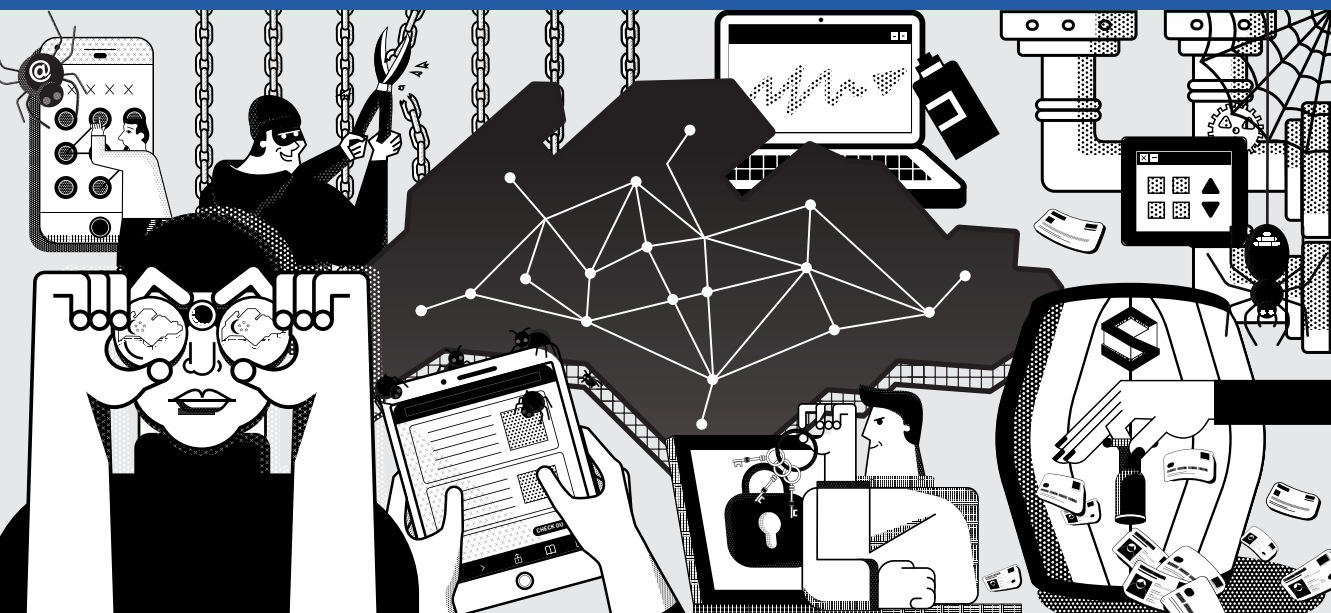
SINGAPORE CYBER LANDSCAPE 2017



CONTENTS

Singapore Cyber Landscape 2017

By Cyber Security Agency of Singapore
with special thanks to the Singapore Police Force
and the Defence Cyber Organisation

ISBN: 978-981-11-7062-1

Cyber Security Agency of Singapore
www.csa.gov.sg

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

FOREWORD

2017 saw some high-profile cyber-attacks globally on national institutions and Critical Information Infrastructure. More worryingly, there was a shift from profit-motivated attacks towards those aimed at causing massive disruptions, such as the *WannaCry* ransomware campaign.

Given Singapore's connectivity, what happens globally is often immediately felt here. *WannaCry* similarly hit some businesses here, but the impact was not as widespread or disruptive as seen elsewhere. The discovery of the "kill switch" over the weekend, when most businesses were shut, helped. However, other cyber-attacks struck elsewhere against government agencies, businesses, and individuals. The breaches suffered by two of our universities and the Ministry of Defence's Internet access system during the course of 2017 reflect the increasingly targeted nature of cyber-attacks. These attacks were carefully planned, and were not the work of casual hackers or criminal gangs.

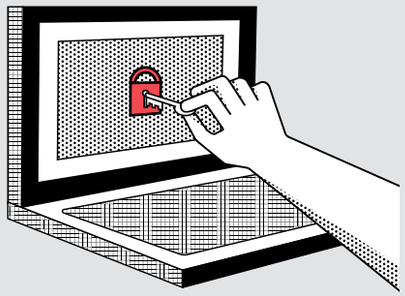
Cybersecurity is not just about threats, but also opportunities – for businesses and individuals. I am particularly encouraged to see greater awareness and interest in cybersecurity among the youth. Six talented youth from Singapore pitted their skills against some of the best in the Cyber Security Challenge UK in November 2017, in rounds of tests that included fending off live cyber-attacks. As cyber-attacks grow in scale and complexity, we will need to grow the talent pool to defend our cyberspace.

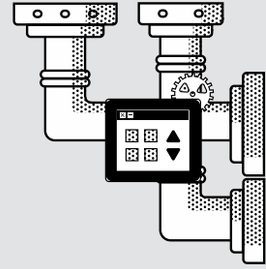
As we review Singapore's cyber landscape in 2017, we hope to draw out the lessons learnt from the incidents of the past year, so that we can be better equipped to tackle the threats in the future. Singapore's move towards being a Smart Nation will bring benefits to many. But we need everyone to be savvy users of this connectivity. We know that we are only as strong as our weakest link. Therefore, we all need to do our part to ensure basic cyber hygiene is in place, such as using stronger passwords, to keep our networks trusted and secure. We hope that this second edition will provide more practical information for you to do your part in keeping Singapore's cyberspace safe and trustworthy for all.

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

OVERVIEW OF
CYBER THREATS IN 2017

As a highly-connected country, Singapore's cyber landscape mirrors global trends. These facts and figures – likely only the tip of the iceberg – highlight the challenges in cyberspace that we need to tackle together.





GLOBAL INCIDENTS

- **Feb**: Mass **defacement** of 2 million WordPress websites due to unpatched vulnerability
- **May**: *WannaCry* **ransomware** hits 200,000 victims in over 150 countries
- **Jun**: *NotPetya* **ransomware** targets Ukraine; spreads globally
- **Sep**: Over 140 million customers exposed by Equifax **data breach**
- **Oct**: All 3 billion Yahoo accounts hit in 2013 **data breach**
- **Oct**: *Bad Rabbit* **ransomware** affects systems in Russia and Eastern Europe
- **Dec**: *Triton* **malware** threat to industrial control systems

Jan | Feb | Mar | Apr | May | Jun | Jul | Aug | Sep | Oct | Nov | Dec

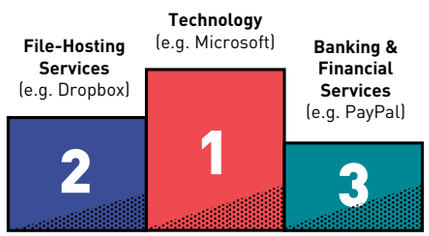
SINGAPORE INCIDENTS

- **Feb**: Details of **850** personnel **stolen** in **breach** of MINDEF's I-net system
- **May**: NUS & NTU breached in **APT attacks**
- **Aug**: Multiple website **defacements**
- **Sep**: Personal data of 5,400 customers compromised in insurance company **data breach**
- **Nov**: First conviction of **Dark Web-related crime** in Singapore
- **Dec**: Uber's 2016 **data breach** affected 380,000 users in Singapore
- Schools hit by **ransomware**

PHISHING

23,420
phishing URLs with a Singapore-link were detected.

Commonly spoofed websites:



WEBSITE DEFACEMENTS

2,040
Singapore-linked website defacements were detected.

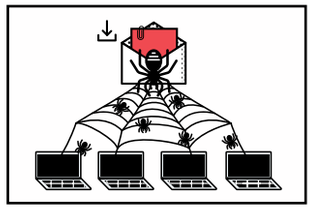
Main targets: SMEs from sectors such as manufacturing, retail, and information and communications technology.

MALWARE

750
unique Command and Control servers were observed in Singapore.

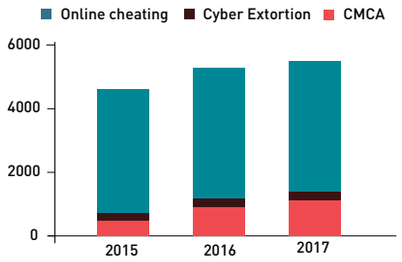
2,700
botnet drones (compromised computers infected with malicious programs) with Singapore IP addresses were observed daily, on average.

>400
malware variants were detected. *Conficker, Mirai, Cutwail, Sality* and *WannaCry* accounted for over half the observed daily infections.



CYBERCRIME

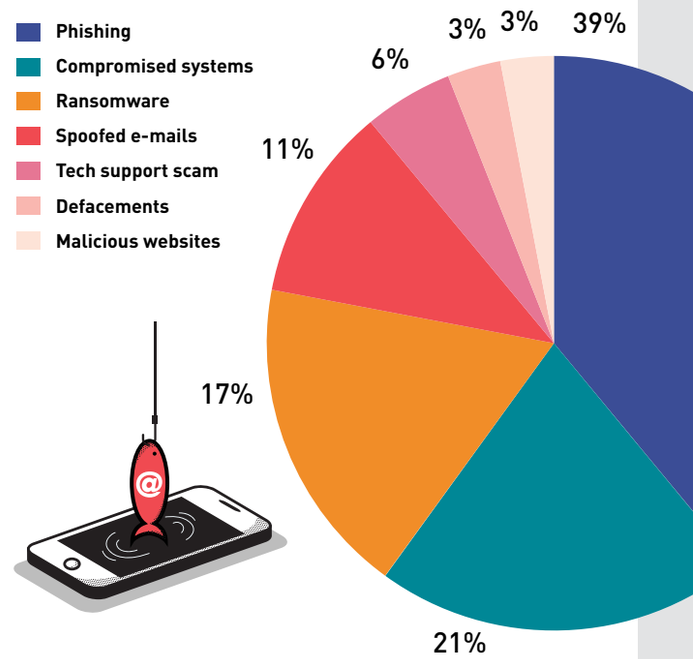
5,430
cybercrime cases accounted for 16.6 per cent of overall crime.



RANSOMWARE

25
cases of ransomware were reported to SingCERT.

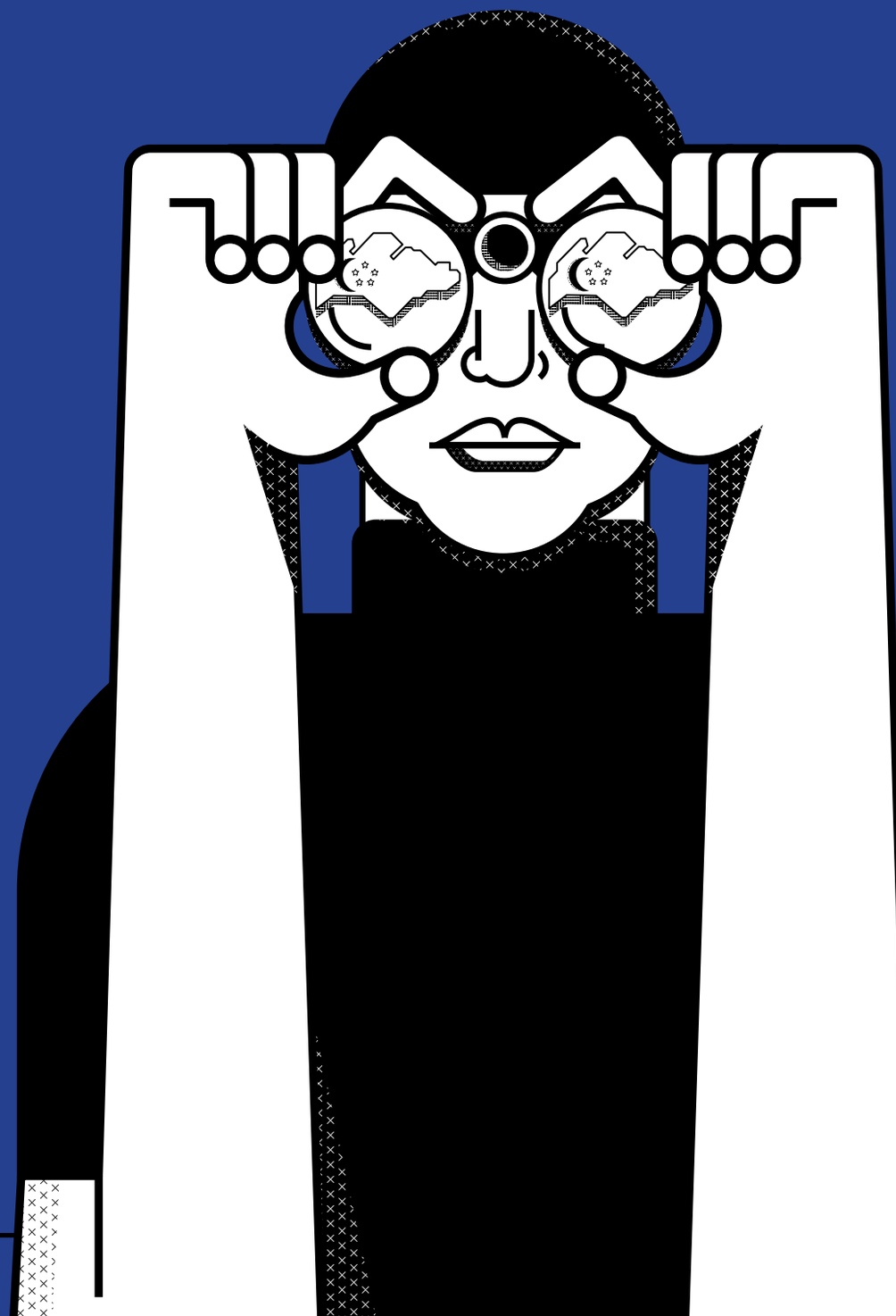
TYPES OF THREATS REPORTED TO SINGCERT*



*Approximate percentages

CHAPTER 1

CYBER THREATS SINGAPORE FACES



The second edition of the **Singapore Cyber Landscape** reviews the cybersecurity situation in 2017 against the backdrop of global trends and events. Through case studies of incidents in Singapore, the publication aims to offer insights and practical lessons to mitigate and recover from cyber-attacks. This edition also features some emerging trends and issues that Singapore is watching closely.

THREATS TO CRITICAL INFORMATION INFRASTRUCTURE

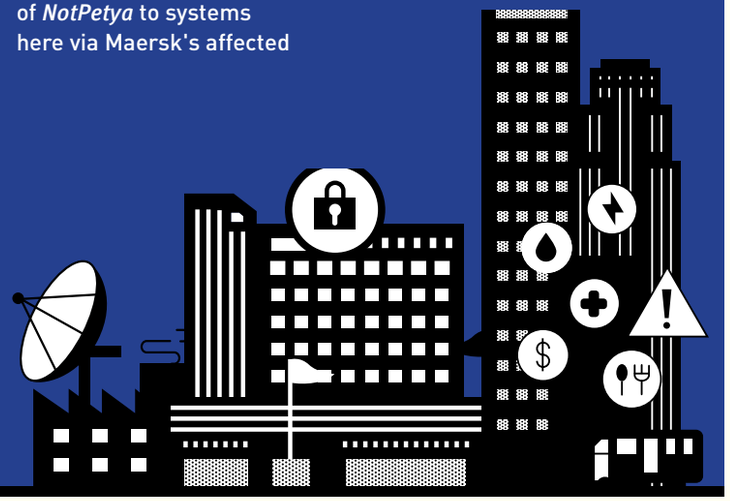
Critical Information Infrastructure (CII) sectors[1] deliver essential services, and a compromise of their systems can have a debilitating impact on Singapore's society and economy. Cyber-attacks targeting CIIs can spill over to unintended victims connected to these systems.

The *NotPetya* ransomware infection in June 2017 was believed to have targeted Ukraine, where more than 12,500 machines in its financial, energy, and government sectors were affected.

The attack also spread globally to at least 64 other countries.[2] International shipping giant Maersk and pharmaceutical heavyweight Merck were some of the large multi-national companies that suffered collateral damage. *NotPetya* crippled Maersk's computer systems and it had to revert to tracking cargo manually.

Maersk's partners and respective maritime authorities in international ports had to make relevant accommodations. In Singapore, the Maritime and Port Authority of Singapore (MPA) and terminal operator PSA Singapore worked closely to rapidly step up cybersecurity measures. That prevented the spread of *NotPetya* to systems here via Maersk's affected systems, while ensuring that Singapore's port operations went on.

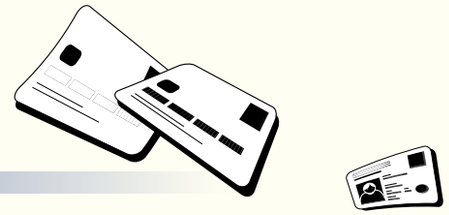
The *NotPetya* infection reiterated the need for CII sector readiness and incident response planning. The interconnectedness and interdependencies of global maritime and other supranational networks underscore the importance of international cooperation in responding to and mitigating the effects of cyber-attacks.



[1] Singapore's 11 CII sectors are: Aviation, Banking & Finance, Energy, Government, Healthcare, Infocomm, Land Transport, Maritime, Media, Security & Emergency, and Water.

[2] "New Ransomware, Old Techniques: Petya Adds Worm Capabilities," Microsoft Secure Blog, Microsoft 29 June 2017, https://cloudblogs.microsoft.com/microsoftsecure/2017/06/29/windows-10-platform-resilience-against-the-petya-ransomware-attack/.

THREATS TO BANKING & FINANCE

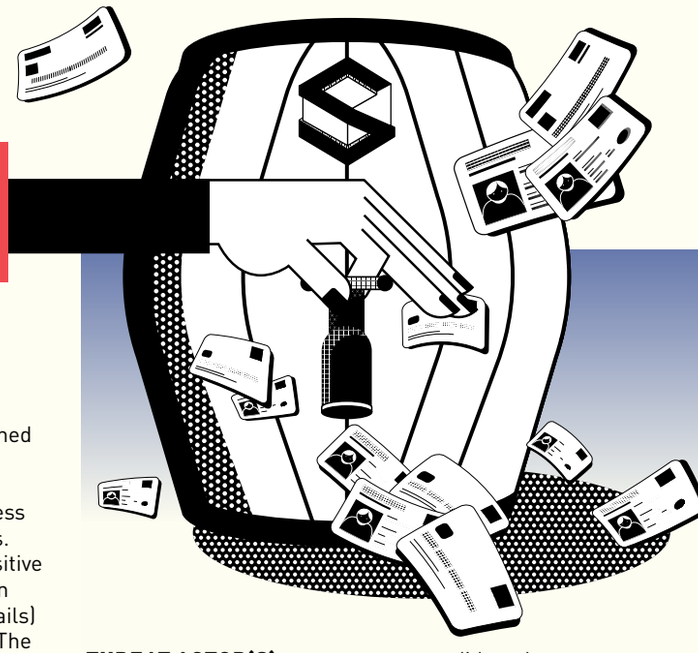


The Banking & Finance sector remains a top target for cyber threat actors given the valuable and sensitive financial data held by these companies.

The Association of Banks in Singapore (ABS), with the support of the Monetary Authority of Singapore (MAS), conducts regular industry-wide exercises to strengthen safeguards in the sector. The most recent one, Exercise Raffles V, was conducted in August 2017 and involved 139 financial institutions. Participants exercised their response plans to various scenarios, including cyber threats.

"AS WE GO MORE DIGITAL AND ONLINE, CYBER RISKS WILL MOUNT. THESE RISKS NEED TO BE MANAGED WELL TO MAINTAIN PUBLIC TRUST AND CONFIDENCE IN TECHNOLOGY. TO FULLY HARNESS THE BENEFITS OF DIGITAL TECHNOLOGY, WE MUST BUILD ROBUST CYBER DEFENCES AND HAVE EFFECTIVE RECOVERY PLANS WHEN THINGS GO WRONG."

- MR RAVI MENON, MANAGING DIRECTOR, MONETARY AUTHORITY OF SINGAPORE



CASE STUDY

Data Breach in Banking & Finance Sector

WHEN

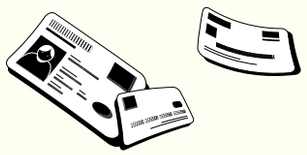
September 2017

BACKGROUND

The website of a Singapore insurance company was breached, compromising the personal data of 5,400 customers, including their e-mail addresses, mobile numbers and dates of birth.

FINDINGS

The attackers accessed the company's system through an unpatched vulnerability.



CASE ANALYSIS

The threat actors exploited an unpatched vulnerability in the company's system. This gave them access to customer records. Fortunately, no sensitive financial information (e.g. credit card details) was compromised. The company made a police report and logged a case with the Personal Data Protection Commission (PDPC).

TACTICS, TECHNIQUES & PROCEDURES

Breached website through exploitation of an unpatched vulnerability.

THREAT ACTOR(S) INVOLVED

Unknown malicious actors compromised the company's website.

FOLLOW-UP ACTION

The vulnerability in the affected server was patched to prevent further compromise. The company also checked that its other servers did not have the same vulnerability. All affected customers were notified via e-mail or phone call.

Companies that collect and hold personal data are attractive targets for cybercriminals, and should ensure that their systems are updated and the proper safeguards are in place.

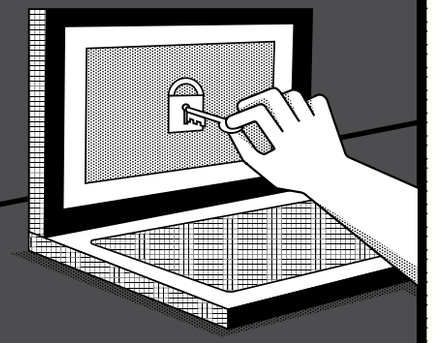
SPECIAL TOPIC

BREACHES OF PERSONAL DATA

Personal data breaches are growing in scale and frequency, with significant disclosures in 2017 coming from tech company Yahoo, US credit bureau Equifax, and ride-sharing company Uber. The Uber breach exposed the names, e-mail addresses, and mobile phone numbers of an estimated 380,000 users in Singapore. The matter is being investigated by the PDPC.

Stolen personal data is often sold in underground markets, and used for identity theft, fraudulent transactions, and social engineering. Systems that store and transmit personal data are therefore highly attractive and profitable targets for cyber-attackers.

As these systems continue to proliferate, especially with the greater digitalisation of services such as online banking and shopping, we need to ensure that cybersecurity measures are robustly implemented and regularly reviewed.



THREATS TO GOVERNMENT

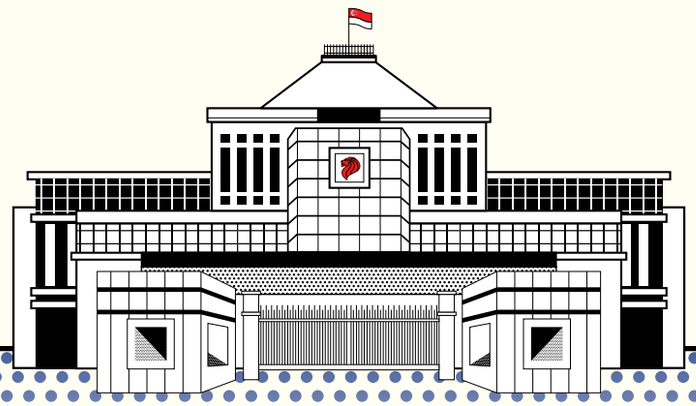
In 2017, Government agencies faced a range of cyber threats including system intrusions and spoofed websites.

Some schools were infected with ransomware on Internet-facing laptops. In a separate incident, the Ministry of Defence's (MINDEF) Internet access system (I-net) was breached in a targeted and carefully planned cyber-attack. The affected devices in both cases were not connected to Government networks and no classified information was compromised.

To reduce the opportunity for cyber-attacks over the Internet and better protect systems and citizens' data, Government agencies separated Internet surfing from Government networks in 2017.

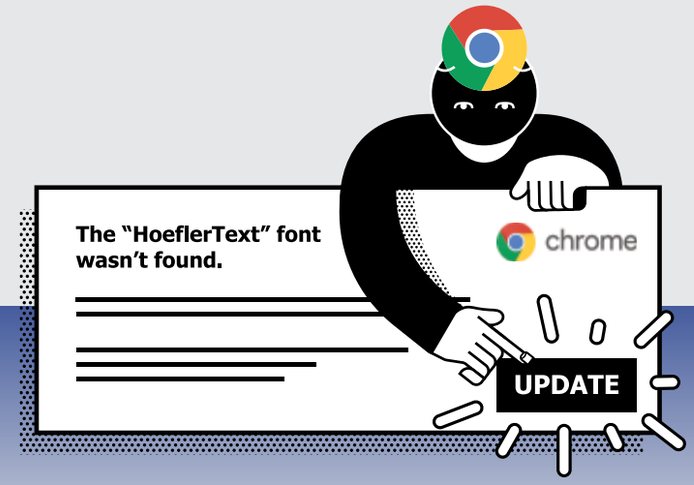
As part of on-going efforts to beef up cyber defences for the Government's systems, a Government Security Operations Centre (SOC) equipped with artificial intelligence and advanced analytics will be set up by 2020 to replace the current Cyber Watch Centre. Government and private sector organisations are encouraged to set aside at least 8 per cent of Information Technology (IT) budgets for cybersecurity, as an investment to manage risk.

Prime Minister (PM) Lee Hsien Loong (seated, centre) being briefed in 2017 about CSA's crisis management processes during a major cyber incident. PM Lee was accompanied by (L-R) Deputy PM (DPM) and Coordinating Minister for National Security Teo Chee Hean, and Minister for Communications & Information and Minister-in-charge of Cyber Security Dr Yaacob Ibrahim. Source: MCI.



"IT'S NO SECRET THAT GOVERNMENT AGENCIES, INCLUDING MINDEF, ARE PRIME TARGETS, AND WE ARE UNDER CONSTANT CYBER-ATTACK. BECAUSE OF THIS, WE NEED TO CONTINUALLY BE VIGILANT AND IMPROVE OUR CYBER DEFENCES SO THAT WE REMAIN RESILIENT AGAINST CYBER-ATTACKS."

- MR DAVID KOH, IN COMMENTS TO THE MEDIA IN FEBRUARY 2017 AS DEPUTY SECRETARY (TECHNOLOGY), MINISTRY OF DEFENCE, FOLLOWING AN I-NET BREACH AT THE MINISTRY



CASE STUDY

Ransomware in Schools

WHEN

June 2017

BACKGROUND

CSA received reports that staff laptops at some schools were infected with ransomware after users visited malicious websites or accessed spoofed e-mails that executed malicious code.

FINDINGS

Attackers hijacked websites to display a fake error message that prompted users to click on a link to update a "Chrome Font Pack".

CASE ANALYSIS

The attacks were assessed to be opportunistic rather than targeted. The ransomware was triggered when the individuals clicked on unfamiliar links or opened malicious e-mail attachments from their personal e-mail accounts.

TACTICS, TECHNIQUES & PROCEDURES

Phishing e-mails; websites hosting malicious files.

THREAT ACTOR(S) INVOLVED

Unknown hackers motivated by financial gain or seeking to cause disruption.

FOLLOW-UP ACTION

The infected laptops were quarantined, re-formatted, and had their programs reinstalled.

In all instances, no ransom was paid, and no classified information was compromised.

THREATS TO BUSINESSES

Businesses are common targets of cyber-attacks. Small and medium enterprises (SMEs) are especially vulnerable, as they often lack the resources or know-how to adopt appropriate cybersecurity practices. In one survey of Singapore SMEs, more than one third of respondents admitted to having no cyber protection.[3]

According to the Singapore Police Force (SPF), a growing threat that businesses in Singapore face is e-mail impersonation scams. Victims may not realise that their business partners' e-mail accounts have been hacked or spoofed. They follow the instructions in the e-mail, thinking that it is a fund transfer to their partner. In effect, the funds are transferred to the attacker's account. These scams may involve large sums of money. SPF observed 328 cases in 2017, up from 257 in 2016. Businesses lost around S$43 million in 2017, with one case alone accounting for close to S$5.7 million.

Almost 40 per cent of the 146 cases reported to SingCERT in 2017 involved businesses, particularly SMEs. Most of the cases involved phishing attacks and ransomware.

Businesses are encouraged to invest in cybersecurity solutions to protect themselves, especially since the cost of a cyber-attack can be far higher than the cost of getting protected in the first place. A cyber-attack on a business could hurt its computer systems and disrupt its entire business operations. It could also result in the loss of customer confidence, and cause collateral damage to business partners.

"THANKS TO SINGCERT FOR YOUR HELP WITH THE VIRUS ATTACK ON OUR COMPANY SERVER. WE HAVE SUCCESSFULLY RECOVERED ALL DATA, INCLUDING FROM OUR BACKUPS, FOLLOWING THE STEPS AS YOU ADVISED."

- MISS MAY LEE, ACCOUNTS EXECUTIVE AT A PRECISION ENGINEERING COMPANY, APPROACHED CSA IN AUGUST 2017 FOR ASSISTANCE WITH A RANSOMWARE ATTACK

CASE STUDY

RAT-infested Businesses

WHEN

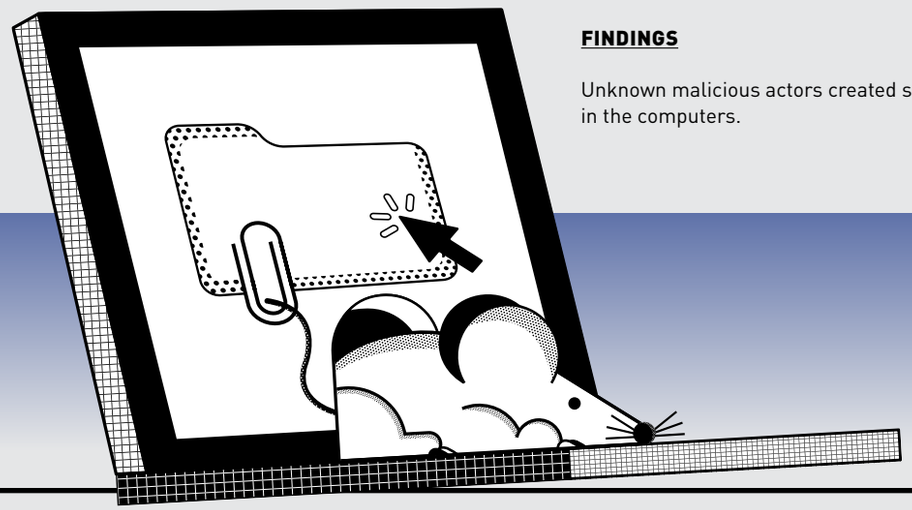
July 2017

BACKGROUND

SingCERT investigated a case of computers that had been compromised by malware which allowed attackers to gain entry into them from another location. Two companies in Singapore and one in Malaysia providing industrial component servicing and supply were affected.

FINDINGS

Unknown malicious actors created suspicious files in the computers.



CASE ANALYSIS

SingCERT found that the computers were infected by a remote access trojan (RAT) that let the attackers control the companies' systems without physical access. Such infections usually arise when a person clicks on unfamiliar e-mail links or attachments. No data was lost or leaked in this instance.

TACTICS, TECHNIQUES & PROCEDURES

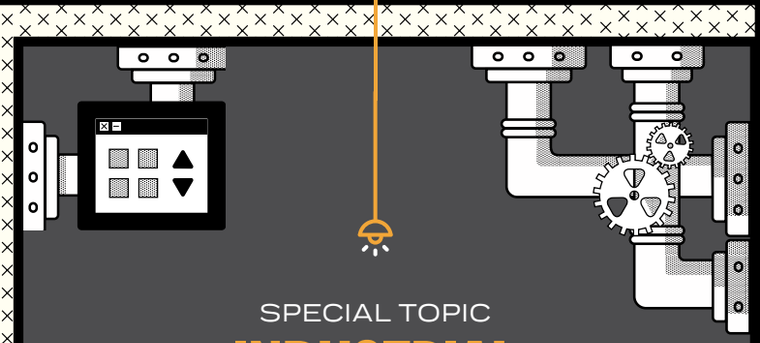
Phishing e-mail; RAT.

FOLLOW-UP ACTION

SingCERT notified its Malaysian counterpart (MyCERT) about the compromised computer there. It explained the situation to the two affected Singapore companies and assisted them in cleaning up the devices.

The victims were advised to change the passwords for their e-mail accounts, so that attackers would not be able to enter the systems again using the old passwords. SingCERT also advised the victims to maintain regular and reliable backups of their data.

[3] Survey conducted in September 2017 by QBE Singapore with 402 local SMEs. "Press Release: Survey shows only 14 per cent of local SMEs intend to internationalise," QBE Singapore press release, 29 January 2018, http://www.qbe.com.sg/retrieveDocument?docName=SME_press_release_and_Infographics_29_Jan_2018.pdf.



SPECIAL TOPIC

INDUSTRIAL CONTROL SYSTEMS

Industrial Control Systems (ICS) refer to the hardware and software used to control equipment and process data in industrial sectors. In Singapore, ICS are found in CII sectors such as Energy, Land Transport, Media, Telecommunications, and Water.

Most ICS are legacy systems originally meant to operate in closed network environments unconnected to the Internet. Today, ICS are increasingly connected to Internet-facing networks to facilitate new processes and boost performance (e.g. data collection or remote monitoring). Consequently, they are similarly exposed to cyber threats through these networks.

As cyber threats to ICS grow in frequency and sophistication, the risks can be severe. In late 2017, *Triton*, a new malware threatening ICS, was discovered. *Triton* allows attackers to prevent the activation of safety measures (e.g. sprinklers or alarms) during hazardous situations (e.g. fires or gas leakages), potentially resulting in life-threatening situations. ICS owners need to assess the risks to their systems regularly and adopt corresponding mitigating actions. They can take immediate measures such as application whitelisting (a list of programs allowed to run on the system), and timely patch management to fix known vulnerabilities.

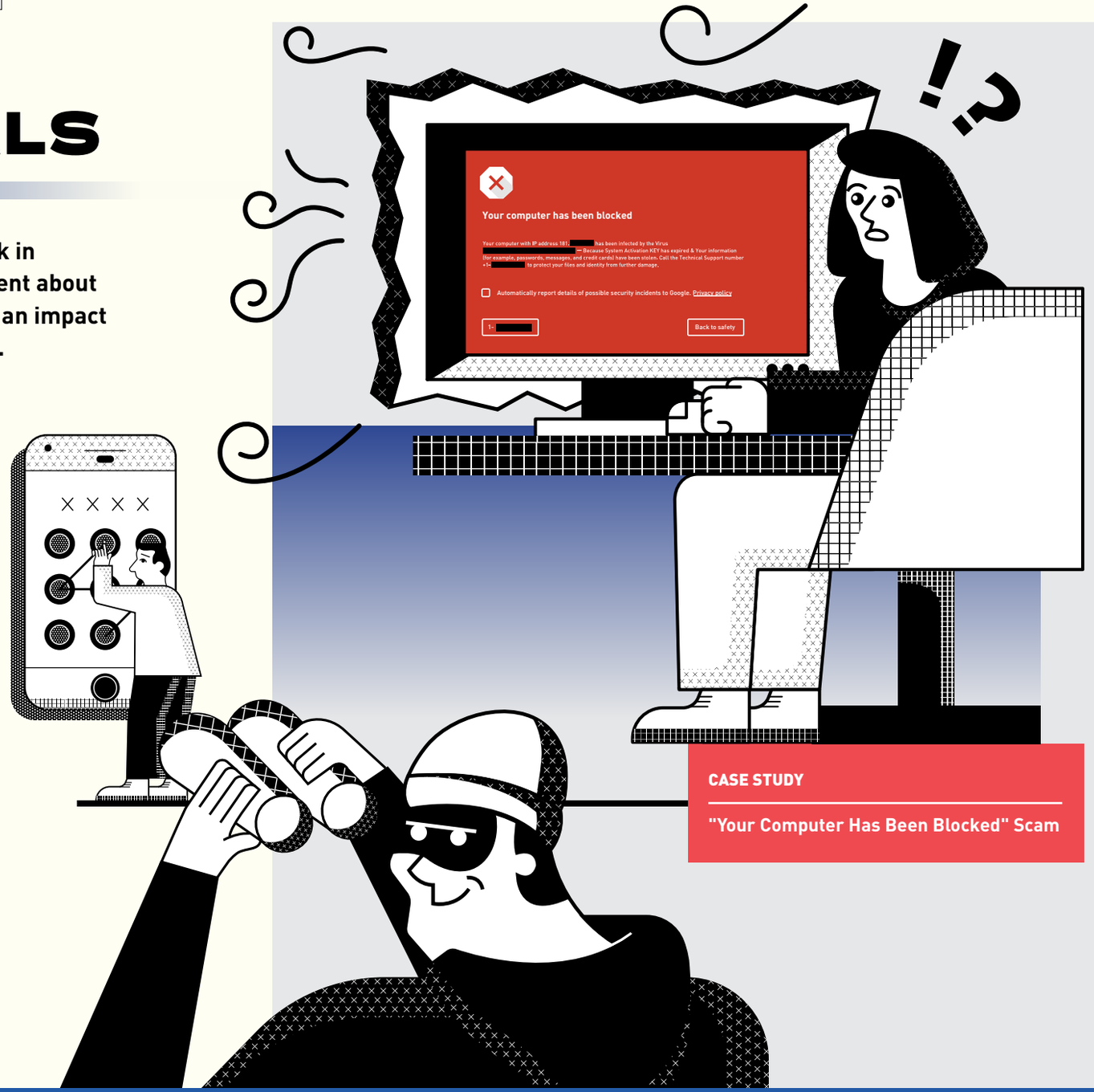
To promote cybersecurity information exchange among ICS operators and security practitioners from CII sectors, CSA initiated the formation of an ICS community in 2017. CSA worked with community members to produce a handbook - "ICS Cybersecurity Guidelines". The handbook offers best practices for strengthening cybersecurity in ICS environments.

THREATS TO INDIVIDUALS

People continue to be the weakest link in cybersecurity. Many are still not diligent about protecting their digital lives. This has an impact on our collective safety in cyberspace.

In Singapore, the three most common cyber threats reported to SingCERT by individuals were phishing, ransomware, and tech support scams.

Separately, the Singapore Police Force (SPF) noted that online scams remained a concern. In 2017, there were 825 cases of Internet love scams, with victims losing a total of S$37 million. There were about 1,960 cases of e-commerce scams, where victims lost a total of S$1.4 million, typically from making payment for online purchases that were not delivered to them.



"IT CAN BE AS SIMPLE AS NOT OPENING E-MAIL MESSAGES OR ATTACHMENTS FROM UNKNOWN SOURCES, AND CHOOSING STRONG PASSWORDS."

- MR JAMES LEE, STUDENT, ON PRACTISING GOOD CYBER HYGIENE IN SCHOOL AND AT HOME

CASE STUDY

"Your Computer Has Been Blocked" Scam

WHEN

August 2017

BACKGROUND

While surfing the Internet, an individual clicked on a link that caused her computer to freeze. A pop-up provided a number for her to call for "tech support". When she dialled the number, a "technician" advised her to purchase a security solution from a given link.

Finding the advice suspicious, she hung up and tried to reboot her system. Despite several attempts, she was unable to do so, and approached SingCERT for assistance.

FINDINGS

A pop-up that appeared while surfing the Internet caused the computer to freeze.

CASE ANALYSIS

SingCERT assessed that the individual had encountered a tech support scam. Such scams scare users into sending money or entering their credit card details on phishing sites, by claiming that their computers have been infected by a virus.

TACTICS, TECHNIQUES & PROCEDURES

Tech support scam; phishing website.

FOLLOW-UP ACTION

SingCERT provided the individual with a step-by-step guide on how to remove the pop-up, which included a reinstallation of the operating system. She was advised on cyber hygiene best practices, such as visiting only known and trusted websites.

TECH SUPPORT SCAMS

The first reports of tech support scams surfaced around 2008 and gained momentum over the years. Fake tech support websites are created by scammers who trick users into believing that their devices are infected or have technical issues. After following through with the scammer's instructions, the user may find their devices inaccessible, and will need to pay a ransom or "service fee" to restore them.

HOW CAN I PROTECT MYSELF FROM SUCH SCAMS?

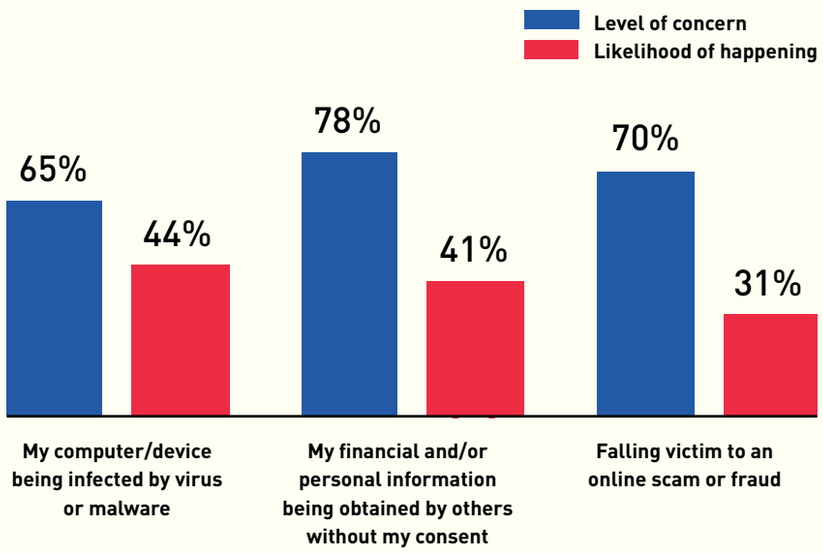
a) Do not call the numbers provided on suspicious websites or pop-ups.

b) Do not provide sensitive information (e.g. log-in credentials, two-factor authentication, financial information) to people who claim to be tech support without proper verification.

c) Do not allow strangers to have remote access to your computer.

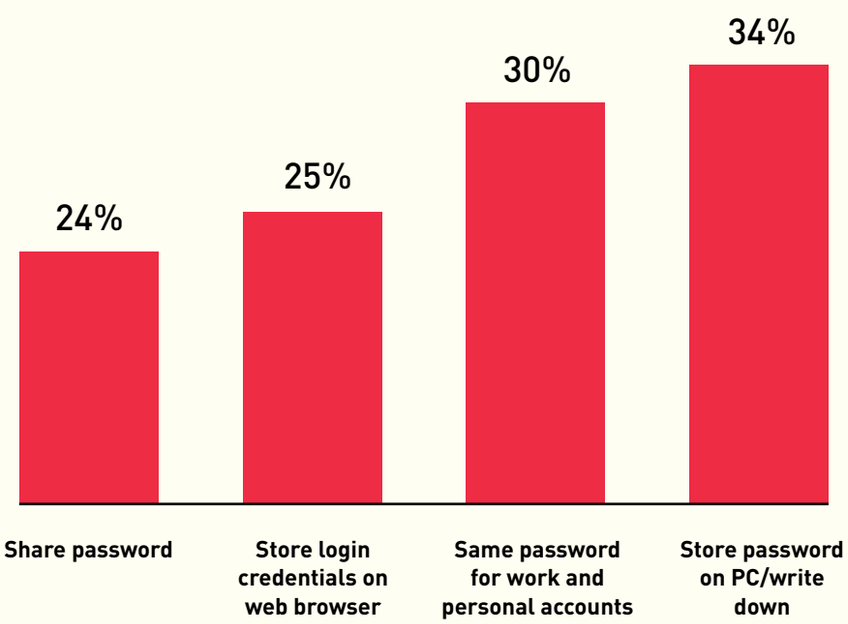
According to a public awareness survey by CSA conducted in 2017,[4] most respondents recognised that everyone had a role to play in cybersecurity, and were concerned about cybersecurity risks. However, fewer than half (about 30 to 40 per cent) of respondents felt they were personally at risk of encountering cyber threats such as malware infections, personal data breaches, or online scams. There is still room for improvement in adopting good cyber habits.

Many respondents expressed concern for cybersecurity risks, but few felt personally at risk.



Many respondents had lax password management habits. Most respondents used their mobile devices for transactions such as shopping and banking. While the majority installed software updates, 38 per cent still did not do so as soon as possible (see facing page). This leaves devices potentially vulnerable in the interim. Translating awareness into good cyber hygiene starts with simple but important practices (see "4 Cyber Tips" on facing page).

Many respondents had lax password management practices.



[4] "CSA's Public Awareness Survey in 2017 Reveals Signs of Improvement in Cybersecurity Practices," CSA press release, 23 April 2018, https://csa.gov.sg/news/press-releases/csa-public-awareness-survey-2017.

4 CYBER TIPS TO GO SAFE ONLINE

USE ANTI-VIRUS SOFTWARE

Installing anti-virus software prevents malware infections which can cause persistent pop-ups, battery drain, or even data loss.

USE STRONG PASSWORDS AND ENABLE 2FA

Prevent cyber criminals from stealing your personal information, as well as money in your accounts. Create long and random passwords, and enable Two-Factor Authentication.

SPOT SIGNS OF PHISHING

Scammers use phishing e-mails to get you to disclose your valuable personal information. Look out for signs of phishing such as URLs that have misleading domain names.

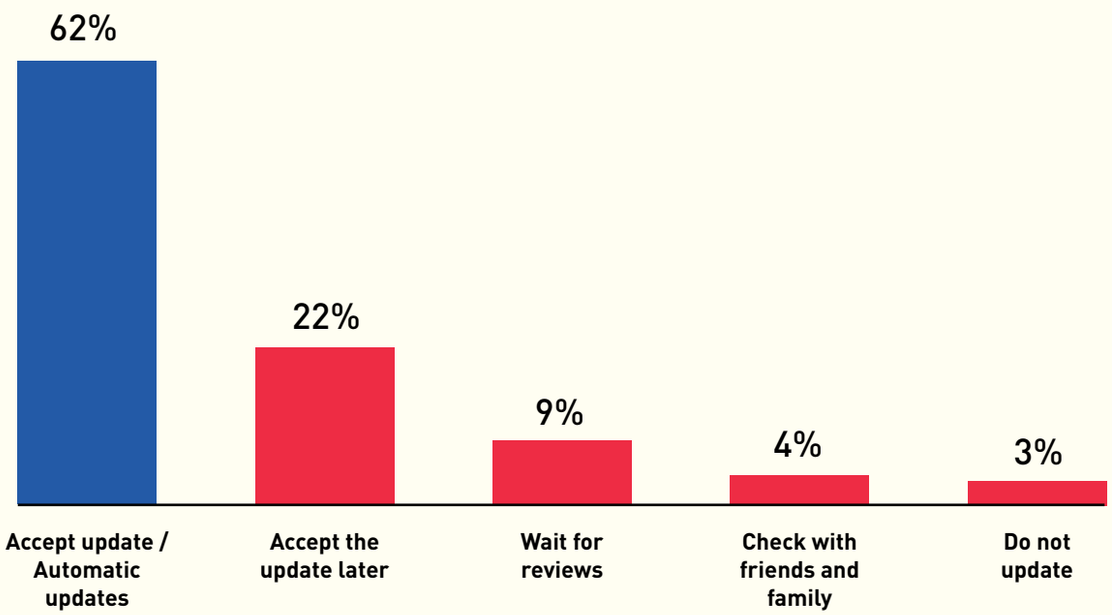
UPDATE YOUR SOFTWARE ASAP

Your devices are more vulnerable to known cyber-attacks when you don't update your software. Install security updates as soon as possible.

Remember to Go Safe Online

To get more cyber tips, visit
www.csa.gov.sg/gosafeonline

Over one third of respondents delayed installing software updates on their mobile devices.



CHAPTER 2

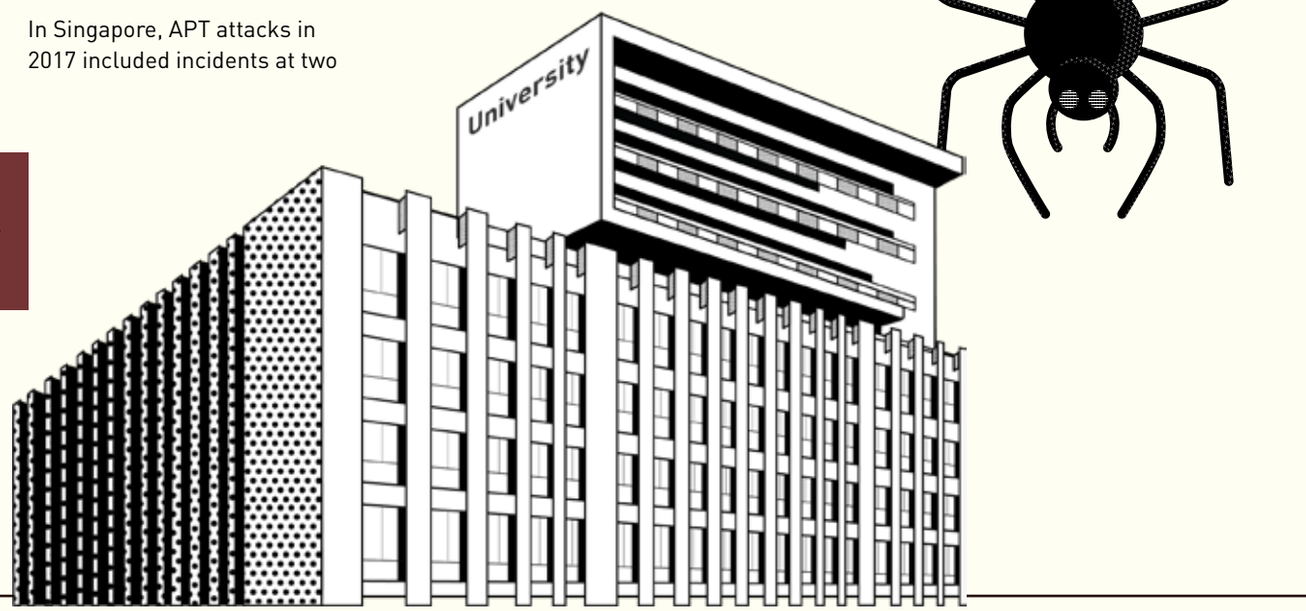
CYBER THREATS IN FOCUS

CSA analyses multiple data sources to provide actionable insights on major threats observed in Singapore's cyberspace. In 2017, Advanced Persistent Threats and cybercriminals continued to be active, while the threats of website defacements, phishing, and malware showed no signs of abating.

ADVANCED PERSISTENT THREATS

Advanced Persistent Threats (APTs), which are often backed by a nation-state, expend significant effort to mount targeted attacks on countries or organisations of interest. Using a range of tactics, techniques, and procedures (TTPs),[5] they conduct malicious activities that include espionage and mass disruptions. Some of the most disruptive global incidents in 2017 have been linked to APTs, including the *WannaCry* and *NotPetya* ransomware campaigns. They are highly adept at masking their tracks, and it is often difficult to definitively attribute a cyber-attack to a particular APT.

In Singapore, APT attacks in 2017 included incidents at two universities (see below). APTs may seek out "softer" or indirect targets as a means to gain access to government or CII sectors, which have relatively well-protected networks.



CASE STUDY

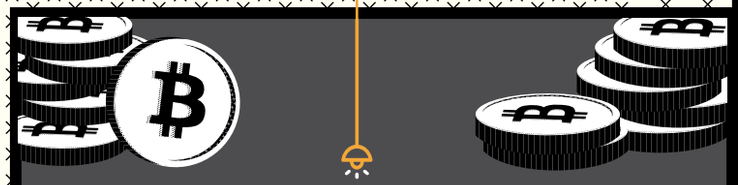
Universities targeted by APTs

In April 2017, two universities – the National University of Singapore (NUS) and the Nanyang Technological University (NTU) – reported intrusions into their networks. Based on investigations, both attacks were found to be the work of APTs.[6] NUS detected an unauthorised intrusion into its IT systems through a server, while NTU faced multiple waves of malware attacks on their systems. Immediate action was taken to isolate the affected desktop computers and servers, and tactical recovery was also done on the universities' networks.

While the universities' networks were separate from the Government's, both incidents were assessed to have been carefully planned and aimed at stealing information related to Government or research. Both universities have since enhanced the security for their networks. CSA also reached out to other universities and informed CII sectors to step up monitoring and checks on their networks.

[5] These TTPs range from simple attacks like phishing and ransomware infections to the highly tailored exploitation of zero-day vulnerabilities. Zero-days are software vulnerabilities that are unknown to the software creator or security researchers, and are considered to be severe threats since there are no mitigating patches available.

[6] "Action Taken Following Breach of Two Universities' IT Networks," CSA press release, 12 May 2017, https://www.csa.gov.sg/news/press-releases/action-taken-following-breach-of-two-universities-it-networks.



SPECIAL TOPIC

CRYPTOCURRENCIES

The sharp price spikes and dips of cryptocurrencies (such as Bitcoin and Ether) have attracted significant public interest. They are increasingly "mined", traded, and transacted across the globe.

Unlike legal tender fiat currencies, the vast majority of cryptocurrencies are neither issued nor backed by any government or centralised authority. Instead, they use cryptography and blockchain technology to enable decentralised, transparent, and secure transactions within a network.

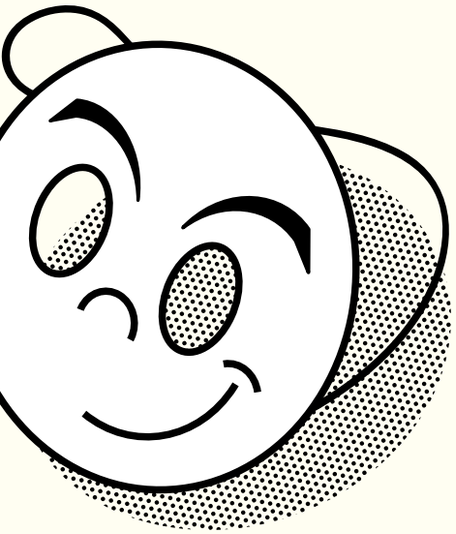
While there is nothing inherently illegal about cryptocurrencies, they may be used to facilitate illegal activities online due to the relative anonymity they afford. In the Dark Web (see p.23), Bitcoin has gained traction as a mode of payment in the trade of counterfeit Singapore identification documents, financial and personal data, and drugs.

Criminals have also asked for payments in Bitcoin for ransomware infections and Distributed Denial of Service (DDoS) extortion attempts detected in Singapore. Computer-facilitated crimes such as e-commerce and "China Officials Impersonation" scams have been observed to ask for payments in Bitcoin.

As interest and speculation in cryptocurrencies continue to rise, criminals will find new means to obtain them, whether for financial gain, or to perpetuate other crimes such as money laundering and the financing of terrorist activities. Experts have also warned about the growing threat posed by "crypto-jacking" – the use of a computer to mine a cryptocurrency through browser-based scripts or malware.

More cyber-attacks against cryptocurrency intermediaries such as exchanges (where cryptocurrencies are traded) and "wallets" (where they are stored) can be expected. Other forms of cryptocurrency-related cyber-attacks may include phishing e-mails and online scams that promise cryptocurrencies as a reward.

CYBER CRIMINALS



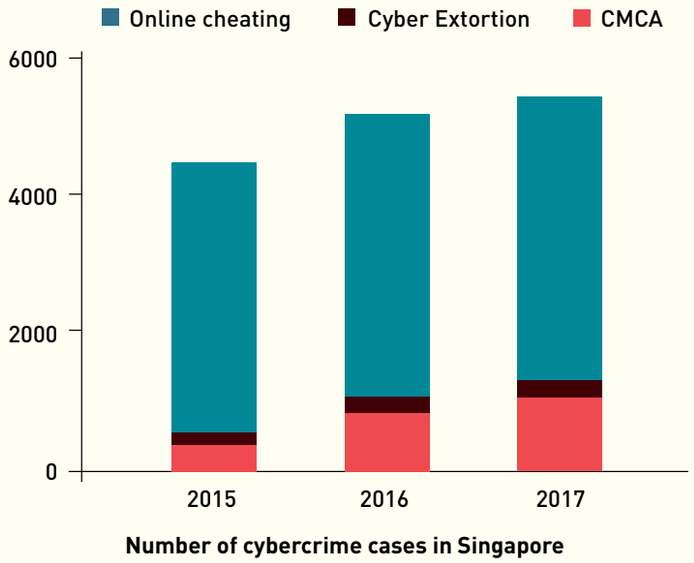
AMENDMENTS TO THE COMPUTER MISUSE AND CYBERSECURITY ACT (CMCA) IN 2017

The CMCA was amended in 2017. It will now be an offence to:

a) Deal in illegally obtained personal information for illegitimate purposes.

b) Obtain hacking tools (including physical devices, software and passwords) to commit cyber offences.

c) Commit criminal acts that create significant risk of harm in Singapore, even while overseas.



Number of cybercrime cases in Singapore

Cybercrime continues to grow in Singapore, with 5,430 cybercrime cases reported in 2017. Between 2016 and 2017, cybercrime cases grew from 15.6 per cent[7] to 16.6 per cent of total crimes, even as the overall level of crime fell. Traditional crime, such as gambling, scams, and vice, has also increasingly gone online.

Online cheating[8] and cyber extortion accounted for 82.7 and 1.4 per cent of all cybercrime cases respectively. 15.9 per cent of cybercrime involved compromised social media and SingPass accounts, impersonation scams, ransomware, unauthorised access (e.g. to corporate servers and systems), among other cybercrimes. These are offences under the Computer Misuse and Cybersecurity Act (CMCA).

In total, cybercrime victims suffered losses amounting to more than S$95 million in 2017, with the highest loss in a single case – an Internet love scam – amounting to about S$6 million.

Cracking down on cybercrime will require continued collaboration between governments, law enforcement agencies, and other stakeholders.

"GOVERNMENTS AND THE PRIVATE SECTOR MUST WORK TOGETHER TO ENSURE THE INTERNET IS SAFE AND SECURE FOR CITIZENS. THE CYBERCRIME CHALLENGE IS COMPLEX AND CANNOT BE SOLVED BY ANY SINGLE ENTITY. WE MUST HAVE A COOPERATIVE APPROACH TO ENABLE COLLECTIVE DEFENCE."

- MR MATTHIAS YEO, CHIEF TECHNOLOGY OFFICER (ASIA), SYMANTEC CORPORATION, ON COMBATING CYBERCRIME TOGETHER

SPECIAL TOPIC

THE DARK WEB

The Dark Web is a section of the Internet only accessible through special software[9] that allows users to remain anonymous or untraceable.

The promise of anonymity and the prospect of evading state surveillance make the Dark Web a choice hideout for cyber-attackers and criminals. Much of the Dark Web's content and services is illegal in nature, including marketplaces selling drugs, pornography, and stolen personal data.

Dark Web marketplaces increasingly facilitate the execution and monetisation of cyber-attacks. These marketplaces are often used to trade malware, ransomware-as-a-service, and do-it-yourself exploit kits, which in turn allow would-be cybercriminals to purchase these products and conduct cyber-attacks.

Law enforcement agencies around the world are closely watching this space. In July 2017, an international law enforcement effort brought down two of the largest Dark Web marketplaces, AlphaBay and Hansa, and disrupted the trade of illegal goods and services.

The Singapore Police Force (SPF) is starting to see cybercrime cases involving the Dark Web. In the first such conviction in Singapore, a 29-year-old Singaporean was sentenced to 36 months' jail in November 2017, after admitting to obtaining and using PayPal Accounts and credit/debit card information bought off the Dark Web to make online purchases, modifying the PayPal accounts obtained, and retaining the illegal proceeds.

Using the compromised PayPal accounts and credit/debit card credentials, the person made fraudulent purchases amounting to about S$25,000 worth of goods, and re-sold them for profit. In addition, he used the stolen credentials to purchase food and hotel accommodation for his own consumption.

Under the CMCA, transacting in and possessing stolen data, malware, and other illicit goods and services – regardless of the means employed to do so – can be illegal.

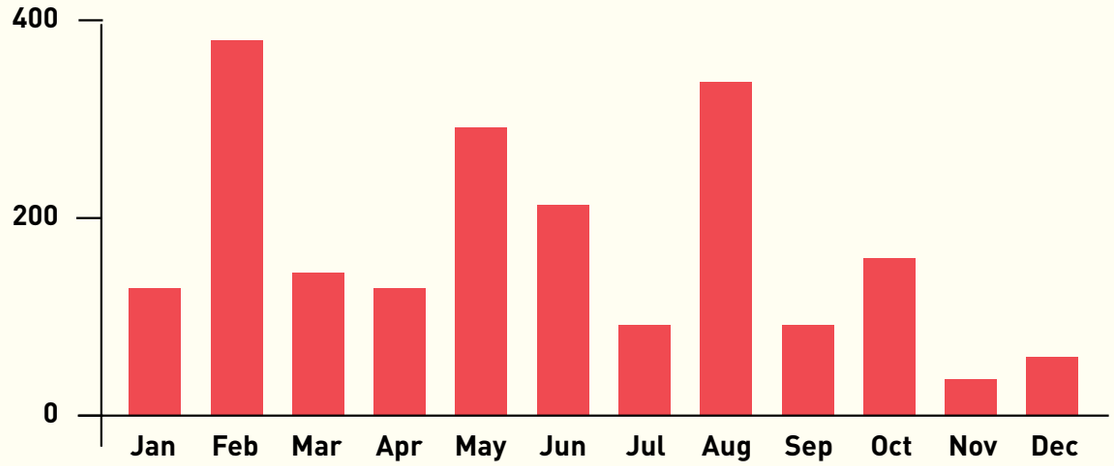
[7] In the Singapore Cyber Landscape 2016, it was reported that cybercrime accounted for 13.7 per cent of all crimes in 2016. SPF has since revised that 2016 figure to 15.6 per cent.

[8] In such cases, criminals coaxed their victims into surrendering sensitive personal and financial information using social engineering techniques.

[9] For example, browsers such as Tor (short for "The Onion Router") route communications through a network of servers in order to mask the location of users.

WEBSITE DEFACEMENTS

Number of Singapore-linked website defacements detected in 2017



Website defacements are a common mode of attack by mischief-makers and hacktivist groups to promote their agenda. Common targets include the websites of governments, schools, and news agencies.

In Singapore, the number of websites defaced increased from 1,750 defacements in 2016 to about 2,040, a 16.6 per cent increase. Many of these were part of global mass defacement campaigns. The defaced websites belonged mostly to SMEs from sectors such as manufacturing, retail, and information and communications technology (ICT). No Government websites were compromised.

Attackers often exploit unpatched vulnerabilities in servers or web applications to deface websites.

When popular content management systems (CMS)[10] are hit, the effect can be inadvertently amplified. This was the case in February 2017, when an exploit of a WordPress vulnerability saw two million websites worldwide defaced.[11] Some Singapore websites were similarly affected as a result, marking the peak in defacements here.

Hacktivists tend to seek out high-profile websites or leverage iconic events to launch defacement campaigns for maximum impact and visibility. For example, CSA noted an increase in defacements of Singapore websites on 9 August, Singapore's National Day. While these were assessed to be opportunistic rather than targeted, it highlights the potential for such incidents during iconic events. Many of the websites had been defaced previously, suggesting that their owners had not taken the appropriate security and patching measures to protect their websites. Website owners should update and patch their software in a timely manner, to reduce the possibility of having their websites defaced.

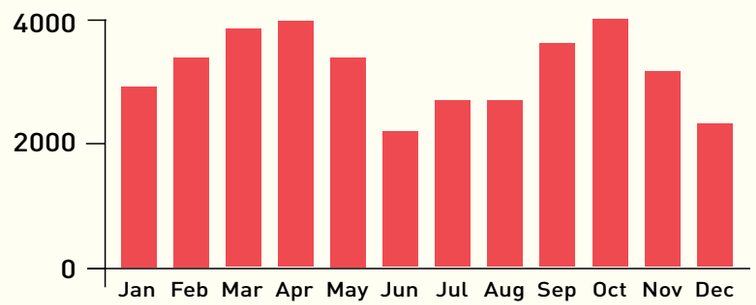
[10] Web-based applications for creating and managing website content.

[11] Goodin, Dan. "Virally growing attacks on unpatched WordPress sites affect ~2m pages," *Ars Technica*, 11 February 2017, https://arstechnica.com/security/2017/02/virally-growing-attacks-on-unpatched-wordpress-sites-affects-2m-pages/.

PHISHING URLs

Phishing is one of the simplest and most effective ways that hackers use to steal sensitive personal data such as passwords, contact information, and credit card details. A phishing e-mail spoofs a legitimate source to trick users into clicking on dubious links or opening file attachments.

Number of phishing URLs with a Singapore-link detected in 2017



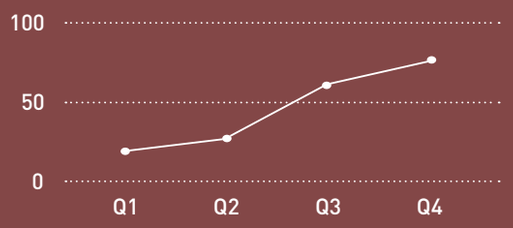
In 2017, phishing remained the favourite tactic for attackers, with 23,420 phishing URLs[12] with a Singapore-link detected.[13] The websites of technology companies such as Apple and Microsoft were commonly spoofed, making up about 40 per cent of the observed phishing URLs.

The websites of Government agencies, including the Immigration & Checkpoints Authority of Singapore (ICA), Inland Revenue Authority of Singapore (IRAS), Ministry of Manpower (MOM), and Singapore Police Force (SPF), were subject to spoofing, though the numbers were relatively low. Attackers may spoof such Government websites to phish for Singaporeans' personal data, including NRIC numbers, passport numbers, and credit card information.

Attackers will continue to pose as trusted entities (see below), to trick more victims into disclosing information. Be alert online, whether shopping, e-mailing or just casual surfing.

ATTACKERS ABUSING INHERENT TRUST IN "HTTPS"

Increasing use of "HTTPS" in phishing URLs in Singapore cyberspace in 2017



"HTTPS" (HTTP Secure) is an extension of Hypertext Transfer Protocol (HTTP) for secure communication over a network. "HTTPS" connections are typically used for online payments, e-mail, and other sensitive transactions.[14]

However, attackers have increasingly been seen to use "HTTPS" in phishing URLs as a tactic to influence a higher click-through rate by victims.

Users are advised to verify URLs before performing any logins or transactions to avoid falling prey to such attacks.

[12] A Uniform Resource Locater (URL) is a unique, specific web address.

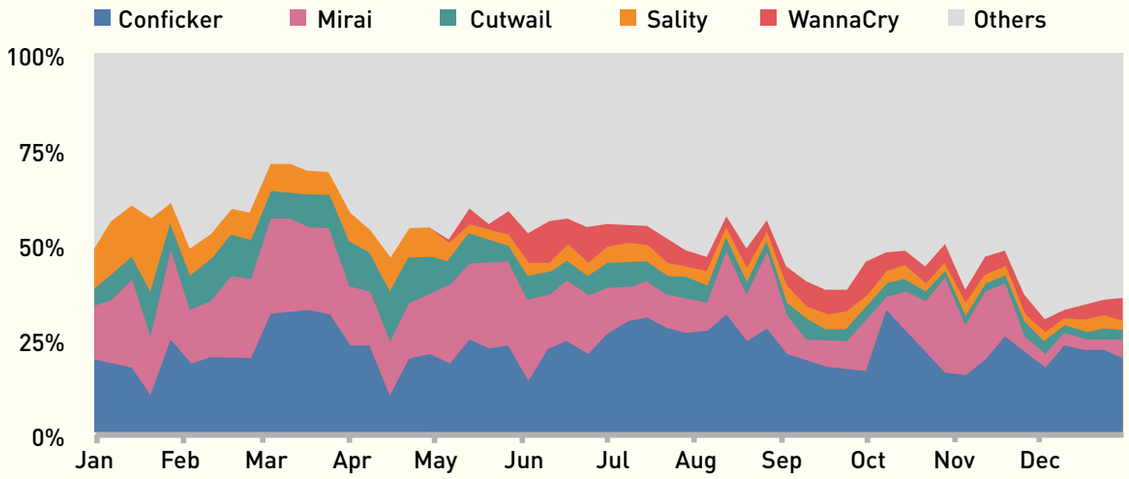
[13] In 2016, 2,512 phishing URLs with a Singapore-link were found. The large difference between 2016 and 2017 numbers is a result of CSA's efforts to expand its view of the overall cyber threat landscape. Figures observed in 2017 are in line with global trends, but are not directly comparable with past years' figures.

[14] Attackers sign phishing domains with a certificate obtained from certificate authorities like Let's Encrypt that provide them for free. Malenfant, Joe. "The Light is Green! But is it Safe to Go? Abusing Users' Faith in HTTPS," Cisco Blogs, 24 May 2017, https://blogs.cisco.com/security/the-light-is-green-but-is-it-safe-to-go-abusing-users-faith-in-https.

Commonly spoofed websites and organisations in 2017

No.	Sector
1 ▲ (3rd in 2016)	Technology (e.g. Microsoft)
2 (no change)	File-Hosting Services (e.g. Dropbox)
3 ▼ (1st in 2016)	Banking & Financial Services (e.g. PayPal)

MALWARE



On average, five common malware accounted for over half the daily infections in 2017

Malicious software, or malware for short, are programs devised to compromise the security of a computer system. Compromised systems may inadvertently become drones that are part of a larger botnet – a network of compromised computers controlled without the owners' knowledge. Threat actors control botnets through Command and Control (C&C) servers to carry out malicious attacks such as e-mail spam and Distributed Denial-of-Service attacks (DDoS).

In 2017, CSA observed about 750 unique C&C servers in Singapore.[15] On average, about 2,700 botnet drones with Singapore IP addresses were observed daily.[16] Of the more than 400 malware variants detected in 2017, five – *Conficker, Mirai, Cutwail, Sality,* and *WannaCry* – accounted for over half the observed daily infections. The majority of these malware are not new.

For example, *Cutwail*[17] and *Conficker*[18] were first detected in 2007 and 2008 respectively. Common tools such as Windows Defender and Microsoft Safety Scanner can detect and remove these threats. The fact that old malware like *Conficker* continue to infect systems suggests that many do not make use of similar tools, to scan for viruses and clean up their systems.

[15] There were slightly more than 60 C&C servers observed in Singapore's cyberspace in 2016. The difference between 2016 and 2017 numbers is a result of CSA's efforts to enhance its view of the overall cyber threat landscape. Figures observed in 2017 are in line with global trends, but are not directly comparable with past years' figures.

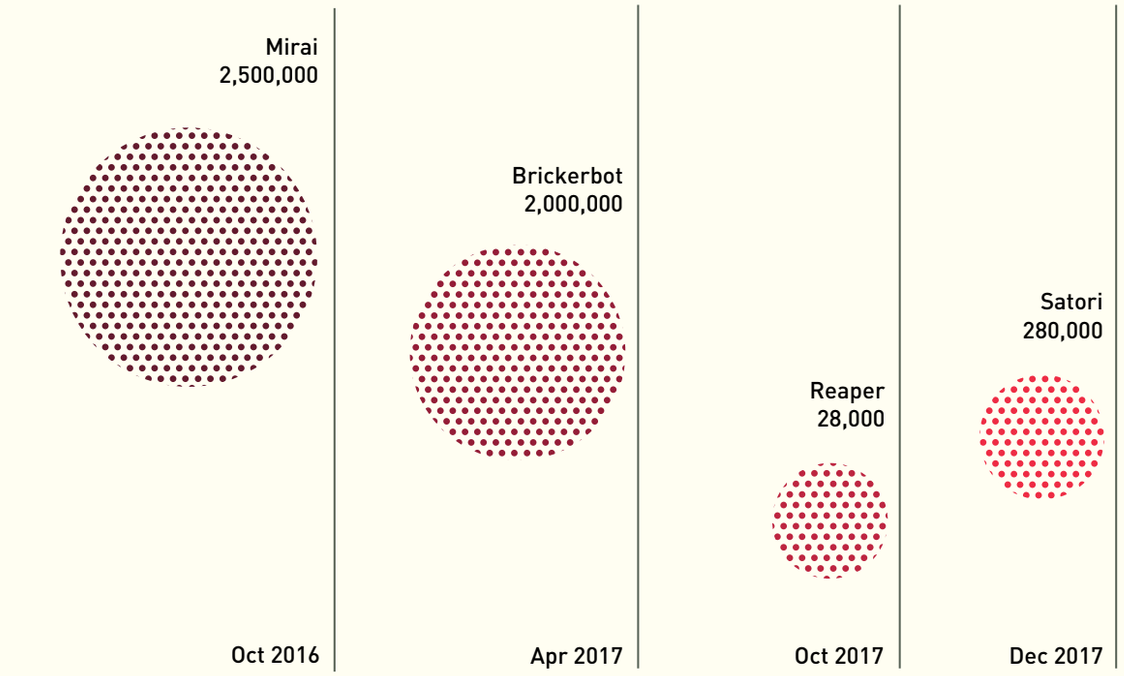
[16] Based on unique Internet Protocol (IP) addresses (the numerical code assigned to each device that can connect to the Internet or other network), approximately 150,000 botnet drones were observed in Singapore in 2017.

[17] Also known as *Pushdo*, it is a spam malware that targets Windows OS and is responsible for a huge amount of spam activity around the world. First detected in 2007.

[18] A computer worm that targets vulnerable Windows operating systems, first detected in 2008.

INTERNET OF THINGS DEVICES

Estimated number of global infections by IoT malware (Sources: McAfee, BleepingComputer, and Qihoo 360 NetLab)



The Internet of Things (IoT) refers to the vast network of everyday objects like baby monitors, printers, televisions, and autonomous vehicles that are connected to the Internet.

With billions more IoT devices expected in the future, the attack surface will grow. This may also result in new vulnerabilities and malware that can be exploited by hackers. In 2017, malware such as *Brickerbot*, *Reaper*, and *Satori* emerged, but these were essentially variants of the *Mirai* malware that infected thousands of vulnerable IoT devices globally in 2016. Like *Mirai*, the variants could have caused massive DDoS attacks, but none were observed in 2017.

Hackers are also increasingly targeting mobile devices, such as smartphones. Smartphones, which are often used to access or control IoT devices, can spread malware to connected devices through mobile apps, e-mail, Bluetooth, and other means of connectivity. Given Singapore's high mobile penetration rate,[19] mobile devices can be a breeding ground for cyber-attacks, if people have poor cybersecurity practices.

STOP YOUR DEVICES FROM JOINING A ZOMBIE BOTNET ARMY

You do not want your IoT devices to turn on you. The timely patching of IoT devices against known vulnerabilities is critical to preventing attackers from exploiting them. Do:

- Update your software as soon as possible.
- Change your devices' default user credentials immediately.
- Turn off unnecessary remote access to your Internet-connected devices like cameras and printers.

[19] The mobile penetration rate – referring to mobile subscriptions over total population in Singapore – was 148.8 per cent at the end of 2017, suggesting that some people have more than one mobile device. Data.gov.sg, https://www.data.gov.sg/dataset/mobile-penetration-rate.

RANSOMWARE

Ransomware is a type of malware that encrypts files on victims' devices, making them unusable until the ransom is paid. Common attack vectors for ransomware are phishing e-mails that contain malicious attachments or links, or pop-ups that exploit vulnerabilities in browsers to install ransomware.

There were three major ransomware outbreaks worldwide in 2017. The *WannaCry* global campaign in May 2017 affected at least 150 countries and infected more than 200,000 systems. Close on its heels, *NotPetya* hit at least 65 countries in June 2017, while *Bad Rabbit* affected almost 200 systems in Russia and Eastern Europe in October 2017. Singapore was relatively unscathed, with only a few incidents of *WannaCry* reported. 25 cases of ransomware were reported to SingCERT in 2017. However, the actual number of ransomware cases is likely to be higher as many go unreported. Besides *WannaCry*, victims were infected by ransomware such as *Cerber*, *Dharma*, and *Sage*, and faced ransom demands ranging between S$2,000 and S$4,000. Businesses affected by ransomware can suffer significant disruptions to their operations, and lose access to important files.

OPEN PORTS OPEN TO INFECTION

Many devices may have open ports, such as those associated with the Server Message Block (SMB) protocol, which are typically used by companies for file-sharing purposes. However, malicious actors can take advantage of these ports to inject malware such as *WannaCry* into devices in the network.

In 2017, most *WannaCry* infections detected in Singapore were rendered benign due to a "kill switch" that deactivated the malware. However, devices with open ports are still vulnerable to other types of malware.

To mitigate this risk, users should protect their devices with updated anti-virus software, patch known vulnerabilities, and check that ports (such as ports 139 and 445) on their devices are not unnecessarily exposed.

WHAT TO DO IF YOUR COMPUTER IS INFECTED BY RANSOMWARE

Ransomware victims are discouraged from paying the ransom. The international "No More Ransom" Initiative, of which CSA is a Supporting Partner, helps most victims successfully retrieve their files through more than 50 free decryption tools against over 100 types of ransomware. Visit the No More Ransom project (www.nomoreransom.org) or SingCERT (www.csa.gov.sg/singcert) for more information and prevention tips.

CHAPTER 3

BUILDING UP SINGAPORE'S CYBER RESILIENCE

"A VIBRANT CYBERSECURITY ECOSYSTEM IS AN IMPORTANT FACTOR CONTRIBUTING TO ROBUST NATIONAL CYBERSECURITY."

- DR YAACOB IBRAHIM, MINISTER FOR COMMUNICATIONS AND INFORMATION, AND MINISTER-IN-CHARGE OF CYBER SECURITY, SPEAKING TO PARLIAMENT IN MARCH 2017

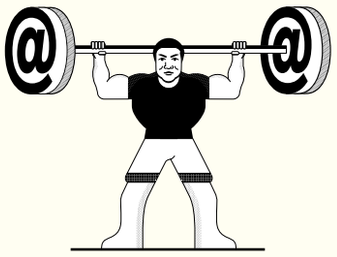
CSA, together with its partners, is working to build up Singapore's cyber resilience, so that when a cyber-attack happens, we can bounce back to business as usual quickly. Efforts to boost Singapore's cyber resilience include:

(a) Enhancing preparedness against cyber threats.
(b) Strengthening international cooperation.
(c) Developing a professional cybersecurity workforce.
(d) Research & development.
(e) Raising cybersecurity awareness.

ENHANCING PREPAREDNESS AGAINST CYBER THREATS

CSA staff briefing DPM Teo on the work of the National Cyber Incident Response Teams during Exercise Cyber Star in July 2017. DPM Teo was accompanied by (L-R) Minister Yaacob Ibrahim and Senior Minister of State, Ministry of Communications and Information Dr Janil Puthucheary. Source: MCI.

CYBER EXERCISES



A cyber-attack is almost inevitable. Therefore, CIIs need to be ready to deal with such scenarios. Cyber exercises enable organisations to regularly review and refine their cyber incident response plans before an actual incident happens. Industry-specific exercises such as Exercise CyberArk are conducted regularly. At the national level, CSA conducts the multi-sectoral Exercise Cyber Star to familiarise stakeholders with the national crisis management system and processes in the event of a major cyber incident in Singapore. Such exercises allow the sectors to reassess their cybersecurity capabilities and identify opportunities for improvement.

CYBER LEGISLATION

The Cybersecurity Act, passed in Parliament in February 2018, establishes a legal framework for the oversight and maintenance of national cybersecurity in Singapore. Its four key objectives are to:

Strengthen the protection of CIIs against cyber-attacks.

The Act provides a framework for the designation of CIIs. It provides CII owners with clarity on their obligations to protect CIIs from cyber-attacks, and requires the owners to report cybersecurity incidents to CSA.

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

The Act empowers the Commissioner of Cybersecurity to investigate cyber threats and incidents to determine their impact and prevent further harm. These powers are calibrated based on the severity of the threat or incident and the measures required.

Establish a framework for sharing cybersecurity information.

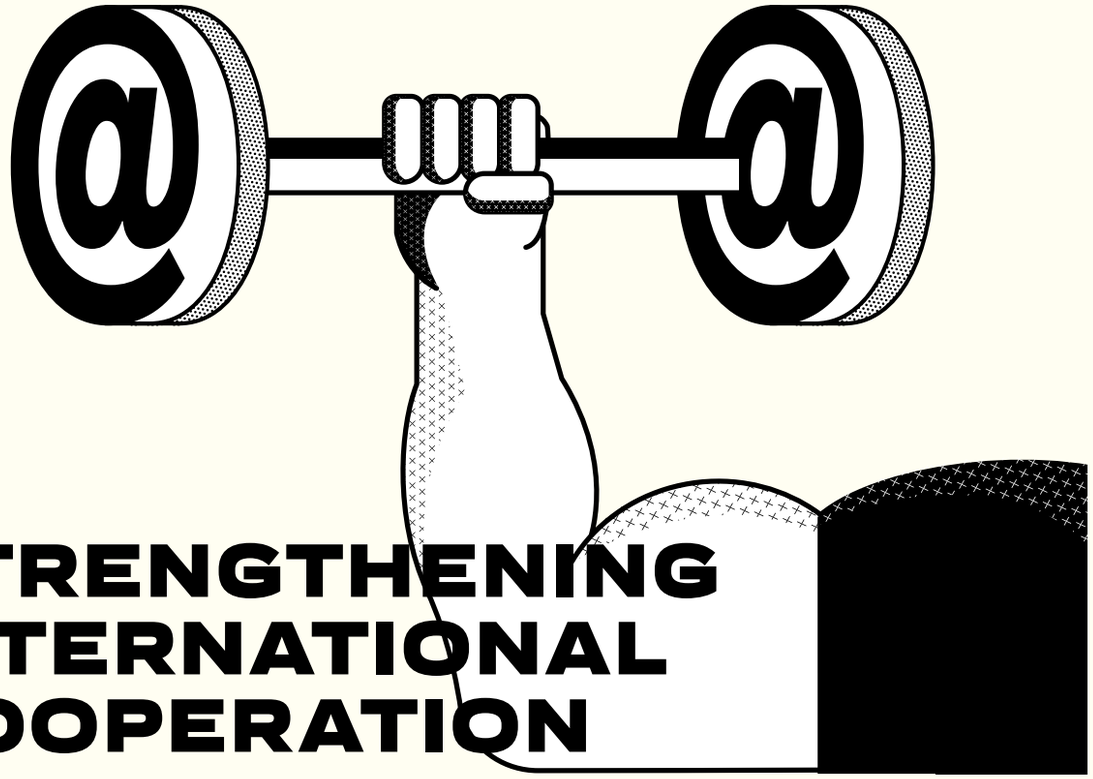
The Act facilitates information sharing, which is critical as timely information helps the Government and owners of computer systems identify vulnerabilities and prevent cyber incidents more effectively. The Act provides a framework for CSA to request for information, and for the protection and sharing of such information.

Establish a light-touch licensing framework for cybersecurity service providers.

Some cybersecurity services can be sensitive because the service providers performing them would know where the vulnerabilities in clients' computer systems are. Licensing cybersecurity service providers will give businesses and clients more assurance in engaging such services.

"THE CYBERSECURITY ACT PROVIDES A STARTING POINT FOR NATIONAL CYBER RESILIENCE, FROM THE LEGISLATION OF MEASURES TO BE TAKEN, TO THE REGULATION OF CYBERSECURITY SERVICE PROVIDERS. IN MANY WAYS, THE ACT IS BOTH TIMELY AND INSTRUCTIVE."

- MR JACK OW, TECHNOLOGY LAWYER, ON THE IMPORTANCE OF CYBER RESILIENCE TO KEEP SOCIETY FUNCTIONING



STRENGTHENING INTERNATIONAL COOPERATION

The borderless nature of cyber threats calls for countries to work together, to achieve collective action and mutual understanding.

Singapore believes in the importance of a rules-based international order for cyberspace, based on applicable international law and the adoption of voluntary cyber norms. This should be complemented by a coordinated capacity building framework, to build countries' capacity in dealing with cybersecurity and cybercrime issues. Robust confidence building measures are also important, to reduce the risk of cyber conflict and foster closer working relationships between international and regional partners. These elements guide Singapore's engagements with our partners.

The annual Singapore International Cyber Week (SICW) brings together international and regional cyber leaders to forge partnerships and engage in critical dialogue on cybersecurity. The second edition of SICW in September 2017 attracted more than 7,000 stakeholders, including policy-makers, industry experts and non-governmental organisations from close to 50 countries. SICW events such as International Cyber Leaders' Symposium, ASEAN Cyber Prosecutors Roundtable, and IoT Cyber Roundtable advanced conversations on cyber norms, regional cybercrime cooperation, and IoT cybersecurity standards respectively.

Singapore's efforts to strengthen international collaboration also include:

- Hosting the 2nd ASEAN Ministerial Conference on Cybersecurity (AMCC) in September 2017, where ASEAN Member States agreed on a Chairman's Statement to move forward on the adoption of voluntary norms to guide state behaviour and the responsible use of ICT.
- Organising ad-hoc events at international fora, including two side events at the United Nations (UN), to discuss how the global community could move forward on cyber norms.
- Establishing partnerships between governments through Memoranda of Understanding (MOU) on cybersecurity cooperation with countries such as Australia, Germany, Japan, and the United Kingdom.
- Engaging in CERT-to-CERT cooperation and exchange of best practices with like-minded partners.
- Working with ASEAN partners through capacity building initiatives such as the ASEAN Cyber Capacity Programme (see box below).

ASEAN cybersecurity and ICT Ministers agreed on the importance of closer coordination of regional efforts in cybersecurity. Source: MCI.

Singapore renewed its MOU on cybersecurity cooperation with the UK in 2017. Source: CSA.

ASEAN CYBER CAPACITY PROGRAMME (ACCP)

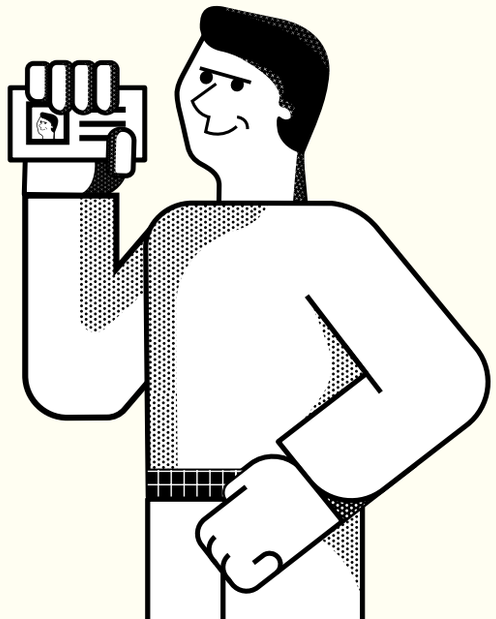
The S$10 million ACCP seeks to build technical, policy, and strategy-building capabilities within ASEAN Member States. Since April 2017, more than 120 ASEAN cybersecurity officials and incident responders have been trained through ACCP initiatives, such as the ASEAN Cyber Norms Workshop, a US-Singapore Workshop on Cybersecurity, and an Australia–Singapore Cyber Risk Reduction Workshop. Singapore also hosted an International Law for Cyber Operations Course in August 2017. The course was conducted by international experts, including the key drafters of the Tallinn Manual. The Manual covers the current global legal landscape for cyber and how laws apply in different situations.

DEVELOPING A PROFESSIONAL CYBERSECURITY WORKFORCE

Cybersecurity is an area for economic opportunity and growth. Building up our talent pool will not only strengthen Singapore's cybersecurity sector, but also ensure a sustainable source of expertise, to contribute to a more resilient national infrastructure.

The Government works closely with industry and academia on several initiatives to promote the growth and career development of professionals. These include:

- Introducing the SkillsFuture Work-Study Degree and Earn and Learn programmes, which help students attain tertiary cybersecurity qualifications while undergoing structured on-the-job training.
- Organising the Cybersecurity Challenge Singapore, comprising competition rounds and a Masterclass Final in the UK, to inspire and spur cybersecurity enthusiasts to join the profession.
- Implementing complementary programmes such as the Cyber Security Associates and Technologists (CSAT) Programme,[20] and Professional Conversion Programmes[21] for fresh graduates and mid-career switchers.
- Implementing the ICT Skills Framework to guide industry and academia on cybersecurity skills development.
- Establishing the Cybersecurity Professional Scheme to provide an attractive career proposition through competitive remuneration for cybersecurity professionals in the Public Service.
- Creating the Cyber NSF Vocation for full-time national servicemen (see facing page).



"THE ASSOCIATION OF INFORMATION SECURITY PROFESSIONALS (AISP) HAS BEEN WORKING CLOSELY WITH CSA ON MANY EXCITING INITIATIVES TO ENHANCE THE QUALITY OF CYBERSECURITY SERVICES AND THE PROFESSION HERE."

- DR STEVEN WONG, PRESIDENT, ASSOCIATION OF INFORMATION SECURITY PROFESSIONALS, ON THE RELATIONSHIP BETWEEN CSA AND PROFESSIONAL ASSOCIATIONS

[20] Jointly implemented by CSA and the Info-communications Media Development Authority (IMDA). The CSAT enables ICT and engineering professionals to take on cybersecurity roles.

[21] Organised by Workforce Singapore and e2i.

SPECIAL TOPIC

MINDEF'S CYBER NSF SCHEME

Every Singaporean male goes through Full-time National Service (NSF)[22] and performs a variety of operational roles in the defence of Singapore. The cyber domain is growing in importance and MINDEF/Singapore Armed Forces (SAF) is committed to boosting their capabilities to secure this domain. The Cyber NSF Scheme will allow MINDEF/SAF to select and harness cyber talent from the NSF population, and train them to defend our networks, systems, and information.

NSFs assessed to have the aptitude and cyber skills will be selected as Cyber Operators. Those with exceptional skills will be offered the Cyber Specialist Award, which is a one to two-year short-term contract. They will be trained for more advanced cyber roles such as incident response, penetration testing, and forensics. The award also comes with a work-learn programme with the Singapore Institute of Technology (SIT), which allows NSFs to earn academic credits towards a future cybersecurity degree. The Cyber Specialist will also be given the opportunity to earn industry-recognised professional certifications during his service.

The Cyber NSF Scheme aims to optimise the potential of NSF cyber talent, and develop their skills and knowledge to defend our networks. With this strong foundation, they can better contribute to national defence and play a part in building the national cybersecurity ecosystem.

Top six players from the Cybersecurity Challenge Singapore with Deputy Chief Executive (Development), CSA, Mr Teo Chin Hock (centre). The players travelled to the UK in November 2017 to compete against 42 other youth there in rounds of challenges, including how to stop a cyber-attack.

"THE MASTERCLASS PROVIDED INSIGHTS ON THE RANGE OF FUNCTIONS REQUIRED IN CYBERSECURITY. IT'S NOT JUST TECHNICAL KNOWLEDGE; SOFT SKILLS ARE EQUALLY IMPORTANT. IT HAS DEFINITELY INCREASED MY INTEREST IN THE FIELD AND I HOPE TO BE PART OF SINGAPORE'S CYBERSECURITY INDUSTRY IN THE FUTURE."

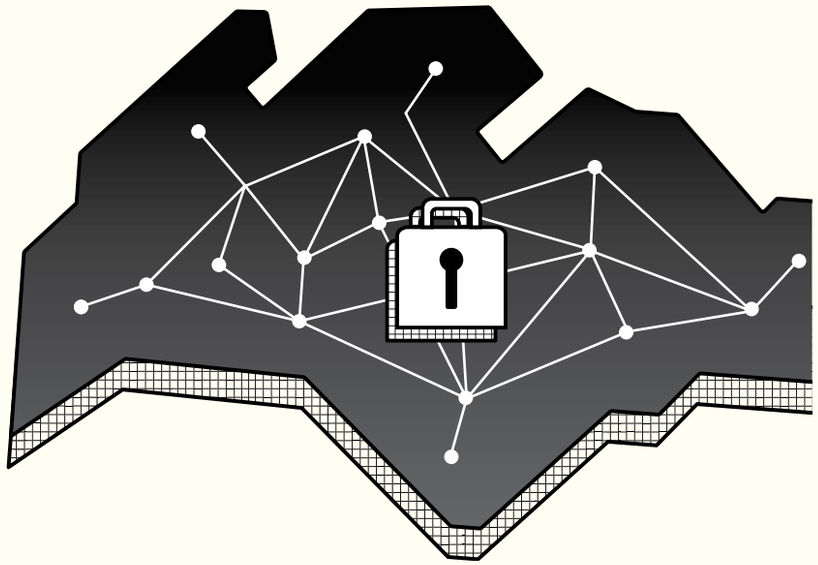
- MR CHUA TIANXIANG, IT SPECIALIST, ON PARTICIPATING IN THE CYBER SECURITY CHALLENGE UK MASTERCLASS FINAL

[22] It is a statutory requirement for all male Singaporean citizens and second-generation permanent residents to undergo a period of compulsory service in the uniformed services. Apart from SAF, NSFs may also serve in the Singapore Police Force (SPF) or the Singapore Civil Defence Force (SCDF).

RESEARCH & DEVELOPMENT

Cybersecurity research and development (R&D) efforts, combined with a Security-by-Design approach, help to provide secure and trusted solutions to current and future security challenges in Singapore.

Cybersecurity is a crucial pillar of Singapore's Smart Nation journey. CSA works closely with its partners to establish the proper security governance frameworks to support Smart Nation initiatives such as the National Digital Identity system. CSA is also developing the proper security architecture for the deployment of IoT solutions which will be used in initiatives such as the Smart Nation Sensor Platform.



Cybersecurity R&D efforts include:

- Developing capabilities in areas like Cyber-Physical Systems security and blockchain technology for the logistics industry.
- Implementing evaluation regimes that make it easier to properly certify and identify cybersecurity, IoT, and related products.

Other efforts to grow the industry pipeline leveraging R&D are:

- Supporting the growth and development of cybersecurity start-ups and accelerators as a key pillar of the future digital economy.
- Catalysing, through the Proof-of-Concept Scheme, the development of innovative solutions meeting national cybersecurity and strategic needs, with potential for commercial application.

SPECIAL TOPIC

MINDEF'S BUG BOUNTY PROGRAMME

MINDEF takes a serious view of cyber threats and the security of its systems. The nature of modern computer coding and programs is such that mistakes and vulnerabilities are inevitable. The MINDEF Bug Bounty Programme was a response to this reality and the rapidly-evolving cyber threat landscape. It served to improve the cybersecurity of MINDEF's Internet-facing systems more quickly and effectively than other conventional programmes would have been able to.

From 15 January to 4 February 2018, selected white hat hackers were invited to test eight major MINDEF Internet-facing systems for vulnerabilities, and were rewarded for any valid bugs found. HackerOne, a reputable international bug bounty company, was engaged to manage the programme. A total of 264 white hats from around the world participated in this programme, including 57 of HackerOne's top 100 white hats and 100 from the local white hat community. 97 vulnerability reports were submitted from 34 participants, with 35 reports deemed valid. The total bounty payout was US$14,750 (S$20,650).

"WE MUST HAVE GREATER VIGILANCE AND SAFEGUARDS AGAINST CYBER-ATTACKS ON INTELLIGENT SYSTEMS AND CRITICAL INFRASTRUCTURE. CYBERSECURITY NEEDS TO BE ADDRESSED IN A HOLISTIC MANNER INVOLVING PREDICTIVE, DEFENSIVE, AND DETECTIVE MEASURES."

- PROF LAM KWOK YAN, PROFESSOR, SCHOOL OF COMPUTER SCIENCE AND ENGINEERING, NANYANG TECHNOLOGICAL UNIVERSITY, ON THE NEED FOR A HOLISTIC APPROACH TO CYBERSECURITY AS SINGAPORE GEARS UP TO BE A SMART NATION

RAISING CYBERSECURITY AWARENESS

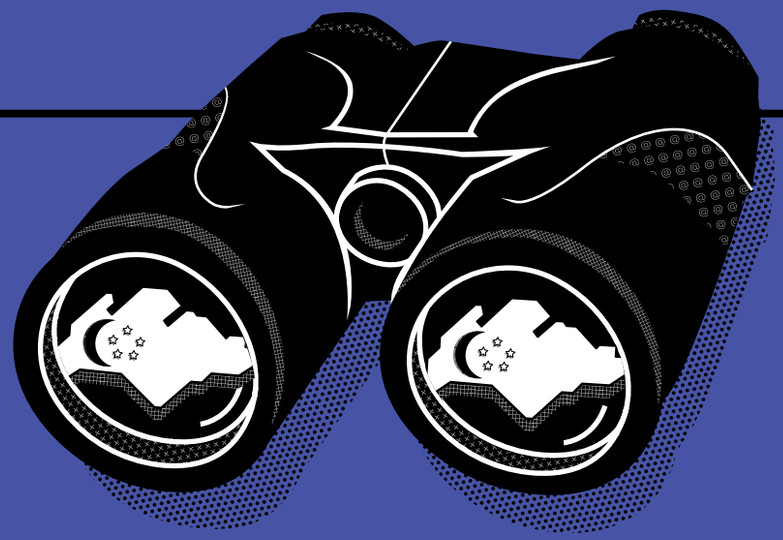
The inaugural National Cybersecurity Awareness Campaign roadshow in February 2017 attracted close to 16,000 visitors from all walks of life. Source: CSA.

An important component of cyber resilience is awareness of cyber threats and how to deal with them. Cultivating good cyber hygiene practices to safeguard our devices and information is a good place to start. On-going efforts to raise cybersecurity awareness in Singapore include:

- Reaching out to a wide audience with the inaugural National Cybersecurity Awareness Campaign to show how cybersecurity can be part of our everyday lives.
- Bringing the message to a younger audience through a series of Cyber Safety activity books aimed at primary school students.
- Providing cybersecurity news and advisories to businesses and individuals via the GoSafeOnline website and other social media platforms.

LOOKING AHEAD: ANTICIPATED TRENDS IN 2018

Singapore was largely unscathed from the various global cyber campaigns of 2017, but everyone needs to remain vigilant. In the near term, we anticipate the following trends to persist.



1

MORE DISRUPTIVE ATTACKS AGAINST COUNTRIES, BUSINESSES, AND INDIVIDUALS

Cyber-attacks are likely to grow more disruptive and destructive. Industrial Control Systems vulnerabilities may continue to be targeted, leading to industrial incidents and even injuries.

2

THREATS TO CONNECTED MOBILE DEVICES WILL GROW

Hackers will target mobile devices using methods such as phishing scams, spoofed mobile applications, and “free” public Wi-Fi. These methods may be used to steal personal information, spread malware, and conduct cyber espionage.

3

STATE-LINKED ACTORS WILL BECOME BOLDER

State-linked cyber actors may make bolder moves – including disruptive attacks against CIIs – to further their backers’ geopolitical agendas.

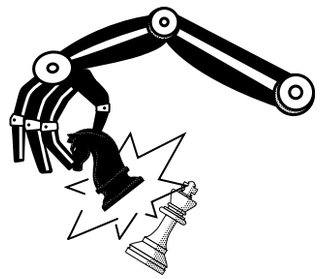
4

THREAT ACTORS WILL ACTIVELY TARGET WEAK LINKS

Determined attackers will seek out less well-protected entities with linkages to critical targets. Once compromised, these “softer” targets may expose their partners to cyber-attacks.

5

MORE SIGNS OF AI-ENABLED CYBER THREATS AND SOLUTIONS



Artificial intelligence and machine learning (AI/ML) technologies can be weaponised by cyber-attackers to infiltrate and wreak havoc on systems, and to make social engineering even more personalised.

On the flip side, AI/ML can be leveraged for cyber defence. Cyber defenders will look to take advantage of new tools and capabilities to detect anomalies and counter malicious activity in cyberspace.

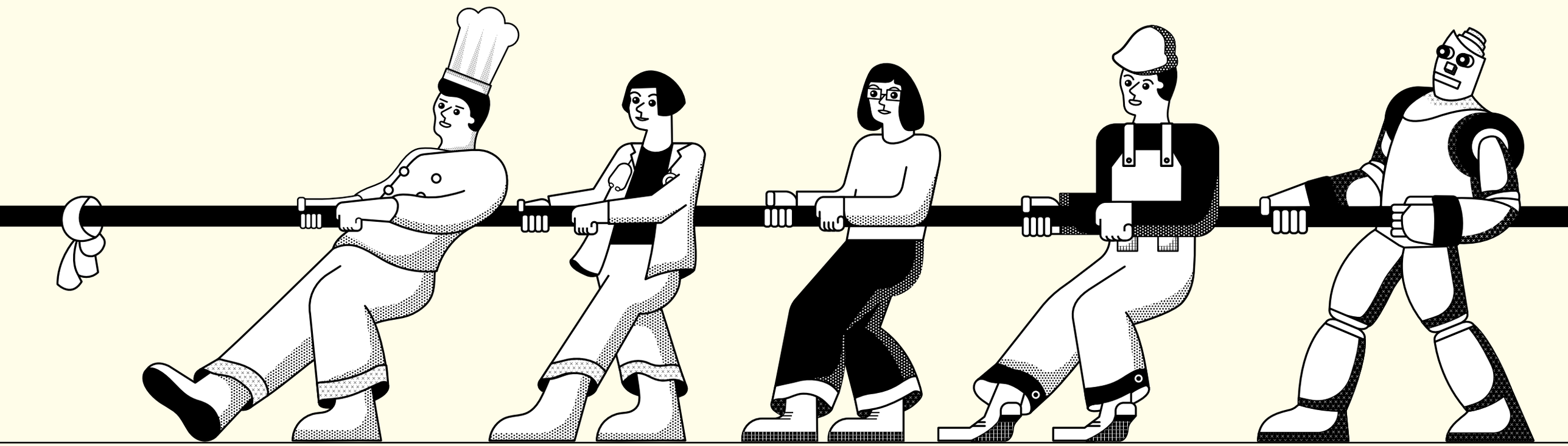
WEAK LINKS IN THE (BLOCK)CHAIN

Blockchain technology offers a decentralised, transparent, and secure record of transactions across a peer-to-peer network. This technology undergirds cryptocurrencies such as Bitcoin and Ether.

But blockchain technology offers other potential uses, which include supply chain management, intellectual property protection, and election security.

Those considering using blockchain technology solutions should ensure that the surrounding ecosystem is secure. For instance, cryptocurrency exchanges and unsecured "wallets” that facilitate such transactions may be vulnerable to other attack vectors, and can be prominent targets for hackers and cybercriminals.

2017 saw more vulnerabilities disclosed and disruptive attacks happening than in previous years. More cyber-attacks are likely. Cybersecurity is a team sport – we all have a part to play, and we all need to play our part well. We can start by practising good cyber hygiene. While we do what we can as individuals, the Singapore Government will also continue to work with stakeholders here and internationally towards a safe and trustworthy cyberspace.



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.
Blockchain Technology	A decentralised record-keeping technology that can be used by cryptocurrencies such as Bitcoin to allow secure, public, and anonymous transactions to take place. Transactions are batched together as "blocks", which are secured using cryptography, and designed to be tamper-resistant and immutable.
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.
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.
Cybercrime	Refers to (a) offences where a computer system is the target of a criminal act; and (b) offences where traditional crimes are committed via the means of a computer system. The first category refers to offences under the Computer Misuse and Cybersecurity Act (CMCA) and the second category refers to traditional crimes performed online such as online cheating, and cyber extortion. See "National Cybercrime Action Plan," Ministry of Home Affairs, 20 July 2016.
Cyber-Physical Systems (CPS)	A new generation of systems with integrated computational and physical capabilities that can interact with humans through many methods.
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. It does not exist in a physical form per se. 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.
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 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.
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	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 hackers 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 or deceiving 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

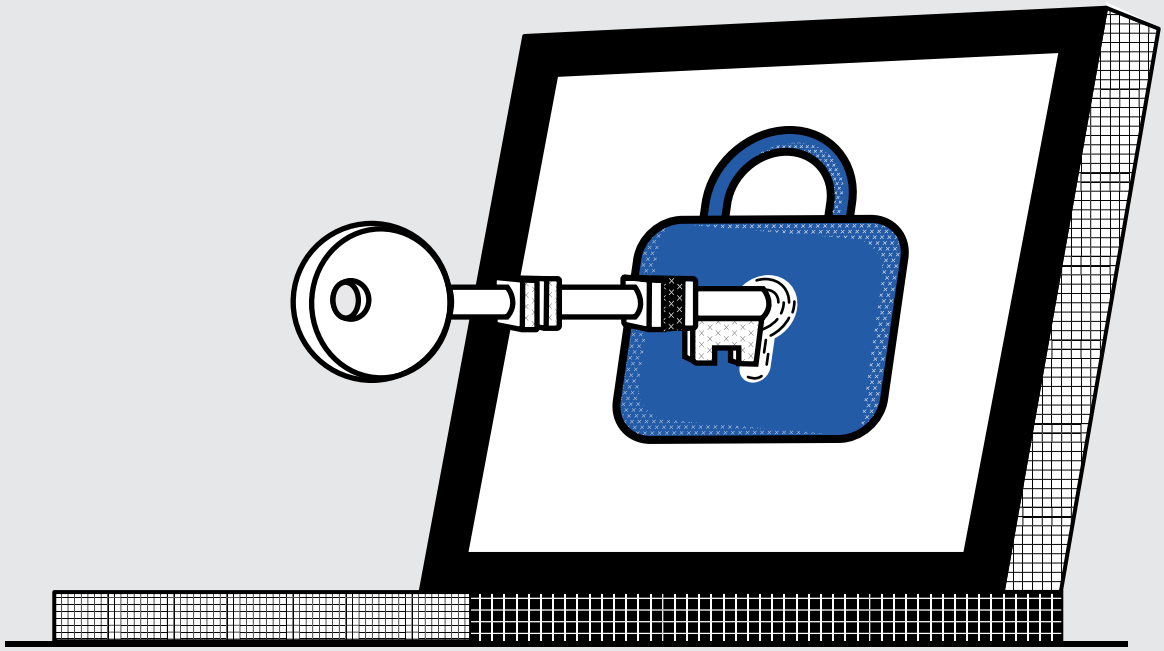
General enquiries/feedback:
gosafeonline@csa.gov.sg

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



CSA SINGAPORE