SINGAPORE CYBER LANDSCAPE 2019

Singapore Cyber Landscape 2019

By Cyber Security Agency of Singapore

With contributions by the Centre of Excellence for National Security, S. Rajaratnam School of International Studies, Defence Cyber Organisation, DSO National Laboratories, Government Technology Agency of Singapore, Hwa Chong Institution, Nexus, and Singapore Police Force.

Designed by APT 811 Design & Innovation Agency

ISBN: 978-981-14-5776-0

Contents

Foreword

Since its emergence in late-2019, COVID-19 has quite literally wreaked havoc all over the world. Borders have been closed, air travel has ground to a halt, while economies, societies and many aspects of human activity have come to a standstill. However, even as nations fight to stem the effects of this pandemic, threat actors have brazenly exploited public fear and uncertainty over the coronavirus to carry out malicious cyber activities, which included phishing campaigns and ransomware attacks on hospitals and medical facilities.

As many organisations adopt “work from home” arrangements, threat actors are likely to capitalise on the new opportunities to gain unauthorised access to users’ data or the organisations’ networks. Aside from these new threats which have emerged from the COVID-19 pandemic, cyber-attacks have already become more prevalent in 2019, with an upsurge of malicious cyber activities locally. Compared to 2018, local observations of website defacements, phishing, ransomware, and Command and Control (C&C) servers and botnet drones all rose in 2019. Several serious cyber incidents also occurred in various sectors, examples of which are detailed in this publication.

The Cyber Security Agency of Singapore (CSA) responded robustly to the increase in malicious cyber threats. This includes taking a proactive role in helping organisations deal with harmful phishing attempts, through analysing malicious e-mails, and subsequently blocking similar e-mails to avert a recurrence of such scams. CSA has also responded swiftly and decisively to take down C&C servers that triggered Distributed Denial-of-Service (DDoS) attacks, and prevented further damage to organisations. These are among the measures undertaken by CSA to make cyberspace safer for businesses and individuals in Singapore.

CSA also continued to raise Singapore’s cybersecurity standards in 2019. For example, we launched Singapore’s Operational Technology (OT) Cybersecurity Masterplan, which serves as a strategic blueprint to guide the development of capabilities to secure Singapore’s OT environment. We also held the third run of Exercise Cyber Star, where participants from public and private sectors tackled complex cyber scenarios to hone their incident response plans. In our continuing efforts to develop a vibrant cybersecurity ecosystem, CSA introduced the “SG Cyber Women” initiative, to ensure a pipeline of talent and encourage more women to join Singapore’s cybersecurity workforce.

On the international front, CSA made strides in facilitating international cooperation in cyber. The ASEAN-Singapore Cybersecurity Centre of Excellence will enhance capacity building efforts of greater scope and depth within the region. CSA also represented Singapore in actively contributing to discussions towards a rules-based international order in cyberspace, through key platforms such as the Group of Governmental Experts and Open-Ended Working Group at the United Nations.

These are some of CSA’s work that we have detailed in this fourth edition of the Singapore Cyber Landscape, which I hope you will find useful. Threats in cyberspace are ever-evolving, and CSA has strived to present a comprehensive account of the key issues and incidents of 2019, alongside advice and insights into how organisations and individuals can better improve their cybersecurity. Some have mentioned that cybersecurity is a team sport, and this saying is now more true than ever. Only by standing together can we overcome the challenges of both the physical and virtual worlds.
#SGUNITED

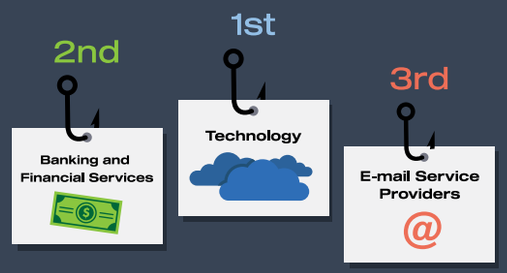
David Koh
Commissioner of Cybersecurity
and Chief Executive
Cyber Security Agency of Singapore

OVERVIEW OF CYBER THREATS IN 2019

PHISHING

47,500

phishing URLs[1] with a Singapore-link were detected.



COMMONLY SPOOFED GOVERNMENT ORGANISATIONS IN SINGAPORE:

IMMIGRATION & CHECKPOINTS AUTHORITY (ICA)

MINISTRY OF MANPOWER (MOM)

SINGAPORE POLICE FORCE (SPF)

70%

of incidents reported to SingCERT by Small and Medium Enterprises (SMEs) and members of the public occurred through phishing attacks.

WEBSITE DEFACEMENT

873

Singapore-linked website defacements were detected.

RANSOMWARE

35 cases of ransomware were reported to SingCERT.

COMMAND AND CONTROL (C&C) SERVERS AND BOTNET DRONES

530 unique C&C servers were observed in Singapore.

2,300

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

[1] URLs — Uniform Resource Locators; colloquially termed web addresses.

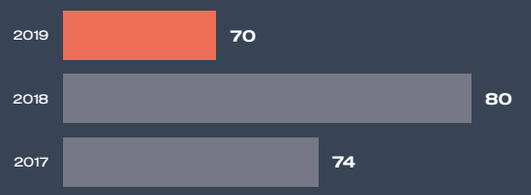
CYBERCRIME IN SINGAPORE

Cybercrime cases accounted for

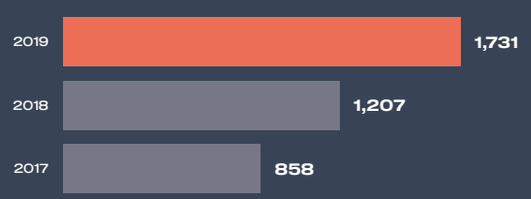
26.8%

of overall crime in 2019.

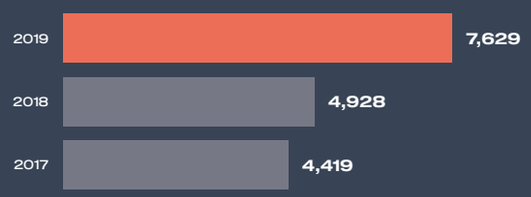
CYBER EXTORTION



COMPUTER MISUSE ACT



ONLINE CHEATING



[2] Figures provided by Singapore Police Force (SPF) as of 10 June 2020.

Featured Topic

Singapore remains a safe city, but scams remain a concern

Cybercrime continues to be on the rise in Singapore, with 9,430 cases reported in 2019 — this was a 51.7 per cent increase from the 6,215 cases reported in 2018, and it accounted for more than one-quarter of all crime in Singapore last year.[2] Online cheating remains a major concern as cybercriminals continue to leverage the anonymity afforded by the Internet to target unsuspecting victims.

E-commerce scam remains the top scam type in Singapore and recorded a 30 per cent increase to 2,809 cases from 2,161 cases in 2018. The total amount cheated in e-commerce scams also increased to S$2.3 million, from S$1.9 million in 2018. Unsuspecting victims continue to be enticed by online deals, such as electronic gadgets and event tickets, which are often too good to be true.

Fighting crime is a community effort. Even while the Police continues to educate the public on crime prevention measures and work with relevant stakeholders to disrupt scam operations, members of the public must also play their part by taking active steps to safeguard themselves online. They should use trusted payment services provided by the e-commerce platforms to mitigate the risk of falling prey to e-commerce scams.

Chapter 1

Spotlight on Cyber Threats

In 2019, the frequency and sophistication of various cyber threats such as website defacements, phishing incidents, and malware activities increased in Singapore. Spotlight on Cyber Threats covers CSA's observations in 2019 on relevant threats in Singapore's cyber landscape, as well as trends, insights and motivations of threat actors.

> **"Cybersecurity is not a static, technical arena; it is a dynamic, contested space. It is constantly evolving, as skilled, cunning malicious actors are always trying to find new ways to get past our defences."**
>
> **Mr S Iswaran**
> Minister for Communications and Information and Minister-in-Charge of Cybersecurity

Advanced Persistent Threats

Mobile Espionage

While the *Pegasus* spyware made headlines in 2019 for enabling its users to read and monitor data on hacked mobile phones, APT groups have also developed and deployed mobile malware to target both individuals and organisations. In the wake of protests in various countries throughout 2019, several APT groups were noted to be hacking into and conducting surveillance on mobile devices belonging to individuals from various countries. These operations involved both iOS and Android malware designed to access and read text messages, contact lists and call logs. They were also found to be monitoring targets through recording functions such as cameras and microphones in the compromised devices. Separately, *Golfspy*, an Android malware linked to a state-sponsored APT group, was used to steal images and military documents from infected mobile devices located mainly in the Middle East. *Golfspy*'s malicious codes were embedded into legitimate mobile applications, which were then hosted on a website and promoted on social media to propagate the spread of *Golfspy*.

False Flag Operations

Cybersecurity experts have observed how APT groups are covering their tracks to avoid attribution by carrying out "false flag" operations — that is, masquerading as other threat actor groups by deliberately adopting their Tactics, Techniques and Procedures (TTPs). In late-2019, an APT group allegedly attacked and stole information from organisations from the same region, by using malware and hacking tools stolen from another APT group based in the Middle East. This might have led victims to believe that they had been targeted by the Middle East-linked APT group.

Globally, several major cybersecurity incidents were attributed to Advanced Persistent Threat (APT) groups observed to be targeting sectors including government, banking and finance, healthcare, infocomm, and media.[3] For example, APT groups have allegedly masterminded high-profile incidents involving financial institutions and cryptocurrency exchanges.[4,5] A number of covert, malicious activities from APT groups stood out for their sophistication, with notable trends as follows:

Hacking the Internet Core

APT groups have exploited vulnerabilities in the Internet's core infrastructure to access sensitive networks and systems. In particular, an APT group was observed to have compromised and changed the Domain Name System (DNS) records of targeted organisations, in order to intercept and re-direct their Internet traffic to malicious servers. These servers then inspected the traffic before routing it to the intended destinations. Victims in this campaign included some 40 government and national security organisations, as well as technology firms, from 13 countries.

Compromising Information Technology (IT) Service Providers to Steal from Victims

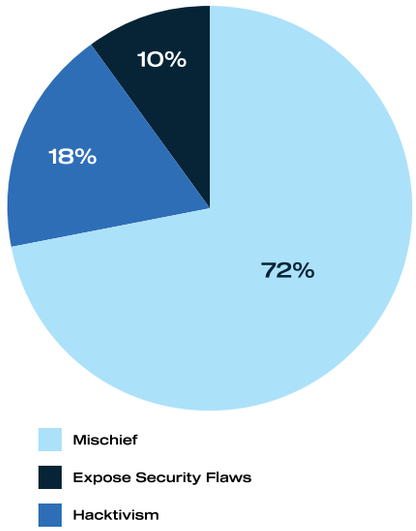
APT groups generally undertake cyber operations to support the intelligence and espionage objectives of their respective state sponsors, which could include economic, diplomatic and technological goals. The popularity of cloud services has inadvertently turned Information Technology (IT) Service Providers, such as Managed Service Providers (MSPs) and Cloud Service Providers (CSPs), into targets for threat actors looking to steal classified information. An APT group was allegedly behind a spate of attacks on MSPs and CSPs to gain access into the networks of their client organisations, which included major technology, telecommunications, and defence companies.

[3] FireEye Mandiant M-Trends 2020 Report, https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html.
[4] Nichols, Michelle. "North Korea took $2 billion in cyberattacks to fund weapons program: U.N. report," Reuters, 5 August 2019, https://www.reuters.com/article/us-northkorea-cyber-un-idUSKCN1UV1ZX.
[5] Salem, Eli. "Threat Actor TA505 Targets Financial Enterprises using LOLBins and a new Backdoor Malware," Cybereason Blog, 25 April 2019, https://www.cybereason.com/blog/threat-actor-ta505-targets-financial-enterprises-using-lolbins-and-a-new-backdoor-malware.

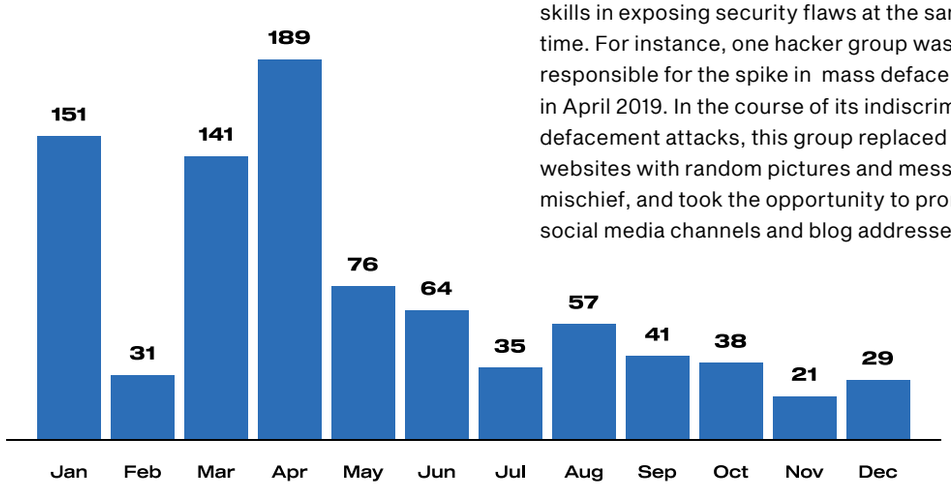
Website Defacements

873 websites in Singapore were defaced in 2019, a 44 per cent increase from 605 in 2018. This increase can be attributed in part to a surge in hacktivism fuelled by the global wave of protests in 2019. The majority of the defaced websites belonged to Small and Medium Enterprises (SMEs) from sectors such as education, finance, manufacturing and retail. No Singapore Government websites were defaced.

Breakdown of hackers' motivations for defacing websites in 2019, by percentage



Number of defaced Singapore websites reported in 2019



Indiscriminate and Opportunistic

Many defacements were opportunistic and self-aggrandising in nature. These threat actors exploit websites and web-hosting servers with vulnerabilities, and many aim to show off their skills in exposing security flaws at the same time. For instance, one hacker group was largely responsible for the spike in mass defacements in April 2019. In the course of its indiscriminate defacement attacks, this group replaced affected websites with random pictures and messages of mischief, and took the opportunity to promote its social media channels and blog addresses.

Known Motivations

18 per cent or 234 of the website defacements in 2019 were by hacker groups with known motivations and agendas.

- A single hacktivist mass-defaced 66 local websites in January 2019 alone, posting various messages on the affected websites.
- The spike in defacements in March 2019 was attributed to an Indonesia-based hacker group which defaced and inserted messages into 60 websites.

Defacements in the second half of 2019 coincided with major conflicts and political developments in the Middle East, as hacktivists from opposing camps conducted mass defacement campaigns to air their political views.

- A hacktivist claiming to support the Kurdish nationalist movement in the Middle East was responsible for most of the defacements observed in Singapore in August 2019. This coincided with the period when several mayors were asked to step down from political office in Turkey.
- In October 2019, mass defacements of websites were carried out not just in Singapore, but also in India and the United States of America (USA). The perpetrators made various references to the ongoing Syrian civil war.

WordPress — The Most Targeted Content Management System

Globally, WordPress was the most targeted content management system (CMS) by threat actors due to its popularity. As of end-2019, WordPress websites accounted for more than 35 per cent of all websites on the Internet.[6] There were similar observations in Singapore, where websites published on the WordPress platform made up the majority of defacements — 159 (about 20 per cent) — in 2019, as compared to 235 (about 40 per cent) in 2018. This decrease might be due to WordPress forcing auto-updates on older versions of the CMS in various stages beginning August 2019, which enhanced the security of the WordPress ecosystem and consequently, the Internet.[7]

[6] "Historical trends in the usage statistics of content management systems," W3Techs — World Wide Web Technology Surveys, 3 January 2020, https://www.w3techs.com/technologies/history_overview/content_management/all.

[7] Dunn, Ian. "Proposal: Auto-Update Old Versions to 4.7", Make WordPress Core, 8 August 2019, https://make.wordpress.org/core/2019/08/07/proposal-auto-update-old-versions-to-4-7.

Phishing URLs

Phishing continues to be one of the most popular — and effective — methods of social engineering, where threat actors impersonate trusted organisations and individuals to steal sensitive data from unsuspecting victims. To further their malicious objectives, threat actors are constantly refining their phishing tactics, which have grown in sophistication over the years.

In 2019, CSA detected 47,500 phishing URLs with a Singapore-link, an increase of about 200 per cent from 2018. This is in line with global observations, which saw 2019 record the highest level of phishing attacks since 2016.[8] More than 90 per cent of the spoofed companies were largely based in the USA, and included technology firms, organisations from the banking and financial sector, and e-mail service providers. These are popular and global companies whose branding resonate well not just with users in Singapore but also those worldwide. Hence, threat actors commonly spoofed them to improve their chances of success in phishing attacks. Separately, the most commonly spoofed websites of Government organisations in Singapore included the Immigration & Checkpoints Authority (ICA), Ministry of Manpower (MOM), and Singapore Police Force (SPF).[9]

Commonly Spoofed Organisations in 2019

Phishing-as-a-Service (PHaaS) — Fuelling Phishing Attacks

The rise of Phishing-as-a-Service (PHaaS) likely fuelled the increase in phishing attacks in 2019, with over 5,300 phishing kits detected for sale on the Dark Web.[10] PHaaS provides professional phishing templates spoofing a range of popular brands and well-known companies from various sectors, as well as web-hosting services.[11] The accessibility to these capabilities gives cybercriminals an easier start for their phishing campaigns in stealing online credentials and sensitive information, without the need for in-depth technical knowledge to develop their own phishing tools.

DigitalOcean and GoDaddy — Most Commonly Abused Web-Hosting Providers

DigitalOcean and GoDaddy were the most commonly abused web-hosting providers, having hosted more than one-third of total phishing URLs detected in 2019. The one-stop and hassle-free nature of setting up websites through these web-hosting providers serve as low barriers to entry for threat actors, making them popular choices for hosting malicious websites.

[8] "Phishing Attacks Reach Highest Level in Three Years," Anti-Phishing Working Group (APWG) Phishing Activity Trends Report 3rd Quarter 2019, 4 November 2019, https://docs.apwg.org/reports/apwg_trends_report_q3_2019.pdf.
[9] Services offered by these Government organisations typically involve personally identifiable information, such as NRIC numbers, passport information and credit card numbers, which could have been stolen and used for malicious purposes, such as identity theft.
[10] Sigurdardottir, Tinna Thuridur and Sigurdsson, Magni. "Evasive Phishing Driven by Phishing-as-a-Service," Cyren Security Blog, 1 July 2019, https://www.cyren.com/blog/articles/evasive-phishing-driven-by-phishing-as-a-service.
[11] Akamai 2019 State of the Internet / Security Phishing: Baiting the Hook Report, Akamai Technologies, Inc., 30 October 2019, https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-phishing-baiting-the-hook-report-2019.pdf.

Featured Topic

The Psychology Behind the Persistence of Phishing

Ms Teo Yi-Ling, Senior Fellow, Centre of Excellence for National Security, S. Rajaratnam School of International Studies

The Pervasiveness of Phishing

Phishing continues to pose a key risk to organisations of all sizes. A recent estimate saw 3.4 billion malicious e-mails being disseminated every day.[13] The sheer volume of scam e-mails is just one aspect of the threat: it is important to realise that when it concerns phishing, scammers are not focused on exploiting systemic or technological vulnerabilities — they are **exploiting vulnerabilities in human nature.**[14] This other aspect of the phishing threat is using the tactic of social engineering, where people are manipulated into carrying out certain behaviours. In the context of cybersecurity or information security, social engineering is about getting people to disclose sensitive information and be exposed to malware. Phishing is a key example of social engineering, as the scams involve impersonating legitimate organisations to attempt to get the recipients of phishing e-mails to comply with requests.

Despite the fact that scam awareness is high due to ongoing public education campaigns in Singapore (including how to spot the signs of phishing e-mails) and frequent reporting in the media, the phenomenon of phishing persists — people still fall prey to phishing scams. In trying to devise more effective countermeasures to phishing, it is necessary to understand the psychology underscoring this tactic, and the strategy of the scammer. The endgame of phishing is persuading the recipient to behave in a way desired by the scammer. There are two paths that lead to persuasion — one appeals to logic, and the other, to emotions.[15] Putting the factor of relative credulity of human beings to one side, as logic requires thinking objectively through action and consequence, it is highly unlikely that a scammer would use logic to persuade. However, it appears that in appealing to emotions to persuade, the stronger the emotional response (positive or negative) induced in the recipient, the greater the probability is for the recipient to not think clearly and carefully.[16] Scammers could prey on fear, greed, curiosity and outrage.

*Read more about **The Psychology Behind the Persistence of Phishing** on **Page 50***

Cybercriminals are quick to take advantage of strong consumer interest during the release of highly anticipated products. Between September and October 2019, there was a surge in phishing attempts spoofing Apple, which coincided with the company's release of new products. These phishing links made up more than 60 per cent of all phishing URLs with known targets in 2019, and were usually disguised within e-mails seeking bill payments for purported purchases of the new products, or e-mails requesting verification of Apple ID authentication data belonging to victims. Notably, this wave of Apple phishing scams appeared to largely target Yahoo! e-mail addresses, suggesting that cybercriminals were possibly utilising compromised e-mail accounts from Yahoo!'s data breach in 2013.[12]

[12] Irwin, Luke. "Catches of the month: Phishing scams for September 2019 — Yahoo Mail customers targeted by Apple scam," IT Governance Blog, 11 September 2019, https://itgovernance.co.uk/blog/catches-of-the-month-phishing-scams-for-september-2019.
[13] Valimail E-mail Fraud Landscape / Spring 2019, https://valimail.docsend.com/view/qndhuhn.
[14] Irwin, Luke, "The psychology behind phishing attacks", IT Governance Blog, 1 August 2019, https://www.itgovernance.co.uk/blog/the-psychology-behind-phishing-attacks.
[15] Rusch, Jonathan J, "The Social Engineering of Internet Fraud", 1999 (Retrieved 1 February 2020), http://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g_2.htm.
[16] Irwin, Luke, "The psychology behind phishing attacks", IT Governance Blog, 1 August 2019, https://www.itgovernance.co.uk/blog/the-psychology-behind-phishing-attacks.

Malware

In 2019, more ransomware cases were reported to CSA. While there was an increase in the number of Command and Control (C&C) servers observed in Singapore, there were fewer botnet drones detected as compared to 2018.

Ransomware

CSA received 35 reports of ransomware cases in 2019, an increase from 21 cases in 2018. Systems across various industries including gaming, travel and tourism, manufacturing, and logistics were affected.

Troldesh Campaign

Several countries were affected by a *Troldesh* (also known as *Shade*) campaign in February 2019, where sharp increases in infections with the ransomware were detected and reported by various cybersecurity firms.[17, 18] Delivered primarily by phishing e-mails and spread by spam containing malicious zip attachments, *Troldesh* uses a strong encryption algorithm to encrypt files. It also mines cryptocurrency on compromised systems, and generates traffic to websites to earn revenue from online advertising. Affected systems typically receive many identical ransom notes written in both Russian and English. A number of companies operating in Singapore were infected by the ransomware as well.

Ransomware will continue to be a menace. Cybersecurity firm FireEye noted how the successful monetisation of ransomware attacks have further contributed to an increase in overall ransomware cases.[19] Cybercriminals that traditionally used phishing to obtain personal and financial information have also turned to ransomware to generate more revenue. Besides demanding a ransom to unlock the system or data, some cybercriminals have also been known to expose or sell the data that they have obtained. Precautions against ransomware attacks include encrypting important or sensitive data, to minimise damage even if the data is accessed, as well as regularly backing up important files and storing them offline. In the event of a successful attack — and where decryptors are unavailable — data restoration can then be performed with the back-up after reformatting the system to remove the malware. Given the evolution of cybercriminal tactics in combining ransomware attacks with threats to leak the affected data unless victims pay up, companies also need to develop contingency plans to deal with such incidents.

Big-Game Hunting

Cybercriminals have been observed to be shifting from the indiscriminate targeting of victims to enterprise ransomware attacks, or "big-game hunting", where they target large organisations in hope of higher payouts. Multiple city and local governments in the USA, as well as manufacturers such as Norwegian aluminium company Norsk Hydro, were affected by ransomware strains such as *Ryuk*, *RobbinHood*, and *LockerGoga* in targeted attacks. In Singapore, a logistics company and an IT equipment supplier were infected with *Ryuk* in October and December 2019, respectively. Ransomware strains used in such attacks globally are stealthier and designed specifically to exploit, propagate and take down the networks of targeted organisations. These strains are unlike earlier strains that usually relied on e-mails or system vulnerabilities to spread, such as during the 2017 *WannaCry* and *NotPetya* malware outbreaks.

[17] Arntz, Pieter. "Spotlight on Troldesh ransomware, aka 'Shade'," Malwarebytes Labs, 5 March 2019, https://blog.malwarebytes.com/threat-analysis/2019/03/spotlight-troldesh-ransomware-aka-shade.

[18] Delos Santos, Ace. "Russian Spam Delivers SHADE Ransomware via Link Embedded in PDF," Trend Micro — Threat Encyclopaedia, 13 February 2019, https://www.trendmicro.com/vinfo/be/threat-encyclopedia/spam/689/russian-spam-delivers-shade-ransomware-via-link-embedded-in-pdf.

[19] FireEye Mandiant M-T'rends 2020 Report, https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html.

Featured Topic

Ransomware — An Evolving Threat

To counter global initiatives[20] aimed at mitigating the scourge of ransomware, and ensure their ransom demands are met, cybercriminals are leveraging the ability of new ransomware strains to exfiltrate data in addition to encrypting it, by forcing organisations to choose between paying the ransom and facing the consequences of having the stolen data released publicly. The exfiltration of data highlights how ransomware incidents should also be regarded as data breaches.

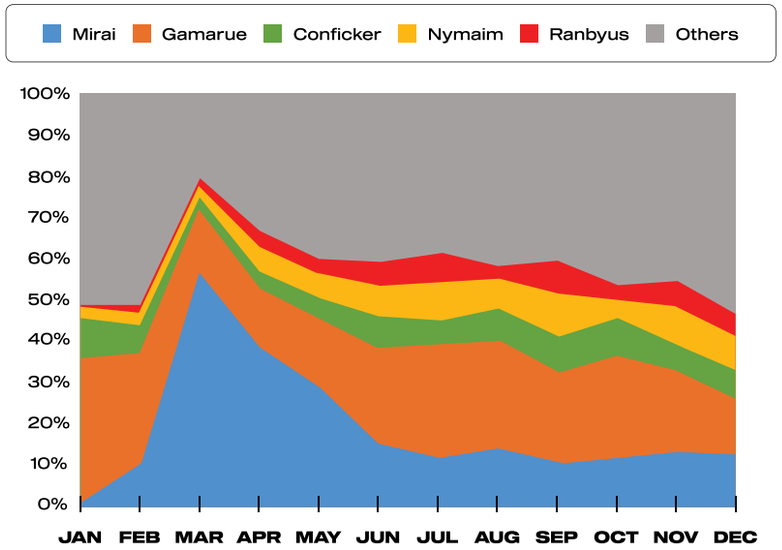
In late-2019, operators behind the *Maze* ransomware retaliated by publishing files allegedly stolen from their victims who refused to pay the ransom. Such tactics — combining extortion and doxxing — were subsequently adopted by other ransomware operators behind *Sodinokibi*, *BitPylock* and *Nemty*. This is not the first time similar tactics have been observed. Earlier in 2016, the *Ransoc* ransomware scanned systems for files containing illegal content, and then demanded ransom payments disguised as "penalty notices" after threatening their victims with fake legal proceedings, or having their personal data and illegal content leaked. Targeted data breaches, such as that in 2017 when a hacker compromised the network of media company HBO and threatened to release stolen files unless the US$6 million ransom was paid, can also easily lead to data being held hostage.

As the ransomware threat continues to evolve, robust cybersecurity practices remain the best defence. Systems and networks should be regularly patched, while individuals should not reuse credentials across accounts. They should also be wary of cyber threats posed by both phishing and malspam — or malicious spam — e-mails. After all, as the adage goes, prevention (of ransomware infections) is better than cure.

[20] The *No More Ransom* project, led by various law enforcement agencies and private cybersecurity firms, aims to help ransomware victims retrieve their encrypted data without having to pay the cybercriminals. According to Europol, as of July 2019, free decryption tools offered by the project have prevented cybercriminals from making at least US$108 million in ill-gotten gains. The National Cybersecurity Centre of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) in the USA has also developed a recovery guide "Data Integrity: Recovering from Ransomware and other Destructive Events" to help ransomware victims mitigate related issues.

C&C Servers and Botnet Drones

In 2019, CSA detected about 530 unique C&C servers in Singapore, a 73 per cent increase from 2018. On average, about 2,300 botnet drones with Singapore Internet Protocol (IP) addresses were observed daily, a 20 per cent decrease from average daily observations in 2018. Close to 370 malware variants were detected, with the top five malware observed — *Mirai*, *Gamarue*, *Conficker*, *Nymaim*, and *Ranbyus* — accounting for over half of all observed infections. These malware are not new, with *Ranbyus* and *Nymaim* first detected in 2011 and 2013, respectively.



On average, five common malware accounted for over half the daily infections of computing devices in 2019.

Mirai — *Internet of (insecure) Things*

Mirai infected more IP addresses in the first half of 2019 than it had the whole of 2018. In fact, while other malware variants observed decreased in 2019, *Mirai* variants continued to grow, increasing in tandem with the adoption of Internet of Things (IoT) devices in Singapore. Since its inception in 2016, *Mirai* has evolved to include more complex attack tools, which take advantage of the weak security that continues to exist in many IoT devices. New exploits in a *Mirai* variant active since January 2019 targeted vulnerabilities of enterprise IoT devices, in addition to generating novel and unusual combinations of log-in credentials for carrying out brute-force attacks.[21] These targeted devices included wireless presentation and display systems, routers, network storage devices and IP cameras, suggesting that threat actors were looking to leverage bandwidths in organisational networks to build bigger botnets for carrying out large-scale Distributed Denial-of-Service (DDoS) attacks.

To avoid takedowns and evade detection, threat actors behind another *Mirai* variant observed in July 2019 hid their C&C server in the Tor anonymity network.[22] This prevented the server from being blacklisted upon discovery of its malicious activities, as its network traffic was encrypted and allowed to blend into Tor's legitimate traffic streams. This tactic could potentially set a trend for other threat actors to follow, and subsequently present new cybersecurity challenges for users.

[21] Nigam, Ruchna. "New Mirai Variant Targets Enterprise Wireless Presentation & Display Systems," Palo Alto Networks — Unit 42, 18 March 2019, https://unit42.paloaltonetworks.com/new-mirai-variant-targets-enterprise-wireless-presentation-display-systems.

[22] Shimamura, Makoto. "Keeping a Hidden Identity: Mirai C&Cs in Tor Network," Trend Micro Security Intelligence Blog, 31 July 2019, https://blog.trendmicro.com/trendlabs-security-intelligence/keeping-a-hidden-identity-mirai-ccs-in-tor-network.

Gamarue — *Down but not out*

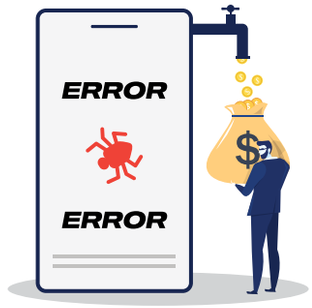
While *Mirai* primarily propagates through infected IoT devices, *Gamarue* is often unwittingly installed via phishing e-mails containing malicious files, and also propagated through infected USB drives and external hard drives. Despite successful international efforts which took down *Gamarue's* infrastructure more than two years ago, the persistent proliferation of *Gamarue* through phishing e-mails and infected storage media underscores the continued need to emphasise good cyber hygiene among all users.

Nymaim — *Malware begets more malware*

Nymaim was notably used by threat actors for targeting the hospitality sector in North America and Europe in early-2019. In this campaign, malspam was observed distributing and using *Nymaim* to download and run other ransomware on infected systems.[23] The continued observation of *Nymaim* throughout the year suggests its growing popularity as a downloader which conveniently deploys different malware at the threat actor's discretion through their C&C servers.

Featured Topic

The Rise of Mobile Malware



Cybersecurity researchers have noted how malware types specifically tailored for attacking mobile devices have dramatically increased in tandem with the global proliferation of mobile devices. Threat actors are seen exploiting vulnerabilities in popular mobile operating systems such as Google's Android and Apple's iOS to infect mobile devices. They do so primarily by capitalising on unsafe user practices — such as downloading applications from unofficial application stores — and disguising mobile malware as reputable applications[24], which are often sold at cheaper prices than legitimate applications, thus enticing the user to download them.[25]

Commonly observed mobile malware in 2019 were designed to evade detection while being persistent and effective, and included banking trojans and adware. Banking trojans, such as *Anubis*[26] and *Cerberus*[27], were easily customisable and available for sale on the Dark Web, making them attractive among cybercriminals. These factors likely contributed to a surge in malicious activity targeting mobile devices, as observed by cybersecurity firm Kaspersky.[28] Most users freely grant various kinds of permissions to applications for the first time they are run, unwittingly permitting embedded malware to steal data and credentials through malicious functionalities. In more severe cases, the malware can even siphon funds from users' bank accounts linked to their mobile banking applications. Separately, adware spams users with unwanted advertisements, and sometimes secretly clicks on advertisements in the background without the users' knowledge, enriching threat actors financially.

[23] Mendoza, Erika, Yaneza, Jay, Sison, Gilbert, Patil, Anjali, Cabuhat, Julie and Soares, Joelson. "Emotet-Distributed Ransomware Loader for Nozelesn Found via Managed Detection and Response," Trend Micro Security Intelligence Blog, 29 March 2019, https://blog.trendmicro.com/trendlabs-security-intelligence/emotet-distributed-ransomware-loader-for-nozelesn-found-via-managed-detection-and-response.

[24] Herman, Jordan. "The Q2 2019 Mobile Threat Landscape Report," RiskIQ Research, 2019, https://www.riskiq.com/research/q2-2019-mobile-threat-landscape-report.

[25] "The risks of third-party app stores," NortonLifeLock — Norton Internet Security Center, Retrieved 1 February 2020, https://us.norton.com/internetsecurity-mobile-the-risks-of-third-party-app-stores.html.

[26] Bao, Tony. "Anubis Android Malware Retuns with Over 17,000 Samples," Trend Micro Security Intelligence Blog, 8 July 2019, https://blog.trendmicro.com/trendlabs-security-intelligence/anubis-android-malware-returns-with-over-17000-samples.

[27] "Cerberus — A new banking Trojan from the underworld," ThreatFabric Blog, August 2019, https://www.threatfabric.com/blogs/cerberus-a-new-banking-trojan-from-the-underworld.html.

[28] Kupreev, Oleg, Sidorina, Tatyana, Chebyshev, Victor, and Kuskov, Vladimir. "Financial threats in H1 2019," Securelist – Kaspersky's cyberthreat research and reports, 31 July 2019, https://securelist.com/financial-threats-in-h1-2019/91899.

Chapter 2

WWW.TARGET.SG

As the global cyber threat landscape continues to evolve and increase in complexity, the methods employed by threat actors have also become more diverse and sophisticated. This section highlights major global cybersecurity trends in 2019, insights from key cyber incidents which targeted specific sectors in Singapore, and CSA's efforts to combat cyber threats.

"Organisations must be prepared to operate through cybersecurity incidents. We are encouraged by the improvements organisations have made to their security programmes, but we also recognise that they must continually adapt to emerging threats. Of all the malware FireEye Mandiant observed in 2019, more than 40 per cent had never been seen before — nor were they stopped or detected by many common safeguards. This demonstrates the need to be continually building and testing your defences. Protecting and strengthening Singapore's cybersecurity ecosystem from cyber threats is an issue that organisations like FireEye and CSA take very seriously."

Mr Kevin Mandia
CEO of FireEye Inc.

Global Trends

Point-of-Sale Attacks

Point-of-Sale (POS) attacks refer to the compromise of touchpoints such as online shopping websites and cash terminals in brick-and-mortar stores, where retail transactions take place. The separation of front- and back-end servers, where the website design and the payment processing functions of e-commerce retailers are outsourced to separate vendors, opens up more vulnerabilities for exploitation. Active since 2016, *Magecart* cybercrime operators have been conducting POS attacks by injecting malicious codes into e-commerce websites to skim credit card details. They have stepped up their activities in recent years, targeting a range of businesses from Small and Medium Enterprises (SMEs) to multinational corporations.

Supply Chain Attacks

According to cybersecurity firm NortonLifeLock (formerly Symantec), supply chain attacks grew by almost 80 per cent in 2018.[29] Supply chain attacks target the less secure components of systems, and could be aimed at accessing and stealing confidential information, or gaining a foothold to springboard attacks into other parts of the system and connected networks. Third-party service providers with access to an organisation's data are often the weak links targeted by threat actors. Notably, many third-party providers which were hit by cyber incidents in 2019 had inadequate cybersecurity measures which placed the supply chains of their clients at risk.

Data Breaches

2019 witnessed an exponential increase in data breaches around the world, with the total number of records exposed registering a near 300 per cent increase, compared to 2018.[30] Data breaches can be costly. Based on a study by IBM Security on the costs of data breaches, organisations stand to lose up to US$4 million on average in the event of a data breach, including investigation and recovery costs, as well as potential lawsuits brought on by clients.[31] The large amounts of personal and financial information held in organisations such as governments, healthcare institutions and technology firms serve as attractive targets for threat actors, who see opportunities to profit from such data.

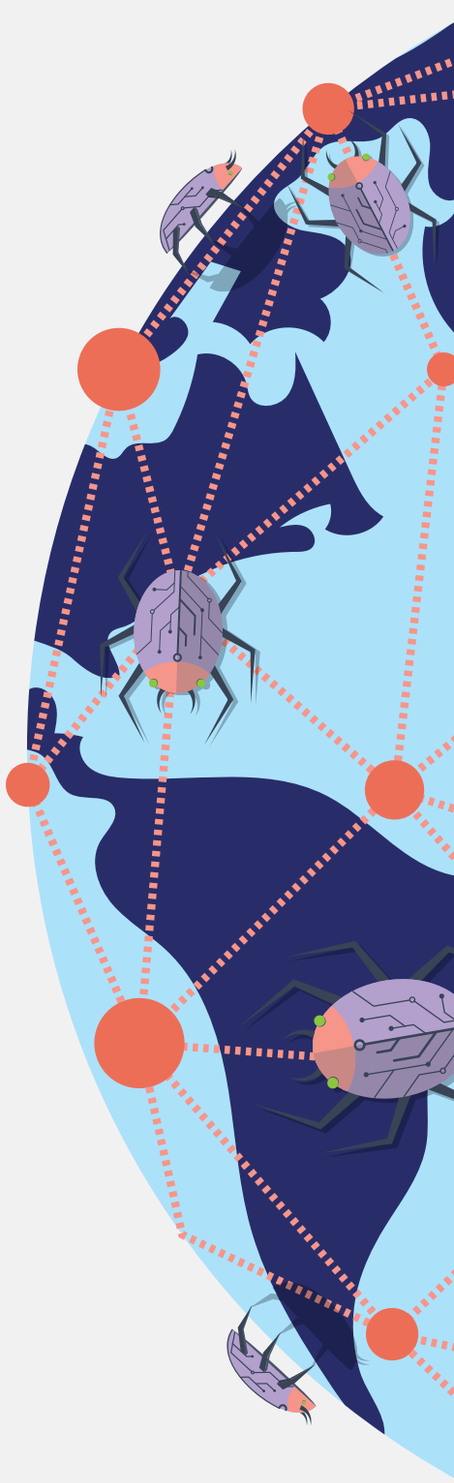
Mobile Attacks

Threat actors are shifting towards targeting mobile devices such as smartphones and tablets to conduct credential theft, surveillance and malicious advertising. The number of attacks using banking malware against mobile devices in the first half of 2019 alone saw a 50 per cent increase over the whole of 2018.[32] A major factor behind this spike in mobile attacks is likely due to the increased usage of mobile banking applications, which provide lucrative avenues for threat actors to gain access to and steal sensitive information such as credit card and bank account details. With more than five billion unique mobile devices in the world[33], and an estimated 8.5 million subscriptions (representing a mobile penetration rate of ~150 per cent)[34] in Singapore, this ever-growing reliance on mobile devices will only increase the attack surface for mobile threats.

Spear Phishing

In 2019, nearly 90 per cent of organisations worldwide have been targeted by spear phishing e-mails pretending to be from trusted senders aiming to obtain information from their victims.[35] To add authenticity to the spear phishing e-mails, threat actors are also observed to adapt the writing styles of spoofed individuals and organisations, as well as use information from publicly available sources, such as social media posts, so that their e-mails appear more convincing to their victims.

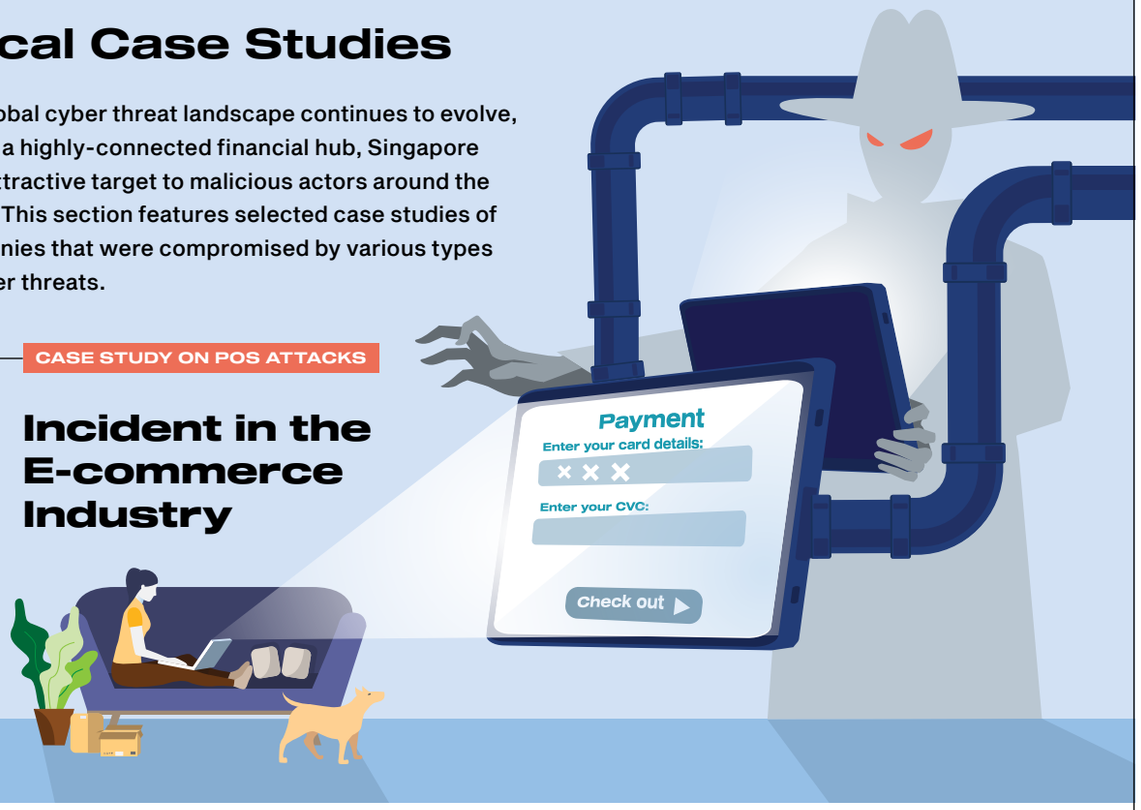
Business e-mail compromise is another form of spear phishing which is increasing. This scam involves phishing e-mails purportedly sent by high-ranking officials or senior personnel to employees and customers of an organisation, in order to trick them into making fund transfers or divulging sensitive information.



[29] Symantec Internet Security Threat Report (ISTR) Volume 24, February 2019, https://docs.broadcom.com/doc/istr-24-2019-en.
[30] "In 2019, a total of 7,098 reported breaches exposed 15.1 billion records," Help Net Security, 11 February 2020, https://www.helpnetsecurity.com/2020/02/11/2019-reported-breaches.
[31] IBM Security — 2019 Cost of a Data Breach Report, https://databreachcalculator.mybluemix.net.
[32] Check Point Research — 2020 Cyber Security Report, https://www.checkpoint.com/downloads/resources/cyber-security-report-2020.pdf.
[33] Koetsier, John. "Why 2020 is a Critical Global Tipping Point for Social Media," Forbes, 18 February 2020, https://www.forbes.com/sites/johnkoetsier/2020/02/18/why-2020-is-a-critical-global-tipping-point-for-social-media/.
[34] "Statistic on Telecom Service for 2019 Jul – Dec," Infocomm Media Development Authority (IMDA), Retrieved 1 March 2020, https://www.imda.gov.sg/infocomm-media-landscape/research-and-statistics/telecommunications/statistics-on-telecom-services/statistic-on-telecom-service-for-2019-jul.
[35] Proofpoint — 2020 State of the Phish Report, https://www.proofpoint.com/us/resources/threat-reports/state-of-phish.

Local Case Studies

The global cyber threat landscape continues to evolve, and as a highly-connected financial hub, Singapore is an attractive target to malicious actors around the world. This section features selected case studies of companies that were compromised by various types of cyber threats.



CASE STUDY ON POS ATTACKS

Incident in the E-commerce Industry

What Happened?

In late-2019, customers of a local online fashion retailer were informed that hackers had tried to harvest their personal information by injecting a malicious code into the retailer's e-commerce website.

Investigations revealed that the injected malicious code allowed a fake form to overlay the genuine web form used for collecting personal information from the retailer's customers. Personal information that was subsequently stolen included the customers' first and last names, e-mail addresses, shipping addresses, order details, payment type, and credit card information.

Follow-up Action

Upon discovering the data breach, the retailer alerted the Singapore Police Force (SPF) and Personal Data Protection Commission (PDPC). It also worked with cybersecurity experts to remove the malicious code from the affected website, and implemented measures to secure their systems. These measures included enforcing two-factor authentication (2FA) for back-end access, password resets for all user accounts, and further digital forensic analysis. Updates about the mitigation measures taken were also circulated to the retailer's customers.

Businesses risk losing their reputations and consumer confidence if they do not take privacy issues seriously, or fail to protect their platforms with robust measures. They should ensure that their websites and databases are secure and regularly patched.

CASE STUDY ON RANSOMWARE ATTACKS

Incident in the Financial Sector

What Happened?

In January 2020, employees at a local financial institution reported for work in the morning only to find that they were unable to access the files on their computer. Their files had been encrypted, and the employees were greeted by a ransom note demanding payment in Bitcoin to enable decryption and regain file access. A number of workstations and servers were affected, and the financial institution alerted the relevant authorities immediately.

The systems were found to be infected with the *Sodinokibi* ransomware, a highly evasive and sophisticated strain likely linked to the *GandCrab* ransomware family due to similarities in their source codes. *Sodinokibi* was also suspected to be deployed in high-profile hits at international foreign currency exchange firm Travelex and the New York State's Albany International Airport.

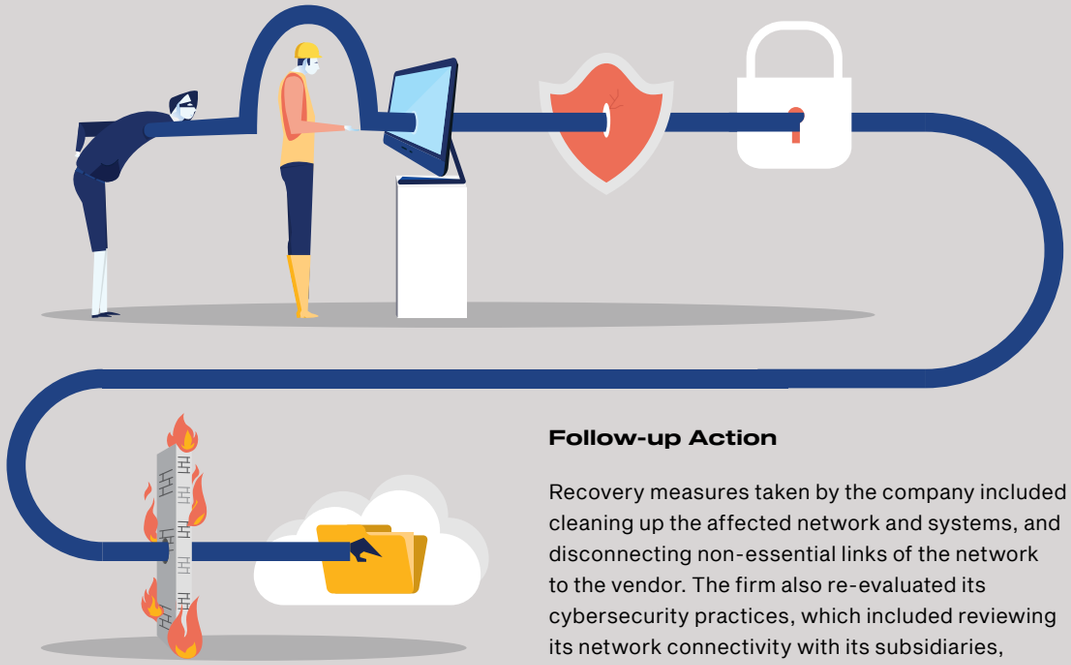
Five suspicious Internet Protocol (IP) addresses related to malicious activities were found during the analysis of the company's server logs. These IP addresses were linked to the Tor anonymity network, which was known to be frequently exploited by cybercriminals seeking to conceal their IP locations from network surveillance and traffic analyses. The discovery of Tor-linked IP addresses, together with the sophisticated nature of the ransomware deployed, indicated the involvement of a cybercrime syndicate.

Follow-up Action

The company disconnected all infected workstations and servers from its networks to prevent further spread of the ransomware. Cybersecurity experts were also engaged to undertake incident response processes, clean up affected systems, and implement recovery efforts. Network sensors were deployed to monitor further malicious activity and signs of data exfiltration. There was no impact on the company's business operations, and no sign that its data had been stolen.

CASE STUDY ON SUPPLY CHAIN ATTACKS

Incident in the ICT Sector



What Happened?

In early-2019, data stolen from a local information and communications technology (ICT) firm was reportedly put up for sale on the Dark Web. The ICT firm took measures immediately to detect signs of unauthorised access into their networks and systems. Cybersecurity firms were also engaged to assist in forensic investigations and gather intelligence.

Investigations revealed that the threat actor accessed the company's corporate network through a vendor, and then compromised two systems related to customer care. There was no indication of data exfiltration from the affected network and systems.

Follow-up Action

Recovery measures taken by the company included cleaning up the affected network and systems, and disconnecting non-essential links of the network to the vendor. The firm also re-evaluated its cybersecurity practices, which included reviewing its network connectivity with its subsidiaries, reconfiguring relevant firewall rules, and scanning their networks and systems for Indicators of Compromise (IOCs).

Many websites are prone to web hacking techniques, such as Structured Query Language (SQL) code injection — the embedding of malicious codes — that allow attackers to send queries to webpages, such as the log-in page. Through such techniques, attackers can assume the identity of the web administrator, access or modify data, or exploit inherent vulnerabilities. In the event of a systems compromise, the recovery process would be costly and time-consuming, especially in cases where the system was damaged, or if company data was stolen or corrupted.

To prevent such attacks and for business continuity, organisations need to ensure that their websites and databases are properly secured, configured and encrypted where necessary. Organisations should also ensure that their systems are regularly patched to address known vulnerabilities in their networks and systems.

CASE STUDY ON SPEAR PHISHING ATTACKS

Business E-mail Compromise and Takedown of Phishing Websites

What Happened?

An employee received a phishing e-mail that looked like it had been sent by the company's IT department, which alerted the employee to update the software on his computer to avoid an account suspension. Unaware that he had been re-directed to a phishing webpage by clicking on the e-mail link, the employee unsuspectingly entered his user credentials, which were then harvested by the attacker.

With the stolen user credentials, the attacker logged into the employee's e-mail account and sent an e-mail to the company's accountant to request for an immediate online fund transfer. Fortunately, the accountant spotted suspicious signs in the e-mail, and checked the veracity of the information via phone calls with the sender instead of replying through the e-mail. Further investigations confirmed that the employee's e-mail account had been compromised and the user credentials were leaked through the phishing webpage.

Recommendations

CSA constantly watches out for phishing e-mails and links. Organisations and members of public can report phishing links to CSA, who will work with the Infocomm Media Development Authority (IMDA) to take down the phishing site. IT administrators can also analyse malicious e-mails to discover the originating IP addresses, and subsequently block all e-mails from them to prevent similar scams. Organisations are encouraged to conduct regular awareness campaigns to educate their employees on good cyber hygiene practices, so that they do not fall victim to phishing scams.

How CSA Combats Cyber Threats

CSA provides dedicated and centralised oversight of national cybersecurity functions to protect the nation on two fronts:

- **by strengthening the resiliency of Singapore's Critical Information Infrastructure (CII) sectors; and**
- **by responding swiftly to cybersecurity threats and vulnerabilities.**

Strengthening Resiliency of the CII Sectors

To maintain situational awareness, CSA tracks developments in cyberspace closely to understand cyber threats and emerging issues. By forewarning CII sectors about cyber threats and issues, CSA can better anticipate and implement actions in a timely manner to prevent and disrupt potential cyber-attacks. In the event of large-scale cyber incidents affecting multiple CII sectors, CSA takes on the role of the National Incident Manager and coordinates cross-sector incident response, directing national-level mitigation measures against cyber threats. When the need arises, CSA will deploy the National Cyber Incident Response Teams (NCIRTs) to assist affected CII sectors. CSA also conducts cyber research and analysis over the long-term to provide strategic insights on both the global and local cyber landscapes and developments. These insights aim to inform CSA's operations and provide valuable guidance to national cyber policy-making.

CSA also conducts regular cybersecurity exercises involving CII sectors to strengthen their preparedness against cyber threats. The exercises allow sectors to assess their capabilities and identify opportunities to enhance their processes.

Featured Topic

Mr Teo Chee Hean (Senior Minister and Coordinating Minister for National Security), Mr S Iswaran (Minister for Communications and Information and Minister-in-Charge of Cybersecurity), and Dr Janil Puthucheary (Senior Minister of State (SMS) for Communications and Information and SMS-in-Charge of Cybersecurity) interacting with exercise participants during Exercise Cyber Star 2019. Source: MCI.

Cybersecurity Exercises

Over the course of a few days, Singapore witnessed a spate of sudden and rapid escalation of cyber-attacks. Several websites belonging to the Government and media outlets suffered from mass defacement attacks. Subsequently, there were disruptions to Internet access and communications networks, leaving users unable to access multiple online essential services. At the airport, flight information systems displayed unintelligible content and baggage handling systems were not sorting passenger baggage properly. Ships in Singapore waters were not able to receive maritime traffic information, while cranes at the ports started malfunctioning. Equipment in healthcare facilities stopped working, severely hampering medical support around the island.

Fortunately, these were only the highlights of the complex intertwined scenarios in CSA's nationwide cyber crisis management exercise codenamed Cyber Star (XCS), which aimed to enhance Singapore's crisis management capabilities and readiness to respond promptly and effectively to a cyber-attack. XCS participants were tested with realistic scenarios of multi-dimensional cyber threats such as Distributed Denial-of-Service (DDoS) attacks, Domain Name System (DNS) manipulation, Industrial Control Systems (ICS) compromise, phishing websites, ransomware and supply chain attacks.

Over 250 representatives from the 11 CII sectors and private sector underwent a series of scenario planning sessions, operational workshops and table-top discussions before culminating in a final operations-based exercise, where they developed and tested their incident management and emergency response plans to these simulated cyber-attacks.

Separately, over 500 participants from CII sectors (such as Banking & Finance, Healthcare, Land Transport, Security & Emergency and Water) took part in exercises codenamed CyberArk (XCA) to review and validate their cybersecurity capabilities and incident response plans. These sector-specific exercises, which were conducted throughout the whole of 2019, were aimed at strengthening readiness and capabilities within CII sectors.

CASE STUDY ON DDOS REMEDIATION

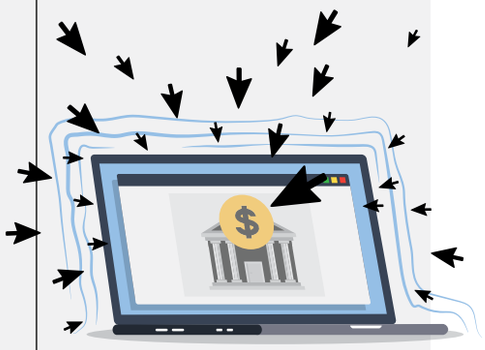
Cooperating with Foreign CERTs

What Happened?

In 2019, the web portal of a local financial institution suffered a DDoS attack. The public-facing server that was connected to this portal experienced a spike in web traffic and was brought down. It was later determined by SingCERT and the local telecommunications service providers that the web traffic originated from overseas.

Follow-up Action

Knowledge sharing among international cybersecurity communities is pivotal to strengthening international cooperation in cyberspace. CSA approached our partners from foreign CERTs and relevant hosting providers for further assistance. The coordinated efforts from all parties subsequently led to the prompt takedown of the C&C servers that were responsible for the DDoS attack.



Responding Swiftly to Cybersecurity Threats and Vulnerabilities

Preventing cybersecurity incidents starts from the identification of threats, and protection of key assets from attacks posed by such threats. In this regard, the Singapore Computer Emergency Response Team (SingCERT) scans for vulnerabilities and analyses the risks that they pose, and recommends appropriate mitigation measures that businesses and members of the public can take to protect themselves.

Given the transnational nature of cybersecurity threats, SingCERT exchanges information proactively with other Computer Emergency Response Teams (CERTs), both foreign and local, for a more comprehensive cybersecurity situational awareness and early warning of emerging threats. Such tight cooperation and links have allowed us to deal with the threats more efficiently, especially as some of the threats originate from outside of Singapore, and require assistance from foreign CERTs to mitigate. CSA's participation in several regional forums has also helped to expedite this process further.

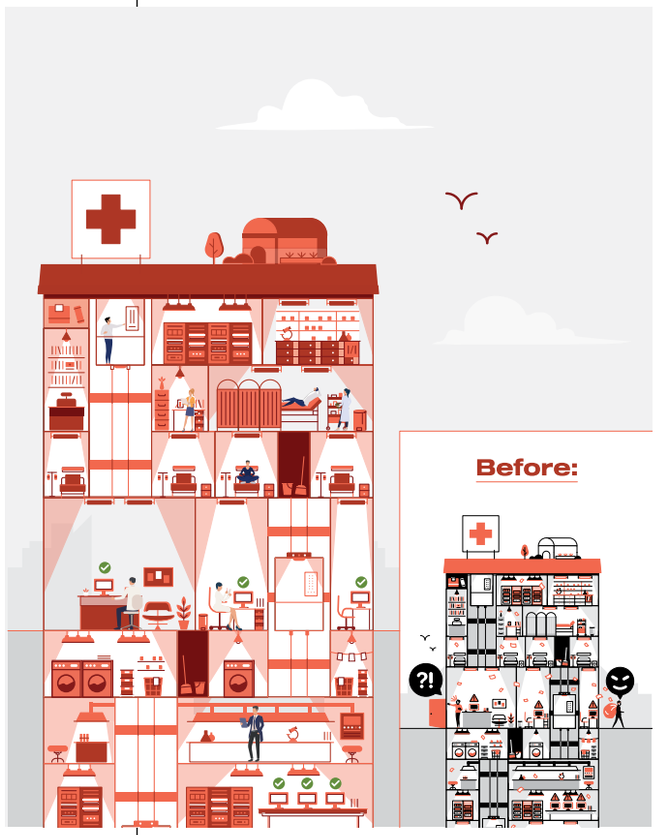
Asia Pacific Computer Response Team (APCERT)

APCERT cooperates with CERTs and Computer Security Incident Response Teams (CSIRTs) to ensure cybersecurity in the Asia Pacific region.

On 31 July 2019, the APCERT Cyber Drill was held with the theme "Catastrophic Silent Draining in Enterprise Network". The drill served as a platform to test and evaluate the response capabilities of leading CERTs/CSIRTs within the region in responding to actual incidents and issues. As a member of the APCERT Drill Working Group, SingCERT participated as an Exercise Controller and conducted the drill with fellow CERTs/CSIRTs.

SingCERT hosted the 17th APCERT Annual General Meeting and Conference in Singapore, themed "Fostering a Safer Cyberspace through Partnerships and Collaboration", from 29 September to 2 October 2019. Over 100 participants from the APCERT community attended the conference, which was held in conjunction with the Singapore International Cyber Week (SICW) 2019, the region's leading conference for cybersecurity. The chosen theme complemented APCERT's efforts in bringing together CERTs/CSIRTs, industry professionals and academia to discuss cyber issues and capacity building measures to create a safer and more secure cyberspace.

CASE STUDY



Post-2018 SingHealth Incident

Background

In June 2018, SingHealth fell victim to an APT group. The incident was the most serious data breach in Singapore to date, with the personal particulars of 1.5 million patients and the outpatient prescriptions of about 160,000 of them illegally accessed and copied. Prime Minister Lee Hsien Loong's records were specifically and repeatedly targeted.

CSA's NCIRT was deployed on site to work with Integrated Health Information Systems (IHiS) — the IT agency serving the public healthcare sector including SingHealth — to carry out joint investigations and remediation. CSA and IHiS took swift measures to contain the threat and prevent recurrence of the incident.

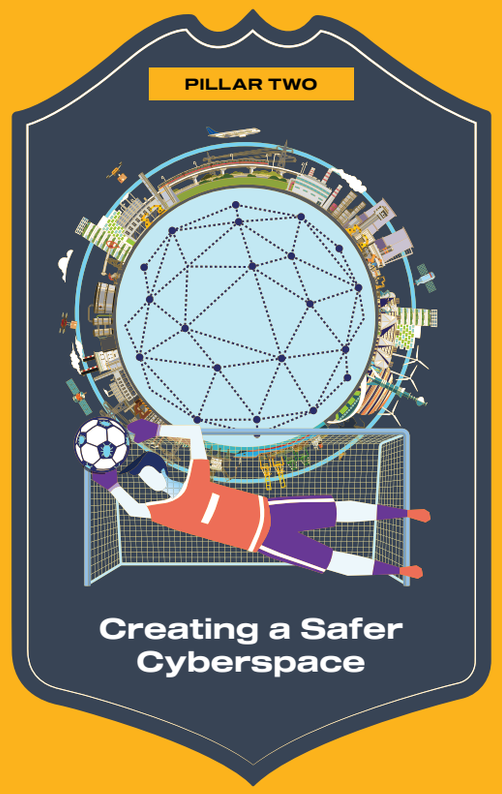
Actions Taken

Following the incident, a Committee of Inquiry (COI) was convened to investigate the events and contributing factors leading to the incident. The COI made 16 recommendations to enhance the capabilities of CII Owners (CIIOs) across Singapore's CII sectors to deter, detect, respond to and recover from cybersecurity incidents.

These recommendations aimed to:

1. Strengthen organisational structure
2. Raise staff cybersecurity competencies
3. Improve system and data protection
4. Enhance security checks on systems
5. Improve incident response processes

The CIIOs have been implementing these recommendations progressively since early-2019. As of end-March 2020, six sectors have completed implementation of both priority and additional recommendations. Other sectors have implemented measures for between 80 to 90 per cent of their CII. Sector leads have to strike a balance between maintaining their CII systems' availability, reliability and safety, together with the implementation of relevant cybersecurity measures. Thorough testing has to be conducted on CII systems after the implementation of the relevant measures to ensure their serviceability. In addition, both implementation and testing have to be completed within certain time periods to ensure the continuous delivery of essential services. However, CIIOs are committed and target to complete the majority of the implementation by end-2020.



Chapter 3

Upping the Game on Singapore's Cybersecurity

Launched in 2016, Singapore's Cybersecurity Strategy sets out the nation's vision, goals and priorities for a resilient and trusted cyberspace. It aims to catalyse participation by all stakeholders — Government, cyber industry, providers of essential services and individuals. Cybersecurity is a team sport, and everyone needs to play their part and play it well. Coordinated teamwork and commitment with the public, enterprises and strategic partners are essential elements to meeting our goals.

Pillar One:

Building a Resilient Infrastructure

Critical Information Infrastructure (CII) sectors are essential pillars which support the foundation of Singapore's economy. The effects of a cyber-attack on the CII sectors could result in significant disruptions to the economy and our society. In addition, there may be ramifications beyond our shores as Singapore is an international hub for trade, finance and logistics. The strategic imperative is to ensure that essential services are resilient to minimise impact and the duration of disruption in the event of a cyber-attack. The Government is committed to working with key stakeholders to strengthen the resilience of our CII sectors.

> **"As a community we have moved beyond the land of theoretical cyber-attacks on industrial operations to a world where these attacks are a reality for denying power, disrupting operations, and even specifically targeting human life as was the case in the TRISIS cyber-attack in 2017. The threat is worse than we realise but not as bad as we want to imagine. It is a worthy cause to invest in and prioritise OT cybersecurity and it is a winnable battle."**
>
> **Mr Robert M. Lee**
> CEO and Founder of Dragos Inc.

Singapore's Operational Technology (OT) Cybersecurity Masterplan 2019

Operational Technology are systems that control physical processes, industrial processes and manufacturing equipment. As many of the CII rely on them, attacks on OT systems can have serious consequences, including physical disruption of its activities. Singapore's OT Cybersecurity Masterplan hence serves as a strategic blueprint to guide national efforts to foster a resilient and secure cyber environment for Singapore's OT environment. Launched at the Singapore International Cyber Week (SICW) 2019, the Masterplan takes a balanced approach between security requirements, rapid digitalisation and ease of conducting business-as-usual activities.

Spanning the areas of "People", "Process" and "Technology", the Masterplan aims to uplift the cybersecurity practices of CII Owners (CIIOs) and organisations that operate OT systems. The key thrusts include:

- Providing OT cybersecurity training to develop human capabilities;
- Facilitating the sharing of information through an OT Cybersecurity Information Sharing and Analysis Centre (OT-ISAC);
- Strengthening OT owners' policies and processes through the issuance of an OT Cybersecurity Code of Practice (CCoP) that provides cybersecurity controls and outcomes specific to OT systems; and
- Adopting technologies for system resilience through Public-Private Partnerships.

International Critical Infrastructure Security Showdown

Supported by the National Cybersecurity R&D Programme (NCR) that is co-chaired by CSA and National Research Foundation (NRF), the 3rd International Critical Infrastructure Security Showdown was conducted at the Singapore University of Technology and Design (SUTD) in August 2019. Teams from the USA, Italy, Japan, Estonia and Singapore took part in the three-day invitation-only exercise, which brought together security assessors and researchers from both industry and academia to develop capabilities in handling a diverse range of attack vectors on a realistic critical infrastructure platform.

Cloud Software-as-a-Service (SaaS) Whitelisting

In 2019, the Government adopted a "Commercial-Cloud first" policy where agencies shall, as a default, use Commercial Cloud for new Restricted and Unclassified ICT systems. This is to deliver better, faster and more cost-efficient digital services to citizens and businesses.

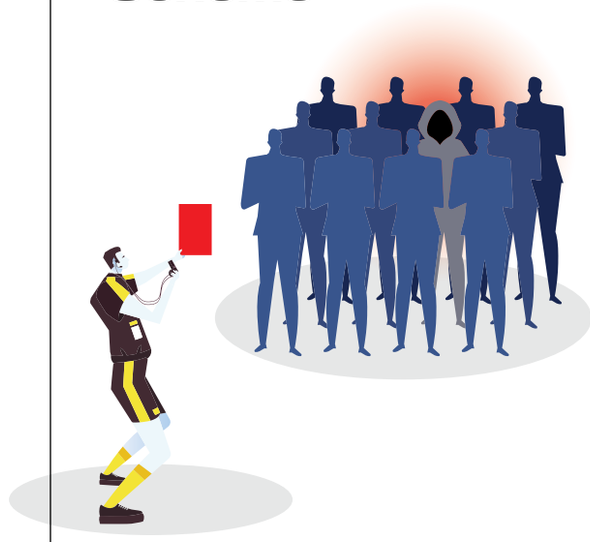
In support of this policy, GovTech launched a Software-as-a-Service (SaaS) whitelisting process. This process ensures that only SaaS with adequate controls can be utilised in the Government environment.

To use the SaaS, an agency has to document the necessary features, controls and contractual agreements of the SaaS. Thereafter, the Government will assess the risk of the software application by investigating areas, such as data jurisdiction, mode of access, use case, contractual agreements and information sensitivity.

With the SaaS whitelisting process, GovTech has evaluated over 20 applications and services on the cloud, and has approved more than 15 SaaS requests that complied with stringent cybersecurity requirements.

Featured Topic

Whistleblowing Scheme



CSA has implemented the Whistleblowing Scheme to provide individuals with a channel to disclose information on cover-ups relating to:

- Incidents that may threaten the cybersecurity of CII sectors;
- Malicious behaviour and dereliction of duty from individuals who may compromise the cybersecurity of CII; and/or
- Deliberate mis-stating or falsification of information to CSA.

The objective of the scheme is to uncover wrongdoings that may threaten the cybersecurity of CII. The scheme will enable CSA to have better oversight of incidents affecting the CII sectors, and for CSA to take prompt and necessary action.

Pillar Two:

Creating a Safer Cyberspace

Cyber technology can enable and empower businesses and society, but only if it is safe and trustworthy. A safer cyberspace is the collective responsibility of the Government, enterprises and everyone in the community. There is a need to constantly raise understanding of cybersecurity issues and promote adoption of good practices among enterprises and the community.

National Cybersecurity Awareness Campaign

Visitors trying their hand at creating a strong password at the second roadshow of "Go Safe Online 2019" at Our Tampines Hub. Source: CSA.

CSA launched the third National Cybersecurity Awareness Campaign "Go Safe Online 2019" at Ang Mo Kio Central Stage on 14 September 2019. The campaign focused on the personal consequences of not adopting good cybersecurity practices, and highlighted CSA's four cyber tips.[36]

This Campaign has expanded since its inception in 2017. The number of roadshows increased from one to three, so that members of the public have more avenues to learn about cybersecurity through interactive games, and obtain face-to-face advice from cyber champions on site. The first two roadshows were held in the second half of 2019 at Ang Mo Kio Central Stage and Our Tampines Hub, and they attracted close to 37,000 visitors. This was followed by a campus roadshow at the Institute of Technical Education College West in January 2020, which drew close to 5,000 students and staff. To expand the reach of the campaign, a series of videos with print and online adaptations also made its rounds on social media, with additional publicity in cinemas, banks, clinics, HDB lift doors, buses and MRT stations.

Since May 2019, CSA has rolled out 50 runs of a "Go Safe Online" drama skit to secondary schools. The skit was seen by over 32,000 students and teachers, and was well-received for conveying cybersecurity messages in an engaging way. The Cyber Savvy Machine Pop Up[37], introduced in November 2018, has toured Singapore's public libraries, schools and organisations including the Singapore Discovery Centre. In 2019, the machine recorded close to 82,000 attempts.

[36] CSA's four cyber tips that Internet users should adopt to safeguard their digital devices and data include: 1) Use strong passwords and enable Two-Factor Authentication (2FA); 2) Spot signs of phishing; 3) Update software promptly; and 4) Install anti-virus software.

[37] The Pop Up comprises a Cyber Savvy vending machine and information panels on the four cybersecurity tips. Participants can test their cybersecurity knowledge through a quiz on the vending machine and win a small gift in the process.

Enhancing IoT Cybersecurity

Distinguished experts from the government, industry, and academia came together at the 4th IIoTSR to galvanise global efforts towards a secure and trusted IoT ecosystem. Source: CSA.

Cybersecurity Labelling Scheme

In recent years, consumers have increasingly adopted Internet of Things (IoT) or smart devices, such as Smart TVs, Home Assistants and IP cameras, with numbers expected to reach 75 billion by 2025. Out of the box, these devices typically have inadequate cybersecurity provisions and are often easily compromised, putting their users at risk.

As part of efforts to better secure Singapore's cyberspace and raise cyber hygiene levels, CSA launched the Cybersecurity Labelling Scheme (CLS) for network-connected smart devices in early 2020. The scheme, which marks a first in the Asia Pacific region, will comprise different levels of cybersecurity ratings to help consumers make informed choices about the security features of the smart devices they purchase. For a start, CLS will focus on products such as routers and Smart Home Hubs that have a greater impact on consumers. The cybersecurity labels issued under CLS will provide an indication of the security provisions in the registered products.

CCCY and the Cybersecurity Standards Roadmap

During SICW 2019, CSA and Enterprise Singapore announced the formation of a Coordinating Committee for Cybersecurity (CCCY) under the Singapore Standards Council (SSC), to coordinate and facilitate sharing of cybersecurity information in Singapore, and to formulate a five-year Cybersecurity Standards Roadmap. The Roadmap will cover standards relating to organisations and the IT user community, to help companies and Government agencies mitigate cyber threats, as well as raise cyber hygiene and security assurance.

Thought Leadership and Knowledge Sharing

During SICW 2019, CSA also hosted the 18th International Common Criteria Conference (ICCC) and the 4th International IoT Security Roundtable (IIoTSR). These events brought together thought leaders and experts from more than 30 countries, ranging from public and private sectors, to discuss and galvanise global efforts in both Common Criteria and IoT security. Singapore has been a Common Criteria Certificate Authorising Nation[38] since January 2019.

As part of ICCC 2019, CSA also hosted the 4th IIoTSR, which serves as an international platform that brings together industry, government and academia to galvanise global efforts towards a secure IoT ecosystem. During the 4th IIoTSR, Singapore and the Netherlands jointly published the IoT Security Landscape Study to enhance understanding on the IoT landscape, and its cybersecurity risks and challenges. Singapore and the United Kingdom (UK) also signed a Joint Statement to strengthen partnerships in this area. These initiatives underscore the concerns that Singapore and various countries share regarding this hyper-evolving and dynamic domain, as well as CSA's joint commitment towards a safer and secure IoT environment.

[38] Singapore attained the status of a Certificate Authorising Nation in January 2019 under the Common Criteria Recognition Arrangement. Common Criteria (CC) is the de facto standard for cybersecurity standard certification around the world, and CC certificates are mutually recognised across 30 nations.

Featured Topic

Digital Defence — Total Defence's Sixth Pillar

Source: Nexus.

As we work towards being a Smart Nation, digital technology will pervade all aspects of how we live, work and play. It will connect us to the world and open up opportunities for us to progress. However, it also makes us increasingly vulnerable to threats from the digital domain. These threats can disrupt our way of life, undermine our social cohesion and affect the psychological resilience of our people. Digital Defence, therefore, becomes more important.

Digital Defence is about being secure, alert and responsible online so that we can protect and defend ourselves and Singapore from threats from the digital domain. Every individual is the first line of defence against threats from the digital domain. We all can do our part to help strengthen Digital Defence by putting in place policies and systems to strengthen cybersecurity, be vigilant and equipped to respond against fake news and disinformation and strengthen digital readiness among Singaporeans.

Featured Topic

Government Bug Bounty Programme / Vulnerability Disclosure Programme

The Government Bug Bounty Programme (BBP) was launched in December 2018 to: (1) identify blind spots in the cybersecurity defences of Government Internet-accessible applications; and (2) build a shared sense of collective ownership over the cybersecurity of our systems, by involving the local and global community of researchers.

The Government BBP focuses on a number of identified systems at a time, and permits conditional exploration by researchers for a short period of about three weeks. The first and second Government BBP garnered participation from close to 700 local and overseas cybersecurity researchers and white hats, and about 60 validated vulnerabilities were remediated.

To provide a wider umbrella and supplement the BBP, the Vulnerability Disclosure Programme (VDP) was launched in October 2019 to: (1) provide a channel for the public to report suspected vulnerabilities; and (2) practise coordination and remediation efforts at both ministry and agency levels in a timely and sustainable manner. The VDP covers all Government-owned Internet-facing systems; the difference between the Government BBP and VDP is that there are no bounty pay-outs for vulnerabilities reported, and no authorisation given for any form of exploitation.

These collaborations with the cybersecurity community-at-large have helped the Government discover vulnerabilities that would otherwise have been undetected, and strengthen the security posture of the Government's ICT systems and digital services.

CSA encourages organisations and companies that want to go beyond baseline cyber hygiene assurances to consider undertaking bug bounty programmes or establishing a responsible vulnerability reporting policy. These steps could strengthen their cyber defences by proactively discovering and eliminating vulnerabilities, which in turn would reduce their reputational risk in the event of a cyber incident.

> **"Amid the rise in scale of cyber-attacks and complexity of systems deployed online, organisations are finding it a challenge to guarantee perfection in their security programmes through their effort alone. A public Vulnerability Disclosure Programme, which invites and rewards members of the public to report security weaknesses, will be a good complement to existing enterprise effort. As the reward is only disbursed if it is a valid report, this is a low-cost, high-return cyber component that every organisation with Internet-facing digital assets should have."**
>
> **Mr Steve Lam**
> Cybersecurity Partner, Ernst & Young Advisory Pte. Ltd.

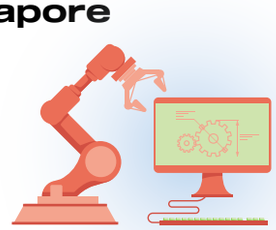
Pillar Three:

Developing a Vibrant Cybersecurity Ecosystem

Cybersecurity is both a security imperative and an economic opportunity. With advanced infrastructure and a tech-savvy workforce, Singapore is well-poised to develop a vibrant cybersecurity ecosystem comprising highly skilled professionals, companies with deep cybersecurity capabilities and strong translational research and development (R&D) efforts. This ecosystem will ensure a sustainable and skilled workforce and drive industry innovation and advanced research to support Singapore's plans for a resilient national infrastructure and a safer cyberspace. This chapter details initiatives by CSA and its partners in 2019.

Enhancing the Cybersecurity Workforce and Encouraging Industry Innovation in Singapore

In partnership with the industry, academia and partner agencies, CSA continues to drive and support initiatives to grow Singapore's cybersecurity workforce, encourage industry innovation to serve and grow local and international markets and strengthen research capabilities. Noteworthy efforts in 2019 included:



Launching the **2019 Cybersecurity Industry Call for Innovation**, which featured 14 challenge statements from 10 end-users including CSA and key stakeholders in the Energy, Healthcare and Maritime sectors. The Call attracted more than 80 proposals from cybersecurity companies eager to work with participating end-users to develop cutting-edge innovative cybersecurity solutions.

Expanding the annual **Cybersecurity Awards**[39] to include the "End-user Award" category and the "Regional Award" category for non-profit organisations. The Cybersecurity Awards recognises significant contributions by individuals and organisations to the local and regional cybersecurity ecosystems.

Setting up the **National Integrated Centre for Evaluation (NICE)** in collaboration with Nanyang Technological University (NTU) to facilitate the testing and evaluation of products, conducting of training, and advanced research for security evaluation techniques.[40]

Organising the inaugural **Cybersecurity Innovation Day**[41] to showcase solutions by local cybersecurity companies and providing a platform for them to interact with potential end-users, collaborators and investors.

[39] The Cybersecurity Awards is organised by the Association of Information Security Professionals (AiSP), and supported by CSA and eight other professional and industry bodies.
[40] The collaboration between NICE and NTU harnesses the strength of NTU's research competencies in hardware security assurance, and aims to reap synergy by optimising the utilisation of resources through the sharing of high-end equipment and pooling of industrial and research expertise.
[41] More than 450 cybersecurity stakeholders, including start-ups, industry, Government, academia and key end-users, attended the Cybersecurity Innovation Day in August 2019.

Dr Janil Puthucheary (Senior Minister of State (SMS) for Communications and Information and SMS-in-Charge of Cybersecurity) delivering opening remarks at the launch of the 2019 Call for Innovation. Source: MCI.

> **"The Singapore cybersecurity landscape suffers from a crucial shortage of people. We need to groom talent from an early stage if Singapore wants to excel in the space. Students need to see cybersecurity as an attractive option that can help them build exciting skills and offer them a richly rewarding career."**
>
> **Ms Tammie Tham**
> CEO of Ensign InfoSecurity

Launching **SG Cyber Youth**, a national programme designed to attract and guide youths in their cybersecurity education and career choices.[42] As part of this, the Youth Cyber Exploration Programme (YCEP) expanded in 2019 to host 400 secondary students for four-day boot-camps. Top student participants were invited back for the inaugural YCEP Central Capture-the-Flag Competition.

Growing research efforts under the three **National Satellites of Excellence (NSoEs)**[43], as part of CSA's collaborative efforts with the research ecosystem on R&D and translational efforts to deepen technological capabilities. Grants totalling S$15 million were awarded to 21 projects spanning various research themes in software security, mobile application security and cyber-physical systems security.

Featured Topic

Updates on Innovation Cybersecurity Ecosystem @ Block71

Supported by CSA and the Infocomm Media Development Authority (IMDA), the Innovation Cybersecurity Ecosystem at Block71 (ICE71)[44] is the region's first cybersecurity entrepreneurship hub. It seeks to create a vibrant and sustainable innovation ecosystem by providing access to funding, go-to-market support, and mentorship support for the cybersecurity innovation community. In just over a year, the ICE71 programmes have benefited 66 individuals (ICE71 Inspire), and 55 start-ups (ICE71 Accelerate and Scale), with more than 4,000 individuals participating in over 40 corporate and investor sessions organised by ICE71. These efforts have resulted in four ICE71 Accelerate start-ups raising over S$4.5 million in follow-on funding as of end-2019. ICE71 has also received interest from the international community, hosting delegations from countries including Australia, France, UK as well as the Netherlands.

[42] The SG Cyber Youth Programme is led by CSA, in collaboration with partners from the cybersecurity industry and academia. There are plans for the programme to reach out to 10,000 youths over the next three years through training boot-camps, learning journeys and career mentoring sessions.
[43] Anchored in local universities, the NSoEs were established to build and consolidate local research strengths in domains of national interest including Trustworthy Software Systems, Mobile Systems Security & Cloud Security, and Design Science and Technologies for Secure Critical Infrastructure.
[44] The three key programmes of ICE71 include ICE71 Inspire, ICE71 Accelerate, and ICE71 Scale.

Featured Topic

SG Cyber Women

SG Cyber Women, a programme under the SG Cyber Talent initiative, aims to interest and develop women in a cybersecurity career. Source: CSA.

Ms Sim Ann (Senior Minister of State for Communications and Information) delivering opening remarks at the inaugural Women in Cyber event, organised as part of SICW 2019. Source: CSA.

The SG Cyber Women (#SGCyberWomen) is a national programme driven by CSA in collaboration with industry partners to encourage more women to join the cybersecurity workforce. The initiative attracts students and professionals from related fields to engender more diversity in Singapore's cybersecurity talent pipeline.

In 2019, CSA and industry partners reached out to at least 3,000 participants through various channels. CSA brought together the Singapore Computing Society (SCS), Division Zero, Association of Information Security Professionals (AiSP) and ISACA Singapore Chapter to organise career mentoring sessions for women. AiSP conducted career talks at girls' schools, and also launched a programme that offers one-to-one career mentoring from cybersecurity practitioners and leaders for female students in Institutes of Technical Education, polytechnics and universities.

During SICW 2019, CSA organised the inaugural Women in Cyber event for 200 participants in collaboration with the High Commission of Canada and with support from the Australian and British High Commissions. CSA also supported the Women in Cybersecurity (WoSEC)'s inaugural Capture-The-Flag (CTF) for Girls in July 2019, which attracted some 50 tertiary students and professionals.

Featured Topic

Cyber Competitions

The World of Science — Computer Security

Students intently honing their cyber skills at the Capture-the-Flag challenge, as part of the World of Science — Computer Security enrichment programme. Source: DSO.

The World of Science — Computer Security is a four-day enrichment programme held during the June school holidays, as part of the Young Defence Scientist Programme. The module covers a wide spectrum of cyber issues, including network, mobile, hardware and web security. Eager students get to learn first-hand from experienced DSO researchers working in the field. Participants are also exposed to both defensive and red-teaming cyber techniques, including intrusion detection, threat hunting, digital forensics, software vulnerability discovery, and software exploitation. For the more advanced students, they are challenged with more complex topics such as binary analysis to understand the deep internal workings of software.

Last year, DSO hosted 25 students across 12 schools for the module, which culminated in a seven-hour Capture-the-Flag challenge to test the skills they learnt from the course. The experience did not end there as these students also got an opportunity to intern at the Young Defence Scientists Programme's research programme, where they got to work alongside DSO mentors on actual research projects.

Hwa Chong Institution — MINDEF Cyberthon

Cyberthon 2019 was an inaugural cybersecurity competition for Junior College (JC) and Centralised Institute (CI) students. It was organised by Hwa Chong Institution (HCI), and supported by MINDEF's Defence Cyber Organisation (DCO) and Centre for Strategic Infocomm Technologies (CSIT).

The competition aimed to excite and inspire students in cybersecurity by providing glimpses of the varied and important roles of a cybersecurity professional. This competition was organised exclusively for JC and CI students, and brought together 96 students from 15 different schools to compete on 6 July 2019.

The Cyberthon comprised a pre-competition training phase followed by the competition. The training was designed to impart fundamental cyber knowledge and skills to students. The competition adopted a Jeopardy-style "Capture the Flag" format, which was suitable for students with minimal hands-on experience in computer science and cybersecurity. The students had opportunities to test their cybersecurity abilities across a variety of challenges including cryptography, penetration testing and web exploitation.

Such competitions are part of MINDEF's efforts to increase interest in cybersecurity and develop a talent base in this field. Students interested in considering a career in cybersecurity can apply for any of the diverse cybersecurity opportunities that MINDEF has to offer, such as the Cyber NSF (Full-time National Service) Scheme which allows enlistees to utilise their cybersecurity skills during their National Service. In addition, youths can apply for the CSIT Undergraduate Scholarship, which is awarded to individuals who are passionate about exploring technologies to advance Singapore's national security.

Pillar Four:

Strengthening International Partnerships

Representatives from the ASEAN Member States reaffirmed their commitment to a rules-based international order in cyberspace at the 4th AMCC, held as part of SICW 2019. Source: CSA.

Singapore believes in the importance of a rules-based international order for cyberspace. International law should thus apply to cyberspace, which will provide greater stability and predictability in the way countries and other actors behave. A trusted and secure cyberspace is a critical enabler for economic progress and a vibrant digital economy. As cyber threats are transboundary and ever-evolving, it is in Singapore's continued interest to work with partners internationally and regionally through dialogue, exchanges and capacity building.

Bilateral Cooperation

In 2019, CSA signed Memoranda of Understanding (MOUs) with New Zealand and the Republic of Korea. These MOUs increase professional exchanges and sharing of best practices for the benefit of Singapore's citizens and the region.

CSA has hosted study visits from Brunei, Indonesia and Thailand, and held Cybersecurity Roundtables with France and Russia. The engagements have helped to facilitate discussions and foster mindshare, in exploring ways on how countries could work together to combat cyber threats.

Regional Cooperation

Facilitating regional discourse on cybersecurity through the 4th AMCC

The 4th ASEAN Ministerial Conference on Cybersecurity (AMCC) in October 2019 built on outcomes of the 3rd AMCC, and saw further discussion on key emerging cybersecurity issues, in particular, the need for a formal coordination mechanism to coordinate cybersecurity efforts across the three pillars and relevant sectoral bodies in ASEAN. In response, Singapore, with input from ASEAN Member States, has drafted the ASEAN Cybersecurity Coordination Mechanism Proposal Paper. Participants at the AMCC also agreed to establish a working-level committee to develop a long-term regional action plan to ensure effective and practical implementation of the 11 voluntary, non-binding norms recommended in the 2015 Report of the United Nations Group of Governmental Experts (UNGGE) on Developments in the Field of Information and Telecommunications in the Context of International Security.

Stepping up capacity building efforts through the new ASCCE

Launched in October 2019, the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) provides a cutting-edge physical facility to carry out capacity building programmes for ASEAN senior policy and technical officials. It adopts a multi-disciplinary, modular, multi-stakeholder and metrics-based approach by engaging top cybersecurity experts and trainers, in collaboration with ASEAN Member States, ASEAN Dialogue Partners, international partners, and the UN Office of Disarmament Affairs, to design and deliver cybersecurity capacity building programmes.

Featured Topic

Singapore's commitment to a Rules-Based International Order in Cyberspace

Mr David Koh (Commissioner of Cybersecurity and Chief Executive CSA) chaired the OEWG informal intersessional consultative meeting with industry partners, non-governmental organisations, and academia — the first ever event involving multiple stakeholders at the UN. Source: UN.

Singapore is committed to being a constructive participant at ongoing UN discussions to build a more resilient and trusted cyberspace. For the first time, Singapore was included in the UNGGE[45] which comprises experts from 25 states. The UNGGE held its first meeting in 2019 and will submit its final report to the UN General Assembly in 2021. Singapore also participates actively in the newly-established Open-Ended Working Group (OEWG).

[45] The work of the UNGGE focuses on the following topics: (a) existing and emerging threats; (b) how international law applies in the use of ICT; (c) norms, rules and principles of responsible behaviour of States; (d) confidence-building measures; and (e) capacity building.

> **"The efforts of CSA and its partners over past years to inculcate a culture of cyber awareness and resilience are starting to bear fruit. But by that very token, the interest of malicious actors in what we have is not going to go away. In the coming years, we can anticipate more sophisticated attacks from Advanced Persistent Threat groups, using ever more nuanced and sophisticated social engineering techniques and understandings of human behaviour. We are continually working on systems and people resilience, but we need to be especially mindful where this intersects with hardware and critical infrastructure. Cyber preparedness in the Ops-Tech domain is something CSA and its partners have particularly emphasised, with good reason: this domain is one where serious and lasting damage can be done if we let our guard down."**
>
> **Dr Shashi Jayakumar**
> Senior Fellow, S. Rajaratnam School of International Studies (RSIS),
> and Head, Centre of Excellence for National Security and Executive Coordinator, Future Issues and Technology

Looking Ahead

Cyber Trends to Watch

Defenders and adversaries are locked in a constant game of cat-and-mouse in the cyber domain. Technological advancement is a double-edged sword that may open up new business opportunities, but also result in an increased attack surface for potential abuse. This section highlights some of the key trends in cyberspace — and how they could potentially alter the rules of the cyber battlefield.

Looking Ahead

Cybersecurity Trends to Watch

NEAR-TERM

A Cloud of Crown Jewels

WHAT IS IT?

Organisations are increasingly moving to the **cloud** to address their data storage and computing needs. For many businesses, the use of cloud services means significant cost savings, as they no longer have to invest heavily on software and hardware. Furthermore, the mobility and reliability of cloud services provide huge convenience to users, who are now able to work on-the-go as long as they are connected to the Internet.

WHY DOES IT MATTER?

Cloud security is a shared responsibility between Cloud Service Providers (CSPs) and its users. CSPs are generally only accountable for the security of the infrastructure or services in the cloud, while its users are responsible for securing their data residing there. A common misconception is that CSPs will take care of absolute security in the cloud. As a result, some companies may view investments in additional cybersecurity measures as unnecessary expenses, and consequently end up with inadequate protection for their assets. In addition, as businesses become increasingly dependent on the cloud, services which are essential to operations are also deployed on the cloud. Threat actors may target these cloud services to maximise their profit as the cloud becomes an aggregation point which enables them to target various companies.

NEAR-TERM

Rise of the Machines — Boon or Bane

WHAT IS IT?

Artificial Intelligence (AI) involves machines simulating human intelligence processes to reason and perform tasks. The workplace has been revolutionised with the introduction of AI, which has helped companies automate tasks to a large degree. Businesses can also become more efficient through AI, as their digital platforms get "trained" and become smarter, performing better in various tasks. AI can also enhance an organisation's cybersecurity posture, by analysing user behaviour, identifying anomalies, and pinpointing irregularities within a network. This, in turn, enables organisations to detect threats and vulnerabilities more swiftly.

WHY DOES IT MATTER?

There is a lurking danger that AI may become weaponised by threat actors. Threat actors can possibly use AI to create malware that is capable of figuring out normal user behaviour patterns of the targeted network, and mimic the behaviour they have learnt to evade detection. In addition, threat actors can also use AI to execute attacks that can self-propagate over a targeted network by leveraging adaptive attack techniques based on network traits. Smart phishing is another AI-powered cyber threat which creates credible-looking lures specific to the victim, based on information gathered earlier about the target. AI will enhance the speed and success rate of cyber-attacks by sophisticated threat actors. The key to defending against AI-powered cyber-attacks could lie in the effective use of AI for timely threat detection and response.

MEDIUM-TERM

5th Generation (5G) — The New Era of High Speed Connectivity

WHAT IS IT?

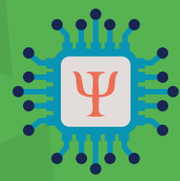
5th Generation communications (5G) heralds a new era of faster speeds and greater bandwidth which will relieve network congestion and improve the mobile experience. Beyond just connecting people, 5G will unlock the potential of connectivity with Internet of Things (IoT) devices in multiple aspects of life, from home and industrial automation to autonomous vehicles. This will precipitate a major change in essential networks, which in turn, will have long-term impact on a large range of applications in smart cities, manufacturing processes, and homes.

WHY DOES IT MATTER?

The transformative potential of 5G is made possible by its Software-Defined Networks (SDNs) and virtualisation technology. As such, the 5G telecommunication network can be subjected to cyber-attacks in traditional IT networks. Vulnerabilities can exist in SDNs like all software, and threat actors may leverage these software weaknesses in the 5G network to carry out malicious activities, such as surveillance and disruption of the network. Additionally, the versatility of 5G and its wide range of applications is expected to bring about a surge in IoT devices. This unfortunately creates a much expanded attack surface that threat actors can exploit to access targeted systems. There is a need to place greater focus on the security of mobile and IoT devices, as these are key to enhancing the cybersecurity posture of the 5G ecosystem.

LONG-TERM

Quantum Leap into the Unknown



WHAT IS IT?

Although **quantum computing** is still at a nascent stage of development, they are strongly predicted to disrupt and impact how industries operate. 2019 saw many breakthroughs in quantum computing, with Google's experiment taking 200 seconds to perform a task that would take the fastest supercomputer 10,000 years to complete. Quantum computers have the potential to become exponentially more powerful than today's supercomputers. Unlike the current binary model of computing adopted by classical computers, quantum computers work on millions of computations in parallel, which drastically reduces the time taken to complete any task.

WHY DOES IT MATTER?

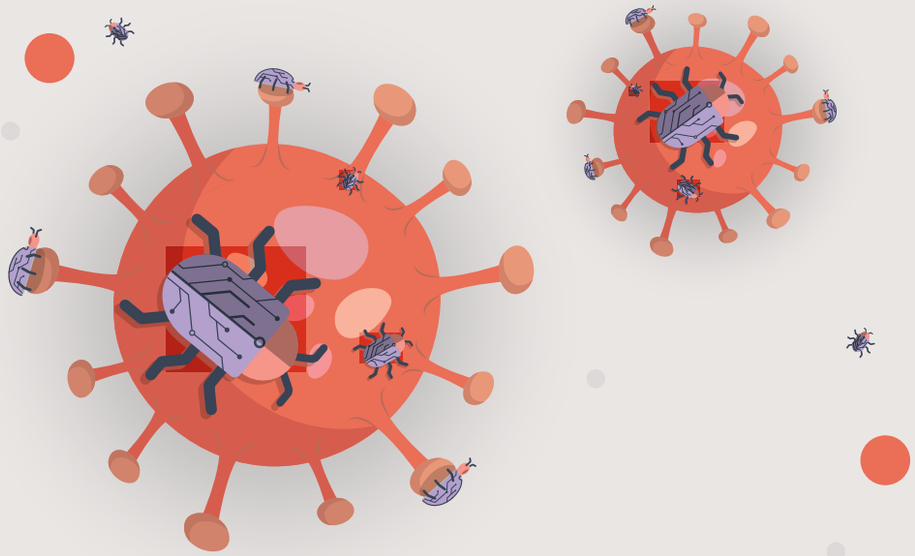
Quantum computing has the potential to break modern cryptographic systems that currently underpin cybersecurity. Hence, there are increasing concerns that quantum computing could pose a major security issue if leveraged by threat actors. A potential scenario would be threat actors capturing and storing encrypted data that is presently available, in the hope that quantum computers can decrypt the data in future. Reports have suggested that quantum computers that are capable of breaking conventional cryptographic algorithms within hours will likely exist by 2030.[46]

[46] Chen, Lily, Jordan, Stephen, Liu, Yi-Kai, Moody, Dustin, Peralta, Rene, Perlner, Ray, and Smith-Tone, Daniel. "NISTIR 8105, Report on Post-Quantum Cryptography," National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC), April 2016, https://csrc.nist.gov/publications/detail/nistir/8105/final.

Looking Ahead

Cybersecurity and COVID-19

Globally, cyber threat actors are exploiting the panic and fear caused by COVID-19 to conduct malicious activities. These actors range from cybercriminals seeking financial gain, to APT groups attempting to gain access to classified information.[47] Consequently, many Internet users have fallen victim to such activities, with cybersecurity vendors noting that the number of successful COVID-19-themed phishing attacks has been increasing throughout the first few months of 2020.[48]



[47] Henderson, Scott, Roncone, Gabby, Jones, Sarah, Hultquist, John, and Read, Ben. "Vietnamese Threat Actors APT32 Targeting Wuhan Government and Chinese Ministry of Emergency Management in Latest example of COVID-19 Related Espionage," FireEye Threat Research, 22 April 2020, https://www.fireeye.com/blog/threat-research/2020/04/apt32-targeting-chinese-government-in-covid-19-related-espionage.html.

[48] "Sophisticated COVID-19-Based Phishing Attacks Leverage PDF Attachments and SaaS to Bypass Defenses," Menlo Security Blog, 4 April 2020, https://www.menlosecurity.com/blog/sophisticated-covid-19-based-phishing-attacks-leverage-pdf-attachments-and-saas-to-bypass-defenses.

Broadly, threat actors targeting telecommuters have attempted to carry out malicious activities by exploiting vulnerabilities on two levels:

At the Infrastructure Level — Applications that facilitate telecommuting and remote collaboration have skyrocketed in popularity in the wake of the pandemic. However, these may contain vulnerabilities that malicious actors can exploit to sneak into meetings, or take over accounts to steal information; the Ministry of Education (MOE), for instance, moved quickly to suspend the use of video conferencing platform *Zoom* on 9 April 2020 after hackers hijacked a home-based learning class using it. In addition, the pandemic has also increased organisations' exposure to hacking attempts through their employees who are working from home, given that home networks are usually less secured than corporate networks.

At the Individual Level — Working from home may also result in occasional lapses in one's security consciousness. Under pressure to meet work targets amidst the challenges of working from home, people may show greater willingness to take on calculated security risks and trade-offs in order to get work done, such as discussing urgent classified work with colleagues over unsecured video conference calls. They may also exercise less discernment or caution than necessary when downloading telecommuting applications or Virtual Private Network (VPN) clients. This heightened cybersecurity risk appetite could increase the individual's exposure to hacking attempts.

Special Feature:

The Psychology Behind the Persistence of Phishing

Ms Teo Yi-Ling, Senior Fellow, Centre of Excellence for National Security, S. Rajaratnam School of International Studies

Phishing has emerged during COVID-19 as one of the most prominent delivery methods of cyber compromise, by preying on human emotion and cognitive bias to craft effective lures. Cyber threats are not always technological in nature — a chain is only as strong as the weakest link, and the human factor remains a distinct vulnerability. Threat actors may hence exploit human behaviour to achieve their aims.

Promoting Logic over Emotions?

Fear is one of the most powerful emotions, and fundamentally, phishing taps into the fears people have to such a degree that they are unable to carefully discern the signs of scam e-mails. Such e-mails appear to be from legitimate organisations or authorities that possess personal or confidential information of the recipient (banks or government agencies, for example), or whose services provide quality of life to the recipient (for example, those provided by Amazon, Apple, or Netflix).[49] Receiving such an e-mail may have the effect of triggering fear in the recipient, and fear, as observed above, reduces the ability to call on his or her ability for logical thinking.

The time at which a phishing e-mail is sent is also crucial — cybercriminals choose certain times when people may be most susceptible psychologically to being phished. Phishing works the least when people are focused on other urgent tasks at hand, and scam e-mails tend to be sent when recipients are least likely to be preoccupied with other matters, and may pay more attention to them. According to research, phishing activity appears to be high around lunch breaks, in the early afternoon, and at the end of the work week. It is all about trying to catch recipients off guard mentally.[50] Messages are targeted to appeal to specific psychological vulnerabilities, the most successful ones linking message with human factors, for example, time-limited communications designed to enact peripheral (i.e. emotional) rather than central information processing (i.e. logic).

[49] Irwin, Luke, "The psychology behind phishing attacks", IT Governance Blog, 1 August 2019, https://www.itgovernance.co.uk/blog/the-psychology-behind-phishing-attacks.
[50] Ibid.

How Social Engineering and Phishing Works

Apart from understanding the effects of instilling fear and provoking emotions, there are also some other psychological vulnerabilities that may explain why people continue to be phished. There has been extensive study and research on what psychological vulnerabilities cause people to fall for online scams, and these are summarised below:[51]

- **Authority.** In the right context, people tend to be very responsive and compliant to assertions of authority. This is even so when the person asserting authority is not physically present;
- **Commitment and consistency.** Society places a high value on people being committed to their promises (otherwise you are untrustworthy), and consistent in their behaviour (otherwise you are unpredictable and unreliable);
- **Reciprocation.** An established norm of social interaction — when someone gives us (or promises to give us) something, we tend to feel a strong inclination to give something in return;
- **Liking and similarity.** People tend to like people similar to them. Recognition of similar traits or characteristics is a mental shortcut in deciding to regard another person more positively; and
- **Scarcity.** If an item is indicated to be in short or limited supply, people tend to be extremely responsive to such indication, as scarcity is perceived as a threat. Research shows that people desire an item even more when they are given urgent cues that their ability to obtain it, is or may be limited in some way. Also, the perception that others might be competing for the limited supply of the item may increase the person's desire further.

Further, there is the phenomenon of people perceiving that they are invulnerable to phishing — people holding the belief that they would be able to spot a scam, and not fall victim to it. This is an example of optimism bias: the notion that people think that others are more vulnerable than they are. This mindset is associated with risk-taking, and the failure to heed precautionary advice and warnings.

[51] Cialdini, Robert B., Influence (Revised Edition 1993).

The unique circumstances wrought by COVID-19 continue to change and develop. Malicious cyber activities have been close on the heels of related developments, demonstrating that threat actors are highly adroit at adapting their tactics to the evolving situation. In the months since the first appearance of the coronavirus, global cyber threats leveraging the COVID-19 pandemic have escalated in three distinct phases:

PHASE 1 INCEPTION

JAN – FEB 2020

Capitalising on public fear and interest

Using COVID-19 to prey on insecurities and lure potential victims — Phishing and watering-hole attacks were observed as threat actors used pandemic-themed lures to impersonate official health authorities (e.g. World Health Organisation (WHO)[52]) and spoof COVID-19-related information feeds.[53] Anxious and eager for information or advice during the initial outbreak, members of the public were more likely to take the bait and follow instructions of seemingly credible e-mails or text messages that referenced the disease. It was also reported that the number of domain registrations (which started rising in mid-January) saw an additional spike in mid-February, which coincided with a large spike in COVID-19 cases — a possible explanation being that threat actors picked up on the attack opportunities arising from the pandemic during this phase.[54]

PHASE 2 EXPANSION

MAR – APR 2020

Growth of enterprise-centric attacks with new or broader attack surface

Amplifying the effectiveness and impact of cyber incidents — Threat actors understand that crises and emergencies can significantly intensify the impact of a cyber incident on critical infrastructure and sectors. The consequences of putting a fire brigade out of action are not nearly as serious when there is no fire, as when there is. The healthcare sector, which was incessantly spoofed by threat actors in Phase 1, now became a target itself. This proved especially insidious given that malicious cyber activities targeting frontline organisations battling COVID-19 not only target the personal details of patients, but also disrupt medical care and put human lives at stake. For example, there were reports of large-scale Distributed Denial-of-Service (DDoS) attacks targeting hospitals in France[55], ransomware attacks against the Illinois public health agency in the USA, as well as a major cyber-attack against Brno University Hospital in the Czech Republic. This phase also saw the launch of malicious cyber activities against companies providing important services during this period, such as Ransom Denial-of-Service (RDoS) attacks on a food delivery

[52] Ducklin, Paul. "Coronavirus 'safety measures' email is a phishing scam," Naked Security by Sophos, 5 February 2020, https://nakedsecurity.sophos.com/2020/02/05/coronavirus-safety-measures-email-is-a-phishing-scam/.
[53] Cao, Elliot, C. Chen, Joseph, Gamazo Sanchez, William, Wu, Lilang, and Xu, Ecular. "Operation Poisoned News: Hong Kong Users Targeted With Mobile Malware via Local News Links," Trend Micro, 24 March 2020, https://blog.trendmicro.com/trendlabs-security-intelligence/operation-poisoned-news-hong-kong-users-targeted-with-mobile-malware-via-local-news-links/.
[54] "Capitalizing on Coronavirus Panic, Threat Actors Target Victims Worldwide," Insikt Group, 12 March 2020, https://www.recordedfuture.com/coronavirus-panic-exploit/.
[55] Fouquet, Helen. "Paris Hospitals Target of Failed Cyber-Attack, Authority Says," Bloomberg, 24 March 2020, https://www.bloomberg.com/news/articles/2020-03-23/paris-hospitals-target-of-failed-cyber-attack-authority-says.

service in Germany.[56] A sophisticated threat actor also reportedly set up a website masquerading as the internal e-mail system of WHO to steal credentials from its members[57], while other threat actors continued to capitalise on pandemic fears to spread malware via "real-time" maps of infection hotspots.[58]

Targeting new or broader attack surface — Many organisations implemented ad hoc systems and "work from home" arrangements as the COVID-19 outbreak grew, to contain the spread of the virus while maintaining business continuity. These arrangements often rely on digital infrastructure to operate, which expand the attack surface that threat actors can target. Cybersecurity firm Carbon Black reported that ransomware attacks increased by 148 per cent between February 2020 and April 2020, as the number of telecommuters increased by 70 per cent during the same period.[59]

PHASE 3 CONVERGENCE

APR – MAY 2020

Targeting the "man-on-the-street"

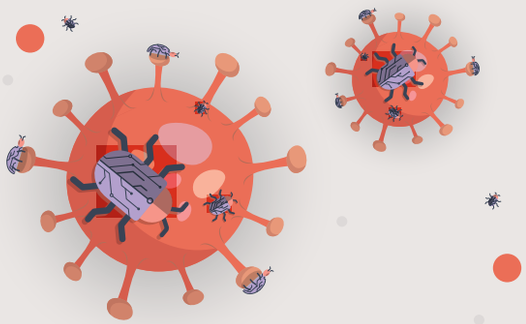
Exploiting business disruptions and new norms — As more stringent stay-home orders came into effect at the start of the second quarter of 2020, threat actors started to utilise specially crafted phishing lures on homebound individuals to obtain credentials or to deliver malicious payloads. Phishing lures have been observed to masquerade as an ever-widening array of services — shipment delay notices, messages from courier services, websites of popular streaming platforms, and even government agencies. Individuals looking for financial relief, government aid or personal loans became targets of phishing campaigns. As countries and citites gradually began relaxing various restrictions and exiting lockdown, phishing lures quickly adapted to spoof official information sites and resources on easing measures.

[56] "DDoS Attack Targets German Food Delivery Service," Dark Reading, 19 March 2020, https://www.darkreading.com/attacks-breaches/ddos-attack-targets-german-food-delivery-service/d/d-id/1337359.
[57] Satter Raphael, Stubbs, Jack, and Bing Christopher. "Exclusive: Elite hackers target WHO as corona virus cyberattacks spike," Reuters, 24 March 2020, https://www.reuters.com/article/us-health-coronavirus-who-hack-exclusive/exclusive-elite-hackers-target-who-as-coronavirus-cyberattacks-spike-idUSKBN21A3BN.
[58] "COVID-19, Info Stealer & the Map of Threats — Threat Analysis Report," Reason Security, 9 March 2020, https://blog.reasonsecurity.com/2020/03/09/covid-19-info-stealer-the-map-of-threats-threat-analysis-report/.
[59] Upatham, Patrick and Treinen, Jim. "Amid COVID-19, Global Orgs See A 148% Spike In Ransomware Attacks; Financial Industry Heavily Targeted," VMWare Carbon Black, 15 April 2020, https://www.carbonblack.com/2020/04/15/amid-covid-19-global-orgs-see-a-148-spike-in-ransomware-attacks-finance-industry-heavily-targeted/.

CSA's Response to COVID-19

Since reports of coronavirus infections started proliferating around the world, CSA has heightened monitoring of COVID-19-related cyber threats and malicious activities.

Concurrently, CSA is working with Singapore's CII sectors to maintain cybersecurity resilience and readiness, and ensure the continuity of essential duties pertaining to incident response, crisis preparedness and digital forensics during the COVID-19 outbreak. To this end, CII Owners (CIIOs) have adopted split team arrangements for their critical cybersecurity functions and implemented precautionary cybersecurity measures. CSA also issues periodic alerts to CIIOs to share information on COVID-19-related malicious cyber activities and mitigation measures for safeguarding network gateways and network infrastructure devices.



As the country transitioned into DORSCON[60] Orange and subsequently into the "Circuit Breaker" period, CSA implemented a number of measures to mitigate the risks of the increased reliance on digital platforms and applications:

- Identifying a list of companies to continue providing cybersecurity services in support of CII sectors and Singapore's digital economy;
- Increasing public outreach, by pushing out advisories and infographics to businesses and the public, including tips on implementing secure remote work policies, using online meeting platforms safely, as well as measures to protect themselves from COVID-19-related malicious activities;
- Maintaining close ties with our foreign counterparts, exchanging best practices and information on the latest cybersecurity threats and vulnerabilities; and
- Collaborating with the Ministry of Health (MOH), Smart Nation and Digital Government Office (SNDGO) and GovTech to secure applications and online platforms implemented to support contact tracing and other important functions.

[60] The "Disease Outbreak Response System Condition" (DORSCON) is a colour-coded framework that shows the current disease situation in Singapore. In order of severity, DORSCON covers four levels, namely Green, Yellow, Orange, and Red.

Looking Ahead

Cyber incidents linked to COVID-19 are likely to persist so long as the pandemic continues to generate a high level of public interest. Even as the graphical curve of COVID-19 infections gradually flattens and we move closer towards normalcy, we anticipate the following cyber-related developments around the world:

Economy

There will be a stronger drive among businesses to digitalise and build capacity to operate remotely. During the pandemic, business owners will have realised the importance of moving online, in the event that they are required to suspend physical operations. This exponential rate of economic digitalisation will broaden the attack surface. However, unless businesses invest further in cybersecurity, they will face heightened risk of malicious cyber activities, such as ransomware, DDoS attacks, and data theft.

Telecommuters will continue to constitute a sizeable pool of potential targets for threat actors, as a significantly larger proportion of the workforce is likely to continue telecommuting compared to pre-COVID-19 levels.[61] This is especially since telecommuting will allow businesses to save on substantial overheads and maximise profits. Moreover, market demand may spur technology firms to devise platforms and solutions to improve the telecommuting experience by addressing productivity pitfalls and lessons learnt during the pandemic.

Government

With the economy reeling from the effects of the pandemic, the number of applications for government relief measures and grants will almost certainly increase. This may attract more phishing e-mails from cyber threat actors posing as government entities or eligible citizens and businesses. Official portals that receive and process such applications may also be at risk of being crippled by DDoS or ransomware attacks, an extended episode of which could cause widespread frustration and slow down recovery efforts.

Society

While the majority of the public would look forward to the resumption of their daily activities — from going to the theatre to shopping for clothes — many may choose to stick with the online alternatives. Continuing high demand for online entertainment, e-retail and delivery services could motivate threat actors to conduct further malicious activities against the most popular of these platforms.

[61] Dingel, Jonathan and Neiman, Brent. "How Many Jobs Can be Done at Home?" Becker Friedman Institute, University of Chicago, 16 April 2020, https://bfi.uchicago.edu/wp-content/uploads/BFI_White-Paper_Dingel_Neiman_3.2020.pdf.

Glossary

Term	Definition
Advanced Persistent Threat (APT)	An attack in which perpetrators successfully gain access to a targeted system, and stay undetected for a long period of time to exfiltrate, modify, or destroy critical data. APTs can also refer to the advanced, and often state-linked or state-sponsored threat actors that conduct extended campaigns, such as cyber espionage.
Attack Surface	Referring to all vulnerable resources of a system, or the sum of the points through which an attacker could try to enter an environment.
Bot/Botnet	An automated software program used to carry out specific tasks. A botnet is a network of compromised computers infected with malicious bots, controlled as a group without the owners' knowledge.
Brute-force attack	A trial-and-error method which involves trying various combinations of usernames and passwords repetitively to gain access into a computer system or website.
Command and Control (C&C) servers	Centralised devices operated by attackers to maintain communications with compromised systems (known as botnets) within a targeted 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 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.
Cyberspace	The complex environment resulting from the interaction of people, software and services on the Internet by means of technological devices and networks connected to it, which does not exist in any physical form. Singapore's cyberspace includes domain names with ".SG" or Singapore-mentions, Internet Protocol (IP) addresses used in Singapore, and Internet Service Providers (ISPs) located here.
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 log-in wall (e.g. paid journal subscriptions).
Data Breach	The unauthorised access, collection, use, disclosure, copying, modification, or disposal of personal data or confidential information in an organisation's possession or under its control.

Term	Definition
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.
Downloader	A type of malware which connects to another website or server to download, and sometimes run, other malware on an affected system.
Hacktivists	An individual or a 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, such as baby monitors, printers, televisions, and autonomous vehicles, that are connected to the Internet.
Malspam	Malicious spam or malware spam; spam e-mail that delivers malware, and usually includes malicious URLs or infected attachments.
Malware	Malicious software intended to perform unauthorised processes that will have adverse impact on the security of a computer system, such as virus, worm, Trojan horse, spyware and adware.
Personal Data/ Information	Data which, on its own (e.g. full name, NRIC number) or in combination with other available data (e.g. medical or educational information), can be used to distinguish or trace an individual's identity.
Phishing	A common technique used by threat actors to trick people (typically through e-mails) into divulging personal information, transferring money, or installing malware.
Ransomware	Malware that encrypts files on a victim's device, rendering them unusable until a ransom is paid, usually in the form of Bitcoin or other cryptocurrencies. It may spread through phishing e-mails that contain malicious attachments or links, or malicious pop-ups that appear when users access unsafe websites.
Spoofing	Tricking computer systems or other users by hiding or faking one's true identity. Commonly spoofed targets include e-mails, IP addresses, and websites.
Trojan	A type of malware which disguises itself as a legitimate software to trick users into downloading and installing it on their systems. Once activated, the malware will carry out malicious actions that it is designed for.
Watering-hole attack	A type of cyber-attack targeting a particular organisation, where malware is delivered from websites that are regularly visited by the organisation's members, and consequently infects its systems.

Contact Details

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

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

SingCERT

Hotline for incident reporting:
(+65) 6323 5052

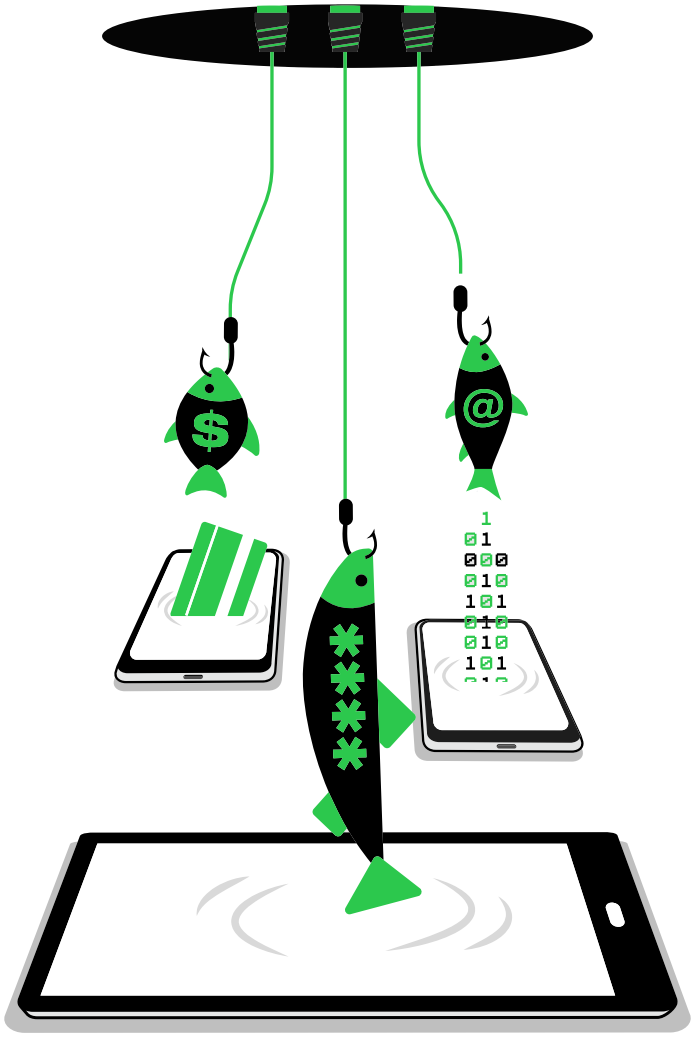
Cyber incident reporting form:
www.csa.gov.sg/singcert

If you wish to seek scam-related advice:

ScamAlert

Contact anti-scam helpline:
1800 722 6688

Visit ScamAlert website:
www.scamalert.sg



CSA SINGAPORE