REPORT FOR QUARTER 1, 2020

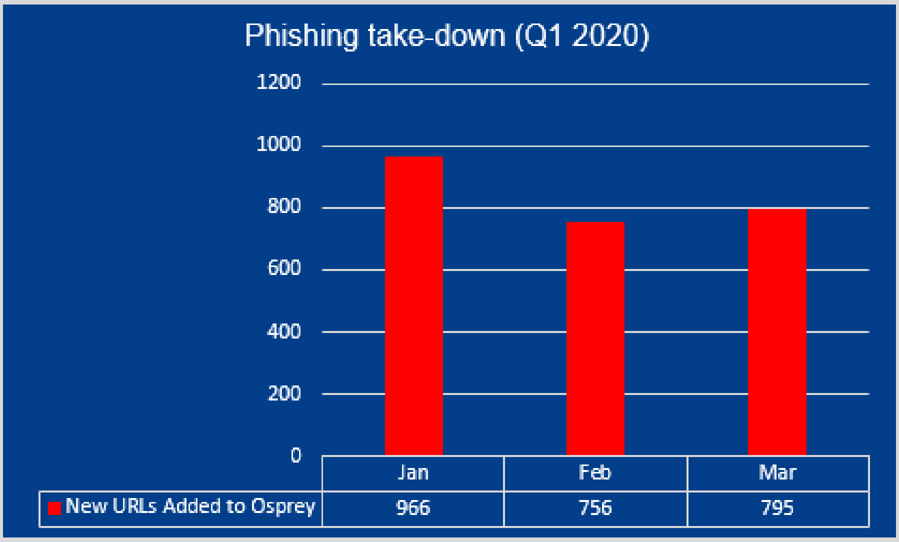
www.auscert.org.au | auscert@auscert.org.au

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 Q1, Osprey added a total of 2517 new URLs to its monitoring database, and the following statistics indicate the number of new URLs added per month.



	Jan	Feb	Mar
🟥 New URLs Added to Osprey	966	756	795

Security bulletins

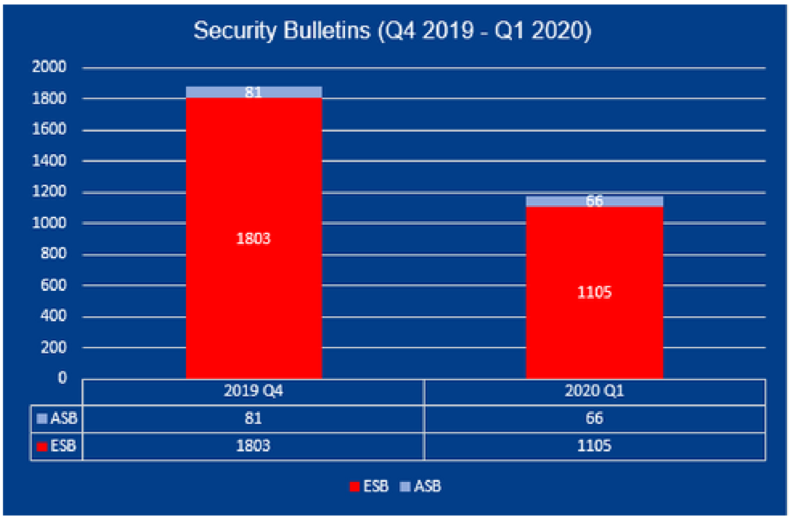
AusCERT distributes security advisories and bulletins to its members by email and publishes a portion of them to its public website.

Bulletins are published in a standardised format with a consistent approach to classifications of vulnerabilities, impacts and affected operating systems.

In Q1 2020, 1105 External Security Bulletins (ESBs) and 66 AusCERT Security Bulletins (ASBs) were published.

In comparison, Q4 2019 saw AusCERT publish 1803 ESBs and 81 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.



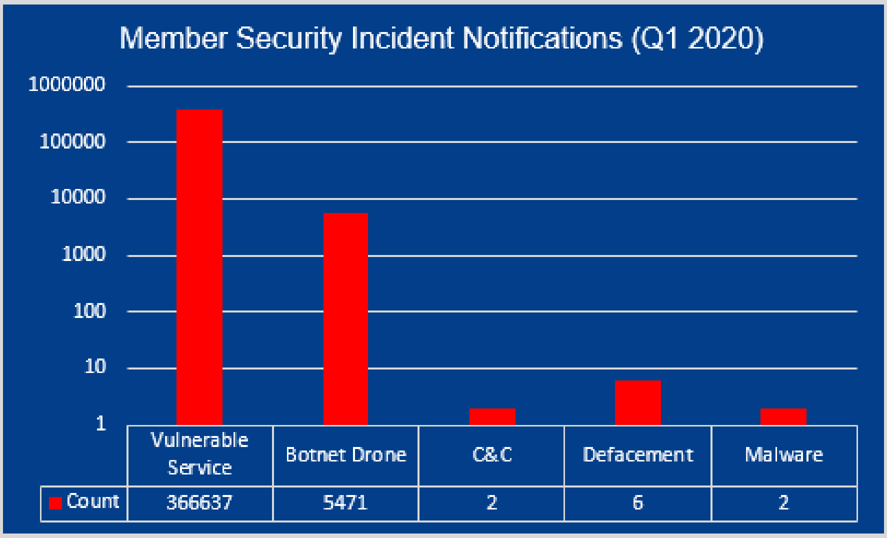
	2019 Q4	2020 Q1
▨ ASB	81	66
🟥 ESB	1803	1105

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, Botnet Drone, C&C, Defacement and Malware.



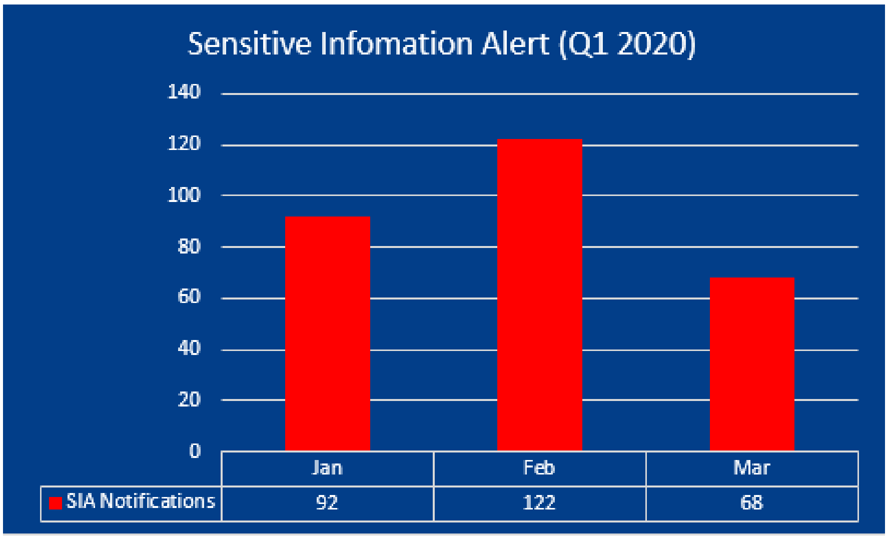
Sensitive Information Alert

Data breaches, credential dumps, and sensitive documents are uploaded to the public web every day by malicious actors, oblivious contractors, and even well-meaning staff.

We continuously monitor common dumping grounds for sensitive information, and alert members to any dangerous information found in public.

These alerts give members the best chance to quickly get on top of and contain the damage to your organisation from these kinds of leaks.

In Q1 2020, AusCERT issued 282 sensitive information alert (SIA) notifications to members for sensitive material found online by our analyst team which specifically targets a member organisation.


Sensitive Infomation Alert (Q1 2020)
Jan
Feb
Mar
🟥 SIA Notifications