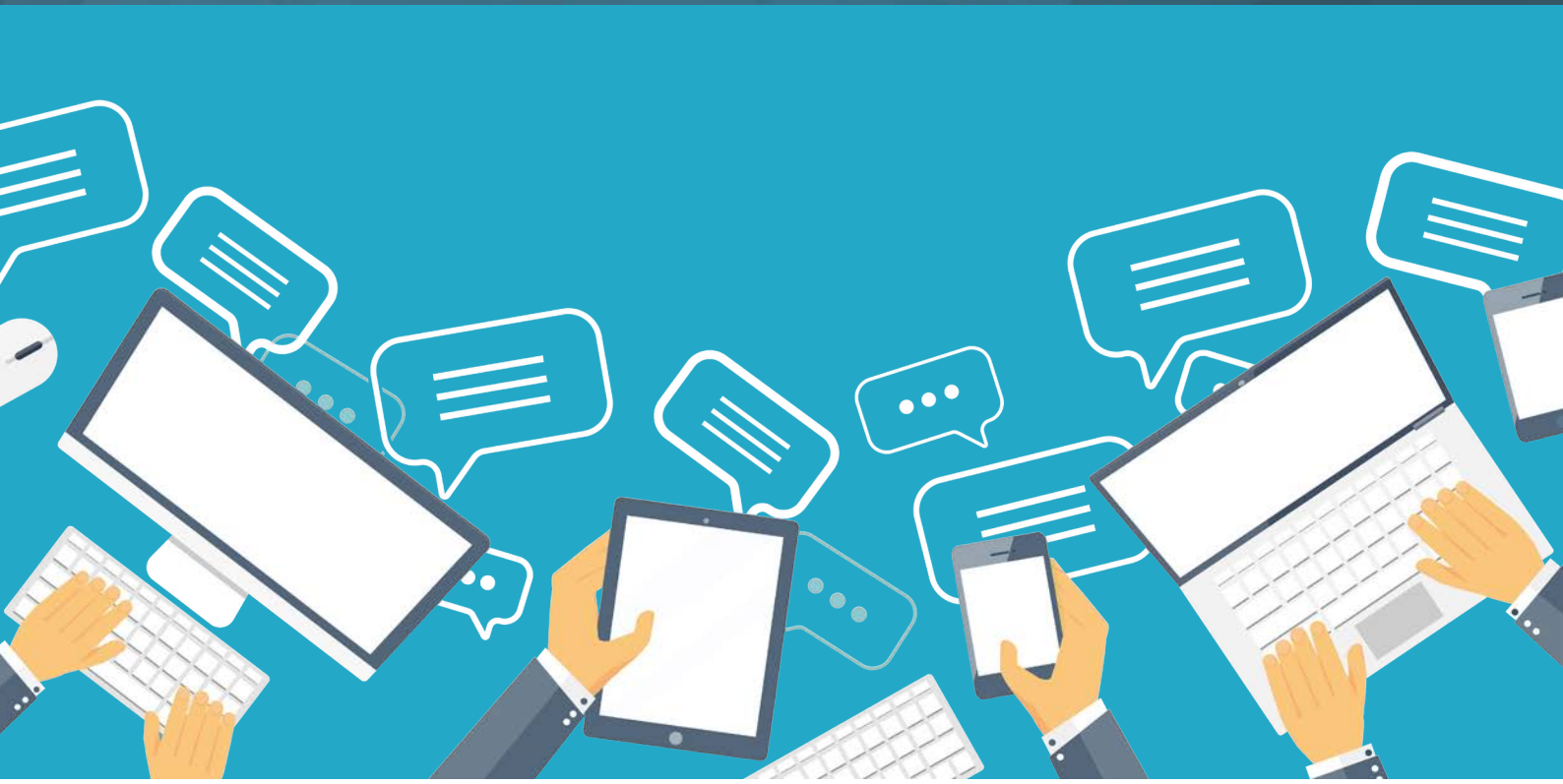
ALI CARTER // CIO

DDoS attacks are costly. Revenues tank. Your brand gets smacked. Sometimes malware slips in. Neustar can help. With flexible solutions for DDoS mitigation, we'll deliver exactly the defense you need from the threats you face. **Learn more at www.neustar.biz/services/ddos-protection.**

neustar

Global domain hijacking incidents a menace to major brands

By **Michael Korjen**
Public Relations Manager, AusRegistry



More than 20 high profile security breaches related to the hijacking of domain names owned by major brands have been publically reported over the past three years, despite the availability of cost-effective security measures to counter such attacks.

The increasing risk posed by domain name infiltration has claimed a number of high profile victims. For example, visitors to Google's Vietnam website were directed to another page in February this year. A Google spokesperson said the company was in contact with the organisation responsible for managing their Vietnam domain names to resolve the issue.[1]

In response, increased security measures have been introduced in Australia by AusRegistry – and abroad by other Registry Operators – to combat the scourge of these hijacking incidents.

Despite this, websites continue to be taken offline. Many unsuspecting businesses and domain name owners remain unaware of the threat and the need for increased security measures on their domain name assets.

What is domain name hijacking?

When it comes to cyber attacks, it's increasingly common for hackers to utilise evermore devious social engineering and phishing tactics in order to inflict maximum damage on their targets. In the case of domain name hijacking incidents, this is especially true.

Domain name hijacking occurs when a hacker gains unauthorised access to a registrant's domain name administration details via their retail provider, referred to as the Registrar.

While many might envisage this type of attack being perpetrated by a highly skillful coder who is unmatched in their technical prowess, more often than not these attacks are committed by someone who impersonates their way around human-based security measures.

When this occurs, a hacker is able to access nameserver delegation information which can be maliciously changed to redirect all visitors from a legitimate website to a fraudulent website.

The end result of this can be devastating for a business, significantly disrupting operations and damaging the brands' reputation.

Recent cases

While any unsecured domain name can be a victim of domain name hijacking, hackers have predominantly focused their attacks on high profile major brands.

Attacks in the United States, Ireland, Malaysia, the Netherlands and other countries around the world have affected the websites of the world's largest brands.

How can you protect yourself?

While a rare occurrence, hackers can attempt to hijack websites by infiltrating Registrar servers or by fraudulently posing as an authorised employee of a business. While Registrars already have measures in place to counter this

1 International Business Times, Google Vietnam domain name briefly hacked and hijacked by Lizard Squad. Available from: < http://www.ibtimes.co.uk/google-vietnam-domain-name-briefly-hacked-hijacked-by-lizard-squad-1489293 >. [10 December 2015].

type of threat, the increasing number of global incidents demonstrate that another level of protection is warranted for high profile targets.

In response to this increasing threat, AusRegistry launched a security measure in 2014 called .auLOCKDOWN, which allows .au domain name owners to lock their domain name records and prevent unauthorised changes.

It also stops mistakes from occurring within an organisation, where domain name records are accidentally updated by employees. This last point is perhaps the most frequent and likely incident to occur. Although innocent in origin, the impact of human error can be just as significant and damaging as actions with a malicious origin.

Peace of mind

In many ways, placing an emphasis on security is comparable to the notion of purchasing travel insurance when holidaying overseas. You may never have a need for it, but you don't want to be caught without it.

In a similar manner, the cost and effort of applying enhanced security measures to your domain name pales in comparison to the financial and reputational costs involved in falling victim to a hijacking incident.

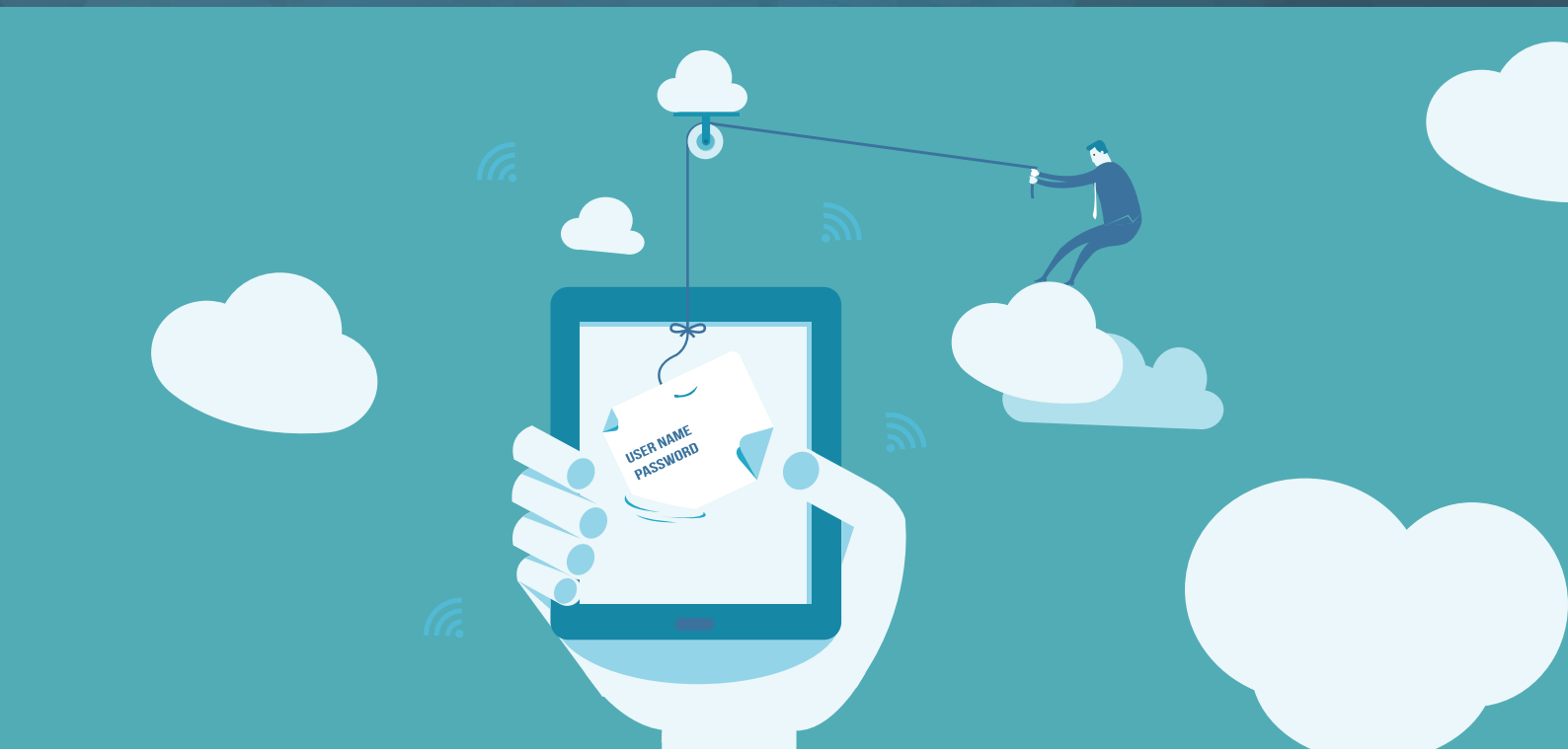
The important rule of thumb in situations like this is: if you can't afford enhanced security, then you can't afford to be online.

5 tips to prevent domain name hijacks

1. Ensure all employees in your business are security conscious and aware of tactics like phishing which are used by cyber criminals to access confidential information.
2. Introduce an Information Security Management Framework (ISMF) and make sure your domain names are included.
3. Employ best practice password management for your Registrar account. This includes using a password manager, enacting two-factor authentication (where possible) and using complex passwords that are at least 8 characters long and include passphrases.
4. Keep domain name records up to date. Many domain names have contact details where the contact person has left the organisation.
5. Ask your Registrar questions about security and how they can help you secure your domain names.

Protect your domain from cyber threats

By **Alison Coffa**
Marketing Communications Coordinator, AusRegistry



Imagine this; you operate an online business and you receive an email purporting to be from your domain name Registrar. It states that your domain name has been suspended following a breach of policy and several attempts to contact you for a response.

The email directs you towards a downloadable list of complaints against your domain, which you were encouraged to access in order to begin the process of reclaiming your domain name.

Unfortunately, the email is actually part of a sophisticated global domain name scam, which mined publically available data about your registration for your contact information in order to deceive you into downloading malware.

This situation is not uncommon. In fact, this exact scam was carried out on domain name Registrants across Australia and around the world in October 2015. The Australian Competition & Consumer Commission (ACCC) reports that in the month of October alone, 'false billing' scams such as this cost Australians over $66,000, or as high as $127,000 in August 2015 (*'False billing'*, ACCC Scamwatch website[1]) – and this is just the cases that were reported. In many cases, victims are too embarrassed to report the scam or feel that there is nothing that could be done in response.

As technologies develop and more data becomes accessible, ensuring your digital assets are secure is a vital step to protecting yourself online and offline.

How domain name scams work

Domain name scams are mostly delivered by email, and encourage consumers to renew their domain name, sell it, list or protect it with a certain service, or buy a similar domain in another namespace (ie. com.au holders may be encouraged to purchase the matching .com).

For example, the 'Chinese domain name scam' is a commonly recognised scenario in which domain name Registrants are contacted by a fraudulent Registrar in China, offering the opportunity to register their domain name under .cn (the Chinese county code Top-Level Domain) for a large fee, often under a highly-pressured time restriction.

The aim is generally to trick consumers into paying large amounts of money, downloading malware or sharing personal information that can be used for fraudulent activities. This can be done by instructing the consumer to respond with information, pay money to rectify the situation or open an insecure link or attachment that contains malware or otherwise opens their computer to outside access.

As in the example above, some scams use a technique known as WHOIS mining to crawl the data publically available in .au WHOIS records. For example, the name, company, email address and associated Registrar of every .au Registrant is available online for anyone to look up.

By merging WHOIS data with the fraudulent message, scammers are able to personalise the email and make it appear to have been written to the recipient individually from their Registrar. These details all contribute to making the message more believable and tricking more consumers into following its instructions.

1 False billing', ACCC Scamwatch <https://www.scamwatch.gov.au/types-of-scams/buying-or-selling/false-billing>

Consumer awareness and customer vigilance is key to addressing these threats beyond what the technology can control.

While AusRegistry has taken steps at the Registry level to place protections on WHOIS data, such as placing a hard-coded limit in WHOIS on the number of lookups that can be conducted in one attempt and placing a CAPTCHA verification tool requiring users to type a series of letters from a scrambled image to prevent automated searches, there is only so much the current technology and policies surrounding .au will allow.

Another potential measure is WHOIS Privacy. It is a technology that can be implemented by the AusRegistry to obscure Registrant information, while still maintaining eligibility data to meet compliance requirements for auDA.

Although WHOIS privacy is not currently supported by .au domain names, it was recently discussed at the 2015 auDA Names Panel and is being considered.

Consumer awareness and customer vigilance is key to addressing these threats beyond what the technology can control.

Vigilance: from industry to individual

Security threats that target individual domain name registrants are not new. Scammers exploit weaknesses such as decreased technological knowledge or consumer confusion and often prey on the most vulnerable for their attacks.

For example, the ACCC explains that while scams target a variety of people, consumers such as the elderly are seen as an easy target due to a relative lack of experience with technology and a sense of 'information overload'. Similarly, the sometimes overwhelming task of running a small business can mean many owners fall for scams simply because they are too busy to notice the warning signs.

While online security is a threat that the industry as a whole recognises and is taking steps to address, there is currently no technology that can prevent scams such as these from taking place. They target human error and as such, can only be combatted through consumer awareness and vigilance.

Recognising the signs of fraudulent activity and ensuring you have a firm grasp on the details of your domain name registration is pivotal to protecting your website, your business and your identity online.

5 tips for recognising scams

There are many resources available with information and advice for recognising fraudulent activity online and protecting yourself and your business from scams targeting domain name owners.

1. Keep a record of your domain name expiry date and make sure to renew it when the time comes. If you fail to renew your .au domain name, it will become available for registration on a first come, first served basis and you do not have any automatic rights to get it back.

   (Being aware of these details makes you less vulnerable to threats aiming to confuse you or force you to meet a false deadline.)

   Source: auDA - 'Regarding domain name security, domain name passwords, domain name data'

2. Be cautious of requests to provide material to prove you would be the rightful user of a domain name – a scammer could steal this and put it to fraudulent use.

   Source: ACCC Scamwatch - 'Think carefully about unsolicited offers to register domain names overseas'

3. Use your common sense and be aware—no reputable ISP or email service supplier will ever ask you to send your username and password via email.

   Source: ACMA - 'Don't 'reply to' phishing emails'

4. If you receive unsolicited emails or letters offering investment opportunities, items for sale, or requests to 'connect' - be alert to things like spelling and grammar mistakes and inconsistencies in their stories.

   Source: ACCC Scamwatch - 'Advice for the elderly'

5. If you notice a supplier's usual bank account details have changed, call them to confirm.

   Source: ACCC - 'Protect your small business'

Protecting Australia's Internet with DNSSEC

By David Goldstein
Publisher, Goldstein Report and Editor, Domain Pulse

Internet security is important. Criminals around the world are constantly trying to break down doors to access personal information, cripple critical infrastructure and steal business and government information. To highlight the risk, in early December it was revealed the Bureau of Meteorology had suffered a cyber-attack while ABC News reported "ventilators, patient-controlled analgesia pumps and MRI machines were all vulnerable to cyber-attacks."

The issue of security online is only going to become more important, particularly as the Internet of Things grows with homes becoming automated, appliances smarter and more and more connected devices. Out of the home, health and fitness devices, personal devices and cars are all becoming more prevalent. The Federal Trade Commission noted in January 2015 there were "over 25 billion connected devices in use worldwide, with that number set to rise significantly as consumer goods companies, auto manufacturers, healthcare providers and other businesses continue to invest in connected devices."[1]

When the domain name system was developed, as the European Network and Information Security Agency (ENISA) explains "its design was focused on data availability and did not address any resilience or security issues."[2]

And the security of the domain name system is of the utmost importance. Imagine a cyber-attack on .au that brought it down. All electronic commerce for every company using a .au domain name would collapse. Emails couldn't be sent or received. Whilst this is a worst case scenario and is highly unlikely to happen – largely due to the work undertaken by auDA, AusRegistry and the .au community – there is still the potential for disastrous cyber-attacks on both the individual and enterprise.

One of the ways in which the .au community is working to enhance security and trust is through the implementation of *Domain Name System Security Extensions* (DNSSEC).

DNSSEC is one very important tool that was developed to address "critical security shortcomings of DNS by defining a process whereby a suitably configured resolver can verify the authenticity and integrity of query results from a signed zone. DNSSEC uses public key cryptography and digital signatures to enable a security-aware validating resolver" to authenticate the data received by the user and ensuring it could only have originated from the requested source, verifying the integrity of the data.[3]

When DNSSEC is implemented, the Internet becomes safer for all users. When an Internet user visits a website, for example their bank, they can be sure they are visiting a legitimate website and not one that criminals have set up. It also means that for a business, the chances of their domain records being successfully modified by an unauthorised party is significantly reduced. Having criminals take control of a website can have severe repercussions for both brand management and sales losses.

Within the .au namespace, DNSSEC was deployed in 2014, first with an experimental test period and now fully deployed.

What is DNSSEC?

DNSSEC was developed by the Internet Engineering Task Force (IETF) after vulnerabilities were detected in the DNS. It uses digital signatures for validating the domain name requested, ensuring the DNS content cannot be modified from its source without being detected. "Once fully deployed," ICANN notes on its DNSSEC resource page, "DNSSEC will stop the attacker's ability to redirect users using the DNS. Of particular interest to ISPs and enterprises, DNSSEC will prevent en masse redirection at the DNS resolver (also known as cache poisoning)."[4]

"DNSSEC works by digitally signing each DNS record so that any tampering of that record can be detected. The digital signatures, and keys used to create them, are distributed just like any other records in the DNS making DNSSEC backward compatible. Keys in each layer in the DNS hierarchy are signed by keys from the preceding layer which effectively vouches for them just like domain names are delegated from one layer to the next. This 'chain of trust' is used to validate the digital signatures accompanying DNSSEC protected records to detect changes."

The vulnerabilities that DNSSEC helps protect against are commonly called "spoofing attacks". Spoofing attacks

1 Federal Trade Commission, FTC Report on Internet of Things Urges Companies to Adopt Best Practices to Address Consumer Privacy and Security Risks - < https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices >.

2 ENISA, Good Practices Guide for Deploying DNSSEC - < https://www.enisa.europa.eu/activities/Resilience-and-CIIP/networks-and-services-resilience/dnssec/gpgdnssec >.

3 ENISA, Good practices guide for deploying DNSSEC, Anne-Marie Eklund Lowinder et al - < https://www.enisa.europa.eu/activities/Resilience-and-CIIP/networks-and-services-resilience/dnssec/gpgdnssec >.

4 ICANN DNSSEC resource page - < http://dnssec-deployment.icann.org/en/dnssec/zzz >.

are where an attacker fools a cache into accepting false DNS data. Additionally, DNSEC also helps prevent man-in-the-middle attacks.

What do Internet users need to do?

The short answer is nothing. The work is done by registries such as AusRegistry and policy and regulatory bodies such as auDA, Internet Service Providers and e-commerce and website providers. For the Internet user, when browsing websites there will be no discernible difference unless there is a verification problem. In this case, they will receive a message indicating the site does not exist through a '404: not found' error message. For the more tech savvy users, some web browsers have add-ons that can be installed that will tell you if the domain name for the website has been enabled.

So who should implement DNSSEC?

Admittedly there is a cost to implementing DNSSEC that business has to factor in. That being said, any organisation that collects data online such as login and registration information, financial data, classified data or deals in intellectual property, as well as the most popular websites, should consider DNSSEC a priority.

However DNSSEC cannot be fully implemented until infrastructure providers support it. The next level in the DNSSEC hierarchy requires Internet Service Providers, webhosts and software developers to support DNSSEC so signatures can be validated by the Internet user and at the website being requested. As more and more domains are signed with DNSSEC, its value increases.

An impediment to implementing DNSSEC is that because consumers are generally not aware of its importance, there is little consumer demand for it.

Around the world, as of June 2015 there were 67 ccTLDs that had DNSSEC operational, including .au as well as the ccTLDs for most developed countries according to statistics published by the Internet Society. There were another 34 that deployed DNSSEC in the root, but it had not yet become operational; four had partially deployed DNSSEC; 11 had announced they are deploying it and nine were in an experimental phase.[5]

To date, the implementation of DNSSEC has been lower than expected. There are a number of reasons for this. Public knowledge of and demand for the security protocol is low.

But there are ways to encourage its implementation. One example was a campaign by the .se registry. The Swedish country code Top-Level Domain (ccTLD) was the first TLD to be DNSSEC-enabled in October 2005. By early 2011, there were 4,299 DNSSEC-signed .se domains. The registry implemented a campaign offering a five percent discount on domain names that were signed. As a result, 160,000 domains were signed in December 2011 alone taking the total at year-end to 171,650.

It wasn't until 2011 that .com, by far the largest of all TLDs, was signed.

For new gTLDs, it is a requirement that they support DNSSEC and hence be DNSSEC-enabled when they go live. But just requiring a TLD to be DNSSEC-enabled does not mean every domain name under it will be. The various registries set policies to dictate how this is to be implemented, from making it compulsory to actively encouraging it.

In December 2015, of the 10.4 million domain names registered across the more than 800 new gTLDs that were delegated, there were only 92,000 domains that are signed with DNSSEC, or less than one percent of all domains registered, according to statistics provided by nTLDstats.com.

Looking to the future, widespread adoption will take time, but it is essential. The widespread adoption of DNSSEC leads to improved security, which leads to improving user trust, in turn meaning internet users will be more willing to conduct business, particular e-commerce, online.

For those with websites, particularly those that collect personal information or provide e-commerce facilities, they should ask their registrar and webhost if they provide DNSSEC services. If they don't, ask why not. Don't sacrifice security for convenience.

5 Internet Society DNSSEC Deployment Maps - < http://www.internetsociety.org/deploy360/dnssec/maps/ >.

Responding to a cyber incident: CERT Australia

By David Goldstein
Publisher, Goldstein Report and Domain Pulse

CERT Australia is a key Australian Government department addressing cyber security issues. David Goldstein spoke to Dr Jason Smith, Technical Director at CERT Australia about CERT Australia's work, how serious the problem of cyber security is, what it costs and what businesses should do if they are the victim of a cyber incident.

DG: *What is the Computer Emergency Response Team and what do they do?*

JS: The national Computer Emergency Response Team (CERT Australia) is part of the Federal Attorney-General's Department and is the point of contact in Government for cyber security issues affecting major Australian businesses, including owners and operators of critical infrastructure and other systems of national interest.

We help protect Australian businesses from cyber incidents, building resilience and improving the cyber security posture of businesses and targeted, and exactly what information may have been extracted. It's very important to understand the root cause for the incident and to address any technical, procedural or personnel vulnerabilities that allowed the incident to occur. It's of the utmost importance to seek assurance that vulnerabilities have been adequately addressed before reconnecting systems to the internet.

If you find your cyber incident is accompanied by a ransom, which is often the case, we recommend not yielding to the demands or communicating with the malicious actor.

Businesses should also adopt a good security culture, such as using anti-virus programs across the network, regularly patching software and operating systems, requiring the use of complex passwords that must be changed regularly and promoting user education to inform staff of the risks.

DG: *What are the types of costs involved when a business has fallen victim to a cyber incident?*

JS: There are several types of 'costs' from a cyber incident, from damage to a business's brand and reputation to a loss of sales through websites going down, equipment damage, psychological impact on employees and compensation to customers.

Apart from the monetary cost, other costs vary depending on the incident and systems affected. A report by Experion in 2013 found 60 percent of small businesses went out of business within six months of a cyber security breach.

"If you find your cyber incident is accompanied by a ransom, which is often the case, we recommend not yielding to the demands or communicating with the malicious actor."

Dr Jason Smith, *Technical Director at CERT Australia*

DG: *In Australia, is there an estimate of how many businesses that have had their websites compromised by hackers and other criminals?*

JS: This is an issue that is increasingly affecting businesses across Australia. We have seen a surge of website compromises in the past year. It is now the most common type of cyber incident that CERT Australia responds to.

In 2014, we received 4,964 notifications of compromised websites. In 2015, this number more than doubled to 13,994. We have to acknowledge though, that our view of malicious activity is incomplete, these numbers only reflect what we have been notified of, not the totality of the threat.

So it's no longer a question of 'if' a business will experience a cyber incident, but 'when' and 'to what extent'. Any business that utilises computers, systems or devices connected to the internet is at risk and no industry sector is immune.

DG: *And what is the most common form of cyber incident suffered by businesses?*

JS: The most common cyber security incidents CERT Australia responds to are compromised websites, which mainly impact SMEs.

In the 2015 ACSC Cyber Security Survey: *Major Australian Businesses*, our partners (systems of national interest and critical infrastructure) indicated that ransomware was the most common and accounted for 72 percent of incidents experienced. This is a drastic increase – four times that of 2013. Ransomware also affected every sector that experienced a cyber security incident, demonstrating the indiscriminate targeting and the sophistication of this type of threat.

DG: *How can I tell if my website has become victim to some form of cyber incident?*

JS: You should regularly monitor your intrusion detection and/or prevention systems, user logs and server logs for suspicious behaviour or activity. You can also scan your website for malicious content using a free website scanning tool.

We regularly receive information on compromised Australian websites. And when we do, we quickly notify website owners by email.

DG: *What does CERT recommend businesses do to protect themselves online from cyber incidents?*

JS: Businesses should be prepared before an incident occurs. Cyber security should be a part of a business's risk management and resilience structures and planning, including developing and implementing business continuity and response plans that outline what steps needs to be taken to remediate the situation.

In general, we recommend patching applications and operating systems, limiting the number of users with administrative privileges, using multi-factor authentication for critical systems and using strong passwords and passphrases.

We also recommend that businesses consider the top 35 strategies for mitigating cyber intrusions released by the Australian Signals Directorate (see http://asd.gov.au/infosec/mitigationstrategies.htm). Additionally, staff awareness training can help protect your business.

Results from the 2015 *ACSC Cyber Security Survey: Major Australian Businesses* show that the top three incidents experienced by respondents were ransomware, malware and targeted malicious emails – all of which only require 'one click' for a malicious file to be successfully executed. We're finding cyber criminals are becoming increasingly sophisticated and socially engineered emails make it very difficult for the user to determine legitimacy.

It's important for businesses to create a culture of cyber security where awareness is raised and staff are regularly educated about security policies and practices, including knowing not to click on links or download attachments unless they are certain the email is legitimate.

7 top tips if your website gets hacked

1. Take the affected website offline for remediation
2. Change the password for access to the website using a known clean computer
3. Restore the website from a clean backup
4. Update the website with the latest Content Management System version and security updates
5. Install security plugins and harden the website to prevent further security compromises
6. Put your website back online and re-scan it
7. Use the Google search engine to perform a security review of your website: http://www.google.com/webmasters/hacked

Channel talk

'What are your market predictions for the .au namespace in 2016?'

Rod Keys – Managing Director, Information Brokers Pty Ltd
My market prediction for the .au namespace in 2016 includes the opening up of direct access to .au namespaces alongside com.au domains, and a move away from the mandatory two year registrations to more flexible renewal periods.

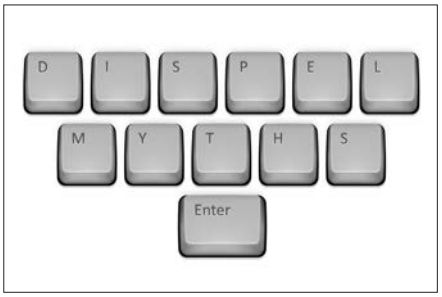
While only second level domains are currently available to users, adding the direct .au option will make it easier to register a name and, in my opinion, will pave the way for more unique, modern looking and memorable domain names in the process.

Meanwhile, a variable licence period for one to five years, allowing renewals at any time, would bring the namespace closer in line with other prominent Top-Level Domains.

It will afford Australian businesses, organisations and charities both a long-term option for future peace of mind and an opportunity to register a domain name for one-off events or other short-term requirements.

Gavin Collins – Chief Operations Officer, Crazy Domains
2016 promises to be an interesting year for the .au domain space. Growth has slowed over the past couple of years and whilst we don't anticipate any movement on .au registrations at the second level through the next 12 months, there is certainly a lot of work to be done within the space as it is.

Hundreds of thousands of small to medium businesses do not have a web presence and many more businesses are being set up daily, leaving a large market segment which should be engaging with .au. Typical 'barriers' to entry remain within this group, including cost, time and difficulty and we are only just scratching the surface in tackling these.



If we, as an industry, can dispel these myths it unlocks a significant portion of the market. Apart from growing the .au industry, this will lead to greater engagement, more positive sentiment and ultimately deliver value to the end user through having the best domain name and products for their Australian business.

Verity Meagher – Chief Marketing Officer, Melbourne IT
2016 will be a critical year for the .au namespace. The growing number of new gTLDs available has caused dilution of .au in the market, and there is ever increasing competition for .au from the myriad additional extensions available to new businesses getting online.

It will therefore be more important than ever to remind businesses of the value .au domains provide in prominently informing their customers that they are Australian. The .au namespace would benefit from being actively promoted to Australian businesses through a revival campaign to increase awareness. In addition, the .au namespace could expand its value proposition in the market by allowing shorter domains through direct .au registrations at the second level.

Angelo Giuffrida – CEO, VentraIP Australia & Synergy Wholesale
I believe that in 2016 there is going to be a small but noticeable contraction in the market due to two main driving factors.

Firstly, the new TLD market will begin to mature, stabilise and raise brand awareness, which will further erode the .au namespace and provide customers with a direct alternate for their domain names. As an example, the Republic of Indonesia recently chose to use the .travel extension as its official tourism website over .id, its own ccTLD.

Secondly, the domain names purchased as part of the largely successful net.au promotion in May 2014 will be up for renewal and I personally expect to see a 20 to 30 percent renewal rate on these domain names. That being said, I do believe the consumer confidence in .au and continued initiatives from AusRegistry, auDA and Registrars will assist in sheltering the .au namespace from the erosion rates other ccTLDs are seeing.

Want to contribute to the next 'Channel Talk' feature?

Reach out to us at behindthedot@ausregistry.com.au with your expression of interest or topic suggestion.

DNS & security

An international perspective: DNSSEC in Austria.

The Registry for the Austrian ccTLD, nic.at enabled DNSSEC in 2012, two years before .au. Like .au they took a cautious approach, learning from the experiences of other TLDs that enabled the security protocol. David Goldstein talks to Robert Schischka, Technical Manager at nic.at about their experiences.

DG: *nic.at enabled DNSSEC in 2012. What were nic.at's experiences in deployment?*

RS: As DNSSEC is a complex technology with a lot of potential pitfalls we decided to not be among the early adopters. When we decided to enable DNSSEC, we chose the established and stable implementation OpenDNSSec instead of writing our own code. We watched carefully the experiences of our peers and took a very conservative approach for deployment which went very smoothly without any real problems.

DG: *What has been the response of Registrars, Internet Service Providers and Registrants?*

RS: We have currently about 18 percent of our Registrars offering DNSSEC and around 20 percent have declared in a recent survey that they are planning to support DNSSEC within the next 12 months. However the rest don't have any plans in the near future.

DG: *How has nic.at encouraged Registrars, Internet Service Providers and Registrants to sign their domains with DNSSEC?*

RS: We see our role as a provider of a crucial core service of the Internet where stability is the paramount goal. It is important that a Registry supports this kind of technology in order to facilitate a uniform deployment and avoid solutions like DNSSEC Lookaside Validation (DLV) or alternate Root-scenarios. But we don't think it is our position – as a Registry – to promote the use of DNSSEC other than explaining the technology, giving presentations at numerous events and technically supporting Registrars and ISPs.

DNSSEC offers some security advantages but at the same time also introduces new ways to fail. Therefore we think in order to make positive use of this technology, it is really important to fully understand the impact of signing a zone. Some Registries pushed the growth of signed domains by offering financial benefits – which leads to a faster DNSSEC deployment but at the costs of domain holders ending up with signed domains without really requesting this service and with a complete lack of understanding of the consequences. For example, one of these is a much more difficult way to move from one ISP to another.

DG: *What differences have you noticed in .at since DNSSEC was deployed?*

RS: Nothing spectacular – of course the zone file has grown and we need to take care of key management processes – but overall this works quite well and we don't see any real differences.

DG: *Looking ahead, how do you envisage encouraging DNSSEC adoption and how can Registries such as nic.at help this?*

RS: Our perception is that the demand for DNSSEC is still very low. There have been some developments that have led to slight increases in DNSSEC demand. But for now the only technology that might help drive DNSSEC deployment is DANE (DNS-based Authentication of Named Entities), which requires DNSSEC, and is an enhancement for Internet security. This is especially so in the aftermath of the Snowden documents and all the initiatives around securing mail traffic and fixing the broken certifying authority infrastructure.

Note: *The 'Snowden documents' reference relates to a 2013 incident involving Edward Snowden revealing details of classified United States government surveillance programs. Read more at https://www.edwardsnowden.com*

Governance & policy

Implementing Information Security Standard (ISS) certification for .au Registrars, by Jo Lim, Chief Operations & Policy Officer, .au Domain Administration auDA.

auDA is responsible for regulatory oversight of the accredited Registrars and their resellers who provide .au domain name registration and management services to Registrants. At the end of 2015, there were 45 accredited Registrars and over 4,500 resellers operating in the .au market.

This edition of *Behind the Dot* has a security theme, and the prevalence of hacking incidents and cybersecurity attacks in the domain name industry, here and overseas, has been highlighted throughout the report.

Recognising the need to take action, and with full endorsement by the industry, auDA implemented a world-first Information Security Standard (ISS) for accredited Registrars (auDA ISS) in October 2013. All auDA accredited Registrars are required to undergo an independent audit to demonstrate their compliance with the ISS.

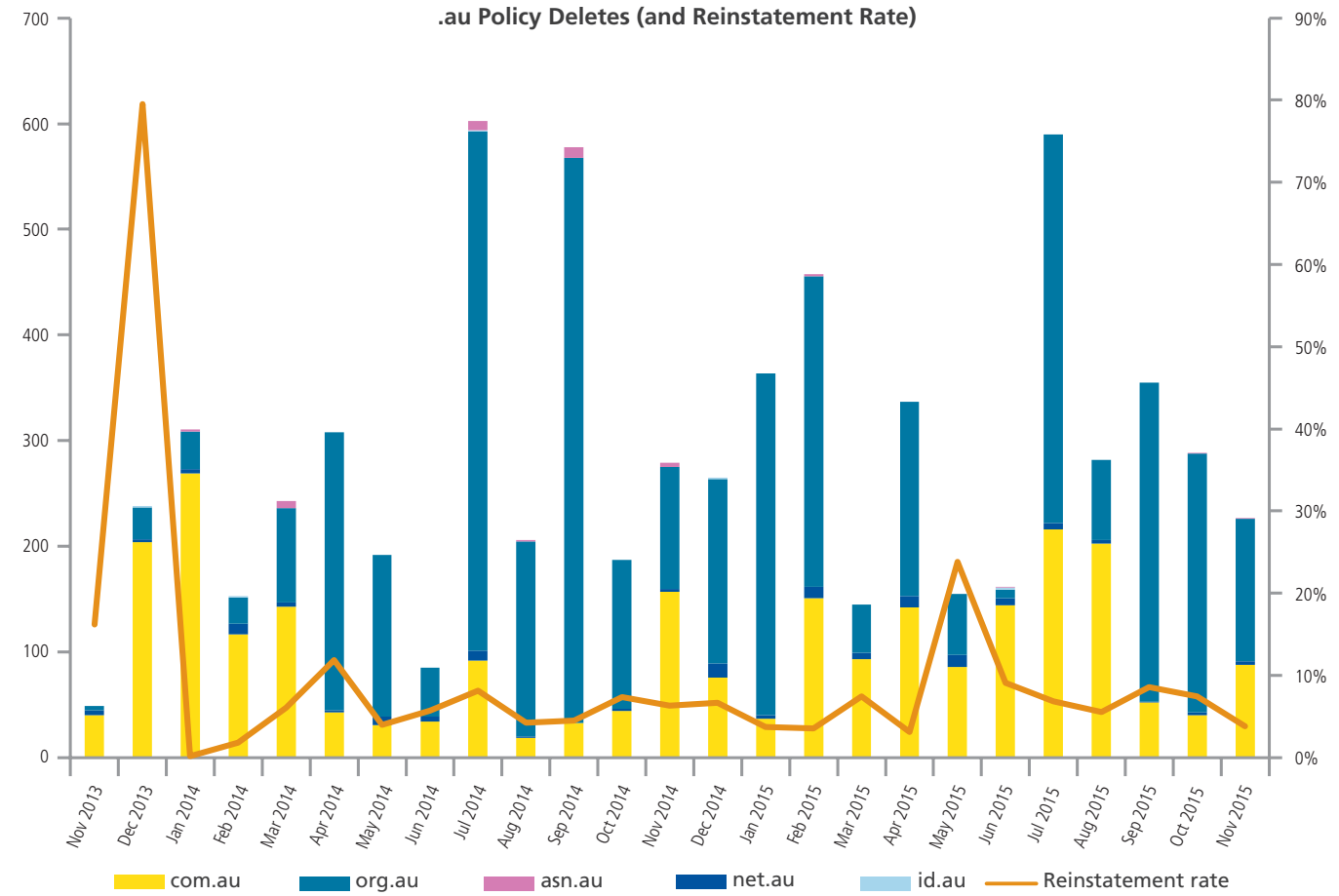
At the end of 2015, 18 auDA accredited Registrars had achieved full ISS certification. Cheaper Domains, Discount Domain Names, and Information Brokers were the first ones to reach this milestone in December 2013. All remaining Registrars are in the process of completing their ISS audit.

General feedback from Registrars who have gone through the ISS assessment process has been positive. These Registrars tell us that since completing the ISS assessment, they have developed a better understanding and documentation of their own business processes, systems and technology.

Given the auDA ISS was modelled on the well-known ISO 27001 and PCI DSS standards, a number of Registrars who already met these standards for information security management were able to complete their auDA ISS assessment with more efficiency and confidence. On the flipside, completing the ISS assessment has motivated some Registrars to take the next steps towards ISO 27001 and PCI DSS compliance – which serves to further enhance security practices in our industry.

We believe that the implementation of the auDA ISS has increased security mindfulness and built a greater capability across all auDA accredited registrars to respond to and remediate potential attacks, reinforcing instilled trust and confidence in .au.

See www.auda.org.au/membership for more information about the benefits of auDA membership and how to join.



Glossary

Abbreviations

2LD
Second Level Domain

ACMA
Australian Communications and Media Authority

AISI
Australian Internet Security Initiative

ANZIAs
Australia and New Zealand Internet Awards

auDA
.au Domain Administration

auIGF
Australian Internet Governance Forum

ccTLD
Country Code Top Level Domain

CERT Australia
Computer Emergency Response Team Australia

DDoS
Distributed Denial of Service

DNS
Domain Name System

DNSSEC
Domain Name System Security Extensions

gTLD
Generic Top level Domain

IANA
Internet Assigned Numbers Authority

ICANN
Internet Corporation for Assigned Names and Numbers

IDN
Internationalised Domain Name

TLD
Top-Level Domain

Definitions

Asia-Pacific Top Level Doman Association (APTLD)
APTLD is an organisation for ccTLD registries in Asia Pacific region. APTLD was originally established in 1998, and in 2003 legally established in Malaysia. APTLD works as the forum of information exchange regarding technological and operational issues of domain name registries in Asia Pacific region.

Australia and New Zealand Internet Awards (ANZIAs)
The ANZIAs are a collaboration between auDA and InternetNZ. An annual event celebrating the achievements of organisations, businesses and individuals who excel in delivering accessible, innovative, informative and secure resources to a diverse and wide community on the Internet.

.au Domain Administration (auDA)
The policy authority and industry self-regulatory body for the .au domain space.

Australian Internet Governance Forum (auIGF)
Developed by auDA, the auIGF provides a unique opportunity for all who use the Internet in Australia to share ideas and experiences, discuss Internet-related policy, identify issues and engage with each other in a multi-stakeholder forum.

.auLOCKDOWN
.auLOCKDOWN a security measure for .au domain names that provides an added level of security for domain name Registrants. Domain names are locked at the Registry level, and changes are only possible through direct communication between the Registrar authorised contact and the Registry, by following a strict authentication process.

AusRegistry
The Registry Operator for the open 2LDs (com.au, net.au, org.au, asn.au, and id.au); the community geographic 2LDs (act.au, nsw.au, nt.au, qld.au, sa.au, tas.au, vic.au and wa.au); and two closed 2LDs (edu.au and gov.au).

Country Code Top Level Domain (ccTLD)
A TLD that is used to represent a country or external territory. Some examples of ccTLDs are '.uk' for the United Kingdom, and '.au' for Australia.

DDoS Attack
A Distributed Denial of Service (DDoS) attack is an attempt to overwhelm and disable a computing resource, usually a website, or email server. Often executed by attackers who assemble botnets–networks of infected computers–to generate the traffic to paralyse a site. When the targeted server receives too many information requests, the main system crashes and the website becomes unavailable.

Domain Name/Domain
An identification string that defines a realm of administrative autonomy, authority, or control on the Internet. Domain names are formed by the rules and procedures of the DNS. Any name registered in the DNS is a domain name.

Domain Name System (DNS)
A hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates easily memorised domain names to the numerical Internet Protocol (IP) addresses needed for the purpose of locating computer services and devices worldwide.

Domain Name System Security Extensions (DNSSEC)
Domain Name System Security Extensions (DNSSEC) is a security extension that facilitates the digital signing of Internet communications, helping to ensure the integrity and authenticity of transmitted data.

Generic Top Level Domain (gTLD)/ Top Level Domain (TLD)
The name at the top of the DNS naming hierarchy. It appears in domain names as the string of letters following the last (right-most) 'dot', such as 'net' in 'www.example.net'. Most TLDs with three or more characters are referred to as generic TLDs, or gTLDs. They can be subdivided into two types; 'sponsored' TLDs (sTLDs) or 'unsponsored' (uTLDs).

Hold / Holding / Held (a domain name)
Hold and its derivatives are terms that have been used throughout this report to denote the act of licencing a domain name. As per auDA's Domain Name Eligibility and Allocation Policy Rules for the Open 2LDs (2012- 04) there are no proprietary rights in the Domain Name System (DNS). A registrant does not 'own' a domain name. Instead, the registrant 'holds' a licence to use a domain name, for a specified period of time and under certain terms and conditions. www.auda.org.au/policies/auda-2012-04

Internationalised Domain Name (IDN)
A domain name that includes characters from scripts other than the 26 letters of the Latin alphabet (a–z). An IDN can contain Latin letters with diacritical marks, or may consist of characters from non-Latin scripts.

Internet Assigned Numbers Authority (IANA)
A department of ICANN, which oversees global Internet Protocol (IP) address allocation, autonomous system number allocation, root zone management in the DNS, media types, and other IP-related symbols and numbers.

Internet Engineering Task Force (IETF)
IETF is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet

Internet Corporation for Assigned Names and Numbers (ICANN)
The global DNS administrator, formed in 1998, is a non-profit public-benefit corporation with global participants dedicated to keeping the Internet secure, stable and interoperable. It promotes competition and develops policy on the Internet's unique identifiers.

Registrant
An entity or individual that holds a domain name licence.

Registrar
An entity that registers domain names for Registrants and in the case of the .au ccTLD, is accredited by auDA.

Registry
The registry comprises of a database of domain names registered in each 2LD and a public WHOIS service for looking up the identity of the registrant of a domain name.

Reseller
An entity appointed by accredited Registrars to increase the retail channel of .au domain names.

Second Level Domain (2LD)
The alphanumeric string before the dot and the TLD. AusRegistry is the Registry Operator for the open 2LDs (asn.au, com.au, id.au, net.au and org.au); the community geographic 2LDs (act.au, nsw.au, nt.au, qld.au, sa.au,tas.au, vic.au and wa.au); and two closed 2LDs (edu.au and gov.au).

Total Domains Under Management (TDUM)
Total number of domain names registered in the namespace.

Zone
A portion of the namespace in the DNS for which administrative responsibility has been delegated.

Zone File
A file on a root server that contains domain name registration information. Zone files contain information necessary to resolve domain names to IP addresses and contains all information related to one domain.

Data References

Domain numbers in the APTLD region:

China - .cn
www1.cnnic.cn/IS/CNym/CNymtjxxcx

Indonesia - .id
https://www.pandi.id/content/statistik

Japan - .jp
jprs.co.jp/en/stat

Korea - .kr
isis.kisa.or.kr/eng

New Zealand - .nz
dnc.org.nz/content/2014-09_stats.html

Qatar - .qa
domains.qa/en

Singapore - .sg
www.nic.net.sg/page/registration-statistics

Malaysia - .my
www.mynic.my/en/statistics.php

Hong Kong - .hk
www.hkirc.hk/content.jsp?id=77#!/&in=/aboutHK/registration_statistics_hkirc.jsp

Protect your business from attack

Cybercrime is alive and well in today's online environment. Unauthorised access to your website could be disastrous for both your business and your clients. Protecting your .au domain name is a positive step towards peace of mind - Safeguard your .au domain today.

Visit www.aulockdown.com.au

Participating Registrars:

CSC DIGITAL BRAND SERVICES CORPORATION SERVICE COMPANY
DomainShield
instra CORPORATION
information brokers
NetNames One step ahead
MarkMonitor PART OF THOMSON REUTERS
MELBOURNE IT
netregistry
Safenames
uberglobal always ahead
ventraip australia