AusCERT Year in Review 2020

Curated by Laura Jiew

FOREWORD

AusCERT state-of-the-union

In many ways, it seems like a lifetime since writing the foreword for the 2020 report where I reflected on the phenomenal rise of cyber activity and the resources available to cybercrime.

Much has occurred over the past twelve months, in all aspects of life, and cyber security has not been exempted. Daily life has changed, and we have been required to adapt in both our social environments and our workplaces. Many have pivoted to working from home using a variety of IT equipment, both old and new, patched, and unpatched, supported, and unsupported.

Additionally, our perception of what is "safe" vs. "unsafe" is very different when sat with a laptop at the kitchen bench with no one to remind us of the ever-present cyber threats. All this has changed the risk profile and sadly, to the cybercriminal, this was an opportunity and one that has been exploited significantly.

Criminals took advantage of the rapid (and often chaotic) transitions that many organisations went through in early 2020 which correlated to AusCERT experiencing a peak of reported member incidents for Quarter 1, 2020 in March.

In addition to the volume of activity, we also know that organisations that did not have an implemented strategy for secure remote working were significantly more likely to be impacted by some form of cyber disruption over those who were prepared.

Preparation is the key word.

We prepare through knowledge and planning with our knowledge informed by information, in this case, cyber threat intelligence (CTI).

Cyber threat intelligence comes in many forms from the operational through to strategic and, during 2021, AusCERT will be developing its capabilities to deliver more of this information, at all levels, to make your organisations safer.

You, the members of AusCERT, need good, reliable, and timely information about emerging threats to understand the landscape as it pertains to your organisation.

AusCERT also understands that no matter how good the intelligence, sometimes things do still go wrong. It is during times like these that the AusCERT team, as an independent, not-for-profit CERT can assist.

In 2020 we assisted with over three thousand eight hundred reported member incidents, on average fourteen incidents ("tickets") per day, with requests ranging from phishing takedowns to general support and all-things-cyber-security.

During 2021 we will be looking to expand the incident response services and offer greater levels of support at the times when help is most required.

The AusCERT team is constantly reminding itself of its mission, of being "*a centre of excellence in handling incidents and improving member's cyber security posture*". **The cyber security landscape is ever-changing, and AusCERT is passionate about engaging with members to empower their people, capabilities, and capacities**.

With such dedicated staff whose personal mission is to create a safer environment for the membership, we look forward to continuing to work with you in 2021

Dr David Stockdale – Director

MEMBERSHIP MATTERS

AS OF FEBRUARY 2021, AusCERT is made up of **605 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 Public Administration & Safety.**

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. As a 24/7 membership benefit, it is perhaps AusCERT's most focal service offering.

The below diagram is the statistics of incidents that required handling for the calendar year of 2020. Overall, AusCERT serviced 3819 tickets which resulted in an average of approximately 14 tickets per each business day of operation.

There are two further diagrams provided here which showcases the breakdown of incident classifications by month and incident classification types.

These tallies are sites that are located around the world that, when interacted with, affects the security of the constituency that AusCERT is serving.

AusCERT members can utilise AusCERT's considerably large overseas and local contact networks for removal of phishing and malware sites.

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.

In 2020, 4504 External Security Bulletins (ESBs) and 226 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.

In recent times, AusCERT has made a conscious move to make ASBs publicly available (apart from a minor few that will be exclusively locked off to members), especially when the data is critical to Australia and not found elsewhere - part of our team's *greater good* philosophy.

MEMBER SECURITY INCIDENT NOTIFICATIONS (MSINs)

AusCERT members benefit from its 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. 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.

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 and has been committed to its constituency, quality services and support from membership within AusCERT.

During 2020, and despite the Covid-19 pandemic, 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), continued to prove itself as a valuable member resource through 2020.

It comes as no surprise to everyone that 2020 has been a particularly challenging year.

As a team, we've summarised our key achievements and milestones via the following blogpost (https://auscert.shorthandstories.com/the-year-that-was-2020/index.html) which we released late last year.

AUSCERT2020 "WE CAN BE HEROES"

4 days of programming, 5 streams, over 80 hours of content, 2 live recording studios, close to 80 remote presenters, over 30 sponsor exhibitors and over 1000 delegate registrations.

Witnessing our delegates, speakers and colleagues rise to the occasion in the spirit of camaraderie and innovation was an amazing experience.

Here's a piece on the conference which we'd written recently: "**The heroes of AusCERT2020** ... *the women in security who made it happen*" (https://auscert.shorthandstories.com/-the-heroes-of-auscert2020-iwd2021/index.html)

Catch up on our conference content via our YouTube channel:

WHAT'S NEXT

Closing remarks

The year 2020 turned out to be an opportunity for AusCERT to learn to communicate in new and different ways.

Our internal communication processes were disrupted by the sudden shift to full time remote working, but not in the ways you may think. The team had already been utilising various office "productivity" tools to stay in touch, share project tasks, collaborate on documentation, organise video calls and kept up with these business practices albeit within different surroundings.

As the disconnection became more glaring, the team took steps to re-introduce that informal chatter that we had been familiar with to cultivate new ideas, unite the team and, well, make us "feel good"!

The point that AusCERT would like to reiterate here is that collaboration and staying connected is even more important than ever, and that is why **when we turned towards 2021 and re-defined our strategic goals, Engagement – was one of three key points.**

Our other two strategy points cover Cyber Threat Intelligence and Incident Response, which forms the core business of a modern CERT. **Read more about our 2021 strategy here** (https://www.auscert.org.au/blog/auscert-what-expect-2021)**.**

For example, we know that each of our members find unique value propositions in their membership with AusCERT.

The type of engagement you've told us you want varies from one member to the next, and that's why we tried really hard to bring information to you faster in the year 2020 and beyond so that you can better utilise our expertise.

This year we are confident that our members will **continue tapping into our AusCERT expertise** – our intention is to increase or introduce new data sets such as additional types of indicators of compromise for automation and response, tactical and analytical information on current threats and we will also provide improved methods for filtering vulnerability data.

The plan does not stop with data flowing *out* of AusCERT though; we will soon bring you new and improved ways to send incidents *in* to AusCERT. **This process improvement will enable us to analyse more incidents**, so we can share more (sanitised) data back with our members.

Our LiTouch Forensics capability remained as a *beta* program in 2020, but we know it is highly valuable to members and we are working to bring this as an official offering in the later part of 2021.

In the immediate future, we foresee phishing as a mainstay of the sector, manifesting itself as the initial vector for large scale, serious attacks.

As a bonus, for each phish AusCERT detects or that members notify us about, **AusCERT will immediately share the URL indicator(s) b**ack to all members. Many of you are already using the Malicious URL Feed in your organisation's content filters, EDR or similar control protocols. If not, we highly encourage you to implement these steps within your organisation.

Members, even if you do not have an incident to lodge or request to submit with our team of analysts, you may simply wish to discuss cyber security matters with peers.

You can engage with fellow members and the AusCERT Team by joining us at the AusCERT - Members Slack space by logging in with your member portal credentials. This channel is a great way to ask others what types of threats they are seeing or to trouble-shoot problems in the immediate instance.

Our regular **webinars and events** are another way you can engage with us and learn about current trends, and of course our **annual AusCERT cyber security conference** this year (AusCERT2021) will feature world-class speakers and plenty of opportunities for you to engage with other cyber security professionals in a relaxed atmosphere, virtually or at our new venue, The Star Gold Coast.

Want to stay up-to-date and in the loop with trending news and alerts within our sector? Feel free to **subscribe to ADIR, the AusCERT Daily Intelligence Report** - a daily summary of curated information security news. You can do so via your AusCERT member portal or send us an email at adir-join@lists.auscert.org.au (mailto:adir-join@lists.auscert.org.au).

Regardless of how you chose to engage with us in 2021 as an AusCERT member, we do hope you benefit from our workstreams on incident response and cyber threat intelligence and **we wish you a productive and successful year ahead!**

Mike Holm – Senior Manager

The AusCERT Year in Review 2020 has been made possible by the following contributors:

Dr David Stockdale
Mike Holm
Geoff Thonon
AusCERT Business Team
Orange Digital