

SINGAPORE CYBER LANDSCAPE

2018



CONTENTS

SINGAPORE CYBER LANDSCAPE 2018

Copyright © 2019

By Cyber Security Agency of Singapore

With contributions by the Defence Cyber Organisation,
Defence Science and Technology Agency, DSO
National Laboratories, Government Technology
Agency of Singapore and Singapore Police Force

All rights reserved.

ISBN: 978-981-14-1612-5

Designed by:
APT811 Design & Innovation Agency
www.apt811.com

Foreword	3
Overview of Cyber Threats in 2018	4
Chapter 1 – Spotlight on Cyber Threats	8
<i>Advanced Persistent Threats</i>	10
<i>Website Defacements</i>	12
<i>Phishing URLs</i>	14
<i>Malware</i>	16
Chapter 2 – Target.SG	20
Target.GOV.sg <i>Case Study – Cyber-attack on SingHealth</i>	22
Target.EDU.sg <i>Case Study – Cyber-attack on Universities</i>	26
Target.ORG.sg <i>Case Study – Crypto-jacking</i>	28
Target.YOU.sg <i>Case Study – Nearly@scammed.com</i>	30
Chapter 3 – Singapore’s Cybersecurity Strategy – Developments in 2018	32
Pillar One: Building a Resilient Infrastructure	36
Pillar Two: Creating a Safer Cyberspace	38
Pillar Three: Developing a Vibrant Cybersecurity Ecosystem	40
Pillar Four: Strengthening International Partnerships	44
Looking Ahead: Anticipated Trends	46
Glossary	50
Contact Details	52



FOREWORD

Cybersecurity incidents made some of the biggest headlines in 2018. Data breaches, in particular, were reported across multiple industries. Facebook, Cathay Pacific and Marriott were just some of the high-profile organisations that were hacked and had sensitive information stolen.

Singapore was not spared as well. We were hit by the most serious data breach in our history – 1.5 million SingHealth patients had their non-medical personal particulars illegally accessed and copied. As cyber threats grow in scale and sophistication, it is clearly no longer a question of “if”, but rather “when” an attack will hit us. Even as we strive to make our systems as secure as possible, it is imperative that we respond to an incident swiftly, robustly and decisively. The cyber-attack on SingHealth was a stark reminder for us to push further in our cybersecurity efforts collectively as a nation. On the international stage, Singapore remains firmly committed to the establishment of a rules-based international order in cyberspace; and condemns all malicious cyber activities, which threaten the safety and security of Singapore and Singaporeans.

2018 also saw significant progress in enhancing Singapore's cybersecurity. We passed and implemented the Cybersecurity Act, which provides a legal framework for the oversight and maintenance of cybersecurity in Singapore. To nurture a vibrant cybersecurity ecosystem, we launched initiatives such as the Industry Call for Innovation, which laid the ground for long-term, holistic cybersecurity investments, and the

Smart Nation Scholarship, to support talented students pursuing a career in cybersecurity. In addition, the establishment of the \$30 million ASEAN-Singapore Cybersecurity Centre of Excellence underscores Singapore's efforts to build regional cyber capacity and promote international collaboration.

Singapore marks its Bicentennial Commemoration in 2019. This journey over the last 200 years has seen us develop from a small trading outpost to a global digital hub. As we advance towards our vision of a Smart Nation, cybersecurity is a vital prerequisite and key enabler – the invisible glue that instils trust and confidence in our digital plans. We hope this third edition of the Singapore Cyber Landscape will provide useful lessons from past incidents, so that we can better prepare ourselves for the digital future. Let us keep Singapore's cyberspace safe and secure, together.

A handwritten signature in black ink, appearing to read "David Koh".

David Koh
Commissioner of Cybersecurity and
Chief Executive
Cyber Security Agency of Singapore

OVERVIEW OF

CYBER THREATS IN 2018



TIMELINE OF SELECTED CYBER INCIDENTS IN 2018

GLOBAL INCIDENTS

- APT-attributed malware (nicknamed 'Olympic Destroyer') disrupted Opening Ceremony of the PyeongChang Winter Olympic Games
- Largest Distributed Denial-of-Service (DDoS) attack in history on unidentified US-based service provider
- SamSam ransomware disrupted Atlanta's municipal services

LOCAL INCIDENTS

JAN

FEB

MAR

APR

MAY

JUN

JUL

AUG

SEP

OCT

NOV

DEC



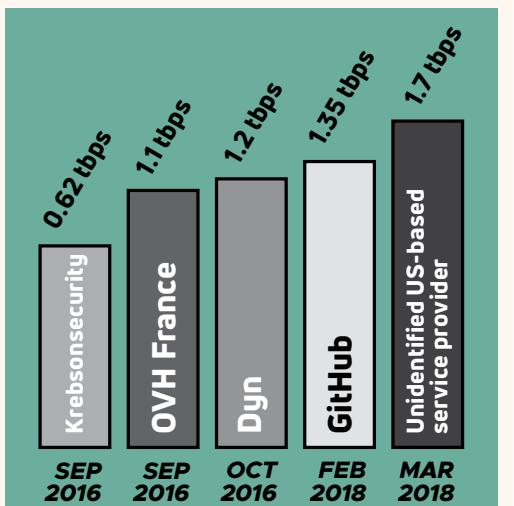
- Ransomware attacks hit Port of San Diego
- Facebook data breach affected 30 million users
- Financial information of 429,000 passengers stolen in British Airways data breach

- Cathay Pacific Airways data breach affected 9.4 million passengers

- Guest information stolen from 383 million Marriott International accounts

- Personal details of German politicians exposed

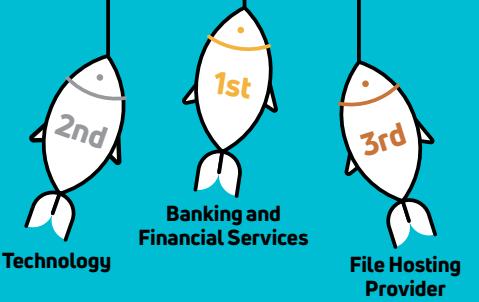
DDoS ATTACK PEAKS



RECORD PEAKS OF DISTRIBUTED DENIAL-OF-SERVICE ATTACKS – A COMPARISON

In 2018, the largest Distributed Denial-of-Service (DDoS) attack ever recorded was conducted using a relatively new method. As threat actors find new attack methods, even higher peaks of DDoS attacks may be seen.

PHISHING



16,100

phishing URLs with a Singapore-link were detected.

MALWARE

21

Cases of [ransomware](#) were reported to SingCERT

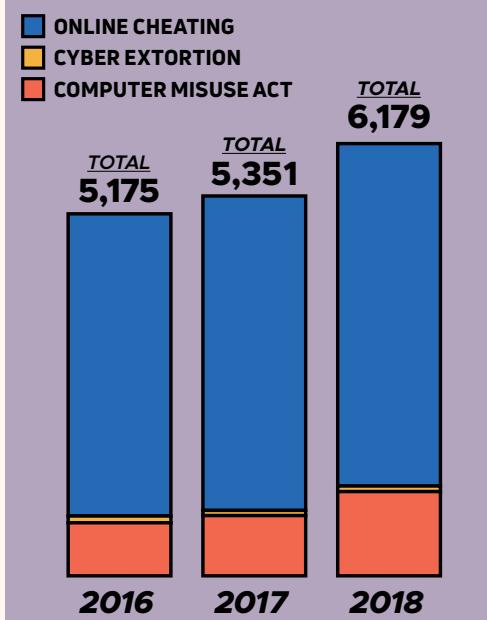
300

Unique [Command and Control](#) servers were observed in Singapore

2,900

[Botnet drones](#) (compromised computers infected with malicious programs) with Singapore IP addresses were observed daily, on average

CYBERCRIME IN SG



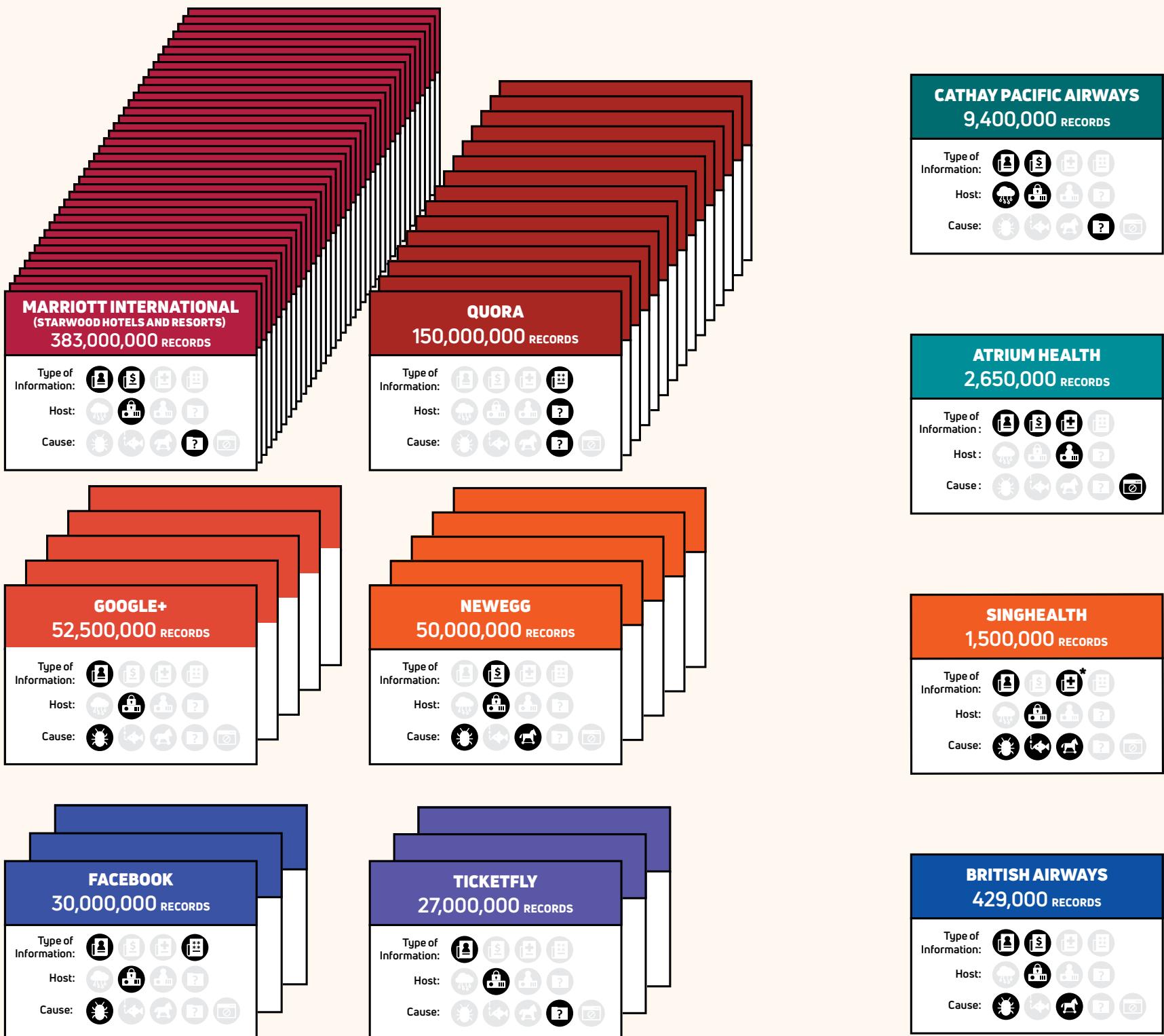
Cybercrime cases accounted for 18.6% of overall crime in 2018.

WEBSITE DEFACEMENT

605

Singapore-linked website defacements were detected.

SELECTED MAJOR DATA BREACHES IN 2018



DATA BREACHES

Threat actors target vulnerable points in public and private organisations, businesses, and even cloud computing systems to pivot to sensitive data they are interested in. The figure shows the relative scale of selected major data breaches that occurred in 2018.

LEGEND

TYPE OF INFORMATION:

- | | | | |
|--|-----------------------|--|---------------------|
| | Personal Information | | Medical Information |
| | Financial Information | | Account Information |

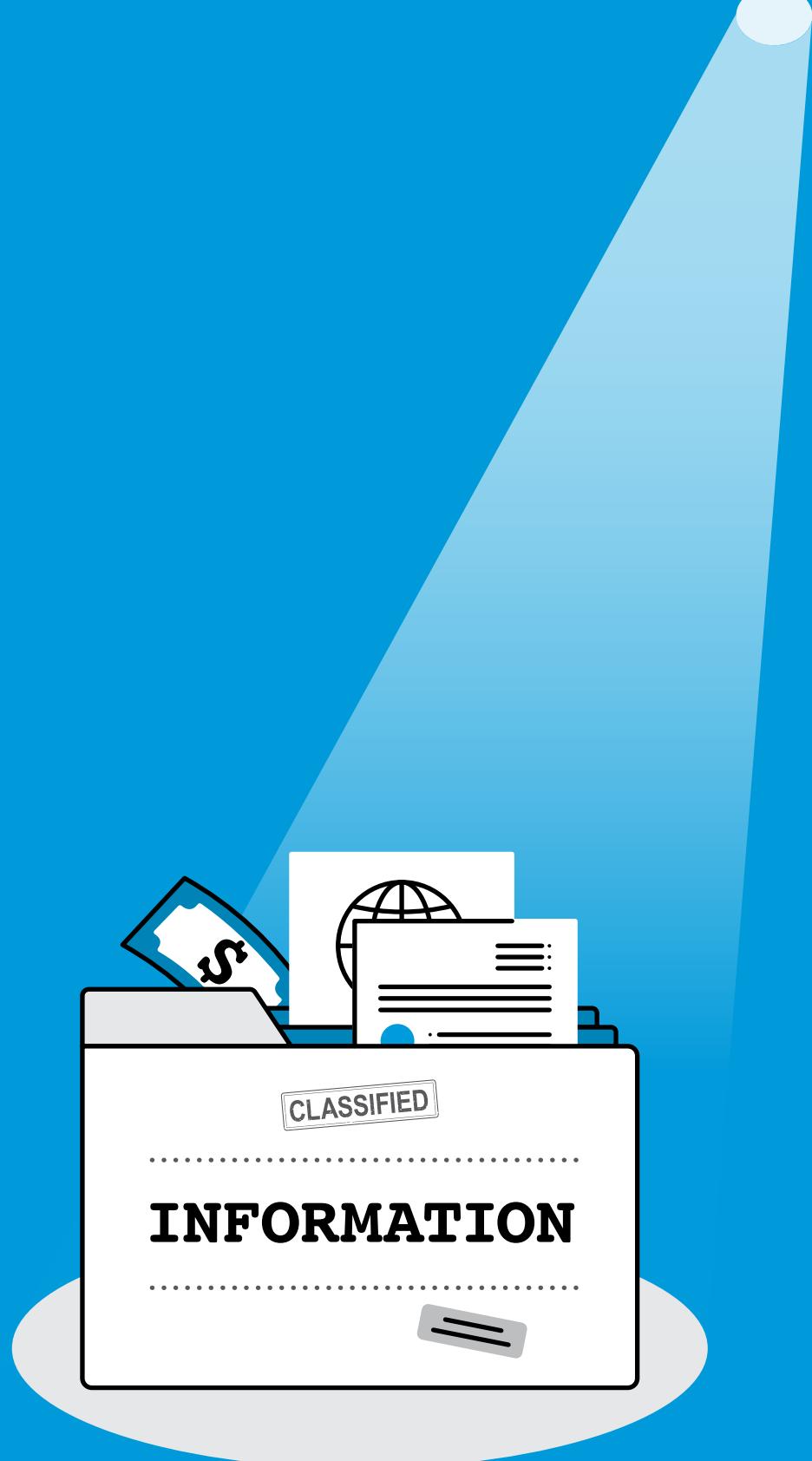
* Limited information compromised

HOST:

- | | | | |
|--|-------------------------|--|---------------------|
| | Cloud Infrastructure | | Third-Party Servers |
| | Company Private Servers | | Undisclosed |

CAUSE:

- | | | | |
|--|--|--|-------------|
| | Vulnerability | | Undisclosed |
| | Phishing | | Malware |
| | Unauthorised access through third-party supplier | | |



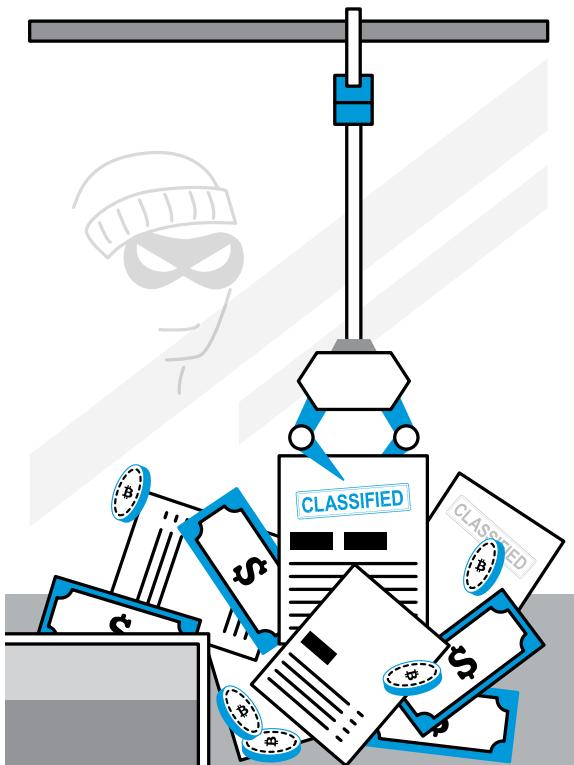
CHAPTER 1

SPOTLIGHT ON CYBER THREATS

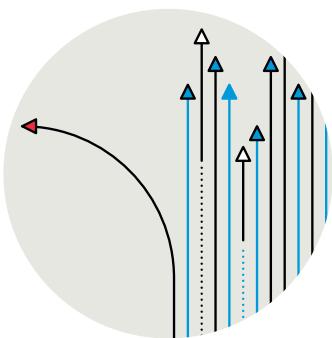
Singapore faced a number of cyber threats in 2018, including Advanced Persistent Threats, website defacements, phishing, and malware activities. This chapter details our observations on some of these cyber threats, trends, and motivations from the period of January to December 2018.

ADVANCED PERSISTENT THREATS

In the past two editions of the Singapore Cyber Landscape, we highlighted the significance and potential impact that Advanced Persistent Threats (APT) have on our cyber ecosystem. Often associated with a nation-state, APT groups have access to a wealth of resources and deep expertise to achieve their objectives, which include causing disruption, cyber theft for financial gain, and conducting cyber espionage.



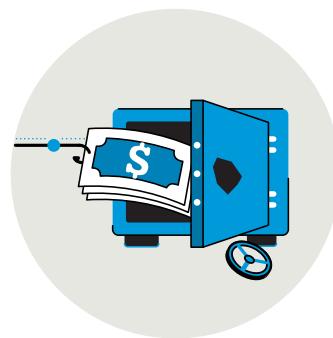
DISRUPTION



APT groups may choose to target prominent, highly-visible international events with the aim of disrupting them to draw attention. The Opening Ceremony of the PyeongChang Winter Olympic Games in February 2018 was one such example. The attack, attributed to an Asia-based APT group, disrupted Internet access and telecasts, and shut down websites covering the event.

Another type of APT attack seeks to disrupt operations. *Shamoon*, a type of wiper malware associated with an APT group based in the Middle East, is designed to wipe data and render endpoints and servers unbootable. This prevents the targeted organisation from conducting business as usual. First seen in 2012 in the energy industry, it re-emerged in December 2018, affecting a number of organisations across many industries in the Middle East.

FINANCIAL GAIN



A number of high-profile cyber-attacks targeting payment systems were attributed to APTs, resulting in significant losses to affected financial institutions. These attacks typically involve tactics, techniques and procedures (TTPs) such as phishing e-mails to compromise employee accounts and gain access to systems and networks, as well as technical methods to cover the attackers' tracks. In June 2018, attackers breached the SWIFT payment system at the Bank of Chile and the Cosmos Bank, siphoning off US\$10 million and US\$13.5 million respectively, through fraudulent wire transfer requests. These attacks were likely conducted by the same APT group.

CYBER ESPIONAGE



APT groups are known for conducting information gathering and cyber espionage. Information gathered can be useful for intelligence purposes, and/or give countries a competitive advantage over rivals during state negotiations. One such example was a watering hole¹ campaign active in the last quarter of 2018 that compromised several government and media websites in Vietnam and Cambodia. These websites were used to infect visitors with spying malware. This attack was attributed to an Asia-based APT group that cybersecurity experts had identified as being behind several espionage and spear-phishing campaigns targeting Southeast Asian countries.

¹ A watering hole attack is a type of cyber-attack targeting a particular organisation, where malware is delivered from websites that are regularly visited by the organisation's members and infects its systems.

NO. OF DEFACED SINGAPORE WEBSITES REPORTED IN 2018

WEBSITE DEFACEMENTS



CSA detected 605 cases of website defacement in Singapore in 2018, a 70 per cent decrease from 2,040 in 2017. These websites belong to a range of organisations – from government agencies, businesses, and media companies. Two Singapore Government websites were among those defaced. While most affected websites belong to Small and Medium Enterprises (SMEs), larger organisations were also hit.

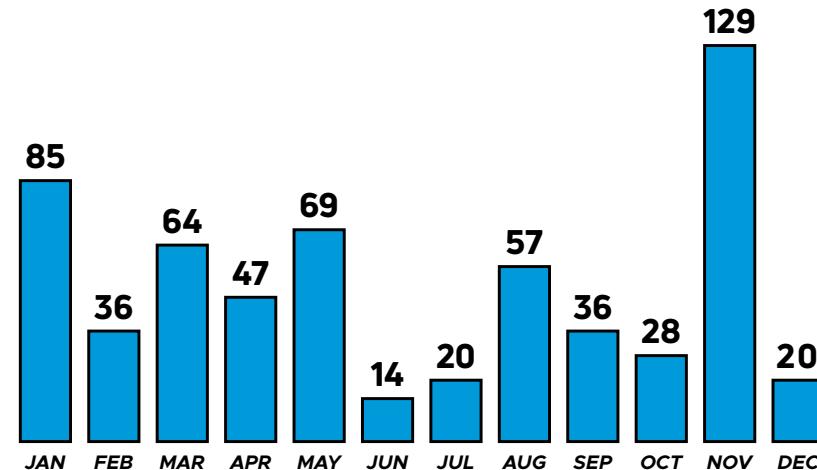
WEBSITE DEFACEMENTS (2016 – 2018)

Year 2016	1,750
Year 2017	2,040
Year 2018	605

For example, the Singapore website of a major Japanese advertising firm was compromised and replaced by a message “Sec == ‘0’” in January 2018.

A spike in defacements observed in November 2018 was likely caused by an attacker exploiting vulnerabilities in an unpatched web server. 101 websites belonging to various businesses hosted on this server were compromised by the same attacker in a single day. Defacements are indicative of vulnerabilities present in a website’s underlying infrastructure. This may be a harbinger of more damaging cyber-attacks, such as hosting malicious content on the website or using it as a platform to launch attacks.

Defacements usually take place when unpatched/ outdated websites and their hosting servers are attacked. Common methods of intrusion include Structured Query Language (SQL) injections,



“**3 IN 10**
websites were
defaced previously



In January 2018, the Singapore website of a major Japanese advertising firm was compromised, with its homepage replaced only with the message “Sec == ‘0’”.

where malicious code is inserted into the web-based application, and by gaining access to the web servers.

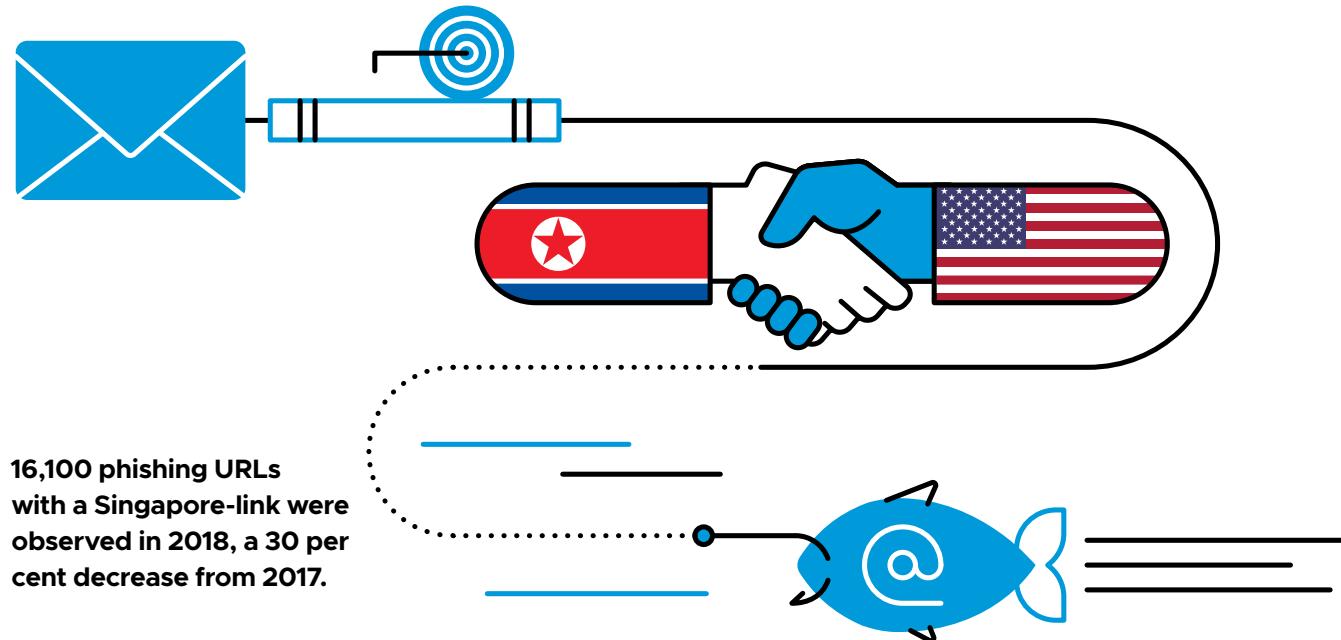
Websites published on the WordPress platform remained the most targeted for defacements in 2018, continuing a trend observed since 2016. In Singapore, over a third of the websites defaced were built on WordPress. A WordPress file deletion vulnerability, first disclosed on 26 June 2018 and affecting all versions of WordPress up to then, could allow an attacker to have full control over the website. WordPress released an updated platform version that fixed the vulnerability on 5 July 2018, and SingCERT published an alert a week later, advising WordPress website owners and web hosting providers to update to the latest version immediately.² However, as of March 2019, about 40 per cent of the defaced WordPress websites had yet to be patched to the latest version.

Worryingly, 185 of the defaced websites – or about 30 per cent of the cases – were defaced previously. Re-defacements suggest that website owners have yet to take appropriate security and patching measures to protect their websites, even after being attacked before. The variety of intrusion and compromise methods underlines the importance of using stronger login credentials and timely patching of known vulnerabilities.

² “[SingCERT] Alert on WordPress 4.9.7 Security Release,” SingCERT Advisories & Alerts, 12 July 2018, <https://www.csa.gov.sg/singcert/news/advisories-alerts/alert-on-wordpress-4-9-7-security-release>.

COMMONLY SPOOFED ORGANISATIONS IN 2018

PHISHING URLs



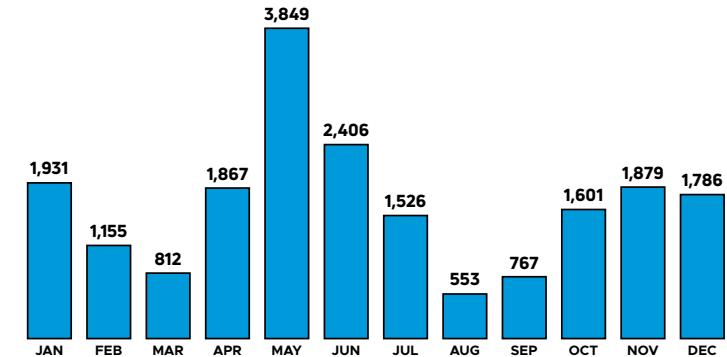
16,100 phishing URLs with a Singapore-link were observed in 2018, a 30 per cent decrease from 2017.

Phishing e-mails usually spoof, or pretend to originate from, reputable firms and organisations. Companies in the banking and financial services, technology, and file hosting services made up almost 90 per cent of spoofed companies in 2018.

In Singapore, websites of Government organisations such as Ministry of Manpower (MOM), Singapore Police Force (SPF) and Immigration & Checkpoints Authority (ICA) were commonly spoofed to steal personal and financial data from victims.

Phishing activity typically increases when major events occur. Threat actors dupe victims into opening phishing e-mails and their attachments

NUMBER OF PHISHING URLs WITH A SINGAPORE-LINK OBSERVED IN 2018



by taking advantage of their interest in such events. During the FIFA World Cup tournament in June 2018, several soccer-themed phishing e-mails and websites were observed, targeting sports fans with fake gifts from FIFA or its sponsors. Fans who responded to these

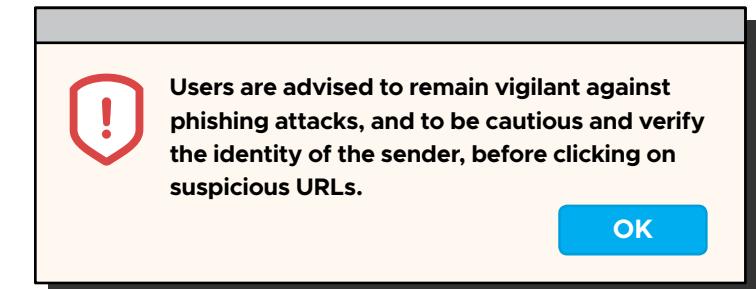
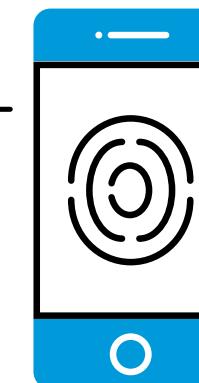
"giveaways" ended up giving away their personal information to cybercriminals. Separately, in the lead-up to the Democratic People's Republic of Korea-USA Singapore Summit held in June 2018, an intelligence-gathering campaign targeted South Koreans with phishing e-mails.

ATB Financial
GitLab
Adobe
Docusign
Bank of America
Chase Bank
Google
Postmaster
Free Mobile France

Apple
PayPal
Facebook
Microsoft
Dropbox
Amazon
Mailbox

Alibaba
AT&T
Yahoo

1st Banking and Financial Services (e.g. Bank of America)
2nd Technology (e.g. Microsoft)
3rd File Hosting Services (e.g. Dropbox)



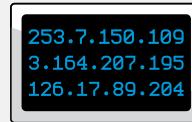
These contained malware that could be used for keylogging and executing malicious commands on compromised devices.

Increasingly, threat actors are also using ingenious tactics to trick individuals and evade detection. Some examples include the use of HTTPS, Dynamic Domain Name System (DDNS) services, and using generic top level domains:



TAKING ADVANTAGE OF "HTTPS"

2,450 phishing URLs were observed using "HTTPS" in 2018, a more than tenfold jump from just 200 of such URLs in 2017. Using "HTTPS" – rather than "HTTP" – lures victims into a false sense of security, by having them believe that they were transacting on a secure website.



USE OF DYNAMIC DOMAIN NAME SYSTEM SERVICES (DDNS) SERVICES

210 URLs were observed using DDNS services in 2018, three times more than in 2017. Such services enable malicious URLs to change their IP addresses constantly to evade applications that block static malicious IP addresses.



LEVERAGING GENERIC TOP LEVEL DOMAINS

Domains such as ".com" (8,100 URLs) and ".club" (700 URLs) were commonly abused, making up more than half the observations for 2018. They are relatively cheap (or even available for free) and lack regulation, allowing threat actors to constantly create new malicious URLs.

MALWARE

Fewer ransomware cases were reported to CSA in 2018. There were also significantly fewer Command and Control (C&C) servers observed in Singapore; however, the number of botnet drones – compromised computers infected with malware – remained largely similar.

RANSOMWARE

21 ransomware cases were reported to CSA in 2018, a decrease from 25 in 2017. Although the number of reported cases is low, the actual number of ransomware cases may be higher as many go unreported. Ransomware affected systems across multiple industries in Singapore, such as construction, education, and food and beverage. While there were no global widespread campaigns like the *WannaCry* attacks seen in 2017, ransomware remains lucrative, and continues to evolve in sophistication.

GandCrab was described as “one of the most aggressive forms of ransomware”³ in 2018. Since its discovery in January 2018, *GandCrab* has infected over half a million computers and is believed to have extorted around US\$300 million

in ransom payments. In February 2018, a private financial institution in Singapore was infected with *GandCrab*, when one of its employees surfed a compromised website and was prompted to install a ‘font update pack’ for displaying the website properly.

Ransomware remains a common threat. Europol has warned that targeted ransomware attacks which are tailored to specific organisations or individuals, such as *GandCrab* and *SamSam*,⁴ may become the new normal.⁵ Organisations should ensure that their systems are regularly updated to thwart known ransomware threats. They should also not make any form of payment demanded, as there is no certainty they would get their data back.

GANDCRAB, THE MONEY-GRABBING RANSOMWARE

GandCrab is offered in the Dark Web as Ransomware-as-a-Service (RaaS) by its criminal developers. Modeled after Software-as-a-Service (SaaS) principles, cybercriminals without programming knowledge would rent such ransomware for their malicious activities, and pay the developers by sharing a portion of the collected ransoms.



Some characteristics of *GandCrab* include: (a) being frequently updated to evade detection and deletion, (b) targeting mainly English-speaking countries, and (c) customisable ransom demands.

As part of the *No More Ransom* initiative, free decryption tools for later versions of *GandCrab* are made available for affected victims to recover their files. This public-private cooperation exemplifies the need for collaboration between government and industry partners to combat global cyber threats together.

FEATURED TOPIC

ADVERSARIAL AI IN CYBERSECURITY

An illustration of a hand holding a dumbbell. A blue gear is attached to the handle of the dumbbell, and a blue plus sign is positioned above the hand. To the right of the hand, there is a large grey arrow pointing upwards. This imagery represents the concept of adversarial AI in cybersecurity, where machine learning models are being strengthened or improved.

Machine learning and data-driven detection systems are being adopted in cybersecurity applications to cope with rapidly evolving cyber-attacks. However, threat actors are now leveraging adversarial Artificial Intelligence (AI) technologies to deceive these systems. One method of deception involves using Generative Adversarial Networks (GANs) to create new variants from known

malware that are able to bypass malware detectors. One way to counter this attack would be to include GAN samples during re-training, so that the malware detector is tuned to identify this class of mutated samples.

To combat against new cyber-attacks, AI engines constantly train and update their models. This adaptive learning process, however, creates an opportunity for threat actors

to poison data used to train the models and thus influence decision boundaries. One method of defending against this type of attack involves processing the training data to identify potential adversarial data manipulation first, before providing them to train the AI engines.

³ “The *GandCrab* Ransomware Mindset,” Check Point Research, 13 March 2018, <https://research.checkpoint.com/gandcrab-ransomware-mindset>.

⁴ On 22 March 2018, the City of Atlanta in the US state of Georgia suffered a ransomware attack which affected several local government systems and disrupted businesses. Almost US\$17 million was reportedly spent in recovery efforts. The ransomware used in the attack, dubbed ‘*SamSam*’, was also linked to another ransomware attack on the Port of San Diego in September 2018.

⁵ Palmer, Danny. “Cybercrime: Ransomware remains a ‘key’ malware threat says Europol,” ZDNet, 18 September 2018, <https://www.zdnet.com/article/cybercrime-ransomware-remains-a-key-malware-threat-says-europol>.

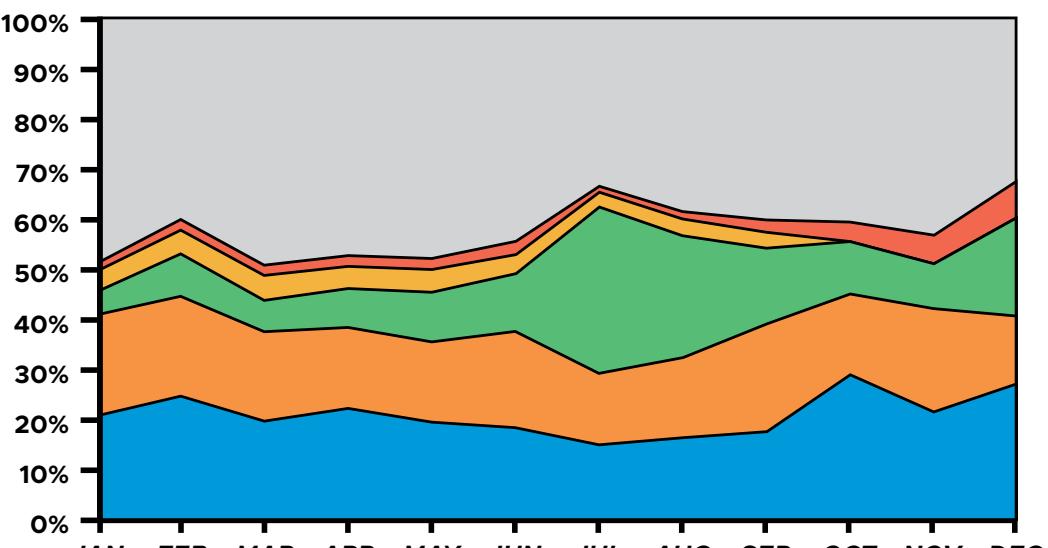
COMMAND AND CONTROL SERVERS AND BOTNET DRONES



In 2018, CSA observed about 300 unique C&C servers in Singapore, a 60 per cent decrease from 2017.

SingCERT is responsible for the prevention, detection and resolution of cybersecurity incidents in Singapore, acting on information provided by government agencies, international counterparts and the public. When SingCERT receives information regarding C&C servers hosted in Singapore, the team first confirms the locations of the servers, and

then asks the relevant agencies such as the Info-communications Media Development Authority (IMDA) or relevant abuse team of the local hosting providers to take them down and restore legitimate services. When the hosting provider is located overseas, SingCERT collaborates with the relevant foreign Computer Emergency Response Teams (CERTs) to do the same.



On average, five common malware accounted for over half the daily infections in 2018.

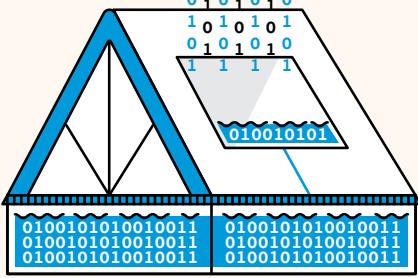
FEATURED TOPIC

OPEN PORTS

Open ports attract malware infection and may be used to launch cyber-attacks, such as Distributed Denial-of-Service (DDoS) attacks. DDoS attacks inundate websites and services with incoming traffic, causing them to become unavailable. In February 2018, the two largest DDoS attacks recorded in history occurred just five days apart from each other. Unlike large-scale DDoS attacks that usually employ malware-driven botnets, these two attacks stemmed from servers where specific ports were left open unnecessarily.⁶

The first attack peaked at 1.35 Tbps and targeted the developer platform, GitHub. The peak was 30 per cent higher than the previous record set by the attack targeting Dyn in 2016. The second attack targeted a US-based service provider, and set the current peak record of 1.7 Tbps.

If users must utilise open ports for their work, they should always safeguard them by avoiding default credentials, and close the open ports promptly when not in use.



On average, nearly 2,900 botnet drones with Singapore IP addresses were observed daily.⁷ About 470 malware variants were detected, but the top five malware observed – Gamarue, Conficker, Mirai, WannaCry, and Gamut – accounted for over half of observed infections, echoing trends observed in previous years. These are not new malware; Conficker, in particular, dates back to 2008.

The top malware, Gamarue, steals personal information and can also function as a medium to distribute other malicious programs. Although Gamarue's infrastructure was largely dismantled in an international operation in December 2017, efforts to wipe it out completely had been slow and challenging,⁸ and Gamarue had continued to infect systems throughout 2018.⁹ The persistence of Gamarue infections into 2018

suggests that many users have yet to patch their devices, or use antivirus software, to prevent infections. This is also the likely explanation for how WannaCry – the ransomware that wrecked havoc across the globe in 2017 that can now be easily detected by antivirus software – continued to persist on local systems and computers.

Separately, the Mirai malware had been linked to botnet campaigns targeting unpatched Internet of Things (IoT) devices. A number of malicious campaigns are increasingly leveraging open-source Mirai malware – shared openly on the Internet – to conduct brute-force attacks with common usernames and passwords. The observations indicate that many users do not change default login credentials of their smart devices.

⁷ Based on unique Internet Protocol (IP) addresses (the numerical code assigned to each device that can connect to the Internet or other networks), about 115,000 botnet drones were observed in Singapore in 2018.

⁸ Parrish, Kevin. "The Andromeda botnet still lingers as nations struggle to clean infected PCs," Digital Trends, 14 August 2018, <https://www.digitaltrends.com/computing/andromeda-botnet-still-infects-pcs-africa-asia/>.

⁹ Brumaghin, Edward and Unterbrink, Holger with contributions from Tacheau, Emmanuel. "Old dog, new tricks – Analysing new RTF-based campaign distributing Agent Tesla, Loki with PyREbox," Cisco Talos Blog, 15 October 2018, https://blog.talosintelligence.com/2018/10/old-dog-new-tricks-analysing-new-rtf_15.html.

⁶ Specifically, memcached servers, used for speeding up networks and improving performance of web applications, were instead hijacked to carry out the two DDoS attacks.

CHAPTER 2

TARGET.SG



Singapore has been, and will continue to be, the target of cyber-attacks by Advanced Persistent Threat groups and other threat actors. This chapter offers insights and practical lessons from cyber-attacks that affected different segments of Singapore in 2018, and how we can learn from them to strengthen our collective cybersecurity.

TARGET.GOV.SG**CASE STUDY****CYBER-ATTACK ON SINGHEALTH**

In 2018, SingHealth's network was the target of a deliberate and well-planned cyber-attack. The scale of this cyber-attack was unprecedented. The personal particulars of 1.5 million patients and the outpatient dispensed medication records of 160,000 of them were illegally accessed and copied. Prime Minister Lee Hsien Loong's records were specifically and repeatedly targeted.

There was, however, no evidence that the data had been tampered with or deleted. No clinical services were disrupted, and patient care remained uncompromised.

The Committee of Inquiry (COI) into the cyber-attack on SingHealth's database system established that the cyber-attack was the work of a skilled and sophisticated actor, which bore the characteristics of an Advanced Persistent Threat (APT) group. The COI found that the attacker was well-resourced, and had used advanced techniques and tools to target the SingHealth patient database and illegally exfiltrate patient data. The attacker was persistent, evaded detection for a long time, and even re-entered the network after being detected.

WHAT HAPPENED?

The attacker gained initial access to SingHealth's IT network around August 2017, by infecting front end workstations, most likely through phishing attacks. After lying dormant for several months, the attacker moved laterally through the network between December 2017 and June 2018, compromising additional endpoints, servers and user accounts.

From May 2018, the attacker made multiple unsuccessful attempts to connect to SingHealth's patient database system. On 26 June 2018, the attacker obtained credentials to the database, and began querying and exfiltrating patient records the following day.

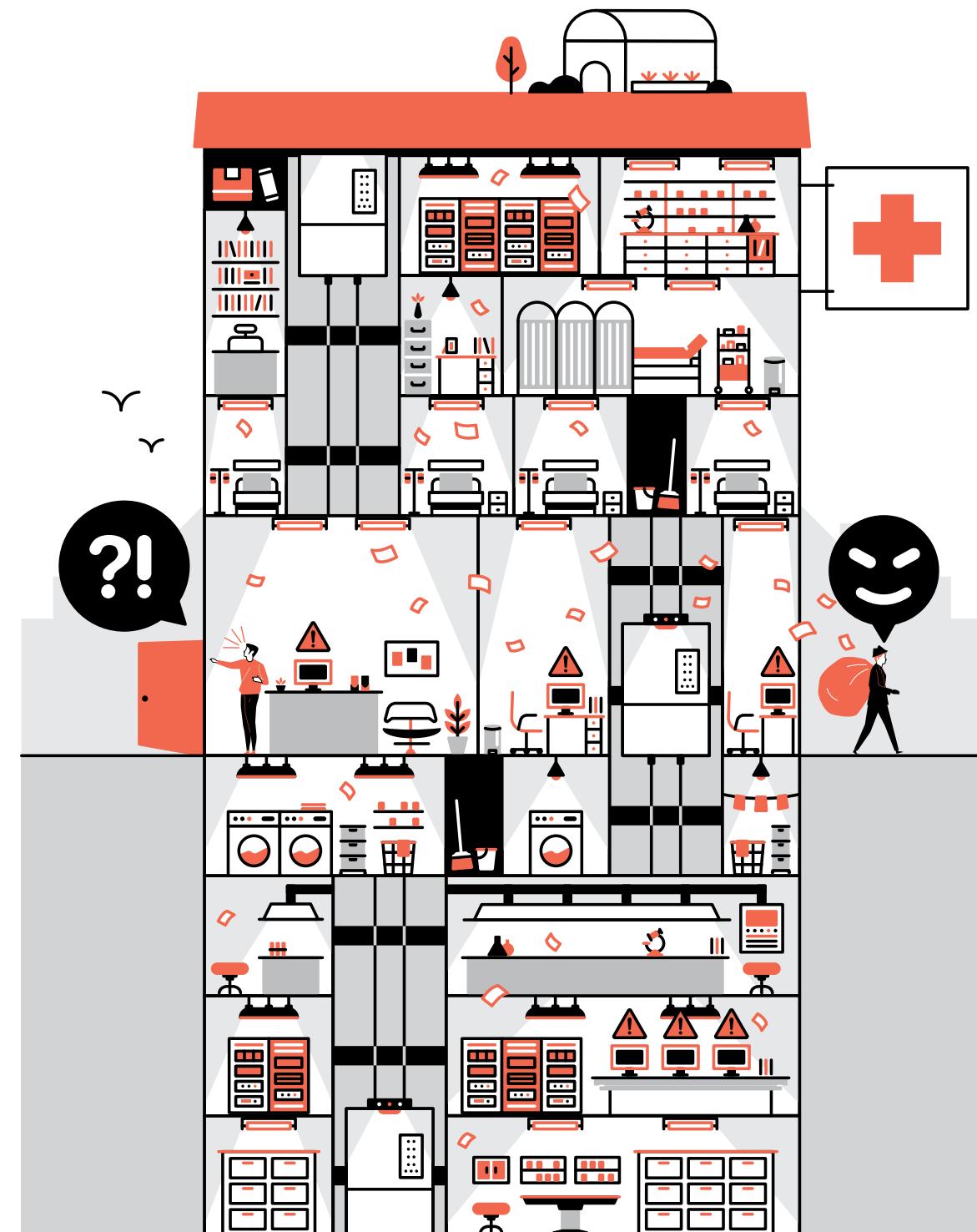
On 4 July 2018, an IT administrator at Integrated Health Information Systems (IHIS), the IT agency serving the public healthcare sector including SingHealth, noticed suspicious queries made on the database. The suspicious queries were terminated by IHIS's IT administrators, and measures were put in place to prevent further queries from being made.

On 10 July 2018, the cyber incident was escalated to the Cyber Security Agency of Singapore (CSA), SingHealth's senior management, the Ministry of Health (MOH), and Ministry of Health Holdings (MOHH). CSA's National Cyber Incident Response Team (NCIRT) was immediately deployed on site to work with IHIS to carry out joint investigations and remediation. They took steps to contain the threat, eliminate the attacker's footholds, and prevent recurrence of the attack.

“ ”

Even as we do our best to secure our systems, it is a matter of when, not if, our systems are breached. The cyber-attack on SingHealth is a reminder for us to do better in our cybersecurity efforts, together as a nation.

– Mr David Koh, Commissioner of Cybersecurity and Chief Executive CSA, emphasising the need for collective cybersecurity



FEATURED TOPIC

STRENGTHEN GOVERNMENT ICT SYSTEMS

To build a secure and resilient Smart Nation, the Government's approach to cybersecurity is underpinned by two key principles. First, we adopt a 'defence-in-depth' strategy, with multiple layers of cyber defence to impede attackers. These layers of defence cascade from the perimeter to within the systems. Given enough time and resources, sophisticated and determined attackers may eventually find their way into the system. The layered defence approach will enable security teams to detect any breach and respond swiftly. Second, we enhance our system defence on three fronts – People, Processes and Technology. In terms of People and Processes, the Government is developing a stronger cybersecurity culture across the Public Service, as well as tapping on technology to support its IT staff and automate cybersecurity tasks, such as patch management. In terms of Technology, the Government will continue to build up the defence and resilience of its systems, while implementing measures to better detect and respond to cyber threats.

The Government can more effectively defend our systems if we involve the global and local communities of cyber defenders to identify vulnerabilities and strengthen the Government's ICT systems. For example, the Government Technology Agency of Singapore (GovTech) and CSA are partnering local and overseas cybersecurity communities on a [Government Bug Bounty Programme \(GBBP\)](#) to help search and uncover vulnerabilities in our system.

CSA also coordinated national efforts to mitigate the risk of a similar attack affecting other Critical Information Infrastructure (CII) systems, by sharing threat intelligence with CII owners and instructing them to undertake relevant security measures.

In view of further malicious activities detected on the SingHealth network on 19 July 2018, Internet Surfing Separation (ISS) was temporarily imposed on SingHealth's IT systems on 20 July 2018. As a precautionary measure, temporary ISS was

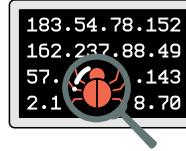
also implemented for IT systems in other unaffected public healthcare clusters (National Healthcare Group and National University Healthcare System) on 22 July 2018. The Government also [paused the rollout of new Government ICT systems](#) from 20 July to 3 August 2018. During the pause, a review of its existing cybersecurity measures was conducted. Although there was no evidence of Government ICT systems being compromised in this attack, additional measures

on critical Government systems were introduced to detect and respond more quickly to cybersecurity threats.

SingHealth began contacting the affected after the Government announced the news of the cyber-attack on 20 July 2018. Concurrently, SingCERT also issued advisories on precautions that [organisations](#) and [members of the public](#) could take, in anticipation of potential opportunistic attacks.

RECOMMENDATIONS MADE BY THE COI INTO SINGHEALTH

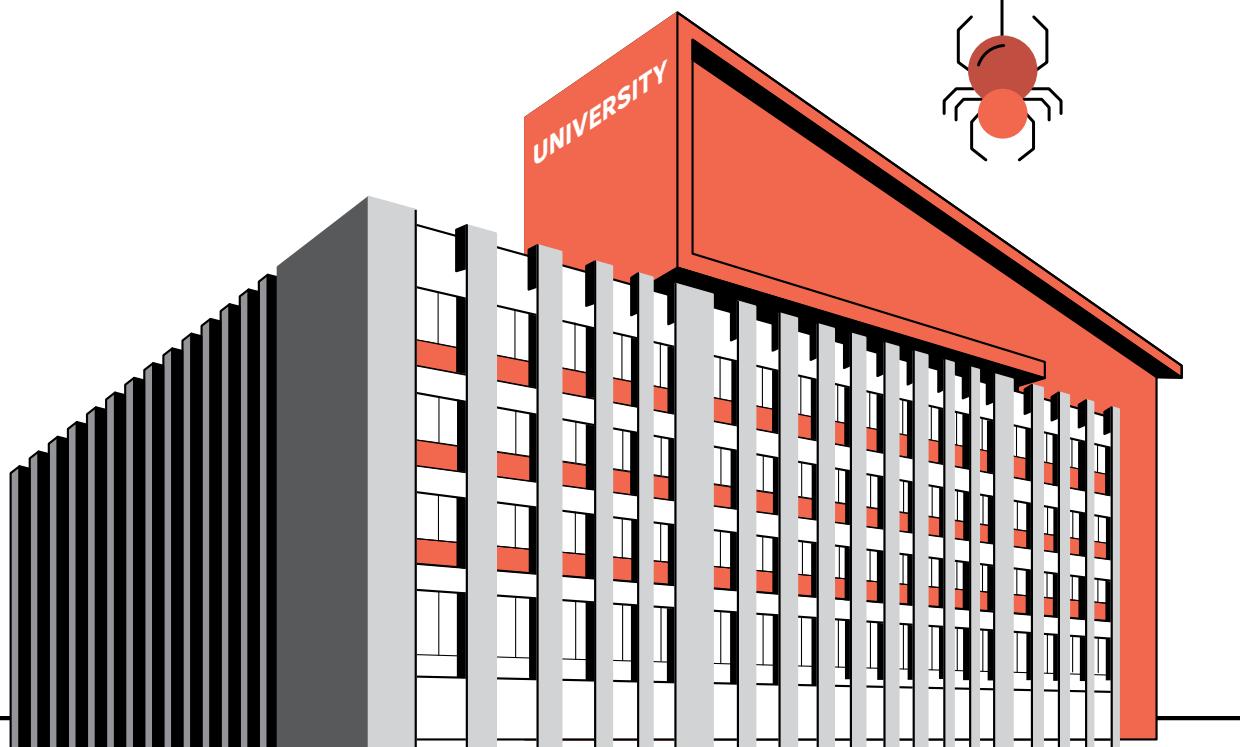
The COI made 16 recommendations relating to strategic and operational measures to strengthen the cybersecurity posture of SingHealth and IHIs. These recommendations are generally applicable to all organisations responsible for large databases of personal data. Some key actions that all organisations must consider implementing are as follows:

- 1  Include cybersecurity as part of the organisation's risk management, with deliberations and decisions on balancing cybersecurity and trade-offs (e.g. cost, operational requirements) based on unique business considerations (e.g. patient safety in the case of the public healthcare sector) managed at the senior level of leadership.
- 2  Provide all staff with training to build awareness on the best cyber hygiene practices, and cultivate an organisational culture where cybersecurity is everyone's responsibility.
- 3  Train and equip all staff to recognise and respond to cybersecurity incidents, and to report these incidents in a timely manner.
- 4  Adopt multiple defences, such as encryption, firewalls and robust data-access practices, to layers of security measures, to better prevent, detect and respond to cyber incidents.
- 5  Carry out comprehensive and regular checks and audits to identify gaps in the design of and compliance with policies, processes and procedures, and to ensure that these gaps are remedied according to plan.
- 6  Develop cyber incident response plans for various scenarios, and test and update them regularly by conducting realistic exercises and simulations.

TARGET.EDU.SG

Threat actors target academic institutions for a variety of reasons. These include stealing sensitive research information, and using them as stepping stones to gain access to high security systems and networks.

In 2017, the National University of Singapore (NUS) and Nanyang Technological University (NTU) were hit by sophisticated cyber-attacks that were assessed to be the work of APTs. These incidents highlight the need for academic institutions to stay vigilant constantly and strengthen their cybersecurity defences, as part of measures to protect their intellectual property.

**CASE STUDY****CYBER-ATTACK ON UNIVERSITIES****WHAT HAPPENED?**

In April 2018, CSA received information that there was a breach of user account credentials at various universities in Singapore. Further investigations revealed that at least 52 accounts from four universities – NTU, NUS, Singapore Management University (SMU), and Singapore University of Technology and Design (SUTD) – had been compromised.

Unsuspecting victims received spear phishing e-mails that directed them to a credential harvesting website, which closely

resembled the web portals of the universities. These portals were made to look as if the victims had accidentally logged out of their accounts and prompted them to enter their login credentials.

The login credentials of the victims were later used to gain unauthorised access to the online libraries of the universities, in order to obtain research publications of staff members across various research fields and academic disciplines.

FOLLOW-UP ACTION

The affected universities reset the passwords of all users, and scanned computers and networks for signs of further compromise. SingCERT sent out advisories to alert all users about the incident, and heighten their vigilance against similar attacks and other potential cyber threats.

TARGET.ORG.SG

Organisations are frequently targeted by threat actors, most often to steal private and personal information from their databases. As more Small and Medium Enterprises (SMEs) go digital, business e-mail impersonation scams are expected to grow in tandem. The Singapore Police Force observed 378 business e-mail impersonation scams in 2018, up from 332 cases in 2017. In total, businesses in Singapore suffered losses of close to S\$58 million in 2018, an increase of about 31 per cent from 2017.

CASE STUDY

CRYPTO-JACKING

WHAT HAPPENED?

In January 2018, SingCERT received information that a training institute's web servers had been infected by malware.

Four of the institute's web servers were later found to be infected by a crypto-mining malware. No other suspicious activity was detected, although the infected web servers were observed communicating to Internet Protocol (IP) addresses associated with crypto-mining operations.

SingCERT later discovered that the institute's web server software had not been patched to the latest versions, leading to its subsequent compromise. The attacker exploited these vulnerabilities to hijack the systems and discreetly link the web servers to a crypto-mining pool. The cryptocurrency produced was then transferred to a cryptocurrency wallet for storage. The attacker remains unknown due to the anonymous nature of the encrypted wallet.



FOLLOW-UP ACTION

SingCERT provided technical assistance to the organisation to investigate and understand the root cause and potential impact of the incident. SingCERT also worked together with the organisation to restore all compromised web servers to their last known serviceable state.

All organisations and businesses should manage their cybersecurity risks appropriately. These include ensuring that all systems are regularly updated and patched for known vulnerabilities, and educating employees on the importance of verifying important email requests with business partners first, before responding to them. The public may refer to the SingCERT alert published on 9 November 2017 for measures to counter the rising crypto-jacking threat.¹⁰

FEATURED TOPIC

UNAUTHORISED CRYPTO-MINING BECOMING MORE PREVALENT

Cybersecurity firms have observed a shift in modus operandi from traditional ransomware to crypto-mining, as mining cryptocurrency becomes more profitable than other criminal business models. Internet of Things (IoT) devices have also emerged as a potential attack vector that may be abused by cybercriminals. *ADB.Miner*, a Monero crypto-mining botnet which borrowed scanning code from *Mirai*, was found in February 2018 targeting Android-based devices. Another Monero crypto-mining botnet, *Smominru*, utilises the *ETERNALBLUE*¹¹ exploit and has since infected more than 500,000 computers worldwide.

In January 2018, security company Sucuri discovered a campaign where over 2,000 WordPress websites were compromised by a malicious script. This script delivered crypto-mining and keylogging malware to devices. Users would experience a decline in computing performance of their devices when they visit these compromised websites, whose malware in turn harness the computing power to mine cryptocurrencies. Sensitive information such as payment details would also be captured by the malware.

¹⁰ “[SingCERT] Alert on Browser-based Digital Currency Mining,” SingCERT Advisories & Alerts, 9 November 2017, <https://www.csa.gov.sg/singcert/news/advisories-alerts/alert-on-browser-based-digital-currency-mining>.

¹¹ *ETERNALBLUE* is an exploit which leverages a vulnerability in Microsoft's Server Message Block (SMB). SMB is a protocol used by computers to share access to files and appliances over a network.

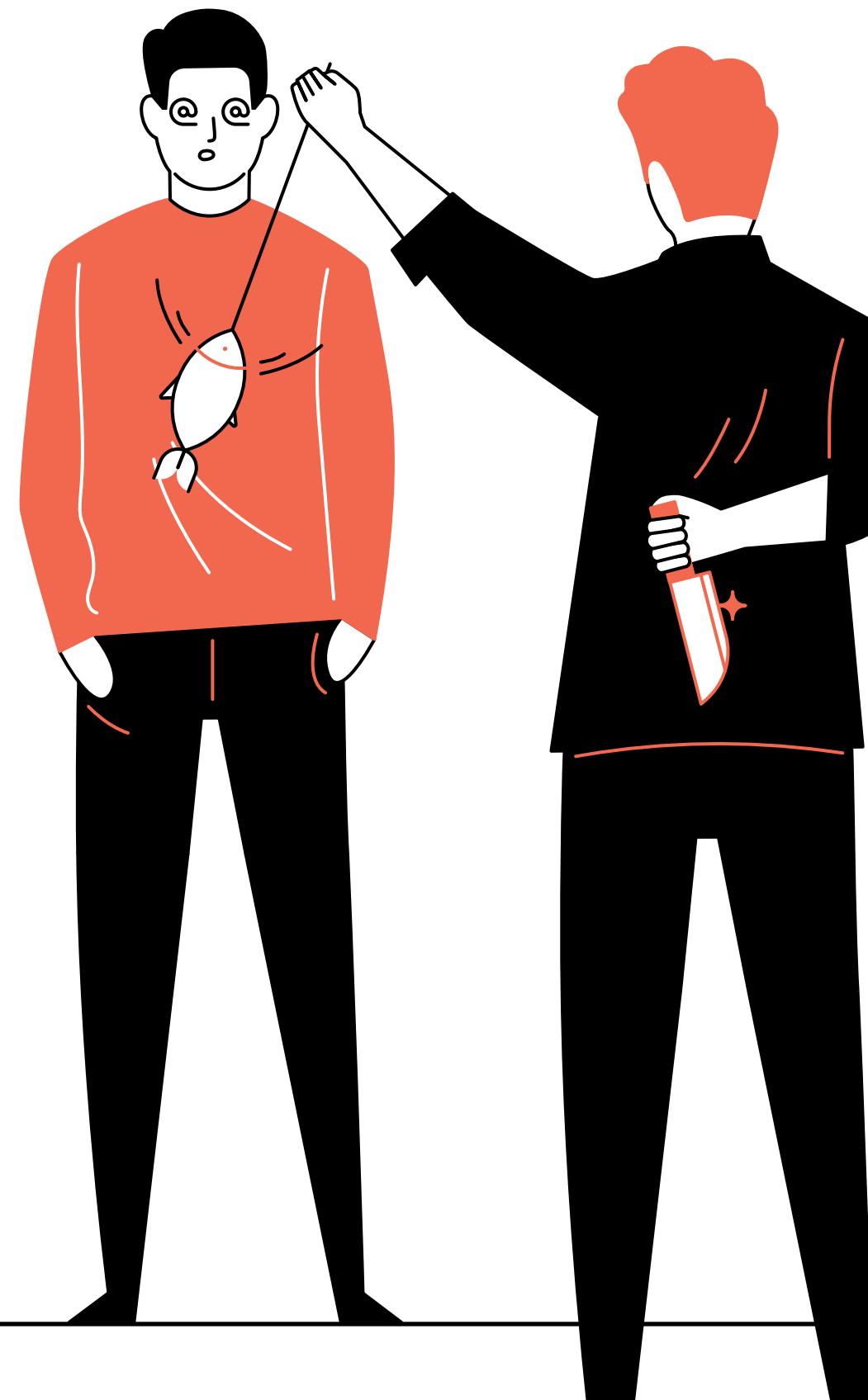
TARGET.YOU.SG

Many individuals continue to lack cybersecurity awareness and practise poor cyber hygiene.

According to the Singapore Police Force, there were 1,204 cases investigated under the Computer Misuse Act (CMA)¹² in 2018, a 40 per cent increase from 2017. Some of these cases were a result of victims who were not alert to phishing e-mails intended to steal their sensitive personal information such as passwords and credit card details.

All individuals should protect themselves from cyber threats proactively, and practise good cyber hygiene habits at all times. These include checking for signs of phishing before clicking on unknown links or opening attachments in suspicious e-mails, installing computer protection software (i.e. anti-virus, anti-spyware/malware, and firewall) and keeping them updated, and enabling Two-Factor Authentication (2FA) where possible.

Separately, online scams continued to be a concern. There were about 2,125 e-commerce scams reported in 2018, with victims losing a total of about S\$1.9 million. 70 per cent of such scams took place on e-commerce platform Carousell, and involved electronic products and tickets to events and attractions. It is important for all individuals to exercise caution towards unrealistic bargains for merchandise on e-commerce platforms to avoid falling prey to such scams.



CASE STUDY

NEARLY@SCAMMED.COM

WHAT HAPPENED?

In July 2018, a member of the public sought SingCERT's help after receiving a threatening e-mail. The e-mail claimed that the victim's computer had been infected with malware, and demanded payment in exchange for not exposing video clips of the victim in compromising situations, allegedly recorded with the computer's own web camera. To substantiate the threat, the e-mail also contained the victim's e-mail password.

It was later determined that the e-mail represented a new form of extortion scam that surfaced recently. The victim's e-mail address and password were likely exposed in a previous data breach – where login credentials of affected individuals were leaked – and not obtained through malware that had compromised the victim's computer, as the scammer had claimed.

FOLLOW-UP ACTION

SingCERT advised the victim to change all passwords associated with the compromised e-mail account immediately, enable two-factor authentication for the e-mail account if possible, and not to make any form of payment. As a precautionary measure, SingCERT also recommended performing anti-virus scans on all the victim's computing devices.

“ ”

As our cyber threat surface increases, potential points of vulnerability will become commonplace. All individuals need to play a conscious role in creating a safe and secure cyberspace.

– Dr Shashi Jayakumar, Senior Fellow, S Rajaratnam School of International Studies (RSIS), and Head, Centre of Excellence for National Security and Executive Coordinator, Future Issues and Technology, highlighting individuals' role in cybersecurity

¹² The Computer Misuse Act (CMA) replaces the Computer Misuse and Cybersecurity Act (CMCA) when the Cybersecurity Act came into force on 31 August 2018.



CHAPTER 3

SINGAPORE'S CYBERSECURITY STRATEGY – DEVELOPMENTS IN 2018

Launched by Prime Minister Lee Hsien Loong at the 2016 Singapore International Cyber Week, Singapore's Cybersecurity Strategy sets out Singapore's cybersecurity vision, goals and priorities to create a resilient and trusted cyberspace. It is only with a safe and trusted cyberspace that we can fully realise the benefits of technology, and secure a better future for Singaporeans.

This chapter looks back on some key milestones of the Strategy in 2018.

The Strategy comprises four pillars:

Pillar One: *Building a Resilient Infrastructure*

Pillar Two: *Creating a Safer Cyberspace*

Pillar Three: *Developing a Vibrant Cybersecurity Ecosystem*

Pillar Four: *Strengthening International Partnerships*

CSA has been coordinating the work to realise [Singapore's Cybersecurity Strategy](#) since it was launched in 2016. This chapter provides some of the highlights and achievements across the four pillars of the Strategy in 2018.

- **PILLAR ONE**

BUILDING A RESILIENT INFRASTRUCTURE



- The first pillar aims to secure our digitally-enabled economy and society, with emphasis on the Government's partnership with the private sector and the cybersecurity community to strengthen the resilience of our Critical Information Infrastructure (CII).

- **PILLAR TWO**

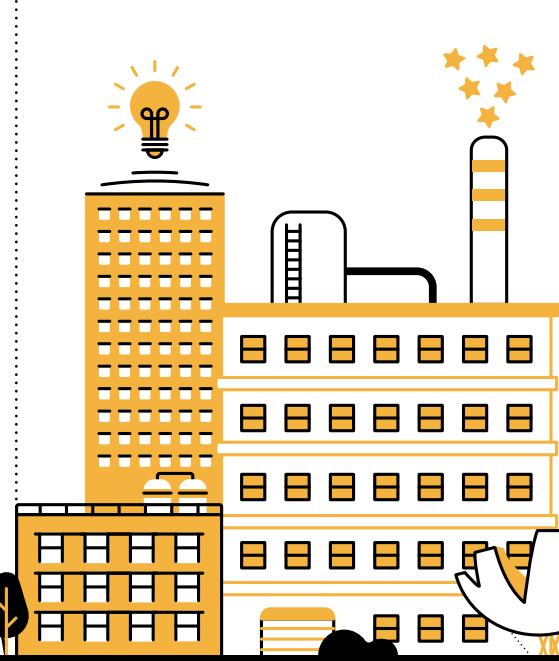
CREATING A SAFER CYBERSPACE



- Cybersecurity is a collective responsibility of the Government, businesses, individuals and the community. The second pillar looks at engaging businesses and the public to collectively build a safer and more secure cyberspace.

- **PILLAR THREE**

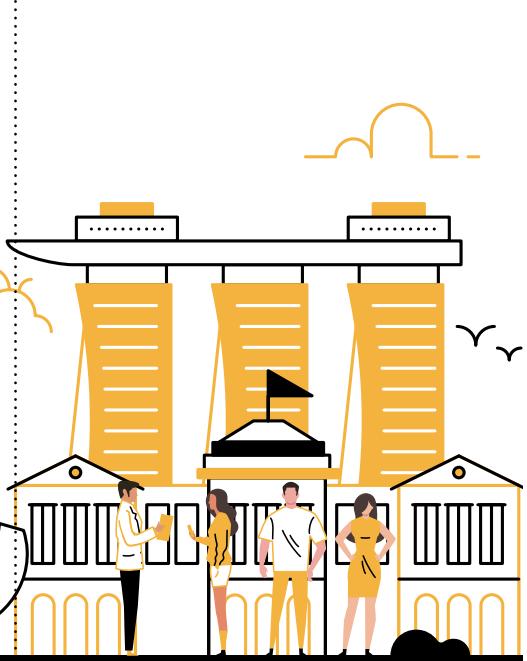
DEVELOPING A VIBRANT CYBERSECURITY ECOSYSTEM



- Cybersecurity is both a security imperative and an economic opportunity. The third pillar focuses on developing a vibrant cybersecurity ecosystem. This includes building a pipeline of talent and a vibrant industry.

- **PILLAR FOUR**

STRENGTHENING INTERNATIONAL PARTNERSHIPS



- Cyber threats are borderless. Strong international collaboration in cybersecurity is necessary to combat the threats in cyberspace. The fourth pillar emphasises the strengthening of international partnerships and creating opportunities for collaboration.

PILLAR ONE:**BUILDING A RESILIENT INFRASTRUCTURE**

Participants from the maritime sector being briefed at the opening address for Exercise CyberArk in July 2018. Source: CSA.

MEASURING MATURITY OF CII SECTORS

As part of efforts to build a resilient infrastructure, CSA launched its CII Protection Programme. Under the programme, the Readiness Maturity Index (RMI) Framework evaluates the cybersecurity maturity of CII sectors delivering essential services, and allows Sector Leads to build cyber capabilities and resilience against evolving cyber threats.

The maturity of a CII sector is measured based on respective CII owners' attributes in the RMI Framework. As of 2018, all 11 CII sectors have attained a maturity level of "measurable", which means that they have demonstrated governance, management oversight, formalised policies, assigned responsibilities, and training of people, with consistent and measurable outcomes. CSA will continue to develop appropriate cybersecurity metrics beyond the RMI framework.

CONDUCTING CYBERSECURITY EXERCISES FOR CII SECTORS

Since its formation, CSA has been conducting sector-specific Exercise CyberArk (XCA) to ensure readiness of all CII sectors in defending against increasingly sophisticated cyber-threats. In 2018, over 300 participants from the Media, Aviation, and Maritime sectors took part in XCA on separate occasions to review, exercise and validate their cyber defence capabilities and incident response plans. The 4-month planning and development cycle for each run of the exercise culminated in a 2-day Table-Top Exercise (TTX), where participants were put through a series of scenarios that gradually built up towards a cyber-crisis. Simulated media conferences were then conducted to validate the sectors' crisis communication processes. Besides the sector-specific XCA, CSA also conducts a national-level, multi-sectoral exercise – Exercise Cyber Star (XCS) – to validate the National Cyber Crisis Management System. Two runs of XCS have been conducted to date, with the third one planned for 2019.

“ ”

PSA remains fully committed towards strengthening the capabilities and resilience of our people, processes and platforms against cyber threats, to ensure the continuity of global trade and realising the "Internet of Logistics".

– Mr Ong Kim Pong, Regional CEO of PSA Southeast Asia,
on contributing to cybersecurity in Singapore's maritime sector

FEATURED TOPIC**CYBERSECURITY ACT: THE JOURNEY**

The Cybersecurity Bill was passed in Parliament on 5 February 2018 and came into force on 31 August 2018. Extensive public consultations were carried out by CSA and the Ministry of Communications and Information (MCI) in the drafting of the Act. This included closed-door consultations with key stakeholders, ranging from Government agencies, potential CII owners, industry associations and cybersecurity professionals, as well as [an open public consultation from 10 July to 24 August 2017](#).

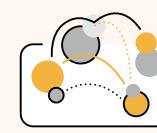
The Cybersecurity Act establishes a legal framework for the oversight and maintenance of national cybersecurity in Singapore. Its four key objectives are to:



Strengthen the protection of CII against cyber-attacks.



Authorise CSA to prevent and respond to cybersecurity threats and incidents.



Establish a framework for sharing cybersecurity information.

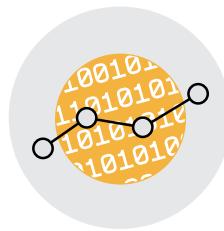


Establish a light-touch licensing framework for cybersecurity service providers (to come into force at a later date).

A key feature of the Act is the appointment of a Commissioner of Cybersecurity who is empowered by the Act to oversee all aspects of cybersecurity in Singapore. The Commissioner is assisted by Assistant Commissioners of Cybersecurity, appointed from the respective sectors, who provide the deep domain knowledge and expertise. The Cybersecurity Act provides the Commissioner and his supporting cybersecurity officers with an important regulatory instrument and statutory powers with which to strengthen Singapore's cybersecurity and combat cyber threats.

PILLAR TWO:

CREATING A SAFER CYBERSPACE



CYBERGREEN

CyberGreen aims to research and aggregate open source information to measure and create awareness of the cyber health status of a country. In partnership with the CyberGreen Institute, Singapore developed cyber health metrics for the ASEAN region to provide an overview of the overall state of cyber health while allowing regional Computer Emergency



INTERNET HYGIENE RATING AND BENCHMARKING

CSA implemented the Internet Hygiene Rating and Benchmarking (IHRB) tool for CII Sector Leads and owners in 2018. The tool incorporates a management-friendly dashboard that improves an organisation's cybersecurity situational awareness, and encourages regular self-checks by benchmarking against entities in the same or similar industries. It also enhances the organisation's Internet hygiene level through the constant

Response Teams (CERTs) to carry out remediation and mitigation efforts proactively.

In 2018, the platform added more scanning locations and enhanced the risk protocols matrix. It also provided better visualisations and allowed countries to compare their state of cyber health with others.

review of ratings based on industry-specific threats and trends.

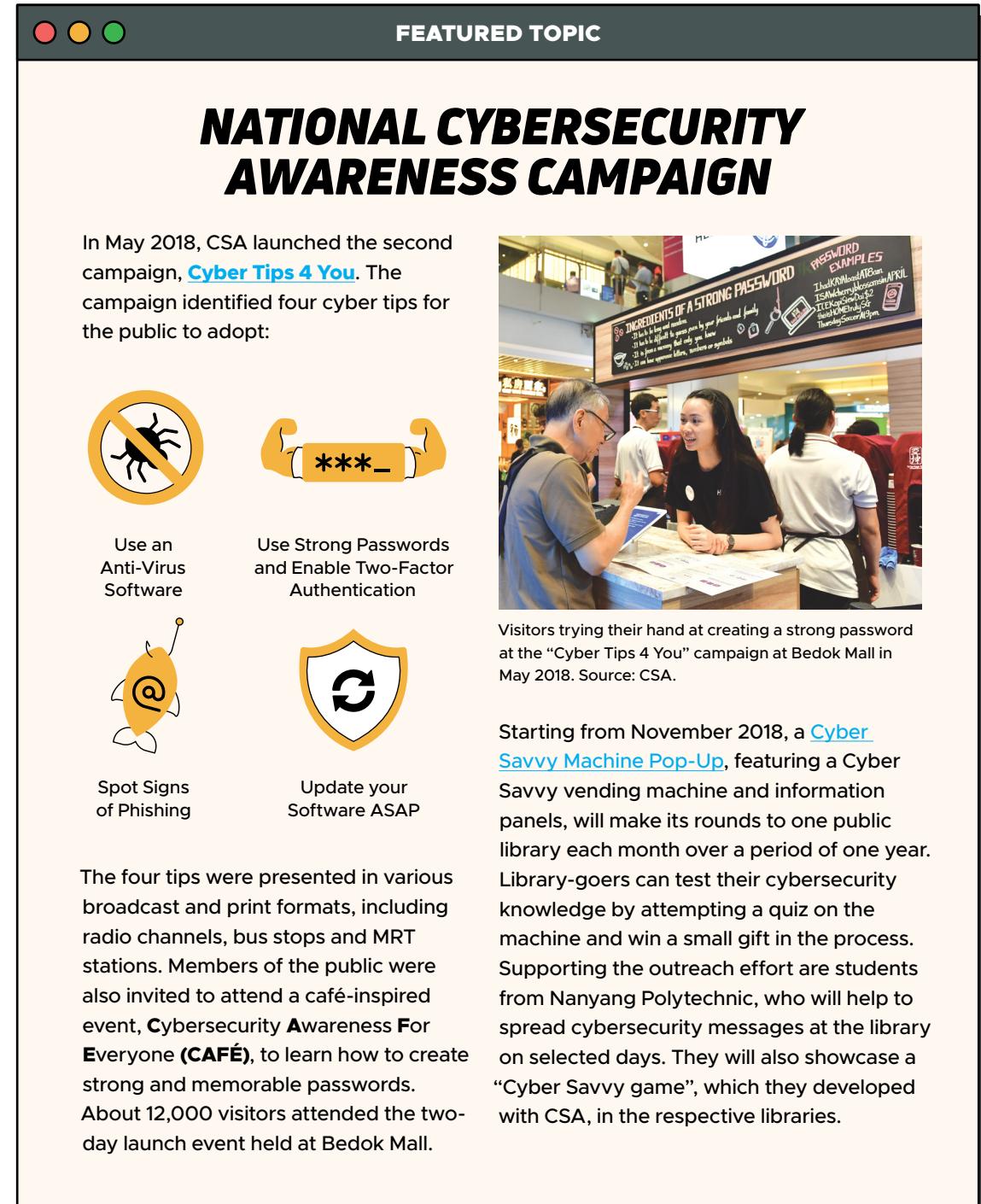
All CII Sector Leads and owners are given access to the IHRB for their continuous internal monitoring. Through this data-driven security performance rating, Sector Leads and owners are able to create a common benchmark for comparison, enabling them to come up with proactive policies to improve their cybersecurity.



FEATURED TOPIC

SECURING OUR COMMUNICATIONS – DSO CRYPTO CHIP

Through R&D, DSO National Laboratories developed the [DSO Crypto Chip](#) to protect Singapore's sensitive communications and information from potential adversaries. Its small size and low power consumption¹³ allow it to be used on space- and power-constrained systems, while meeting the challenging demands of high throughput and security. The chip incorporates DSO's unique protection mechanism, which destroys all secret data when tampered. This would render the chip useless.



¹³ The size of the DSO Crypto Chip is similar to a 50-cent coin, and the chip consumes up to 5 times less power than a commercial chip with similar performance.

PILLAR THREE:**DEVELOPING A VIBRANT CYBERSECURITY ECOSYSTEM****ENCOURAGING INDUSTRY INNOVATION AND BUILDING ADVANCED CAPABILITIES THROUGH R&D**

CSA works with Government agencies, universities, research institutes, and industry to encourage innovation for next-generation solutions to meet the needs of local and international markets. Efforts in 2018 included:

- a. [Lean LaunchPad Programme \(LLP\)](#)
Cybersecurity Track. CSA and the National Research Foundation (NRF) supported the LLP Cybersecurity Track, a 10-week experiential learning programme to equip cybersecurity researchers and young start-ups with the necessary networks, tools, and market validation to bring their inventions to market.
- b. [Industry Call for Innovation](#). To catalyse the development of innovative cybersecurity solutions and adoption by end users, CSA initiated an Industry Call for Innovation in 2018. CSA collaborated with industry¹⁴ to consolidate their cyber needs into challenge statements. The Call drew more than 70 proposals from industry solution providers to develop solutions for 10 challenge statements.
- c. [Establishing National Satellites of Excellence \(NSoEs\)](#). Anchored in local universities, the NSoEs were established to build and consolidate local research strengths in domains of national interest. Their research focuses on Trustworthy Software Systems, Mobile Systems Security & Cloud Security, and Design Science and Technologies for Secure Critical Infrastructure.
- d. [Singapore Common Criteria Scheme](#). Singapore attained the status of a Common Criteria¹⁵ Certificate Authorising Nation in January 2019. With this, local developers need not send their product overseas for certification, saving time and costs. This increases the potential of IT-security products produced in Singapore for export, strengthens Singapore's competitiveness in the global cybersecurity market, and attracts global evaluation and testing laboratories to base their operations in Singapore.
- e. [National Cybersecurity R&D Programme \(NCR\)](#). Together with NRF, CSA chairs the NCR to fund projects¹⁶ that seeks to improve the trustworthiness of cyber infrastructure with emphasis on security, resilience, and usability. Examples of funded projects include SecureAge-NUS's advanced anti-malware solution using deep learning, and Scantist-NTU's smart binary-level vulnerability assessment for cyber-attack prevention.

¹⁴ They include Ascendas-Singbridge, PacificLight Power, Singapore LNG Corporation, Singapore Press Holdings, and SMRT Corporation.

¹⁵ The Common Criteria product assurance certification, or ISO/IEC 15408, is the de facto standard for cybersecurity product certification around the world.

¹⁶ In 2018, the NCR secured additional S\$50 million of funding till 2020 to focus on four areas – cloud security, cyber forensic and assurance, applications security and edge computing, and artificial intelligence for cybersecurity.

**FEATURED TOPIC****INNOVATION CYBERSECURITY ECOSYSTEM @ BLOCK71**

A participant pitching his ideas to a panel of cybersecurity experts and representatives from investment spaces at the ICE71 Inspire programme in July 2018. Source: ICE71.

In March 2018, CSA and the Info-communications Media Development Authority (IMDA) supported the establishment of the [Innovation Cybersecurity Ecosystem at Block71 \(ICE71\)](#), for three key programmes:

1. **ICE71 Inspire** – A bootcamp targeting the academia and industry to deepen appreciation for entrepreneurship, provide networking opportunities, and enable potential entrepreneurs to get valuable insights from cyber and innovation experts.
2. **ICE71 Accelerate** – An accelerator programme for early-stage start-ups to gain access to talent, mentors, funding and local ecosystem events.
3. **ICE71 Scale** – To provide access to complimentary working space, testing facilities, regional markets and corporate support services for start-ups.

In less than a year, ICE71 has organised a total of 40 events and reached out to more than 50,000 members of the public. Its programmes have also engaged some 200 mentors who have helped guide the start-ups in their go-to-market strategies.



The Call provides an excellent platform for us to share with innovators and solution providers the challenges facing our sector, and for all of us to work together to strengthen the country's capacity to address growing cybersecurity threats.

– Mr Chong Nai Min, Vice President, Information Technology at Singapore LNG Corporation (SLNG), on CSA's Industry Call for Innovation



Smart Nation Scholars with Dr Vivian Balakrishnan (Minister for Foreign Affairs, and Minister-in-Charge of the Smart Nation initiative), Mr Teo Chin Hock (Deputy Chief Executive (Development), CSA), Mr Kok Ping Soon (Chief Executive, GovTech) and Mr Tan Kiat How (Chief Executive, IMDA) at the inaugural Smart Nation Scholarship Award Ceremony in August 2018. Source: Smart Nation and Digital Government Group.

BUILDING A WORLD-CLASS TALENT POOL

To promote the growth and development of cybersecurity students and professionals, CSA worked closely with industry, academia and associations to build a pipeline of cybersecurity talent for Singapore through the following initiatives in 2018:

- Launching the annual [Youth Cyber Exploration Programme \(YCEP\)](#) with Singapore Polytechnic, to inculcate student interest in cybersecurity.
- Co-organising the Cybersecurity [Career Mentoring Programme \(CCMP\)](#) with the Singapore Computer Society (SCS) to provide career guidance in the field of cybersecurity.
- Launching the [Student Volunteer & Recognition Programme \(SVRP\)](#) with the Association of Information Security Professionals (AiSP). CSA also supported AiSP in updating and maintaining a cybersecurity Body of Knowledge (BOK), to provide knowledge-based perspectives for industry, Institutes of Technical Education (ITEs), polytechnics and universities.
- Establishing the annual [Cybersecurity Awards](#) with AiSP and the support of seven¹⁷ other professional and industry associations, to recognise contributions to the cybersecurity ecosystem.
- Launching the Cyber Security Competency Framework (CSCF)¹⁸ in CSA and introducing it to the Whole-of-Government (WoG) for cybersecurity professionals. CSCF lays out structured development pathways to drive capability development through targeted training, professional certification and career progression.
- Launching the [Smart Nation Scholarship \(SNS\)](#) with the Government Technology Agency of Singapore (GovTech) and IMDA to develop and nurture tech leaders and talents in the Public Service. Four scholarships for cybersecurity were awarded in 2018.

¹⁷ The seven other associations are: (i) Cloud Security Alliance; (ii) ISACA Singapore Chapter; (iii) (ISC)² Singapore Chapter; (iv) IT Service Management Forum Singapore Chapter; (v) The Law Society of Singapore; (vi) Singapore Computer Society; and (vii) SGTech.

¹⁸ Adapted from the Infocomm and Technology Security Track of the National Skills Framework.

“ ”

Cybersecurity is essential to safeguard the convenience and productivity we enjoy with digital connectivity and smart devices. I look forward to serving as a cyber defender to protect our cyberspace.

– Mr Sng Yu Feng Chester, recipient of Smart Nation Scholarship, expressing his commitment to Singapore's cybersecurity

FEATURED TOPIC

MINDEF/SAF'S CYBERSECURITY EFFORTS

A key component of the Ministry of Defence (MINDEF)/Singapore Armed Forces' (SAF) cybersecurity workforce development is the [Cyber NSF \(Full-time National Service\) Scheme](#). MINDEF/SAF signed a Memorandum of Understanding (MOU) with the Singapore Institute of Technology (SIT) in February 2018 to offer an [academic work-learn programme for Cyber Specialists](#). Upon graduation, they will be deployed to operational roles in MINDEF/SAF and CSA.

MINDEF/SAF has also formed and operationalised [Defence Cyber Incident Response Teams \(DCIRTs\)](#). These DCIRTs are made up of personnel from MINDEF, SAF, Defence Science and Technology Agency (DSTA), and DSO National Laboratories. Their responsibilities include responding to cyber incidents in the Defence Sector, and supporting and augmenting CSA's cyber incident response efforts at the national-level.

PILLAR FOUR:**STRENGTHENING INTERNATIONAL PARTNERSHIPS**

ASEAN cybersecurity and ICT Ministers at the 3rd AMCC in September 2018 agreed to subscribe in-principle to the 11 voluntary, non-binding norms recommended in the 2015 UNGGE report. Source: CSA.

Singapore is an active participant at international platforms and fora on cybersecurity. As an ASEAN member, Singapore supported and contributed to regional efforts to build cybersecurity capabilities.

Singapore is partnering with the UN Office for Disarmament

Affairs (UNODA) on an online training course to promote understanding and implementation of agreements reached by the UNGGE, and a UN-Singapore Cyber Programme to build awareness of cyber norms and cyber scenario policy planning in ASEAN Member States.

“ ”

Singapore has consistently advocated for the international community to build consensus and develop a rules- and norms-based international order in cyberspace, where its users can remain safe and secure. Singapore stands ready to work with all parties toward closer international cooperation in the cyber and digital sphere.

– Mr S. Iswaran, Minister for Communications and Information, and Minister-in-Charge of Cybersecurity, on Singapore's efforts in building a safe and secure cyberspace

In April 2018, under Singapore's ASEAN Chairmanship, a first-ever [ASEAN Leaders' Statement on Cybersecurity Cooperation](#) was adopted at the 32nd ASEAN Summit. Singapore has worked closely with ASEAN Member States, industry partners and international organisations such as the INTERPOL Global Complex for Innovation to follow up on tasks set by ASEAN Leaders.

Singapore hosted the annual ASEAN Ministerial Conference on Cybersecurity (AMCC) over the past three years to bring together Ministers from all ASEAN Member States who are responsible for ICT and cybersecurity issues, including the ASEAN Secretary-General. We helped to draft the ASEAN Cybersecurity Cooperation Strategy, which was adopted in March 2017 and provides a blueprint for coordination of cybersecurity capacity building efforts. Participants at the 3rd AMCC in September 2018 agreed to [subscribe in-principle to the 11 voluntary, non-binding norms](#) recommended in the 2015 Report of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE). They also agreed to focus on regional capacity building in implementing these norms.

FEATURED TOPIC

ENHANCING CAPACITY AND CAPABILITIES IN CYBERSECURITY TOGETHER

Singapore will launch the \$S30 million **ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE)** in 2019, an extension of the \$S10 million [ASEAN Cyber Capacity Programme](#) that has been contributing to the enhancement of ASEAN's cybersecurity capabilities in both the technical and policy aspects. The ASCCE will complement existing initiatives, such as the ASEAN-Japan Cybersecurity Capacity Building Centre in Thailand. It will focus on strengthening ASEAN Member States' cyber strategy development, legislation and research capabilities, increasing technical expertise and incident response skills of national CERTs in the region. The ASCCE will also promote CERT-to-CERT open-source information sharing.

**FEATURED TOPIC****GALVANISING GLOBAL EFFORTS**

In 2017, the National Cyber Security Centre of The Netherlands (NCSC-NL) together with CSA conducted a landscape study to identify gaps in Internet of Things (IoT) security standards and technology. The findings were refined into a set of working initiatives for IoT security that were jointly proposed by Singapore and The Netherlands at the Annual Meeting of the Global Forum on Cyber Expertise (GFCE), co-branded with SICW's IoT Security Roundtable, during [SICW 2018](#). The initiatives aimed to lead and galvanise global efforts in creating a safer and more secure IoT.

In the initial phase of the IoT Security Initiative, NCSC-NL and CSA agreed to prioritise the efforts on three most critical areas, namely, Certification and Testing, Supply Chain Security, and Unique Device Identities.

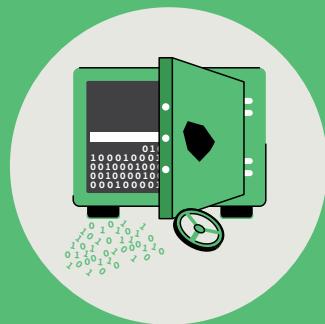
LOOKING AHEAD

ANTICIPATED TRENDS

What would the next few years portend for cybersecurity? The combination of technological advancements and our transition into ever higher levels of connectivity means that cyber threats will become even more targeted, sophisticated and deceptive. These are six trends we foresee happening in the near future:

1

MORE FREQUENT DATA BREACHES



Data has become the most valued ‘commodity’ in cyberspace, which means cybercriminals will try even harder to breach computer databases – especially those that store large amounts of private and personal information.

2

INCREASED THREAT TO GLOBAL SUPPLY CHAINS



Threat actors will focus on disrupting supply chains which have become highly interconnected and automated. Industries dominated by a few companies are especially vulnerable, as problems in one stage of production may potentially lead to a breakdown in the entire supply chain.

3

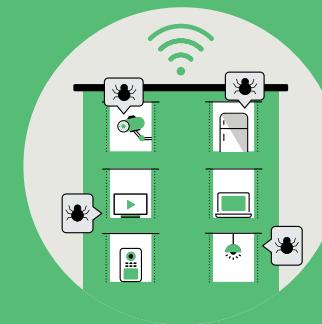
MORE DISRUPTIVE ATTACKS AGAINST THE CLOUD



With more databases hosted in the cloud, threat actors will be on the lookout for potential vulnerabilities in cloud infrastructure. While their primary goal remains data theft, threat actors will also try to exploit cloud services for other malicious aims, such as to amplify Distributed Denial-of-Service (DDoS) attacks.

4

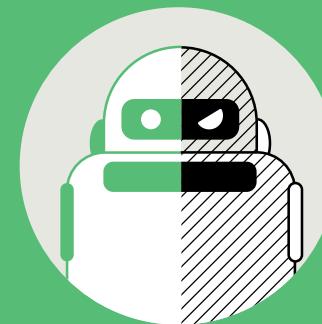
GREATER RISKS FOR SMART BUILDINGS AND CONNECTED SYSTEMS



As buildings and factories become ‘smarter’ – through the proliferation of Internet of Things (IoT) devices and connected industrial control systems (ICS) – the risk of them being attacked to hold their owners to ransom, or exploited to spread malware or conduct DDoS attacks, also increases.

5

ARTIFICIAL INTELLIGENCE – DOUBLE-EDGED SWORD



Artificial Intelligence (AI) will be a double-edged sword for cybersecurity – it can significantly enhance the capabilities of security systems, such as in anomaly detection and response. However, threat actors can also leverage AI to search for vulnerabilities in computer systems, and create ‘smarter’ malware.

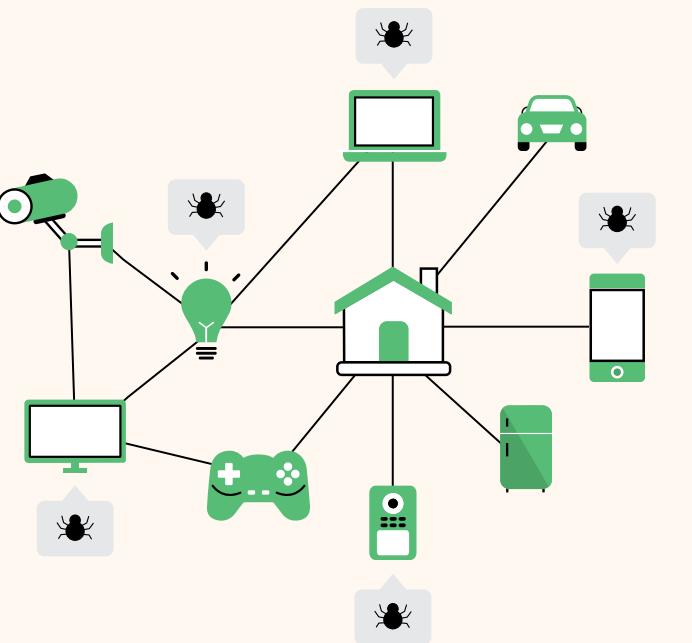
6

BIOMETRIC DATA MORE VALUABLE TO THREAT ACTORS



As biometric authentication becomes increasingly common, threat actors will shift to target and manipulate biometric data, to build virtual identities and gain access to personal information.

FEATURED TOPIC



IoT – THE INSECURITY OF THINGS?

The IoT has been an industry buzzword for years. As we become increasingly reliant on interconnected devices in every aspect of our lives, there lies the concomitant need to protect potentially billions of them from intrusions and interference that could compromise personal privacy or threaten public safety.

In recent years, massive IoT botnets such as *Mirai*, *Hajime* and *Persirai* have shown themselves to be capable of globally destructive attacks. A report released by cybersecurity firm *F5 Labs* last year stated that Singapore has constantly appeared in the top five

destinations for IoT attacks¹⁹. There are also privacy concerns when IoT devices are being targeted, with the Police having received reports of victims finding their IP cameras compromised and sometimes manipulated to film in a particular direction.

has never been more crucial to secure this interconnected world that we live in. For a start, every stakeholder must play their role in ensuring basic security mistakes – such as open ports, faulty credentials, and data sent without encryption – are excised from equipment.

¹⁹ Boddy, Sara and Shattuck, Justin. "The Hunt for IoT: The Growth and Evolution of Thingbots Ensures Chaos," F5 Labs – Threat Analysis Report, 13 March 2018, <https://www.f5.com/labs/articles/threat-intelligence/the-hunt-for-iot-the-growth-and-evolution-of-thingbots-ensures-chaos>.

GLOSSARY

Term	Definition
Advanced Persistent Threat (APT)	An attack in which perpetrators successfully gain access to a targeted system, and stay undetected for a long period of time to exfiltrate, modify, or destroy critical data. APTs can also refer to the advanced, and often state-linked or state-sponsored threat actors that conduct extended campaigns, such as cyber espionage.
Attack Surface	Referring to all vulnerable resources of a system, or the sum of the points through which an attacker could try to enter an environment.
Bot/Botnet	An automated software program used to carry out specific tasks. A botnet is a network of compromised computers infected with malicious bots, controlled as a group without the owners' knowledge.
Brute-force attack	A trial-and-error method which involves trying various combinations of usernames and passwords repetitively to gain access into a computer system or website.
Command and control (C&C) servers	Centralised devices operated by attackers to maintain communications with compromised systems (known as botnets) within a target network.
Critical Information Infrastructure (CII)	The computer or computer system necessary for the continuous delivery of an essential service, which the loss or compromise thereof will have a debilitating effect on the availability of the essential services in Singapore.
Cryptocurrency	A form of digital token secured by cryptography and can be used as a medium of exchange, a unit of account, or a store of value. Used synonymously with digital or virtual currency. Examples include Bitcoin, Ether, and Litecoin.
Crypto-jacking	The unauthorized use of a computer or computer system by cybercriminals to mine cryptocurrency.
Cybercrime	Refers to cyber-extortion, online cheating cases, and offences under the Computer Misuse Act (CMA) such as unauthorised access of computer material and unauthorised use of computer service.
Cyberspace	The complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form. Singapore's cyberspace includes domain names with ".SG" or Singapore-mentions, Internet Protocol (IP) addresses used in Singapore, and Internet Service Providers (ISPs) located here.

Term	Definition
Dark Web	A section of the Internet only accessible through software that allows users to remain anonymous or untraceable. The Dark Web is part of the Deep Web. The Deep Web encompasses web resources that search engines like Google and Yahoo cannot find, such as legitimate but private resources (e.g. e-mail), or public resources behind a paywall or login wall (e.g. paid journal subscriptions).
Data Breach	The unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks of personal data/information in an organisation's possession or under its control.
Denial of Service (DoS) / Distributed DoS (DDoS)	Where an attacker attempts to prevent legitimate users from accessing information or services online. The most common and obvious type of DoS attack occurs when an attacker "floods" a network with information. In a distributed DoS attack, an attacker takes unauthorised control of multiple computers, which may be harnessed as a botnet, to launch a DoS attack.
Hacktivists	An individual or group who wants to undermine the reputation or destabilise the operations of an entity, or to publicise their political or social agenda and gain recognition, usually by hacking an organisation's website.
Industrial Control Systems (ICS)	ICS belong to a class of operational technology (OT) systems used in nearly every industrial sector to monitor, control and automate industrial operations and processes.
Internet of Things (IoT)	The vast network of everyday objects, like baby monitors, printers, televisions, and autonomous vehicles that are connected to the Internet.
Keylogging	The use of a software to record every keystroke that is made by a user on a computing device. It is usually done covertly for malicious intent, such as gaining knowledge of passwords.
Malware	Malicious software intended to perform unauthorised processes that will have adverse impact on the security of a computer system. E.g. virus, worm, Trojan horse, spyware and adware.
Personal Data / Information	Data which, on its own (e.g. full name, NRIC number) or in combination with other available data (e.g. medical or educational information), can be used to distinguish or trace an individual's identity.
Phishing	A common technique used by threat actors to trick people (typically through e-mails) into divulging personal information, transferring money, or installing malware.
Ransomware	Malware that encrypts files on a victim's device, rendering them unusable until a ransom is paid, usually in the form of Bitcoin or other cryptocurrency. It may spread through phishing e-mails that contain malicious attachments or links, or malicious pop-ups that appear when users access unsafe websites.
Spoofing	Tricking computer systems or other users by hiding or faking one's true identity. Commonly spoofed targets include e-mails, IP addresses, and websites.

**If you have any feedback on this publication,
or wish to find out more about Singapore's
efforts in cybersecurity, please visit the
following websites or contact us:**

Cyber Security Agency of Singapore

Website:

www.csa.gov.sg

General enquiries/feedback:

contact@csa.gov.sg

GoSafeOnline

Website:

www.csa.gov.sg/gosafeonline

General enquiries/feedback:

gosafeonline@csa.gov.sg

**If you wish to report a cybersecurity incident,
please contact:**

SingCERT

Hotline for incident reporting:

(+65) 6323 5052

E-mail for incident reporting:

singcert@csa.gov.sg

If you wish to seek scam-related advice:

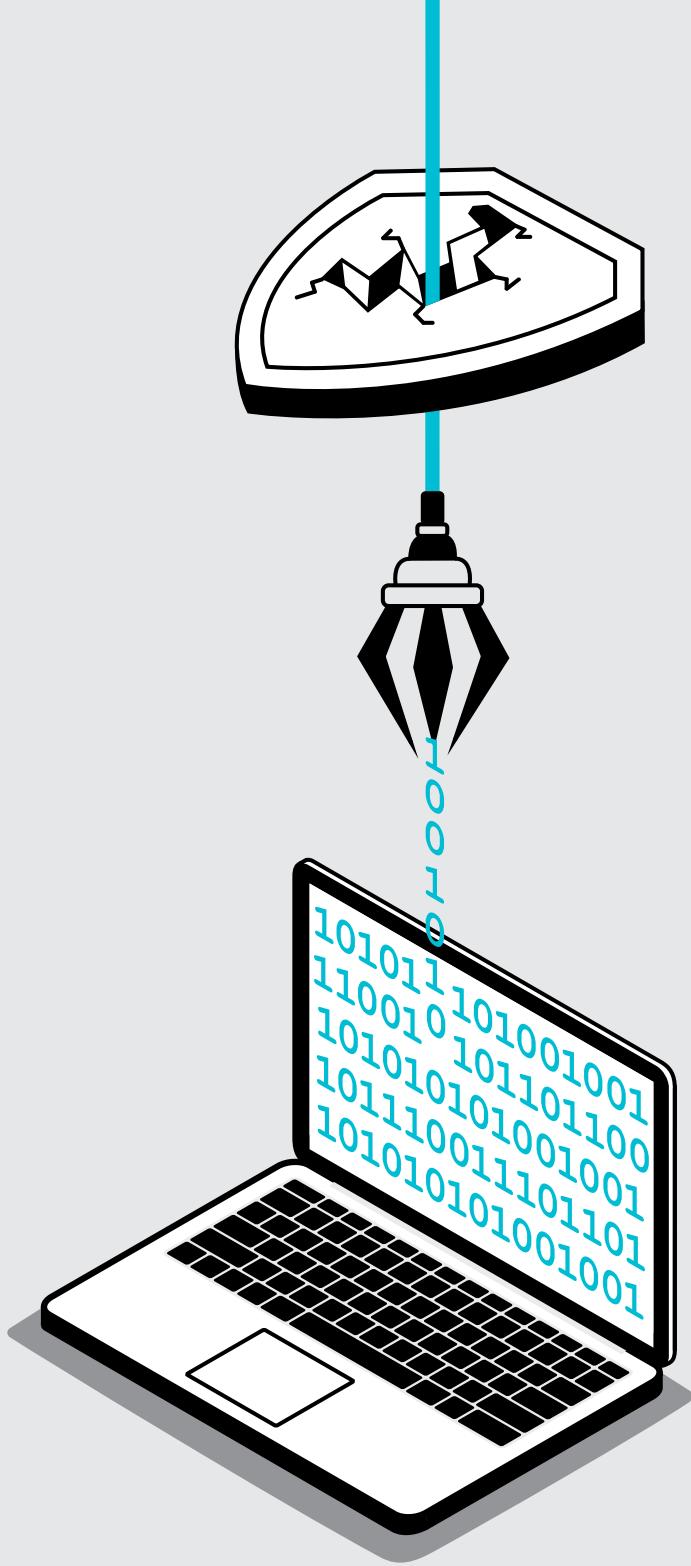
ScamAlert

Contact anti-scam helpline:

(+65) 1800 722 6688

Visit ScamAlert website:

www.scamalert.sg



CSA
SINGAPORE