Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

7 August 2020

Dr Sean Turner
Committee Secretary
Parliamentary Joint Committee on Law Enforcement
Department of the Senate
PO Box 6100
Parliament House
CANBERRA ACT 2600
AUSTRALIA

Dear Dr Turner,

The Australian Signals Directorate (ASD) appreciates the opportunity to make a submission to the Parliamentary Joint Committee on Law Enforcement in relation to criminal activity and law enforcement during the COVID-19 pandemic.

ASD has a legislative function to prevent and disrupt cybercrime activities conducted outside Australia under Section 7(1)(c) of the *Intelligence Services Act 2001*.

While ASD is not a law enforcement agency, we do provide technical advice and assistance to federal, state and territory law enforcement agencies in accordance with Sections 7(1)(e) and 7(1)(f) of the *Intelligence Services Act 2001*.

Further details about ASD's activities supporting law enforcement during the COVID 19 pandemic is contained in the attached submission.

Kind regards,

Rachel Noble PSM
Director-General
Australian Signals Directorate

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Signals Directorate Submission – Parliamentary Joint Committee on Law Enforcement

Role of the Australian Signals Directorate (ASD) in support of law enforcement

ASD has three principal missions: the collection of signals intelligence; our cybersecurity mission; and our cyber offensive role. In all cases, our primary imperative is to protect Australians and the integrity of Australian systems.

ASD's functions are set out in legislation, in particular, Section 7 of the Intelligence Services Act 2001. Our functions include:

- Obtaining intelligence about the capabilities, intentions or activities of people or organisations outside Australia (s7(1)(a))
- Providing material, advice and other assistance to Commonwealth and State authorities on matters relating to the security and integrity of information (cybersecurity) (s7(1)(ca))
- Providing assistance to the Defence Force in support of military operations (s7(1)(d))

In July 2018, the Australian Government expanded ASD's functions under the Intelligence Services Act to include the ability to prevent and disrupt, by electronic or similar means, cybercrime undertaken by people or organisations outside Australia (s7(1)(c)). This change also included the authority for ASD to prevent and disrupt cybercrime undertaken by, or enabled by, an Australian person offshore, in special circumstances, subject to authorisation by the Minister under Section 8(1)(iii) of the Act.

While ASD is not a law enforcement agency, in performing its functions, ASD has a range of specialised technical capabilities that can also be used to assist other government agencies in the performance of their own roles. This includes providing assistance to law enforcement and security agencies. This assistance function is clearly set out in the Intelligence Services Act (s7(1)(e) and s7(1)(f)).

ASD's support to law enforcement in combatting cybercrime

The ASD's Australian Cyber Security Centre (ACSC) supports federal, state and territory law enforcement agencies to combat cybercrime by hosting Australia's online portal for reporting cybercrime called ReportCyber. Individuals and businesses can report cybercrime incidents such as cyber abuse, online image abuse, online shopping fraud, romance fraud, identity theft, email compromise, internet fraud, ransomware or malware.

Once a report is submitted, it is referred based on Australian and New Zealand Policing Advisory Agency (ANZPAA) protocols to law enforcement agencies for triage and assessment. This reporting also assists the Australian Government to understand the scale and nature of online threats impacting our community, and it provides reporters with a reference number that can be presented to organisations as part of recovery efforts (such as telecommunications carriers, banks, and credit reporting bodies).

Over the first 12 months of ReportCyber's operation (1 July 2019 to 30 June 2020), the ACSC has received 59,806 cybercrime reports from individuals and businesses across Australia, which equates to an average of 164 cybercrime reports per day, or one report every 10 minutes. It is also worth noting that reporting cybercrime via ReportCyber is not compulsory, and as such, it is likely there is significant under reporting occurring.

ACSC Australian Cyber Security Centre

Cybercrime threat in Australia

Cybercrime is one of the most pervasive and endemic threats facing Australia – and the most significant threat in terms of overall volume and impact to individuals and businesses. The Cyber Security Review, led by the Department of the Prime Minister and Cabinet, found that cybercrime is costing the Australian economy up to $1 billion annually in direct costs alone. While the true cost of cybercrime to the Australian economy is difficult to quantify, industry estimates have previously placed cyber security incidents as high as $29 billion annually[1].

Cyber criminals follow the money. Australia's relative wealth, high levels of online connectivity, and increasing delivery of services through online channels make it very attractive and profitable for cybercrime actors. The increasing interdependence of technology and systems in cyberspace creates new and profitable opportunities for malicious cyber actors.

Of particular concern are transnational cybercrime syndicates and their affiliates, who develop, share, sell and use sophisticated tools and techniques. There are lucrative underground marketplaces offering cybercrime-as-a-service, or access to high-end hacking tools that were once only available to nation states.

As a consequence, malicious actors with minimal technical expertise can now purchase illicit tools and services to generate alternative income streams, launder the proceeds of traditional crimes or undertake network intrusions on behalf of more sophisticated adversities.

ASD has observed cybercrime actors are clearly opportunistic and capitalise on natural disasters or significant events to generate profit. They seek to prey on vulnerable people, consumers and organisations, using fear and urgency tactics to distribute malware or steal personal and financial information. Cyber criminals regularly attempt to trick victims into revealing sensitive information, or donating money to fraudulent charities or causes. ASD observed examples of this during the recent bushfire crisis, where a number of fraudulent charity scams were targeting Australians based on this theme.

Cybercrime during the COVID-19 pandemic

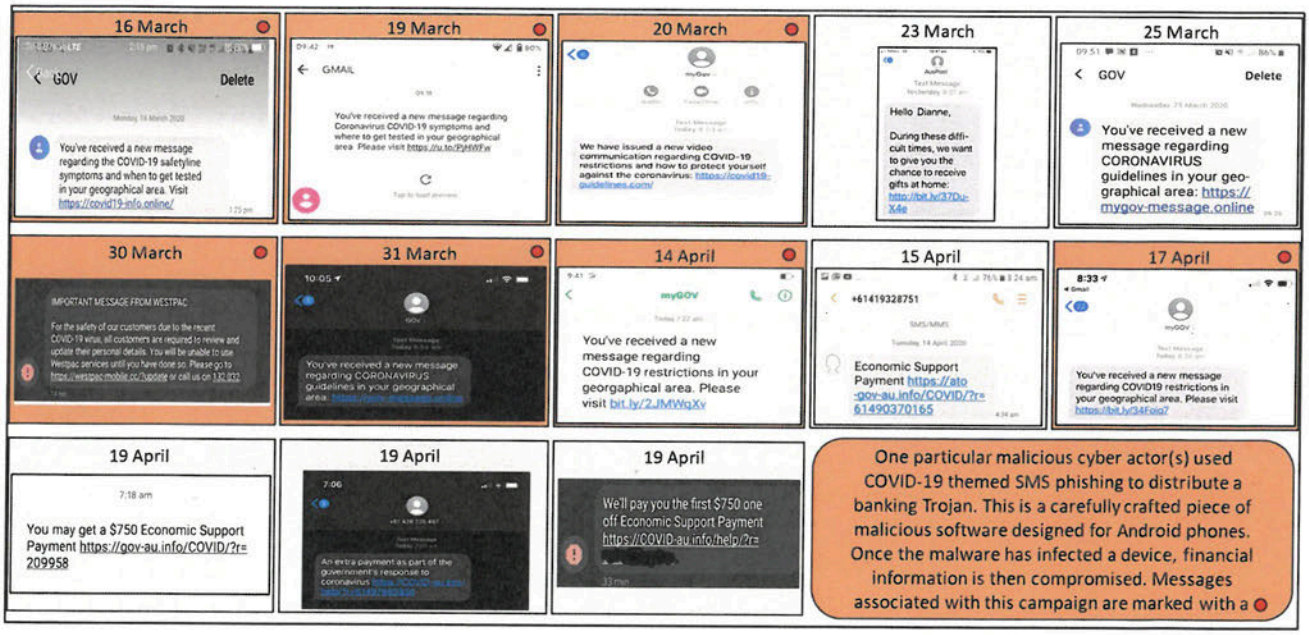
During the onset of the COVID-19 pandemic, ASD observed cybercrime actors adapting a range of existing methodologies to take advantage of increasing numbers of Australians looking for information about COVID-19 testing, social distancing restrictions and government assistance.

In February 2020, the ACSC identified that cybercrime actors started registering COVID-19 themed websites in Australia and overseas. These websites were designed to host malicious software (malware) or harvest personally identifying information. To direct unsuspecting Australians to these malicious websites, cyber criminals distributed a range of different email and SMS phishing campaigns, often impersonating government agencies or other trusted organisations. The cyber criminals behind these phishing campaigns were quite agile, adapting the messages to closely align with breaking developments, such as government relief payments or public health guidance, within days, even hours, of these announcements occurring (see Figure 1). The ACSC, in conjunction with the Australian Federal Police, tracked a particular malicious actor(s) that was using SMS phishing to distribute a banking Trojan, which is a specific form of malware designed to steal financial information.

[1] https://news.microsoft.com/en-au/features/direct-costs-associated-with-cybersecurity-incidents-costs-australian-businesses-29-billion-per-annum/

ACSC Australian Cyber Security Centre

Figure 1: Examples of COVID-19 SMS phishing campaigns



To raise awareness about this malicious COVID-19 themed cyber activity, the ACSC released two public threat updates that detailed the various methodologies being used by cyber criminals, and the steps that individuals and businesses can take to protect themselves.

- https://www.cyber.gov.au/threats/threat-update-covid-19-malicious-cyber-activity
- https://www.cyber.gov.au/threats/threat-update-covid-19-malicious-cyber-activity-20-apr-2020

The ACSC also worked closely with our law enforcement and industry partners to actively disrupt or prevent this malicious COVID-19 themed cyber activity. For example, between 10 March and 30 June 2020, the ACSC disrupted (i.e. blocked for end users and/or website take-down issued and actioned) over 170 malicious COVID-19 themed websites, with assistance from Australia's major telecommunications providers, such as Telstra and Optus as well as major technology providers Google and Microsoft. The success of these disruption activities was greatly assisted by the close working relationship that the ACSC has with the telecommunications sector and major technology providers.

In parallel, ASD undertook an offensive cyber campaign against the offshore cyber criminals behind some of these COVID-19 cybercrime activities. Those operations included disabling online infrastructure used by the cyber criminals and blocking their access to stolen information. The Minister for Defence announced this publicly on 7 April 2020.

Overall, there was a modest increase in cybercrime during the COVID-19 pandemic (February 2020 – June 2020, see Figure 2). Over the period from 1 July 2019 to 31 March 2020, the volume of cybercrime reporting in Australia remained fairly stable, with a monthly average of 4,503 reports. Then in April 2020 there was a bulk extortion campaign that resulted in 3,793 cybercrime reports – 44% of all cybercrime reports in April related to this one campaign. This was not related to COVID-19, but rather a malicious actor(s) had emailed thousands of Australians and threatened to release sensitive information to the recipients' friends and family unless they paid an amount in untraceable crypto currency. The ACSC issued an alert on this campaign through cyber.gov.au, the StaySmartOnline service and social media channels, together with the ReportCyber portal.

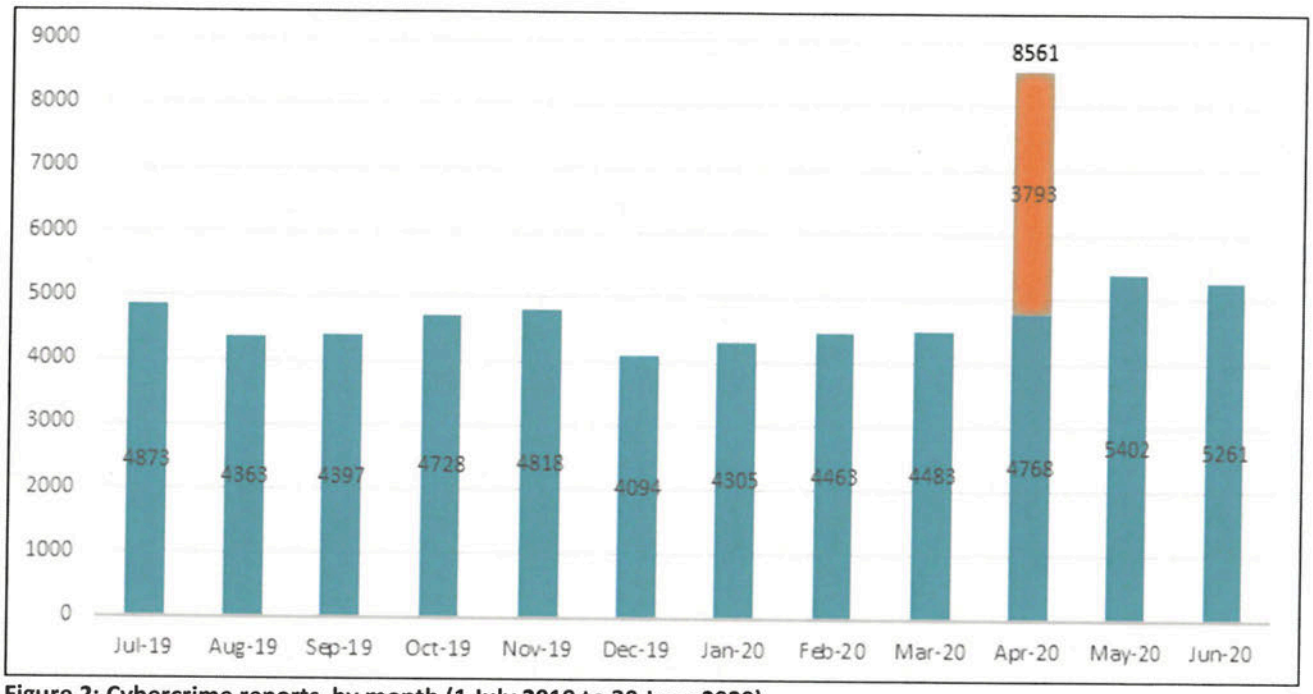


Figure 2: Cybercrime reports, by month (1 July 2019 to 30 June 2020)

Since early March 2020, the ACSC and our federal, state and territory law enforcement partners were closely monitoring all reports for a spike in COVID-19 related cybercrime. In total, 287 cybercrime reports since 1 March 2020 were associated with COVID-19 online scams and fraud, representing around 1.3% of all reported cybercrime.

ASD assess that the recent increase in May and June 2020 is correlated to a rise in cybercrime reports associated with online fraud. These are incidents where individuals and businesses have lost money through deception, such as online shopping, investment or romance scams. The proportion of cybercrime reports categorised as fraud in May (43.4%) and again in June (44.6%) was 3-4 percentage points higher (39.9%) than the total proportion since 1 July 2019. The ACSC considers this recent increase in cybercrime reports is most likely associated with a combination of:

- increased awareness raising by the ACSC and other federal, state and territory agencies, including widespread social media messaging about online scam and fraud activity; and
- a significant increase in Australians working from home and shopping online as a result of social distancing during COVID-19.

Since early March 2020, the ACSC has responded to 26 cyber security incidents affecting COVID-19 essential services and/or major national suppliers, including across the health, water, transport/logistics, agriculture and energy sectors. The ACSC provided technical advice and assistance to the affected organisations in remediating their systems and preventing future malicious cyber activity.

The ACSC assesses that ransomware attacks are most commonly associated with financially motivated cybercrime actors. These types of incidents can cripple organisations that rely on computer systems to function, by encrypting all connected electronic devices, folders and files and rendering them inaccessible. Cyber criminals will then demand a ransom in return for the decryption keys, often in the form of untraceable crypto currency. In responding to ransomware incidents, the ACSC focuses on providing technical advice and assistance to the affected organisation in restoring their network. At the same time, the ACSC supports the Australian Federal Police who lead the criminal investigation into the actor responsible.