SINGAPORE CYBER LANDSCAPE

2020

Singapore Cyber Landscape 2020

Copyright 2021
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; Government Technology Agency of Singapore; Operational Technology Information Sharing and Analysis Center (OT-ISAC); and the Singapore Police Force.

All rights reserved.

ISBN: 978-981-18-1420-4

The "Singapore Cyber Landscape 2020" publication reviews Singapore's cybersecurity situation in 2020 against the backdrop of global trends and events. CSA utilises multiple data sources to provide clarity on the common cyber threats observed in Singapore's cyberspace. CSA does not specifically endorse any third-party claim made in this material or related references, and the opinions expressed by third-parties are theirs alone. The enclosed facts, statistics and analyses are based on information available at the time of publication. The contents of this publication are provided on an "as is" basis without warranties of any kind. To the fullest extent permitted by law, CSA does not warrant and hereby disclaims any warranty as to the accuracy, correctness, reliability, timeliness, noninfringement, title, merchantability or fitness for any particular purpose of the contents of this publication. CSA shall also not be liable for any damage or loss of any kind caused as a result (direct or indirect) of the use of the publication, including but not limited to any damage or loss suffered as a result of reliance on the contents contained in the publication. CSA also reserves the right to refine its analyses as the threat situation evolves, and/or as further information is made available.

Contents

Foreword 4
Overview of Cyber Threats in 2020 6

Chapter 1
Spotlight on Cyber Threats 7

Stalking the Pandemic Trajectory 10

Effects of COVID-19 on the Cybersecurity Landscape 12
- COVID-19 and its Impact on Global Cybercrime 12
- Widened Attack Surface Bodes Ill for Data Security 13
- Intensification of Vaccine-related Cyber-attacks 14
- The Contact Tracing Conundrum 15
- TraceTogether App – Behind the Scenes 16

Topical Focus: Phishing and COVID-19 17
- COVID-19 Sparks Spike in Phishing Lures, Singapore not Spared 18

Topical Focus: Ransomware and COVID-19 19
- A Double Dose of Coronavirus and Ransomware 20

The SolarWinds Supply-chain Breach and Fallout 21

Chapter 2
WWW.TARGET.SG 24

Local Case Studies
- Case Study: SolarWinds Supply-chain Breach 26
- Case Study: Ransomware Incidents in Small and Medium Enterprises 27
- Case Study: Spate of Data Breaches Affecting Local Enterprises 28
- Case Study: Malicious Cyber Activity Targeting Public Agencies 29
- Case Study: Cyber Scams Targeting the Man-in-the-Street 29

Topical Focus: Malicious Command and Control (C&C) Servers and Evolution of Emotet Malware in Singapore 30
- The Evolution of Emotet 33

Strengthening the Resilience of the Critical Information Infrastructure (CII) Sectors 35
- Key Observations of the Operational Technology Landscape in 2020 35
- International Critical Infrastructure Security Showdown 37

Topical Focus: Observations on Local Website Defacements and GE 2020 38
- Delivering a Cyber-secure Singapore General Election 2020 39

Chapter 3
A Retrospective Look 40

Pillar 1: Building a Resilient Infrastructure 42
Pillar 2: Creating a Safer Cyberspace 44
Pillar 3: Developing a Vibrant Cybersecurity Ecosystem 46
Pillar 4: Strengthening International Partnerships 48

Chapter 4
Looking Back to Look Forward 50

A Retrospective of Threat Trends, and a Pondering on the Future 52

Cybersecurity Trends to Watch 55

Glossary 58
Contact Details 62

Foreword

"It was the best of times, it was the worst of times." So began A Tale of Two Cities, one of the best-known works of the great English writer Charles Dickens. This could easily apply to the year 2020, a transformative year that will be remembered for COVID-19 and the sweeping changes it engendered. On the digital front, the pandemic accelerated digitalisation efforts worldwide, impacting how we live, work and interact with one another. New apps and software were quickly developed to facilitate the needs of entire populations living in lockdown and for contact tracing.

Unfortunately, with accelerated digitalisation came cybersecurity challenges and threats as businesses and activities increasingly shifted online. Globally, state-sponsored Advanced Persistent Threat groups carried out a number of high-profile attacks on vaccine-related research, while cybercriminals capitalised on the widespread anxiety and fear wrought by the pandemic to conduct phishing campaigns and ransomware attacks for financial gain. Such trends were mirrored in the local cyber threat landscape, which saw spikes in both ransomware and COVID-19-related phishing activities. Just when the tumultuous year seemed to be winding down, the tail end of 2020 witnessed the game-changing SolarWinds cyber incident, in which hackers managed to gain access to many organisations by first compromising a trusted supplier. Cybersecurity threats to supply chains have been around for more than a decade, but the impact of the SolarWinds attack was unprecedented. Although there is no indication to date that Singapore was targeted, the incident is a stark reminder of the cybersecurity risks that all companies – big and small – face within their supply chains and when engaging third-party vendors, which is a near-certainty in today's highly-interconnected global economy.

People who thought that 2021 would be any different were quickly proven wrong. A number of high-profile data leaks affecting local organisations carried right over into the new year. The causes include technical and human error, as well as opportunistic hacks. Like supply-chain attacks, data leaks are not new, but have been occurring at an increasing frequency and at scale. However, it would be ransomware that dominates the headlines in 2021 so far. A spate of high-profile attacks against essential service providers and key firms grabbed global headlines. Ransomware is no longer a sporadic nuisance, affecting a handful of machines. It has been transformed into a massive, systemic threat affecting entire networks of large enterprises. This is now a major security issue that affects Critical Information Infrastructure (CII) sectors and nations.

Taken together, these shifts in our threat landscape over the past year underscore the diverse challenges in cybersecurity, which must be met by a whole-of-society effort and collective responsibility between stakeholders in the public and private sectors. The Government has and will always take the lead in national cybersecurity efforts. In 2020, the Cyber Security Agency (CSA) launched Singapore's Safer Cyberspace Masterplan, which laid out a blueprint to better protect Singaporeans and our enterprises in the online space. The Masterplan aspired to enhance the general level of cybersecurity in Singapore, and included initiatives such as the SG Cyber Safe programme to help firms improve their cybersecurity posture, and the Cybersecurity Labelling Scheme to raise cyber hygiene levels for smart devices.

CSA also undertook other steps to augment our collective cybersecurity in spite of the pandemic, outlined in this Singapore Cyber Landscape publication. CSA worked with our partner agencies, like the Government Technology Agency of Singapore and the Infocomm Media Development Authority, to ensure that contact tracing apps and digital solutions were securely implemented. Notably, Singapore organised our 18th General Election amid the pandemic, the first General Election where political campaigning activities were conducted mainly online – and which CSA helped to secure from a cybersecurity perspective. At the end of the year, when the SolarWinds incident was first disclosed, CSA immediately raised the alert level and apprised all CII sector leads of the situation, and worked with them to step up vigilance and daily monitoring.

The fight against COVID-19 is far from over. For Singapore to emerge stronger from this "crisis of a generation" that is COVID-19 and reap the benefits of a digitalised economy, cybersecurity will be front and center. We will continue to drive and implement cybersecurity measures to support our businesses and individuals, boost the resilience of our CII sectors, and work with international partners to coordinate cross-border efforts to combat cybercrime. CSA looks forward to working with partners from the public and private sectors, both locally and internationally, to co-create a safe, secure and resilient cyberspace.

Cybersecurity is a Team Sport. In fact, it is an International Team Sport. I look forward to partnering with all of you in this common endeavour.

#EmergingStronger #SGCyberSecure

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

Overview of

Cyber Threats in 2020

CYBERCRIME IN SINGAPORE

16,117

Cybercrime cases accounted for

43%

of overall crime in 2020

ONLINE CHEATING

2020: **12,251**
2019: **7,580**
2018: **4,928**

COMPUTER MISUSE ACT

2020: **3,621**
2019: **1,701**
2018: **1,207**

CYBER EXTORTION

2020: **245**
2019: **68**
2018: **80**

WEBSITE DEFACEMENTS

495

'.sg' websites were defaced, a sharp decrease of 43% from 873 cases in 2019

RANSOMWARE

89 ransomware cases were reported to CSA, with cases hailing from the manufacturing, retail and healthcare sectors. This was a significant rise of 154% in cases over the whole of 2019

PHISHING

47,000 phishing URLs[1] with a Singapore-link were detected. A slight decrease of 1% as compared to 2019

NUMBER OF CASES SINGCERT HANDLED IN

2020: **9,080**

2019: **8,491**

COMMONLY SPOOFED GOVERNMENT ORGANISATIONS IN SINGAPORE:

- MINISTRY OF EDUCATION (MOE)
- MINISTRY OF MANPOWER (MOM)
- SINGAPORE POLICE FORCE (SPF)

COMMONLY SPOOFED SECTORS

- **TECHNOLOGY**
- **BANKING AND FINANCIAL SERVICES**
- **SOCIAL NETWORKING FIRMS**

AMAZON, PAYPAL AND FACEBOOK WERE COMMONLY SPOOFED BRANDS

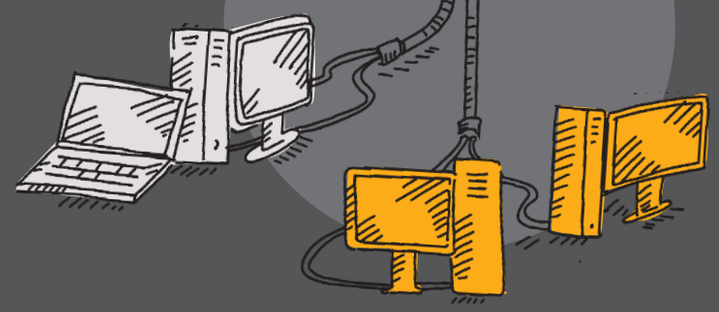
1. URLs — Uniform Resource Locators; colloquially termed web addresses.

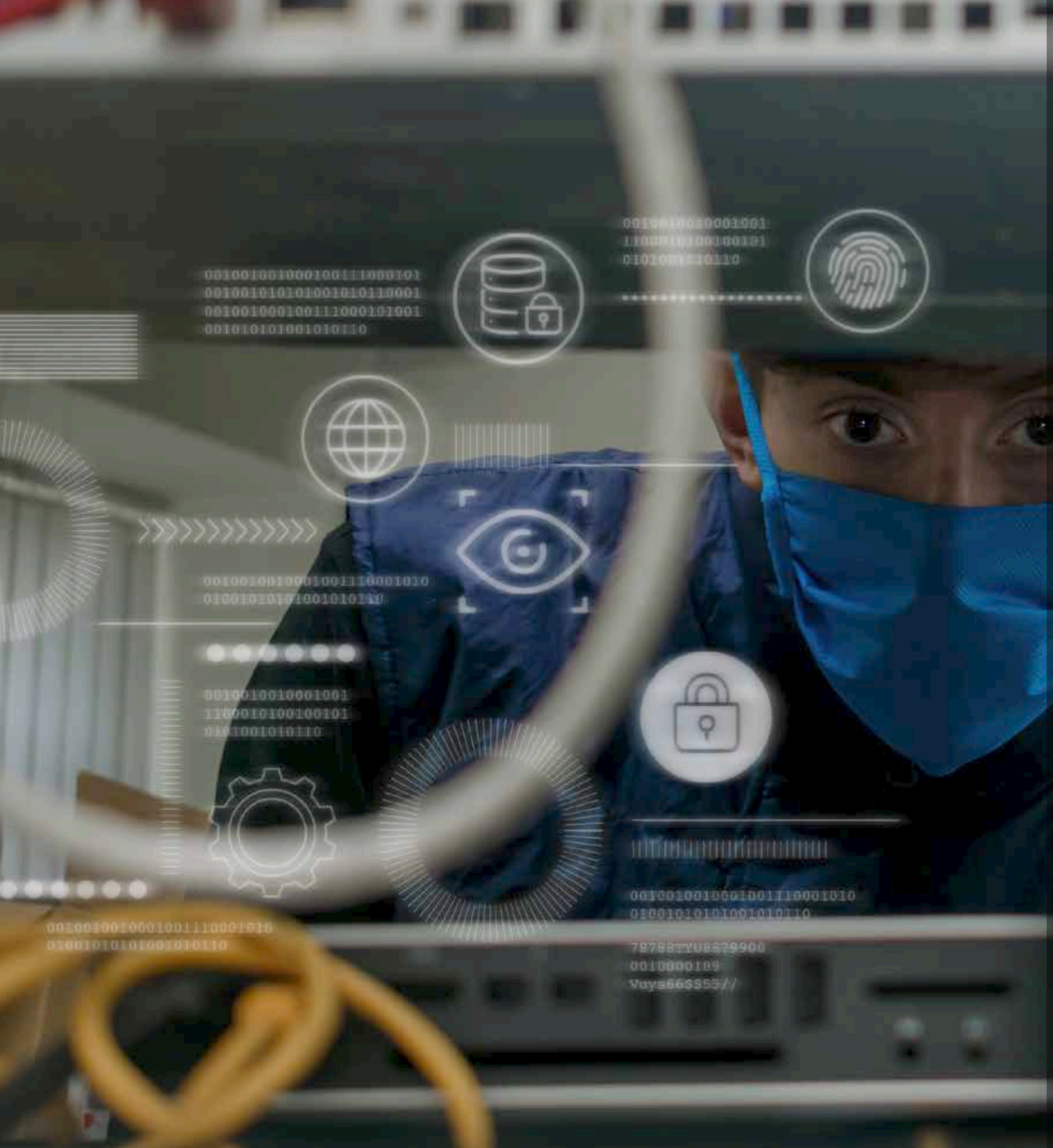
C&C SERVERS AND BOTNET DRONES

1,026 unique and locally hosted C&C servers were discovered, a spike from 530 recorded in 2019

About **6,600**

botnet drones were observed daily on average in 2020, also a significant increase from 2019's daily average of 2,300





Spotlight on Cyber Threats

In 2020, the global cybersecurity landscape was fraught with malicious cyber activities such as ransomware and phishing – a significant portion of which fed off and took advantage of the Coronavirus outbreak. Late in the year however, the world would be further stunned by news of a supply-chain breach that left thousands of companies worldwide vulnerable to attack. **Spotlight on Cyber Threats** delves into two pivotal cybersecurity issues in 2020 – **the cyber-repercussions of the COVID-19 pandemic, and the SolarWinds supply-chain attack**.

Stalking the Pandemic Trajectory

Throughout 2020, threat actors capitalised on a series of COVID-19-related milestones to carry out their malicious cyber activities. In Singapore, observations of COVID-19-related cyber threats, such as phishing and ransomware, were generally in line with global trends and coincided with the rise of work-from-home arrangements, as individuals and businesses adopted new technologies to maintain business continuity. With the increasing reliance on digital infrastructure and keen public interest in vaccine developments and distribution, threat actors are likely to continue adjusting their tactics to match the pandemic's trajectory[2].

Dec 2019 - Mar 2020

Coronavirus spread across the globe. Singapore reported first case. World Health Organisation declared COVID-19 a pandemic.

Global Observations

- Customisation of lures.
- Healthcare sector a key target.

Local Observations

Mar - May 2020

More than one-third of humanity under some form of lockdown. Singapore's Circuit Breaker measures kicked in.

Global Observations

- Peak in phishing lures targeting homebound individuals, relief and stimulus measures.

- Ransomware escalated.
- Rise in data leaks and credentials put up for sale.
- Cyber espionage of COVID-19 research heated up.

Local Observations

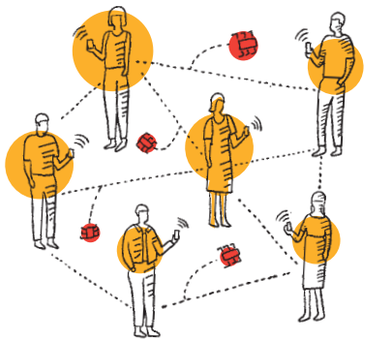
- Spike in COVID-19-related phishing, scams and ransomware cases.
- Zoom for home-based teaching suspended after lesson hijacking incident.
- Key targets: Healthcare, Education.

Jun - Jul 2020

Global cases surpassed 10M. Singapore moved into Phase 2 of reopening. Countries started to ease lockdown measures.

Global Observations

- Pivot to exploit vulnerabilities in contact tracing app technology.
- Telecommuting workforce and online users constantly targeted by social engineering lures.



Local Observations

- 12 fake COVID-19 contact tracing apps, including fake TraceTogether app, with the ability to deliver malware detected.

- Singapore a target of global phishing campaign on government support.

Aug - Dec 2020

Resurgence of cases globally as countries try to restart economies. Rollout of approved vaccines globally.

Global Observations

Intensification of vaccine-related cyber incidents

- Three APT* groups reportedly targeted seven COVID-19 vaccine makers.
- Cyber espionage and ransomware attacks targeted vaccine research centres, regulatory bodies (European Medicines Agency hack), and vaccine distribution channels.
- Authorities warned of surge in vaccine-related cybercrime.

Local Observations

- Increasing trend of Business Email Compromise (BEC) and data breaches/leaks.

- Alert by Singapore Police Force warning of vaccination scams.

2. The observations covered in the timeline were derived from reports from cybersecurity firms, online sources and media reports.
*Advanced Persistent Threat.

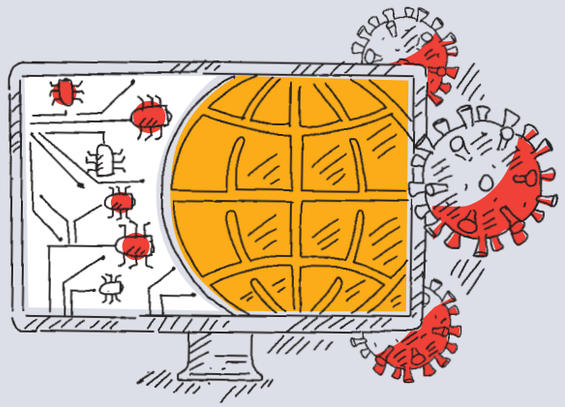
Effects of COVID-19 on the Cybersecurity Landscape

COVID-19 and its Impact on Global Cybercrime

CONTRIBUTION BY THE SINGAPORE POLICE FORCE

The ongoing COVID-19 pandemic sparked a global surge in cybercrime in 2020. People and businesses shifted activities online due to social distancing requirements in the physical world. The digital acceleration provided more opportunities for cybercriminals to exploit victims through vectors such as Business E-mail Compromise (BEC) scams and security intrusions via Internet-of-Things (IoT) devices. This shift in the cyber threat landscape can be expected to continue for the foreseeable future, as remote working measures and online transactions become even more prevalent in 2021.

Cybercriminals were swift to exploit fears and anxieties about COVID-19 to deceive victims[3]. These included the impersonation of government or health agencies[4], and creation of thousands of malicious COVID-19-related websites for credentials theft, malware distribution, and fraudulent peddling of fake cures and vaccines[5]. As the pandemic continues to afflict nations, and amidst the development of vaccines and implementation of



In Singapore:

384 **COVID-19-related scams reported in 2020**

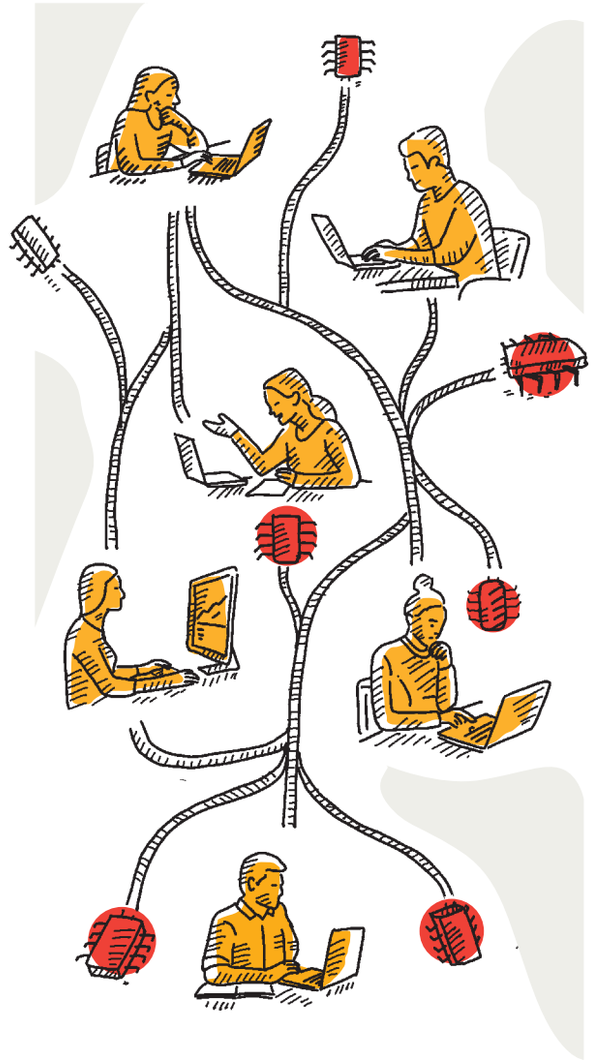
population inoculation plans across the world, the use of contextual criminal lures in phishing will likely remain a favoured tactic.

Meanwhile, as fears and anxieties around COVID-19 persist, cyberspace could become fertile ground for contention and provocation. Digitalisation has sped up and widened the deliberate circulation of fake news and misinformation, which reinforces existing tensions and prejudices. Cyberspace may end up hosting launch points for cyber-attacks[6] and hybridised criminal threats against the physical world.

3. "COVID cybercrime: 10 disturbing statistics to keep you awake tonight", 15 September 2020 - https://www.zdnet.com/article/ten-disturbing-coronavirus-related-cybercrime-statistics-to-keep-you-awake-tonight/.
4. "COVID-19 Phishing Update: Threat Actors Impersonating CDC, WHO", 26 March 2020 - https://info.phishlabs.com/blog/covid-19-phishing-update-threat-actors-target-cdc-who.
5. "Thousands of COVID-19 scam and malware sites are being created on a daily basis", 18 March 2020 - https://www.zdnet.com/article/thousands-of-covid-19-scam-and-malware-sites-are-being-created-on-a-daily-basis/.
6. "INTERPOL report shows alarming rate of cyberattacks during COVID-19", 4 August 2020 - https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19.

Widened Attack Surface Bodes Ill for Data Security

The commencement of government-enforced lockdowns caused consumers and employees to migrate to remote working *en masse*, often hastily, to minimise physical contact and the spread of COVID-19. This had two important implications for cybersecurity. First, this abrupt migration forced enterprises to adopt technological solutions and workarounds, such as cloud-based storage and video conferencing platforms, to facilitate telecommuting. The need to maintain business continuity meant companies had little time to stress-test the cybersecurity of the underlying technology and new work processes. Second, this sudden shift also greatly expanded the cyber-attack surface, as the spike in telecommuters resulted in a much larger pool of potential targets for hackers. US telecommunications firm Verizon reported that for the period between March 2020 and June 2020, 474 data breaches were recorded globally, of which 36 incidents were identified as being directly related to the pandemic[7].



With the upwelling of online transactions brought about by more people shifting work and leisure activities online, the attack surface has further expanded, providing more avenues for threat actors to exploit. In Singapore, several local companies were affected by data breaches and leaks. The causes ranged from security lapses with third-party service providers to cloud assets that were accessible from the open Web. Hackers were also observed to be selling the stolen data on hacker forums.

Another development that is becoming increasingly correlated with the increase in data breaches is the rise in ransomware attacks. The frequency of data breaches is expected to remain high, especially as ransomware operators widely adopt the tactic of threatening to leak data if their ransom demands are not acceded to.

7. "Analysing the COVID-19 data breach landscape", 4 August 2020 - https://enterprise.verizon.com/en-sg/resources/articles/analyzing-covid-19-data-breach-landscape/. Verizon collected non-incident data from contributors (Recorded Future and KnowBe4) and obtained incident data in the form of 35 publicly disclosed incidents gathered for their Vocabulary for Event Recording and Incident Sharing (VERIS) Community Database (VCDB) project. Verizon noted that this article is not solely based on data, but also includes their observations and anecdotal sources.

Intensification of Vaccine-related Cyber-attacks

The various global efforts to develop an effective vaccine for COVID-19 have led cyber threat actors to expand their operations to encompass the entire vaccine value-chain, including research, production, regulation and distribution.

Firms within this supply chain are likely to remain prime targets for both state-sponsored threat actors and financially motivated cybercriminals. In November 2020, Microsoft reported that several state-sponsored APT groups had targeted seven companies directly involved in COVID-19 vaccine research and development, for the purpose of data theft[8]. At around the same time, Europe's drug regulator, the European Medicines Agency, was breached by hackers who "unlawfully accessed" documents related to Pfizer and BioNTech's COVID-19 vaccine.

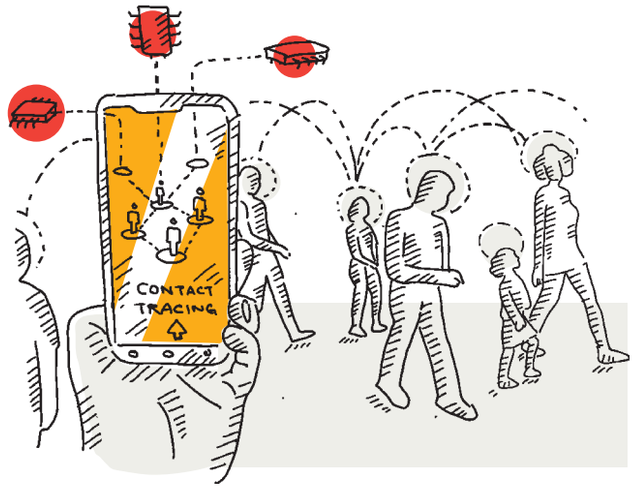
Cybercriminals did not waste any chance to exploit the pandemic as the distribution of COVID-19 vaccines ramped up towards the end of 2020. IBM Security warned of a sophisticated global phishing campaign which tried to harvest credentials from companies across six different countries specialising in the "cold chain" logistics to transport COVID-19 vaccines. With the stolen credentials, threat actors may be able to gain access to corporate networks and sensitive information related to vaccine distribution.

Successful attacks against organisations in the healthcare, pharmaceutical and other sectors involved in pandemic response could severely hamper frontline COVID-19 recovery efforts. Global law enforcement agencies[9] have issued alerts warning of a surge in organised crime activity tied to COVID-19 vaccines, including schemes to sell counterfeit vaccines on the Dark Web, as well as cyber-attacks targeting supply-chain companies. Locally, the Singapore Police Force (SPF) urged public vigilance towards vaccination-related scams as the Ministry of Health (MOH) commenced nationwide vaccination operations in February 2021.

8. "APT Groups Target Firms Working on COVID-19 Vaccines", 13 November 2020 - https://www.bankinfosecurity.com/microsoft-warning-a-15363.

9. Interpol warned of the organized crime threat to COVID-19 vaccines and Europol warned that the COVID-19 vaccine rollout will be vulnerable to fraud and theft.

The Contact Tracing Conundrum



Historically, contact tracing has been core to disease control efforts. Research has shown that disease transmission can be reduced through the tracing and isolation of a sick person as swiftly as possible. Globally however, many contact tracing apps developed in response to the COVID-19 pandemic have been fraught with adoption obstacles, fuelled by reports of app vulnerabilities.

The pressure that governments worldwide faced in quickly developing contact tracing systems to contain the spread of the virus often led them to prioritise functionality over security. Throughout 2020, security researchers reported bugs and vulnerabilities in official contact tracing apps that a number of countries introduced, ranging from leaving the data that the app collected unencrypted, to letting hackers modify the data of persons currently in quarantine. In response, UK's National Cyber Security Centre (NCSC) and the team behind the UK government's contact tracing app (NHSX) published the technical details of the app including its code, to demonstrate the app's capabilities and to get peer review through a vulnerability disclosure programme.

The Contact Tracing Con

In early June 2020, cyber researchers uncovered fake COVID-19 contact tracing apps that imitated the Android versions of 12 official government-issued apps[10], including Singapore's TraceTogether. Sophisticated threat actors were exploiting the COVID-19 theme by developing fake apps with the aim of compromising and harvesting information stored on victims' devices. The fake apps were distributed by various threat actors through other channels outside the official Google Play Store (e.g. third-party app stores). Such schemes demonstrated how threat actors were able to exploit the trust that people placed in apps released by government agencies.

10. "Anomali Threat Research Identifies Fake COVID-19 Contact Tracing Apps Used to Download Malware that Monitors Devices, Steals Personal Data", 10 June 2020 - https://www.anomali.com/blog/anomali-threat-research-identifies-fake-covid-19-contact-tracing-apps-used-to-monitor-devices-steal-personal-data.

TraceTogether App – Behind the Scenes

CONTRIBUTION BY GOVERNMENT TECHNOLOGY AGENCY OF SINGAPORE

TraceTogether was developed by the Government Technology Agency (GovTech) and the Ministry of Health (MOH) to support Singapore's response to the COVID-19 pandemic and facilitate faster contact tracing to curb the spread of the virus. Citizens could choose from two options – mobile app or physical token. The mobile app was developed in a short span of eight weeks and released on 20 March 2020.

Due to the critical role of TraceTogether in Singapore's contact tracing efforts, it was paramount to ensure that security was taken into consideration even with the rapid pace of development. GovTech's Cyber Security Group (CSG) collaborated with its developers throughout the development process to ensure that security was built into the design, and not as an afterthought. In addition, active security testing enabled vulnerabilities to be discovered and remediated early. TraceTogether Tokens are also labelled under Level Four of CSA's Cybersecurity Labelling Scheme (CLS), which means the Tokens are secure by design.

CSG considered security and privacy requirements while designing the software, hardware, communication channels and backend architecture of TraceTogether. Once the design had been implemented, CSG proceeded to conduct a series of security assessments to validate the effectiveness of security measures and uncover vulnerabilities for timely remediation with the support of the Smart Nation and Digital Government Group (SNDGG), MOH, CSA and other Government security agencies. This agile and collaborative security assessment approach ensured the successful and swift delivery of a secure TraceTogether product.

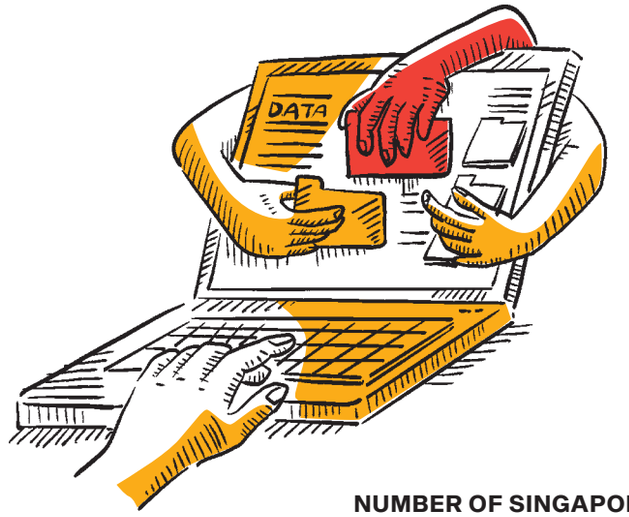
In total, CSG helped to assess and enhance the security of over 30 apps, amongst which were the TraceTogether, SafeEntry and GoWhere.sg product suites. These security assessments spanned diverse domains, including web/mobile app, IoT and cloud. Reflecting the spirit of SGUnited, this was achieved through the collaborative efforts of multiple Government agencies.

As the COVID-19 situation evolves, CSG will continue to work closely with Government agencies to bolster the security of key technological enablers that support Singapore's fight against the pandemic.

TOPICAL FOCUS

Phishing and COVID-19

1% URLS FROM 2019

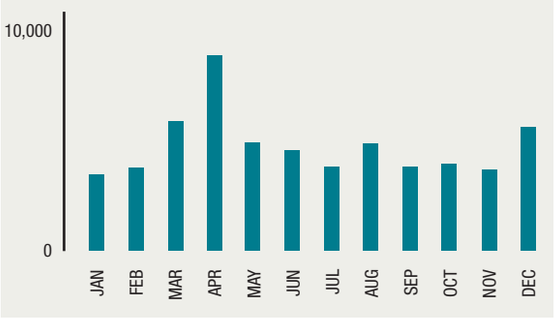


About 47,000 unique phishing URLs were observed in 2020, a slight decrease compared to the three-year record high of 47,500 URLs seen in 2019. Of these, more than half of the organisations spoofed were big technology or social networking firms (such as Apple, Facebook, LinkedIn and WhatsApp) and entities in the banking and financial sector (Chase Personal Banking, PayPal and Bank of America).

For the government sector, the SPF, the Ministry of Manpower (MOM), and the Ministry of Education (MOE) remained the three most commonly spoofed Singapore government agencies. Many of these cases were phishing e-mails spoofing these government agencies, in attempts to elicit favourable responses by invoking authority.

Facebook was overall the top spoofed brand in 2020, especially in the months of September to December 2020. This could be due to threat actors leveraging Facebook's announcement in September that they would be offering US$100 million in grants to businesses in over 30 countries affected by the COVID-19 pandemic.

NUMBER OF SINGAPORE-HOSTED PHISHING SITES IN 2020



COMMONLY TARGETED ORGANISATIONS

TECHNOLOGY

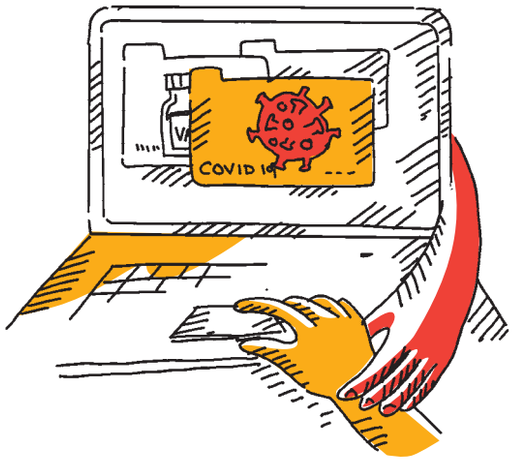
SOCIAL NETWORKING FIRMS

Apple, Facebook, LinkedIn and WhatsApp

BANKING AND FINANCIAL SECTOR

Chase Personal Banking, PayPal and Bank of America

COVID-19 Sparks Spike in Phishing Lures, Singapore Not Spared



Globally, 2020 saw a surge in phishing campaigns that leveraged pandemic-related references and spoofed relevant health authorities (such as the World Health Organisation). The range of themes broadened to capitalise on increased demands for services – including popular online shopping, streaming and web conferencing services (e.g. Amazon, Netflix, Zoom) – as countries entered government-enforced lockdowns to halt the spread of COVID-19.

In Singapore, while the overall volume of malicious phishing URLs remained comparable to the record-high seen in 2019, COVID-19 themes very likely accounted for over 4,700 of these malicious URLs spoofing local organisations.

This malicious activity was most pronounced in the period between March to May 2020, with some 1,500 malicious URLs observed – more than double the number from the preceding quarter. The increase was likely due to hackers attempting to spoof entities and services that were in greater demand during Singapore's circuit breaker period, which included online retail and payment portals.

This trend tapered off in July 2020 as cybercriminals switched tactics to exploit public interest in key events and developments. The number of phishing sites continued to rise towards the end of the year, likely the work of cybercriminals capitalising on developments such as COVID-19 vaccine research and distribution, relief efforts, as well as increased e-commerce activities during the holiday sales season.

TOPICAL FOCUS

Ransomware and COVID-19

154% CASES FROM 2019

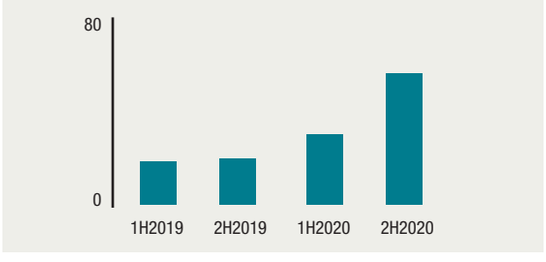
Ransomware types observed include older variants such as *Dharma/CrySIS, CryptoLocker* and *GlobeImposter*, as well as newer ones such as *Netwalker* and *REvil/Sodinokibi*

89 ransomware cases were reported to CSA in 2020, a significant increase from 35 cases reported in 2019. While most of the cases reported were from Small-and-Medium Enterprises (SMEs), ransomware operators were observed to be fishing for larger victims in the manufacturing, retail and healthcare sectors.

Based on the reported ransomware cases, these local incidents were likely related to, and a consequence of, the global ransomware outbreak. This latter phenomenon bore three distinct characteristics exemplifying the evolution of ransomware activities: (a) shifting from indiscriminate, opportunistic attacks to more targeted "Big Game Hunting (BGH)", i.e. targeting large businesses in hope of higher ransom pay-outs; (b) the adoption of "leak and shame" tactics, whereby victims' stolen data would be publicly leaked if ransom demands were not acceded to; and (c) rise in "Ransomware-as-a-Service" (RaaS)[11] models, which made sophisticated ransomware strains accessible to less technically-adept cybercriminals.

Indeed, ransomware strains detected in local ransomware cases, such as *REvil* and *Netwalker*, were observed to both operate under the RaaS model and leverage leak sites to pressure victims into paying their ransoms. As these trends gain further traction, Singapore organisations need to be increasingly vigilant against cyber threats. Beyond just backing up data regularly and storing it offline, organisations and companies need to put in place strong preventive measures to defend against the BGH trend. Ransomware no longer means a straightforward denial of access to one's data and systems, but now entails consequences that are more akin to a data breach.

NUMBER OF RANSOMWARE CASES REPORTED TO CSA IN 2020



11. "Ransomware-as-a-Service" employs an affiliate scheme where hackers focus on malware development, while relying on third parties to distribute their malware for a share of the ransomware "profits".

A Double Dose of Coronavirus and Ransomware

The pervasiveness of ransomware was never more pronounced than in 2020, as ransomware cartels innovated their tactics at an accelerating pace to ride on the pandemic wave. Globally, cyber researchers reported that ransomware incidents had increased 715 per cent year-on-year[12] in the first half of 2020; by the third quarter, there had been a 50 per cent increase in the daily average of ransomware attacks compared to the first half of the year[13]. The average ransom payment also saw a steady rise since the beginning of 2020[14] as ransomware operators scaled their tactics to target large enterprises.

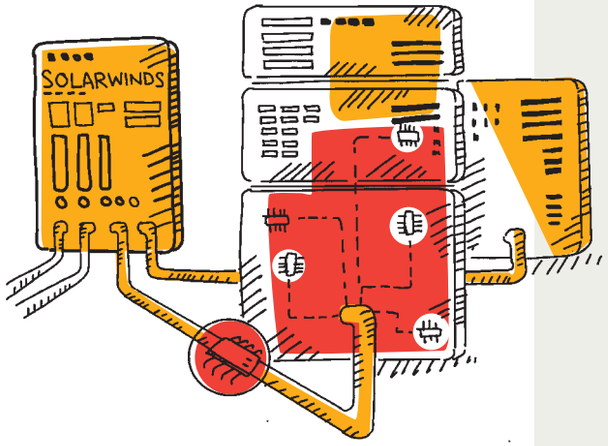
Globally, a spate of ransomware incidents was also observed targeting essential healthcare services during the pandemic, which caused disruption to several medical facilities and hospitals. There were instances where data was stolen from affected entities, in furtherance of the "leak and shame" tactic. One of the most high-profile cases happened to Düsseldorf University Hospital where a ransomware attack disrupted its treatment and emergency services, as well as its IT systems. An emergency patient had to be transferred to another hospital for treatment, and the delay in receiving care might have contributed to her death.

Notably, the monthly average number of local cases increased from April 2020, coinciding with the rise in work-from-home arrangements during the circuit breaker and post-circuit breaker period. It is possible that the rise in telecommuters and adoption of insecure practices to get work done during the prolonged lockdown periods contributed to the spike in ransomware cases. It is also observed that cybercriminals increasingly formed extortion cartels to collaborate and exchange tactics and intelligence.

With the shift in global focus to vaccine development and rollouts, ransomware operators are likely to evolve their campaigns accordingly and target the vaccine-related supply chains and industries.

12. "Bitdefender Mid-Year Threat Landscape Report 2020", 6 April 2021 - https://www.bitdefender.com/files/News/CaseStudies/study/366/Bitdefender-Mid-Year-Threat-Landscape-Report-2020.pdf.
13. "Global surges in Ransomware Attacks", 6 October 2020 - https://blog.checkpoint.com/2020/10/06/study-global-rise-in-ransomware-attacks/.
14. "Ransomware Demands continue to rise as Data Exfiltration becomes common, and Maze subdues", 4 November 2020 - https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report#payment.

The SolarWinds Supply-chain Breach and Fallout



Towards the tail end of 2020, the world witnessed the uncovering of a massive supply-chain attack where hackers targeted victims through their trusted vendor, US-based company SolarWinds, a dominant industry player which provides computer network monitoring services to corporations and government agencies around the world. Hackers infiltrated SolarWinds' production network and implanted malicious code[15] into software updates from *Orion*, SolarWinds' key network management software. Any organisation that downloaded the tainted updates effectively gave the hackers a backdoor into its network. The impact was worsened by the fact that the network management platform was commonly used by numerous Fortune 500 corporations and government agencies worldwide.

Anatomy of the SolarWinds Supply-Chain Attack

The hackers were patient and prioritised stealth to minimise exposure of their operations. Once inside the victims' networks, the hackers looked for ways to escalate their privilege[16], allowing them to abuse authentication mechanisms. They were observed to forge trusted tokens, which could grant them unrestricted access to the victims' networks, as well as assets housed in the cloud, such as e-mails. In this way, the hackers could roam the targeted network at will, as if they were a trusted employee. This made it extremely difficult to detect their presence within the network.

Around 18,000 organisations downloaded the tainted update and were exposed to the injected malware, which researchers named *Sunburst*. Of these, cybersecurity experts believed that the hackers targeted a much smaller group with follow-on activity. This smaller group comprised mainly US-based entities – US government agencies and leading technology companies, including the likes of Cisco, Microsoft and VMWare.

15. "Global Intrusion Campaign Leverages Software Supply Chain Compromise", 13 December 2020 - https://www.fireeye.com/blog/products-and-services/2020/12/global-intrusion-campaign-leverages-software-supply-chain-compromise.html.
16. Privilege escalation is an intrusion by unauthorised users by exploiting bug or vulnerabilities to gain elevated access status.

What is SUNBURST and how does it work?

Malware subverts and abuses trust within networks and systems

Gains initial access to on-premises network through the compromised software update	Lies dormant to evade detection; subsequently conducts extensive checks to ensure it is in the targeted environment	Gathers system info; calls out to C2 server; sends info to and receives commands from C2 server	Gains privileged access in components of the federated single sign-on infrastructure	Leverages privileged access to abuse federated authentication mechanisms	Forges trusted authentications to access cloud assets/resources

Manipulating trust in federated authentication environments to gain access to protected information in the cloud, and potentially broader access to data across network (on-premises or in the cloud)

The Chain Reaction

Supply-chain attacks are insidious and difficult to guard against because the attacks compromise part of the trusted information technology (IT) ecosystem. These often bypass organisations' cybersecurity defences, slipping in through upstream vectors. In addition, the complexity of modern supply chains makes defending against such attacks extremely difficult. While such attacks are not new, they are becoming more sophisticated.

NOTABLE SUPPLY-CHAIN ATTACKS

- Over one million ASUS users[17] were potentially impacted after attackers managed to inject a backdoor in the ASUS Live Update utility in a sophisticated supply-chain attack which took place in 2018, but was only discovered in early 2019. To hide the malicious activity, the actors also used a stolen digital certificate that ASUS signed legitimate binaries with.

- The actors behind the *NotPetya* incident in June 2017[18] targeted the update server of a widely deployed accounting software, M.E.Doc, to deliver the *NotPetya* ransomware. One of its most high-profile victims was global shipping conglomerate Maersk. The company suffered severe disruption to its operations and restored them only after 10 days as the ransomware spread throughout the core IT systems and prevented data access.

- In the third quarter of 2017, threat actors infiltrated popular software NetSarang and CCleaner, and corrupted software updates to deliver malware to their customers. These attacks were significant as these software products were widely used by businesses and individuals, and affected millions of users worldwide.

17. "Supply-chain Attack Used to Install Backdoors on ASUS Computers", 25 March 2019 - https://www.securityweek.com/supply-chain-attack-used-install-backdoors-asus-computers.

18. "The Chain Reaction", 4 May 2020 - https://www.csa.gov.sg/singcert/publications/the-chain-reaction.

The Domino Effect

The compromise of a single, trusted supplier – or a popular and widely-used product – can result in multiple victims, some of which could be major vendors themselves. The SolarWinds hack rendered large tech firms like Cisco Systems, Intel Corp and Microsoft susceptible to a second-level breach, whereby the attacker could further compromise other supply chains independent and distinct from SolarWinds'. This could potentially impact a far greater number of organisations and victims worldwide.

TAKEAWAYS

The SolarWinds breach fundamentally arose from a vulnerability in trusted software exploited by a sophisticated and advanced threat actor. Adeptly undermining authentication mechanisms, the hackers were able to disguise themselves as legitimate users in the network. To deal with such threats, there is a need to constantly monitor for anomalous activities and behaviour within networks. In the longer run, the 'zero-trust' model[19] would be crucial to enhancing organisations' cybersecurity posture against similar threats. In addition, the cybersecurity of supply chains is not purely an IT problem. Organisations will also need to adopt sound cybersecurity practices and processes in sourcing, vendor management and evaluation of supply-chain quality across multiple functions.

19. Zero-trust is a concept of network design that embraces two core principles: (i) trust no one – a regime of constant authentication and monitoring within a network, with continuous visibility and analytics; and (ii) least-privilege access – users being given only as much access as they need, to minimise each user's exposure to sensitive parts of the network.

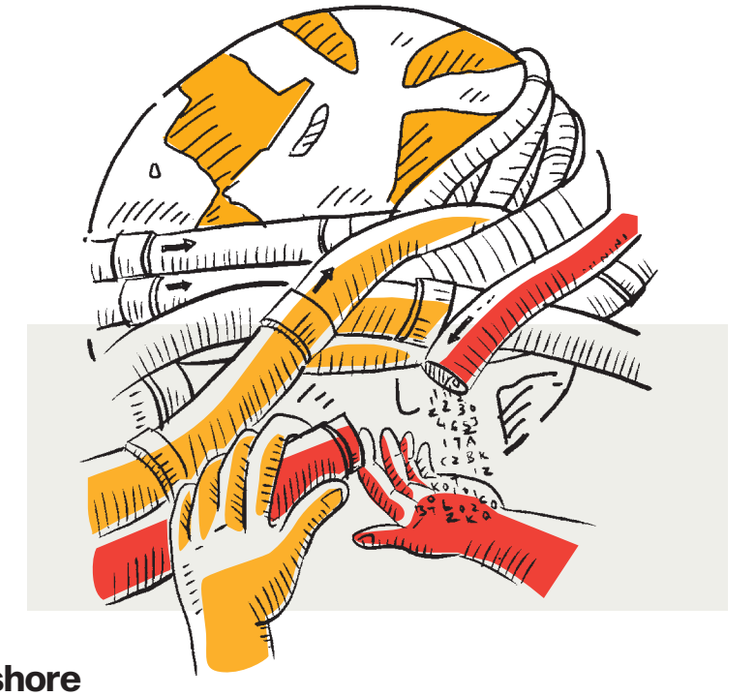
WWW.TARGET.SG

2020 proved to be a highly eventful year both in the physical and virtual worlds. As Singapore hunkered down to deal with the COVID-19 outbreak, the local cyber threat landscape saw an array of malicious cyber activities, many of which attempted to capitalise on the ongoing pandemic. In addition to ransomware and phishing, the prevalence of botnets and website defacements continued to be a cause for concern. This section highlights several cyber incidents in the form of case studies, observed trends in our local cyber landscape, and what we can learn from them.

Local Case Studies

This section features selected case studies of companies and individuals that were compromised by various cyber threats, and lessons that can potentially avoid a recurrence.

SolarWinds Supply-chain Breach



A Global Storm Blows Ashore

What Happened?

The interdependencies of the global technology supply chain meant that local systems were not spared the fallout from the SolarWinds breach. On 23 December 2020, a local organisation was observed to have been affected by the SolarWinds breach. One of the affected organisation's IT systems – which had SolarWinds *Orion* installed – had downloaded the infected update and thus became exposed to the malware. However, the hackers were subsequently found to have "deactivated"[20] the malware, possibly indicating that they were not interested in the organisation.

Follow-up Action

CSA investigated the incident and advised the company on the proper remediation measures, including scanning for related Indicators of Compromise (IOCs) and running anti-virus scans on all systems. No further suspicious activities, malicious processes or signs of intrusion were found.

20. Deactivated mode is when the malware has been disabled and will no longer perform any network activity.

Ransomware Incidents in Small and Medium Enterprises

Putting All Your Eggs in One Basket

What Happened?

In August 2020, staff from an F&B business discovered that their company servers and devices were infected with *NetWalker*, a prevalent ransomware strain. The ransom note instructed the victim to visit a webpage on the Dark Web to view the ransom demands. As the company had also stored its backups on the affected servers, none of its data could be recovered.

Follow-up Action

A report was made to the Singapore Police Force (SPF), and the company was also given a list of cybersecurity companies to assist in remediation efforts. However, as both primary and backup systems were affected by the ransomware, the company was unable to recover its data and had to rebuild its IT system from scratch.

Backing Up Instead of Backing Down

What Happened?

In September 2020, a creative firm suffered a ransomware infection resulting in the complete shutdown of three database servers, as well as the encryption of files within these servers. None of its data was observed to have been stolen. The ransomware involved, called *JungleSec*, was first discovered in late 2018 and is rarely observed in Singapore. It is known to infect servers through Intelligent Platform Management Interface (IPMI)[21] cards.

Follow-up Action

All three database servers were taken down and reformatted immediately after the incident. The databases were rebuilt from a backup from the previous day. The database servers as well as their IPMI interfaces, including the unaffected ones, were isolated and access was further tightened. A cybersecurity firm was engaged to assist with containment measures, review the company's data protection policies and processes, and conduct vulnerability assessment and penetration testing.

TAKEAWAYS

Prevention is key to avoid falling victim to ransomware. Organisations need to put in place strong preventive measures to secure their systems. These include measures such as formulating a backup and recovery plan, performing data backups regularly, storing data offline and not connected to the organisation's network as certain ransomware variants can propagate across the network.

21. IPMI is a set of computer interface specifications which are built into server motherboards or installed as an add-on card and allows remote administration of a computer.

Spate of Data Breaches Affecting Local Enterprises

Data Breaches Hit Home

What Happened?

In 2020, several Singapore-based enterprises were targeted by hackers, resulting in a series of data breaches involving sensitive customer data. In one case, over one million accounts in a local firm's customer database were affected. The database included the names, phone numbers and addresses, account passwords (which were encrypted) and financial details of the company's customers, which was later put up for sale online. The database, which was illegally accessed, had been hosted on a third-party cloud service provider.

Follow-up Action

The firm reported the incident to the Personal Data Protection Commission (PDPC) and worked closely with the SPF on investigations. The company swiftly alerted all affected users regarding the incident, commenced investigations and published a detailed statement on their website. They promptly blocked all unauthorised access to the exposed database and engaged a commercial vendor to strengthen their cybersecurity measures.

TAKEAWAYS

Threat actors are constantly probing for weak links to access, exfiltrate and monetise stolen credentials and personal data. With COVID-19 shifting transactions and services online, organisations have come to rely heavily on Internet-based workarounds such as cloud and mobile services, resulting in increased risks for both enterprises and consumers.

While there is generally no single cause for data breaches, there are typically several contributing factors. These include (a) errors by employees and/or insider threats; (b) security lapses within third-party service providers; and (c) misconfigured cloud settings. Such practices can lead to an organisation's assets and services becoming openly accessible to malicious threat actors, much like leaving one's front door open.

Malicious Cyber Activity Targeting Public Agencies

Phished by a "Colleague"

What Happened?

In early 2020, an officer from a statutory board received e-mails from a colleague's e-mail account requesting for an urgent transfer of more than $1 million dollars to an unfamiliar bank account. This suspicious request startled the officer, who reported the e-mail. He did not transfer the money. Investigations revealed that a cybercriminal had gained access to his colleague's account through a phishing e-mail, and sent a total of six e-mails to other staff to trick them into transferring money to the bank account.

Follow-up Action

The incident was reported to the SPF. Upon discovery, the credentials of the compromised e-mail account were reset to deny the hacker access. As a precaution, all officers in the statutory board were advised to change their e-mail account credentials, and notices were issued to enhance employee awareness about phishing scams.

Cyber Scams Targeting the Man-in-the-Street

Whats-Hacked!

What Happened?

In 2020, several members of the public lost access to their WhatsApp (WA) accounts after falling prey to social engineering scams. Scammers contacted would-be victims and pretended to be friends or family members pleading for help: they had lost access to their WA accounts, and needed a six-digit verification code that they had sent to victims' phones. In reality, the scammers had sent a One-Time Password (OTP) to transfer access of the victim's WA account to the hacker's own device. This resulted in the victims being locked out of their WA accounts. The scammers then used the compromised accounts to message the victim's contacts for information such as credit card details or their OTPs sent to their mobile numbers, in order to hijack additional devices or steal their victims' money.

TAKEAWAYS

The case studies highlight the prevalence of social engineering techniques, which continue to be popular among cybercriminals who are constantly customising their lures. Common attack vectors include bogus e-mails, compromised social messaging accounts and fake websites. Members of the public are reminded never to share their OTPs with anyone.

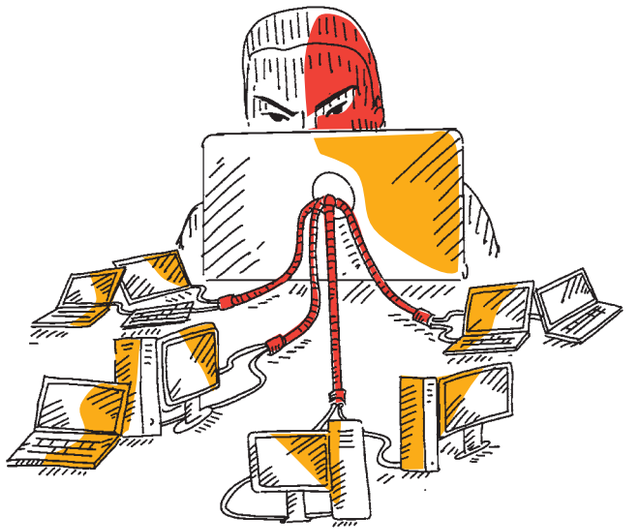
Follow-up Action

Both SingCERT and the SPF issued advisories alerting members of the public to be aware of such scams and to protect themselves by securing their WA accounts. Some of the measures include enabling the "Two-Step Verification" feature found in the settings of the app, and never sharing WA account verification codes with anyone.

TOPICAL FOCUS

Malicious Command and Control (C&C) Servers and Evolution of Emotet Malware in Singapore

94% CASES FROM 2019



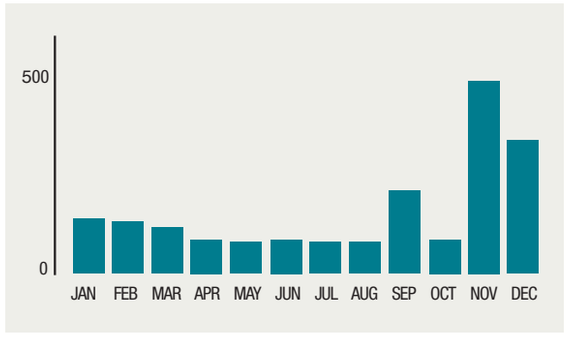
C&C Servers

Centralised devices operated by attackers to maintain communications with compromised systems (known as botnets) within a targeted network.

2020 saw a sharp rise in the number of malicious C&C servers observed locally, not least because of the resurgence of the Emotet malware in the latter half of the year. This section provides an overview of the C&C server and botnet drone threat landscape in 2020, before turning the spotlight to *Emotet* and its footprint in Singapore.

In 2020, CSA observed 1,026 unique C&C servers hosted in Singapore, a 94 per cent increase in cases from 2019. The large increase

UNIQUE C&C SERVERS OBSERVED PER MONTH IN 2020



was in part attributed to the increase in C&C servers distributing *Emotet* and *Cobalt Strike* malware, which accounted for one-third of the malware C&C servers observed.

Malware

Malicious software intended to perform unauthorised processes that will have adverse impact on the security of a computer system.

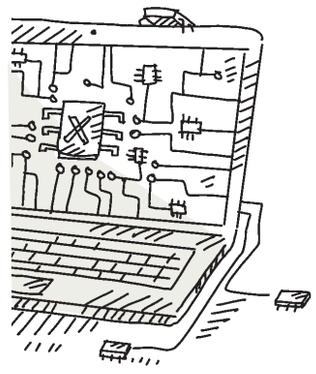
A common thread among the malware families observed was their focus on post-compromise distribution and reliance on C&C call-backs to identify critical systems within networks. Once these systems were breached, threat actors would then deploy other payloads such as ransomware to lock up or exfiltrate sensitive data and credentials.

Emotet operators appeared to follow a cyclical pattern, taking advantage of holiday periods (with increased Internet traffic and potentially weaker network defences due to staff being away[22]) to launch new campaigns[23]. This increase was especially pronounced during the holiday period from November to December 2020. In addition, *Emotet* operators also leveraged contextualised "phishing" lures capitalising on COVID-19-related themes such as vaccine developments to lure potential victims. They also partnered cybercriminal and threat actor groups utilising *Trickbot* malware and *Ryuk* ransomware to carry out damaging cyber-attacks. International law enforcement operations successfully dismantled most of *Emotet's* infrastructure in January 2021, but it remains to be seen if the malware has been eradicated for good.

Cobalt Strike was originally a paid penetration testing product that emulated adversarial threats for cybersecurity researchers to test network defences. However, it has since been abused by hackers to deploy malware through *Cobalt* "beacons" planted on infected hosts.

About 6,600 botnet drones with unique Singapore IP addresses were observed daily on average, a significant increase from 2019's daily average of 2,300. *Mirai* and *Gamarue* were the key malware types that contributed to the spikes in daily observations, accounting for a

Emotet and Cobalt Strike malware accounted for one-third of the malware C&C servers observed.



22. "GitHub-hosted malware calculates Cobalt Strike payload from Imgur pic", 28 December 2020 - https://www.bleepingcomputer.com/news/security/github-hosted-malware-calculates-cobalt-strike-payload-from-imgur-pic/.

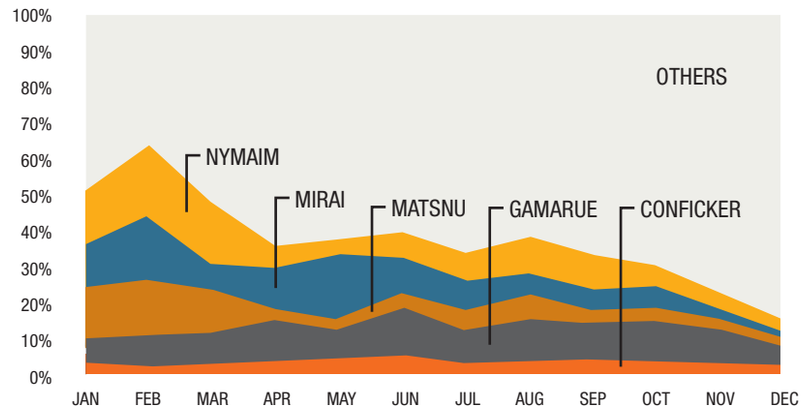
23. "Emotet returns just in time for Christmas", 23 December 2020 - https://blog.malwarebytes.com/cybercrime/2020/12/emotet-returns-just-in-time-for-christmas/.

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.

total of 25 per cent of infected Singapore IP addresses in 2020.

As with 2019, variants of the *Mirai* and *Gamarue* malware were most prevalent among infected botnet IP addresses in 2020. *Mirai* infections continued to stay strong with the growth of IoT devices locally, and new variants were observed to exploit known and recently discovered vulnerabilities alike. Globally, these malware types were also observed to increasingly target IoT devices to create large botnet armies to launch DDoS attacks[24]; similarly, *Gamarue* continued to account for a significant proportion of infected Singapore IP addresses in 2020 even though its bots have been dormant for several years, as *Gamarue's* infrastructure was dismantled in an international operation in December 2017. However, as long as these systems remain infected, there is always the possibility that these dormant botnets would be revived to carry out malicious activities. It is crucial that users scan and clean their systems regularly to purge them of malware.



24. "Mirai variant Mukashi conducts Brute-Force Attacks against Vulnerable NAS Devices", 23 March 2020 - https://securityintelligence.com/news/mirai-variant-mukashi-conducts-brute-force-attacks-against-vulnerable-nas-devices/.

The Evolution of Emotet

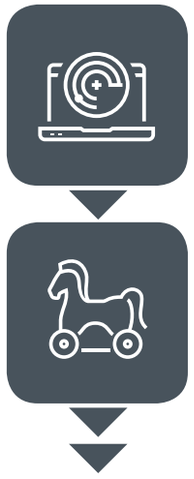
What is *Emotet*?

Emotet is a sophisticated Trojan functioning as a downloader/dropper of other malware. Spread primarily through phishing attacks using e-mails with malicious links or macro-embedded attachments, *Emotet* has been involved in multiple cyber-attacks since 2014. In June 2019, a ransomware attack via an *Emotet*-laced e-mail took out Lake City, Florida's local computer network, costing the city USD$460,000 to remediate. In 2020, the United Nations was also targeted by *Emotet* phishing campaigns.

Rise of *Emotet*

Emotet was initially a banking Trojan that stole financial information from online banking sessions. Its later iterations were observed to possess capabilities beyond mere information theft. As a banking Trojan-turned-botnet, *Emotet* evolved into a delivery platform for other malware, targeting many governments and organisations worldwide. Its resurgence in mid-2020 led to US authorities issuing an alert that labelled *Emotet* "one of the most prevalent ongoing threats".

Deconstructing an *Emotet* Attack



1
- Conducts reconnaissance to gain understanding of current affairs and topics of interest to target; contextualised lures are created.

2
- Spam emails with malicious attachments or links are sent to victims.
- Victims open documents with malicious macros that download *Emotet.*
- Other malicious payloads such as *Trickbot* and *Ryuk* are also delivered through backdoor vulnerabilities.

3
- Utilises various evasion techniques, lying dormant within sandbox environments, waiting for opportune moments to be triggered to achieve maximum impact.
- Leverages exploits (e.g. *EternalBlue*) to move laterally within the victim's network and identify key systems to serve as targets.

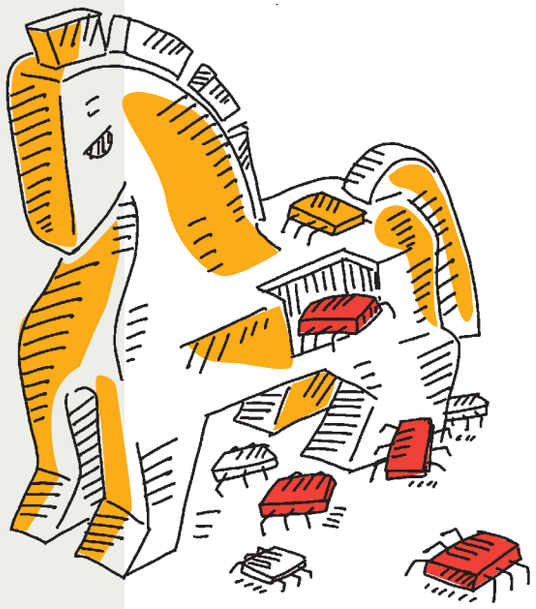
4
- Connects to remote C&C servers, downloads and installs additional modules to steal credentials, spoof emails and proliferate across connected vunerable devices on networks.
- Malicious malware installed runs on each endpoint to achieve respective objectives. In the case of a disruptive attack, the malware causes networks to be shut down, or may encrypt files while displaying a ransom note.

Emotet in Singapore

12,930 *Emotet*-infected drones with Singapore IP addresses were detected in 2020, compared to 6,008 in 2019 – a 115 per cent increase.

The number of local *Emotet* infections plunged as its operators went on a self-declared hiatus between early February to late June 2020, and picked up again from July onwards, mirroring a global resurgence in infections.

Local *Emotet* infections exhibited similar Tactics, Techniques and Procedures (TTPs) as those observed globally – sophisticated social engineering tactics, such as e-mail thread hijacking, employee impersonation and obfuscation by hiding malicious URLs within benign-looking URLs.



Implications

Emotet's sheer prevalence makes it a formidable threat. Based on numbers, *Emotet* was the most prevalent botnet in the world in 2019, with *Trickbot* its closest competitor[25], but also frequent partner-in-crime. A single device infected with *Emotet* can send a few hundred thousand spam e-mails in just one hour. The number of *Emotet*-infected drones with Singapore IP addresses detected in 2020 shows that as we continue to digitalise, our networks will be increasingly exposed to global cyber threats.

In January 2021, Europol announced that a coalition of law enforcement agencies across several countries had coordinated with private security researchers to disrupt and take over *Emotet's* C&C infrastructure while simultaneously arresting at least two *Emotet* crew members. Authorities expect the takedown (which included the disruption of backups) to significantly hinder the reconstruction of the *Emotet* botnet. Whether this remains the case in the long-term remains to be seen. The global trail of disruption and destruction that *Emotet* has engendered underscores the continued need to maintain good cyber hygiene standards and vigilance.

25. Check Point Research, "2020 Cyber Security Report", 22 January 2020 - https://www.bristol.de/wp-content/uploads/2020/03/2020-security-report.pdf.

Strengthening the Resilience of the Critical Information Infrastructure (CII) Sectors

CSA provides dedicated and centralised oversight of national cybersecurity functions to protect Singapore on two fronts: (1) by strengthening the resilience of Singapore's CII sectors; and (2) by exercising constant vigilance and preparedness to respond effectively to cyber incidents.

In 2019, CSA and the Global Resilience Federation Asia Pacific launched the Operational Technology Information Sharing and Analysis Center (OT-ISAC). OT-ISAC is a platform supporting organisations in the CII sectors on cyber threat information sharing. This helps companies respond to cyber threats in a more timely manner, and facilitates recovery from cyber incidents.

Key Observations of the OT Landscape in 2020

CONTRIBUTION BY OPERATIONAL TECHNOLOGY INFORMATION SHARING AND ANALYSIS CENTER

Threats to Operational Technology (OT) networks remained high in 2020 as threat actors sought to disrupt critical services and industrial processes. The OT-ISAC witnessed a worrisome development in the OT cyber threat landscape driven by the growing sophistication of threat actors. There were several high-profile incidents in 2020 where OT systems were targeted by cyber-attacks. This was generally due to three reasons: (a) increased IT-OT convergence, (b) ransomware actors targeting OT assets, and (c) rise in critical OT vulnerabilities discovered.

Increased IT-OT Convergence

Adversaries have continued to use proven TTPs to attack OT networks. Top on this list was the exploitation of Internet-accessible devices and phishing[26] to gain access to industrial networks. The series of attacks on Israel's water infrastructure in 2020 highlighted the risk of exposing OT assets to the Internet. Hackers

26. Adversaries have also taken advantage of the pandemic to launch phishing attacks against industrial organisations; an estimated 56 per cent of industrial organisations worldwide experienced more cyber threats during the COVID-19 pandemic as compared to before COVID-19, according to cybersecurity firm Claroty. "Majority of industrial enterprises face increase in cyber threats since COVID-19 pandemic began", 6 October 2020 - https://www.claroty.com/resource/majority-of-industrial-enterprises-face-increase-in-cyber-threats-since-covid-19-pandemic-began/.

exploited insecure Internet-facing devices on multiple occasions to target critical systems in wastewater treatment plants, water pumps and sewerage facilities[27]. Thankfully, these attacks were stopped before any major damage was inflicted.

Ransomware Actors Targeting OT Assets

Ransomware has grown to be one of the most prolific threats to industrial organisations and critical services, with over 450 incidents recorded worldwide in 2020 (around 8 per cent of which occurred in Asia Pacific)[28]. Malicious actors leveraging ransomware are often granted opportunistic access to OT networks due to the lack of proper security controls between IT and OT environments. This has led to operators of ransomware types such as *SNAKE* and *CLOP* developing capabilities to specifically target OT assets[29].

Rise in Critical OT Vulnerabilities Discovered

The number of OT vulnerabilities discovered and reported annually by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)[30] has grown steadily at an estimated rate of 16 per cent year on year from 2017 to 2020[31]. In 2020, notable critical vulnerabilities — such as the *Ripple20* and *Amensia33* which collectively

impacted hundreds of millions of OT and IoT devices such as medical and power equipment – were discovered. In addition, operating systems commonly used in OT environments such as Windows 7 and Windows Server 2008 R2 announced their end-of-life[32]; such software will no longer receive updates despite new vulnerabilities being found. These developments increase the attack surface of OT environments and present asset owners with new challenges in securing their networks.

What You Can Do

Just as adversaries work together to conduct cyber-attacks, organisations should form cross-sector collaborations and partnerships to share information on cyber threats, which can help them identify similar attacks, and better defend their networks.

27. "Vulnerable Cellular Routers Targeted in Latest Attacks on Israel Water Facilities", 21 July 2020 - https://www.securityweek.com/vulnerable-cellular-routers-targeted-latest-attacks-israel-water-facilities.
28. Based on OT-ISAC's analysis of victims impacted by the top 20 ransomware families in 2020, which includes Conti, Nefilim, Netwalker, Egregor, Maze, etc. Sectors with the greatest number of incidents include manufacturing (50 per cent), healthcare (16 per cent) and transportation/logistics (10 per cent). These attacks have caused major impact to operations ranging from train service disruptions to the shutdown of manufacturing plants.
29. "Financially Motivated Actors Are Expanding Access Into OT: Analysis of Kill Lists That Include OT Processes Used With Seven Malware Families", 15 July 2020 - https://www.fireeye.com/blog/threat-research/2020/07/financially-motivated-actors-are-expanding-access-into-ot.html.
30. ICS-CERT is part of the Cybersecurity & Infrastructure Security Agency in the United States. It provides timely information on the latest industrial control system vulnerabilities through its advisories published in collaboration with US-CERT.
31. OT-ISAC Analysis.
32. "Windows 7 support ended on January 14, 2020", 14 January 2020 - https://support.microsoft.com/en-us/windows/windows-7-support-ended-on-january-14-2020-b75d4580-2cc7-895a-2c9c- 1466d9a53962#:~:text=The%20specific%20end%20of%20support,longer%20available%20for%20the%20product.

Organisations should also adopt industry best practices to protect themselves against the increasing threat of ransomware and targeted attacks. These practices include enforcing segmentation between IT and OT networks, using anti-virus solutions and ensuring risks associated to system and software vulnerabilities are mitigated; whenever possible, important and sensitive data should also be encrypted, backed-up regularly and stored offline. Finally, organisations should increase efforts to raise the cybersecurity awareness of employees such as sharing notifications on the latest threats and training them to spot signs of phishing, and other malicious cyber activities.

International Critical Infrastructure Security Showdown

CONTRIBUTION BY MINDEF DEFENCE CYBER ORGANISATION

MINDEF/SAF and iTrust, Centre for Research in Cyber Security, co-organised the 4th Critical Infrastructure Security Showdown (CISS) at the Singapore University of Technology and Design (SUTD) from 27 July to 7 August 2020.

The exercise was conducted online for the first time – given COVID-19 restrictions – and saw 146 global participants from academia, as well as the public and private sectors. Participants across blue and red teams faced off against each other, with the red teams attempting to disrupt the operation of iTrust's Secure Water Treatment Testbed (SWaT). The cyber defenders in the blue teams, including the SAF's Cyber Defence Group, had to detect anomalies in large datasets to evaluate whether the SWaT was under attack, figure out which systems the attackers were attempting to disrupt, and their *modus operandi*. iTrust and MINDEF/SAF's green team also cooperated to develop and set up an ICS honeynet as part of the exercise platform.

Then-Commander of the Cyber Defence Group Colonel Edward Chen said, "OT forms the backbone of our daily lives, particularly in providing essential services such as water and power... MINDEF/SAF recognises the importance of developing deep OT cyber defence expertise, and understanding new vulnerabilities as potential attack vectors continue to evolve." Through working with its partners in industry and academia to organise and participate in activities like the CISS, MINDEF/SAF continues to develop its own cyber defence capabilities while also contributing to our local cybersecurity ecosystem and safeguarding national security against cyber threats.

TOPICAL FOCUS

Observations on Local Website Defacements and GE 2020

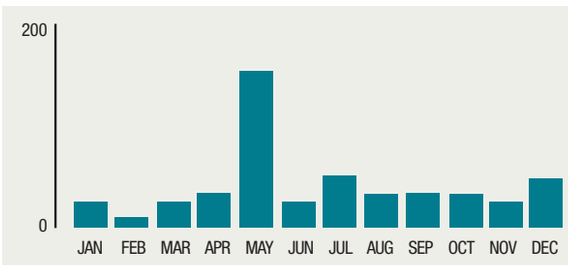
▼ 43% FROM 2019

The number of local website defacements dipped in 2020 despite high profile events such as Singapore's General Election (GE 2020) and the US Presidential Election. This section provides an overview of website defacements in Singapore in 2020, and the measures taken to ensure a smooth GE 2020 on the cyber front.

495 '.sg' websites were defaced in 2020, a sharp decrease of 43 per cent from 2019. The majority of victims were SMEs; no government websites were affected.

The number of website defacements was at its highest in May 2020. These appeared opportunistic in nature and consisted of random messages in Bahasa Indonesia and YouTube music videos of popular Indonesian songs embedded in the defaced pages. These defacements mostly targeted Joomla-published websites despite its small market share relative to WordPress, which suggests that the former had more vulnerabilities that hackers could readily exploit.

NUMBER OF DEFACED SINGAPORE WEBSITES REPORTED IN 2020



In 2019, politically motivated website defacement activities relating to global event developments contributed to the larger number of defacements observed. The significant fall in 2020 suggests that activist groups could have chosen other platforms with potentially wider reach (e.g. social media) to disseminate their messages. In fact, there were over 320 million total Facebook interactions[33] (reactions, comments, shares) relating to the two US 2020 Presidential Election candidates (Biden and Trump) from July to October 2020, while an average US business would have received only 1,100 page views per month[34].

Despite major political events in 2020 such as GE 2020 and the aforementioned US Presidential Election – which have often been the catalyst for hacktivist activities – there was no discernible trend of defacements on ".sg" websites.

33. "Can Social Media Data Predict the Winner of the 2020 US Presidential Election? A Look at the Latest Trends", 23 October 2020 - https://www.socialmediatoday.com/news/can-social-media-data-predict-the-winner-of-the-2020-us-presidential-electi/587693/.

34. "Over 50% of Local Business Websites Receive Less Than 500 Visits Per Month", 30 November 2019 - https://www.searchenginejournal.com/over-50-of-local-business-websites-receive-less-than-500-visits-per-month/338137/#close.

Delivering a Cyber-secure Singapore General Election 2020

A secure and reliable IT infrastructure was pivotal to the successful conduct of GE 2020. With social distancing measures in place, additional workarounds and processes had to be developed to facilitate election proceedings. An example was the use of a new VoteQ mobile app to manage overcrowding issues at polling stations.

Broadly, CSA observed no significant increase in malicious cyber activities such as phishing and website defacements both in the lead-up to and after the GE 2020 period. Phishing e-mails were predominantly opportunistic in nature, and mostly continued to leverage COVID-related lures rather than election-related themes.

Nonetheless, to ensure a smooth GE 2020, CSA worked closely with the Ministry of Communications and Information (MCI), GovTech, the Ministry of Home Affairs (MHA) and the Elections Department (ELD) on plans to prevent and counter potential cyber threats to the event. Preparation work included:

- Identifying and preparing key CII sectors that were crucial to the smooth conduct of GE 2020;
- Table-top exercises and joint incident response planning operations to strengthen the cybersecurity of GE 2020-related systems;
- Threat assessments to identify potential cyber threats and risks surrounding GE 2020, with the aim to drive various protection enhancements and curate necessary response efforts;
- SingCERT's issuance of cybersecurity advisories to political parties and candidates, and members of the public to raise their awareness of cyber threats; and
- Review of the security architecture of the VoteQ mobile app, including its source code. CSA conducted penetration testing on the app and website to ensure that vulnerabilities were detected and addressed prior to public use on Polling Day.

ELD and CSA also helped secure GE 2020 by keeping political parties and candidates well-informed of potential cybersecurity risks. ELD's *Candidate Handbook* included advisories on how to ensure the cybersecurity of the political parties' IT infrastructure and online campaigning activities. As the key election authority, ELD's efforts were helpful in ensuring that the message on the importance of a cyber-secure GE 2020 reached the broadest possible audience.

A RETROSPECTIVE LOOK

The Singapore Cybersecurity Strategy that was launched in 2016 sets out the nation's vision, goals and priorities for a resilient and trusted cyberspace. It aimed to catalyse participation by all stakeholders – Government, providers of essential services, cybersecurity industry, individuals, and international partners – through four key Pillars:

Pillar One: Building a Resilient Infrastructure
Pillar Two: Creating a Safer Cyberspace
Pillar Three: Developing a Vibrant Cybersecurity Ecosystem
Pillar Four: Strengthening International Partnerships

This special edition of the Singapore Cyber Landscape looks at milestones across the four Pillars since 2015, and considers how they have contributed to building and developing a safer and trusted cyberspace in Singapore and abroad.

PILLAR 1

Building a Resilient Infrastructure

This Pillar ensures that essential services are resilient to minimise impact to our day-to-day lives in the event of a cyber-attack. Today, our essential services are underpinned by various Critical Information Infrastructure (CII), which the Government, private sector, and the cybersecurity community work hand-in-hand to strengthen and secure.

MILESTONES

2016

Prime Minister Lee Hsien Loong launched Singapore's Cybersecurity Strategy to build a resilient and trusted cyber environment.

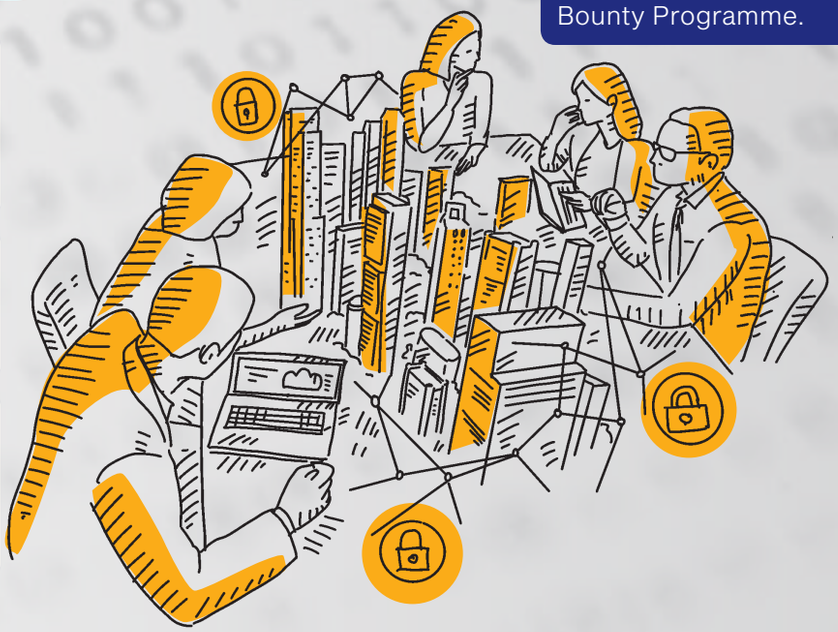
Mounted Exercise Cyber Star, CSA's first cybersecurity exercise involving four CII sectors.

Unveiled Cyber Forensics Laboratory to support CSA's operational role in investigating and responding to major cyber incidents.

2017

Expanded Exercise Cyber Star to include over 200 participants across all 11 CII sectors for the first time.

Announced creation of CSA Academy to train cybersecurity professionals in government and CII sectors.



2018

Passed the Cybersecurity Act to establish a legal framework for the oversight and maintenance of national cybersecurity.

Designated critical systems across 11 CII sectors from the public and private sectors.

Partnered GovTech and the cybersecurity community on the first Government Bug Bounty Programme.

2019

Established a Whistleblowing Channel for individuals to disclose useful information that could impact the cybersecurity of CII.

Introduced more complex cyber-attack scenarios at Exercise Cyber Star.

Launched the Operational Technology (OT) Cybersecurity Masterplan.

Built up a community of over 500 Cyber Assurance Practitioners and Risk Practitioners to exchange ideas and share cybersecurity audit and risk assessment best practices.

2020

Worked with GovTech, the Ministry of Health and other agencies to ensure the cybersecurity of Government e-services such as Singpass and Corppass, e-services using Commercial Cloud, and COVID-19 technology such as TraceTogether.

Oversaw the cybersecurity of Singapore General Election 2020, and apprised political parties and candidates of potential cyber threats that could disrupt the election.

PILLAR 2

Creating a Safer Cyberspace

Digital technologies can enable and empower businesses and society, but only if they are safe and trustworthy. This Pillar comprises initiatives to engage businesses and the public to collectively build a safer and more secure cyberspace.

MILESTONES

2016

Published "Cyber Safety" series of student activity books to raise awareness of the importance of cybersecurity among primary school students.

2017

Launched first National Cybersecurity Awareness Campaign - "Live Savvy with Cybersecurity".

Unveiled results from first national Cybersecurity Public Awareness Survey.

The Singapore Police Force (SPF) launched the Alliance of Public PrivAte Cybercrime sTakeholders (APPACT) to deepen partnerships and raise cybercrime awareness in the private sector.

2018

Introduced four essential cybersecurity tips to help the public to go safe online under the "Cyber Tips 4 You" cybersecurity awareness campaign.

Launched a "Cyber Savvy Machine Pop-up" which travels to libraries and community spaces, and has since recorded over 82,000 attempts for its quiz segment.

2019

Unveiled the "Go Safe Online 2019" campaign with expanded public outreach.

Established three National Satellites of Excellence (NSoE)[35].

Singapore attained the status of a Certificate Authorising Nation under the Common Criteria[36] Recognition Arrangement.

The SPF launched the Anti-Scam Centre to disrupt scammers' operations and mitigate victims' losses.

The SPF launched the National Police Cadet Corps Cybercrime Prevention Proficiency Badge to enhance students' knowledge on cybercrime prevention.

2020

Launched Singapore's Safer Cyberspace Masterplan which outlined blueprint for a safer and more secure cyberspace.

Rolled out first-of-its-kind Cybersecurity Labelling Scheme to improve IoT security for smart devices.

Collaborated with local cybersecurity firms to implement cost-effective security solutions and services for enterprises amid COVID-19 conditions.

PDPC amended the Personal Data Protection Act to enhance consumer protection and encourage data innovation.

35. 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.
36. Common Criteria is the de facto standard for cybersecurity standard certification around the world, and CC certificates are mutually recognised across 30 nations.

PILLAR 3

Developing a Vibrant Cybersecurity Ecosystem

This Pillar is aimed at enhancing the vibrancy and sustainability of Singapore's cybersecurity industry, and its research and talent pipelines. While cybersecurity is imperative for a resilient national infrastructure and a safer cyberspace, it is also an economic opportunity for Singapore's Digital Economy.

MILESTONES

2015

Inked developmental partnerships with major local and foreign industry players including Singtel, Check Point Software Technologies and FireEye.

2016

Signed Memoranda of Understanding with Nanyang Polytechnic and the Singapore Institute of Technology to develop cybersecurity curriculum, and research and development projects.

2017

Introduced the Cybersecurity Professional Scheme to attract cybersecurity experts to the public sector.

Organised "Cybersecurity Challenge Singapore" competition to inspire and uncover locals with a talent for cybersecurity disciplines.

2018

Launched Co-Innovation and Development Proof-of-Concept Scheme to encourage cybersecurity innovation in Singapore through the funding of innovative projects.

Unveiled the inaugural Cybersecurity Industry Call for Innovation for industry providers to develop innovative solutions addressing specific cybersecurity challenges.

Collaborated with IMDA, SingTel Innov8 and NUS Enterprise to set up Innovation Cybersecurity Ecosystem @BLK 71 (ICE71), the region's first cybersecurity entrepreneurship hub.

Organised inaugural Youth Cyber Exploration Programme (YCEP) bootcamp to introduce secondary school students to cybersecurity fundamentals.

2019

Introduced SG Cyber Youth, a national programme designed to guide youths in their cybersecurity journey.

Introduced funding support for eligible Small and Medium Enterprises (SMEs) under the "SMEs Go Digital" programme for pre-approved cybersecurity products and services.

Announced the launch of a new National Integrated Centre for Evaluation to facilitate testing and evaluation of cyber products.

2020

Took over the National Cybersecurity Research & Development (NCR) programme[37] to coordinate Singapore's cybersecurity R&D and innovation processes.

Pushed out SG Cyber Women initiative to expand cybersecurity talent pool and encourage more females to join the profession.

Unveiled SG Cyber Talent initiative which aims to reach out to 20,000 individuals over three years.

Launched SG Cyber Educators at the inaugural Singapore Cybersecurity Education Symposium.

37. The NCR Programme was launched in 2013 to build and extend Singapore's cybersecurity capabilities.

PILLAR 4

Strengthening International Partnerships

This Pillar aims to strengthen international partnerships towards a rules-based multilateral order in cyberspace. As cyber threats are transboundary and ever-evolving, strong international collaboration through dialogue, capacity building, norms development and implementation is necessary to combat the threats in cyberspace.

MILESTONES

2016

Inaugurated the Singapore International Cyber Week (SICW). Key outcomes of the event included:

- Launch of inaugural ASEAN Ministerial Conference on Cybersecurity (AMCC) as an informal platform for Cybersecurity and ICT[38] Ministers to discuss cybersecurity issues that affect the region and ways to tighten cybersecurity coordination.
- Announcement of Singapore's $10 million ASEAN Cyber Capacity Programme to build cyber capacity in ASEAN Member States (AMS).

2017

AMS expressed support for the development of voluntary norms of State behaviour, taking reference from the norms set out in the 2015 UNGGE[39] Report, to guide the responsible use of information and communication technologies in ASEAN.

2018

AMCC participants agreed to subscribe in-principle to the 11 voluntary, non-binding norms recommended in the 2015 UNGGE Report.

Adoption of first-ever ASEAN Leaders' Statement on Cybersecurity Cooperation by ASEAN Leaders at the 32nd ASEAN Summit, during Singapore's ASEAN Chairmanship.

2019

Established the multi-disciplinary ASEAN-Singapore Cybersecurity Centre of Excellence.

For the first time, Singapore hosted the flagship international forum for the Common Criteria Industry – the International Common Criteria Conference (ICCC).

AMS agreed to move forward on a formal Cybersecurity Coordination Mechanism and to reaffirm the region's commitment to a rules-based international order in cyberspace. A working-level committee was established to consider a long-term action plan to effectively implement the 11 UNGGE norms.

Singapore selected, for the first time, to be one of 25 members of the UNGGE. Singapore also took part in the first Open-Ended Working Group (OEWG)'s discussions on developments in the field of information and telecommunications in the context of international security.

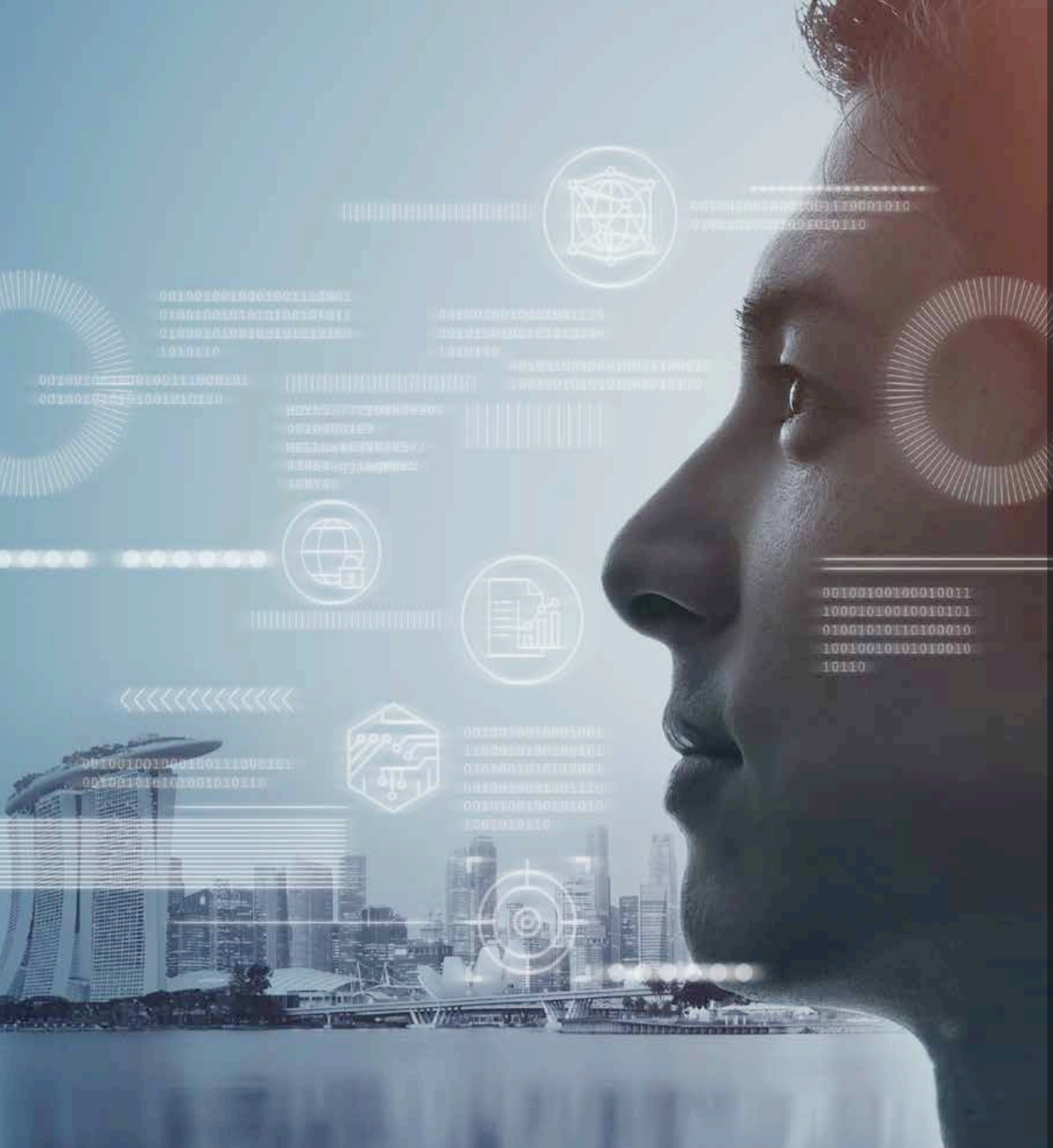
2020

Organised the fifth SICW 2020 in a "hybrid" format, which saw over 6,000 participants from across 60 countries.

AMCC participants reiterated their commitment to develop a long-term action plan to effectively implement the 11 UNGGE norms at a pace that is agreeable to all AMS. Participants also agreed on the urgent need to protect national and cross-border Critical Information Infrastructure (CII).

Announcement of collaboration with the United Nations to develop a checklist for implementing cybersecurity norms.

38. Information and Communications Technology.
39. United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, which seeks to address norms guiding responsible behaviour in cyberspace, confidence building measures and capacity-building, and how international law applies to cyberspace.



LOOKING BACK TO LOOK FORWARD

Since CSA's inception in 2015, the cyber threat landscape has become more complex and dynamic. Cyber defenders have had to face a host of ever-evolving threat trends and challenges. In this milestone fifth edition of the Singapore Cyber Landscape, CSA has invited the Centre of Excellence for National Security, S. Rajaratnam School of International Studies to contribute a commentary that provides a stakeholder perspective on CSA's work in regard to Singapore's cyber threat landscape, while ruminating on future challenges. This section concludes with thought-provoking major trends in cyberspace to watch out for in the future.

A Retrospective of Threat Trends, and a Pondering on the Future

Teo Yi-Ling and Benjamin Ang[40]

CONTRIBUTION BY CENTRE OF EXCELLENCE FOR NATIONAL SECURITY (CENS)

For those of us operating in the cybersecurity domain, the annual Singapore Cyber Landscape editions published by the Cyber Security Agency of Singapore have been a vital and authoritative resource for study and analysis in formulating and recommending policy responses. They are extensions to and supplement Singapore's Cybersecurity Strategy, and reflect the progress made in meeting Singapore's cybersecurity goals. They are a record of wins and losses, successes and failures; unsparingly putting down for the record errors and omissions within government agencies, institutions, and private sector enterprises both large and small that have led to security breaches. They sound the alarm on emerging and anticipated cyber threats, seek to educate about the same, and in doing so testify to the fact that cybersecurity cannot be the responsibility of the few.

Looking back at the trends that shaped the cyber threat landscape, what is immediately clear is that baseline threats including malware, phishing, website defacements, supply-chain attacks, and Advanced Persistent Threats will continue to persist. What is critical is having the mindset that these threats will evolve and manifest themselves in new forms. Several threats which were discussed for years have gained international scale and attention in the early months of 2021: cyber-physical attacks (on a water utility in Florida), supply-chain attacks (through the SolarWinds Orion network management system), and compromise of core systems like e-mail servers (exploitation of zero-day vulnerabilities in Microsoft Exchange Servers).

40. Teo Yi-Ling is a Senior Fellow with the Cyber and Homeland Defence Programme at the Centre of Excellence for National Security (CENS), S Rajaratnam School of International Studies (RSIS). Benjamin Ang is Senior Fellow, Head of the Cyber and Homeland Defence Programme, and Deputy Head of CENS, RSIS.

With Great Progress Comes Greater Responsibility

Arguably – and to borrow from military parlance — what must crystallise is the realisation that we cannot "fight the last war" in our approach to cybersecurity responses. Having said this, the observation is made that in the last five years, strides have been made in terms of bolstering cybersecurity defences and capabilities in the various Critical Information Infrastructure domains, with drills and joint exercises coordinated by CSA. This is augmented by CSA's continuous efforts to keep Singapore's cyberspace safe and secure. CSA has also engaged with schools, educational institutions, businesses, and grassroots communities to promote cybersecurity awareness alongside executing its mandate for creating a vibrant cybersecurity ecosystem. MINDEF has committed resources to developing cyber defence capabilities and enshrined digital defence as the sixth pillar of Total Defence. The SPF continues its work on educating the public about online scams and promoting cyber hygiene.

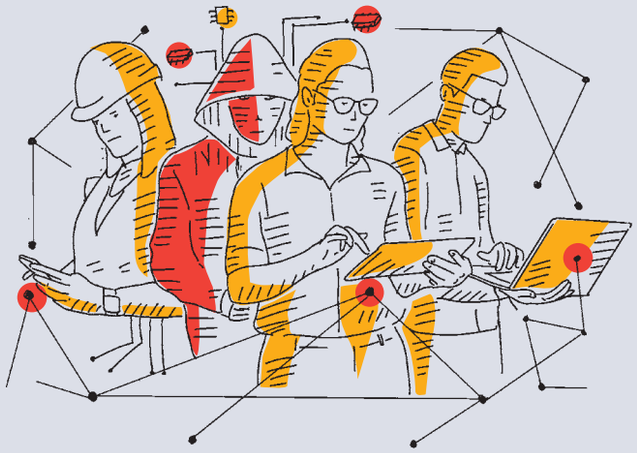
Indeed, in the wake of every major cyber-attack and data breach affecting Singapore in the last few years, the call to arms to tackle cybersecurity on a whole-of-government/whole-of-nation effort is sounded. While this is necessary, the danger is that this becomes a repetitive chorus of motherhood statements if the public is not correspondingly informed about progress or successes on this front – for example, instances where cyber-attacks have been detected and countered or data breaches mitigated or foiled. As we advocate digital transformation of society and the goals of the Smart Nation, we also need to build up personal data protection and cybersecurity, which are key factors to the success of these goals. The progress, prosperity, and sustainability of Singapore cannot be achieved without functional security, of which cybersecurity has become a vital aspect. The public communication around this needs to be modified appropriately, otherwise the perception of a lack of a coordinated multi-stakeholder approach will sharpen.

Cultivating a Mindset of Vigilance

More can be done on the part of individuals and organisations because cybersecurity remains the responsibility of all end users. It cannot be "departmentalised" or be someone else's problem – the ongoing digital transformation of our lives and work means that a mindset of accountability and responsibility has to be inculcated across the board. On the continuum of peripheral awareness to activated vigilance, are we able to say broadly where we sit, as of now?

The water utility employee in Florida, who initially ignored the fact that someone was controlling his computer, was vigilant enough to notice later that the chemical levels in the water had changed.

If he had left the breach to the IT department instead, this cyber-attack could have had serious consequences to public health. On the other hand, if it is true as alleged that SolarWinds was breached with the help of a default password "solarwinds123" which had been left unchanged for two years, then that lack of vigilance is unacceptable. Vigilance includes timely patching of vulnerabilities once they are disclosed, such as those in Microsoft Exchange Server. The importance of patching known vulnerabilities is one of the lessons we should have learned from the SingHealth data breach of 2018.



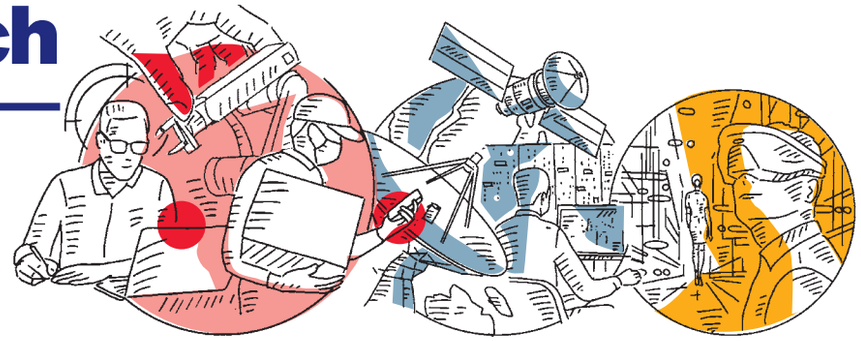
Vigilance is also needed in ensuring cybersecurity for Singapore's many impressive and visionary digital transformation projects, such as autonomous vehicles, autonomous delivery robots, e-payments for hawkers, personal learning devices for students, blockchain projects, and artificial intelligence projects. These can only be secured through effective communication and cooperation among project owners, regulators, cybersecurity experts, and end users.

Fortifying Digital Defences for Our Future

Further, the call to digitally transform Singapore essentially means that data will be central to how our lives are lived. We will increasingly use data to fuel the decisions we make on a daily basis. Governments and businesses rely on it for managing society and making business and economic decisions. Data is the bounty that cybercriminals, state-sponsored actors, and hacktivists seek. Despite the enormous role it plays, it is an ongoing struggle to secure it. As a city is only as structurally secure as the foundations upon which it is built, so too is a networked infocommunication framework functioning off data sources and repositories. The proposition for coherent cybersecurity protection may be in deeming the data industry sector as a foundational critical information infrastructure, allowing it to be more stringently regulated. With this, we could work towards comprehensive data security and enforce transparency in and accountability for data use and management – all players and stakeholders in the public and private sectors will be required to coordinate and collaborate in bolstering cybersecurity measures for data protection.

Finally, the messaging around the notion of "digital transformation" and becoming a Smart Nation must change across the landscape. It must communicate holistically the strengths, weaknesses, opportunities, and threats involved in this enterprise, and it must be an ongoing process. It must reflect the sobering imperatives of engaged cybersecurity practice, in lockstep with the promises of a brilliant future with the benefits of digitalisation. In practice, this translates to requiring active cybersecurity practice in the context of empowering digital transformation. This messaging must be owned by, passed on, and acted upon within our cybersecurity landscape – because in reality, the landscape is all of us. Hopefully, future editions of the SCL will be able to reflect such transformation.

Cybersecurity Trends to Watch



NEAR TERM
Risk of Remote Workforce, Increased Risk of Supply-chain Attacks and the Ransomware Threat

MEDIUM TERM
Cybersecurity of Space Infrastructure

LONG TERM
Hyper-Connectivity and the Metaverse

NEAR TERM: Risk of Remote Workforce

What Is It?

Social distancing measures during the COVID-19 pandemic have led to the rapid adoption of remote working. Overnight, many organisations had to implement new processes and systems to facilitate business continuity. Threat actors were quick to capitalise on this expanded – and often more vulnerable – attack surface brought about by these new work-from-home ecosystems.

Why Does It Matter?

Remote working is here to stay, even after the pandemic. It has become an increasingly attractive alternative to working from the office[41]. Companies have found that remote working reduces overheads, without reducing employee efficiency.

Poorly configured network and software systems to facilitate remote work can expose organisations to greater risk of cyber-attacks. Defending the infrastructure needed to sustain a large remote workforce against malicious threat actors will present a daunting challenge for organisations moving forward.

NEAR TERM: Increased Risk of Supply-chain Attacks

What Is It?

Organisations often rely on vendors, such as technology firms and managed service providers, for products and services to support their business operations. Cyber threat actors have exploited such interdependencies to carry out supply-chain attacks. Supply-chain attacks involve targeting an organisation by exploiting weak links and trusted relationships in the supply network.

Why Does It Matter?

A successful breach in the supply chain, as seen in the SolarWinds incident, provides cyber threat actors a single pivoting point to multiple victims. The compromise of a trusted supplier – or a popular and widely-used product – can result in massive and widespread

41. The Straits Times article published on 24 March 2021 said that 9 in 10 employees in Singapore wanted to continue working from home for reasons such as flexibility and cost savings.

repercussions worldwide, as victims could include major vendors with huge customer bases. The supply-chain attack also highlighted the level of sophistication, patience and operational security that determined threat actors can be capable of. Cyber threat actors of all stripes, whether motivated by financial rewards or privileged access to information and systems, are likely to emulate such methods and attempt propagating to as many victims as possible by targeting and compromising supply chains.

NEAR TERM : The Ransomware Threat – From Sporadic and Isolated, to Massive and Systemic

What Is It?

From sporadic and isolated incidents, which targeted a handful of machines and caused nuisance to individuals and small businesses, ransomware has evolved into a massive and systemic threat. Today, ransomware attacks target large organisations and even government agencies, disrupting not just IT operations but also the provision of essential services, with the potential to inflict severe cyber-physical impact. Threat actors have become more operationally sophisticated, exploiting loopholes in victims' business processes, or dependencies between victims' operations and business flows, to maximise the likelihood of success and impact of their attacks. Compounding the problem, threat actors have also become more directed in their targeting, striking key assets such as the Active Directory[42] to launch commands that lock up hundreds – if not thousands – of machines and entire networks almost simultaneously.

Why Does It Matter?

Ransomware attacks are financially-driven ventures. The higher the stakes, the more likely the victims are to be cowed into paying larger ransoms. Attackers are deliberately causing extensive disruptions to victims' operations, putting the latter under ever-greater pressure to accede to the ransom demands. The proliferation of Ransomware-as-a-Service affiliate models[43] means attacks now occur at scale, and at a growing intensity. We can therefore expect ransomware operators to be increasingly audacious and savvy at hitting targets which are "too important to fail". These attacks have already caused real-world effects and harm, and may have the potential to become national security concerns.

These developments underscore an urgency for organisations to regularly review their cyber hygiene, network connections, and operational dependencies. First, ransomware typically enters via relatively unsophisticated means. So organisations can protect themselves if they maintain good cyber hygiene. This includes keeping systems and software updated, raising employees' awareness of threats, and detecting intrusions quickly. Second, organisations must ensure that crucial systems' linkages are adequately protected, especially any connections or linkages between Internet-connected systems and OT systems. Thirdly, organisations must understand their dependencies. These include operational and business-type flows. Key dependencies must be mapped and protected. And last, organisations must develop and practise contingency plans, including business continuity, technical recovery and disaster recovery plans, involving appropriate key decision makers and stakeholders from both operations and business functions.

42. Active Directory is a Windows OS directory service that allows admins and users to search for resources stored anywhere on the network.
43. Ransomware-as-a-Service (RaaS) affiliate models grant cybercriminals access to shared infrastructure to conduct ransomware attacks without the need to develop native capabilities, lowering barriers to entry for even technically unsophisticated hackers.

MEDIUM TERM : Cybersecurity of Space Infrastructure

What Is It?

Space infrastructure includes not only the approximately 2,000 satellites in orbit, but also their Earth-bound command and control centres. Space infrastructure provides critical support to many aspects of daily life, including navigation, communications, weather monitoring and financial transactions.

Why Does It Matter?

Cyber threat actors may compromise space infrastructure in order to disrupt activities that they support. They may also hack space infrastructure in order to obtain strategic information that satellites are now capable of yielding on Earth-bound targets of interest. Compared to other types of threats that could compromise space infrastructure, cyber-attacks are among the most affordable, accessible and difficult to attribute. In 2008, hackers managed to seize control of a civilian imaging satellite named Terra, but refrained from issuing their own commands to the satellite, apparently to reduce their footprint. Space is also a domain that sees increasing levels of activity by big private entities, which may attract financially motivated cyber threat actors.

LONG TERM : Hyper-Connectivity and the Metaverse

What Is It?

Hyper-connectivity is the use of many systems and devices in networks to enable person-to-person, person-to-machine, and machine-to-machine communication. Hyper-connectivity is envisaged to give rise to the Metaverse, which has been described as a hybrid virtual-physical space, the sum of virtual reality (VR), augmented reality and the Internet, where users can interact with a computer-generated environment and other users.

Why Does It Matter?

The proliferation of Internet-connected devices from manufacturers that have prioritised usability and cost over security massively broadens the potential attack surface. Technologies such as 5G and cloud compound the risk by increasing both the capabilities of devices and the available entry points for attacks. Hyper-connectivity vastly boosts the reach of the Metaverse, which is emerging as a new marketplace for both personal data and commerce. Users in the Metaverse could be exposed to risks ranging from contactless payment transaction fraud and data breaches to identity theft and alteration of VR content[44].

44. Lack of encryption on VR platforms can give hackers free reign to alter content for malicious intent, the consequences of which could be fatal. In 2018, a research team from the University of New Haven in Connecticut, found that in a controlled attack, they were able to alter what a person could see in VR.

Glossary

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.
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.
Hacktivist	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.
Indicators of Compromise (IOC)	Pieces of forensic data, such as data found in system log entries or files, that indicate that a system or organisation has been breached
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.
Malware	Malicious software intended to perform unauthorised processes that will have adverse impact on the security of a computer system.

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.

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.
Website: www.csa.gov.sg/singcert/reporting

If you wish to seek scam-related advice, please contact ScamAlert.
Anti-scam Helpline: 1800 722 6688
Website: www.scamalert.sg

CSA
SINGAPORE

www.csa.gov.sg