REDITE.
Cyber & Data Security

AUTHORISED DISTRIBUTOR SentryBay ASIA PACIFIC

Annual Cyber Threat Report

July 2019 - June 2020

This report summarises the key data points from the ACSC Annual Cyber Threat Report 2019-20.
The link to the full study can be found at the end of this report.

Contents

REDITE.
Cyber & Data Security

AUTHORISED DISTRIBUTOR SentryBay ASIA PACIFIC

SECTION 1: Key Findings

Cyber adversaries are harvesting personal information or user credentials to gain access to networks, or to distribute malicious content.

Over the past 12 months the ACSC has observed real-world impacts of ransomware incidents.
These typically originate from a user executing a file received as part of a spearphishing campaign.
Ransomware has become one of the most significant threats given the potential impact on the operations of businesses and governments.
Cybercriminals illicitly obtain user logins and credentials through spearphishing, before utilising remote desktop protocol (RDP) services to deploy ransomware on their targets.
Recovering from ransomware is almost impossible without comprehensive backups.

Phishing and spearphishing remain the most common methods used.

Malicious cyber activity is increasing in frequency, scale and sophistication.

$634,000,000

LOST TO SCAMS IN 2019

$634 million lost to scams in 2019. The Australian Competition and Consumer Commission's (ACCC) Targeting Scams 2019 report.

$29,000,000,000

COST TO THE ECONOMY

$29 billion is the estimated true cost of cybercrime to the Australian economy annually.

164 on average

REPORTS PER DAY

59,806 cybercrime reports at an average of 164 per day or approximately one report every 10 minutes since the launch of ReportCyber on 1 July 2019.

Most common categories of cybercrime reported:

39.86%

23,841

Fraud which relates to criminals obtaining benefit through deception, such as investment, shopping or romance scams.

32.40%

19,467

Identity-related crimes incorporating the theft and misuse of personal information was the second most common category.

22.15%

13,309

Cyber abuse crimes include things such as online harassment, sexting, cyber bullying and other forms of online abuse.

The ACSC assesses ransomware as the highest threat because:

- Ransomware requires minimal technical expertise
- Is low cost
- Can result in significant impact to an organisation, potentially crippling core business functions.

Covid-19

There was an increase in reported spearphishing campaigns and an increase of COVID-19 themed malicious cyber activity. Between 10 and 26 March 2020, the ACSC received over 45 pandemic themed cybercrime and cyber security incident reports, with the Australian Competition and Consumer Commission's (ACCC) Scamwatch receiving over 100 reports of COVID-19 themed scams. During March 2020, cybercriminals quickly adapted their phishing methods to take advantage of the COVID-19 pandemic.

SECTION 2: Visual Representation of Findings

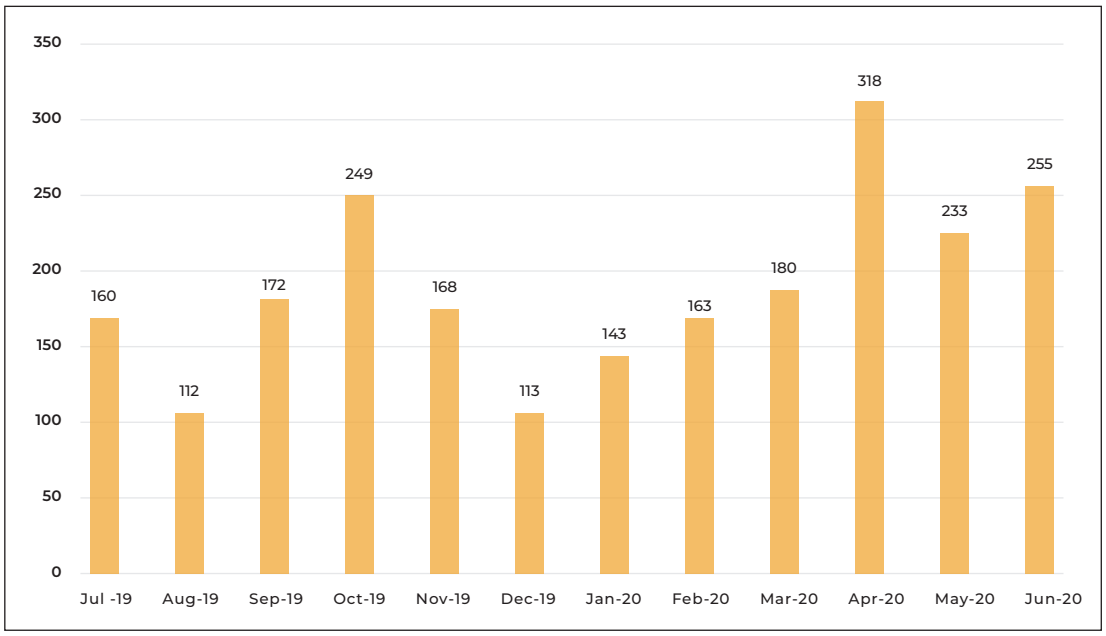


Figure 1:

Cyber Security Indicidents (monthly) (1 July 2019 - 30 June 2020)

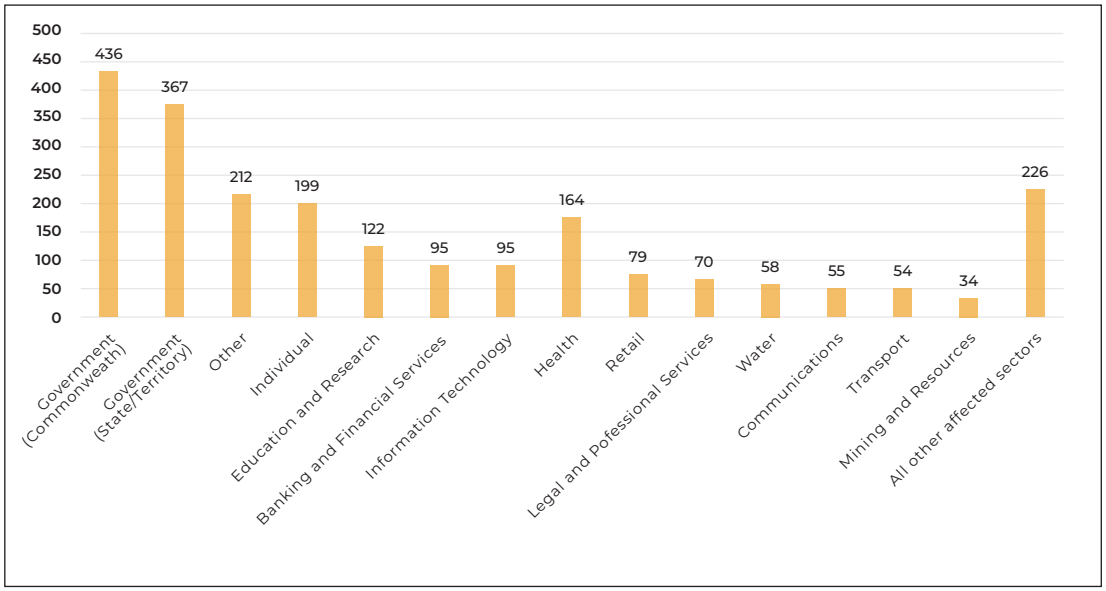


Figure 2:

Cyber Security Indicidents, by affected sector (1 July 2019 - 30 June 2020)

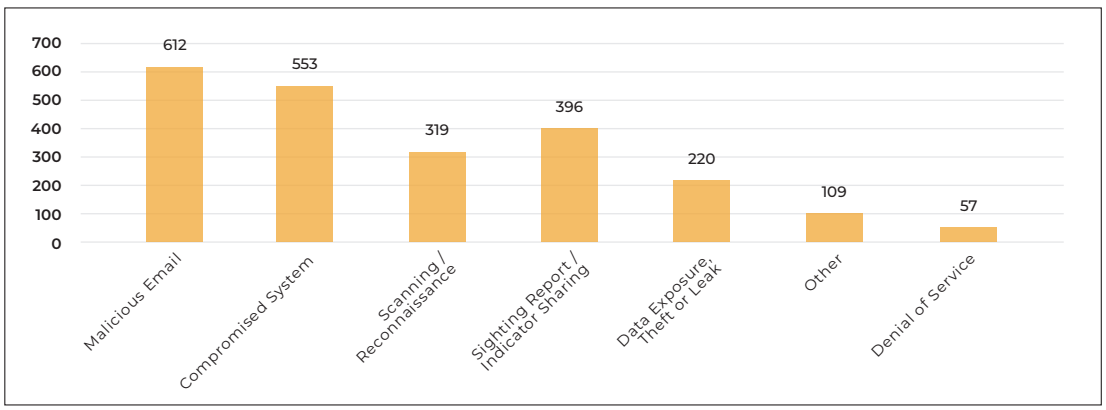


Figure 3:

Cyber Security Indicidents, by type (1 July 2019 - 30 June 2020)

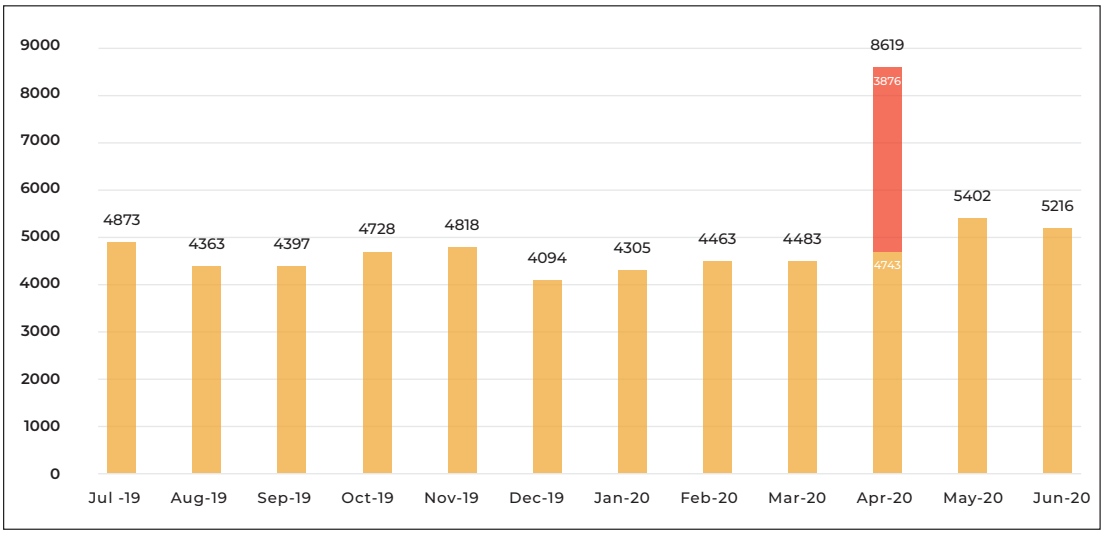
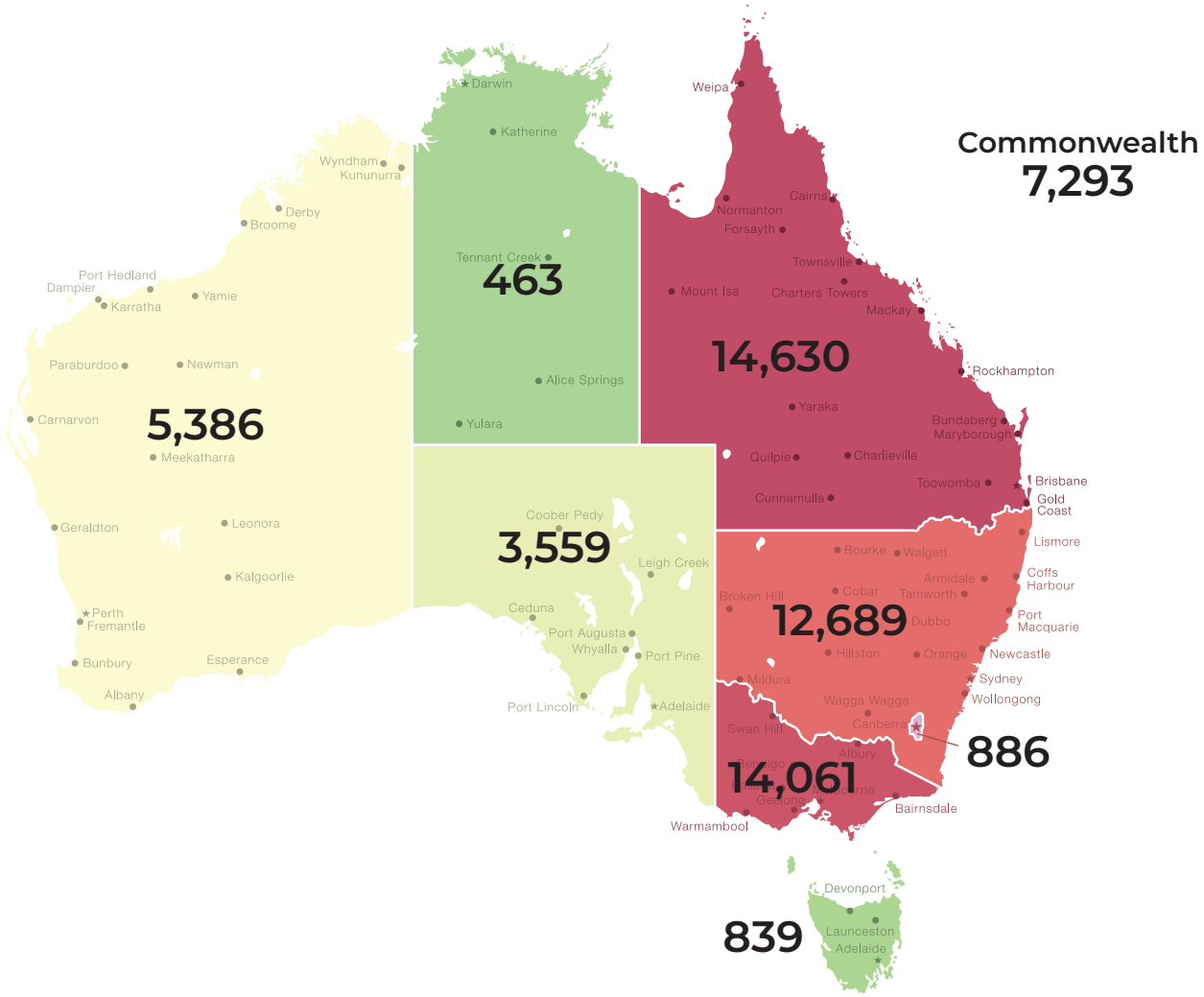


Figure 4:

Cybercrime Reports (monthly) 1 July 2019 - 30 June 2020)

Breakdown by Region



REDITE.
Cyber & Data Security

AUTHORISED DISTRIBUTOR SentryBay ASIA PACIFIC

Common Corporate Threats: Emotet and Trickbot

While there are numerous different malware and ransomware variants, the ACSC has responded to several incidents affecting organisations in Australia where an adversary has used a combination of **Emotet and Trickbot** as the initial access into a network and then deployed Ryuk ransomware.

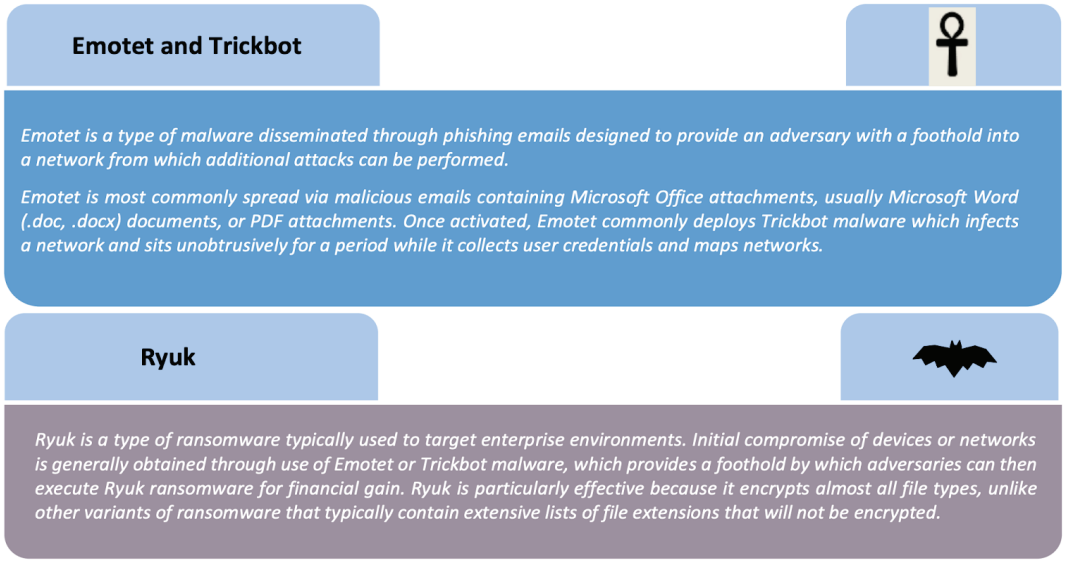


Figure 5:

A description of Emotet and Trickbot, and Ryuk

What Is Emotet?

Emotet malware generally arrives via email, often as part of a spam campaign. A user will click a malicious link, and the malware will download itself to that machine. It attempts to steal information such as victims' bank account numbers, wire transfer information, usernames and passwords. Its goal is to conduct fraudulent transactions to steal money from its victims' financial accounts or intercept and redirect valid transactions.

The malicious code puts itself persistently on a machine, attempting to steal login credentials by looking in the computer's registry. It also has been known to add plug-ins to browsers and to use keyloggers, so it can not only see stored usernames and passwords but also copy information as a user enters it in websites or forms.

The malware may try to propagate itself through the network, looking for open shares and attempting to log in to them and spread itself laterally to other machines.

Recent versions of the malware appear to have evolved to evade detection. Most common antivirus tools are based on signatures or file hashes. Because Emotet changes to look different to antivirus tools, it's harder to identify.

Before IT teams realize they have an infection, they often notice an increased number of account lockouts. Users can't log in because the malware on their machines is trying to spread itself throughout the network by logging into different network nodes. It does this by trying passwords from a dictionary of common, weak passwords and by reusing passwords that it learns from other systems.

For organizations with password policies that lock accounts after a set number of failed login attempts, this increase in lockouts is often the first notification IT staff have about the infection

Though ransom demands may exceed millions of dollars, affected organisations have reported experiencing other substantial financial impacts and data losses associated with recovering from a Ryuk Emotet and Trickbot 13 ransomware incident, regardless of whether they paid the ransom.

These additional costs include:

- **rebuilding and hardening networks**
- **implementing additional IT security controls**
- **time and money spent on data recovery**
- **absorbing the impact of lost productivity and revenue incurred while offline.**

SECTION 3: Case Studies

Case Study 1:

Widespread exploitation of vulnerable systems via Emotet malware

The Emotet malware campaign, first identified in 2014 as a banking Trojan disseminated via email, targets sensitive personal and financial information. It continues to evolve, enabling the download of malicious code such as ransomware onto infected devices. In October 2019, the ACSC identified that adversaries were using Emotet in a widespread campaign to target hundreds of vulnerable systems across Australia. At its peak, the ACSC detected over 4,500 malicious emails per day including nearly 50 variations of malicious emails used to infect systems. The campaign resulted in the networks and systems of at least 22 Australian organisations being infected. In response, the National Cyber Security Committee (NCSC) activated Australia's Cyber Incident Management Arrangements (CIMA) to 'Level 3 – Alert'. These arrangements empowered cooperation between the ACSC and State and Territory governments to undertake increased monitoring, intelligence sharing and widespread distribution of mitigation advice to vulnerable organisations, emphasising the need to implement urgent protections. In November 2019 the NCSC successfully mitigated the threat posed by Emotet during this campaign through coordinating the development, collection and sharing of indicators and tradecraft, as well as public messaging by Australian Governments to ensure organisations took appropriate action to mitigate the threats. As a result, the CIMA was returned to 'Level 5 – Normal Conditions'.

Case Study 2:

Consulting firm is tricked into sending $240,000 to fraudster in Malaysia

In September 2019 a 36-year-old woman who works in the finance section of an Australian consulting firm received an email from her boss requesting urgent payment of an invoice to a supplier in Malaysia. At the time her boss was on a work-related trip to Malaysia and the email was sent from his personal email account which he had used on previous work trips. The woman quickly organised payment of the AUD$240,000 invoice from the company account and replied to the email, providing a screenshot of the transaction. When her boss returned a few days later, he discovered his personal email account had been compromised and the funds had been paid into a fraudster's account. The matter was referred to police for assessment.

Case Study 3:

Adversaries targeting Citrix Vulnerability CVE-2019-19781

On 17 December 2019, Citrix disclosed the existence of a vulnerability in Citrix Application Delivery Controller (ADC) and gateway devices known as CVE-2019-19781. If exploited successfully, this vulnerability would allow an adversary to execute code, gain unauthorised access to resources and deploy malware on an affected Citrix device. The ACSC released information on 25 December 2019 and 30 January 2020 about the Citrix vulnerability to alert organisations to advise on how to detect and mitigate compromises resulting from the Citrix vulnerability. On 10 January 2020, a technical proof-of-concept script was released publicly outlining how the Citrix vulnerability could potentially be exploited. From this date the ACSC observed adversaries scanning and attempting to exploit the Citrix vulnerability. Although Citrix did not have software patches available upon vulnerability disclosure, they provided an interim protection measure while they developed a patch. Citrix released software patches for this vulnerability from 19 to 24 January 2020. The ACSC observed actors using this vulnerability to compromise networks, to then deploy ransomware, cryptominers and other malicious software.

REDITE.
Cyber & Data Security

AUTHORISED DISTRIBUTOR SentryBay ASIA PACIFIC

SECTION 4: Recommendations on Securing Corporate Devices

Cyber threats are only going to increase as we continue to transition to a digitally dependant and remote work environment.

With over 230,000 new malware threats created daily, and the challenges that corporates face with unmanaged devices it's imperative that smart investments are made in reputable security measures, that are able to respond to evolving threats.
No matter the security built into cloud ecosystems or network infrastructure, if malware is already present on the end user devices connecting to the corporate environment, data will be compromised.

SentryBay Armored Client protects the endpoint no matter the threats already present on the device, through kernel level anti-keylogging software and additional patented security measures.

With over 5 million users secured globally, SentryBay Armored Client can be trusted to secure BYOD, managed and unmanaged endpoint devices. Contact us to request more information or book a demo.

https://redite.co

Get more information on SentryBay Armored Client:

www.redite.co

Link to complete report:

https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf