# SINGAPORE CYBER LANDSCAPE 2016

# CONTENTS




**Singapore Cyber Landscape 2016**


Copyright © 2017
by Cyber Security Agency of Singapore
All rights reserved.



ISBN: 978-981-11-3519-4

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

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

# FOREWORD

The global cyber landscape in 2016 saw new attempts to disrupt critical information infrastructure, rising ransomware incidents and the growing use of Internet of Things (IoT) devices to launch attacks.

Singapore similarly faced such threats. Our high level of connectivity comes with a corresponding level of vulnerability. While advances in digital technology have opened up new possibilities to enhance our lives, they have also exposed us to cyber threats that aim to cheat us, steal or alter our data, disrupt our daily business activities, and cripple our critical infrastructure.

Cyber-attacks are becoming more frequent and damaging. The impact of a cyber-attack was keenly felt in the United States of America in October 2016, when a major Domain Name System (DNS) faced a Distributed Denial of Service (DDoS) attack. Usually, DDoS attacks target websites, but that attack struck at a core infrastructure of the Internet – essentially the Web's "telephone directory". More than 80 organisations that relied on it to connect visitors to their respective websites, could not do so. That incident may have resulted in inconvenience mostly, but it could also be considered a harbinger of things to come.

Even as this publication reviews the incidents in 2016, major cyber-attacks in the first half of 2017 continue to put everyone on alert. The "WannaCry" and "NotPetya" cyber-attacks led to disruptions in many services. These incidents will be more fully presented in the Cyber Landscape 2017 report, including how Singapore managed them even though we were relatively unscathed. Such incidents, and their rapid global impact, remind us that we must continue to do our part, to make cyberspace a safer and more trustworthy one.

We hope that this first edition of the Singapore Cyber Landscape can point you in the right direction. This review of Singapore's cyber threat situation provides some understanding of the gravity of what we as individuals, organisations and the nation, are dealing with. Knowing the enemy, their motivations and techniques, will allow us to have a fighting chance of detecting intrusions earlier and dealing with them promptly.

In cyber, it is important to aim for resilience. This is because it is impossible to prevent successful attacks 100 per cent of the time. As Singapore pursues its plans to build a Smart Nation, we cannot afford to ignore the threats that come with it. The Cyber Security Agency of Singapore (CSA) will be your partner in making cyberspace a safer space for all.

**David Koh**
Chief Executive
Cyber Security Agency of Singapore

# EXECUTIVE SUMMARY

## CYBER LANDSCAPE 2016

Globally, in 2016, IoT devices like Wi-Fi routers and webcams were hijacked to launch cyber-attacks, specifically DDoS attacks. This resulted in many websites and services being inaccessible. Ransomware was another significant type of cyber-attack that hit industries and individuals, locking them out of their systems. Singapore is certainly not immune to these cyber threats, which can be expected to evolve and emerge in bigger, bolder and faster ways. CSA is keeping a close watch on the cyber landscape and, in this publication, will provide an analysis of the cyber threats that Singapore faced between January and December 2016.

The cyber-attacks and threats covered in this publication are just the tip of the iceberg. The absolute number of incidents will be hard to determine – despite best efforts, not all cases are reported or can be detected – but CSA's observations could provide a baseline towards a further understanding of Singapore's cyber threat landscape. In turn, that may illuminate more ways to better defend ourselves against similar or new threats. The Government will take the lead, and partner the industry, academia, public and people sectors, and international counterparts, to enhance cybersecurity for the nation, so that Singaporeans and Singapore can reap the long term benefits of having a safe and trustworthy cyberspace.

## THE NATIONAL CYBER SECURITY COMMAND

At the frontline to monitor and respond to cyber threats in Singapore is CSA's National Cyber Security Command (NCSC). It comprises the National Cyber Threat Monitoring Centre (NCTMC), National Cyber Incident Response Centre (NCIRC), and the National Cyber Threat Analysis Centre (NCTAC). The centres work closely together and with stakeholders to respond to cyber threats, research, and make sense of the cyber landscape to protect Singapore's Critical Information Infrastructure (CII), and to enable a safer cyberspace for businesses and individuals.

In 2016, NCSC saw cyber-attacks of varying nature and impact across many sectors, including the Government, Banking & Finance, and Healthcare sectors. For instance, the Healthcare sector was struck by ransomware attacks that left some individual healthcare practitioners unable to access patient data. However, the attacks did not disrupt Singapore's healthcare system as the incidents were contained and no other systems were compromised.

The Government sector also continued to be targeted, facing attacks from website defacements to phishing. The Internet Surfing Separation (ISS) policy announced in June 2016 will go a significant way towards securing the Government's Infocommunications Technology (ICT) environment as it would enhance the security of the Government's network from attacks originating from the Internet.

Besides attacks targeting these critical sectors, NCSC also saw individuals and small and medium enterprises (SMEs) being victims of website defacements, business e-mail scams, phishing, and ransomware. In Singapore, 43 per cent of cybersecurity incidents reported by individuals and SMEs to the Singapore Computer Emergency Response Team (SingCERT)[1] were phishing attacks. One of the most common cyber threats SMEs reported to SingCERT was business e-mail scams.

[1] SingCERT is the focal point in Singapore for the public to report cybersecurity incidents and issues, and liaises with CERTs in other countries to better manage the borderless nature of cyber threats. Businesses and individuals could report incidents to SingCERT by dialling its hotline – (+65) 6323 5052 or e-mail to singcert@csa.gov.sg

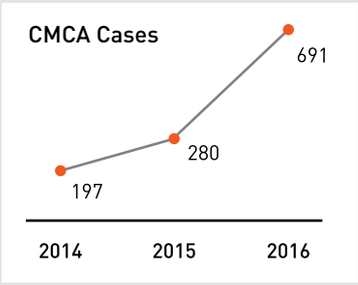
## CRITICAL CYBER CONCERNS

### Actors Targeting Singapore

Cyber threats can be carried out by a host of different cyber-attackers, or threat actors as they are commonly known. The cyber community has long struggled with the challenge of definitively attributing the specific source of a cyber-attack or crime, as attackers can use a range of tools to cover or distort their tracks. Threat actors targeting Singapore run the gamut from script-kiddies to Advanced Persistent Threats (APTs). Their behaviour, intentions, and capabilities are always evolving and require close watch. Globally, APTs are a growing concern as they are often undetectable in networks for long periods. APTs may refer to both the nature of the attack (persistent and sophisticated), and the attackers (well-organised and usually state-sponsored). APT groups generally target government institutions and large organisations for the purpose of espionage and other illegal acts.


### Cybercrime

Under Singapore's Cybersecurity Strategy launched in 2016, one key priority is to build a safer cyberspace for Singaporeans and businesses. The area of cybercrime comes under the responsibility of the Singapore Police Force (SPF).




The SPF noted an increase in the proportion of cybercrimes to overall crime cases from 7.9 per cent in 2014 to 13.7 per cent in 2016, underscoring the growing attractiveness of digital platforms for criminals. Cases reported under the Computer Misuse and Cybersecurity Act (CMCA) more than doubled year-on-year to 2016, with ransomware, and the compromise of online and banking accounts, constituting the top five categories in 2016.

# EXECUTIVE SUMMARY

## COMMON CYBER THREATS IN SINGAPORE

**Prevalent cyber threats observed in Singapore's cyberspace[2] in 2016 were defacements, phishing, ransomware, and compromised Command & Control (C&C) Servers, the last being potential launch-pads for other cyber-attacks, such as DDoS. A snapshot of these common cyber threats is as follows:**

### Ransomware:

It is one of the biggest cybersecurity threats to businesses and individuals today. Some reports noted that there may be as many as 550 ransomware-related attacks every day in Singapore. However, many cases may go unreported. Some people may decide to reformat their affected computer, and companies may not want to report it to protect their corporate reputation. CSA received 19 reports of ransomware cases from individuals and SMEs in 2016. Cerber, CryptoLocker and Locky were among the types of ransomware reported. As ransomware attacks grew in 2016, SingCERT issued an advisory in May 2016 to warn the public of such dangers and provided precautionary measures to be adopted.

### Defacements:

Nearly 1,800 website defacements were detected in Singapore in 2016, with the majority being websites of SMEs from a range of businesses such as interior design and manufacturing. The perpetrators included hacktivists keen to promote a certain ideology, and whose attacks were observed across other countries as well. One in 10 defaced websites was hosted on servers running outdated operating systems, which may have resulted in them being vulnerable to such attacks.

### C&C Servers & DDoS:

More than 60 C&C servers were detected. It is not immediately apparent who might have set them up, what they intended to do with these servers, and if any damage was done. Whenever a new C&C server is detected, SingCERT will inform the respective Web hosting providers to rectify the issue. Potentially, C&C servers could be used to control botnets – a network of compromised computers ¬– that in turn could be mobilised for DDoS attacks. The thousands of IoT devices marshalled for DDoS attacks in the USA in October 2016 may hint of similar threats to come. DDoS ransom threats were also observed in Singapore's cyberspace, believed to be carried out by cyber criminal groups.

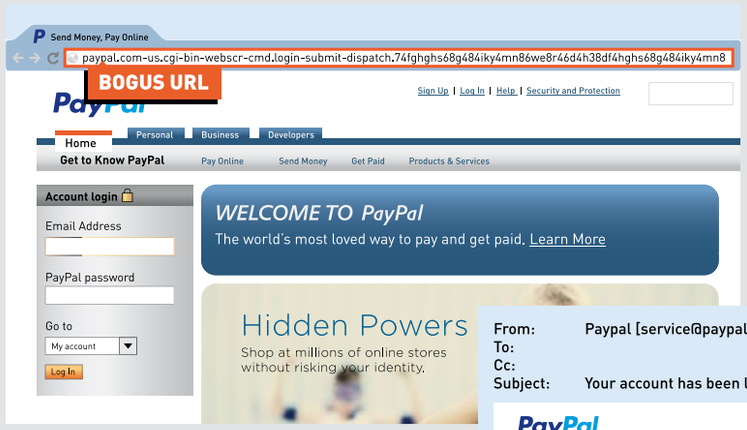
### Phishing:

More than 2,500 phishing URLs were detected in 2016, with the Banking & Finance sector appearing to be the most spoofed (31 per cent of all observed phishing URLs). Among online services, PayPal was spoofed most often in phishing campaigns. CSA also observed that file-hosting service providers were popular targets as hackers could easily harvest user credentials from there. Some Government institutions were also spoofed, as attackers sought personal data such as passport numbers that could be traded in underground markets.

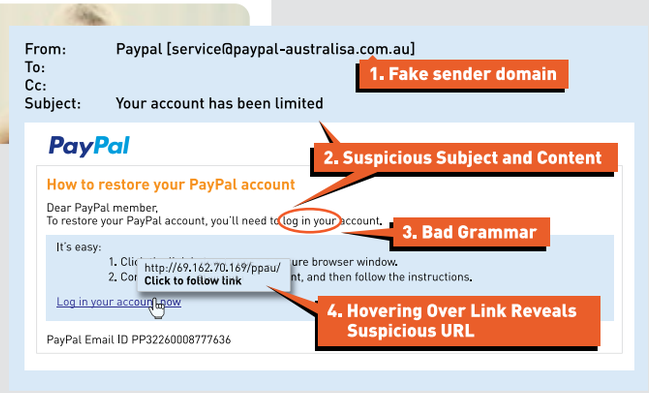
[2]"Singapore cyberspace" refers to websites ending with the .SG domain or mention Singapore in its URL, IP addresses used in Singapore or Internet Service Providers (ISP) that are located in Singapore.



**Examples of Phishing Scams:**




Phishing Site




Phishing E-mail

## KEEPING OUR CYBERSPACE SAFE AND TRUSTWORTHY TOGETHER

**A conducive environment for monitoring, early detection, and quick response to cyber threats and attacks also requires effort in these areas:**

### Raising Cyber Awareness

Our outreach programmes and roadshows aim to promote cyber-savviness among businesses and individuals. SingCERT has issued advisories to educate the public on cyber issues such as ransomware, DDoS attacks and compromised remote servers.

### Developing Cybersecurity Professionals

Singapore is also growing its cybersecurity ecosystem, which includes boosting the talent pool. The Cyber Security Associates and Technologists (CSAT) programme, a joint initiative by CSA and the Infocomm Media Development Authority (IMDA), was launched in 2016 to train and upskill new and existing ICT and engineering professionals for cybersecurity roles.

### Regional and International Exchanges

Singapore has been actively involved in the past year in various international platforms on cybersecurity, from multilateral discussions on cyber norms to bilateral co-operation and regional capacity-building programmes.

CHAPTER 1

# CYBER THREATS SINGAPORE FACES

This inaugural edition of the **Singapore Cyber Landscape 2016** will provide a closer look at the cybersecurity situation here, including qualitative and quantitative reviews of the nation's cyber health, and some of the Cyber Security Agency of Singapore's (CSA) response and recovery efforts.

On the frontline of such efforts is the National Cyber Security Command (NCSC), which monitors and responds to cyber threats, and research and makes sense of the implications of these threats to Singapore's CII, businesses and individuals. The NCSC carries out such work through three teams, namely the National Cyber Threat Monitoring Centre (NCTMC), National Cyber Incident Response Centre (NCIRC), and National Cyber Threat Analysis Centre (NCTAC). Through the NCSC, data from incidents in Singapore's cyberspace are analysed. "Singapore's cyberspace" will include domain names with ".sg" or Singapore-mentions, Internet Protocol (IP) addresses used in Singapore, or Internet Service Providers (ISPs) based in Singapore.

In the event of major cyber incidents affecting Singapore's CIIs, CSA, supported by NCSC, will take on the role of the national incident manager, coordinating cross-sector incident response, implementing specific national-level mitigation measures, and providing incident response assistance to the affected CIIs.

# NATIONAL CYBER SECURITY COMMAND

## NATIONAL CYBER THREAT MONITORING CENTRE (NCTMC)

**NCTMC** plays a key role in maintaining cyber situational awareness to aid in the discovery of cyber threats that are of national significance.

NCTMC also forewarns the nation's critical sectors on emerging cyber threats unique to their operating environment.

In cyber incidents involving multiple sectors, the centre will coordinate with the Sector Leads to provide quick and timely alerts to cross-sector threats as part of the national-level response.

## NATIONAL CYBER INCIDENT RESPONSE CENTRE (NCIRC)

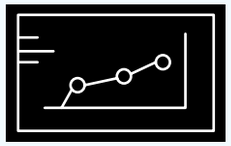
**NCIRC** is the operational arm of NCSC that responds to cyber threats and incidents affecting the critical information infrastructure in Singapore.

As the National Cyber Incident Manager, NCIRC maintains strategic oversight of significant cyber incidents in the critical sectors to assess Singapore's cyber posture.

During cyber crises, NCIRC is responsible for coordinating cross-sector incident response efforts and directing national-level mitigation measures.

**SingCERT** is the national CERT. Under the aegis of NCIRC, it tracks the broader Singapore cyber landscape to identify significant threats, and issues cybersecurity advisories to Singaporeans. SingCERT also works with foreign CERTs to manage cross-border cyber incidents.

## NATIONAL CYBER THREAT ANALYSIS CENTRE (NCTAC)



**NCTAC** conducts all-source research and analysis to provide strategic insights on the Singapore cyber landscape.

NCTAC's research and analysis also include geopolitical perspectives, which often underpin the motivations and actions of cyber actors.

NCTAC's insights aim to inform CSA operations, national cyber policy-making, and contribute to public education.

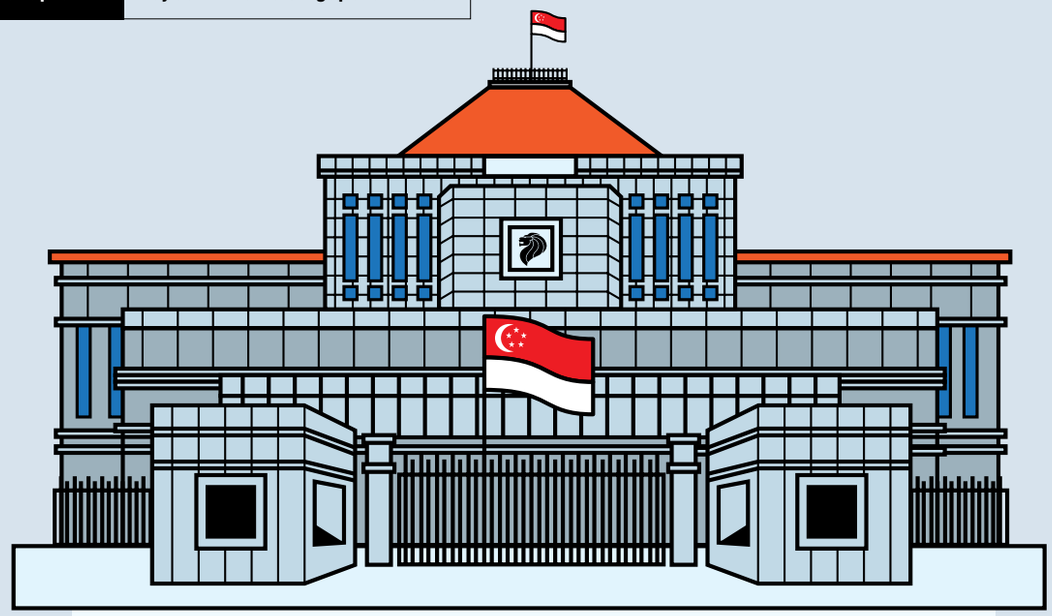


# THREATS TO CRITICAL INFORMATION INFRASTRUCTURE (CII)

Cyber-attacks on CIIs can result in widespread disruptive and destructive impact on society and the economy. A particularly severe attack could even have spillover effects on the region and the rest of the world. Cyber-attackers are constantly sharpening their ability to carry out such attacks, and their objectives range from financial gain to ideological or nationalistic causes.

CSA has identified 11 CII sectors. They are: Energy, Water, Banking & Finance, Government, Healthcare, Media, Infocomm, Land Transport, Maritime, Aviation, and Security & Emergency. In 2016, several CIIs were affected by malware infection, in particular, ransomware.

To better guard against such threats and attacks, the Government has been conducting cyber exercises over the years to improve the critical sectors' readiness and incident response plans. In March 2016, Exercise Cyber Star, a multi-sector exercise was conducted by CSA. It brought together representatives from the Infocomm, Energy, Banking & Finance, and Government sectors to exercise their responses to a nationwide cyber-attack.



# THREATS TO GOVERNMENT

The Singapore Government had its share of cyber-attacks in 2016. Public agencies faced attacks that included phishing and APTs (See Chapter 2, Page 24 for an analysis on APT). The **Internet Surfing Separation (ISS)** policy announced in June 2016 will go a significant way towards securing the Government's ICT environment. In removing the link between the public officers' computers from the Internet, it can disrupt the attackers' cyber kill chain. Without a path out to the Internet, the attacker will not have remote access to the Government's network, and will not be able to extract data as easily.



**CASE STUDY**

**APT Malware Infection in Government Organisation**

**WHEN**

Late-2016

**BACKGROUND**

CSA was alerted to a possible APT malware infection in an organisation in the public sector.

CSA found the malware infection – which had backdoor capabilities – on one Internet-facing computer. Fortunately, the infected computer had not been used to process sensitive information.

**EVIDENCE**

Suspicious attempts to connect at regular intervals to a C&C server, which was later determined to be a compromised server.

**CASE ANALYSIS**

From the investigations, CSA assessed it to be the work of a state-sponsored APT actor, which up till then had not been known to be active in Asia. The incident however was assessed to be more an opportunistic one than a targeted attack.

Investigations also concluded that data was not exfiltrated, though the malware had the capability to do so. The malware was also not observed to have spread beyond the infected computer to the rest of the organisation's network. The organisation did not detect the malicious network traffic earlier because the warning indicators and malware signatures were not on known anti-malware databases.

The APT actor was believed to be a group supported by a foreign government (also referred to as a "state-sponsored group"), to engage in cyber espionage to further their national interests. It had not been known to value targets in Asia, but with this incident, it could suggest an expanded scope of targets in the region.

**TACTICS, TECHNIQUES & PROCEDURES**

Attackers used sophisticated anti-detection and infection techniques: multi-stage infection through a phishing e-mail that ultimately allowed the attacker backdoor access.

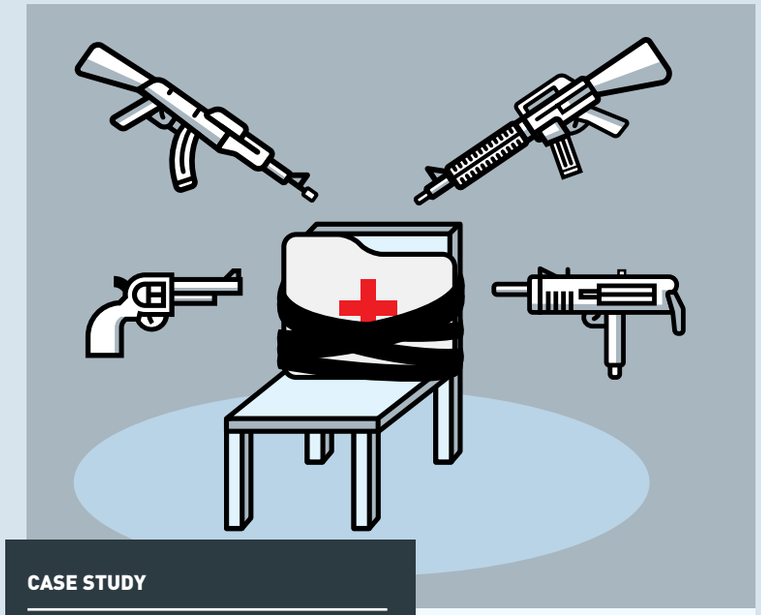
**FOLLOW-UP ACTION**

Recommendations were provided to the organisation to further secure its ICT environment and prevent similar incidents. These included blocking unauthorised macros or programs, implementing application whitelisting, and segregating networks.

**One example of segregating networks is the Internet Surfing Separation policy the Singapore Government announced in June 2016, that will help to prevent data from being transmitted to or extracted from the Internet.**

# THREATS TO HEALTHCARE SECTOR

In 2016, the Healthcare sector experienced the highest number of ransomware attacks compared to other sectors. Although these attacks did not affect Singapore's overall healthcare system, they served to remind everyone to be more careful when handling files and data in their day-to-day work.



**CASE STUDY**

## Ransomware in Healthcare Sector

**WHEN**

Late-2016

**BACKGROUND**

Ransomware incidents were detected in Singapore's Healthcare sector, with individual users unable to access their files on the network. Investigations by CSA showed that these users were infected after they opened attachments or clicked on links found in e-mails they had received.

Immediate action by the respective institutions and the healthcare authorities helped to contain the issue.

**EVIDENCE**

Cryptoware found in system, and files were encrypted.

**CASE ANALYSIS**

Upon detection, affected computers were successfully isolated to prevent the ransomware infection from spreading to the wider network. As a result, there was no impact to the sector's CII assets. The affected computers were wiped clean, had their programs reinstalled, and data restored from back-ups.

**TACTICS, TECHNIQUES & PROCEDURES**

Phishing e-mails, websites hosting malicious files.

**FOLLOW-UP ACTION**

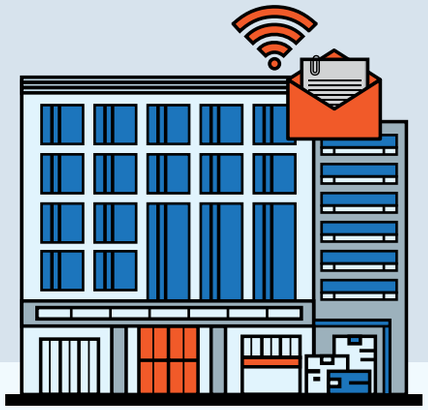
Strengthen human security of networks and systems by increasing user awareness of ways to avoid ransomware and other malware infections.

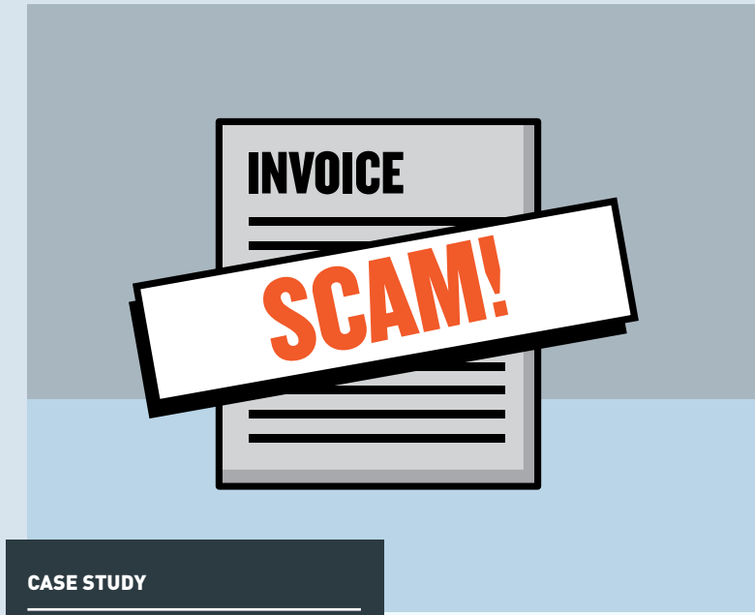



# THREATS TO SMEs

As more SMEs go digital, they may find themselves facing new threats, such as phishing attacks and defacements. Through greater awareness and some technical know-how, SMEs may be better able to defend themselves against cyber-attacks.

In Singapore, 43 per cent of security incidents reported to SingCERT by individuals and SMEs occurred through phishing attacks. Cyber criminals may attack SMEs as a means of getting to larger corporations, to which SMEs are suppliers. One of the most common cyber threats SMEs reported to SingCERT in 2016 was business e-mail scams. Millions of dollars were lost through phishing scams where hackers impersonated company executives or business partners via e-mail. SPF figures also showed that there was a 20 per cent rise in e-mail impersonation scams in 2016 compared to 2015.






**CASE STUDY**

## Invoice Scam Case

**WHEN**

May 2016

**BACKGROUND**

A Singapore company received an e-mail apparently from a known supplier, requesting for the payment for the purchase of company supplies from Japan.

The company found the e-mail suspicious as it contained an unfamiliar domain name, and reported it to SingCERT. No funds were transferred to a bank in Hong Kong as requested in the e-mail, and no financial loss was reported.

**EVIDENCE**

Invoice attachments, e-mail headers.

**CASE ANALYSIS**

Results from an analysis of the e-mail headers showed that the e-mail was spoofed, and suggested that the Japanese supplier's e-mail account might have been compromised.

**TACTICS, TECHNIQUES & PROCEDURES**

E-mail spoofing, impersonation.

**FOLLOW-UP ACTION**

SingCERT provided its findings to the Singapore company owner, and proposed that they alert the Japanese supplier of the possible compromise of its e-mail account. The company owner also lodged police reports in Singapore and Hong Kong.

Such incidents are not new; SingCERT observed that several businesses have been tricked into transferring funds to scammers. It recommends SMEs to always verify details – for instance to call the supplier (telephone) first to confirm the sums – before making any funds transfer.

# THREATS TO INDIVIDUALS

Individuals tend to fall victim to cybercrime for two reasons: **lack of cybersecurity awareness**, **and poor cyber hygiene practices.** While having a connected lifestyle is almost a necessity today, many individuals are not sufficiently diligent about securing their digital lives.

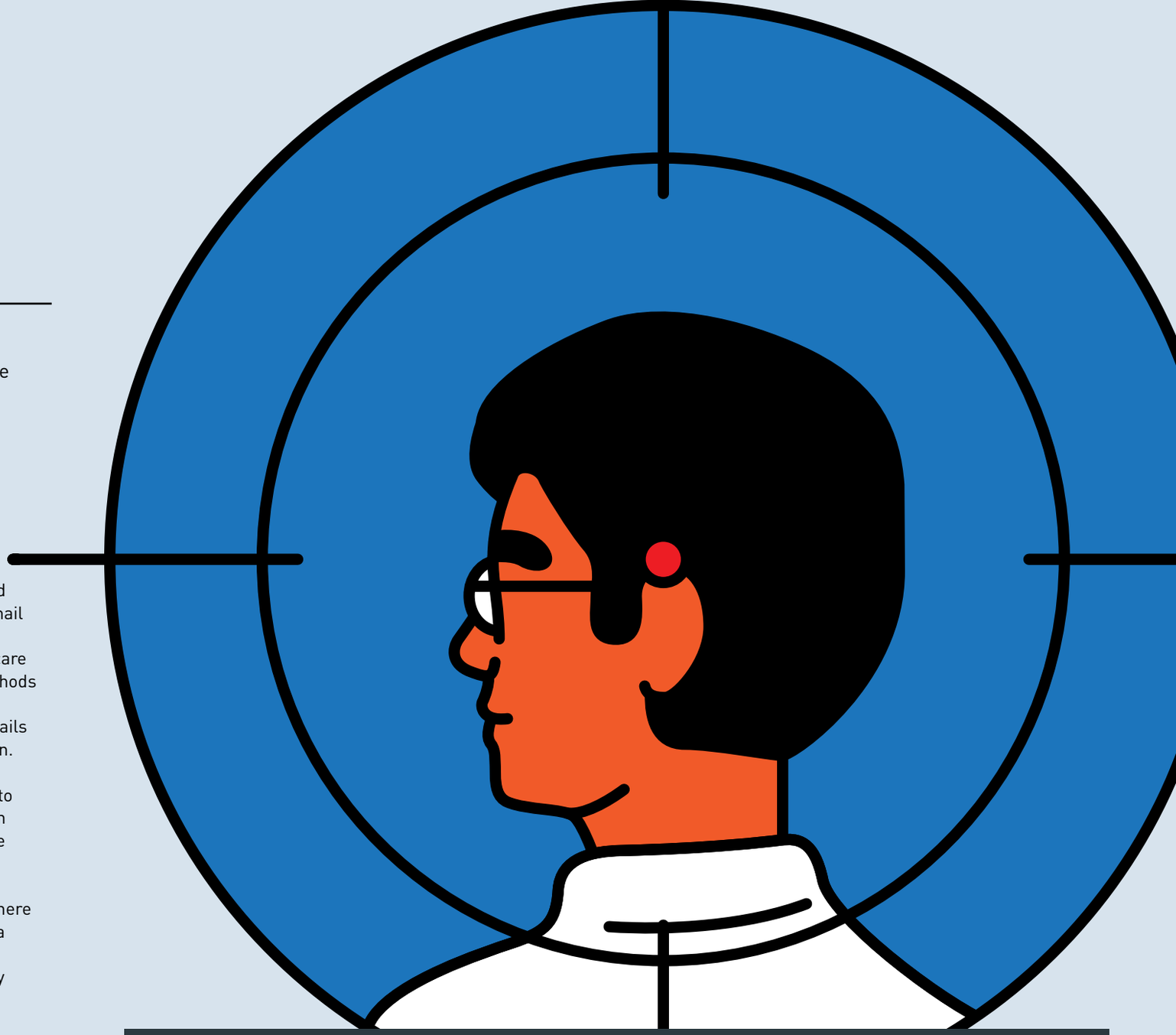
From CSA's Public Awareness Survey conducted in August 2016, one in three respondents said that they did not install security apps in their mobile phones, citing reasons such as not seeing the need to, or that the app took up too much space. Other poor practices include not managing their passwords securely, connecting to open and non-password protected Wi-Fi networks in public places, and not adopting Two-Factor Authentication when the option is available.

The most common cyber threats to individuals are compromised e-mail accounts and malicious websites. E-mail accounts may be compromised by malware sent through e-mails (e.g. phishing e-mails). Such e-mails are targeted and may appear personal. They prey on the likelihood of a person clicking on links or opening attachments, with messages containing payment requests, warnings, threats or other triggers for action. By clicking on malicious links or opening malicious attachments, individuals unwittingly allow unauthorised access to their e-mail account. Once the attackers have gained entry, they can carry out more e-mail scams by impersonating the legitimate e-mail account holder, or they could dig deeper into the victim's system to steal login credentials, banking information and other personal data.

Some users assume that the standard filters in Web-based or corporate e-mail servers will block out all malicious e-mails, and therefore exercise less care when opening e-mails. As attack methods evolve, attackers will keep trying to circumvent such filters. In short, e-mails should always be handled with caution.

Many individuals may also fall victim to malicious websites when they click on unfamiliar Web links or pop-ups while surfing the Web. Malicious websites generally attempt to spoof legitimate ones, luring people into transacting there instead of the actual website. This is a common technique to elicit personal data, login credentials, or even money from unsuspecting individuals.

In Singapore, legitimate online merchants and services that have been spoofed include PayPal, Google, Dropbox, and the e-services offered by the Ministry of Manpower and the Immigration & Checkpoints Authority. As e-commerce, e-services, and Cloud storage services continue to grow in availability and use, users need to be more aware of such attempts to steal their personal data and money, to avoid falling into such traps.

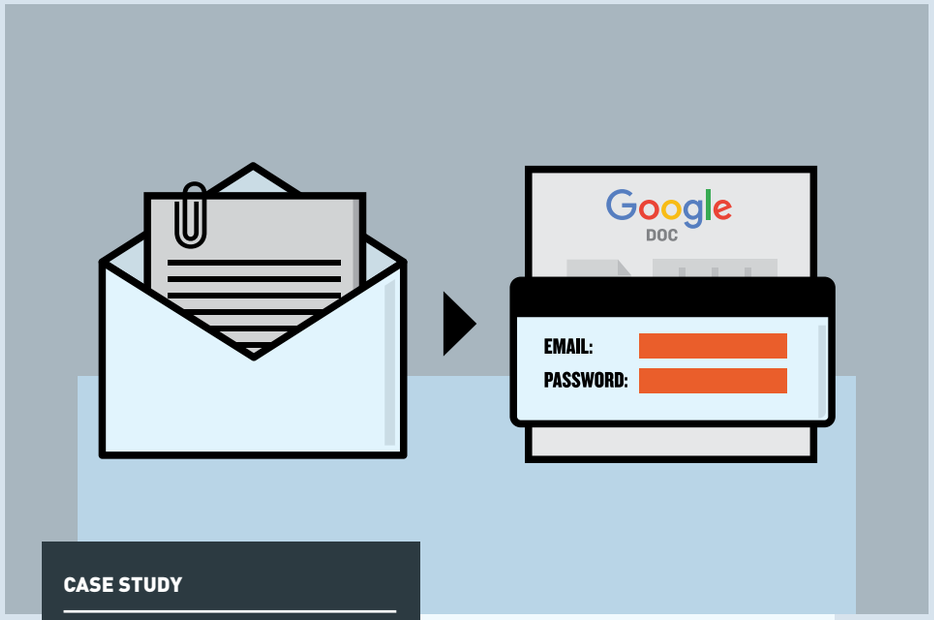


**Ransomware is a category of malware used by attackers to encrypt data on targeted systems and demanding a ransom for the data to be decrypted.**

2016 also saw an increase in the number of ransomware incidents reported to SingCERT. Individuals and SMEs in Singapore who reported being victims of ransomware have generally chosen not to pay the ransoms, but instead would restore their data from backups. Performing regular backups is one of the key ways to deal with ransomware[3].

(See Page 31 on ways to deal with ransomware)

[3] SingCERT released an advisory on May 2016 providing tips on how to deal with ransomware – [SingCERT] Ransomware. (2016 May 6). Retrieved from https://www.csa.gov.sg/singcert/news/advisories-alerts/ransomware




## CASE STUDY

### Compromised Gmail Account

**WHEN**

February 2016

**BACKGROUND**

An individual reported to SingCERT that his Gmail account may have been compromised.

This was after he had clicked on an attachment in an e-mail that led him to a website apparently containing Google Doc templates. At the website, he was prompted to enter his e-mail password. Concerned that he might have already gone too far by opening the attachment, he checked with the sender of the e-mail, who informed him that the e-mail was fake.

**EVIDENCE**

Suspicious e-mail with a malicious document attached.

**CASE ANALYSIS**

A hyperlink was observed when the mouse cursor hovered over the attachment icon. The hyperlink directed the individual to a website set up to phish information from Internet users.

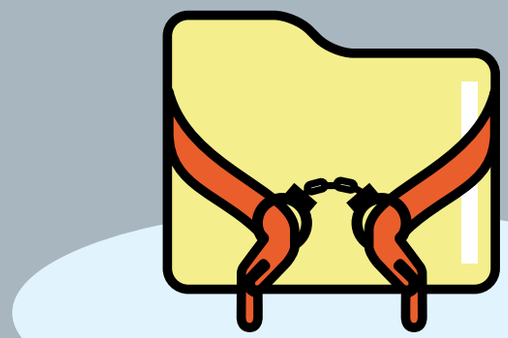
**TACTICS, TECHNIQUES & PROCEDURES**

E-mail with suspicious links or malicious attachments, stealing credentials.

**FOLLOW-UP ACTION**

SingCERT advised the individual to check if his account had indeed been compromised by reviewing the log-in sessions via his Gmail security settings, a section which would show the devices that had access to his account. SingCERT also advised the individual to strengthen his e-mail account settings by activating the Two-Factor Authentication option.





## CASE STUDY

### Individual infected with Ransomware

**WHEN**

February 2016

**BACKGROUND**

An individual reported to SingCERT that his computer was displaying a message that his files had been encrypted, and that payment in Bitcoins was required to restore the files.

**EVIDENCE**

Ransom note displayed on computer screen, detailing steps that needed to be taken to decrypt the files.

**CASE ANALYSIS**

SingCERT found that the individual's computer had been infected with the CryptoLocker ransomware.

**TACTICS, TECHNIQUES & PROCEDURES**

Malware infection, encryption.

**FOLLOW-UP ACTION**

As a decryption tool for this ransomware was available online, SingCERT guided the affected individual in using it to restore his files. The individual was also advised on cyber hygiene best practices to avoid being infected again.


Screenshot of Ransom Note

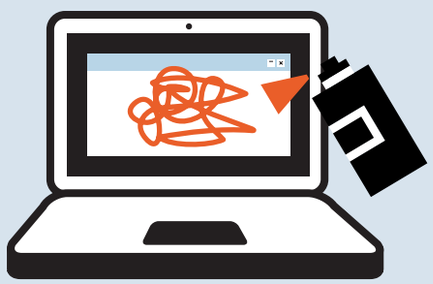
*Facts and figures from Cyber Security Agency (CSA) and Singapore Police Force (SPF)

# OVERVIEW OF CYBER THREATS IN 2016

## RANSOMWARE

- **19 RANSOMWARE** cases reported to SingCERT in 2016, up from two cases in 2015
- Many cases may go unreported: Companies may be reluctant to admit being affected, as that may affect the reputation of their business
- **Companies of all sizes and individuals** can be victims
- **Cerber, CryptoLocker and Locky** among the types of ransomware reported

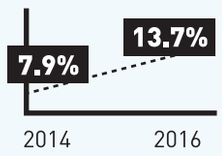
## WEBSITE DEFACEMENT



- **1,750** Singapore (.SG) website defacements reported
- Main targets: **Small and medium-sized enterprises (SMEs)** from a range of businesses, including interior design, logistics, manufacturing and construction.
- 1 in 10 defaced websites found hosted on old or outdated operating systems such as Windows Server 2003

## INCIDENTS REPORTED

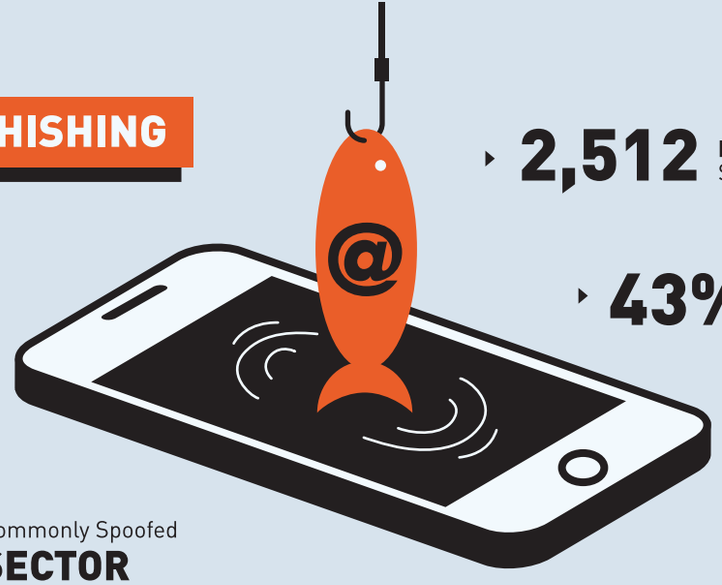
### RISING CYBERCRIME OVER THE YEARS




Proportion of cybercrime to overall crime cases rose from **7.9% in 2014** to **13.7% in 2016**.

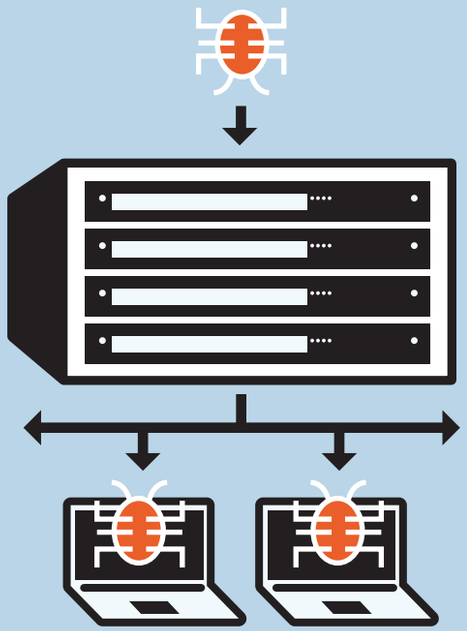
Cybercriminals also commited more crimes under the Computer Misuse and Cybersecurity Act (CMCA) in 2016, including ransomware, hacking and compromise of online accounts. **CMCA cases more than doubled year-on-year to 691 in 2016.**

## PHISHING



- **2,512** **phishing URLs** with Singapore-link
- **43%** of security incidents reported to SingCERT by **individuals and SMEs** occured through phishing attacks
- Commonly Spoofed **SECTOR**
  - **BANKING & FINANCE**
- Commonly Spoofed **BRANDS**
  - **PayPal**
  - **Dropbox**
  - **Google**
- Commonly Spoofed **GOVERNMENT ORGANISATIONS**
  - **Ministry of Manpower (MOM)**
  - **Immigration & Checkpoints Authority (ICA)**

## COMMAND AND CONTROL (C&C) SERVERS



- **60 C&C SERVERS** have been observed within Singapore's cyberspace, capable of conducting malicious activities such as data theft, email-spam campaigns and **Distributed Denial of Service (DDoS) attacks**
- **Growth of DDoS ransom e-mails:** A number of organisations in Singapore have received such e-mails where hackers threaten to launch a DDoS attack against them unless payment is made, usually via Bitcoin

These five malware account for over half of botnets observed in Singapore's cyberspace

1. **Conficker**
2. **XcodeGhost**
3. **Zeroaccess**
4. **Mirai**
5. **Sality**

- Simple Service Discovery Protocol (SSDP), Domain Name System (DNS) and Network Time Protocol (NTP) account for **70 per cent** of vulnerable services in Singapore that can be used in a DDoS attack

## KEEPING OUR CYBERSPACE SAFE AND TRUSTWORTHY TOGETHER

- **Raising Cyber Awareness Among Individuals and Businesses**
- **Developing Singapore's Cybersecurity Professionals**
- **Facilitating Exchanges with Regional and International Partners**
- **Cybersecurity for a Smart Nation**

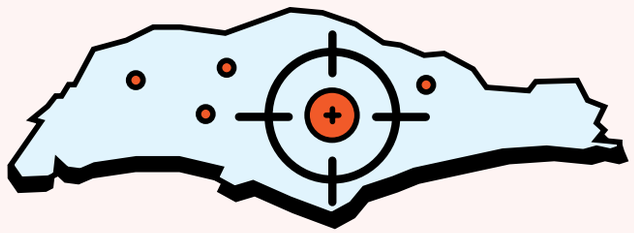
CHAPTER 2

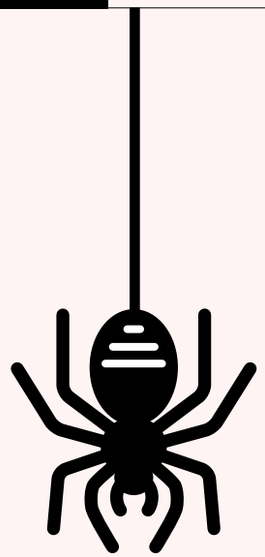
# CYBER THREATS IN FOCUS ACTORS TARGETING SINGAPORE

Because of the nature of cyberspace and the design of the Internet, it is always a challenge to attribute cyber-attacks to specific individuals or groups. There may be some who would openly publish their success story – such as those who post on public websites about their website defacements – but even then, they hide behind a pseudonym or "nickname" that may be hard to link to a specific individual or group.

There are elusive cyber-attackers that remain at-large, after having caused significant damage or losses. For example, the attackers behind major global cyber-attacks in 2016 who remain largely unknown include those behind the attacks against the SWIFT global banking network and the DDoS attacks in the United States of America and France. These actors often hide or mask their tracks to make it difficult to pin them down physically or geographically. Some usual means of doing so include using spoofed IP addresses that may not show the physical location in which they operate.

Threat actors targeting Singapore run the gamut from the script-kiddies to APTs. Their behaviour, intentions, capabilities, are always evolving and require close monitoring. CSA studies the trends of cyber-attacks in order to identify measures that individuals, businesses and the nation can adopt to better defend against similar or new threats.





# ADVANCED PERSISTENT THREAT(APT)

APTs operate stealthily and with sophistication, often hiding in networks for prolonged periods to plan their targeted attacks. APTs, which may refer to the type of attack, or the threat actor or group, are also often state-sponsored. Their mission includes espionage, data exfiltration, and data manipulation.

**CII SECTORS SUCH AS THE GOVERNMENT, BANKING & FINANCE, HEALTHCARE AND ENERGY SECTORS ARE ATTRACTIVE TARGETS FOR APT ATTACKS BECAUSE A STRIKE ON THEM COULD HAVE SIGNIFICANT IMPACT ON THE ECONOMY AND SOCIETY.**

Cyber activities associated with state actors are becoming more overt in recent times. Cyberspace is one environment through which sensitive information is obtained for state-on-state espionage. As geopolitical tensions rise, the need for international cyber norms becomes more pressing. [See Page 40 on Singapore's efforts to promote International Cyber Norms).

APT groups active in the Asia-Pacific region include APT1 and APT30; and Southeast Asia-based PLATINUM. CII sectors such as the Government, Banking & Finance, Healthcare and Energy sectors are attractive targets for APT attacks because a strike on them could have significant impact on the economy and society. One APT group was discovered to be eyeing a Singapore institution, using its signature tactic of phishing on individuals there. Through close collaboration between the institution and the authorities, the APT attempt was detected and halted before further harm could be done.

The early identification and stopping of malicious APT activity is a multi-stakeholder effort that would involve the intelligence community, law enforcement agencies, the targeted institution, and even foreign counterparts.

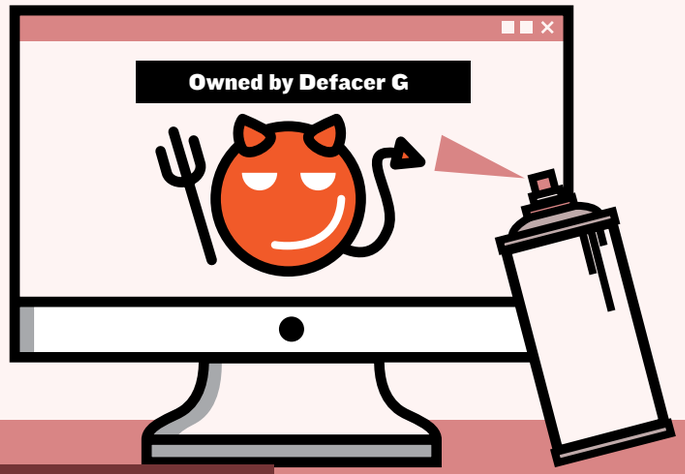
**Cyberspace presents a rich target environment and the rise in geopolitical tensions may potentially spill over into cyberspace with APT groups targeting key assets in Singapore and the region.**



# HACKTIVISTS

Hacktivism is the act of hacking, or breaking into a computer system, and/or defacing webpages to promote a political or ideological message. Hacking has arguably become an increasingly attractive alternative to conducting physical street protests as the Internet affords hacktivists anonymity and reach.

In 2016, there were a total of **1,750** Web defacement cases related to Singapore. Most of the websites defaced belonged to SMEs from a range of sectors including home interior design to healthcare. The hacktivists appear to be politically-motivated groups from the Middle East, and had also concurrently conducted their mass defacement activities on websites around the world.



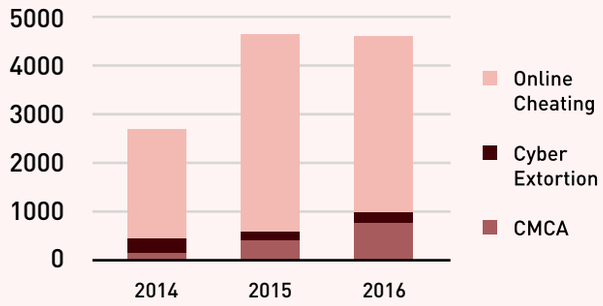

**CASE STUDY**

**Top Defacer in Singapore**

This group appears to be a politically-motivated hacktivist group from the Middle East. The group carried out website defacement attacks that often included messages bearing their views on issues such as the conflicts in Syria and Palestine. The group would typically replace the home page of the affected website with a cartoon of a devil carrying a pitchfork.

This group has been responsible for defacing as many as 339 Singapore websites in 2016, accounting for about 20 per cent of Singapore websites that were defaced last year. Targets included organisations in the non-profit sector. However, the group does not appear to target Singapore companies alone, as their acts of mass defacements were also carried out against company websites in other countries, including India and Iran. [See Page 32: Common Cyber Threats in Singapore - Website Defacement).

# CYBER CRIMINALS




**PROPORTION OF CYBERCRIME TO OVERALL CRIME CASES ROSE FROM 7.9 PER CENT IN 2014 TO 13.7 PER CENT IN 2016**

Singaporeans rely on the Internet for news and information, to connect with friends on social media, and to shop and transact online. Consequently, they have also become targets of cyber criminals who go online to seek illicit monetary gains.

SPF has observed that criminals have been increasingly moving their activities online, with the proportion of cybercrimes to the total number of crimes in all categories (inclusive of physical crimes) increasing over the past two years. The proportion of cybercrime to the total number of crime cases has been growing from 7.9 per cent in 2014 to 13.7 per cent in 2016.

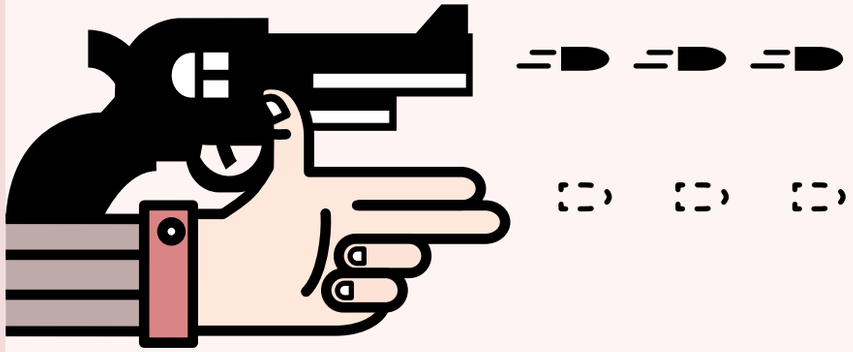
In 2016, cyber criminals mostly committed online cheating cases (83 per cent), followed by CMCA cases such as unauthorised access to computer material (15 per cent) and cyber extortion (2 per cent) respectively[4]. The top three categories of online cheating cases were namely e-commerce, Internet love scam and credit-for-sex.

Notably, CMCA cases more than doubled year-on-year, from 280 in 2015 to 691 in 2016. The top five CMCA cases in 2016, in no particular order, were related to ransomware, hacking, compromise of online accounts (such as Facebook), SingPass and Internet banking accounts.

Cyber criminals will continue to be a significant threat actor group as they adopt more sophisticated social engineering techniques to lure their victims. The anonymity provided by the Internet and the borderless nature of cyberspace allow cyber criminals to operate freely and anonymously. Given this challenge, the Government, law enforcement agencies and the international community will have to work even more closely together to fight cybercrimes.

[4] The term 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 of offences refers to offences under the Computer Misuse and Cybersecurity Act (CMCA) and the second category of offences refer to traditional crimes performed online such as online cheating, and cyber extortion. Ministry of Home Affairs, National Cybercrime Action Plan. (2016, July 20). Retrieved from https://www.police.gov.sg/news-and-publications/media-releases/20160720_others_-launch_of_the_national_cybercrime_action_plan_others





**CASE STUDY**

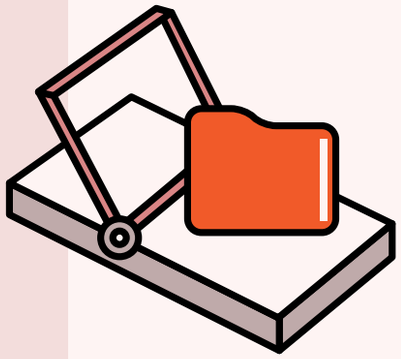
**DDoS Copycats**

In June 2016, a Singapore institution received a cyber threat which appeared to be from a cyber criminal group known for its DDoS attacks. They demanded the payment of a ransom, failing which they would launch a DDoS attack on the institution. The threat was sent in the form of a ransom e-mail to the institution, demanding for Bitcoins to be paid. A "demo attack" – akin to a warning shot by the attackers – was launched before the due date, but the DDoS threat was eventually not carried out.

CSA assessed that the threat was likely from a copycat group. The actual cyber criminal group is infamous for being able to launch DDoS attacks of more than 1 Tbps, and had previously issued similar ransom threats to several companies in Switzerland.

Identifying attackers and attributing attacks to them becomes even more challenging as actors within the community mimic one another to hide their tracks.

# INSIDER THREATS



**FROM CSA'S SURVEY CONDUCTED IN AUGUST 2016, MANY SINGAPOREANS WERE FOUND TO BE UNAWARE OF PROPER CYBERSECURITY PRACTICES**

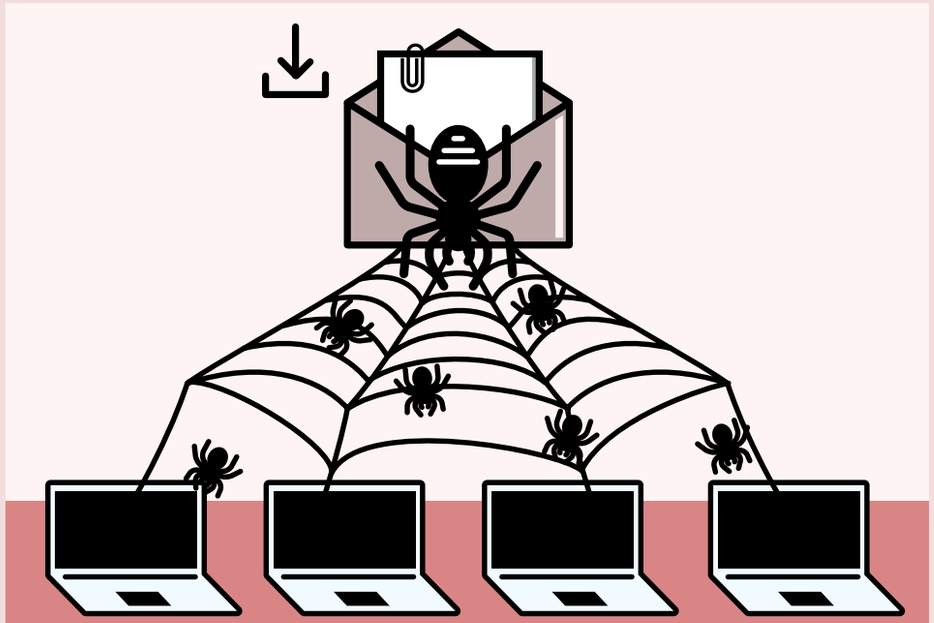
Insider threats pose a significant threat to organisations. Insiders – unintentionally or intentionally malicious – can weaken the best cyber defences. From IBM's 2016 Cyber Security Intelligence Index, insiders were found to be responsible for 60 per cent of cyber-attacks[5]. Insiders are a potent source of threat and a significant concern as they can unintentionally or intentionally leak data or compromise systems, and it takes more than technology to prevent insider threats. Processes for instance, need to be in place to ensure access to the organisation's data, especially sensitive ones, is strictly controlled.

Many Singaporeans were found to be unaware of proper cybersecurity practices based on a Public Awareness Survey conducted by CSA[6]. Consequently, this may make them potential "insider threats". They may inadvertently cause their office network to be compromised when they use an infected thumb drive that opens a "backdoor" for the attacker to enter the system. Using weak passwords that can be easily guessed, like "ABC123" or "password", would allow the attacker to enter otherwise confidential areas of the organisation's network.

There are also malicious insiders who could abuse their existing access to sensitive data and intellectual property for unlawful purposes. Malicious insiders could be disgruntled former employees who leave deliberate backdoors to exfiltrate data after they leave the organisation. They are a particularly dangerous group of threat actors because they know the network well and can find ways to disrupt or degrade critical services without raising suspicion.

[5] "Reviewing a year of Serious data breaches, major attacks, and new vulnerabilities," IBM X-Force Research 2016 Cyber Security Intelligence Index, p.11.

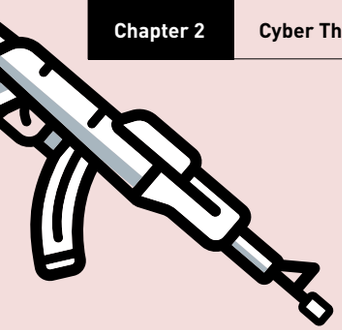
[6] Tiffany Fumiko Tay, "6 in 10 connect to unprotected Wi-Fi networks: Cyber Security Agency, The Straits Times, 16 February, 2017, http://www.straitstimes.com/singapore/6-in-10-connect-to-unprotected-wi-fi-networks-cyber-security-agency

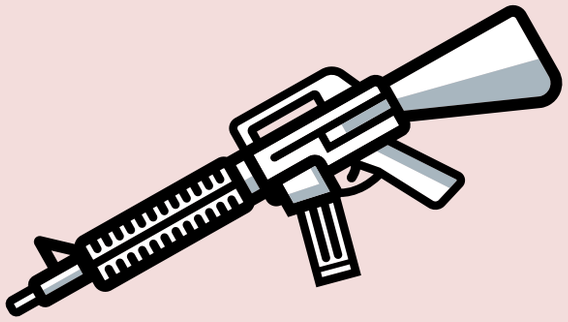


**CASE STUDY**

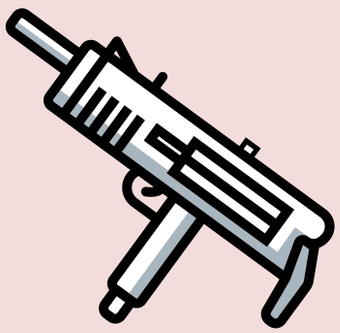
**Ransomware downloaded via personal e-mail infects office network**

In March 2016, an employee from the Healthcare sector used her workplace computer to access her personal e-mail account. She opened what appeared to be a Microsoft Office document but was in fact a malicious file, that downloaded a ransomware into the workplace computer. As the computer was connected to the rest of the organisation, the infection quickly spread to other machines on the network. The infection forced the organisation to reformat all the affected computers and restore data from backups. This incident highlights the need to heighten cyber awareness among employees, and always be ready to kick-in business continuity plans.





# COMMON CYBER THREATS IN SINGAPORE



NCSC analyses internal and other data sources, which include open source data, to provide actionable insights on four common threats and attacks in Singapore's cyberspace[7]. The four cyber threats in focus are ransomware, website defacement, phishing websites/URLs, C&C servers and DDoS. By understanding the means and motivation behind these attacks on Singaporeans and Singapore, one can try to take measures to prevent, detect and/or mitigate such threats.

[7] "Singapore cyberspace" can refer to websites ending with the .SG domain or mention Singapore in its URL, IP addresses used in Singapore or Internet Service Providers (ISP) that are located in Singapore.



## RANSOMWARE

**Definition:**

A type of malware that encrypts files on a victim's device, rendering them unusable until a ransom is paid, usually in the form of Bitcoin. It is spread through e-mail or malicious advertisements that appear when users access unsafe websites.

**Motivation:**

Financial gains and/or business disruptions.

**Target(s):**
Usually opportunistic, involving any individuals and companies of all sizes.

In 2016, there were 19 ransomware cases reported to SingCERT, up from the two cases reported in 2015. Cerber, CryptoLocker and Locky were among the types of ransomware reported. The actual number of victims may be more as ransomware cases tend to go unreported. According to Trend Micro, an international cybersecurity company, it detected about 550 ransomware-related threats in Singapore each day[8].

Singapore is especially vulnerable due to its high Internet penetration rate.[9] Individuals and SMEs accounted for most of the ransomware cases reported to CSA. Companies may be reluctant to admit being affected, as this may affect the reputation of their business.

Globally, hospitals and universities were also hit by ransomware attacks in 2016. Payments are usually made using Bitcoin, a type of online currency preferred by cyber criminals given it is harder to trace it back to them. Unfortunately, there is no guarantee that the hacker will decrypt the files as promised once they receive the payment.

## "NO ONE IS SPARED FROM RANSOMWARE"

[8] Shukla, A. (2016, July 13). Singapore receives 550 cyber threats each day. Retrieved from http://www.computerworld.com.sg/resource/security/singapore-receives-550-cyber-threats-each-day/

[9] Singapore ranks 4th in Asia in terms of Internet penetration rate (81.3 per cent), after South Korea (92.1 per cent), Japan (91.0 per cent), and Taiwan (83.8 per cent) respectively. Source: www.internetworldstats.com/stats3.htm

Singapore has joined the "No More Ransom" initiative by Europol's European Cybercrime Centre (EC3) to fight cybercrime in both the public and private sectors. The initiative aims to assist victims of ransomware to decrypt their encrypted data by offering the decryption tools made available free of charge on the portal and to teach users how to protect themselves. The portal is now available in 14 languages and contains 40 free decryption tools. More about EC3's initiative can be found here:

www.nomoreransom.org.

Following a noticeable rise in ransomware infections in Singapore and overseas, SingCERT released an advisory on ransomware in May 2016. Preventive measures against ransomware include:

- Follow Internet-browsing best practices, such as not clicking on suspect links as that may download ransomware;
- Updating software with the recommended patches to reduce the likelihood of known vulnerabilities being exploited;
- Performing regular backups to recover files that have been encrypted;
- Using available decryption tools to restore files that the attacker has "locked up".

# WEBSITE DEFACEMENT

## "1 IN 10 WEBSITES FOUND HOSTED ON OUTDATED OPERATING SYSTEMS"

**Definition:**

Much like virtual graffiti, hackers change the visual appearance of a single webpage or an entire website by gaining unauthorised access to the web hosting server. Defaced websites may also contain malicious code to infect visitors to the affected site.

**Motivation:**

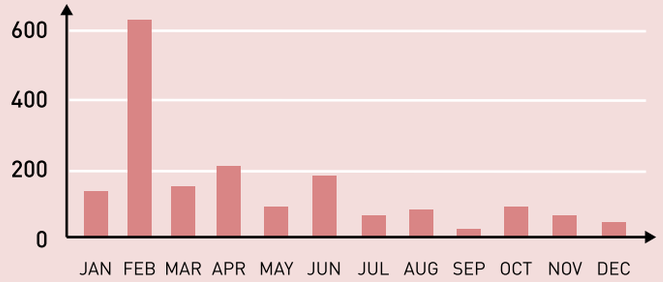
Promote political or religious agendas through "hacktivism", achieve online fame in hacker communities, and/or distract victims from the "real" cyber-attack such as a data breach.

**Target(s):**

Usually opportunistic, involving websites and/or web servers with known vulnerabilities.

**Website owners should keep their applications (including plug-ins) and operating systems regularly updated to prevent hackers from exploiting known vulnerabilities on outdated systems. Companies that rely on third-party hosting providers for their Web hosting needs should find out from their providers about the measures that are in place to address potential vulnerabilities.**

Number of defaced Singapore websites



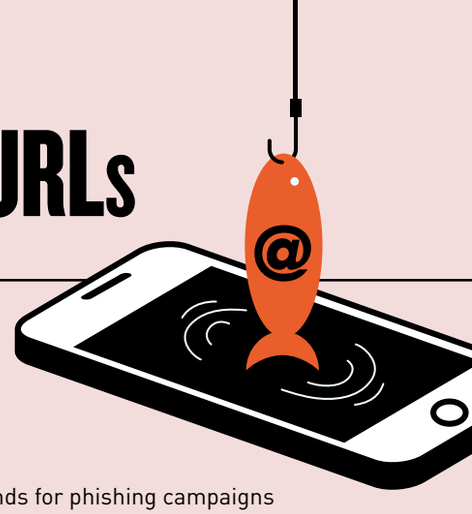

In Singapore, 1,750 website defacements were reported in 2016. The majority of the affected websites belonged to SMEs from a range of businesses, including interior design, logistics, manufacturing and construction.

One in 10 defaced websites were hosted on outdated operating systems such as Windows Server 2003 for which Microsoft ended its support in July 2015. Such operating systems may no longer have security patches for new vulnerabilities and hence are easier for hackers to exploit.

According to Sucuri[10], an American website security company, WordPress was the most targeted content management system (CMS) in 2016 globally. Popular CMS such as Joomla and WordPress, which most websites run on, can be infiltrated by hackers due to vulnerabilities, and improper deployment, configuration or maintenance by their webmasters.

[10] Sucuri is a security company which focused on detecting and remediating compromised websites.

# PHISHING WEBSITE / URLs




**Definition:**

Websites that are compromised or created by hackers to trick Internet users into believing they are accessing a legitimate, trusted website.

**Motivation:**

Obtain personal information, which can be used for future cyber-attacks, and/or financial gain.

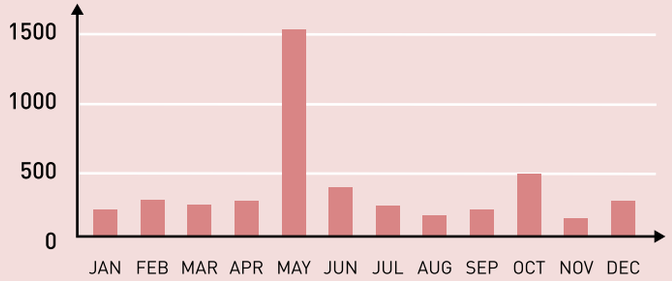
**Target(s):**

Usually opportunistic, involving potentially anybody and everybody.

**Users should always seek to verify the URL and e-mail address of senders, and look out for warning signs such as poor spelling or grammar. When in doubt, users should always verify the website's address before submitting any sensitive information online.**

Most targeted brands for phishing campaigns


Number of phishing URLs linked to Singapore




In 2016, 2,512 phishing URLs with a Singapore-link were found. Banking and financial services websites appeared to be the most commonly spoofed websites in Singapore. They represented more than 30 per cent of the phishing websites found. File-hosting service providers such as Dropbox and Google Drive, and technology companies such as Apple and Google are commonly spoofed by hackers.

Government organisations such as Ministry of Manpower (MOM) and Immigration & Checkpoints Authority (ICA) were also spoofed in 2016.

Online payment service provider PayPal was the most targeted brand, likely due its widespread use among online merchants and its customers[11]. File-hosting and Cloud storage service providers are becoming popular targets as well.

[11] PayPal holds 77 per cent of the market share in online payment industry. Source: https://www.datanyze.com/market-share/payments/

# COMMAND & CONTROL (C&C) SERVERS AND DISTRIBUTED DENIAL OF SERVICE (DDOS)

**Definition:**

A C&C server is a machine operated by hackers to communicate with devices that have been infected with malware. Instructions are communicated to the group of infected devices, collectively known as a botnet, to perform malicious activities such as DDoS attacks. A DDoS attack occurs when a system is bombarded with large volumes of data or specially-crafted malicious traffic sent from a botnet, affecting the system's ability to respond to legitimate users in a timely manner.

**Motivation:**

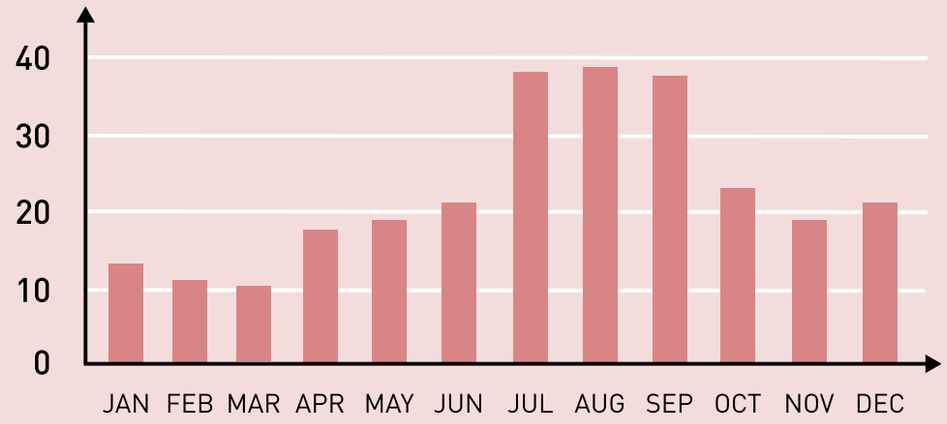
Conduct malicious activities such as data theft, e-mail spam campaigns and DDoS attacks. DDoS attacks create disruptions to victim's business operations, and/or distract victim from the "real" cyber-attack such as a data breach.

**Target(s):**

Any organisation, although those in the financial and gaming industries are commonly targeted.

**"SSDP, DNS AND NTP ACCOUNT FOR 70 PER CENT OF VULNERABLE SERVICES IN SINGAPORE THAT CAN BE USED IN A DDOS ATTACK"**

Number of Unique C&C Servers observed per month in Singapore




More than 60 C&C servers were observed within Singapore's cyberspace in 2016. The number of C&C servers was observed to be growing gradually in the first eight months of 2016, peaking in August, before decreasing towards the end of the year. Such servers often serve as the launch pad for cyber-attacks, including DDoS attacks. Whenever a new C&C server is detected, SingCERT will inform the respective Web-hosting providers to rectify the issue.

In 2016, DDoS attacks globally crossed the peak attack volume of 1 Tbps (DDoS attacks commonly fall in the 10 – 50 Gigabit per second range). Attacks of this scale were enabled through new malware (e.g. Mirai) that exploited vulnerabilities in unsecured IoT devices, such as webcams, routers and printers. The malware essentially would hijack these devices, causing them to generate malicious traffic that can be directed at specific systems.

2016 also saw the growth of DDoS extortion threats. Organisations receive e-mails from hackers threatening to launch a DDoS attack against them unless payment is made, usually via Bitcoin. A number of organisations in Singapore have received such threats.

Misconfigured services on servers continued to be seen in Singapore's cyberspace throughout 2016. Simple Service Discovery Protocol (SSDP), DNS and Network Time Protocol (NTP) are some of the services that, if not configured properly, can be used to facilitate DDoS attacks. Remediation for these vulnerabilities can be as simple as unchecking an option in the server settings.

**SingCERT published an advisory in Oct 2016 to inform business and individuals of the need to enhance the security of IoT devices. This could reduce the likelihood of that these devices are leveraged to conduct widespread DDoS attacks. Some measures include:**

- **Ensuring that remote access capabilities were disabled; and**
- **Changing device usernames and passwords from the default.**

CHAPTER 3

# KEEPING OUR CYBERSPACE SAFE AND TRUSTWORTHY TOGETHER



While digital connectivity exposes everyone to cyber threats, it also continues to open up opportunities for all. Through cyberspace, we keep in touch with one another, do our work, and run enterprises. Given the heavy reliance on cyberspace, it is therefore important that our cyberspace is kept safe and trustworthy, for everyone to continue benefitting from it.

The ways to doing so include:

**a)** raising cyber awareness and capabilities among individuals and businesses,

**b)** developing cybersecurity professionals in Singapore,

**c)** facilitating exchanges with regional and international partners, and

**d)** investing in Research and Development (R&D) for a secure Smart Nation.

# RAISING CYBER AWARENESS AMONG INDIVIDUALS AND BUSINESSES

CSA conducted a Public Awareness Survey in August 2016 with 2,000 respondents on their cybersecurity awareness and cyber hygiene. While seven in 10 respondents agreed that everyone has a role to play in cybersecurity, many of them were also found to be not taking safety measures when going online. For example, one in three respondents do not manage their passwords carefully. These findings, among others, reveal that there is room for improvement when it comes to individual cyber hygiene practices.

To educate and reach out to the public on cybersecurity, CSA manages the GoSafeOnline and SingCERT websites and social media platforms that provide cybersecurity news and resources to individuals and businesses. Members of the Cyber Security Awareness Alliance, which CSA co-chairs, have also been giving media interviews, talks to schools, the public, and businesses to raise cybersecurity awareness.

Advisories issued by SingCERT in 2016 covered topics like ransomware, DDoS attacks, and compromised remote servers, which were timely given the increasing number of incidents stemming from ransomware infections and exploitations of weak system configurations.

To bring the message to an even wider audience, two episodes of CrimeWatch, a long-running television programme, were produced on cyber-related topics. These were aired on free-to-air television channels in Singapore. CSA worked with the SPF and National Crime Prevention Council (NCPC) to produce these episodes covering cybercrimes involving banking malware, ransomware, and unauthorised access to data in computer networks and systems.

Together with the Personal Data Protection Commission (PDPC), CSA produced a series of activity books to educate primary school students on cyber safety. Two issues were produced in 2016 and distributed to all Primary 5 students in Singapore with copies made available online.

To expand the outreach to SMEs, CSA worked with the Singapore Business Federation (SBF) and the National Security Coordination Secretariat (NSCS) on the National Security Conference in November 2016 to raise cybersecurity awareness among businesses. The conference attracted more than 500 attendees from SMEs.

To help SMEs build their digital capabilities to seize opportunities for growth in the digital economy, CSA is working with IMDA on the cybersecurity aspects of the SMEs Go Digital programme. For example, the new SME Digital Tech Hub (slated to be opened in the third quarter of 2017) will provide specialist technology advice to assist SMEs on their cybersecurity needs.


**Cyber Safety Activity Book**

# DEVELOPING SINGAPORE'S CYBERSECURITY PROFESSIONALS

Close to 40 students and young professional participated in the 'The Future For You: Be a Cyber Security Champion' engagement session organised by CSA on 23 Feb 2016

While Singapore works towards increasing cyber-savviness among her people, it requires competent cybersecurity professionals, capable of protecting both the infrastructure and the individuals who use the infrastructure. Singapore's efforts to groom its pool of cybersecurity professionals include:

**Enhancing and augmenting the professional pipeline**

The Cyber Security Associates and Technologists (CSAT) programme, a joint initiative by CSA and IMDA, aims to boost the pipeline of cybersecurity professionals. CSAT trains and upskills new and existing ICT and Engineering professionals for cybersecurity roles.

**Deepening the technical depth of professionals.**

CSA has been engaging the Institutes of Higher Learning (IHL) to shape cybersecurity into their curriculum. CSA will promote industry-IHL collaborations for more structured internships and leading edge cybersecurity training facilities.

Young participants at the WhiteHacks@SG cybersecurity workshop and competition held from 12-13 Mar 2016. The event was organised by SMU Whitehat Society in partnership with ThinkSecure and CSA.

A way to build a common identity and increase the recognition of the cybersecurity profession is to foster strong Communities of Practice (COPs). Professional bodies are instrumental to driving the development of COPs to tackle cyber threats and career pathways for professionals. Such bodies are also integral to enhancing talent retention in the profession. CSA has engaged four key professional bodies – Association of Information Security Professionals; Singapore Computer Society; International Information System Security Certification Consortium also known as (ISC)[2]; and Information System Audit and Control Association (ISACA) – to build stronger communities. CSA will also work with IMDA and Workforce Singapore (WSG) on delivering better training and career opportunities for cybersecurity professionals.

Complementing these efforts is the development of Singapore's cybersecurity industry to spur the growth of high value jobs in Singapore that will in turn sustain efforts at developing the nation's manpower. The availability of sophisticated and high value jobs, provided by a vibrant cybersecurity industry, provides for the professional growth and career progression of professionals, all of which are critical to countering cyber threats effectively.

# FACILITATING EXCHANGES WITH REGIONAL AND INTERNATIONAL PARTNERS

International collaboration is pivotal to global cybersecurity. Singapore has been actively involved in various international platforms on cybersecurity, from multilateral discussions on international cyber norms to bilateral cooperation.

In 2016, CSA signed Memoranda of Understanding (MoUs) with the Netherlands and the USA. The MoUs cover cooperation in areas such as operational exchange of cyber threat and attack-related information; sharing of best practices on national cybersecurity approaches, strategies and procedures and CII protection; certification of cybersecurity products and services; and training.

Singapore has also initiated discussions on cyber norms with its ASEAN partners, including at the ASEAN Ministerial Conference on Cybersecurity (AMCC). The AMCC was organised during the Singapore International Cyber Week (SICW) in October 2016 for ASEAN Ministers and senior officials from the telecommunications and other relevant sectors to discuss regional cybersecurity issues. It also saw ASEAN Member States agreeing on the value of developing a set of practical cybersecurity norms of behaviour in ASEAN, and calling for closer cooperation and stronger coordination on regional capacity-building initiatives.

Such new initiatives will add to existing efforts which have been ongoing for many years. These include a capacity-building workshop jointly organised by Singapore and the USA for ASEAN countries in August 2016, and the annual ASEAN CERT Incident Drill (referred to as "ACID" by its participants), which has been testing the incident-handling procedures of ASEAN CERTS over the last 10 years.


Cyber Norms discussion at the International Cyber Leaders' Symposium held at the inaugural Singapore International Cyber Week on 10 Oct 2016


Ministers and Senior Officials from ASEAN Member States at the inaugural ASEAN Ministerial Conference on Cybersecurity held on 11 Oct 2016

## CYBERGREEN

Initiated by the Japan Computer Emergency Response Team in 2014, the CyberGreen project aims to provide a cyber-health check of countries by highlighting the levels of infections seen in each country. In 2016, Singapore became one of the founding sponsors of the global initiative. CSA will work with IMDA and telcos to clean up the infections in cyberspace to improve Singapore's overall cyber hygiene.

# CYBERSECURITY FOR A SMART NATION


Official opening of the CREST examination facility at the Singapore Institute of Technology on 28 July 2016

CSA strongly advocates the security-by-design approach, which means designing and building in security from the outset, and throughout every phase of the software and hardware development lifecycle. This approach involves a rigorous process that includes (i) threat-risk assessments, (ii) optimising system design by balancing the trade-offs among security, usability and cost, and (iii) penetration testing.

This approach will also underpin the design and development of Singapore's Smart Nation. While a Smart Nation creates new opportunities for work and leisure, it inadvertently expands the attack surface as well with the greater connectivity between devices, and among us. The cyber-attack in the United States in October 2016, carried out through compromised IoT devices, exemplifies such a threat.

In April 2016, the CREST Singapore Chapter was established by CSA in collaboration with the Association of Information Security Professionals (AISP), IMDA, GovTech, the Association of Banks in Singapore and the Monetary Authority of Singapore. This is also the first CREST Chapter in Asia. CSA has directed that from June 2017, all penetration testing professionals and service providers who provide penetration testing services for CII need to be certified and accredited through CREST or equivalent certifying bodies.

R&D work in cybersecurity will also be another critical front to push in the Smart Nation journey. Together with the National Research Foundation (NRF) and the other stakeholder agencies, CSA is driving Singapore's cybersecurity R&D effort through the S$190m National Cybersecurity R&D programme, which aims at improving the trustworthiness of cyber infrastructure, raising the barrier for attackers, and developing threat-based solutions.



# LOOKING AHEAD

The Singapore Cyber Landscape 2016 has given an initial glimpse of the nation's cyber health. We believe it is but the tip of the iceberg. We hope it will spur greater involvement of all stakeholders – Government agencies, Singapore's cyber industry, professionals and students, academia and researchers, and providers of essential services – to come up with new ways to better defend ourselves against ever-evolving cyber threats.

Cybersecurity is a team effort. Everyone has a part to play, and everyone has to play their part. At the national level, CSA will continue to spearhead initiatives and engage stakeholders to enhance Singapore's cybersecurity posture. At the organisational and individual levels, efforts must be made too to raise awareness, capabilities and resilience to counter the cyber threats that Singapore will continue to face. If we work together as a team, we can make Singapore a safe and trustworthy Smart Nation.

**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

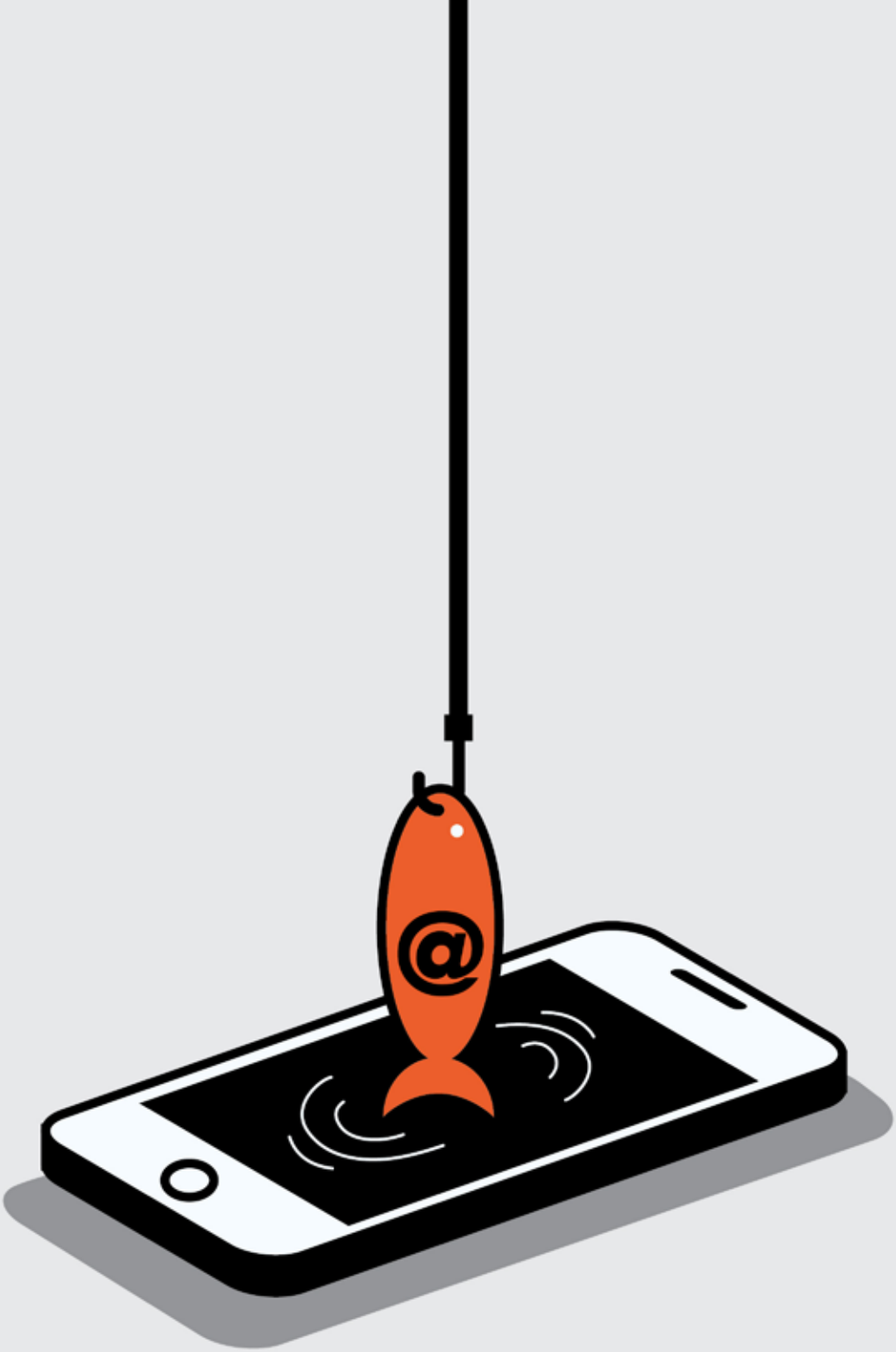
General enquiries/feedback:
gosafeonline@csa.gov.sg

**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