AUSCERT

REPORT FOR QUARTER 2, 2020

www.auscert.org.au | auscert@auscert.org.au

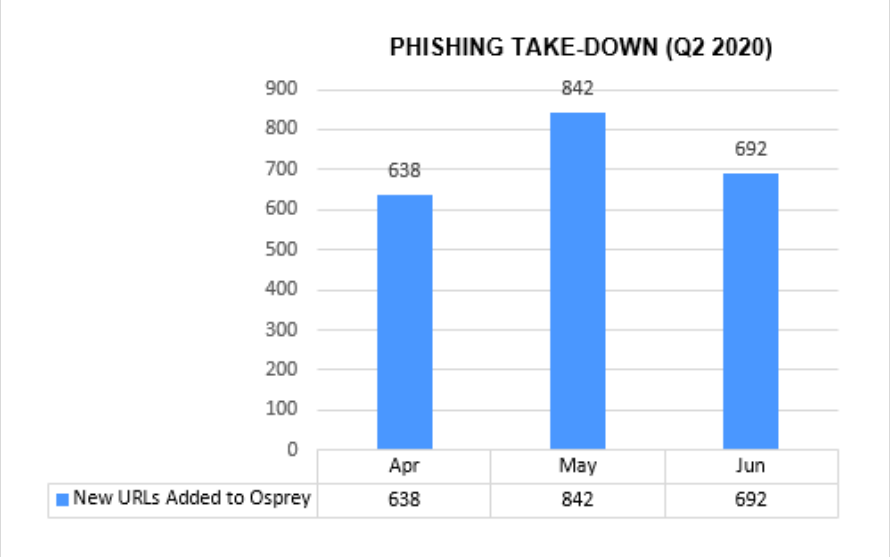
Phishing take-down

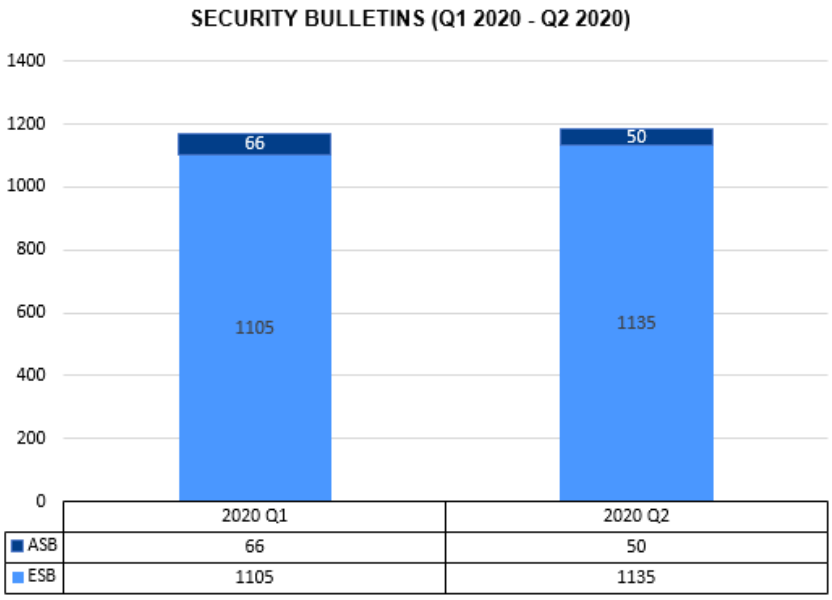
In 2019, AusCERT completed an innovative project to automate the process of monitoring malicious websites utilising Osprey.

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 Q2, Osprey added a total of 2172 new URLs to its monitoring database, an increase from Q1 and the following statistics indicate the number of new URLs added per month in this quarter.





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 Q2 2020, 1135 External Security Bulletins (ESBs) and 50 AusCERT Security Bulletins (ASBs) were published.

In comparison, Q1 2020 saw AusCERT publish 1105 ESBs and 66 ASBs.

For context, 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.

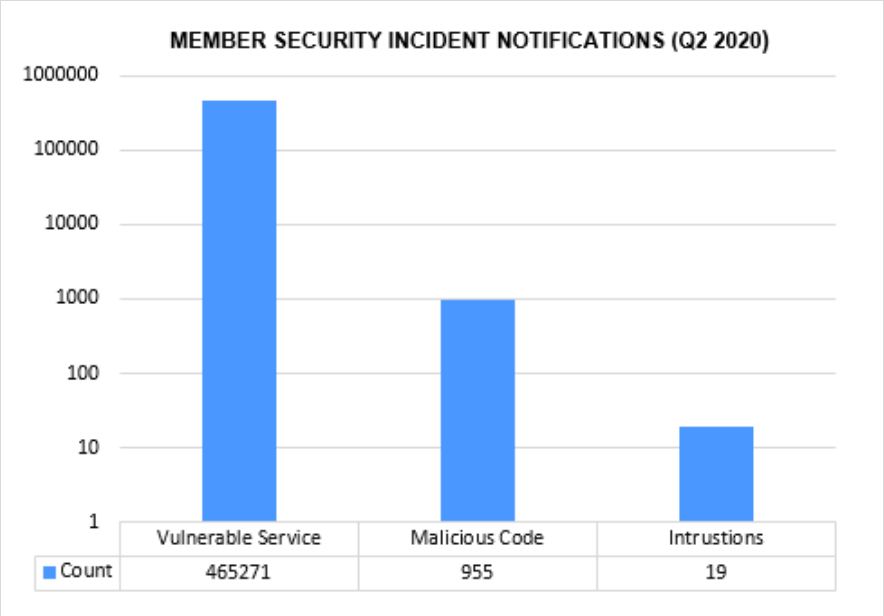
Member Security Incident Notifications (MSINs)

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.



Other key successes in Q2 2020

The past quarter has seen AusCERT overcome a number of challenges as a result of the Covid-19 pandemic. Nevertheless, the team has managed the transition to remote-working seamlessly and our member incident hotline continued to operate 24/7 during this entire period.

In addition to this, the AusCERT team responded quickly and efficiently to a number of things that took place within the industry, namely:

- Responding to several critical vulnerabilities. Examples include: Citrix (NetScaler), the "Let's Encrypt" CAA Code Bug, Palo Alto, F5 BIG IP etc.

- And, most importantly the ACSC-issued "Copy-Paste" compromises which the Prime Minister, Scott Morrison highlighted via a nationwide press conference on the 19th of June. In particular, the team had produced a widely circulated how-to guide on the topic of How to use the YARA rules for the "Copy-paste compromises" advisory.

The past quarter also saw the establishment of a member Slack replacing our IRC channel leading to an increased interaction from members.

And last but not least, the AusCERT team has also pivoted and adapted to the ever-changing rules around mass events by bringing our AusCERT2020 conference into a virtual platform, hosting keynotes and speakers from very diverse organisations.