



AUSCERT



— AUSTRALIAN PIONEER CYBER EMERGENCY RESPONSE TEAM

YEAR IN REVIEW 2019





FOREWORD

AUSCERT STATE-OF-THE-UNION

The last decade has seen a phenomenal rise in all forms of cyber related activity, from mischievous individuals with access to seemingly unlimited resources, through to organised criminals who operate outside our state boundaries and with little to no accountability in their home countries. Whoever the threat actor may be, the common elements that exist are our organisations and assets are under constant attack and we are better protected by sharing knowledge and working closely together.

The traditional approach of strong network borders and other technology solutions are no longer solely adequate but need to form part of a multi-layered protection strategy. Additionally, acknowledging the inevitability of cyber events should be encouraging organisations to spend some of their hard earned funds in early detection and limiting the impact of these events. By implementing good governance processes and understanding the data assets of the organisation allows funds to be targeted wisely and prevents a “technical blowout” within budgets.

As many cyber-attacks start with a human victim, investing in the skills across all the workforce, from operatives to executives, is extremely important. Having robust and tested plans for when incidents

occur is critical to reducing impact and minimising additional fallout such as reputational damage. Finally, strategic investment in technology with capabilities to operate through automation (e.g. the ability for threat intelligence to flow to control points without the need for “cut and paste”) is essential in enabling the technical staff to pursue higher value activities.

As AusCERT enters its 28th year, it constantly strives to understand the threat landscape, is mindful of the needs of its membership and as an independent not-for-profit CERT¹, be there to support and actively help protect organisations in the ANZ pacific region by delivering high quality cyber intelligence and supporting members during incidents. Over recent years, AusCERT has worked hard to create communities where the sharing of information can be carried out in a safe manner and help educate, both informally through member meetups and the annual conference and formally with training courses. We strive to support members through the occurrence of cyber incidents, both prior with good incident response planning and during, with advice and assistance.

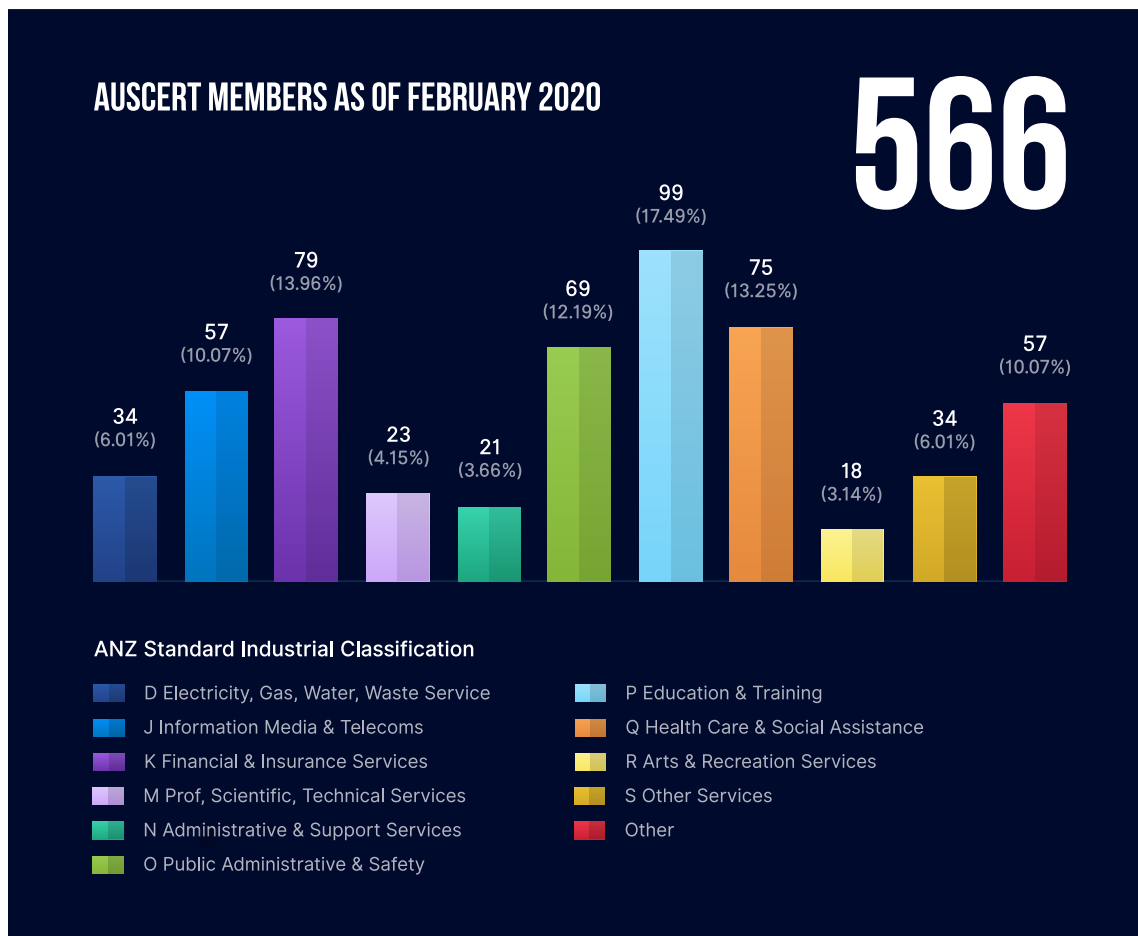
Dr David Stockdale - Director

1. A computer emergency response team (CERT) is a group of experts who respond to cyber security incidents.

STATISTICS AND REPORTING

AS OF FEBRUARY 2020, AusCERT is made up of 566 member organisations comprising several tiers of membership levels (small to enterprise). Members are grouped into defined Australian and New Zealand Standard Industrial Classification categories and

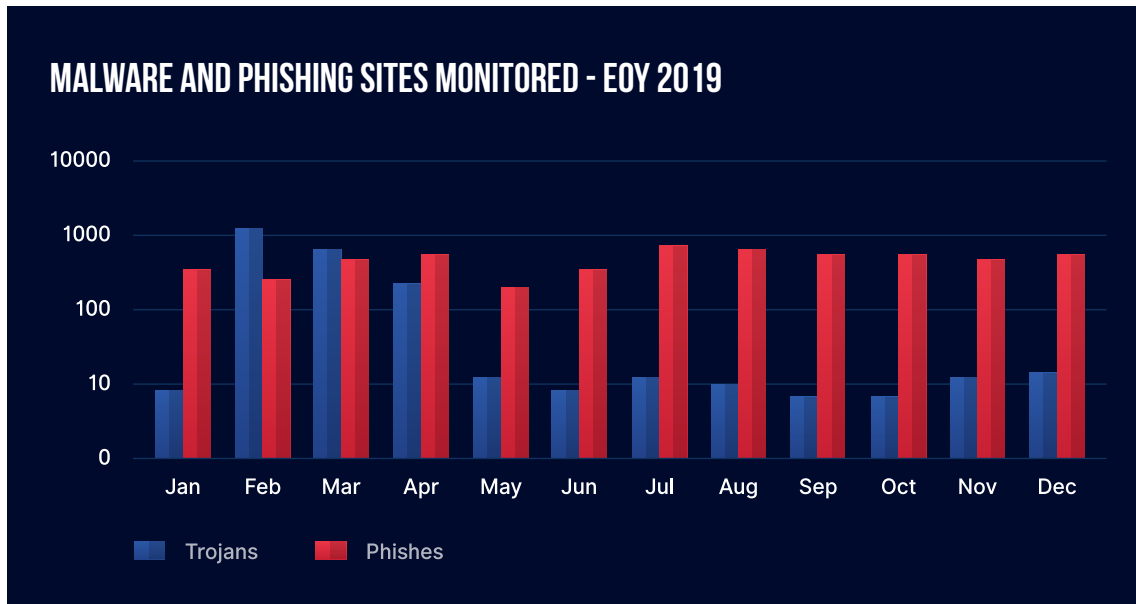
the top 3 industries represented by our members are from the following sectors: Education & Training, Financial & Insurance Services and Healthcare & Social Assistance.



01 INCIDENT MANAGEMENT

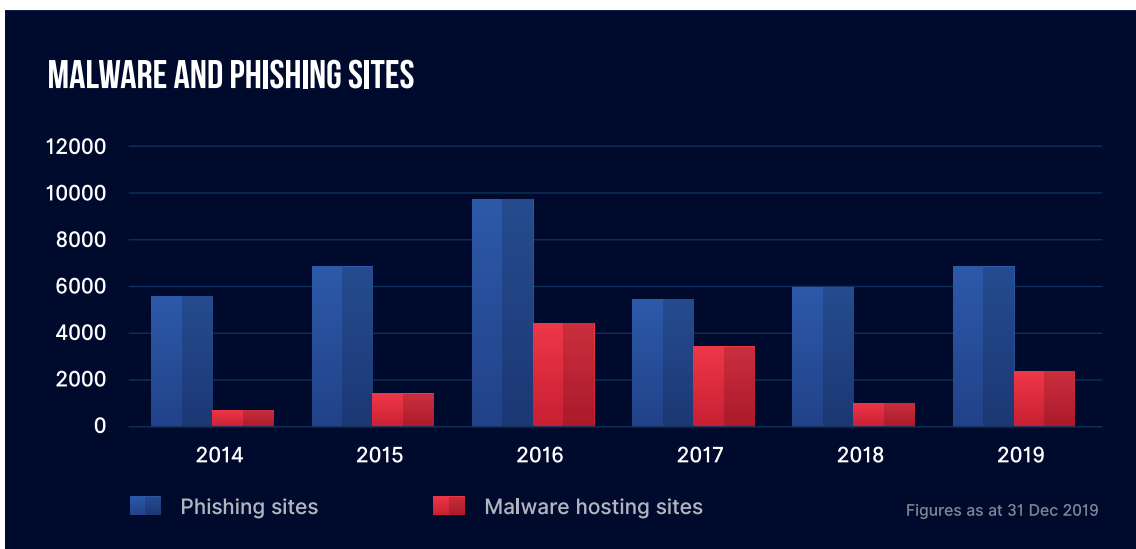
AusCERT's Incident Management Service (sometimes referred to as incident response) includes incident coordination and incident handling, both of which are standard inclusions as part of AusCERT's membership services. The below diagram is the statistics of

incidents that required handling either of phish site or that of malware, for the calendar year of 2019. These tallies are sites that are located around the world that, when interacted with, affects the security of the constituency that AusCERT is serving.



02 PHISHING TAKEDOWN

AusCERT members can utilise AusCERT's considerably large overseas and local contact networks for removal of phishing and malware sites. The number of sites that were handled in the past six years are shown below.



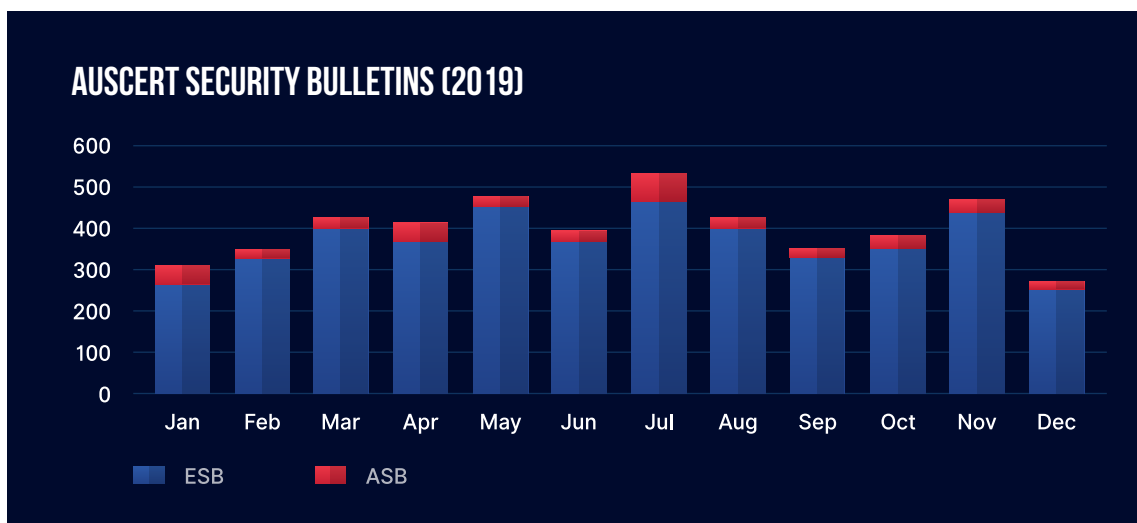
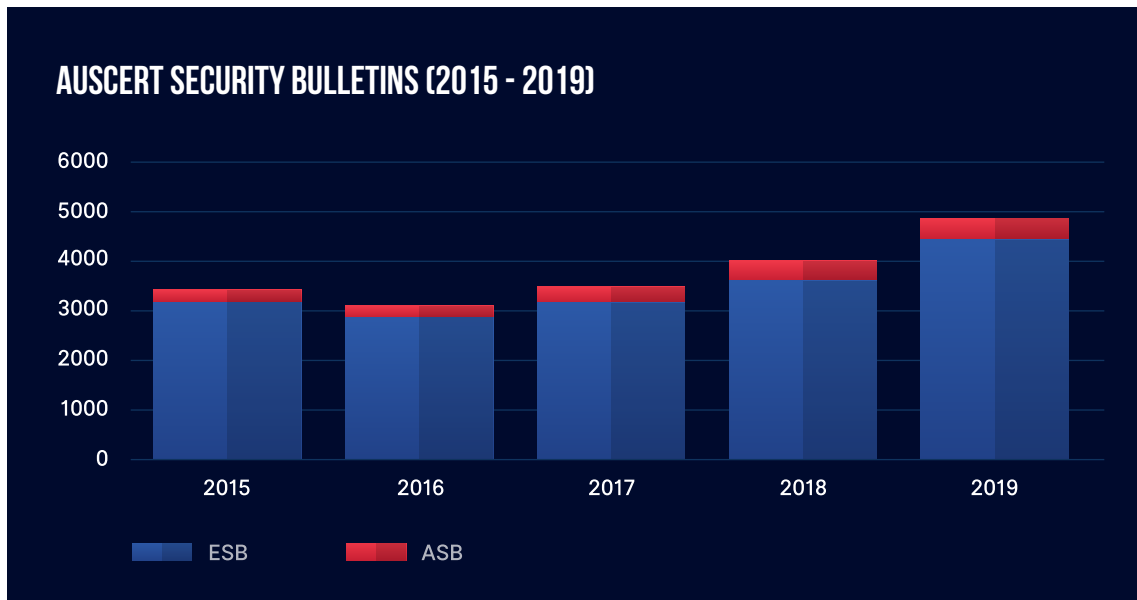
03 SECURITY BULLETINS

AusCERT distributes security advisories and bulletins to its members by email and publishes a portion of them to its public website. Bulletins are published in a standardised format with a consistent approach to classifications of vulnerabilities, impacts and affected operating systems.

During 2019, 4788 External Security Bulletins (ESBs)

and 354 AusCERT Security Bulletins (ASBs) were published.

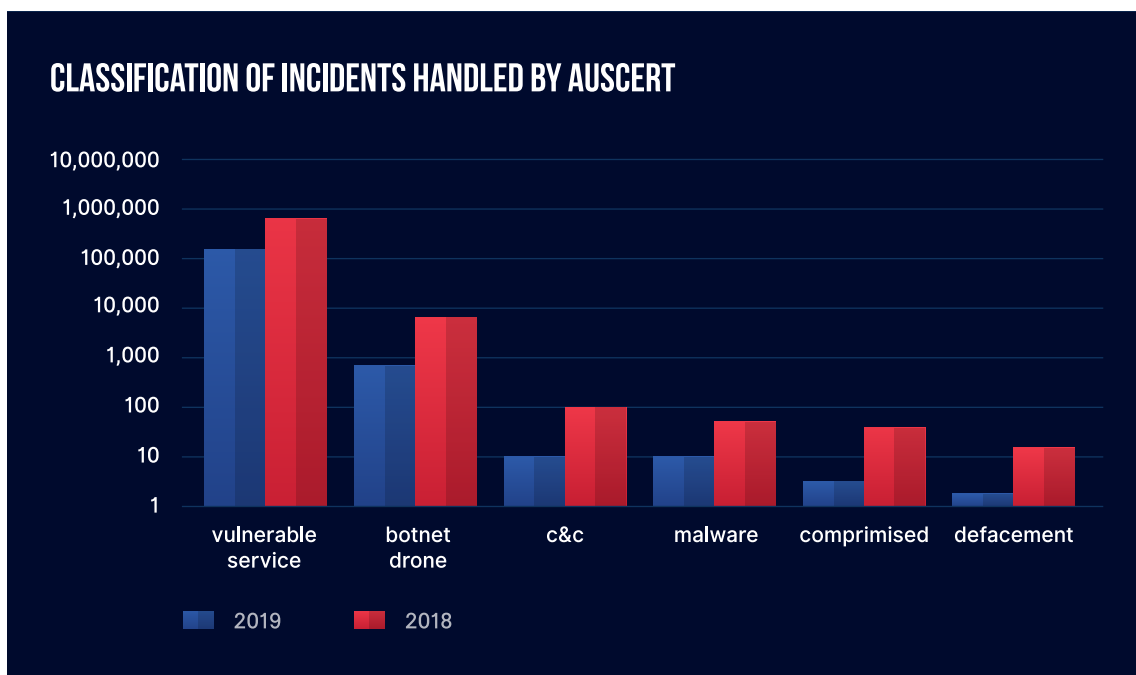
The ESBs are made publicly available immediately however the ASBs are available only to members for a period of one month after which they become available for public consumption.



04 MEMBER SECURITY INCIDENT NOTIFICATIONS

AusCERT members benefit from AusCERT's considerably large overseas and local threat intelligence feeds with respect to incidents that have been detected by other parties but concern the members. There are several categories of incidents and this service has been running for members for several years. 2019, as compared with 2018, follows

the same distribution of incidents. These notifications are a mix of Indicators of Vulnerabilities (IoV) and Indicators of Compromise (IoC). The numbers of IoV far outweigh other categories and hence to be able to better display all the categories, the notifications are plotted on a logarithmic scale.



05 EARLY WARNING

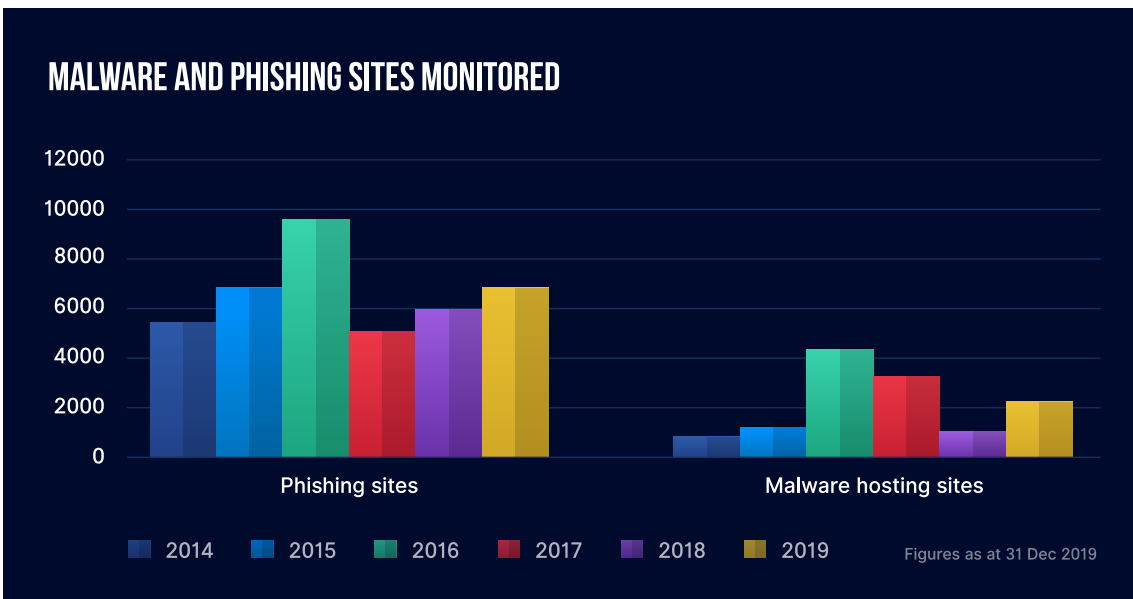
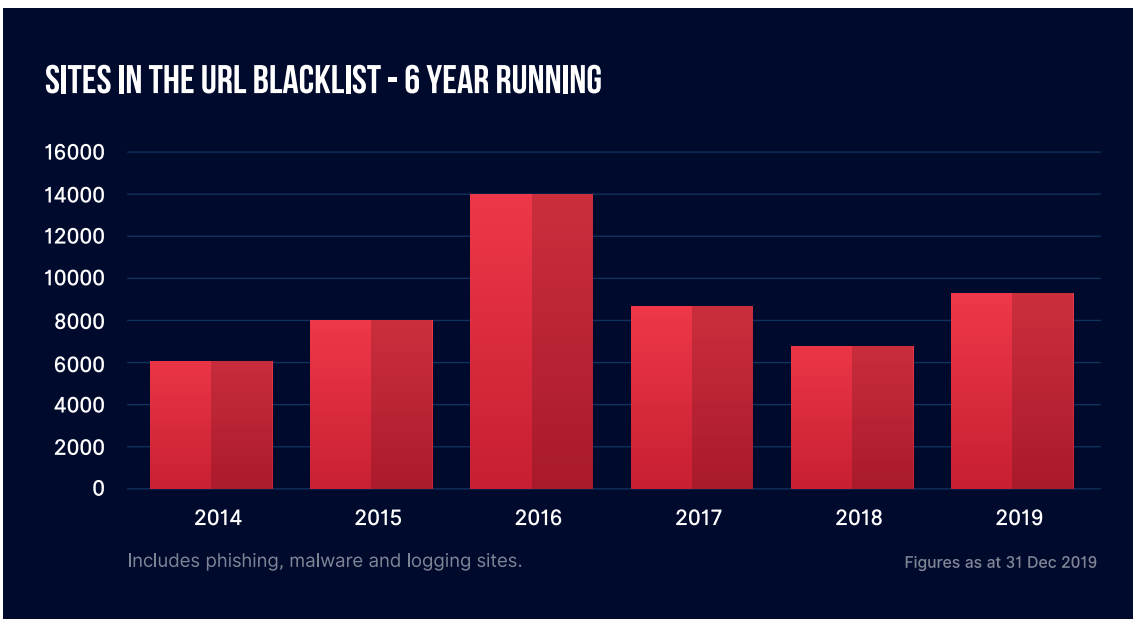
Members can subscribe to receive urgent SMS notifications when AusCERT's Security Bulletin Service identifies a vulnerability that has reached critical stages. In most circumstances this occurs when AusCERT is aware of active, in-the-wild exploitation of a vulnerability. Alerts are sent along with Bulletins,

with additional flagging of the Bulletins. These Bulletins are given special importance with respect to the nature of the issue. Of note is the growing number of bulletins that are being handled, this is in line with the increased capacity at AusCERT to process additional streams of advisories.

06 MALICIOUS URL FEED

On a daily basis, AusCERT encounters numerous phishing, malware, malware logging or mule recruitment web sites, including those directed at Australian Internet users. AusCERT collects this information and provides a feed that can be added to a firewall blacklist to prevent inadvertent compromise of

client computers on the protected network; or that list can be used to check web log files to see if any client computers on the protected network may have already connected to these web sites. The Malicious URL Feed is an effective resource to assist in detecting potential compromises as well as protecting client computers.



ACHIEVEMENTS AND MILESTONES

AusCERT continues to deliver sought after computer security incident handling and early warning information, whilst engaging members in cyber security. As a membership-based constituency, AusCERT has increased the breadth of organisations that it serves.

AusCERT has been committed to its constituency, quality services and support from membership with AusCERT. During 2019, AusCERT expanded its

operational capacity to provide more information and worked on capability improvement projects for the purpose of improving the value of AusCERT to its constituency.

The AusCERT instance of Malware Information Sharing Platform (MISP), which was first piloted for key sectors in 2017, placed in full production in 2018, continued to prove itself as a valuable member resource through 2019.

ADDED CAPABILITY

On-premise automated use of open source sandbox

AusCERT grew capability to perform automated malware analysis. The team deployed an advanced Cuckoo Sandbox, a 100% open source industry known automated malware analysis system, which provides infinite application opportunities. By default, it is able to:

- Analyse many different malicious files (executables, office documents, pdf files, emails, etc) as well as malicious websites under Windows, Linux, macOS, and Android virtualized environments.
- Trace API calls and general behaviour of the file and distil this into high level information and signatures comprehensible by anyone.
- Dump and analyse network traffic, even when encrypted with SSL/TLS. With native network routing support to drop all traffic or route it through a network interface, or a VPN.

- Perform advanced memory analysis of the infected virtualized system through Volatility as well as on a process memory granularity using YARA.

The open source nature and extensive modular design of the AusCERT Cuckoo Sandbox means it can be customised according to needs regarding any aspect of the analysis environment, analysis results processing, and reporting stage.

ON PREMISE MALICIOUS WEBSITE MONITORING

During 2019, AusCERT completed an innovative project to automate the process of monitoring malicious websites. Osprey was originally born from a vision to develop a script to simply automate lookups of malicious websites.

Osprey is capable of monitoring URLs and incorporating applications of various APIs. Osprey is integrated with several AusCERT systems and services (Malicious

URL Feed, Cuckoo Sandbox, MISP) and varying known public resources. Integration allows Osprey to automatically extract URLs from the Malicious URL Feed every 5-10 minutes for sophisticated processing tasks or actions.

Osprey is an important monitoring and investigative tool, performing sophisticated tasks using unique approaches to determine when a given site changes status, so that alerts can be automatically generated. Osprey is continually evolving in capability to bring additional, valued functionality to members.

IMPROVED CAPABILITY

Expanded and further automated Bulletins ESB/ ASB creation.

During 2019, AusCERT developed a replacement of its Security Bulletin creation system. This new system will allow for increased automation, additional filtering options, and provide a flexible platform for future feature enhancements.

Training Material

During 2019, AusCERT focused on both updating and creating training material that would provide value to members through the AusCERT Education service.

AusCERT updated both Risk Management and Incident Response Planning training course materials to ensure quality and relevant information to our members. Details relating to these two updated courses are as follows:

- **Cyber Security Risk Management**
Attendees gain the confidence to perform a risk assessment of cyber security risks and the ability to rate and assess business risks rather than technical vulnerabilities
- **Incident Response Planning**
Attendees are equipped with the tools to write a bespoke incident response plan for their organisation

During 2019, AusCERT introduced material for two brand new training courses. The courses focus on providing members with valuable introductory cyber security knowledge, and in imparting technical skills and knowledge relating to the Malware Information Sharing Platform (MISP). Details relating to these two new courses are as follows:

- **Introduction to Cyber Security for IT professionals**
Attendees will gain an understanding of information security principles, cyber security as a risk to business objectives; and cultivate an appreciation of the current cyber threat landscape
- **MISP**
Attendees learn the skills needed to set-up, configure and integrate Malware Information Sharing Platform into their organisation's cybersecurity defence strategy.

The aim of **AusCERT Education** is to provide exceptional training experience to individuals and organisations.

INTERNATIONAL AND COMMUNITY ENGAGEMENT

SecTalks

On Thursday, 24 October 2019, an AusCERT representative delivered a talk to sixty-two attendees of SecTalks Brisbane meetup at the Brisbane Telstra Offices. The subject was blue-team related, specifically the talk on the topic of automating data entry and indicator enrichment using MISP (Malware information sharing platform).

Feedback from SecTalks organisers was the talk was well delivered, received and the AusCERT representative described as "thought-inspiring".

Cyber Security Training in Samoa with APNIC

AusCERT participated with APNIC as trainers for the third Regional Workshop "Building cyber security capability for #CERTs #CSIRTs in the Pacific" in Apia, Samoa. Thirty-five participants from seven Pacific Island nations joined the event. The program for the workshop was structured around three days, and included practical hands-on sessions, review of case-studies and interactive discussions.

During the workshop a drill exercise was conducted, during which every participant was able to play as a CERT and work together to handle an ongoing attack/breach. The workshop was organized by the APNIC Foundation with support from APNIC and SAMOA MCIT, with funding from the Cyber Cooperation Program of the Australian Government Department of Foreign Affairs and Trade.

Transits Training in South Korea

AusCERT participated in the APISC Security Training Course, organised by KrCERT/CC, operated by the Korea Internet & Security Agency in the last week of 8th -12th July 2019. AusCERT sent a team member to join three other instructors to facilitate the TRANSITS material to CERT/CSIRTs gathered from across the globe.

Along with the instruction of TRANSITS material, there were also other CERT/CSIRT exercises and economy reports of CERT/CSIRT operations, that helped share experience in organising and operating a CERT/CSIRT. AusCERT is honoured to have been part of the APISC Security Training Course organised by KrCERT.



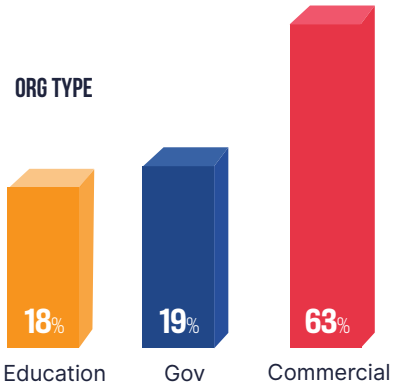
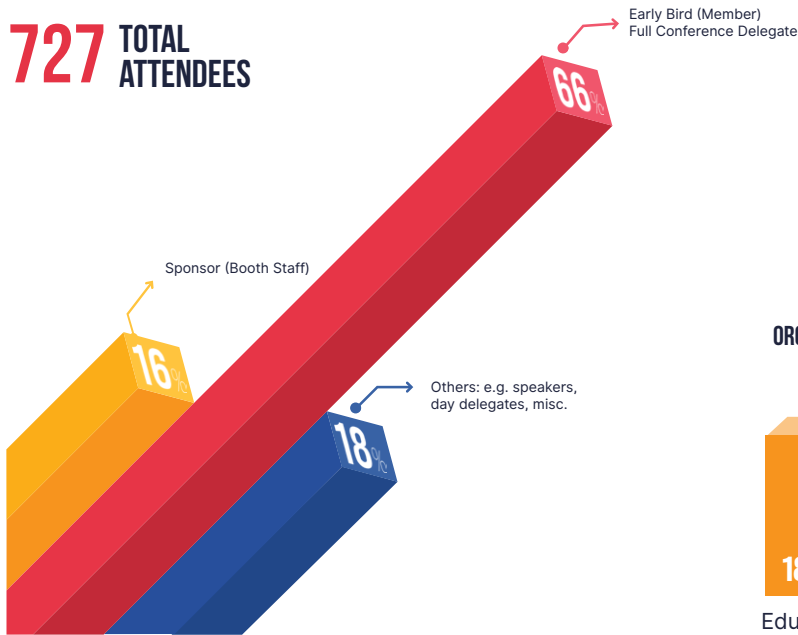
EVENTS, MARKETING & COMMUNICATIONS

AUSCERT2019 CONFERENCE

The AusCERT Conference is the oldest information security conference in Australia; this year we celebrated our 18th conference anniversary. The event was held at the Surfers Paradise Marriott Resort & Spa on the Gold Coast between the 28th to the 31st of May 2019 and the theme was *"It's Dangerous to Go Alone"*.



727 TOTAL ATTENDEES



OVERVIEW OF DELEGATE ORGS AND ROLES

THE FOLLOWING CATEGORIES WERE THE HIGHEST NOMINATED JOB TYPES

01 IT / SECURITY ANALYST
220 delegates

02 MANAGER / DIRECTOR HEAD OF DIVISION
116 delegates

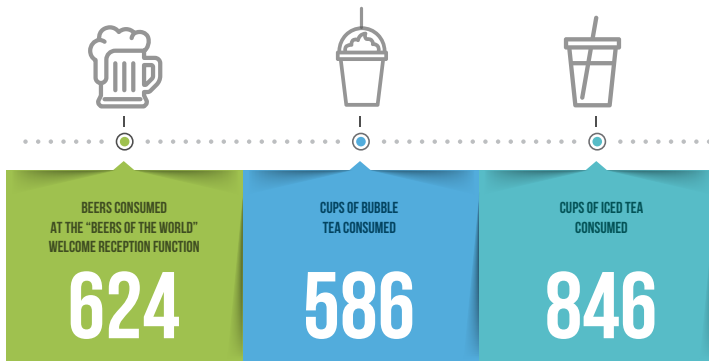
03 SALES, MARKETING EVENTS AND BUSINESS DEVELOPMENT
50 delegates

04 DEV / DEVOPS
40 delegates

05 SYSTEMS
38 delegates

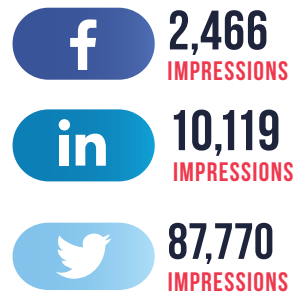
FYI C-SUITE
17 delegates

FUN FACTS



SOCIAL MEDIA HIGHLIGHTS

(WEEK OF CONFERENCE)



EXTERNAL INDUSTRY EVENTS

AusCERT participated in over 20 external engagement events. These include:

- Linux Conference 2019
- BSides Canberra
- Major General Marcus Thompson presentation with UQ Cyber
- BrisSEC19
- Bryan Lee (Palo Alto Networks) presentation at QODE
- CrikeyCon19
- ABCC Business Seminar : Finance, Fintech & Cyber Security
- Networkshop19 by AARNet
- 2019 FIRST AGM & Conference
- Malware and Reverse Engineering Conference 2019
- Celebrating Diversity and Inclusion in Queensland's ICT security sector (NAIDOC Week 2019)
- Boss of the SOC - Splunk CTF 2019
- Cyber Security in Government
- Interbank
- CLOUDSEC2019
- 2019 APCERT AGM and Annual Conference
- CAUDIT Spring members meeting
- 2019 AISA Annual Conference (CyberCon)
- TWCERT/CC Annual Conference
- CEBIT2019
- NAUDIT Community of Practice meeting
- Dr Stephen Banghart (NIST) presentation with UQ Cyber
- Cybercation Security Arena event

MEMBER ROADSHOWS

In 2019, we ran a member-exclusive meetup event in several cities including: Brisbane, Sydney and Melbourne.

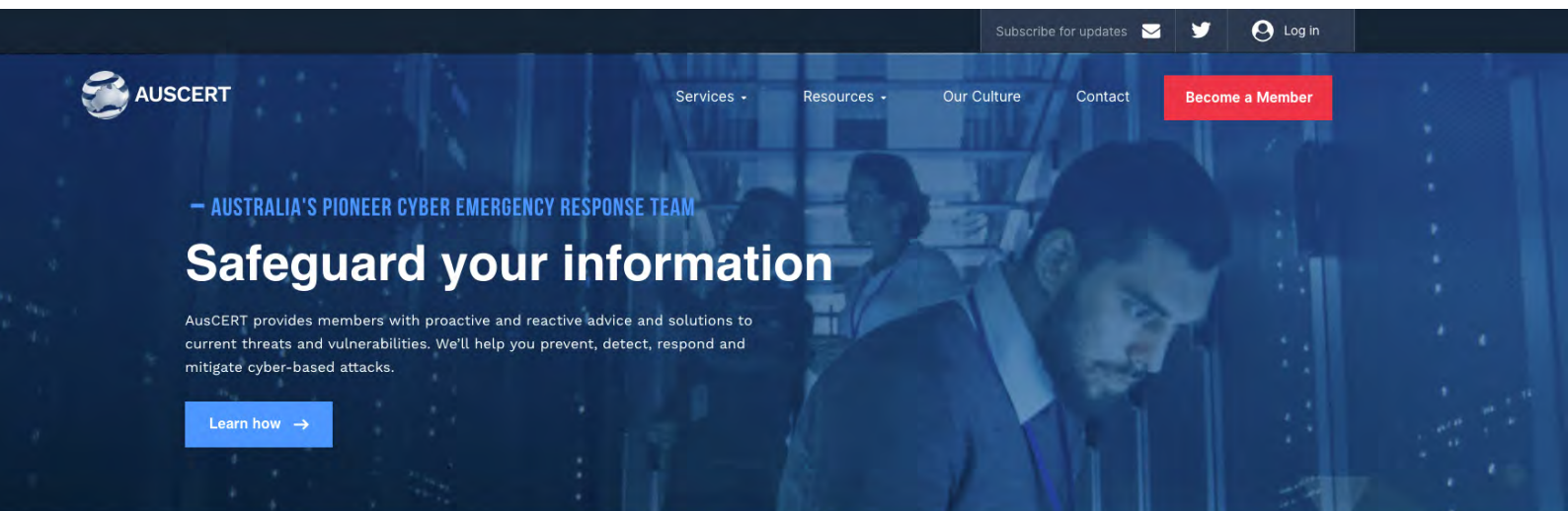
Quarterly catch ups with our Victorian Government members were also scheduled throughout the year.

The aim of these events is to update members on our state-of-the-union and roadmap as well as foster a best-practice habit of maximising their membership benefits by tapping into the entire breadth of our AusCERT services.

WEBSITE AND PUBLICATIONS

We launched our new-look website on 20 May and it has so far been very well received. This was the last step in our rebranding exercise which started in 2017.






Along with our website, AusCERT also now has a range of membership publications which can be found at our various industry events and roadshows.



Services

Our range of member services ensure your network is protected 24/7.

[MORE](#)

 Incident Management	 Phishing Take-Down	 Security Bulletins	 Member Security Incident Notifications	 Become a member
--	---	---	---	--

Latest Security Bulletins

[MORE](#)

- ESB-2020.0644 - 24 FEBRUARY 2020 [LINUX] →
IBM Spectrum Protect Plus: Multipl...
- ESB-2020.0643 - 24 FEBRUARY 2020 [LINUX] →
IBM MobileFirst Platform Foundatio...
- ESB-2020.0642 - 24 FEBRUARY 2020 [SUSE] →
java-1_7_1-ibm: Multiple...
- ESB-2020.0641 - 24 FEBRUARY 2020 [SUSE] →
libsolv, libzyp, zypper: Read-only...

Trusted Australia-wide by over 500 Member Organisations





STAY AT THE FOREFRONT OF SECURITY

Our unique range of services means we can be your main point of contact when dealing with data security incidents.

- Incident Management**
Whether it is proactive or reactive sensors you're after, we will help you detect, interpret and respond to attacks from across the globe.
- Phishing Take-Down**
Drawing on our strong international CERT relationships we have a high success rate in delivering phishing take-downs.
- Security Bulletins**
Receive up to date and consistent security advice across a wide range of vendors, streamlining security patching.
- Security Incident Notifications**
Be proactive with your security and receive our daily Member Security Incident Notifications (MSINs) custom to your network.
- Malicious URL Feed**
Add this Australian Based feed to your threat detector and feed to prevent compromises to your network.
- Sensitive Information Alert**
Alert notifications provided to email for sensitive material found online by our analyst team which potentially targets your organisation.
- Early Warnings**
Receive SMS notifications for the most critical security threats and vulnerabilities.
- ADD-ONS**
 - Certificate Services**
An add-on ecosystem to help manage digital certificates for education and government organisations.
 - Information Sharing & Analysis Centre (ISAC)**
This add-on service allows your organisation to ingest our advanced threat intelligence through MSIN's API integration.
 - AUSCERT Education**
Enhance your knowledge with our international one day training offerings for individuals and organisations.

SAFEGUARD YOUR INFORMATION

AUSCERT.ORG.AU

MEMBERSHIP PERKS

- 24/7 support**
against cyber security threats
- Safe & secure**
all information shared is secure & encrypted
- Regular events**
monthly meetups, workshops & more
- Access to all Threat Intel Services**
and a nationally trusted team
- Conference discounts**
and free tickets to the Annual Cyber Security Conference
- Not-for-profit**
existing for the greater good of our members

BECOME A MEMBER

Don't wait for a security incident. Act now to proactively protect you and your organisation.

CONTACT US NOW TO SIGN UP
+61 7 3365 4417
membership@auscert.org.au

AUSCERT

PROUDLY PART OF THE UNIVERSITY OF QUEENSLAND

AUSTRALIA'S PIONEER CYBER EMERGENCY RESPONSE TEAM

NOT-FOR-PROFIT, 25 YEARS STRONG

AUSCERT is a not-for-profit Cyber Emergency Response Team based in Australia, the world for the greater good of our members and provide proactive solutions for data-based threats. We offer a range of services to secure your network proactively and reactive solutions. Keep your data safe with AusCERT.

EXTERNAL COMMUNICATIONS

AusCERT engages with members and the public via several social media platforms. The most active being Twitter (over 6,700 followers), followed by LinkedIn (over 4,600 followers), with Facebook and YouTube sharing an equal number of followers (over 670 followers each).

In addition to social media, we also engage with

members and the public via the AusCERT Daily Intelligence Report (ADIR) which has over 1,100 followers.

We hope to continue to engage with members as well as the public on all things related to AusCERT and the greater cyber and information security sector.

AUSCERT

Daily Intelligence Report

AusCERT Daily Intelligence Report
Wednesday 06 June 2019

Hi there,

PARTNERSHIPS AND COLLABORATIONS

AusCERT works alongside a number of partners and collaborators to help growth, adaptability and enabling us to provide better services to members.

We love our collaborators just as much as we love our team. Take a look at some of the organisations we have the pleasure of working with:



CERTs /
Trusted Partners

WHAT'S NEXT?

As we step into a new decade, it is a well-known fact that automation is key to the success of any organisation.

A good example of this can be found in the Cyber Security Operations Centre (CSOC) of all modern organisations. A CSOC analyst might traditionally automate a task such as processing a dump file containing stolen credentials which require Active Directory accounts to be security-suspended; but an advanced CSOC would also automate gathering or receiving additional threat intelligence feeds in order to collect more credential dump files.

Thus, it comes as no surprise that our Sensitive Information Alert Service is on the 2020 roadmap for improvements, to help our members with this exact scenario.

The past couple of years has seen AusCERT forging ahead with the ISAC model (Information Sharing &

Analysis Centre) of people, process and technology by first studying established methods in the USA such as the REN-ISAC, and then establishing our own Australian-based version. AusCERT has successfully led this initiative for the higher education sector with the establishment of CAUDIT-ISAC, and similarly for our Victorian Government members, and in 2019 we extended our ISAC model to the general AusCERT membership audience, currently operating in a beta mode.

We know that the technical threat intelligence available through our ISACs is valuable to our members; the knowledge provided by our analysts on how to use the technology more efficiently is even more valuable and automation is central to our 2020 roadmap.

This year, we will be releasing some new features in our Security Bulletins Service which includes advanced filtering options and programmatic methods

of accessing the feed (via an API). In addition to this, we have worked hard to increase the usefulness and utilisation of MISP, our threat sharing open-source platform; by assisting members with automations to increase the cyber security resilience of their organisations.

Throughout the remainder of this year, we will be targeting the most commonly used vendor platforms to influence their roadmaps to utilise standard, “best-practice” supported methods of threat sharing.

And last but not least, member feedback from last year emphasized the fact that they would like to utilise the expertise of AusCERT in a the form of a service we’re calling the “LiTouch Forensics Service” – essentially providing a solution for the gap between members’ internal capability, and that of commercial forensics vendors. We are anticipating that members will be able to access this affordable, defined-scope, high quality service in the later part of 2020.

Mike Holm - Senior Manager

CREDITS

Content and copywriting

Dr David Stockdale, Director

Mike Holm, Senior Manager

Geoff Thonon, Operations Manager

Colin Chamberlain, Principal Analyst

Laura Jiew, Events and Marketing Communications Coordinator

AusCERT membership team

Design

Orange Digital

TLP: WHITE



AUSCERT

AUSCERT.ORG.AU

**AUSTRALIA'S PIONEER
CYBER EMERGENCY RESPONSE TEAM**