Phishing take-down

In 2019, AusCERT completed an innovative project to automate the process of monitoring malicious websites utilising Osprey.

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.

In Q3, Osprey added a total of 813 new URLs to its monitoring database, and the following statistics indicate the number of new URLs added per month.

PHISHING TAKE-DOWN (Q3 2020)

July 284, August 217, September 312 — New URLs added to Osprey
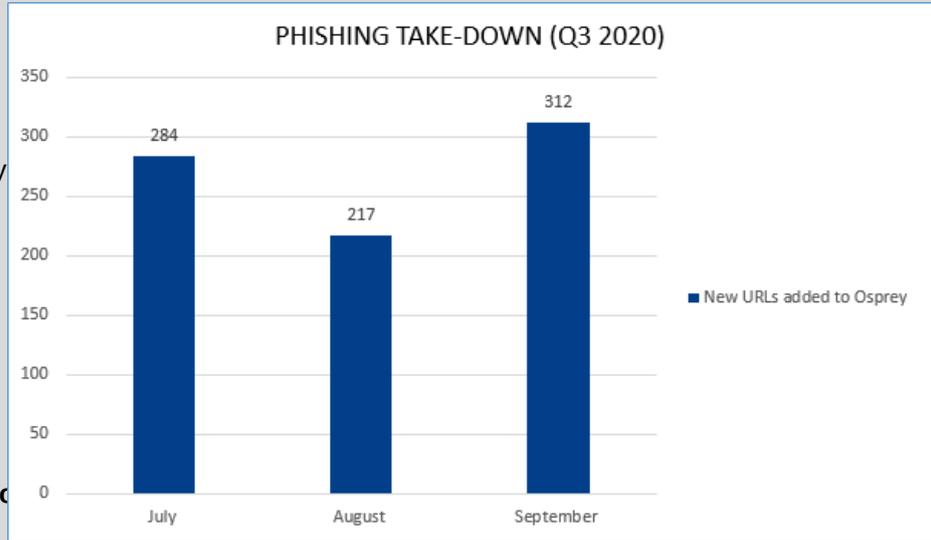
Security bulletins

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.

I**n Q3 2020, 1162 External Security Bulletins (ESBs) and 44 AusCERT Security Bulletins (ASBs) were published.**

In comparison, Q2 2020 saw AusCERT publish 1135 ESBs and 50 ASBs.

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.


SECURITY BULLETINS (Q2 2020 - Q3 2020)

Q2: ESB 1135, ASB 50; Q3: ESB 1162, ASB 44
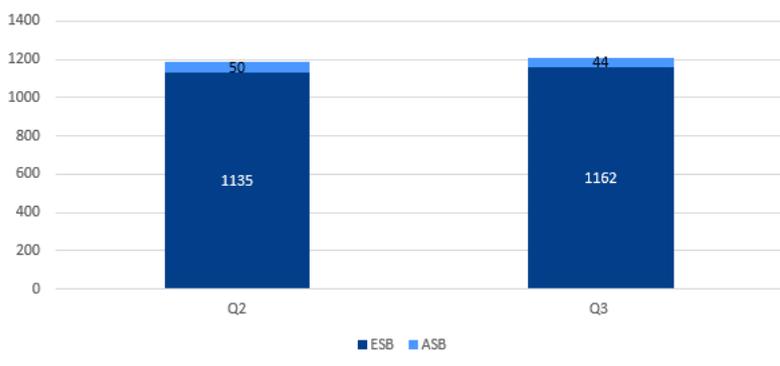
Member Security Incident Notifications (MSINs)

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.

These notifications are a mix of Indicators of Vulnerabilities (IoV) and Indicators of Compromise (IoC). Incident classifications include: Vulnerable Service, Malicious Code and Intrusions.

MEMBER SECURITY INCIDENT NOTIFICATIONS (Q3 2020)

Category	Count
Vulnerable service	716
Malicious code	61
Intrusions	8
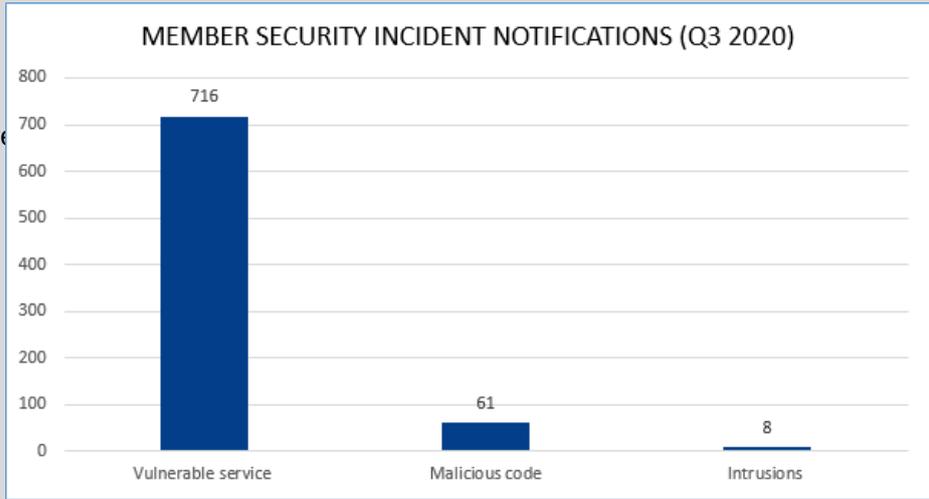
19th Annual AusCERT Cyber Security Conference (15th - 18th September)

Virtual AusCERT2020

We Can be Heroes

conference.auscert.org.au
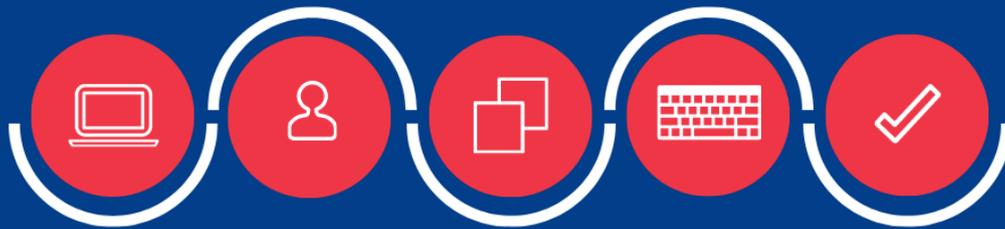
REGISTRATIONS

1153 delegates registered | Over 893 logged in | Over 650 delegates tuned in to each keynote and plenary session

PRESENTERS

78 presenters: from ANZ, USA, UK, Europe, UAE, Russia and Japan | Two female keynotes: CODE BLUE JP and eSafety Australia | Over 60 organisations represented | 2 live broadcasting studios

PROGRAM

4 days | 5 streams | Over 80 hours of content | 3 keynotes | 4 plenaries | 40 talks |14 tutorials | Over 12 information and cyber security themes covered

INTERACTIVE ACTIVITIES

3 offerings: Capture the Flag, Secure Code Warrior tournament, Online Cyber Escape Room | Over 30 sponsors in Sponsor Hubs 1 and 2 | Virtual Gala Dinner

I WAS A HERO AND I STAYED HOME

AusCERT partnered with mental health charity LIVIN' and donated all registration proceeds to support their cause "Breaking the stigma of mental health."

Other key successes in Q3 2020

The past quarter has seen AusCERT taking on uncharted territory in the form of hosting our annual (19th edition) cyber security conference AusCERT2020 virtually.

Our team is so very proud to have been able to deliver the conference despite the challenges it presented.

We hope our delegates enjoyed their virtual conference experience and we look forward to seeing everyone SOAR with cyber in 2021.

In addition to our key event AusCERT2020, the team also ran a number of webinar sessions in Q3, namely:

- 22nd July - Malicious URL Feed
- 5th August - Security Bulletins
- 19th August - Phishing Takedowns

All of these webinars were recorded and shared on our public YouTube channel: www.youtube.com/AusCERT

And last but not least, Q3 saw the team working on a number of key external communications and public relations pieces, some of which were picked up by major news channels such as iTnews and ZDNet:

- 30 July There's a hole in the boot
- 6 August AusCERT mailout: ProctorU breach
- 3 September AusCERT investigating a data dump claimed to be from the Department of Education
- 7 September AusCERT at the forefront of Cybersecurity and AusCERT2020 "We Can be Heroes"