

WHY DO WE ★.au?

THE 2017 ANNUAL SURVEY RESULTS



WHY.au?

Why Aussies still choose .au
pg.10

PROTECTING .au

How auDA tackles unauthorised use
pg.16

DDoS ATTACKS

What's changed and what's to come
pg.14

FEMALE FOUNDER CHLOE BLATTMANN

RagTagd co-founder on success & startups
pg.12



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:



BtD

www.btdmagazine.com.au

Contributors

Publisher:
AusRegistry

Editor in Chief:
George Pongas

Managing Editor:
Maggie Whitnall

Creative Director:
Amy Prell

Contributors:
Alison Coffa
Adrian Kinderis
Richard McKenzie
Robin Schmitt
Maggie Whitnall

Data Analysis:
Penelope Green

Account Management and Circulation:
Courtney Fabian
Lucian Popaly

Subscription and advertising Enquiries:
email: behindthedot@ausregistry.com.au

Features

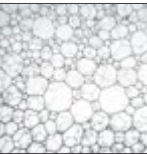


AusRegistry's 2017 .au survey 6
Learn more about Australians' views on the internet and .au domain names in our annual .au survey.



Why Australians still choose .au 10
.au still reigns supreme for Australian consumers, but what makes Aussies gravitate to these two letters when they operate online?

Departments



Under the microscope 9
A closer look at renewals and retention rate in .au and why this is an important measure for a mature namespace.



Governance & policy 16
Discover how auDA tackles the challenge of unauthorised business use – or UBUs – in .au domains.



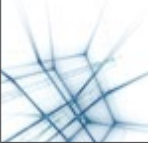
Women in technology 12
Behind the Dot chats to Aussie female founder and previous ELEVACAO program participant Chloe Blattmann of RagTagd.



Channel talk 17
News and views from the .au retail channel. This edition: What is one piece of advice you'd give someone who is starting an online business?



DNS & security 14
Distributed denial of service (DDoS) attacks continue to threaten businesses around the world. Learn how they've evolved in 2017 and what's next in solutions.



Glossary 18
Abbreviations and definitions of key terms.

30 September 2017
3,136,713
.au domain names



Foreword

Welcome to the 13th edition of Behind the Dot. This month, we're pleased to bring you the results of our annual .au survey. Now in its 31st year, .au is still the leading choice for Australian businesses, even with more Top-Level Domains than ever to choose from.

We surveyed more than 1,200 respondents across the country to understand what .au means to residents. Our 2017 wrap-up sheds light on why .au remains, by far, the extension of choice. We also delve into how Aussies are using the internet, what they're doing once they're online, and who holds a domain name.

Our Editor in Chief and Senior Director of Product Management, George Pongas also takes a closer look at why .au continues appealing to businesses, whether they're in the start-up phase or established names. The .au namespace conveys a connection to Australia, and businesses are leveraging it not only for their websites, but across other platforms, including ever-important social media. Using the extension builds a connection with Australian customers that other domain name extensions haven't been able to replicate.

Proving just how supportive our start-up community is, in this issue we chatted with Chloe Blattmann, the founder of RagTagd, an innovative young business that connects parents with their children's lost school items. Chloe attended a start-up program run by ELEVACO, whose founder Marisa Warren was featured in the last edition of our magazine. In just three weeks, Chloe honed her skills and made connections that have helped her not only successfully launch RagTagd, but see it expanding internationally. I think you'll find her story inspirational.

Finally, we take a look at what auDA is doing to combat the rise in unauthorised business use in .au domain name registrations. auDA has implemented a three-step approach to target websites preying on customers and so far, the strategy is working.

I'm pleased to present this issue of Behind the Dot. I hope you'll find the survey information useful. As always, we welcome your feedback. Thank you and enjoy this issue.

Adrian Kinderis
CEO, AusRegistry



WHY DO WE .au?

THE 2017 ANNUAL SURVEY RESULTS

By Maggie Whitnall – Senior Client Services Manager, AusRegistry

After 31 years in operation, it's fair to say that the .au namespace is part of the Australian fabric, firmly entrenched in our lives as we live in an ever-connected world. The essentialness of .au is unquestionable, as is the expectation for .au to perform in a stable, seamless, and secure manner.

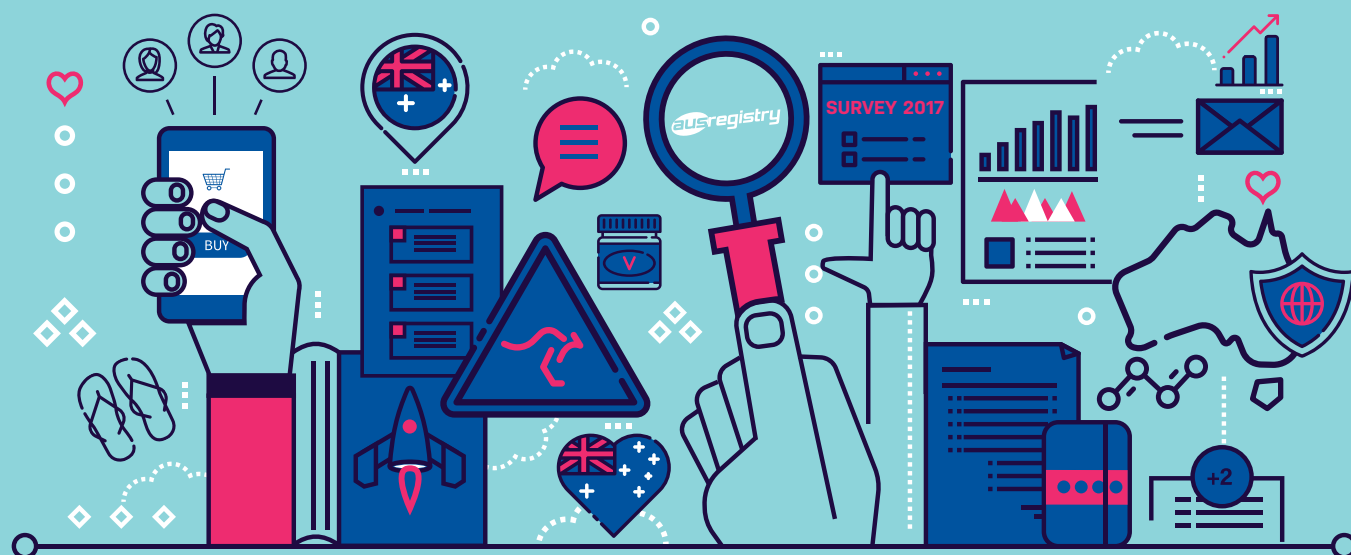
In order to gauge just how important .au is to Australians and whether it meets today's expectations, AusRegistry conducts an annual survey asking a broad mix of Australians what .au means to them.

So who did we speak to? Just over 1,200 respondents were called upon, aged 15 and above and an equal mix of men and women, living either regionally or in the capital cities.

Unsurprisingly, as with previous years, .au maintains its presence as the most trusted, most utilised domain extension amongst the range of domain name options available. It also maintains a strong brand recognition and connection to Australia.

The overall results of the survey shed a positive light on .au and its dominance in the marketplace. When asked what the .au domain name signifies, two-thirds of respondents answered, 'Australia'. The second most popular response was 'Australian businesses'. Results also indicate an uptick in a respondent's willingness to purchase .au domain names, greater domain ownership overall, and a level of trust in .au returning to above 60 per cent.

It would seem .au is continuing to 'do what it says on the tin' with positive indicators for the future.



Survey highlights

On behalf of AusRegistry, Research Now surveyed 1,201 Australians via their online survey panel in June 2017. The respondents were balanced by age, gender, and state to be representative of Australia as per the proportions in the 2011 census.

The 2017 survey was slightly abbreviated compared to 2016, focusing on internet users in Australia and did not delve into domain ownership as deeply as previous surveys. The findings from previous .au surveys can be found at btdmagazine.com.au

Who responded to our survey?

- 51% of respondents were female.
- 207 (17%) of respondents owned or ran businesses, the vast majority of which (152) employed fewer than 10 people.
- Australia was the most common birthplace (80%), followed by the United Kingdom, New Zealand, and India.



How do the respondents behave online?

- The most common reasons for using the internet are personal, such as email, shopping, and banking (92%). Social media was second and business use a distant third.
- Facebook remains the dominant social media service (75%), and free email the dominant email address type (80%).
- Navigating to content is all about search engines (69%) and social (58% for Facebook). Only 23% use domain names for this reason.
- .au was the most trusted extension (61%), followed by .com at 41%.

Who holds a domain name?

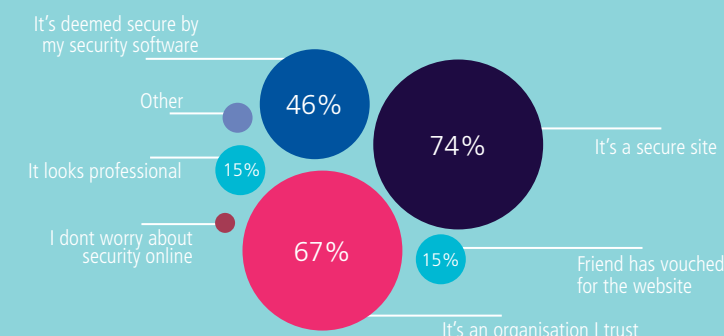
- 48% of domain holders were women, compared to 44% in 2013, our first year conducting the survey.
- Of those without a domain name, 18% wanted to expand their online presence.
- 34% of domain name holders were aware of new generic Top-Level Domains.
- When asked what the .au domain name meant, two thirds (67%) of respondents selected 'Represents Australia', with 'Australian Business' second at 30%.

27% of respondents held a **DOMAIN NAME** compared to **23% IN 2016**

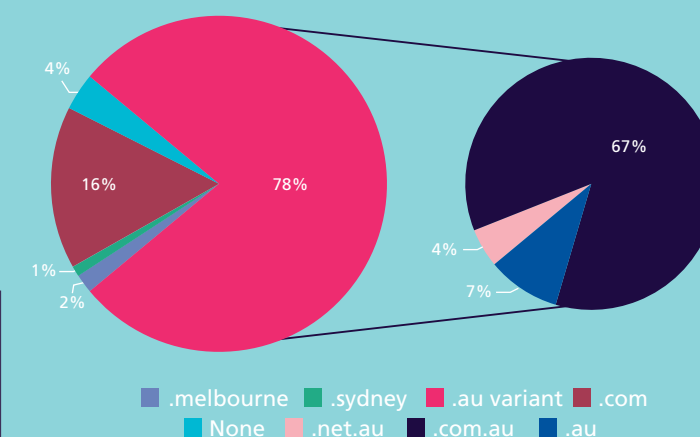
For those involved in research or requiring further data on the 2017 .au survey, please contact us at behindthedot@ausregistry.com.au for the complete set of survey tables summarising all survey results.

AusRegistry will continue running our yearly pulse check on the Australian public and share the data with the stakeholders that support, govern and provide services for the .au namespace. ■

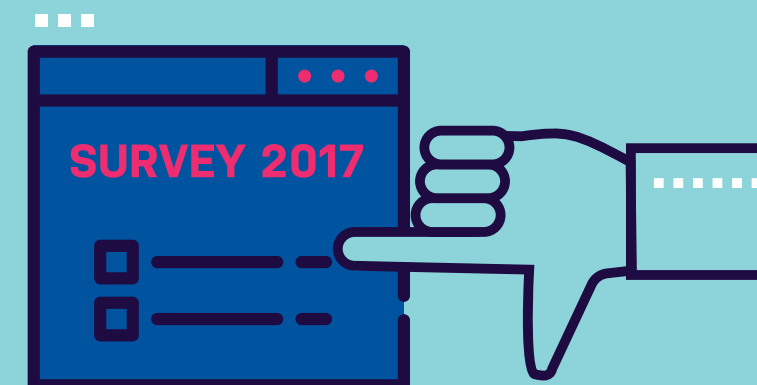
Respondents were security conscious, looking for secure sites (74%) and trusted organisations (67%) before entering personal information.



2017 – New Website Preferred Zone



If purchasing a new domain name, the preference was **com.au** by a long way at 67%. Trailing behind were **.com** (16%), **.au** (7%), and **.net.au** (4%)



MEMBER BENEFITS

AUSTRALIANS VIEW .au AS A TRUSTED SPACE ON THE INTERNET. IF YOU CARE ABOUT THE INTERNET IN AUSTRALIA, BECOME A MEMBER

auDA MEMBERSHIP BENEFITS:

- A VOICE IN THE FUTURE OF .au
- VOTE IN auDA BOARD ELECTIONS
- INVITATIONS TO SPECIAL EVENTS
- QUARTERLY MEMBERS' NEWSLETTER
- AND MORE...

www.auda.org.au/Membership



...
**BECOME AN
 auDA MEMBER
 TODAY & HAVE
 YOUR SAY**



Under the microscope

By **Penelope Green** – Senior Data Analyst, AusRegistry

Although most attention is usually given to the new namespace additions (New-adds), a critical indicator of the health and value of a namespace is its retention rate. As has been discussed in previous Behind the Dot issues, the growth of New-adds to the .au namespace has slowed in recent years as the market and internet has matured.

However, this larger and maturing namespace means more names are coming due for renewal each month. Tracking the renewal rate is essential in understanding the domain name market.

While the instant visual impact of the top chart is the lower renewal rate in May 2016 this is due to promotional names falling due – approximately 31,000 names registered at a deep discount in May 2014 – and renewing at a lower rate than typical. A deeper look reveals a distinct upward trend is also evident, particularly developing in 2017.

In 2014, the renewal rate fell to 62% but in 2017, over 66% of names that fell due are being renewed. This may appear lower than other namespaces but this is largely due to .au having fixed 2-year terms; only half of .au domains fall due each year. The annualized retention rate to 30 June 2017 was 84%.

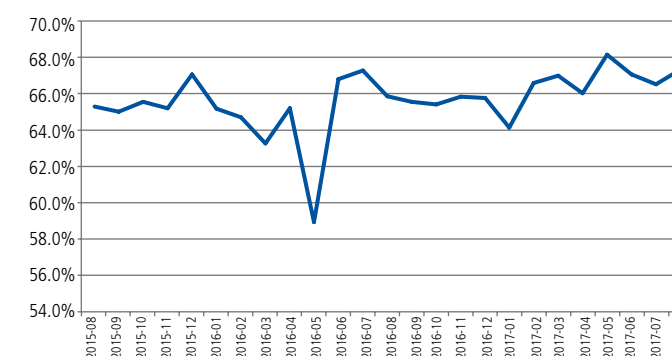
There are several driving factors to this increase. As discussed, the .au namespace is getting older. Just five years ago, in 2012, 48% of names were in their first 2-year term, with many of these falling due in 2014.

In 2017, over 60% of names are repeat customers of over 2-years standing. This aging of the namespace could reasonably be expected to contribute half of the increased retention.

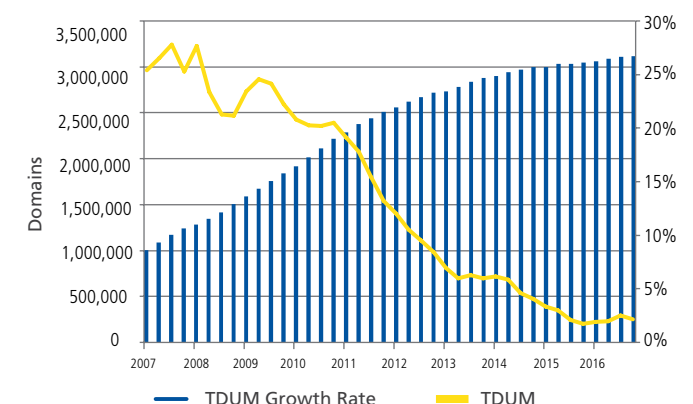
Better registrar client management and auto-renew changes may be responsible for some of the increases as well. Renewal rates within each age segment have increased, most notably in names six years and older. (While the first-time renewal rate has increased, once the promotional names from 2016 are removed, the significance of that increase is questionable.)

The driving force behind renewal rates is likely the value of domain names to registrants. Businesses and individuals who participate in the .au namespace clearly value it and wish to retain their .au domain name. ■

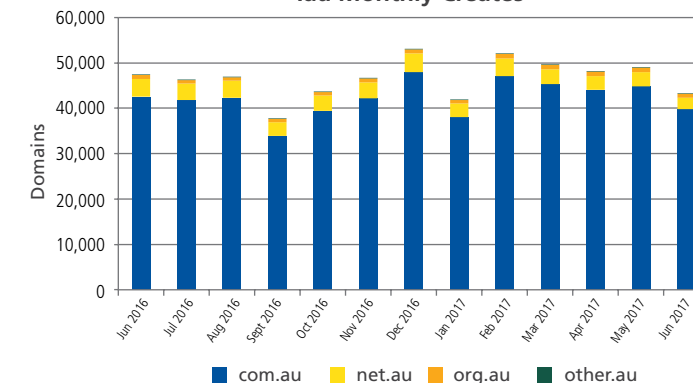
.au Domain Renewal Rate



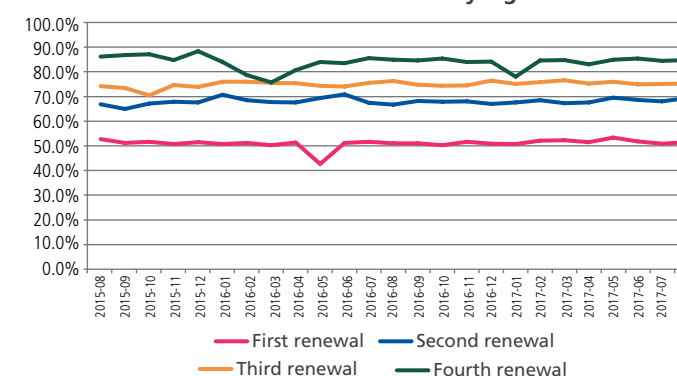
.au Domains Under Management



.au Monthly Creates



.au Renewal Rates by Age



WHY AUSTRALIANS STILL CHOOSE .au



By **George Pongas** – Senior Director Product Management, AusRegistry

One of the most important choices start-ups and new business owners will make is choosing a brand name and online identity. During brainstorming sessions all over the world, you can bet furious searching is taking place not only to come up with a memorable and catchy name, but also to verify a matching domain name is available.

But this is just one part of the decision-making process, because you must choose the Top-Level Domain (TLD) extension you want, too – these days, you can opt for a .com, .au, or one of the newer options, such as .sydney, .co, .club, or .xyz as your TLD.

So what's the best option? Well, each presents a different value proposition for a business. What we do know is in 2017, based on our Behind the Dot Annual Survey results, in Australia .au still reigns supreme.

What makes the preference for .au especially powerful is its connection to Australia. This is important for smaller, local businesses, who want to make it clear to visitors where they're located. It's also how larger companies prove they're committed to their Australian customer. This applies to large, Australian-founded brands like Woolworths or ABC News, as well as international companies with a strong in-country presence catering to our population. It improves the user experience for visitors, too.

BMW, for example, uses bmw.com.au to make it clear that visitors are now at the BMW Australia site and will see vehicles they can purchase for our roads. It's a much smoother experience than digging around a website just to find that

the content isn't tailored for Australia and the standards, pricing and availability aren't the same.

Similarly, Amazon's audiobook service Audible uses audible.com.au for its Australian customers so consumers are shown products that meet Australian digital rights and currency preferences.

Of course, the Woolworths, BMWs, and Amazons of the world could just as easily stick to .com, or perhaps do the 'au' subdomain (au.bmw.com) or forward slash Australia (audible.com/australia). However, by adopting .au these businesses are saying, 'Hey, we want to meet you where you are, not force you to come to us. We want to make you feel special and tailor your experience'. It also makes in-market advertising easier, and aligns nicely with all the other online mediums that need to be considered.

The .au extension is particularly useful on social media, where it's often added onto a brand name to make it clear that this account and its content is geared toward an Aussie audience. BMW, for example, uses the handle [@bmwAU](https://twitter.com/bmwAU) on its social channels to align its brand to the Australian market.

Using .au is also a simple way to avoid cases of mistaken identity. ABC News shares the same name

as an American TV network. So on Facebook, they go by abcnews.au; if you're scrolling through Instagram, you'll find them as [abcnews_au](https://www.instagram.com/abcnews_au). Interestingly, ABC News doesn't have a .com.au web address – they use .net.au. Why? Because the value is the .au that denotes ABC's connection to Australia.

For real estate site Domain, there's value in connecting with the Australian identity for something as localised and emotional as looking for a new home. The .au at the end of Domain's URL carries through to its various social media handles.

Similarly, Mental Health Australia goes by [@AUMentalHealth](https://www.instagram.com/AUMentalHealth) on social media. Not only are they making it clear where their focus is, but the not-for-profit organisation is owning the mental health space in the country by using .au. It builds a certain level of trust with their audience – they understand the Australian psyche and nuances of life here, and are able to support the public in a very specific way.

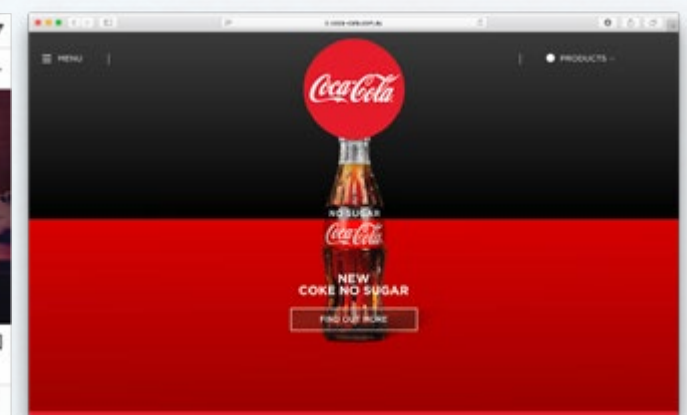
And that boils down to what's likely the .au extension's strongest selling point. Consumers understand that .au signifies Australia, and it's comforting. There's a level of trust that comes with .au that's unmatched by any other extension and a sense of pride in Australia. Unlike .com, which is used globally, .au is our domain. ■



Twitter



Instagram



Website

Examples of how Coca-Cola Australia digitally connects to local customers.

WOMEN IN TECHNOLOGY

Female founder Chloe Blattmann of RagTagd



By Maggie Whitnall –
Senior Client Services Manager, AusRegistry

In our 12th edition of **Behind the Dot**, we spoke to **Marisa Warren**, the CEO, Chair, and Founder of **ELEVACAO Foundation**. **ELEVACAO** empowers women entrepreneurs to succeed in an environment supported by both men and women, and Marisa highlighted startup **RagTagd** and its co-founder **Chloe Blattmann** as a shining example of the organisations that have emerged from the program.

RagTagd's smart tags help parents find their child's lost property at school. Chloe Blattmann secured funding for the business in her final round of pitches during the **ELEVACAO** program. We spoke to Chloe about the startup process, her approach to entrepreneurship, and how she launched **RagTagd**.

When Chloe was accepted into the program in 2016, she didn't know what to expect. **RagTagd** was only a few months old and still in development. She had no pitching experience and no idea about investors, but knew that she wanted the business to succeed.



During the intensive three-week program, Chloe received mentoring and coaching from experienced entrepreneurs in a number of areas and skills, including pitching her business plan and talking to investors. After each pitching round, she received advice from a range of industry professionals, culminating in a final 10-minute pitch to a 70-person audience comprised of investors, judges, and industry professionals that landed her the funds necessary to kick off **RagTagd**.

"Chloe nailed it," said Marisa. "She fielded some very tough questions, which forces you to know your business from back to front. She was adept and was able to confidently think on her feet, the qualities of a successful entrepreneur."



Ragtagd.com.au cofounder *Chloe Blattmann* at the **ELEVACAO** pitch event.

At 24, Chloe is a confident young woman who doesn't think for a second her achievements are unusual. *"I'm the standard personality type for an entrepreneur – I've always done my own thing."* She is an engineering graduate who studied mechatronics at the University of New South Wales and considers herself a rule breaker.

"My initial interest has always been in innovation, to be a part of work that changes the world and influences and impacts people in a big way."

The idea for **RagTagd** came about with business partner Eugene Holdenson, who provides the marketing arm to the business. As with any successful startup, **RagTagd** addresses an existing problem with a fairly simple solution.

RagTagd helps solve the issue of lost property at schools by attaching smart tags to clothing, notifying parents via text message when the item winds up in lost property.

Already used by more than 100 schools across Australia, **RagTagd** is growing quickly with plans to track other school items, like lunch boxes and shoes. The company also hopes to replicate its use for public transport depots, allowing passengers to track items left behind on buses, trains, and trams.

The startup also recently signed a deal with an Australian supplier and are expanding internationally.

Chloe Blattmann is co-founder at Radtagd. RagTagd is a Smart Tag which helps you to quickly and easily recover lost things at school. www.ragtagd.com.au ■





What's next for DDoS attacks?

By **Robin Schmitt** – VP Security Services Asia Pacific, Neustar

Distributed Denial of Service (DDoS) attacks have been threatening organisations across the globe in recent years, damaging corporate reputations and causing down time that has inconvenienced customers at best and crippled businesses at worst. 2016 was marked by the rise of massive Internet of Things (IoT) fuelled volumetric attacks surpassing 1Tbps, while 2017 has seen the size, complexity and sophistication of attacks increase, typically leveraging DDoS attacks to steal valuable information or raise a ransom.

According to the findings of the October 2017 Neustar Global DDoS Attacks & Cyber Security Insights Report, more than eight in ten organisations surveyed globally have been attacked at least once in the previous 12 months (an increase of 15% since 2016). Furthermore, 81% of those attacked were hit more than once.

Despite knowing the threats, companies are still struggling to detect and respond to DDoS attacks effectively and efficiently. In fact, 36% of respondents globally were only alerted to a DDoS attack by customers, a major embarrassment for their brands. This figure is up from 29% in 2016.

How have DDoS attacks evolved throughout 2017?

DDoS attack size, complexity and sophistication has continued to grow throughout 2017. Attack volumes greater than 10Gbps are up 5% as compared to 2016, and continued use of IoT-enabled botnets to deliver massive (greater than 500Gbps) volumetric attacks has led to an arms race, with Neustar responding by increasing its mitigation capacity to 10Tbps by the end of Q1 2018.

Multi-vector attacks have become a near-universal experience – 75% of attacks during early 2017 were multi-vector, as seen by the Neustar Security Operations Centre - demonstrating that attackers are consolidating the most effective methods to launch multi-pronged attacks on the network, servers and software in organisations.

Theft resulting from complex multi-vector attacks has also increased, with 58% of attacked organisations reporting the theft of financial data, customer data and/or intellectual property in concert with the DDoS attack (up 9% on 2016). We have also seen the number of APAC organisations that encountered ransomware in unison with a DDoS attack rise sharply, from 16% in October 2016, to 30% a year later.



How are organisations impacted?

With organisations across the APAC region being attacked more often, businesses should regularly re-examine the effectiveness of existing security strategies, including DDoS mitigation. The consequences of a DDoS attack can be significant.

To provide insight into the potential financial impact of an outage, after a DDoS attack 52% of APAC organisations reported average revenue losses of \$130,000 or more per hour of peak downtime. Furthermore, over half of the organisations attacked within APAC took more than three hours to detect an attack (53%, up 10% compared to 2016), and then an additional 3 hours or more to respond to (mitigate) the attack (51%, up 5% compared to 2016). Considering these findings together, over 50% of organisations, if attacked during peak times would have

suffered a minimum of \$780,000 (\$130,000 x 6hrs) loss. This is alarming given increased investment in DDoS protection and that an average time to mitigate of 90 seconds is achievable (i.e. Neustar's average response time for 2016).

The increase in detection and response times, driven by an increase in complexity of attacks, coincides with increased spending, with 80% of organisations spending more on DDoS defences.

While 80% of organisations globally are investing more in DDoS-specific defences today, 90% report that more expenditure is required to strengthen defences to quickly and effectively mitigate the growing risk DDoS attacks impose.

In addition, more sophisticated attacks, focused on the application layer have led to a 40% increase (2016 13% vs 2017 53%) in the adoption of Web Application Firewalls (WAF) to protect against ISO Layer 7 attacks.

What solutions are in the market?

By understanding the risk imposed and technical infrastructure organisations can determine the required defences and associated spending, allowing for the selection of the right solution for the specific organisation.

In making a decision, there are several solutions in the market that organisations could consider.

Several low cost, Content Delivery Network (CDN) style services can offer inexpensive DDoS protection, however they may impose usability issues and be unable to stop a significant attack.

Similarly, DDoS mitigation appliances can be effective against certain types of attacks, however increasingly popular large-scale floods can overwhelm circuit capacity and render the appliance ineffective.

On-demand cloud, where network traffic is redirected to a mitigation cloud, is reliable and cost effective. However, it

is dependent on swift failover to the cloud in order to avoid downtime. This can be automated, with integration between the client's routers and the mitigation partner. A good service will provide integrated protection and monitoring of network and application layer (ISO Layers 3, 4 and 7) attacks.

Always-routed cloud, on the other hand, involves the redirection of web traffic on a constant basis. The constant redirection can affect network latency, even during non-attack conditions, and additional services may be required to address application layer attacks. Integration with a CDN and support of a cloud based WAF is common for this type of solution.

Adopting a DDoS mitigation approach that includes a managed appliance and cloud (hybrid) is the best option, if you operate your own infrastructure, yet can be costly. The appliance will stop any DDoS attack within the circuit capacity feeding the network, and automatically trigger cloud mitigation, if the circuit is in danger of becoming overwhelmed.

No matter the solution used, given that DDoS is often used as a smoke-screen, the organisation must be able to effectively monitor the attack, while ensuring that all other defences are on heightened alert. Having a single user interface, real-time (or near real-time) monitoring and reporting and a unified 24x7 Security Operation Centre (SOC) is a must.

In conclusion, DDoS attacks have reached unprecedented levels during 2017, with complex (multi-vector) attacks being the norm, continued leveraging of IoT devices to generate massive volumetric attacks and a dramatic rise in the use of ransomware in conjunction with a DDoS attack. Those working to protect corporate revenue and reputation would be wise to work with knowledgeable partners that have extensive experience in identifying and addressing DDoS attacks, plus access to multiple sources of intelligence and a product roadmap that ensures they will meet the 'threats of tomorrow'. ■



Governance & policy

By **Richard McKenzie** – Marketing and Research Coordinator, auDA

If there's one ever-present tension in the online world, it's the balance between opportunity and risk – the opportunity of exchanging ideas and goods in a global marketplace and the risk of being swindled, either financially or through loss of data.

These risks can arise in a number of ways, from email phishing scams and malicious file downloads to ransomware. It is also possible that the online store you're visiting isn't what it claims and, if you purchase an item, will send you the wrong goods – if you're lucky – or nothing at all.

Many of these sites have domain names ending in .com, .net, or another country's Top-Level Domain (TLD). Given the global and sometimes anarchic nature of the internet, it can be hard to seek recourse on such scam websites hosted far beyond our geographic borders. However, if they exist in the .au domain name space, we can fight back against the scammers.

The .au domain space is Australia's home on the internet. It is a trusted and well-regulated space used by millions of Australians every single day for work and play. Unlike generic TLDs, such as .com, .net, .info, not everyone can get a .au domain name. There are rules and policies in place to ensure only eligible registrants can register a domain name, and it's these requirements that have helped make .au a more trusted space for all Australians.

Sadly, however, in the online world as in the physical world, there are always people trying to take advantage of others. Ironically, Australian consumer trust in .au also makes it a target for criminals to exploit, and one way is for a malicious actor to use unauthorised business details, such as Australian Business Numbers (ABN), to register a .au domain name for their nefarious activities.

In some instances, online stores are set up to fraudulently trade and deceive consumers, including delivering poor-quality goods or nothing at all.

Combating the unauthorised use of business details to register .au domain names remains a priority for auDA's compliance team. Popularly known as Unauthorised Business Use, or UBUs, auDA has implemented a three-pronged strategy to tackle the problem:

- Auditing the .au Registry to identify and investigate any existing UBU domain names;
- Monitoring the daily New-add registrations for any new UBU activity; and
- Working with the Registrars who have been targeted by these bad actors, to identify possible UBU activity and stop it in its tracks.

As a direct result of UBUs, since May 2017, auDA has deleted 10,569 domain names that were registered using unauthorised business information. Currently, at time of print, there are investigations into a further 587 suspected UBUs registrations.

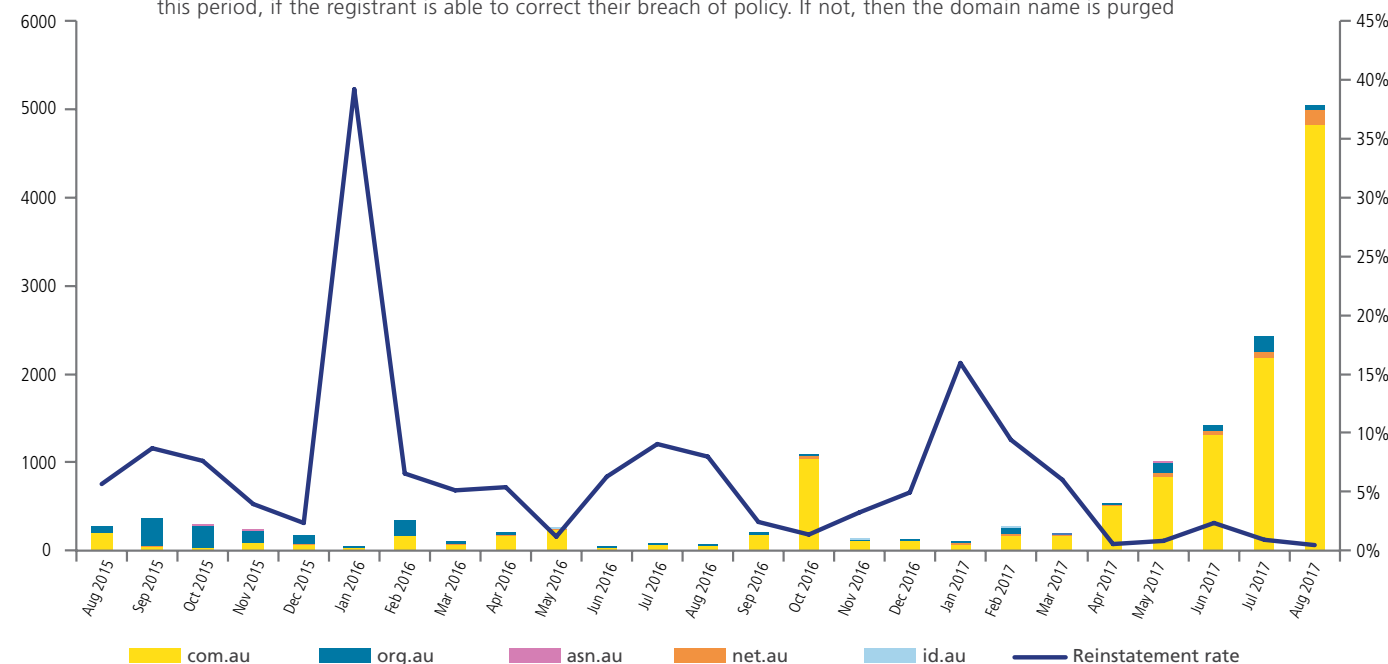
This strategic approach to addressing the recent UBU trend has also resulted in an 81% drop in the number of new UBUs domain name registrations between June 2017 and August 2017. Clear evidence that the approach is working.

Additionally, auDA is examining the potential of collaborating with other regulators and technology experts around the world to identify processes and systems to help streamline the verification of business details at the point of registration. Hiring of new compliance staff at auDA will also expand and enhance the ability to monitor unauthorised use and take action where necessary.

Given the potential for UBUs to damage public confidence in the .au domain name space, be assured that combating unauthorised use is a key priority for auDA. ■

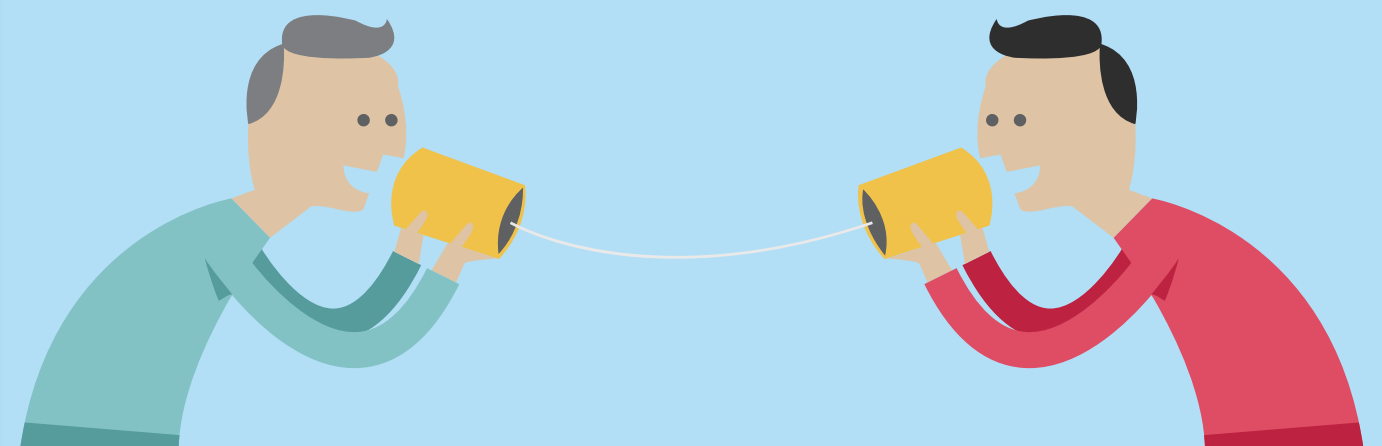
.au Policy Deletes (and Reinstatement Rate)

When auDA or the Registrar of record deletes a domain name for breach of policy, the domain name is placed into "pending policy delete" status for 14 calendar days. The domain name can be reinstated during this period, if the registrant is able to correct their breach of policy. If not, then the domain name is purged



Channel talk

“What is one piece of advice you'd give someone who is starting an online business?”



MADDISON SELLECK

VentralP Australia

Take the time to research the perfect web address for your business.

Registering a remarkable domain name when getting started online can give your business a competitive edge in the early days and is significantly easier than trying to make the change once your brand has built a solid foundation online. The ideal domain name will not only help your business stand out from the virtual crowd but will be easy to remember, represent your brand accurately, and resonate with your ideal customer.

With more than 1,500 Top-Level Domains available, it's now easier than ever to craft a memorable web address for your business that will help boost your brand's online presence. Consider registering a ccTLD if your business will be primarily servicing an audience located in a specific country or region as these domain names are easy to remember and are often given preferential treatment by many search engines.

JONATHAN HORNE

Terrific / LIS.com.au

The best piece of advice I can give to anyone wanting to start an online business is to go to market before the product is ready. A lot of online businesses get stuck in a development loop and stall going to market because they want to add 'one last' feature.

The iron fist of the market may not like your product at all, or you may need to pivot, so the faster you have the market feedback to lead your decisions, the faster you will be on track to a successful online business.

FRED SALEM

Melbourne IT Group

How? It starts with careful planning. A trendy name isn't enough; your online brand needs to be defined, trusted, and provide good service. Start with a domain name that suits your brand or industry, either a traditional com.au or a new TLD.

Make sure your website is well-designed, mobile-friendly and easy to use. Whether

it's templated or custom built, the copy and imagery should be solid and aligned to your brand identity. Don't forget to link to your business's social media accounts!

Finally, security is critical to protecting your online brand. A valid (2017 and beyond) SSL certificate is all about trust. Online users are becoming increasingly wary of sites without encryption, particularly when submitting personal information, and actively check for https:// in the URL bar. As a great side motivator, you'll avoid being penalised by Google for not having one!

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

Channel Talk compiled by Courtney Fabian and Lucian Popaly. To contribute to Channel Talk, please contact behindthedot@ausregistry.com.au. ■

Glossary

Abbreviations

APNIC	Asia-Pacific Network Information Centre
APTLD	Asia-Pacific Top Level Domain Association
auDA	.au Domain Administration
ccTLD	Country Code Top Level Domain
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
EPP	Extensible Provisioning Protocol
gTLD	Generic Top level Domain
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communications Technology
IDN	Internationalised Domain Name
IP	Internet Protocol
TDUM	Total Domains Under Management
TLD	Top-Level Domain
UBU	Unauthorised Business Use
WHOIS	A combined phrase to denote ‘who is’

Definitions

Asia-Pacific Top Level Domain 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.
.au Domain Administration (auDA)	The policy authority and industry self-regulatory body for the .au domain space.
.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.
Domain Name	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.
EPP	Extensible Provisioning Protocol is a flexible protocol designed for allocating objects within technical registries over the Internet.
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.

Information and Communications Technology (ICT)	ICT refers to technologies that provide access to information through telecommunications. It is similar to Information Technology (IT), but focuses primarily on communication technologies. This includes the Internet, wireless networks, cell phones, and other communication mediums.
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.
Internet Protocol (IP) Address	An IP Address is the numerical address by which a location in the Internet is identified. Computers on the Internet use IP Addresses to route traffic and establish connections among themselves; people generally use the human-friendly names made possible by the Domain Name System.
New-adds	New domain name registrations i.e. new additions to the number of names under management
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).
WHOIS	WHOIS (a combined phrase to denote ‘who is’) is a query and response protocol that is standard within the Domain Name Industry for querying Registry databases to determine certain information about a particular Domain Name.
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.

Disclaimer
This report has been produced by AusRegistry and is only for the information of the particular person to whom it is provided (the Recipient). This report is subject to copyright and may contain privileged and/ or confidential information. As such, this report (or any part of it) may not be reproduced, distributed or published without the prior written consent of AusRegistry.
This report has been prepared and presented in good faith based on AusRegistry’s own information and sources which are believed to be reliable. AusRegistry assume no responsibility for the accuracy, reliability or completeness of the information contained in this report (except to the extent that liability under statute cannot be excluded).
To the extent that AusRegistry may be liable, liability is limited at AusRegistry’s option to replacing, repairing or supplying equivalent goods or paying the cost of replacing, repairing or acquiring equivalent, or, in the case of services, re-supplying or paying the cost of having such re-supplied.

© 2016, AusRegistry Pty Ltd.



ausregistry.com.au

