

SINGAPORE CYBER LANDSCAPE 2021



Contents

Singapore Cyber Landscape 2021

Copyright 2022
By Cyber Security Agency of Singapore

All rights reserved.

Designed by Urban Forest Design Pte Ltd

ISBN: 978-981-18-5412-5

The “Singapore Cyber Landscape 2021” publication reviews Singapore’s cybersecurity situation in 2021 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.

Foreword	4	Chapter 3	
Overview of Cyber Threats in 2021	6	Transitioning to Cybersecurity Strategy 2021	34
Significant Cyber Incidents in 2021	8	Updating Strategy 2016	36
		Strategic Pillar 1: Build Resilient Infrastructure	37
Chapter 1		Strategic Pillar 2: Enable a Safer Cyberspace	40
Global Trends in 2021	10	Strategic Pillar 3: Enhance International Cyber Cooperation	44
Cyber Implications of the Russia-Ukraine Conflict	12	Foundational Enabler 1: Develop a Vibrant Cybersecurity Ecosystem	47
Massive and Systemic: Ransomware’s Coming-of-Age	14	Foundational Enabler 2: Grow a Robust Cyber Talent Pipeline	48
Each Sold Separately: Proliferation of Cyber Tools and Access Services	18		
Living Off the Land	20	Chapter 4	
		Cyber Trends to Watch	50
Chapter 2		Increased Geopolitical Tensions	
WWW.TARGET.SG	24	Decoupling From Western Technology	52
Survey on Cyber Awareness – Findings and Insights	26	Non-State Actors Playing a Larger Role in Geopolitical Conflict	53
Case Study: Data Breaches Affecting Local Enterprises and SMEs		Web3, Blockchain Technology and the Metaverse	
All Your Data Belongs to Us: Data Breaches in the Infocomm Sector	27	Cryptocurrency Scams	55
Piling on the Pressure: Extortion-related Data Breaches by ALTDOS Group	28	Securing Our Digital Assets in the Metaverse	56
Case Study: Phishing Attacks Targeting Oversea-Chinese Banking Corporation Limited (OCBC) Clients	29	The Future of Ransomware	
State of Singapore’s Cyberspace	30	Targeting Critical IoT Devices	56
		Glossary	58
		Contact Details	62

Foreword



The cyber landscape in 2021 was fraught with increasingly sophisticated threats and more brazen threat actors. Sun Tzu in *The Art of War* said that “all warfare is based on deception. Hence, when we are able to attack, we must seem unable; when using our forces, we must appear inactive; when we are near, we must make the enemy believe we are far away”. Cyber threat actors appeared to have imbibed that lesson. They certainly threw a few curveballs that kept cyber defenders all over the world, including here at the Cyber Security Agency of Singapore (CSA), on their toes.

The extent to which the effects of cyber-attacks spilled over into the physical realm was one such curveball. The world witnessed a number of vivid examples of how cyber-attacks resulted in real-world impact, causing severe consequences such as supermarkets shutting down, petrol stations running short of fuel, and patients being denied timely healthcare services. Not only did these cyber-attacks unleash their impact on the physical world, they also demonstrated that cybercriminals had the potential to be every bit as dangerous, resourceful and sophisticated as state-sponsored Advanced Persistent Threat (APT) groups.

The proliferation of zero-days – previously unknown vulnerabilities in a system that

attackers discovered – and the speed with which cyber threat actors exploited them, was not so much a curveball but a cannon-shot out of the blue. Take for example LOG4SHELL, a zero-day vulnerability in Log4j, a popular open-source Java package used in innumerable applications and services. Within a couple of days of its disclosure, malicious attempts to exploit it surged by 300 times, keeping just about every IT team in Singapore and around the world busy throughout December 2021 and beyond. As cloud hosting, mobile and Internet of Things (IoT) technologies propel the volume and complexity of systems connected to the Internet, the attack surface will grow, and the number of exploits will rise.

Cyberspace cannot detach itself from real-world developments any more than the physical world can remain isolated from digital developments. When war broke out in Ukraine earlier this year, so did cyber-attacks. Critical information infrastructure was not spared. There were even instances when cyber-attacks not only hit their primary targets, but also caused collateral damage across the broader region. Given possible spillover effects on Singapore from such cyber incidents, CSA has stepped up our efforts to remain vigilant against such threats, and has been keeping all Critical Information Infrastructure (CII) sector leads regularly

apprised of the latest situation. CSA also launched the SG Cyber Safe Programme to help enterprises beyond CII sectors to better protect themselves in the digital domain and strengthen their cybersecurity posture.

Some may find these turns of events dispiriting. Rather than throw our arms up in despair, we see an opportunity to refocus our attention on the fundamentals – work with all partners to secure our key networks; enable more secure digital access for enterprises and the public; move cyber norms forward; and create cybersecurity business and job opportunities for Singapore. This is the spirit behind the new iteration of Singapore’s Cybersecurity Strategy, first launched in 2016 by Prime Minister Lee Hsien Loong.

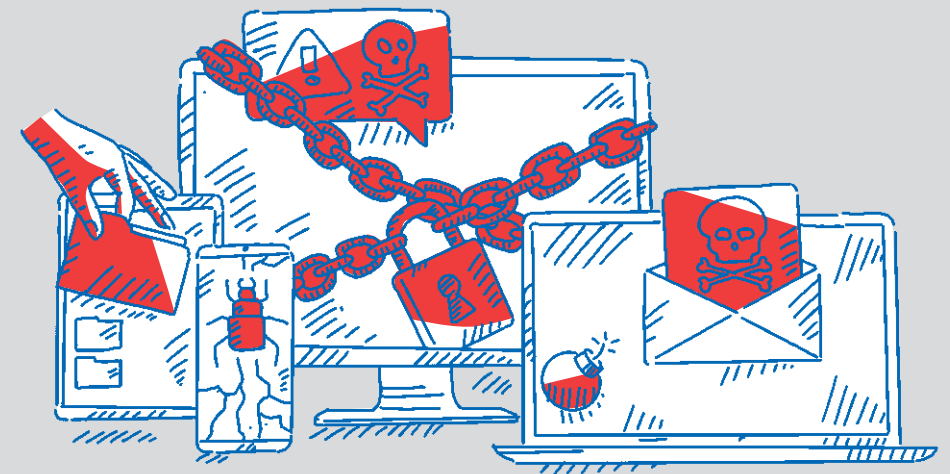
The maturing of disruptive technologies and increasing convergence of the physical and digital realms are happening amidst a more uncertain world. This has spurred a reorganisation of our Cybersecurity Strategy to improve on and expand the key pillars that underpin it. Cybersecurity Strategy 2021, which Senior Minister and Coordinating Minister for National Security Mr Teo Chee Hean launched in October 2021, has been designed precisely to meet the emerging challenges from our operating landscape.

Effective implementation of Cybersecurity Strategy 2021, even as our digitalisation journey continues apace, requires active and coordinated participation from all stakeholders. After all, cybersecurity is a team sport playing out in a borderless world. Only by banding together and working across borders, do we stand a fighting chance against the ever-evolving threat. CSA looks forward to working even more closely with governments, businesses and civil society towards a safe, secure and resilient cyberspace.

A handwritten signature in black ink, appearing to read 'David Koh'. The signature is stylized and fluid.

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

Overview of Cyber Threats in 2021



NUMBER OF CASES HANDLED BY SINGCERT:

2021: **7,342**

2020: **9,080**

2019: **8,491**




PHISHING

55,000

phishing URLs¹ with a Singapore-link were detected, an increase from 47,000 in 2020

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

COMMONLY SPOOFED SECTOR

-  **1ST > SOCIAL NETWORKING**
-  **2ND > FINANCIAL**
-  **3RD > ONLINE/CLOUD SERVICE**

WHATSAPP, FACEBOOK, LLOYDS, CHASE BANK AND MICROSOFT WERE COMMONLY SPOOFED BRANDS



ONLINE CHEATING

2021: **18,068**

2020: **12,242**

2019: **7,580**



COMPUTER MISUSE ACT

2021: **3,731**

2020: **3,482**

2019: **1,701**



CYBER EXTORTION

2021: **420**

2020: **245**

2019: **68**

CYBERCRIME IN SINGAPORE

Cybercrime cases accounted for

48%

of overall crime in 2021

WEBSITE DEFAACEMENTS

419

Singapore-linked website defacements were detected, a slight decrease from 495 in 2020

RANSOMWARE

137

cases of ransomware were reported to SingCERT in 2021, a 54% increase from 89 cases in 2020

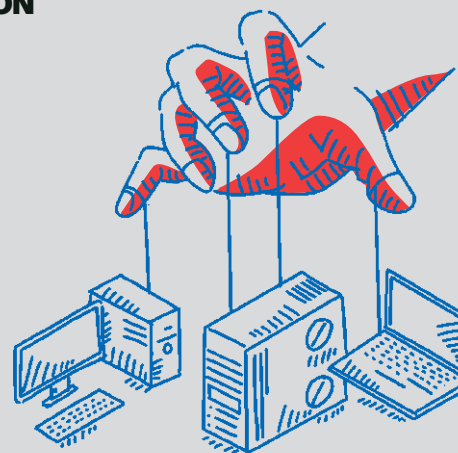
COMMAND AND CONTROL (C&C) SERVERS AND BOTNET DRONES

3,300

unique C&C servers were observed in Singapore, more than triple the 1,026 unique C&C servers in 2020

4,800

botnet drones (compromised computers infected with malicious programs) with Singapore Internet Protocol (IP) addresses were observed daily on average, a decrease from 2020's daily average of 6,600



Significant Cyber Incidents in 2021

GLOBAL INCIDENTS

Jan 2021

Use of zero-day vulnerabilities in Accellion's FTA* software for data breaches and extortions.

*File Transfer Appliance

Jan - Mar 2021

Mass exploitation of zero-day vulnerabilities in Microsoft's Exchange Server.

Feb 2021

Attempted poisoning of Florida's water supply via cyber intrusion.

May 2021

Colonial Pipeline hit by *Darkside* ransomware.

May 2021

JBS Foods attacked by *REvil* ransomware.

Jul 2021

REvil ransomware delivered via Kaseya's VSA* software.

*Virtual System Administrator

Jul 2021

Exposé on NSO Group's *Pegasus* spyware.

Jul 2021

Cyber-attack on Iranian train systems.

Aug 2021

Alleged targeting of telcos in Southeast Asia by APT groups.

Nov 2021

Cyber-attack on Iranian gas stations.

Nov 2021

Emotet makes a comeback.

Dec 2021

Exploitation of Log4j vulnerabilities.

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

LOCAL INCIDENTS

Jan 2021

Singtel data breach via Accellion's FTA.

Mar - Aug 2021

Multiple companies suffer ransomware attacks and data extortion by ALTDOS.

Jul 2021

StarHub data breach involving third-party data dump site.

Sep 2021

Exploitation of SMS one-time-password verification channel for credit card fraud.

Dec 2021

High-profile phishing scams targeting OCBC customers.

Aug 2021

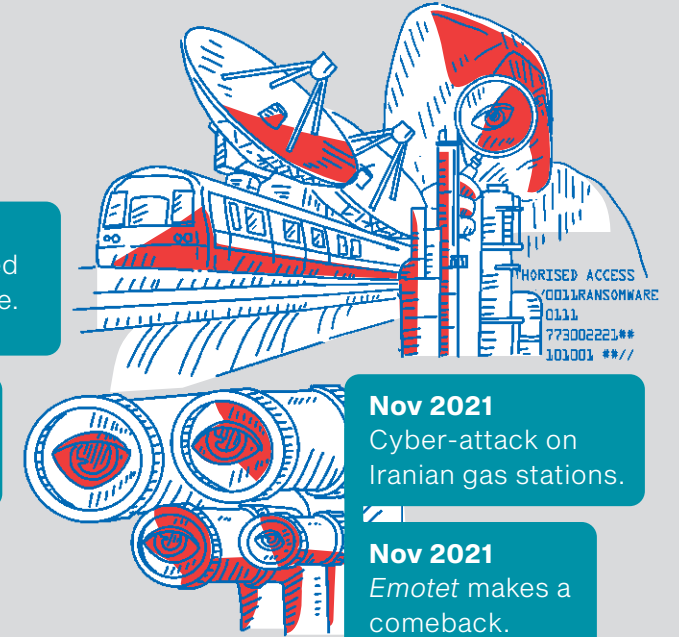
Ransomware attack on Eye & Retina Surgeons.

Aug 2021

Unauthorised access of MyRepublic's mobile customers' data.

Nov 2021

Cyber-attack with data theft on Swire Pacific Offshore.





Global Trends in 2021

2021 saw a spate of high-profile malicious cyber activities, such as ransomware attacks on Colonial Pipeline and JBS Foods, as well as attacks exploiting weaknesses in popular software such as Accellion FTA, Microsoft Exchange Server and Kaseya VSA. At the end of 2021, the disclosure of zero-day vulnerabilities on the widely used open-source Log4j library sent shockwaves across cybersecurity communities around the world, with hundreds and thousands of applications and enterprise services affected. In this chapter, we take a look at the most significant trends that characterised the cyber landscape of 2021.

Cyber Implications of the Russia-Ukraine Conflict

“While Singapore may be geographically distant from the conflict, we must be alive to such threats, as cyber-attacks have no respect for geographical boundaries, and cyber threats can emerge quickly.”

MINISTER FOR COMMUNICATIONS AND INFORMATION AND
MINISTER-IN-CHARGE OF SMART NATION AND CYBERSECURITY
MRS. JOSEPHINE TEO

In late February 2022, Russia’s invasion of Ukraine set off a significant conflict that had potentially serious cyber implications not only for Ukraine, but also for other countries and entities that were not directly involved. Prior to the invasion, Ukraine had already experienced a number of cyber-attacks that saw many of its government and private organisations hit by Distributed Denial-of-Service (DDoS) attacks and disruptive wiper malware attacks (which erased data on networked computers).

The following weeks saw various hacker groups keep up cyber-attacks on both Ukraine and Russia during the conflict. There was a real danger of such cyber-attacks escalating in intensity and impact over time, with consequences spilling beyond the two countries. For instance, a cyber-attack against Viasat’s KA-SAT telecommunications satellite disrupted satellite Internet services for subscribers not only in Ukraine, but across Europe.

The high level of activity by hackers in this conflict also presented concerns. Days after the invasion of Ukraine commenced, Ukraine’s Vice Prime Minister and Minister of Digital Transformation Mykhailo Fedorov called for the creation of a volunteer cyber army – the “IT Army of Ukraine” – to defend Ukraine’s critical infrastructure, as well as carry out

offensive cyber operations against Russia-linked entities. This quickly led to a call to arms by various groups.

There are serious implications when hackers rally under any particular banner. Any serious cyber incident resulting from hacking may inadvertently escalate the

conflict itself, or even be used as a pretext for escalation by one side or the other. Further, cybersecurity researchers have pointed out that hackers often lack the coordination and discipline to prevent collateral damage or unintended effects to uninvolved parties. For instance, German firm Rosneft Deutschland suffered a cyber-attack allegedly carried out by hackers claiming to represent the *Anonymous* collective, which wanted to get at Rosneft – a major Russia state-owned petroleum company.

Given the heightened geopolitical tensions and increased cyber threats arising from the conflict, CSA has been working closely with foreign counterparts, partners and vendors to monitor the evolving situation. CSA has also apprised CII owners and Trade Associations and Chambers (TAC) representatives of the conflict’s cybersecurity situation so that they may take the necessary precautions. SingCERT also published advisories, carried by local and Internet news platforms, to remind organisations and members of the public to remain vigilant.

Thus far, although most of the cyber-attacks in the conflict have been localised within Russia and Ukraine, other countries have also been targeted for their stance on the conflict through retaliatory cyber-attacks. Hacktivist



groups have already claimed responsibility for cyber-attacks in numerous countries across Europe. Beyond this, threat actors are also taking advantage of the crisis for opportunistic gains. Some are scamming their targets using

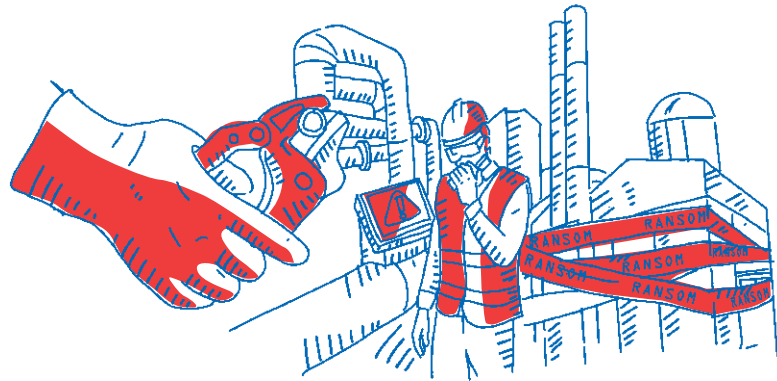
the pretext of sending money to support combatants, while others are using the conflict as a lure to trick targets into downloading malware.

Implications

Global conflicts can manifest in cyber spillover effects that may cause collateral damage beyond its intended target. Opportunistic cybercriminals can also exploit the conflict for their own benefit. To deal with such threats, there is a need to prevent, or at least minimise, direct damage to organisations’ computer systems. This includes ensuring the adoption of sound cybersecurity practices and processes, such as using up-to-date software and anti-virus software, and backing up your important data.

On a broader level, the conflict has posed a significant challenge to the rules-based international order in cyberspace. Cyber-attacks levelled against critical information infrastructure undermine the hard work by the global community to establish norms of responsible behaviour in cyberspace. The conflict may also result in a more fragmented digital landscape. The less countries have in common, the less incentive they may have to avoid damaging supranational digital infrastructure that they have no stakes in.

Massive and Systemic: Ransomware's Coming-of-Age



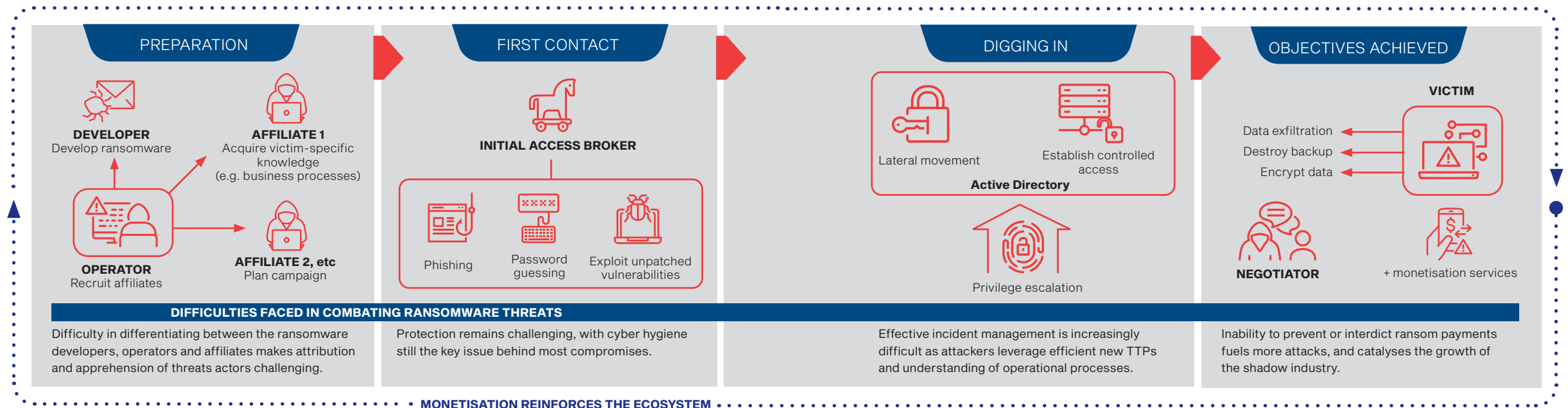
situation, local ransomware incidents reported to SingCERT spiked to 137 in 2021, 54% more than in 2020. Organisations that were most affected consisted of small and medium enterprises (SMEs) in the manufacturing and IT industries. As not every attack was reported, however, the figures may very well represent only the tip of the iceberg.

2021 marked an inflection point for ransomware. Coming off strong from years of growth, ransomware attacks further surged across multiple sectors and regions, and also caused greater impact in terms of the targets hit and the amount of ransom extorted¹. Mirroring the global

Most importantly, the year saw ransomware attacks 'graduate' fully from once sporadic and isolated incidents, into legitimate national security risks – capable of massive and systemic attacks affecting entire networks of large enterprises.

Expanded life cycle of a targeted ransomware attack

Adapted from the ODNI (Office of the Director of National Intelligence) Cyber Threat Framework



1. According to the 2022 Global Threat Report from cybersecurity vendor CrowdStrike, there were 2,686 cases of ransomware-related attacks leading to data leaks in 2021, an 82% increase from 2020. The average amount of money demanded per ransom in 2021 was US\$6.1 million, a 36% increase from 2020.

Increased Brazenness

Ransomware gangs deliberately targeted large organisations and essential service providers that could not afford downtime. Their intention was to cause extensive disruption to victims' operations and force the latter to acquiesce to high ransom demands. May 2021 saw three of the most significant ransomware incidents of the year in terms of scale and the extent of disruption caused:

- a) A ransomware attack on the IT network of the Colonial Pipeline company, which supplies some 45% of the oil and gas supply to the US East Coast, prompted the company to shut down its operations, leading to fuel shortages and price hikes.
- b) Ransomware attacks on Ireland's Health Service Executive and New Zealand's Waikato District Health Board not only leaked sensitive patient data, but also caused the shutdown of their IT systems, disrupting the delivery of essential healthcare services.

- c) A ransomware attack on JBS Foods, the world's largest meat producer by net sales, brought about a shutdown of its IT network and temporarily suspended operations at its processing plants, threatening to throw food supply chains into disarray and further inflate food prices.

Enhanced Operational Sophistication

Ransomware gangs have become more savvy and attuned to their victims' operational processes. Their improved knowledge enabled ransomware gangs to exploit weaknesses in victims' business practices, or dependencies between victims' operations and business flows, to maximise the likelihood of success and impact of their attacks. For example, hackers chose to launch their attack on JBS Foods during the US Memorial Day weekend, when organisations typically have fewer resources – and less ready – to respond to attacks. Ransomware gangs have also been known to target firms with cyber insurance, as these firms would be more likely to pay up.

More Diversified and Specialised Ransomware Ecosystem

The ransomware ecosystem matured sufficiently in 2021 for ransomware attacks to become a more accessible venture. The proliferation of Ransomware-as-a-Service (RaaS) affiliate models gave cybercriminals – even those who are less technically skilled – the wherewithal to conduct their own attacks, greatly upscaling the ransomware threat.

The diagram (previous page) illustrates the complexity of a modern ransomware operation. A sprawling cybercriminal shadow industry has risen to provide a panoply of diverse and specialised services to augment ransomware attacks, including provision of initial access to targeted networks, hosting and infrastructure services, and money laundering services. A mutually reinforcing model is now in place – the shadow industry helps ransomware gangs conduct more sophisticated and impactful attacks, while the funds from successful attacks fuel research and development, levelling up the industry’s expertise for more insidious and effective attacks to compel higher ransomware

payments. Multiple variants within the same ransomware malware family – that can either be used by different affiliated threat actors or a single group – also make it extremely challenging for law enforcement agencies to identify the actual parties responsible.

Intrusion Methods Largely Unchanged; Cyber Hygiene Remains Key

The spike in global ransomware incidents conjures up images of cybercriminals carrying out sophisticated hacks, breaking into organisations and holding valuable data to ransom. This is far from the truth: despite their increasing operational savviness, ransomware gangs typically tweak existing malware to derive new variants, and continue to rely on stolen credentials, unpatched vulnerabilities or phishing attacks to gain access into their targets. This means that organisations can largely mitigate the threat of ransomware attacks by practising good cyber hygiene, backing up data regularly, and mapping out business dependencies and ensuring business continuity plans are updated.

Implications

The ransomware incidents in 2021 were a stark demonstration of the real-world impact of cyber-attacks. The consequences of these incidents were neither abstract nor limited to merely the loss of confidentiality, integrity and availability of data and systems. With real-world impact came increased pressure to fork out ransom payments that would go into funding even more sophisticated and impactful cyber-attacks in the future. In terms of advanced

capabilities and their potential impact, these incidents showed cybercriminals rapidly catching up with the capabilities of state-sponsored APT groups. CSA is monitoring the situation closely, in case the number and impact of local cases take a more serious turn. Given the escalating threat, organisations should review their preparedness, resilience and mitigation measures vis-à-vis ransomware attacks.

Topical Focus: Global Response to the Scourge of Ransomware



As the global ransomware scourge grew in 2021, so did the global community response to the challenge it posed. Recognition that the massive and systemic ransomware attacks deserved to be treated as a national security issue galvanised multi-stakeholder coalitions, to jointly address means of mitigating the threat. Such efforts made significant headway in 2021.

- In June 2021, after tracking the ransom payment as it moved through a series of electronic accounts belonging to the ransomware group behind the Colonial Pipeline attack, the US government recovered 63.7 of the 75 Bitcoins (about USD 3 million of the USD 5 million) in ransom paid by the victim.
- Following an EU-US Ministerial Meeting on Justice and Home Affairs in June 2021, both sides agreed to improve coordination and set up a working group to fight ransomware.
- In October 2021, the US government hacked into the IT infrastructure of REvil, a major ransomware gang, gaining control over a few of the gang’s servers and forcing the websites that it used to leak victims’ data and conduct business offline. Shortly after, the US government arrested and indicted members of the gang and seized USD 6 million of its assets.
- At the Counter Ransomware Initiative Meeting convened by the US in October 2021, officials from more than 30 countries, including Singapore and countries from Europe, Africa and the Middle East, agreed to step up cooperation to fight ransomware, including through information exchange and promotion of rules-based behaviour.

Declaring victory on ransomware is premature at this point, but the global response to ransomware has had notable effects.

- Ransomware groups’ ability to advertise to potential customers has been adversely affected. The global spotlight on ransomware has made cybercrime forums more hesitant to host ransomware operators. Fewer trusted platforms to host and facilitate interactions means less easy access to customers and potential affiliates, greater difficulty in transferring money, and higher risk in the transactions that do manage to take place.
- As a result of governments’ more proactive information-sharing and issuance of advisories, industries and the general public have become more informed and aware of how to defend themselves from ransomware attacks.
- Some ransomware groups appeared to be redirecting efforts from prominent big companies to more modest targets in a bid to escape attention. Such a shift may reduce the chances of a disruption of essential services, but does not preclude the possibility of major campaigns resulting in serious consequences.

Each Sold Separately: Proliferation of Cyber Tools and Access Services



Over the course of 2021, there were a number of developments regarding the proliferation and possible abuse of cyber tools and network access services on a global scale, including:

- A growing market for initial access brokers (IAB) – hackers who sell access to breached networks or systems. One study estimated a more than 50% increase between 2020 and 2021 in the number of IAB listings advertised on underground forums². The listings from 2021 promised access, for a fee, to networks of organisations across more sectors and more countries than any previous years.
- Microsoft and Canada-based think-tank Citizen Lab’s allegations that a spyware by Israeli firm Candiru had infected the devices of more than 100 victims based in Palestine, Singapore, Israel, Iran, Lebanon, and the UK, among other countries. In its advisory on Candiru’s spyware, Microsoft emphasised that the presence of victims in a country did not indicate that they had been targeted by the country’s government, since international targeting was common.

- An investigation by a group of 17 news outlets worldwide revealed possibly widespread abuse of a military-grade spyware, *Pegasus*. The findings uncovered more than 50,000 phone numbers that belonged to people whom *Pegasus* may have been directed to target – government officials (including ministers and heads of government), human rights activists, business executives, journalists, academics and religious figures from more than 45 countries across four continents. *Pegasus* is able to extract messages, photos and e-mails, obtain the target’s location, record calls and secretly activate microphones and cameras. It can be installed on a targeted device through vulnerabilities in common apps, or by tricking the target into clicking a malicious link. In response, the firm behind *Pegasus* said that its product was intended only for use against terrorists and criminals, and that its customer base comprised only vetted government bodies.

² Initial Access Brokers in 2021: An Ever Expanding Threat, 16 February 2021 – <https://digitalshadows.com/blog-and-research/initial-access-brokers-in-2021-an-ever-expanding-threat/>.



Implications

The selling of malware for profit, or hacking-as-a-service, is not a new phenomenon. Demand is strong, and likely to remain so, for three reasons: (a) customers are not technically proficient enough to create effective malware or breach networks on their own; (b) using readily available toolsets or access allows threat actors to commit more time and resources to scale up their malicious cyber operations; and (c) because they wish to mask their tracks and stymie attribution efforts.

Commercial cyber tools and initial access broker services “democratise” cyber-attacks. Where highly sophisticated cyber espionage capabilities and privileged access with domain administrator rights used to be the preserve of “cyber superpowers”, they are now available to any who can afford them. There is also scant evidence that peddlers exercise any significant oversight as to whether their customers are using the purchased tools and network access judiciously. Taken together, the implication is that we can expect a bigger pool of more reckless and indiscriminate cyber threat actors should the market continue expanding.

Living Off the Land: Vulnerabilities in the Supply Chain and Popular Software

Targeting software supply chains allows cyber threat actors to increase the scale of their attacks. They can access multiple victims by leveraging the vulnerabilities of a popular software, or through a single initial compromise. Several notable incidents in 2021 spoke to this method's effectiveness.

- In February 2021, hackers, likely from the Clop ransomware group, exploited zero-day vulnerabilities on Accellion's File Transfer Appliance (FTA) software, a file-sharing program widely used by large corporations, to conduct a series of cyber-attacks on companies worldwide, threatening to expose stolen data if their ransom demands were not met. Even Singtel, a customer of Accellion, was affected when hackers exfiltrated data belonging to Singtel customers.
- In March 2021, Microsoft reported that a state-backed hacking group, HAFNIUM, had exploited four zero-day vulnerabilities within on-premises versions of Microsoft Exchange Server, a widely used e-mail-management software. This enabled HAFNIUM to steal information such as e-mails and credentials, and plant malware that would facilitate persistent remote access to targeted networks. Microsoft said that HAFNIUM had targeted primarily US entities. The exact number of affected entities was unknown but, owing to the ubiquitous use of Microsoft's software, insiders with knowledge of investigations into this malicious campaign estimated that "at least 30,000 organisations across the US" along with "tens of thousands" of organisations in Asia and Europe had been affected.

- In July 2021, the REvil ransomware group exploited a zero-day vulnerability in Kaseya's Virtual System Administrator (VSA) software, a platform popular among corporations and managed service providers (MSPs) to help organisations manage IT services remotely. In doing so, the hackers were able to directly deploy ransomware to the MSPs, and through these MSPs, further infect the organisations whose IT services were managed by these MSPs. The impact was widespread and, in some cases, had real-world impact. For instance, Swedish supermarket chain Coop had to halt operations across 500 stores in Sweden when its system was infected with ransomware delivered via its MSP, which was a user of Kaseya VSA.

Implications

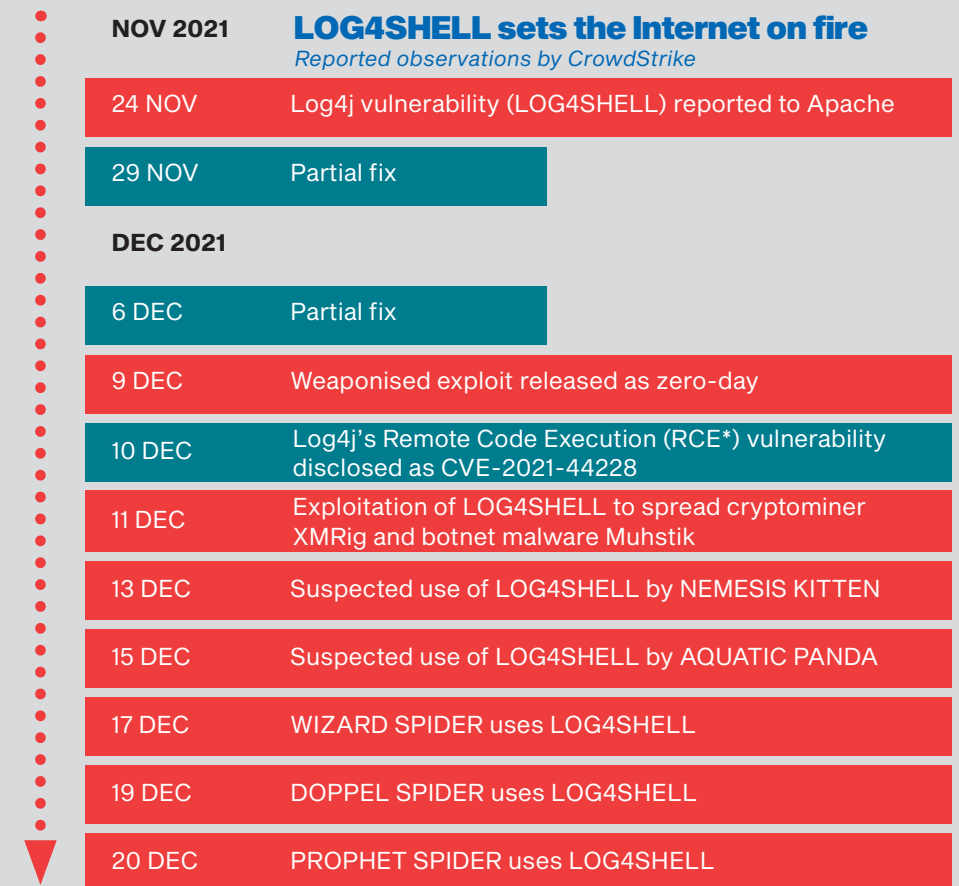
Exploiting supply chain vulnerabilities undermines the trust-based relationships that organisations have with their MSPs and with the software they use. Managing cybersecurity of the supply chain is not purely an IT preoccupation. It is a coordinated business endeavour involving sourcing, vendor management and careful evaluation of the supply chain quality across multiple functions. The average application today contains well over 500 open-source components, each one of them a potential source of vulnerability. Enhancing IT asset visibility and employing layered defensive measures will help. As 2021 wound down, the global cybersecurity community would find itself contending with the fallout of a critical vulnerability in Log4j, a ubiquitous open-source component.

Topical Focus: Opening the Floodgates – Log4j's Widespread and Critical Vulnerability

CONTRIBUTED BY CROWDSTRIKE

High-profile software vulnerabilities may be discovered at a moment's notice, without any prior warning to either their existence or severity. There were a number of noteworthy vulnerability discoveries, disclosures, and subsequent exploits by sophisticated adversaries throughout 2021. The discovery of the Log4j vulnerability at the end of the year culminated in far more attention than any other, primarily due to its ubiquity across Apache Web Server installations which power more websites than any other web server software.

The vulnerability, nicknamed "LOG4SHELL", was reported on 24 November 2021 and a proof-of-concept soon circulated on social media and code-sharing platforms on 9 December 2021. Thereafter, both cybercriminals and state-sponsored threat actors exploited LOG4SHELL in multiple products and services to deliver malicious payloads. Threat actors were able to inject arbitrary Java code into these affected services, crafting special requests resulting in access into the system, delivery of malware, or acquisition of sensitive data such as user credentials.

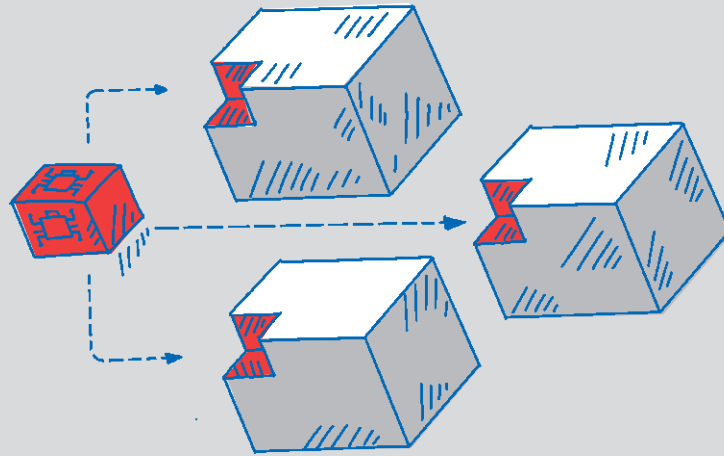


*Remote Code Execution (RCE) attacks allow an attacker to remotely execute malicious code on a computer.

During the final weeks of 2021, CrowdStrike Intelligence observed multiple threat actors incorporating LOG4SHELL exploitation into their operations. Cybercriminals, ever so opportunistic, enthusiastically adapted their tradecraft, leveraging LOG4SHELL in common botnet malware, such as *Muhstik* and others. DOPPEL SPIDER and WIZARD SPIDER, two of the most active cybercriminal groups throughout the year, incorporated LOG4SHELL as an access vector to drive their *Grief*, *Conti*, and *Ryuk* ransomware operations. State-sponsored actors, such as NEMESIS KITTEN and AQUATIC PANDA, were also observed adopting LOG4SHELL exploitation in their offensive operations.

The LOG4SHELL vulnerability is serious because of how pervasively Apache is used across the Internet and the ease with which exploitation can be accomplished. Akin to a screw used in the construction of everything from chairs to cloud servers, any flaw in such a basic build component can result in far-reaching and potentially catastrophic consequences downstream. This makes it an attractive target for adversaries who recognise the difficulty of patching these systems due to their importance. One minor misstep during a security update may lead to excessive downtime, potentially affecting mission-critical operations. Given the abundance of unpatched systems, attackers seized upon this vulnerability to conduct financially- and espionage-motivated attacks. Additionally, the use of different protocol and obfuscation techniques has led to essentially limitless techniques for triggering the exploits.

Widespread media attention and rapid remediation efforts likely dampened the impact



of widespread and persistent LOG4SHELL exploitation. However, public proof-of-concept code to exploit LOG4SHELL in additional products and servers will likely surface throughout 2022, and may potentially lead to intermittent exploitation surges.

Many additional state-sponsored actors are likely to integrate LOG4SHELL exploits into their toolchain, since this logging library provides a method through which actors can gain access to target environments via vulnerable entry point systems or move laterally by exploiting internal servers on already compromised networks. This assessment is based on the vulnerability's massive prevalence. However, not all impacted products can be exploited with the same technique, and tailoring of exploits for specific targets will likely be required.

Threat actors are likely to continue integrating increasingly effective exploit chains to rapidly achieve remote code execution, seeing the substantial number of related incidents – such as the ProxyLogon and ProxyShell³ hacks – that emerged over the whole of 2021.

3. ProxyLogon and ProxyShell refer to two groups of vulnerabilities within the Microsoft Exchange Server software identified in March 2021 and July 2021 respectively. Hackers have been exploiting these vulnerabilities to conduct multiple cyber-attacks.

Implications

We should all operate under the assumption that there will be a future LOG4SHELL-like event, with potentially the same if not more significant impact across the globe. Specifically, LOG4SHELL is an important lesson in recognising that open-source software, even if it is ubiquitous and has presumably been validated by generations of users, is likely just as vulnerable as closed-source or proprietary software.

Apache Web Server is a free open-source software (FOSS). This potentially played a significant role in the high volume of affected servers available for exploitation by threat actors, as Log4j is commonly incorporated into Apache Web Server installations. In addition, the incident also demonstrates how organisations are willing to easily adopt FOSS even though it lacks robust quality assurance standards.

The cybersecurity community's swift mobilisation

Overall, the global cybersecurity community swiftly mobilised to assess the situation, with a fix being provided essentially at the same time the disclosure was published. This rapid identification of the LOG4SHELL vulnerability, assessment of its impact, and quick deployment of an updated version

made available to the global community likely contributed to far fewer opportunistic attacks, than had there been longer timelines between disclosure and security patching.

The timely patching and mitigation efforts were likely the result of a world much more attuned to cyber-attacks of increasing sophistication. This is no coincidence: the acceleration of malicious cyber activities, due to the intricate cybercriminal ecosystem materialising over the last two to three years, has caused the cybersecurity community to be far more vigilant than before. In addition, major events like the Solarwinds and Kaseya attacks have had a unique impact on how cybersecurity practitioners are evolving their situational awareness of the attack surface.



67DZ88Z002Z59Z09Z355D008G008Z9Z997Z265Z(<A>+RETURN) ?#



355D008G008Z9Z997Z265Z(<A>+RETURN) ?#

67DZ88Z002Z59Z09Z355D008G008Z9Z997Z265Z(<A>+RETURN) ?#

67DZ88Z002Z59Z09Z355D008G008Z9Z997Z265Z(<A>+RETURN) ?#





WWW.TARGET.SG

In 2021, various cyber threats – such as ransomware attacks, phishing campaigns and data breaches – continued to affect Singapore organisations and remained a key concern. Phishing attacks targeting users of Internet banking services continued to rise, culminating in a series of high-profile phishing scams affecting OCBC bank in December 2021. This chapter expounds on such threats through case studies of actual incidents in Singapore. Also included are CSA's observations of trends and insights on the level of cyber awareness in Singapore, and key threats to Singapore's cyber landscape in 2021.

Survey on Cyber Awareness – Findings and Insights

Improved Cyber Awareness, But Adoption Remains Low

CSA conducted the national Cybersecurity Awareness Survey 2020 in December 2020, polling 1,052 Singapore citizens and permanent residents aged 15 years old and above to better understand their general attitudes and behaviours towards cybersecurity practices and incidents.

The survey results – announced in June 2021 in conjunction with the launch of CSA’s national cybersecurity awareness campaign – showed that nearly four in 10 respondents had fallen victim to a cyber incident at least once in 2020, an increase from three in 10 in 2019. This increase reflected global trends of increasing prevalence of cyber incidents. In addition, the results indicated that although general awareness of cybersecurity had improved, adoption of good cyber hygiene practices – such as enabling two-factor authentication (2FA) and installing anti-virus applications – continued to be low.

For example, perceived awareness of phishing in 2020 had improved with seven in 10 respondents knowing what phishing was – a six percentage point increase from 2019. Three-quarters of respondents were able to correctly identify more than half the e-mails, an improvement of 12 percentage points over 2019.

A slight increase was also seen in those who adopted desirable password practices: close to nine in 10 respondents used a combination of letters in upper and lower cases, numbers and symbols in their passwords. However, only slightly more than half of the respondents (56%) were able to identify a strong password – unchanged from the year before.



There was also a slight increase in respondents who adopted 2FA, although only about half had adopted the additional practice of enabling 2FA as an additional layer of protection for their communication, online shopping and social media accounts.

While nearly eight in 10 respondents were aware of the risks of not having cybersecurity applications, only 39% of respondents had installed cybersecurity applications on their mobile devices, a drop from 47% in 2019.

The results of the survey, while encouraging, clearly demonstrated the need for greater efforts in driving both the awareness and adoption of good cyber hygiene practices. CSA continues to work with our partners to deliver suitable initiatives on both fronts.



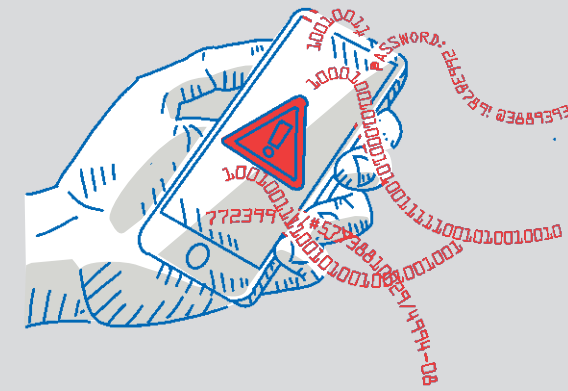
Local case studies

This section features selected case studies of local enterprises and companies that were compromised by cyber threats in 2021, so that organisations can take suitable precautions to prevent similar incidents from happening to them.

Case Study: Data Breaches Affecting Local Enterprises and SMEs

All Your Data Belongs to Us

Data breaches in the Infocomm sector



Follow-up Action

The telecommunications companies responded quickly in mitigating the effects of the data breaches and preventing further unauthorised access. Remediation efforts included the removal of unauthorised access and securing the data storage platform, as well as informing and working closely with relevant authorities, such as CSA, Singapore Police Force (SPF), and Personal Data Protection Commission (PDPC). In one of the incidents, non-essential systems were immediately shut down to prevent further exfiltration of data. In addition, activities on the Dark Web were also monitored for attempts to sell the stolen data.

What Happened

In 2021, local telecommunications companies suffered data breaches, causing the personal data belonging to victims to have potentially been leaked online. In one incident, hackers obtained unauthorised access to the system via a third-party data storage platform, leaking personally identifiable information (PII), including identity verification documents related to customer applications for mobile services. In another incident, details of the telecommunications firm’s corporate customers were stolen as part of a wider global data breach when French technology firm Accellion’s File Transfer Appliance (FTA) software was compromised by hackers.

Due to the high penetration rate of mobile and Internet subscribers in Singapore, firms in the telecommunications industry contain treasure troves of personal data and information that cybercriminals may target. Organisations with massive customer databases, in particular, would be attractive to cybercriminals gunning for a large payday through extortions or selling the data via Dark Web marketplaces. Firms with large amounts of customer data should always secure their data, back up their systems where appropriate, upkeep proper cyber hygiene, and most importantly, ensure their third-party vendors also do the same.



Piling on the Pressure

Extortion-related Data Breaches by ALTDOS Group

What Happened

Although relatively new, the ALTDOS cybercriminal group nonetheless made waves by breaching and attempting to extort from a number of local enterprises, targeting four different SMEs from March 2021 to August 2021. The cybercriminal group's tactics were inconsistent; while they encrypted victims' data and also threatened to leak it unless their demands were met (a tactic known as 'double-extortion'), in some cases, ALTDOS merely exfiltrated data and demanded a ransom in others. The group also launched DDoS attacks against the online assets of several victims, as an additional pressure tactic. ALTDOS appeared to be focused on ASEAN; other than Singapore, several organisations in Bangladesh, Thailand and Malaysia were also hit.

Follow-up Action

Like ALTDOS, cybercriminal groups that have a geographical focus tend to be opportunistic, and utilise similar TTPs against victims across different countries. CERT-to-CERT cooperation and information sharing are hence crucial in mitigating the threat of such cybercriminal groups, and developing a better appreciation of their tactics. CSA worked closely with the Singapore Police Force (SPF), the Personal Data Protection Commission (PDPC) and our overseas partners, issuing an advisory and warning of the threat posed by the group and its corresponding TTPs.

The fact that some of ALTDOS' victims were unaware that their systems had been breached – until contacted by the cybercriminals – highlights the need for organisations to have strong situational awareness of their network activities. In addition, organisations would need to properly secure their data, schedule regular patching, practise network segregation, and create backups in business continuity plans to mitigate these threats.

Case Study: Phishing Attacks Targeting Oversea-Chinese Banking Corporation Limited (OCBC) Clients

What Happened

Local media reported a sharp increase in the number of victims falling prey to phishing scams spoofing OCBC bank between late December 2021 to early January 2022, which saw 790 customers lose \$13.7 million to the scammers. OCBC reported that the phishing campaign was "particularly aggressive and coordinated".



What made this particular phishing campaign stand out was the fact that the scammers leveraged seemingly legitimate SMS SenderIDs to impersonate OCBC and direct their victims to imitation websites to share their user credentials. This lent credibility to the scam SMS messages, whilst invoking a sense of fear and urgency in the users by threatening a suspension of account, or ironically, claiming that the user had been hacked.

Looking back, the phishing campaign was also successful due to the sheer number of phishing links that were set up to target OCBC. In fact, phishing links targeting OCBC sharply increased in December 2021 (i.e. 25 times over the monthly averages in 2021, mirroring the 20 times increase in the average call volume the bank received over the scams in December 2021). Further, many of the malicious links detected had similar domain-naming conventions and were likely set up by the same group of scammers. While phishing scams have traditionally been opportunistic and relied on unsophisticated social engineering techniques, this particular campaign seemed to be targeted and coordinated. It also demonstrated how

the scammers leveraged their understanding of bank processes to maximise the chances of success.

Follow-up Action

CSA worked with the Singapore Police Force (SPF) and OCBC to take down more than 350 phishing websites throughout December 2021 and January 2022. However, the scammers were quick to create new phishing websites as quickly as they were taken down. Hence, public awareness was essential to prevent more members of the public from falling prey to this scam. The Monetary Authority of Singapore (MAS) has since worked with financial institutions in beefing up their cybersecurity and tightening their business processes (such as implementing compulsory cool-down periods during which high-risk transactions are prohibited) to prevent scams from succeeding. Clickable links within SMSes or e-mails sent to customers have since been removed.

State of Singapore's Cyberspace

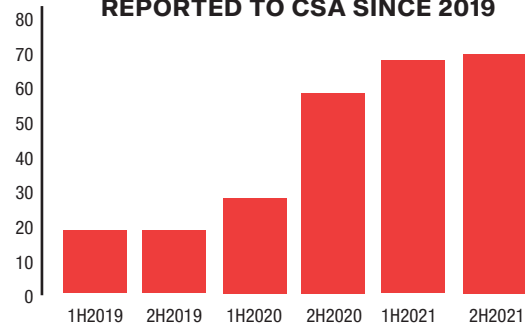
The increasing pace of digitalisation worldwide and in Singapore greatly expanded the attack surface. This section looks at some of the malicious threat activities that CSA observed in our local cyber landscape – such as ransomware, phishing, botnet drones and website defacements.



Ransomware

Ransomware remained a major issue globally, with cybersecurity vendors observing an increase of over 80% in the number of incidents reported worldwide. For Singapore, 137 ransomware cases were reported to CSA in 2021, continuing an upward trend that began in 2019. Affected entities were largely SMEs, hailing from sectors such as manufacturing and IT. As these two sectors often run 24/7 operations and may not be able to afford the downtime to patch their systems, ransomware groups may exploit such vulnerabilities, targeting them as “low-hanging fruit”.

NUMBER OF RANSOMWARE CASES REPORTED TO CSA SINCE 2019



The sustained increase in the number of ransomware cases is a worrying trend. Local developments have begun to mirror global trends. Indeed, several ransomware groups that targeted Singapore SMEs were already observed to utilise the RaaS model, where developers lease shared infrastructure to affiliates for distribution of the ransomware payload without the need to develop native organic capabilities.

This significantly lowers the barrier to entry for even amateur or less-skilled hackers, even if this ‘spray-and-pray’ approach often only manages to compromise SMEs with weaker cybersecurity. Ransomware strains that employed the RaaS model and were observed to target Singapore SMEs included *LockBit*, *MedusaLocker*, *Makop*, and the infamous *REvil/Sodinokibi*.



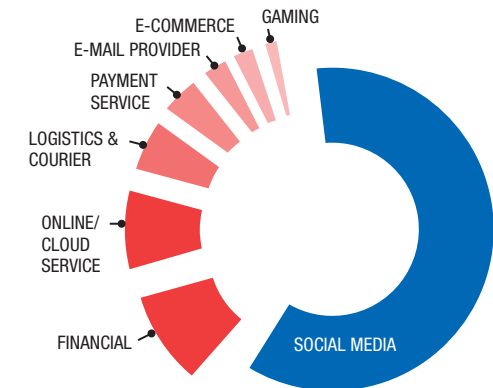
Phishing

About 55,000 unique phishing URLs were observed to be hosted on Singapore infrastructure in 2021, a 17% increase from 2020's figures, mirroring global trends. Phishing continues to be a popular attack vector for malicious actors to gain access into systems before deploying other payloads such as ransomware and other malware.

public interest in WhatsApp's updated privacy policy announcement on how users' phone numbers would be shared with Facebook.

Social networking firms (WhatsApp and Facebook, both owned by Meta) made up more than half of the spoofed targets. Spikes in the months of March, June and July were driven by increases in phishing URLs spoofing these social networking firms, as malicious actors exploited

The Ministry of Health (MOH) was the most commonly-spoofed Singapore Government agency, given the ongoing COVID-19 pandemic. There were also a number of cases in which scammers impersonated the Ministry of Manpower (MOM) and CSA. In most of these cases, scammers spoofed the authorities to trick victims into divulging their credentials or personal data. Impersonation of MOH grew substantially as Singapore's COVID-19 cases surged with the emergence of the Omicron subvariant in the last quarter of 2021.



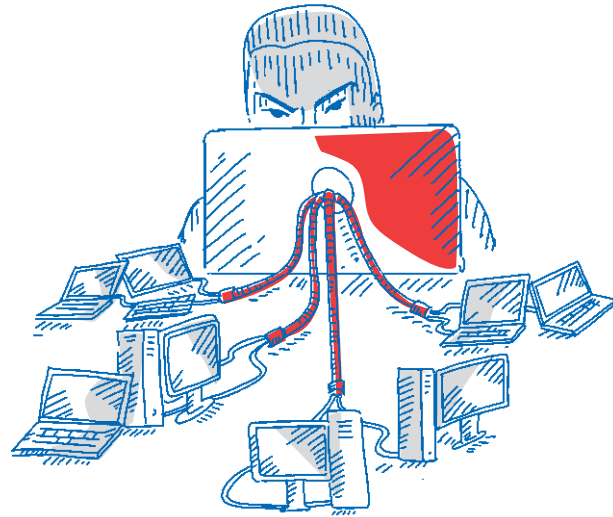
COMMONLY SPOOFED SECTORS

NUMBER OF SINGAPORE-HOSTED PHISHING SITES IN 2021

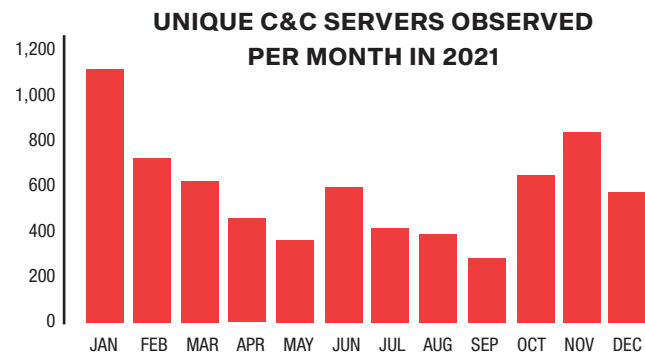


C&C Servers

3,300 unique C&C servers were observed to have been hosted in Singapore across the whole of 2021, almost three times more than in 2020, and the largest number recorded since 2017. This was near-identical to the three-times increase in global C&C servers activity that cybersecurity vendors reported over the same period.



This spike was driven by a large increase in servers distributing *CobaltStrike* malware, which made up nearly 30% of all C&C servers observed. *CobaltStrike*, originally a paid penetration testing product, has become a common tool for threat actor groups to gain initial access to computer systems, and exploit them for malicious activities such as ransomware attacks. This development was consistent with observations by cybersecurity firm Recorded Future, which had also reported a large spike in threat actors compromising servers to distribute *CobaltStrike* globally, and that these were the most commonly observed type of C&C infrastructure in 2021.



Cybersecurity researchers had warned in January 2021 that a DanaBot malware variant was targeting cryptocurrency wallets and infecting systems with cryptomining malware. As Bitcoin prices soared during the first quarter of 2021, the malicious activities of DanaBot also increased correspondingly.

DanaBot, a relatively new banking trojan, also made the list of top malware types distributed by C&C servers hosted in Singapore for 2021.

Botnet Drones

The number of infected botnet drones in Singapore closely mirrored the decreasing trend in global infections, with about 4,800 botnet drones with unique Singapore IP addresses were observed daily on average, a 27% decrease from 2020's daily average of 6,600. Malware strains for the infected drones varied greatly, and there was no single strain that had a clear majority among the compromised devices. This was dissimilar to the situation in 2020, where *Mirai* and *Gamarue* variants dominated within the infected botnet drones.



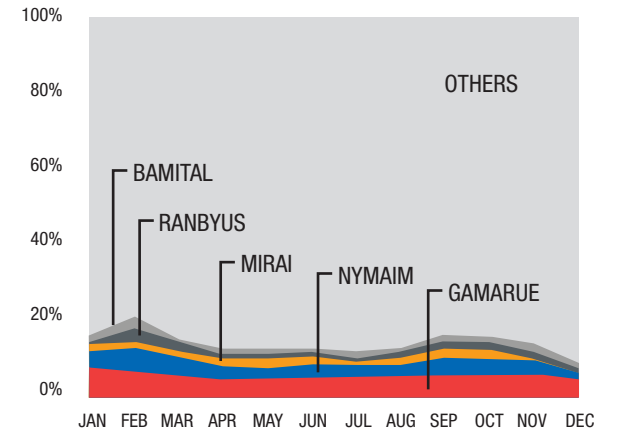
This trend could have been caused by threat actors diversifying away from 'old' malware strains and exploring new infection methods, as system owners cleaned up their infected computers and devices progressively, a process likely catalysed by the takedown of *Gamarue* malware infrastructure in 2017.



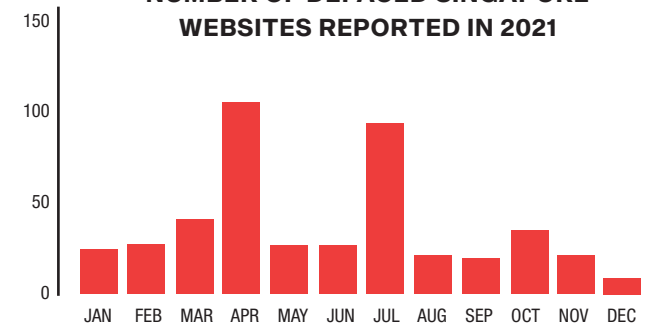
Website Defacements

419 '.sg' websites were defaced in 2021, a decrease of 15% from 2020. An overall downward trend in website defacements has been observed since 2019 as hacktivist activities continued to move to other platforms which have a wider reach, such as social media.

The overwhelming majority of victims were SMEs. April and July 2021 saw noticeable spikes in the number of website defacements as hackers 'Ren4Sploit' and 'imam' conducted mass defacements indiscriminately on Singapore SMEs' websites. Other than claiming credit for the defacements, the hackers left no additional messages in their handiwork. This was in contrast to previous years where



NUMBER OF DEFACED SINGAPORE WEBSITES REPORTED IN 2021



politically-motivated website defacements would draw references to global developments.

As the mass defacements by 'Ren4Sploit' and 'imam' occurred within one-day periods, it is likely that they used automated scripts to deface unpatched websites indiscriminately. A quarter of the total defaced websites were also re-defacements, as vulnerable websites were repeatedly targeted due to poor security and cyber hygiene on the part of the website owners. Checks on a representative sample of defaced websites revealed poor website maintenance and negligence towards patching. Hackers also tended to target WordPress websites running outdated versions (ver. 5.6 and earlier).



Transitioning to Cybersecurity Strategy 2021

The original cybersecurity strategy was launched in 2016 to set out the nation's vision, goals and priorities for a resilient and trusted cyberspace. As the strategic and technological environment evolved over the years, our cybersecurity strategy has been refreshed to address new and emerging cyber threats. Strategy 2021 takes a more proactive stance in addressing threats via a broader scope of protection, closer relationships with international partners, and a greater emphasis on workforce and ecosystem development as key enablers towards a safe and secure cyberspace.

With the launch of Cybersecurity Strategy 2021, CSA has embarked on various initiatives under each of the pillars and foundational enablers. This edition of the Singapore Cyber Landscape highlights some of the key efforts and thrusts that support the transition to Strategy 2021, and how they contribute towards strengthening the security and resilience of our digital infrastructure.

Updating Strategy 2016



Singapore's Cybersecurity Strategy, first launched in 2016, needed to adapt to key shifts in our operating landscape.

The maturing of disruptive technologies such as AI, 5G, and cloud has reshaped old operating models, requiring new approaches to cybersecurity. Physical and digital worlds are increasingly converging, creating risks of physical harm and challenging our previous approach to preventing disruption and data exfiltration. Attack surfaces have grown, and there has been a surge in the volume and sophistication of threat actors. International cyber discussions have expanded in scope, and are increasingly affected by geopolitical tensions.

These shifts present new challenges. The focus of our capability development and legislative efforts would need to change to keep up with the pace of technological change. Given cyber-physical risks associated with Operational Technology (OT), dedicated effort is needed to shore up defences in this area. Cybersecurity measures would need to be calibrated, both to secure a wider attack surface in a resource-efficient manner, and to manage threats beyond critical information infrastructure.

International discourse on cybersecurity should be kept technical and objective to avoid the pitfalls of politicisation amidst ongoing geopolitical contestation.

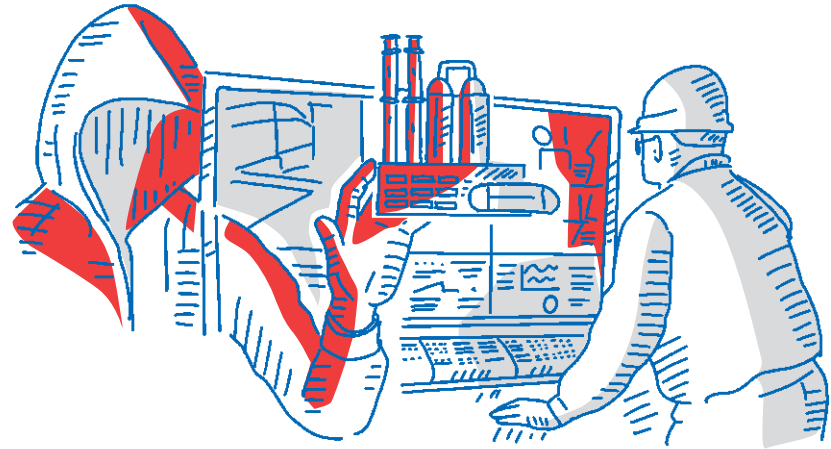
To meet these challenges, CSA has updated and reorganised Singapore's Cybersecurity Strategy. As a technological domain, cybersecurity is enabled by strong capabilities. Harnessing cybersecurity requires building strong capabilities in the private, public and people ecosystems that can come together to achieve our security and economic objectives. To that end, CSA has positioned the development of a vibrant cybersecurity ecosystem as a foundational enabler. Another foundational enabler is a new category of initiatives to grow a robust cybersecurity talent pipeline, as success in cybersecurity requires a robust and sustainable pool of talent. This new horizontal emphasises our commitment to growing the talent pipeline and developing cyber professionals. Key pillars from Strategy 2016 – building resilient infrastructure, enabling a safer cyberspace, and strengthening international partnerships – remain integral, and have been improved upon and expanded where necessary to remain up-to-date with the shifts in the digital landscape.

Strategic Pillar 1: Build Resilient Infrastructure

2021 provided a stark reminder that cyber-attacks have crossed from the digital to the physical realm. As more industries adopt OT to manage their systems and meet the growing demand, the attack surface increases. Episodes like the Oldsmar water plant hack in Florida in February 2021 and the Colonial Pipeline ransomware attack in May 2021 reinforced the urgency with which CSA has been putting the **Operational Technology Cybersecurity Masterplan** into action.

Launched in October 2019, the OT Cybersecurity Masterplan serves as a blueprint for enhancing the security and resilience of Singapore's CII sectors, improve cross-sector responses to mitigate cyber threats in the OT environment, and strengthen partnerships with stakeholders. This section showcases progress made in three key aspects of the OT Cybersecurity Masterplan, as well as exercises with the CII sectors.





OT Cybersecurity Expert Panel (OTCEP)

The OTCEP was established to augment efforts under the OT Cybersecurity Masterplan. The OTCEP comprises 11 local and international OT cybersecurity experts. It allows Singapore’s OT cybersecurity practitioners, operators, industry, researchers, and policymakers from the Government, CII sectors, academia and other OT industries to have direct access to the internationally renowned experts. The inaugural meeting of the OTCEP, held in September 2021, initiated conversations about OT cybersecurity, with the OTCEP presenting recommendations on strategies to enhance the cyber resilience of Singapore’s OT sector.

OT Cybersecurity Competency Framework (OTCCF)

OT professionals, organisations and training providers share a common need for guidance in enhancing their skillsets. To meet this need, CSA developed the OTCCF in consultation with more than 70 stakeholders from the OT and cybersecurity industry, Institutes of Higher Learning (IHLs) and government agencies. The OTCCF was launched on 8 October 2021, by Minister for Communications and Information and Minister-in-Charge of Smart Nation and Cybersecurity Mrs. Josephine Teo. The OTCCF serves as a guide for:

- CII leads and operators to identify skillsets and training for their engineers;
- Training providers to develop best-in-class courses and certifications that cater to local training needs; and
- OT professionals to chart a pathway in enhancing their OT cybersecurity competencies.

OT Train-The-Trainers (OT TTT) Programme

With a growing demand for OT knowledge and COVID-19 travel restrictions limiting invitations to overseas OT experts to Singapore to provide training, CSA conceptualised an OT TTT programme to develop a pool of OT trainers. The programme aims to achieve the following outcomes:

- Build a pool of local trainers to deliver OT cybersecurity training;
- Empower participating IHLs to incorporate OT cybersecurity into current courses; and
- Drive the development of OT cybersecurity training courses to align to the OTCCF.

There are two modules in the OT TTT programme. The run for the first module was conducted in November 2021. CSA will continue to work closely with local IHLs to roll out more modules of the programme.

Exercise Cyber Star 2021

Building a resilient infrastructure requires strong cooperation amongst stakeholders. CSA works closely with CII sector leads and CII owners to conduct cybersecurity exercises to ensure that cybersecurity capabilities and measures are in place to detect, respond to and recover from cyber-attacks. These exercises help CSA assess the capabilities of sector leads and CII owners in managing sector-specific cyber incidents and identifying gaps for improvement.

One such exercise that was conducted from November 2021 to January 2022 was Exercise Cyber Star 2021, which saw more than 200 exercise participants representing sector leads and CII owners. Participants responded to various scenarios ranging from supply chain compromise to ransomware and compromise of OT systems. The conduct of the exercise started to ramp up in November 2021 with a series of technical exercises, operational workshops, table-top discussions and crisis management meetings conducted at the sectoral and national level to exercise and validate CII sectors’ response plans. CSA led incident management and response while government agencies and CII owners coordinated in information sharing and knowledge exchange as they responded to cyber incidents. Processes pertaining to crisis response and recovery were also tested and reviewed to ensure critical systems could be restored as quickly as possible in the event of a significant cyber-attack.

The exercise culminated in a presentation by exercise participants to senior leadership on 28 January 2022 regarding their incident management and remediation plans. Mrs. Josephine Teo, the Minister for Communications and Information and Minister-in-Charge of Smart Nation and Cybersecurity, was the Guest-of-Honour for the exercise and was briefed on the efforts undertaken by CII sector leads to improve cyber readiness.



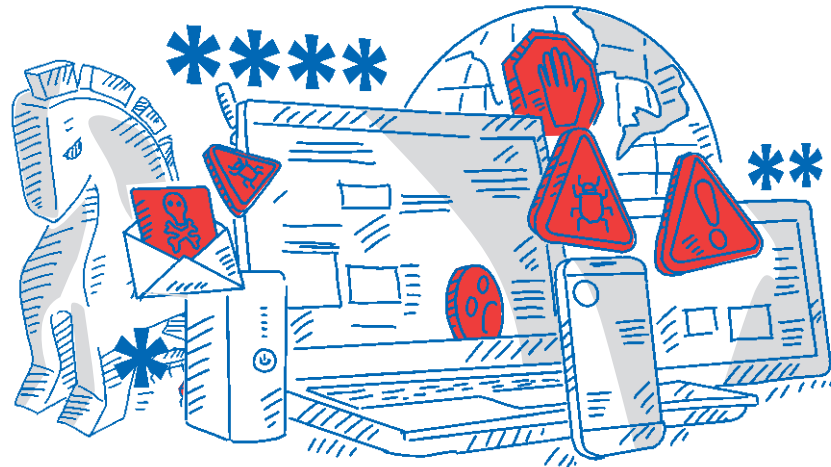
Top: Minister for Communications and Information & Minister-in-Charge of Smart Nation and Cybersecurity Mrs. Josephine Teo interacting with exercise participants at Exercise Cyber Star 2021. Source: MCI

Bottom: Minister for Communications and Information & Minister-in-Charge of Smart Nation and Cybersecurity Mrs. Josephine Teo at Exercise Cyber Star 2021. Source: MCI

Red Teaming Exercise

CSA, in collaboration with a CII sector lead, embarked on a learning journey through a Red Teaming exercise in 2021 to enhance the cybersecurity resilience of our CII. The goal was to augment the conventional approach of passive and reactive cybersecurity defence with an “assume breach” and more proactive mindset. Beyond just testing technical systems for vulnerabilities and potential intrusion vectors, this meant adopting a more holistic perspective covering people, processes and technology for enhanced real-world cyber resilience and readiness. The six-month long exercise highlighted that, beyond prevention measures, building up detection and response capabilities against real-world threats will significantly limit the attack surface and increase the costs associated with carrying out cyber-attacks.

Strategic Pillar 2: Enable a Safer Cyberspace



The Cybersecurity Labelling Scheme

The Cybersecurity Labelling Scheme (CLS) for consumer smart devices seeks to improve Internet of Things (IoT) security and raise overall cyber hygiene levels. By labelling smart devices, the CLS provides greater transparency to these devices' cybersecurity provisions. Consumers can then make more informed purchasing decisions with greater cybersecurity consciousness.

Since its launch in October 2020, the CLS has garnered interest locally as well as in countries such as Australia and the US. It has received more than 250 applications, with more than 150 labelled devices – from Wi-Fi routers and smart home hubs to smart switches and sensors. CSA is in talks with like-minded partners on mutual recognition of labelling schemes. Singapore and Finland signed a Memorandum of Understanding in October 2021 to mutually recognise each other's cybersecurity labels.

Securing Contracting Systems in Singapore

CSA's COVID-19 Cybersecurity Taskforce (C19TF)'s mandate was to swiftly secure and improve the cybersecurity posture of key contact tracing systems in Singapore such as contact tracing databases, SafeEntry, and TraceTogether.

CSA's C19TF collaborated with the Government Technology Agency's (GovTech) developmental teams to provide just-in-time technical security design review, hardware assurance testing and penetration testing within short timeframes to ensure that all systems and data complied with the public sector's cybersecurity and data security requirements. In May 2021, the TraceTogether tokens achieved the highest security label under the voluntary CLS, demonstrating strong security against cyber threats.

As COVID-19 transitions to an endemic state in Singapore, CSA and GovTech remain committed to jointly create effective solutions designed to be citizen-centric and secure, yet easy to use and deploy.

Cybersecurity Campaigns and Outreach Programmes

In June 2021, CSA launched the fourth edition of our national cybersecurity awareness campaign, entitled "Better Cyber Safe than Sorry". The campaign focused on raising awareness and driving adoption of four good cybersecurity practices: using strong passwords and enabling 2FA; spotting signs of phishing; using anti-virus software; and updating computer software promptly.

The campaign has expanded its reach since its inception in 2017. Although roadshows were not possible due to COVID-19 restrictions, CSA worked with e-commerce players – Shopee and Carousell – to publicise the campaign online. In addition, CSA partnered with supermarket chain NTUC FairPrice to disseminate our campaign messages through their stores and digital platforms. These initiatives came on top of public outreach through advertisements at bus stops, bus wraps, on television and social media platforms.

CSA also launched a new **SG Cyber Safe Seniors Programme**, which aimed to reach out to 50,000 seniors by 2023 to raise their awareness of cybersecurity and encourage adoption of good cyber hygiene practices. CSA and our partners, the SPF, and the Infocomm Media Development Authority (IMDA), engaged seniors on a range of cybersecurity-related topics in the four official languages, through a mixture of physical and online platforms.

To help young digital users reap the benefits of technology safely, CSA's **SG Cyber Safe Students Programme** engages students through fun and interactive activities to impart the importance of cybersecurity, explain cybersecurity concepts and promote adoption of good cyber hygiene practices. In support of Ministry of Education (MOE)'s Cyber Wellness curriculum, CSA collaborates with MOE and partner agencies such as SPF and IMDA to develop initiatives and resources



Primary school students attempting the motion-sensor game during a Go Safe Online Pop-up deployment.

for cybersecurity lessons in schools. A cybersecurity module under the Code for Fun programme offered to upper primary students since January 2021 is one such example.

Other initiatives included the revamped Go Safe Online Pop-up, launched in June 2021, and the new edition of the Go Safe Online drama skit, launched in August 2021. The former helped to raise awareness of the importance of cybersecurity and impart cyber tips through motion-sensor games. The latter, staged during the assembly periods in primary and secondary schools, saw students learn about cybersecurity and cyber dos and don'ts through the portrayal of various characters' online encounters. The skit was performed via live-action or hybrid formats to adhere to the prevailing COVID-19 safe management measures.

SG Cyber Safe Programme

CSA launched the SG Cyber Safe Programme in March 2021 to help enterprises better protect themselves in the digital domain and strengthen their cybersecurity posture. Under the programme, CSA has developed a suite of initiatives that are designed to help enterprises raise awareness of cybersecurity, take action to implement cybersecurity and drive adoption by recognising enterprises' efforts.



Cybersecurity Toolkits for Enterprises

To help simplify cybersecurity for enterprises, CSA has developed a set of cybersecurity toolkits targeted at enterprise leaders, SME owners, employees and IT teams.

Cybersecurity is a risk management issue that requires board-level decisions. The toolkit for enterprise leaders and SME owners seeks to drive home the message that “it is in the interest of the business to invest in cybersecurity, and your investment will pay for itself”. Examples of topics covered in the toolkit include strategy and investment, as well as building a strong cybersecurity culture in the organisation.

Employees are the first line of defence for all organisations. Enterprises can use the cybersecurity toolkit for employees as a curriculum to raise awareness and conduct cybersecurity training for their employees. The content of the toolkit focuses on how employees can exercise cyber safe behaviours, such as setting strong passwords and reporting cyber incidents promptly.

The cybersecurity toolkit for IT teams aims to address the challenge of keeping pace with the constant evolution of cyber threats by providing guidance on how IT or cybersecurity teams should prioritise and find relevant resources. The toolkit will also include technical tools that teams can adopt, such as self-assessment tools for evaluating their cyber hygiene and incident response simulation.

The toolkits are available for download on CSA's website:



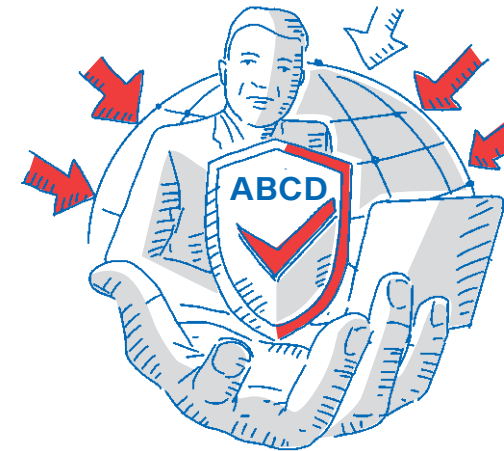
Cybersecurity Certification for Enterprises – Cyber Essentials and Cyber Trust

Given the unabating trend of supply chain cyber-attacks, there is concern that smaller enterprises may be used as conduits to target larger companies or even government agencies. Hence, even as companies expand their portfolios of partnerships, it is important that their vendors or supply chain partners demonstrate a baseline level of cybersecurity.

CSA introduced a cybersecurity certification scheme for enterprises in March 2022, so that businesses can leverage such certification to demonstrate their cybersecurity posture and potentially distinguish themselves from their competitors.

The Cyber Essentials mark recognises enterprises that have put in place cyber hygiene measures, while the Cyber Trust mark is a mark of distinction to recognise enterprises with comprehensive cybersecurity measures and practices. The two cybersecurity certification marks were developed in consultation with industry partners such as certification practitioners, technology providers and trade associations. They take into consideration the diverse organisational profiles and operational needs of enterprises in Singapore.

For more information, please refer to:



ABCD Programme

The Asset-Based Cyber Defence (ABCD) programme is a one-stop cybersecurity-as-a-service for both businesses and individuals. Subsidised for SMEs in Singapore under IMDA's SME Go Digital programme, the ABCD programme has helped SMEs improve their cybersecurity posture by providing advice, consultancy services and technical solutions, including assistance to SMEs that suffered cybersecurity breaches. CSA works with several Singapore security companies to provide clients with these services.

The programme focuses on securing the endpoints using a zero-trust defence-in-depth approach to help SMEs protect themselves against common threats like ransomware. Endpoints are often the entry point for malicious cyber activities. The ABCD programme aims to help organisations level up sufficiently to attain the CSA Cyber Essentials mark. To date, more than 100 SMEs have subscribed to the ABCD service.

Licensing Framework for Cybersecurity Service Providers

CSA officially launched the licensing framework for cybersecurity service providers on 11 April 2022. The licensing framework is administered by the Cybersecurity Services Regulation Office. Under the framework, cybersecurity providers providing Managed Security Operations Centre monitoring services and/or penetration testing services to the Singapore market are required to be licensed. Each licence is valid for two years.



As the demand for licensable cybersecurity services increases, the light-touch licensing framework aims to: (a) provide greater assurance of security and safety to consumers; (b) improve the standards and standing of cybersecurity service providers; and (c) address information asymmetry between consumers and cybersecurity service providers. Prior to the implementation of the licensing framework, an industry consultation was conducted, with relevant feedback incorporated into the framework, where applicable.

To facilitate transition to the licensing framework, cybersecurity service providers are given a six-month grace period from launch to apply for a licence. Those that do so during this grace period may continue to provide the licensable service while their applications are being processed. In view of the COVID-19 pandemic's adverse impact on businesses, a one-time 50% waiver of licence fees will be granted for all applications lodged within the first 12 months from the launch of the licensing framework.

For more details on the licensing framework, please refer to:



Strategic Pillar 3: Enhance International Cyber Cooperation

International Engagements and Outreach

ASEAN Engagement

The ASEAN Regional Action Plan (RAP) Matrix on Norms Implementation was adopted at the 2nd ASEAN Cybersecurity Coordinating Committee (ASEAN Cyber-CC) in November 2021. The RAP Matrix is intended to guide ASEAN Member States (AMS) in implementing the 11 UN voluntary, non-binding norms of responsible State behaviour in cyberspace. Following its adoption, the RAP Matrix remains a living document to be reviewed whenever required. The ASEAN Cybersecurity Cooperation Strategy 2021-2025 was approved at the 2nd ASEAN Digital Ministers (ADGMIN) Meeting in January 2022, and serves as an updated roadmap for ASEAN's approach in creating a safer, resilient, interoperable and more secure cyberspace in the region, undergirding and enabling ASEAN's digital ambitions. The ASEAN Computer Emergency Response Team (CERT) Implementation Paper, which was endorsed at the same ADGMIN Meeting, formalises regional CERT-CERT cooperation, including through the ASEAN CERT Information Exchange Mechanism.

ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE)

The ASCCE Campus was officially opened in October 2021 during the 6th Singapore International Cyber Week (SICW). To date, the ASCCE has delivered more than 30 programmes attended by over 1,000 senior officials from ASEAN and beyond, and collaborated with over 40 partners from across governments, private sector, academia, and NGOs.



The official ASCCE LinkedIn page was also launched to facilitate networking among ASCCE alumni and other cyber capacity-building stakeholders as well as to update the community on programme offerings and latest capacity-building news and events.

Memorandum of Understanding (MOU) with the Republic of Finland to Mutually Recognise Cybersecurity Labels

For the first time, CSA concluded an agreement with the Transport and Communications Agency of Finland (Traficom) to mutually recognise each other's cybersecurity labels for IoT, or smart consumer devices. The MOU was signed during the Opening Ceremony of SICW 2021's International IoT Roundtable on 6 October 2021 by CSA Chief Executive David Koh and his counterpart, Traficom's Deputy Director-General, and Head of Finland's National Cyber Security Centre, Sauli Pahlman.

Under this MOU, a consumer IoT device that has been issued Traficom's Cybersecurity Label will be recognised as having complied with Singapore's Cybersecurity Labelling Scheme (CLS) level 3 requirements. Similarly, a consumer



Minister for Communications and Information & Minister-in-Charge of Smart Nation and Cybersecurity Mrs. Josephine Teo chairing the 6th ASEAN Ministerial Conference on Cybersecurity. Source: Image Engine

IoT device that has been issued a CLS level 3 or 4 will be recognised as having met the requirements of Traficom's Cybersecurity Label.

UN Cyber Processes

CSA participated in the inaugural Open-Ended Working Group (OEWG) and sixth UN Group of Governmental Experts (UNGGE). Both processes concluded successfully with their respective consensus reports in March and May 2021 respectively.

These UN outcome documents are significant milestones in the global effort towards strengthening a rules-based multilateral order in cyberspace. The OEWG consensus report identified concrete actions and cooperative measures to address ICT threats, and to promote an open, secure, stable, accessible and peaceful ICT environment. The UNGGE consensus report provided deep dives into the international cyber stability framework and developed an additional layer of understanding to the voluntary, non-binding norms and confidence-building measures.

At the 76th UN General Assembly, the UN First Committee adopted the Russia-US resolution on "Developments in the field of information and telecommunications in the context of international security, and advancing responsible State behaviour in the use of information and communications technologies" by consensus.

Notably, in June 2021, Singapore's Permanent Representative to the UN in New York Ambassador Burhan Gafoor was elected as Chair of the five-year OEWG on Security of and in the use of ICTs.

Cyber Events and Conferences

6th Singapore International Cyber Week (SICW)

The 6th SICW was held from 4 to 8 October 2021 in a hybrid format, attracting nearly 2,000 local and international attendees. High-level government and industry speakers included UN Under-Secretary-General and High Representative for Disarmament Affairs Izumi Nakamitsu and Google Cloud CEO Thomas Kurian.

6th ASEAN Ministerial Conference on Cybersecurity (AMCC)

The 6th AMCC participants built on the progress made on key cybersecurity matters as discussed at the last meeting, including the ASEAN RAP Matrix on Norms Implementation.

In addition, participants:

- (a) welcomed the update to ASEAN's strategy for cybersecurity cooperation, as laid out in the ASEAN Cybersecurity Cooperation Strategy 2021 – 2025, and the ASEAN CERT Implementation Paper which will guide AMS on the operationalisation of the ASEAN CERT; and
- (b) recognised the importance of cybersecurity in supporting economic growth for AMS.

Foundational Enabler 1: Develop a Vibrant Cybersecurity Ecosystem



In just a few short years, our domestic cybersecurity Research and Development (R&D) network has blossomed from just a handful of researchers in 2015, into a diverse ecosystem with hundreds of active academics and researchers spanning our Institutes of Higher Learning (IHLs) and domestic companies. CSA continues to build on this solid foundation and double down on efforts to guide research into their eventual translation into cybersecurity products and services. This not only helps ensure that our local industry keeps up with the cutting-edge of capabilities in cybersecurity, but also stimulates our digital economy by generating new, higher value employment opportunities for Singaporeans. Some of these key initiatives are:

Support for Industry Innovation

Given the rapidly evolving cyber threat landscape, cybersecurity firms need to constantly innovate and invest in new solutions to stay ahead of the curve. CSA will continue to support industry-led innovation in cybersecurity. For example, the Cybersecurity Industry Call for Innovation encourages cybersecurity companies to innovate on pressing cybersecurity challenges by matching them with key local end-users (e.g. CII, commercial sector leads) which may have specific operational cybersecurity needs. This initiative also helps provide opportunities for local companies to tap into Singapore's growing cybersecurity market and grow demand in our local cybersecurity industry.

Supporting the Growth of Cyber Entrepreneurs and Start-ups

Apart from supporting established cybersecurity firms, it is also important to encourage budding cyber entrepreneurs and start-ups. The Innovation Cybersecurity Ecosystem at Block 71 (ICE71), the region's first cybersecurity start-up hub, is one such initiative. ICE71's programmes aim to provide support for innovators and start-ups at all growth stages. These include community outreach and entrepreneurship programmes to engage the cybersecurity ecosystem and promote collaboration between stakeholders.

Growing Markets and Exports

CSA is looking to support promising local cybersecurity companies to expand overseas and export "made in Singapore" solutions. For instance, CSA will be working closely with economic agencies such as Digital Industry Singapore (DISG) and Enterprise Singapore (ESG) to curate, organise and support these cybersecurity companies in profiling their solutions internationally.

Driving Cybersecurity Standards

Standards is an important tool to raise cybersecurity posture and enhance risk management across the ecosystem. Standards can be leveraged as a strategic advantage to capture economic growth. The reinforced branding can give companies an advantage in terms of perceived quality and market

access, facilitating the growth of the digital economy.

Singapore rolled out two national standards in 2021: one for autonomous vehicles (Technical Reference 68, or TR 68) and the other for cybersecurity labelling of consumer IoT (TR 91). CSA helped to enhance the cybersecurity principles and assessment framework of TR 68, particularly in the areas of security by design, defence in depth, operations management and oversight, resiliency, and testing. TR 68 was referenced in the development of ISO 37181 on "Smart community infrastructures – Smart transportation by autonomous vehicles on public roads". TR 91 provides guidance on the design principles and concepts of the CLS labels and assessment tiers to developers and suppliers.

On the international stage, Singapore is working with like-minded partners to develop a universal labelling framework for consumer IoT to harmonise established international standards and labelling requirements, as well as to facilitate mutual recognition. This would minimise the fragmentation of standards, eradicate duplicated testing across countries, reduce the cost of compliance to national regulations, and facilitate market access for developers. This effort is agnostic to binary or multi-level labelling schemes and has been tabled as a Proposed Work Item (PWI) ISO 27404 at ISO/SC27/WG4.

World-class R&D and Innovation – Opening of NiCE

Launched in May 2022, the National Integrated Centre for Evaluation (NiCE) is a joint initiative by CSA and the Nanyang Technological University (NTU) to grow the cyber domain of Singapore's Testing, Inspection and Certification (TIC) industry. NiCE is a one-stop centre to facilitate the testing and evaluation of products, education and training, and advanced research for security evaluation techniques. The collaboration harnesses the strength of

NTU's research competencies in software and hardware security assurance, and optimises resource utilisation through sharing of high-end equipment, and pooling of industrial and research expertise.

In line with Singapore's Cybersecurity Strategy to promote Security-by-Design, NiCE aims to drive initiatives to achieve the following goals:

- To seed a community of practice by providing access to advanced equipment and expertise for evaluators and developers to perform evaluation at the highest assurance levels;
- To foster a vibrant R&D ecosystem in advanced security evaluation techniques, covering areas such as software and hardware security protections; and
- To build a pipeline of local product evaluation talent through training, development, and certification to equip students and professionals with relevant security evaluation competencies.

Whole of Government (WOG) Capability Development Efforts

Through its Cybersecurity Capability Development Masterplan, CSA is playing a leading role in ensuring that the Government is well positioned to meet the threats of today and tomorrow. By utilising a risk-based approach, CSA is able to strike a balance between three key imperatives – to safeguard our Critical Information Infrastructure (CII) sectors, our Digital Economy, and Digital Way of Life.

Together with our sister technology agencies such as Defence Science and Technology Agency (DSTA), Home Team Science and Technology Agency (HTX), GovTech, and IMDA, we have embarked on a deep level of collaboration on capability development, to optimise the use of the inherent strengths of each agency whilst minimising duplication of effort.

Foundational Enabler 2: Grow a Robust Cyber Talent Pipeline

SG Cyber Talent

Introduced and led by CSA since 2020, SG Cyber Talent is a national initiative to grow and develop the cybersecurity workforce in Singapore.

Through SG Cyber Talent, CSA looks to:

- Grow the talent pipeline by attracting a diverse local pool of students from as early as at the secondary school level, to consider cybersecurity as a future career;
- Provide up-skilling and re-skilling opportunities for new and mid-career professionals moving into cybersecurity job roles; and
- Help the existing pool of cybersecurity professionals advance their careers through deep skills training and leadership development.

SG Cyber Talent is on track to reach out to at least 20,000 individuals over three years starting from 2020, to support them in embarking on and advancing their journeys in cybersecurity. As announced under SG Cyber Youth in July 2019, half of these 20,000 individuals will comprise youths. The other half will comprise professionals and leaders engaged through other programmes under SG Cyber Talent. As of end-2021, we have engaged over 16,000 individuals.

The programmes under the SG Cyber Talent initiative include SG Cyber Youth, SG Cyber Professionals, SG Cyber Olympians, SG Cyber Women, SG Cyber Leaders, and the newly launched SG Cyber Talent Development Fund in 2022.



Spotlight: Temasek Polytechnic's Malware Analysis Centre

Temasek Polytechnic has worked with industry partners and CSA to provide industry-relevant cybersecurity training. On 17 November 2021, Senior Minister of State for Communications and Information Dr Janil Puthuchearu opened the Malware Analysis Centre in Temasek Polytechnic's School of Informatics and IT. This facility was set up in collaboration with ST Engineering, Palo Alto Networks and CrowdStrike to foster the development of academic collaboration, staff capability and research projects in the field of cybersecurity.

The Malware Analysis Centre is the first of its kind in an educational institution in the region. It focuses on the identification, detection, and forensics investigation of malware. The Centre is unique as it functions as a Learning Enterprise where senior students from the Diploma in

Cybersecurity & Digital Forensics programme support the Polytechnic's students who suspect their devices might have been compromised by malware. Using leading industry technologies and processes, the students scan the devices, isolate the malware, restore the devices and analyse the malware. The students take on roles such as Security Manager, Tier 1 Security Analyst, Tier 2 Security Analyst and Support Services in the Centre's operation. They are supervised by academic staff and mentored by industry partners.

Temasek Polytechnic accepts about 200 students into the Diploma in Cybersecurity & Digital Forensics programme each year. All of them will undergo training at the Malware Analysis Centre as part of their curriculum, and approximately 20 students will have a chance to join the Centre as interns.



Malware Analysis Centre at Temasek Polytechnic. Source: Temasek Polytechnic



Cyber Trends to Watch

The cyber landscape is constantly changing. The previous edition of the Singapore Cyber Landscape focused on potential upheavals wrought by the increasing pace of digitalisation and shift to telecommuting due to COVID-19. Recent global developments, however, threaten to disrupt the cybersecurity landscape further. Beyond the ever-evolving tactics of cybercriminal and hacktivist groups, the emergence of Web3 and the Metaverse, as well as heightened geopolitical tensions, will likely result in lasting impact and reshape various cybersecurity issues.

Increased Geopolitical Tensions

Decoupling from Western Technology

As the Russia-Ukraine conflict rages on, major technology firms, such as Apple, Google and Meta, have increasingly limited their operations and services offered to Russia. Most of these sanctions were voluntary and even exceeded the scope and extent of sanctions imposed by states. These include limiting the use of Apple Pay and Google Pay, as well as suspending all of Apple's product sales, Google Play Store billing, and access to Meta's platforms (Facebook and Instagram) in Russia. Intel and Advanced Micro Devices (AMD) also ceased semiconductor supplies to Russia. Meanwhile, China continues to decouple from US technology, driving homegrown innovation due to a growing desire for self-reliance.

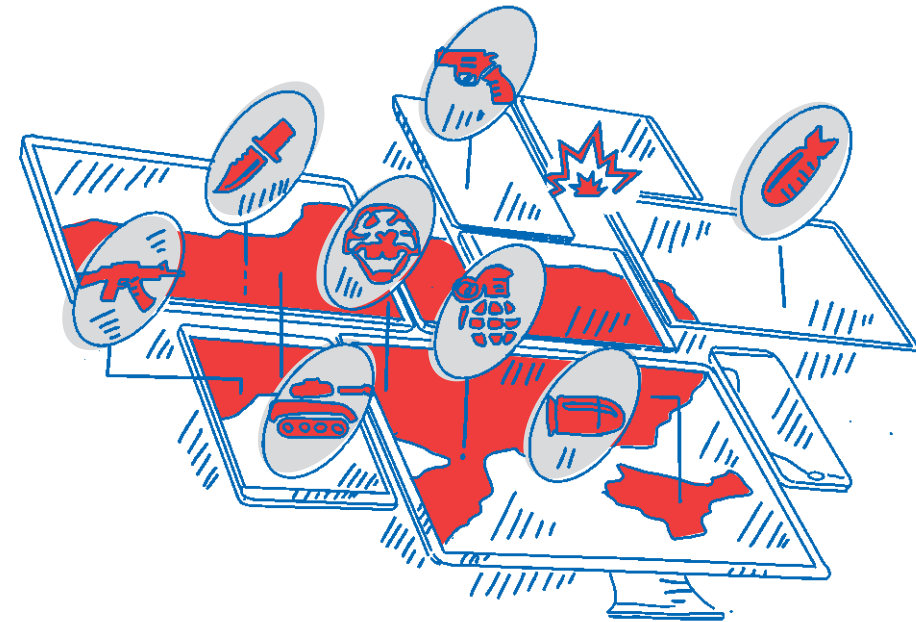


Implications

These technology firms' sanctions may be seen to be taking an adversarial position against Russia. A major hurdle for Russia to decouple from US technology was the high inertia that would come with the suspension of various payment services and product offerings to Russian citizens. With this hurdle removed, this may strengthen Russia's desire to wean itself off Western technology entirely.

Countries such as China would have watched the developments closely. The manufacturing giant, which had its access to US high-tech

supply chains increasingly curtailed since 2017, had reportedly initiated a movement to attain self-sufficiency in advanced technologies. As countries continue to decouple from US technology, differing cyber norms, ecosystems and standards, may become a reality in the near future. Even the use of cybersecurity vendors across different ecosystems may be scrutinised, as evidenced by the statement issued by the German Federal Office for Information Security warning companies against using Russian cybersecurity vendor Kaspersky's anti-virus products in March 2022.



Non-State Actors Playing a Larger Role in Geopolitical Conflict

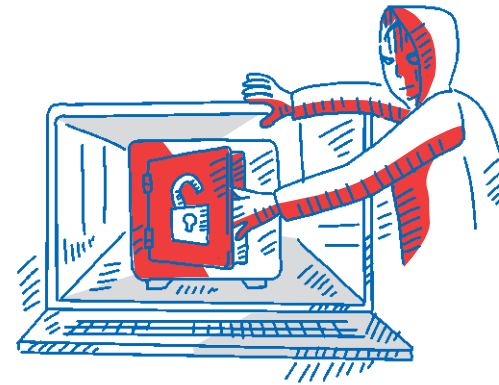
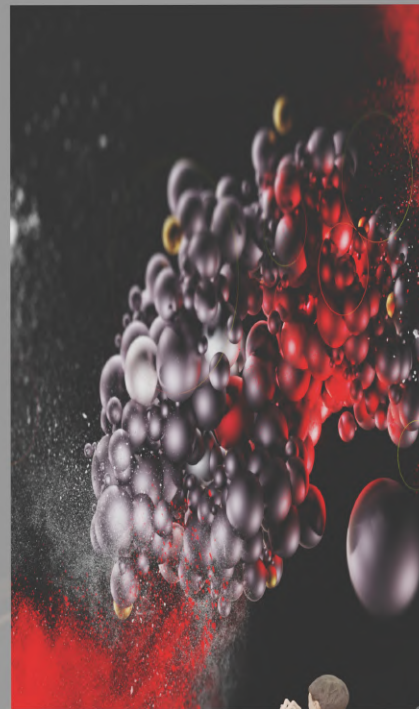
Cybercriminal and hacktivist groups have been observed taking sides in the Russia-Ukraine conflict. In February 2022, the 'IT Army of Ukraine' was founded, as Ukraine's Vice Prime Minister and Minister for Digital Transformation Mykhailo Fedorov encouraged volunteers to participate in Ukraine's hacker underground army to provide cyber defence for Ukraine's critical infrastructure, as well as carry out offensive cyber operations against Russia-linked entities. Prominent hacktivist groups such as the Anonymous collective and AgainstTheWest promptly took up digital arms in support of Ukraine, as they engaged in multiple denial-of-service attacks and infiltrated the networks of various Russian organisations in data breaches. At the same time, the infamous Conti ransomware gang also waded into the fray, declaring that it would attack Russia's enemies.

Implications

The sudden explosion of volunteer and amateur hackers can have a destabilising effect on global cybersecurity. An already chaotic situation could get messier as hackers on both sides engage in a 'free-for-all', with many eager to burnish their credentials by carrying out increasingly audacious attacks. This increases the risk of reprisals as any serious cyber incident resulting from hacktivism may be used as a pretext for escalation by one side or the other. The Conti group has even declared that they would retaliate accordingly if there was "attempt to target critical infrastructure in Russia". In a hyper-connected global cyberspace, collateral damage or unintended consequences to organisations not linked to Russia or Ukraine may be possible.

Web3, Blockchain Technology and the Metaverse

These three buzzwords have recently gained intense popularity in 2021, as interest in cryptocurrencies and their underlying technology soared. Web3 refers to the next generation of the Internet where emphasis is placed on the decentralisation and user ownership of data or digital assets. Blockchain technology supports this new 'iteration' of the Internet as it builds a digitally distributed database where building blocks of data or transactions are dynamically shared across the nodes of a peer-to-peer network. Put together, the idea of non-fungible tokens (NFTs) was conceived as a unique piece of digital asset backed by blockchain technology to be used in the Metaverse – a universal and highly immersive virtual world where people can work, play, shop and socialise. Regardless of whether one is a believer in Web3, it has certainly emerged as fertile ground for new malicious cyber activities.



Securing Our Digital Assets in the Metaverse

Many think NFTs will be one of the core components of experiencing the Metaverse. Imagine this: your Metaverse self, a collector of many priceless NFT pictures, adding a pair of NFT sneakers onto your virtual avatar. Unfortunately, you are hit by a stroke of bad luck, and your account was hacked and digital assets stolen. An improbable scenario, you say? Perhaps, but as the masses grow more receptive to the concept of the Metaverse (fuelled by Meta's high-profile rebranding), securing our own digital assets will become ever more important.

Cryptocurrency Scams

According to blockchain data platform Chainalysis, crypto-based crime hit a high in 2021, with cryptocurrency wallets linked to illicit activities receiving USD 14 billion – an increase of some 79% from 2020. Decentralised Finance (DeFi) – peer-to-peer financial platforms that enable transactions without the need for financial intermediaries – has been a key factor in the rise of crypto-based crime.

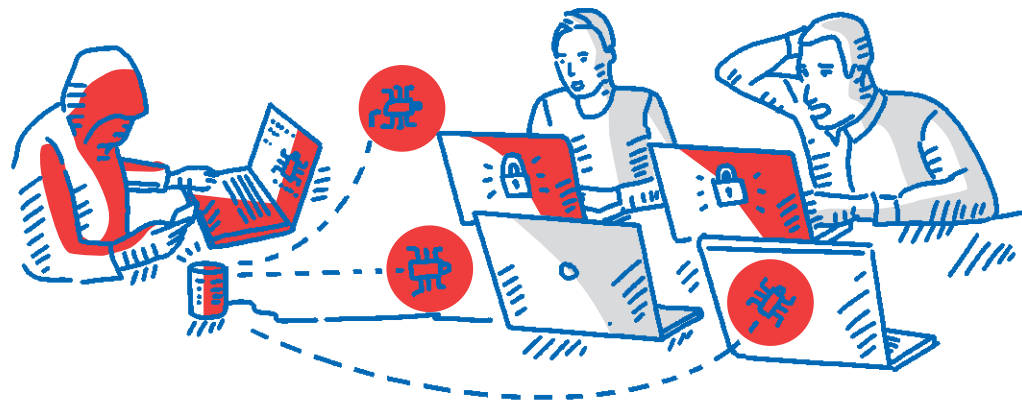
Implications

The anonymity afforded by DeFi, which has opened up opportunities in crypto-based crime, has also impeded investigations by law enforcement agencies. In addition to being "trustless" – in that users of DeFi platforms do not depend on intermediaries for a network or payment system – DeFi's open and distributed nature also poses problems for regulators as it is difficult to track illicit activity and enforce regulations across borders. Furthermore, money trails associated with crypto laundering may only appear long after the incidents have taken place, as cybercriminals sit on stolen cryptocurrency in the hope that they can cash out unnoticed once law enforcement efforts die down. Such challenges incentivise and embolden cybercriminals to engage in crypto-based scams.

Implications

Given the emphasis on decentralisation in Web3, there will be no secure platforms or protected spaces for individuals to park their assets under: all users are potentially at risk in this presently unregulated space. While organisations typically have greater resources to secure their assets, individuals will likely be much more susceptible to cyber-attacks by cybercriminals. This is because scammers are likely to employ the same TTPs such as phishing and impersonation in their attacks, despite the move towards the Metaverse. Notably, there is also a liability shift as users will have to assume full responsibility of their own digital assets in the Metaverse. Cyber hygiene will be of utmost importance to prevent hacks; increased vigilance and cyber awareness will be more important than ever, to guard against scams and spear-phishing attacks.

The Future of Ransomware



Targeting Critical IoT Devices

Deploying ransomware against IoT devices is not new. Since 2014, researchers have observed cyber threat actors leveraging botnets to infect IoT devices like cameras and printers. Such attacks have traditionally been considered as low likelihood events, when compared to traditional ransomware attacks, as there is little data of value stored on IoT devices for threats actors to hold ransom (most IoT data are stored externally, e.g. uploaded on cloud platforms). Furthermore, regaining access to device functionality could be as simple as hitting reset and installing new patches and updates.

However, cybercriminals are coming to recognise that infecting critical IoT devices, such as Internet-connected Uninterruptible Power Supply (UPS) units, can inflict devastating impact on organisations due to the potential

costs in downtime. The US Cybersecurity and Infrastructure Security Agency (CISA) also noted that it is essential to prevent attacks on these devices as they are often used as emergency backup solutions when core system applications lose connectivity to the Internet. However, IoT devices often lack critical cybersecurity protection, and company employees have even been observed to connect their personal IoT devices to the organisation's networks without the knowledge of their IT teams. By timing their attacks to ensure that the critical IoT device cannot be reset, or to prevent effective mitigation, the potency of the cyber-attack greatly increases. Such attacks have the potential to cause disruptive effects on operational systems by cutting them off from the Internet, which may result in serious, real-world consequences.



Implications

IoT ransomware attacks will likely be timed to maximise disruptive effects, and a successful compromise could upend the provision of important services to scores of users. To compound the problem, the increasing prevalence of IoT devices in everyday use means this is a threat across multiple levels. At an individual level, important personal digital devices could be targeted, resulting in potentially devastating consequences.

For instance, 'connected' medical devices such as insulin pumps and ECG patches, which collect patient data in real-time and dispense treatments accordingly, could serve as entry points for attacks through unpatched vulnerabilities and have life-threatening consequences if compromised. At an organisational level, cybercriminal gangs may target multiple kinds of IoT devices used

within firms and enterprises, banking on the likelihood that they can find numerous devices that have poor security features which can then be encrypted *en masse*. At a national level, the expanding use of IoT devices in OT systems, which can be found in numerous CII and essential services, means such attacks could threaten national security.

Organisations need to have full awareness and visibility of the IoT devices that are used and connected to their networks, and ensure that any suspicious Internet traffic is quickly identified and blocked. They should segregate their networks into subnets to reduce the risk of an IoT attack. All organisational IoT devices should also be patched regularly and subjected to cyber hygiene controls – such as avoiding the use of factory-default passwords.

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.
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 which 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	<p>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.</p> <p>Singapore's cyberspace includes domain names with ".SG" or Singapore-mentions, IP addresses used in Singapore, and Internet Service Providers (ISPs) located here.</p>

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.
Hactivist	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.
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, such as virus, worm, Trojan horse, spyware and adware.
Personal Data/ Information	Data which, on its own (e.g. full name, NRIC number) or in combination with other available data (e.g. medical or educational information), can be used to distinguish or trace an individual's identity.
Phishing	A common technique used by threat actors to trick people (typically through e-mails) into divulging personal information, transferring money, or installing malware.

Ransomware	Malware that encrypts files on a victim's device, rendering them unuseable 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.
Red Teaming	An exercise that focuses on systematically and rigorously (but ethically) identifying an attack path that breaches an organisation's security defences using real-world attack techniques.
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.
Spyware	Software designed to enter a device to gather data and forward it to third-parties without knowledge or consent.
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.
Zero-Day Vulnerability	A vulnerability in a system or device that has been disclosed but is not yet patched.

Editorial Team

Willis Lim
Tan Wei Kee
David Lim
Sophia Tan
Grace Dong
Faith Tan
Ivan Teng
Yeo Wee Cheng
Ang Jia Xi

Contributors

CrowdStrike
Singapore Police Force
Temasek Polytechnic

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**.

Cyber incident reporting form:

<https://go.gov.sg/singcert-cyber-aid>

If you wish to seek scam-related advice, please contact **ScamAlert**.

Anti-scam Helpline: 1800 722 6688

Website: www.scamalert.sg



www.csa.gov.sg