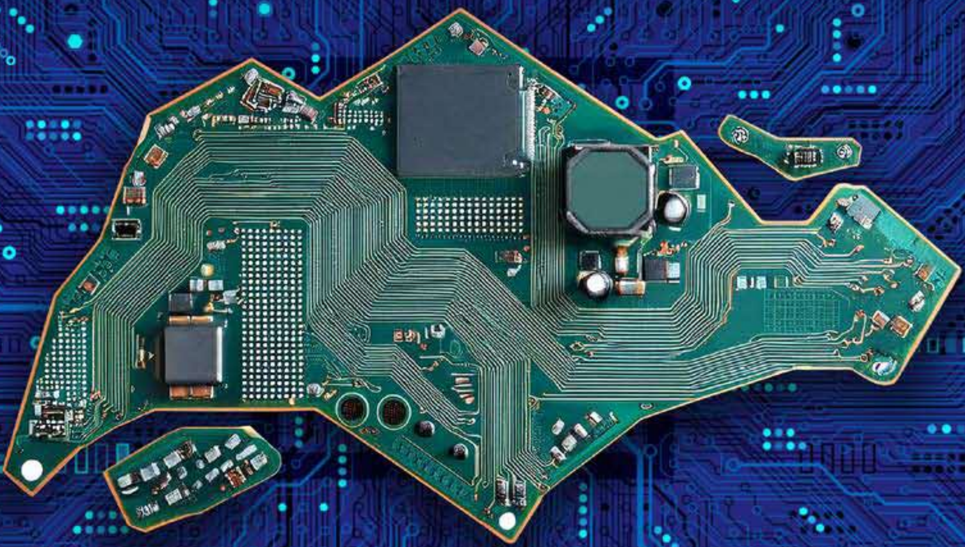
SINGAPORE CYBER LANDSCAPE 2024/2025



CSA SINGAPORE

Cyber Security Agency of Singapore

10 YEARS OF SECURING OUR CYBERSPACE

EDITORIAL TEAM

Mr Willis Lim
Dr Luke Ho
Ms Charissa Ong
Mr Jonathan Khoo
Mr Leon Teo
Mr Yong Jia Quan

CONTRIBUTORS

Chapter 1

Google Threat Intelligence Group

Liz Martin, Global Technical Lead Threat Intelligence, Dragos

Mr Omer Yoachimik, Senior Product Manager for DDoS Protection & Security Reporting, Cloudflare

Recorded Future's Insikt Group

Ms Yong Ying-I, Senior Advisor, Ministry of Digital Development and Information (MDDI) and Chairman, Central Provident Fund Board (CPFB)

Chapter 2

CrowdStrike

Cybercrime Command (CCC), Singapore Police Force (SPF)

Mr Lim Minhan and Mr Melvin Seah, Ensign InfoSecurity

Mr Ng Hoo Ming, former Deputy Chief Executive (National Cyber Resilience), Cyber Security Agency of Singapore (CSA)

Chapter 3

Digital and Intelligence Service (DIS), Ministry of Defence (MINDEF)

Government Technology Agency of Singapore (GovTech)

Mr Teo Chin Hock, former Deputy Chief Executive (Development), CSA

Chapter 4

Mr Huang Shao Fei, Group Chief Information Security Officer, SMRT Corporation (SMRT); Vice-Chair, Cybersecurity Committee, International Association of Public Transport (UITP); Immediate Past-President, Cybersecurity Chapter, Singapore Computer Society (SCS)

Mr Benjamin Ang, Head, Centre of Excellence for National Security and Future Issues and Technology, S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU)

Mr Willis Lim, Director, National Cyber Threat Analysis Centre (NCTAC), CSA

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 enquires/feedback: contact@csa.gov.sg

If you wish to report a cybersecurity incident, please contact **SingCERT**.
Cyber Incident Reporting Form: https://go.gov.sg/singcert-incident-reporting-form
Contact Email: singcert@csa.gov.sg

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

SINGAPORE CYBER LANDSCAPE 2024/2025

Designed by Urban Forest Design Pte Ltd

Printed by HoBee Print Pte Ltd

ISSN: ISSNAPP25052210

The "Singapore Cyber Landscape 2024/2025" publication reviews Singapore's cybersecurity situation in 2024/2025 against the backdrop of global trends and events. CSA utilises multiple data sources to provide clarity on the common cyber threats observed in Singapore's cyberspace. CSA does not specifically endorse any third-party claim made in this material or related references, and the opinions expressed by third-parties are theirs alone. The enclosed facts, statistics and analyses are based on information available at the time of publication. The contents of this publication are provided on an "as is" basis without warranties of any kind. To the fullest extent permitted by law, CSA does not warrant and hereby disclaims any warranty as to the accuracy, correctness, reliability, timeliness, noninfringement, title, merchantability or fitness for any particular purpose of the contents of this publication. CSA shall also not be liable for any damage or loss of any kind caused as a result (direct or indirect) of the use of the publication, including but not limited to any damage or loss suffered as a result of reliance on the contents contained in the publication. CSA also reserves the right to refine its analyses as the threat situation evolves, and/or as further information is made available.

CONTENTS

CONGRATULATORY MESSAGE
FROM MINISTER FOR DIGITAL DEVELOPMENT AND INFORMATION AND MINISTER-IN-CHARGE OF SMART NATION AND CYBERSECURITY

The Cyber Security Agency of Singapore (CSA) enters its 10th year in 2025. A decade ago, the cyber threats we faced were more limited in scale and scope. Our cybersecurity governance frameworks were still in their infancy. Awareness of cyber risks was also low, among members of the public and leaders of organisations.

Even then, we recognised the urgency of organising a coordinated response to address the fast-evolving threat landscape. Digitalisation was poised for take-off. The expanding digital world is inherently borderless and cyber risks will grow in complexity. This prompted the Government to establish CSA to lead and coordinate Singapore's national cybersecurity efforts.

From the outset, CSA played a central role in building our national capabilities, forging strong partnerships with our sister agencies to secure our digital future. Its two national Cybersecurity Strategies – launched in 2016 and refreshed in 2021 – demonstrated a clear vision to strengthen Singapore's cyber defences through a whole-of-nation effort, while contributing to a rules-based multilateral order in cyberspace. At the same time, we remain agile and responsive to emerging risks. Many of our key initiatives are detailed in the chapters of this book.

Within Singapore, CSA led the introduction of the Cybersecurity Act in 2018, which has since been refreshed to keep pace with evolving threats. CSA has also worked closely with enterprises to strengthen their cybersecurity posture, and collaborated with the industry to ensure that their products are secure-by-design. These public-private partnerships extend to the broader cybersecurity ecosystem, supporting the development of solutions that meet national needs, and strengthening the local cybersecurity talent pipeline.

Internationally, Singapore has contributed actively to shaping norms and strengthening trust in cyberspace. In 2021, we were elected to serve as Chair of the United Nations Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies. Singapore also became a founding member of the international Counter Ransomware Initiative, and has a leading role in fostering international cooperation to disrupt the criminal ransomware ecosystem. On a regular basis, we hold bilateral cyber dialogues with key partners such as the US, the UK, India and Malaysia. These exchanges allow for sharing of best practices to enhance our collective resilience.

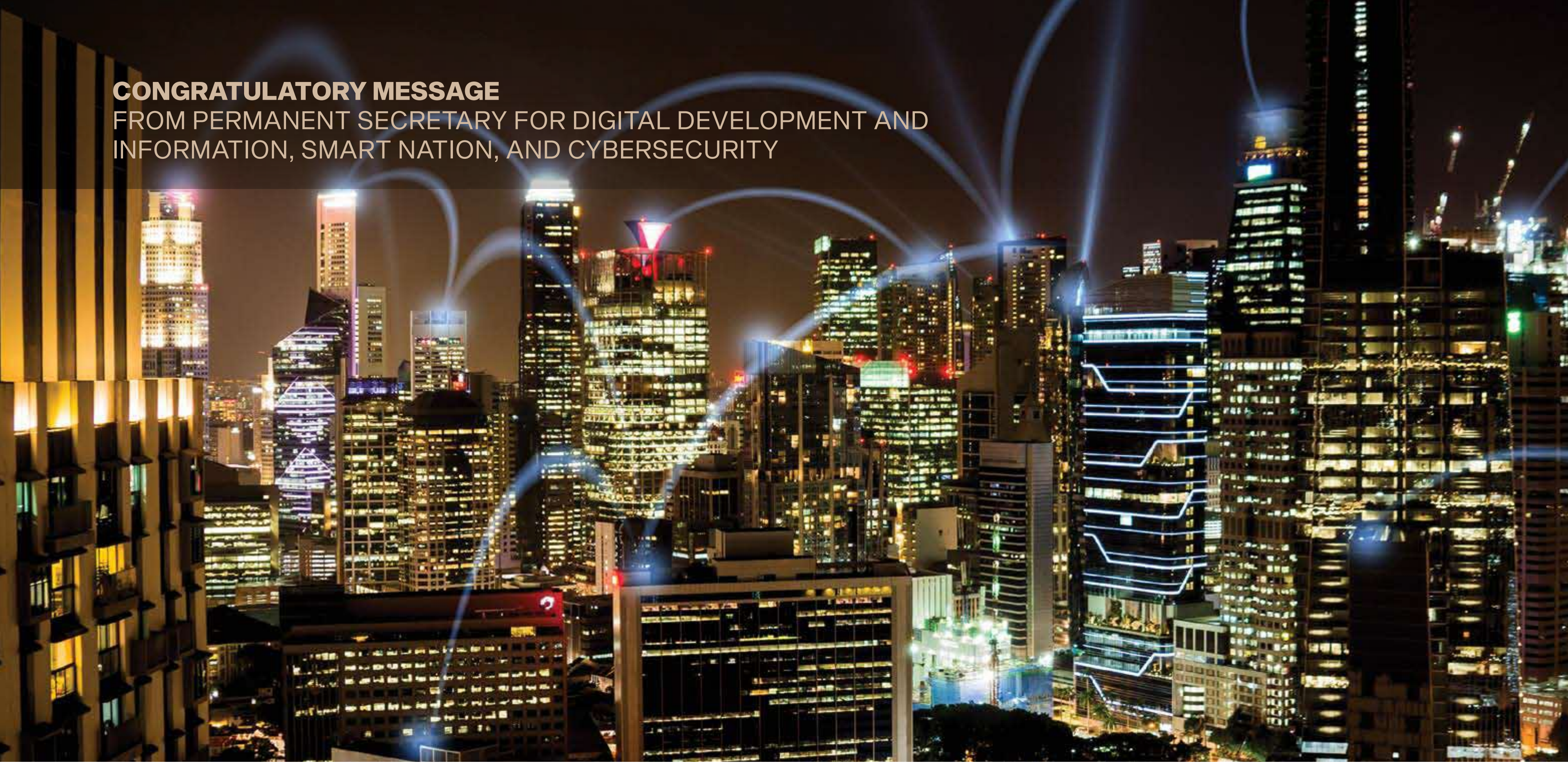
Looking ahead, CSA's move to the Punggol Digital District in 2026 will mark an important new chapter. It will house the new National Cybersecurity Command Centre, enhancing Singapore's capabilities to detect, respond to, and mitigate cyber threats at the national level.

I would like to extend my heartfelt appreciation to all CSA officers for your tireless efforts in keeping our cyberspace safe and secure. My appreciation also goes to CSA's partners and stakeholders for the invaluable support over the past decade. This includes government agencies in Singapore and abroad, our industry and academic partners, as well as the many organisations and individuals who have embraced cybersecurity as a shared responsibility.

In this milestone year, I look forward to the continued support and collaboration of our partners as we collectively raise Singapore's cybersecurity capabilities to new heights.

Mrs Josephine Teo
Minister for Digital Development and Information and
Minister-in-charge of Smart Nation and Cybersecurity

CONGRATULATORY MESSAGE
FROM PERMANENT SECRETARY FOR DIGITAL DEVELOPMENT AND INFORMATION, SMART NATION, AND CYBERSECURITY



For Singapore to thrive as a Smart Nation, Singaporeans must be able to go online with confidence – confident that digital systems and services are secure and reliable, and their safety and well-being will not be compromised. This is why the Singapore Government established the Cyber Security Agency of Singapore (CSA) some 10 years ago, to oversee the safety and security of Singapore's cyberspace.

As the national cyber authority of Singapore, CSA wears different hats. These hats can be described using 4Es – Educator, Enabler, Enforcer, Exemplar. As an Educator, CSA has helped to raise public awareness of cyber threats and educated Singaporeans on common cyber hygiene practices to protect themselves from threat actors through nationwide cybersecurity awareness campaigns. As an Enabler, CSA has developed various tools and frameworks to help organisations and individuals protect themselves from common cyber threats. CSA's SG Cyber Safe Programme and the Cybersecurity Labelling Scheme are good examples of the initiatives CSA has introduced to support organisations on their cybersecurity journey. CSA is also an Enforcer, responsible for ensuring that organisations with critical and important systems uphold their cybersecurity obligations stipulated in the Cybersecurity Act. On the international stage, CSA is an Exemplar – helping to shape and uphold international rules and norms to create a cyberspace where Singapore can remain safe and continue to thrive.

CSA led our efforts through various major cyber incidents and digital disruptions. Following the cyberattack on SingHealth in 2018, CSA worked closely with MOH to investigate and remediate the incident, and partnered with Critical Information Infrastructure owners to strengthen their defences against future attacks. CSA's incident response capabilities were once again tested in 2024 when a faulty CrowdStrike update led to a global tech outage and disruptions to digital services in Singapore. CSA quickly issued an advisory to guide affected system administrators and users on how to manually recover their systems. Singapore's ability to swiftly respond and recover from these major incidents is testament to the operational capabilities that CSA has honed over the years.

Cyberspace evolves quickly, with rapid advancements in cybersecurity tools and technologies, and equally rapid advancements in hackers' ability to exploit vulnerabilities. CSA must stay agile and nimble, and partner with the private sector and international partners to keep abreast of these developments. I congratulate CSA on your 10th anniversary and wish you every success in the years ahead!

Mr Joseph Leong
Permanent Secretary for Digital Development and Information, Smart Nation and Cybersecurity

FOREWORD

BY COMMISSIONER OF CYBERSECURITY AND CHIEF EXECUTIVE OF CYBER SECURITY AGENCY OF SINGAPORE (CSA)

In 2016, I wrote: "We hope this first edition of the Singapore Cyber Landscape ...provides some understanding of the gravity of what we as individuals, organisations, and the nation are dealing with." Nearly a decade later, these words still resonate, though the threat landscape has evolved dramatically.

Today, cyber threats emerge and spread at astonishing speed. Breaches happen in minutes, thousands of devices can be exploited instantly, and entire systems taken down with the push of a button. And the threat actors involved are increasingly sophisticated, particularly Advanced Persistent Threat (APT) groups which are typically state-linked. As Coordinating Minister for National Security Mr K Shanmugam shared at CSA's 10th anniversary dinner on 18 July 2025, Singapore has not been spared amidst heightened APT activity globally, with our critical information infrastructure targeted by *UNC3886*. Hence, as CSA marks its 10th anniversary, it is timely that we reflect on a decade of safeguarding Singapore's digital space and outline how we anticipate and respond to the challenges ahead.

Humble Origins

Our journey of strengthening Singapore's cybersecurity has been long but fruitful. When we first started out, we were a small outfit of under 70 staff, drawn from vastly different backgrounds and possessing varied skillsets. Nevertheless, this founding team was united in our purpose of safeguarding Singapore's cyberspace. We knew we could not do everything by ourselves – we were too small – but our key value was to be the orchestrator and coordinator for the many stakeholders who all had significant capabilities and resources. Together, we would be able to safeguard Singapore's cyberspace.

The responsibilities and challenges before us were daunting: Overseeing Critical Information Infrastructure (CII) protection, developing Singapore's cybersecurity industry, and leading Singapore's efforts in international cyber engagement, to name a few. Yet we knew that we could only succeed by working together. When Singapore launched its first Cybersecurity Strategy in 2016, our primary focus was on fortifying the resilience of our CII by having a common vision, and through stronger public-private partnerships.

Yet even as we strengthened our defences, the evolving cyber threat landscape always posed unexpected challenges. The SingHealth breach of 2018 remains Singapore's largest data breach to date, while ransomware – once dismissed as a nuisance affecting smaller businesses – evolved into a global menace capable of disrupting entire nations.

Perhaps the most sobering development has been the rise of online scams. Whether through Artificial Intelligence (AI)-enabled fraud schemes targeting corporations or deceptive cyber scams that drain the life savings of individuals, cybercriminals have demonstrated relentless adaptability. The human cost of these malicious criminal operations is starkest for those with the least means to recover, and this underscores the importance of a broader cybersecurity approach that safeguards the digital well-being of all Singaporeans.

Impactful Achievements

To this end, we – the collective ecosystem, spanning government agencies, private industry and academia – have embarked on many endeavours to secure Singapore's broader cyberspace. Guided by the 2021 Cybersecurity Strategy, we have worked towards two goals: responding to the immediate needs of the present, and continuing to lay foundations for stronger cybersecurity in the future.

An example of the former is our work in recent years to directly combat cyber scams. This involves a two-pronged approach based on education and proactive protection. These initiatives, together with those by the Singapore Police Force's Anti-Scam Command, the Banking and Finance sector, the Telecommunications sector, and various government agencies have encouragingly begun to bear fruit in recent years.

In addition, several landmark initiatives position us well for the future. The Cybersecurity Act of 2018 established a robust framework which enhanced our national security, while the Cybersecurity Labelling Scheme launched in 2020 has been pivotal in reshaping the consumer electronics cybersecurity landscape here.

The Government Technology Agency of Singapore (GovTech) and CSA's Government Bug Bounty Programme (GBBP), launched in December 2018, has played a crucial role in helping to uncover potential vulnerabilities across Government systems and digital services, and to address them before they can be exploited. The annual Critical Infrastructure Defence Exercise (CIDeX), co-organised by CSA and the Ministry of Defence's (MINDEF) Digital and Intelligence Service (DIS) since their formation in October 2022, helped sharpen the whole-of-government's collective responses towards real-world cyber-attack scenarios. Such collaboration reflect the close, longstanding relationships which our agencies have towards furthering Singapore's cyber defence. Even as we build on the success of these initiatives, I am confident the 2024 Operational Technology Masterplan will similarly place us in good stead as society and industries move towards greater automation of their operations.

International Efforts

Cybersecurity, by definition, is borderless. As such, we had to have an international outlook. Early in CSA's history, recognition of CSA by her international counterparts was scant. However, we have established a reputation for reliability, competence and principled behaviour that has facilitated development of productive working relationships. The Singapore International Cyber Week (SICW) has flourished as a key forum for pivotal cybersecurity discussions in the region and internationally. Singapore has been privileged to be part of international cybersecurity efforts such as the United Nations working groups and the Counter Ransomware Initiative. We have been honoured to work alongside steadfast international partners in contributing to global cybersecurity, and look forward to continued cooperation with them.

Appreciating Past and Present Staff

Where we are today would not have been possible without the determination and spirit of our leaders and officers, as well as the many stakeholders and partners who looked beyond narrow agency interests and saw the bigger goal of working together to safeguard Singapore's cyberspace. Thanks to their teamwork and our joint efforts, Singapore's cybersecurity has come a long way in just a decade.

In this special edition of the Singapore Cyber Landscape, several early leaders have drawn upon their memories of CSA's history to share their *Founders' Stories.* I am sure the knowledge and insight within each story will be of great value to the next generation. To those who have come before us, and to those who strive alongside us at present, you have my deep and heartfelt gratitude.

Looking Ahead

In the decade that has passed, new technologies, such as AI and quantum computing, have shown great potential in enhancing the capabilities of both threat actors and cyber defenders. Yet other aspects of cybersecurity remain unchanged, such as the fact that there will always be malicious actors seeking to weaponise the cyber domain. Coincidentally, Singapore held its General Election this year, just as it did when CSA was formed in 2015. As before, vigilance by CSA and other agencies helped ensure the elections remained secure and free from disruption, even with the advent of new threats like AI-enhanced misinformation campaigns and ransomware attacks. However, our greatest partner in the cybersecurity journey has been the public: While the government takes strategic measures, companies need to be diligent in practicing strong cyber hygiene, and individuals at the "last mile" need to exercise caution when confronted with suspicious links. As the old Malay saying goes, *Berat sama dipikul, ringan sama dijinjing* – "The heavy loads we carry together, and the light we lift together". Cybersecurity is, and will always be, a shared responsibility – one that binds us together in safeguarding our digital future.

As we look back over the past decade, the progress we have made has helped to make Singapore's cyberspace a safer place. However, there can be no rest, as malicious cyber actors continue to pose a threat to our national security, digital economy and digital way of life. As CSA prepares for many more years ahead at the Punggol Digital District, I have every confidence that we, on the shoulders of those who brought us thus far, will be able to bring Singapore's cybersecurity further. Together with our many partners, stakeholders, and Singaporeans, let us forge ahead towards a bright future where future generations can live, work and play online in a trusted, resilient, and vibrant cyberspace.

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

10 YEARS OF SECURING SINGAPORE'S CYBERSPACE: 2015-2025

Before 2015

Singapore's cybersecurity efforts were fragmented across various agencies, leading to occasional coordination challenges during significant incidents.

Coupled with ever escalating cyber threats, this necessitated a unified and centralised management of Singapore's cybersecurity operations.

2015
Formation of CSA

CSA was thus formed on 1 April 2015. It took over the functions previously carried out by:

Singapore Infocomm Technology Security Agency (SITSA), under Ministry of Home Affairs (MHA).

Singapore Cyber Emergency Response Team (SingCERT*) under then – Infocomm Development Authority of Singapore (IDA).

*Then known as Singapore Computer Emergency Response Team.

Dr Yaacob Ibrahim, appointed as the Minister-in-charge of Cyber Security.

Mr David Koh, appointed as Chief Executive, CSA.

2016
We took the first of many big steps, launching the:

Singapore International Cyber Week

ASEAN Ministerial Conference on Cybersecurity

Singapore Cybersecurity Strategy

Exercise Cyber Star

Singapore Cyber Landscape publication

2017
... and our efforts continued:

National Cybersecurity Awareness Campaign

Cyber Security Associates and Technologists Programme and Professional Conversion Programmes (joint initiative with IMDA)

Exercise Cyber Knights

MINDEF/SAF establishes the Defence Cyber Organisation

2018
We drove various cyber initiatives:

Cybersecurity Act 2018 passed in parliament

CII Protection Programme

Internet Hygiene Rating and Benchmarking tool for CII Sector Leads and Owners

Cybersecurity Code of Practice

Jointly launched Government Bug Bounty Programme with GovTech

2019
... And broadened our scope to encompass more domains and partners:

Singapore's Operational Technology (OT) Cybersecurity Masterplan

SG Cyber Women

ASEAN-Singapore Cybersecurity Centre of Excellence

Attained Certificate Authorising Nation status under the Common Criteria Recognition Arrangement

CSA invited to join the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

2020
We laid the foundations of a vibrant cybersecurity ecosystem:

Cybersecurity Labelling Scheme

Singapore's Safer Cyberspace Masterplan 2020

SG Cyber Talent

Cybersecurity Development Programme

2021
... And continued to push boundaries of important domains:

Cybersecurity Strategy 2021

OT Cybersecurity Expert Panel Forum

OT Cybersecurity Competency Framework

SG Cyber Safe Programme

Singapore served as Chair of the Open-Ended Working Group on security of and in use of ICTs 2021-2025

2022
We strove to strengthen cyber hygiene practices and partnerships:

Licensing Framework for Cybersecurity Service Providers

Counter-Ransomware Task Force

CII Supply Chain Programme

Internet Hygiene Portal

National Integrated Centre for Evaluation (joint initiative with NTU)

Cyber Essentials and Cyber Trust Mark

Launch of SPF Anti-Scam Command

Critical Infrastructure Defence Exercise

MINDEF/SAF launches the Digital and Intelligence Service

2023
... And these efforts continued to grow:

Cybersecurity Talent, Innovation and Growth (TIG) Plan

Cybersecurity Labelling Scheme for Medical Devices

SG Cyber Associates

ISO 27404 – Cybersecurity Labelling Framework (joint effort with USA and international partners)

Cloud Security Companion Guides

CyberSG R&D Programme

2024
We have consistently adapted to dynamic challenges:

Safe App Standard for Mobile Applications

TIG Collaboration Centre (joint initiative with NUS)

OT Cybersecurity Masterplan 2024

2025
And we look forward to the next 10 years of securing our cyberspace.

INAUGURAL ASEAN REGIONAL CERT TASKFORCE MEETING 2014

OTCEP FORUM 2024

CSLP OVERSEAS IMMERSION TRIP IN UK

LAUNCH OF CYBERSG TIG COLLABORATION CENTRE

CYBERSECURITY IS A TEAM EFFORT

9TH ASEAN MINISTERIAL CONFERENCE ON CYBERSECURITY

CONGRATULATORY MESSAGE

REFLECTIONS ON CSA'S JOURNEY BY SENIOR ADVISOR, PRIME MINISTER'S OFFICE AND FORMER COORDINATING MINISTER FOR NATIONAL SECURITY TEO CHEE HEAN

Even before Singapore formally embarked on our Smart Nation journey a little over 10 years ago, it was clear that digital technology had the potential to supercharge our economy and revolutionise the way we live. At the same time, it had also become apparent that digitalisation was increasingly being exploited by malicious actors and criminals to do significant harm.

This is why we established the Cyber Security Agency of Singapore (CSA) in 2015. As the lead agency providing dedicated and centralised oversight of Singapore's cybersecurity, CSA brought together an array of peacetime and crisis functions under a single unified structure. Its mission was to protect Singapore's cyberspace so that we could reap the full potential of digital technology with trust and confidence.

CSA's placement under the Prime Minister's Office reflected both the national importance of this issue, as well as the need for the agency to operate across the whole of government, beyond any specific ministry. To be effective, CSA had to collaborate not just with the rest of Government, but also with the public, academia, and particularly with industry, where the bulk of cyber resources and capabilities resided.

From a core founding team of 70 officers 10 years ago, CSA is now 500 strong. Through its partnerships, CSA has helped develop strong domestic cybersecurity capabilities and a vibrant cybersecurity ecosystem. It works closely with Critical Information Infrastructure owners and others to strengthen the security and resilience of our essential services and digital infrastructure, while also engaging the public to educate and equip them against cyber threats and online harms.

The borderless nature of cyberspace means that threats can come from anywhere. I am therefore glad that CSA has been actively driving international collaboration, dialogue and collective action, to shape a cyberspace that is trusted, secure, stable and interoperable.

But the challenge of preserving Singapore's cybersecurity will only grow. There are two key reasons for this.

Not so long ago, digital technology was primarily assistive: interruptions in digital services brought some measure of inconvenience and delay, but life could go on. Digital technology is now mission critical in many sectors – healthcare, banking, emergency response, transport, to name just a few. A major cyber disruption can bring essential services, and our lives, to a grinding halt.

The second reason is that cyber threats are becoming more sophisticated, persistent and difficult to detect. This trend is now being fuelled by new technologies like generative AI. Rising geopolitical tensions are also playing out in cyberspace as states jostle with each other in pursuit of their national interests.

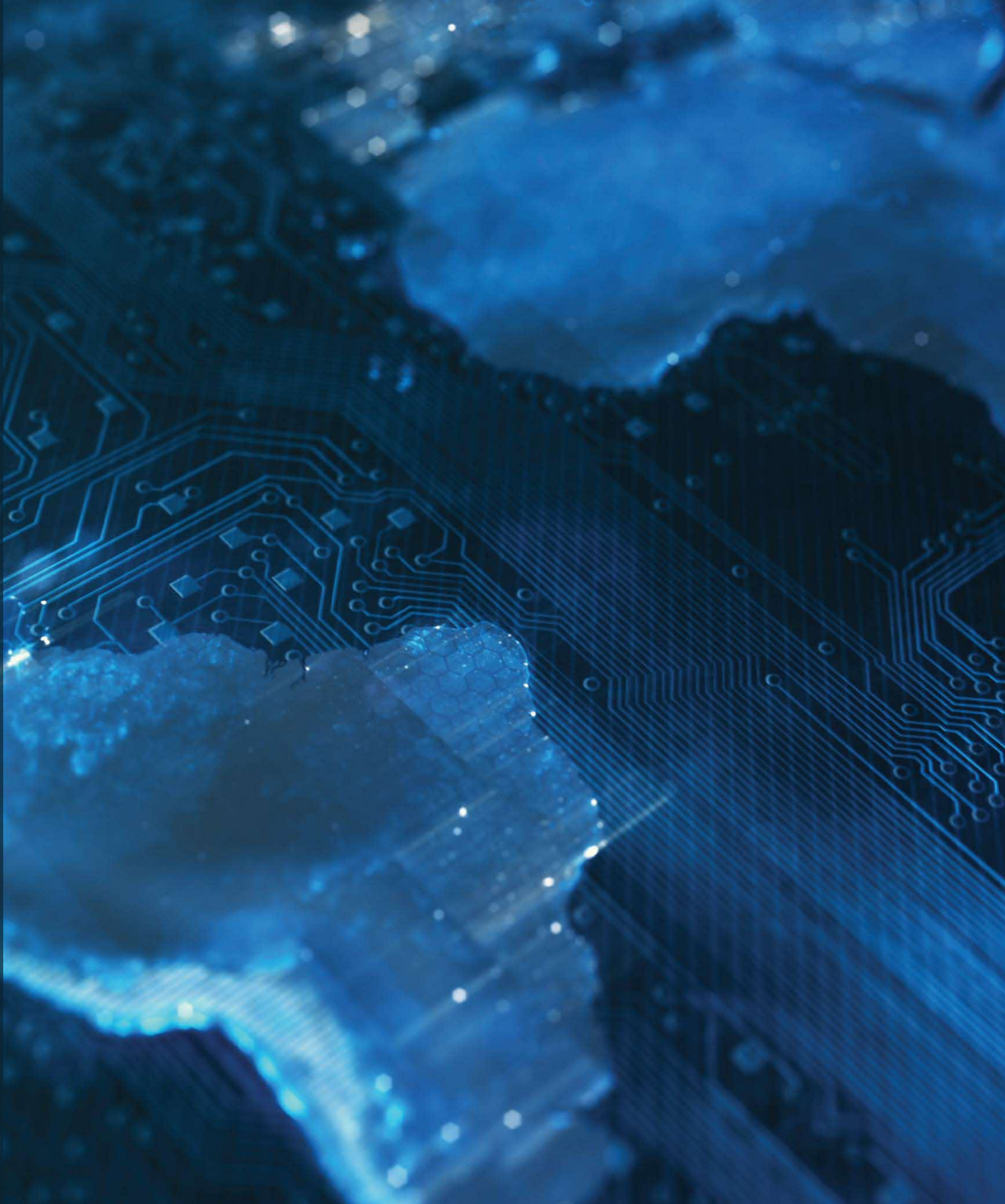
Against this backdrop, CSA's mission is even more important. I thank CSA and its officers for their contributions and steadfast efforts in keeping our cyberspace safe and secure. I wish CSA continued success in fostering a trusted and resilient cyberspace that allows Singapore to continue capturing the benefits of a more connected world.

Mr Teo Chee Hean
Senior Advisor, Prime Minister's Office
Former Coordinating Minister for National Security

GLOBAL TRENDS IN 2024

2024 was an eventful year in the global digital landscape, with several high-profile cybersecurity incidents and internet disruptions. State-sponsored hacking groups and cybercriminals carried out large scale hacking campaigns, while a series of subsea internet fibre cable cuts rekindled fears over how fragile our global connectivity network truly is. What set 2024 apart though, was the increasing scale and pervasiveness of these incidents. Distributed denial-of-service (DDoS) attacks increased, while advanced persistent threats (APTs) became stealthier and more sophisticated in their tactics. Operational technology (OT) systems were increasingly targeted by cyber-attacks, while ransomware remained a pressing concern for organisations worldwide.

To delve deeper into these critical areas, CSA's valued partner contributors: Cloudflare, Dragos, Google Threat Intelligence Group, and Recorded Future's Insikt Group – acknowledged leaders in the cybersecurity and tech domains – have provided insights into the evolving cyber threat landscape within this chapter.



INTERVIEW WITH SENIOR ADVISOR YONG YING-I, FORMER PERMANENT SECRETARY (COMMUNICATIONS AND INFORMATION) AND PERMANENT SECRETARY (CYBERSECURITY)

What Were Some Pivotal Moments in CSA's Early Days That Shaped Singapore's Cyber Security and Digital Evolution?

1. Having previously led the Ministry of Communications and Information, now known as Ministry of Digital Development and Information (MDDI), as Permanant Secretary (PS) to strengthen Singapore's position in the digital space, how do you envisage Singapore's continued development, and what key opportunities or challenges do you foresee within the next decade?

The digital landscape has evolved dramatically in recent years. Artificial intelligence (AI) has developed rapidly, and likewise the recognition of new cybersecurity challenges and the demand for governance and ethical frameworks for its use. And there is deployment of quantum technologies on the horizon.

This is not new. This is clear from my various involvements in digital since setting up and leading the Infocomm Development Authority (now-IMDA) just before 2000. I have worked in various areas such as healthcare IT; research and innovation in digital, including AI and cybersecurity; driving public sector digital transformation, and digital policies and governance. I have been privileged to have had a front row seat working on and watching the development of many aspects of digital, from the investment in deep-technologies and complex projects, to encouraging widespread adoption and managing risks. There were major waves – the dot-com boom and bust, cloud adoption, broadband/ fibre to the home/ 5G, proliferation of apps and use of application programming interfaces (APIs), growth of data centre infrastructure and software-as-a-service (SaaS). Now, we see a flourishing of proof-of-concept projects in AI. I have no doubt there will be more waves of digital.

Singapore has placed priority on having a trusted digital environment. We want our enterprises and citizens to benefit from the efficiencies and convenience of digital services, but this only works in an environment of trust and online safety. Digital offers so many new opportunities, but it has also generated new risks and threats. Other than mainstream cyber threats of hacking, data theft and disabling services, there are the scourges of scams, fake news, cyberbullying etc. We cannot go digital successfully if the law of the jungle prevails. The government has therefore also

put in resources to strengthen our technical defences in this broad space, enacted new laws and regulations to protect our people and worked with other countries in international platforms to strengthen the international rule of law and improve governance standards.

"Going digital" means adopting a balanced approach. I chair Singapore's Central Provident Fund Board, which is our national social security fund. While the organisation has been one of the most progressive organisations in "going digital to the core", and greatly improving services to citizens and increasing efficiency of operations, we also recognise that it does not mean "only digital". There will be segments of the population unable or unwilling to go digital, and it may be safer for them not to. To counter the scourge of scams, we have indeed "thrown sand in the wheels" of our online services, because we want to increase protection for citizens. The default online withdrawal limits has been reduced (which individuals can change); likewise the total maximum daily online withdrawal limits. Backroom checks have been strengthened; likewise close collaboration with other agencies on the shared goal of protecting our people. We are grateful that citizens have been understanding and supportive of these efforts.

2. Amid increased cyber threats globally during your time as PS (CI) and PS (Cybersecurity), what were some of the pressing cyber/digital threats? How did Singapore adapt its cybersecurity strategies to address these emerging and increasingly sophisticated threats?

I was closely involved in orchestrating funding for a stronger integrated national-level research and development (R&D) effort for cybersecurity as PS/National Research Foundation, and then more aspects of cybersecurity as PS/Cybersecurity. I also worked on various significant cyber incidents such as some major hacking breaches and data leaks, including incidents like SolarWinds and Log4j. These highlighted several learning points:

a. In CSA's early years, the focus was on protecting our national level critical information infrastructure (CII). These includes our banks, communications infrastructure, power and water systems, major transport systems etc. Requirements elsewhere were more limited. Beyond the Personal Data Protection Act provisions, much of it was voluntary. Additionally, cyber expertise in enterprises was also limited.

   This "narrow, steep pyramid" needs to broaden its base significantly, as online services expand dramatically. We need many, many more enterprises to strengthen their cybersecurity capabilities. Hackers, scammers and other criminals may steal some data from systems with weaker protection, but by putting data from various sources together (like solving jigsaw puzzles), threat actors can develop profiles of target victims quite effectively.

   The government will support this expansion of capabilities with funding for skills training and upgrading and other support. Shared services by technically capable providers is also part of the solution for small and medium enterprises (SMEs) in various industries.

b. The global tech giants have to take accountability and responsibility for the reality that the global system is interconnected and virtually all enterprises rely on them. The SolarWinds incident highlighted that we are all reliant on major players and gaps on their part can affect us all. Global regulations and standards are slow to develop – they exist for more mature industries, but not quite yet in digital. The massive externalities involved in global digital systems point to the need for this accountability.

c. Cybersecurity is no longer the narrow responsibility of the IT leader or chief information security officer (CISO) in our organisations. All members of boards and all senior management teams need to accept they have shared accountability for cybersecurity of their organisations. This means they have to learn enough about the technicalities of the subject to participate meaningfully in its management. Why? Because "ops" and "tech" designs must align. And it is the broader management team, not the IT leader or CISO, that understand their operations best and own the decision rights for choices made. It is critical that they consider the cyber risks of the operational processes they are choosing, whether digital or non-digital. Cyber protection should be designed into the processes from Day 1, and the broader management team must own it. Boards likewise have to make investment decisions impacting the enterprise's cyber stance, sometimes major ones. They need to debate the risks of various options they choose.

d. We are right to invest in R&D, to build up our own capabilities. We must have technical knowledge to make better design and deployment choices. We need to have sharper capabilities to know what to buy and not buy, and when we must try to build our own. It is not easy, but we will continue to invest and build. Having our own capabilities expand our options, all the more important in a geopolitically more uncertain world.

3. Do you have any quotes as a prelude to our Chapter on the Global Trends in 2024?

As we move forward, let me end with this quote, "However impenetrable it seems, if you don't try it, then you can never do it". (Prof Sir Andrew J Wiles)

When Cyber Becomes Real - Convergence of the Cyber, Physical and Digital Domains

Netflix's *Zero Day*, which premiered in February 2025, delivered a gripping portrayal of a catastrophic cyber-attack that disrupted critical infrastructure – causing train collisions, airplane malfunctions and hospital equipment failures – and claimed thousands of lives. Beyond its dramatised narrative, *Zero Day* reflected a stark reality: the increasingly blurred boundaries between the cyber, digital, and physical domains in our interconnected world. In this section, we cover two notable developments in 2024, illustrating how digital disruptions can result from causes other than a cyber-attack, and even due to physical impact. Both demonstrate the tangible impacts of intangible bits and bytes flowing throughout our daily lives, and the continued importance of cybersecurity in this digital age.

CrowdStrike

The Friday morning of 19 July 2024 began like any other: as people across Asia woke up and headed to work, those in the Western hemisphere began winding down for the night. The day before, isolated reports of users affected by outage issues with Microsoft's cloud services had emerged, but these were largely confined to the US and were soon resolved. No signs or warnings indicated that this was going to be an unforgettable day.

Within the span of a few hours, thousands of Windows systems froze and crashed, causing flight delays and cancellations as queues of weary and frustrated travellers snaked across multiple airports. The impact was worldwide, with cash registers in Japan, train ticket dispensers in Europe, and even gantries across some 185 carparks in Singapore failing to operate in what soon emerged as the biggest IT outage in history.[1] For the generation that had lived in fear of the Y2K scare – a global technological collapse brought about by a bug in computer systems – the CrowdStrike outage on 19 July seemed

[1] Housing & Development Board, "Housing & Development Board's Post," Social Media, Facebook, July 19, 2024, https://www.facebook.com/SingaporeHDB/posts/update-as-of-this-morning-all-185-carparks-in-hdb-estates-that-were-affected-by-/902649185240789/.

:(
Your PC ran into a problem and ne
Restart will be available:(15% comp

to vindicate concerns over society's over-dependence on technology.

The technical root causes of the outage are well known by now: an update by CrowdStrike for its security software contained an error, which triggered a series of software failures that resulted in the Windows operating system crashing. As multiple Windows systems running CrowdStrike's security software received the update with the error, the impact multiplied, likely triggering cascading failures in downstream secondary and tertiary systems that depended on these upstream systems for continued operations. The incident's immediate impact was staggering: 8.5 million devices affected across multiple industries worldwide,[2] financial losses of US$5.4 billion to Fortune 500 companies,[3] and nearly 40,000 flight cancellations or delays on 19 July alone.[4] CrowdStrike responded by speedily isolating and rectifying the initial error in several hours while remaining communicative and responsive to their clients throughout the incident. Additionally, CrowdStrike demonstrated their commitment to transparency by publishing their detailed root cause analysis (RCA) less than a month after the initial incident.

The events of 19 July brought a sobering reminder that the digital and physical worlds are inextricably connected. While the CrowdStrike outage was the first of such scale, it is unlikely to be the last, given the complexities inherent in the millions of lines of code underpinning the systems we use daily for work, transportation, and entertainment. Organisations seeking to better prepare themselves for the next outage may benefit from building their digital resilience and business continuity. To that end, CSA's advisory may be helpful as it explores the risk-based strategies available to organisations at all levels of maturity.[5] Data resilience – which includes ensuring availability of one's access to data, even during an outage – is also important, and the advisory also provides tips for organisations seeking to achieve this resiliency.[6]

Submarine Cables – Our Digital Lifelines

Hundreds of metres beneath the waves of the Baltic Sea lies a stretch of bundled glass strands, wrapped in multiple layers of protective sheathing. This is but a fraction of around 1.5 million kilometres of submarine cables, extending across Earth's ocean floors, acting as conduits for electricity, gas, and data.

With diameters no larger than soda cans, these fibre optic cables carry over 97% of intercontinental telecommunications traffic – and are appropriately nicknamed "the backbone of the internet". However, and contrary to the essential role that they play – these digital lifelines are also highly vulnerable, regularly snapping, severing, or even becoming corroded. When this happens, the impact to the countries the cables serve is often catastrophic, and may even affect other countries downstream.

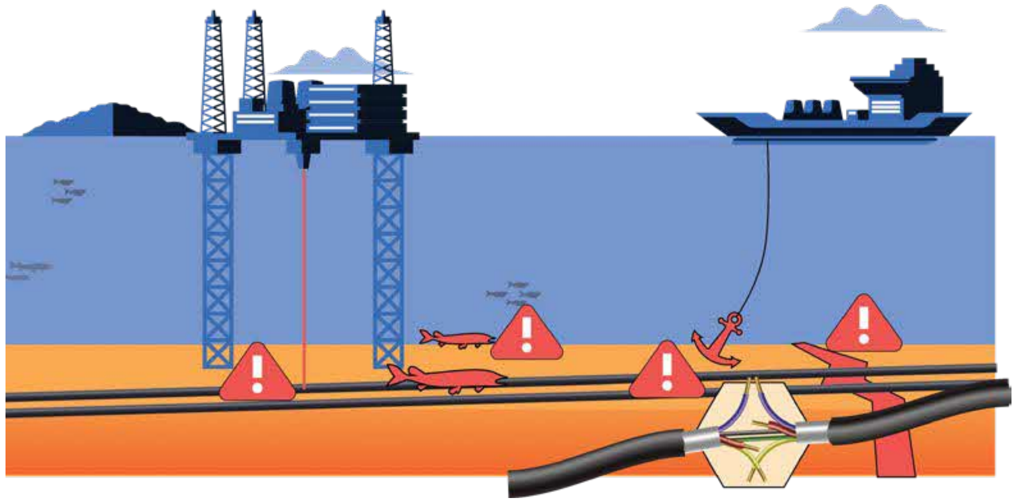
[2] Microsoft, "Helping Our Customers through the CrowdStrike Outage", Blog, Official Microsoft Blog (blog), July 20, 2024, https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/.

[3] Parametrix, "CrowdStrike to cost Fortune 500 $5.4b; Insured Loss Range of $0.54b - $1.08b", July 24, 2024, https://www.parametrixinsurance.com/in-the-news/crowdstrike-to-cost-fortune-500-5-4-billion-insured-loss-range-of-540-million-to-1-08-billion.

[4] Aarian Marshall, "Why the Global CrowdStrike Outage Hit Airports So Hard," Wired, July 19, 2024, https://www.wired.com/story/crowdstrike-windows-outage-airport-travel-delays/.

[5] Cyber Security Agency of Singapore, "Building Digital Resilience for Organisations," Advisories, July 31, 2024, https://www.csa.gov.sg/alerts-and-advisories/advisories-ad-2024-014.

[6] Cyber Security Agency of Singapore, "How Individuals and Organisations Can Ensure Data Resilience," Advisories, August 5, 2024, https://www.csa.gov.sg/alerts-and-advisories/advisories/ad-2024-015.



Incidents involving damage to subsea infrastructure have been occurring since the early 2000s. Most recently, in November 2024, two submarine telecommunication cables in the Baltic Sea (*BCS East-West Interlink* and *C-Lion1*) were cut. Spanning 218km, the *BCS East-West Interlink* connected Lithuania and Sweden, while the 1,170km long *C-Lion1* connected Finland to Germany. Notably, there were no significant outages due to implementation of existing redundancy measures. The following month, on Christmas Day 2024, another four submarine telecommunication cables (which connected Finland, Estonia and Germany) and a submarine power cable (*Estlink 2*, which supplied electricity from Finland to Estonia) in the Baltic Sea were severed in a separate anchor dragging incident. The damage to the submarine power cable reduced the cross-border electricity transmission capacity between Finland and Estonia by nearly 65%, but the impact was minimised due to redundancy measures. The affected countries blamed Russian sabotage for both incidents; Russian authorities, in turn, dismissed the claims as absurd, pointing to the lack of evidence.

In contrast, incidents involving the cutting of submarine cables in the Red Sea and African coast had more severe consequences. In February 2024, four submarine cables were severed, reportedly by the anchor of a sinking ship *Rubymar*, which dragged across the seabed after a missile attack by Houthi militants. About 25% of telecommunications traffic within the region in West Asia and the African continent was disrupted as a result. Reports estimate approximately 100 million people across the African continent were affected, with Ghana, Liberia and Cote d'Ivoire experiencing the outages for up to ten days. Tech and telecommunication companies such as Google, Meta, SubCom, Orange, Ogero, Bayobab and Vodafone mitigated the disruptive effects by rerouting data traffic across land-based routes.

In March 2024, 13 countries across the African continent yet again experienced internet outages from unspecified damage to submarine cables near Cote d'Ivoire and Senegal.[7] Nearly all internet-dependent services were impacted, with financial institutions, telecommunication companies and enterprises having their services disrupted. Many eventually had to scale down their operations, by resorting to alternative platforms for transactions, activating backup systems to reroute traffic, and dispatching engineers to repair the damaged cables.

[7] Some reports indicate the cable cuts were caused by seismic activity on the seabed.

While the recent submarine cable disruptions primarily affected entities in Europe and Africa, it is important to note that Singapore is equally susceptible to submarine cable disruptions. In December 2006, an earthquake of magnitude 7.0 struck Taiwan's southwest coast, causing catastrophic damage and severing eight submarine cables in total. This event had significant consequences on telecommunications and internet connectivity across Asia, including Singapore:

- Chunghwa Telecom, the largest telecommunications operator in Taiwan, reported complete internet outage to Hong Kong and Southeast Asia.
- Phone service capacities in Taiwan, Japan and South Korea were reduced by approximately 50 to 60 percent.
- Singtel and StarHub reported slow internet access and difficulty in connecting to international websites and search engines, such as Google, Yahoo and MSN.
- Locally, ripple effects were felt on financial and online services, with internet banking and overall connectivity becoming intermittent.

Singapore's telecommunications infrastructure eventually recovered over the course of a week, with local telecommunication companies routing traffic through alternative routes to restore internet access. 18 years later, in 2024, Singapore is connected to 26 submarine cables, landing across three designated sites. While natural disasters can still occur in any part of the world, Singapore is today more resilient through route diversification and robust safeguards. These efforts will not only safeguard Singapore's critical information infrastructure, but also our digital way of life.

In November 2024, the United Nations (UN), along with international counterparts, created the International Advisory Body for Submarine Cable Resilience. This advisory body, involving organisations such as the UN's International Telecommunications Union (ITU), seeks to address challenges such as submarine cable damage, cyber threats, and geopolitical tensions that might threaten these critical networks. With an average of 150 to 200 incidents causing damage to submarine cables each year, this necessitates about three cable repairs each week. The establishment of this advisory body aims to promote best practices for governments and industry players globally, to strengthen the resilience of our submarine cable networks. As these submarine cable incidents demonstrate, the digital age is not just about firewalls and encryption — it is also about protecting the physical infrastructure that makes the internet possible.

Conclusion

As our world becomes increasingly digitalised, disruptions like the CrowdStrike outage and submarine cable cuts will likely become more impactful. To navigate this new reality, it is crucial for us to adopt a proactive mindset:

1. **Stay Informed**. Educate ourselves on the importance of our digital infrastructure and the risks it faces. Understanding its significance and vulnerabilities will help us better navigate potential disruptions.
2. **Stay Prepared**. Develop contingency plans tailored to our needs. For organisations, this may include having backup communication methods and redundancy for critical systems. For individuals, it could involve regularly backing up data, and ensuring these backups are accessible during emergencies.
3. **Stay Resilient**. Aside from developing systems and strategies that can withstand and recover from digital disruptions, it will be equally important to foster a culture of adaptability to ensure continuity in the face of emergencies.

By embracing these principles, we can build a more resilient digital society that is better equipped to handle the challenges of our increasingly interconnected world.

2024 Global Distributed Denial-of-Service (DDoS) Landscape

Contribution by **Mr Omer Yoachimik, Senior Product Manager for DDoS Protection & Security Reporting, Cloudflare**

DDoS attacks in 2024 saw an unprecedented, record-breaking rise in both sophistication and volume – driven in part by powerful global botnets spun up by easily available generative artificial intelligence (GenAI) tools. Countries in Asia led the DDoS rankings, comprising 60% of the most attacked locations globally.

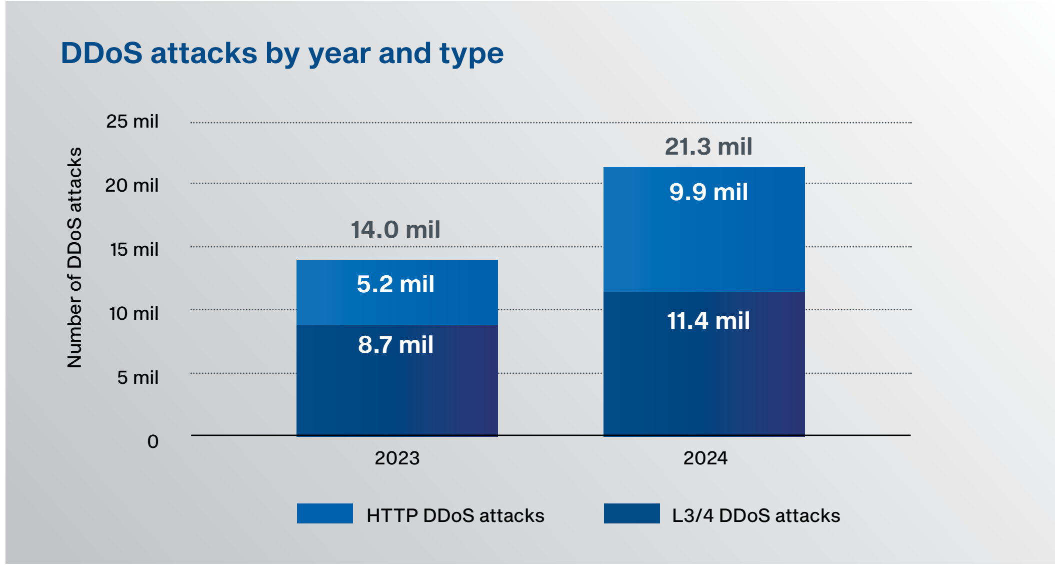
2024 also saw novel techniques and targets – in addition to a rise in Ransom DDoS attacks, the range of targets has broadened, driven by geopolitical factors and hacktivists looking to create chaos.

A rise in short-duration attacks and botnet-driven traffic further underlines the need for Singapore organisations to recognise and respond to threats by employing best-in-class DDoS protection. Understanding trends can help organisations better prepare for the growing threat landscape.

This segment offers insights into the evolving DDoS threat landscape in 2024 based on data from the Cloudflare network – one of the largest in the world – which encompasses about 20% of the Internet.[1] This extensive infrastructure uniquely positions Cloudflare to provide key insights and trends that benefit the wider internet community.[2]

[1] https://www.cloudflare.com/network/

[2] All editions of Cloudflare's DDoS threat reports are available on the Cloudflare blog and on Cloudflare Radar, a publicly available interactive hub with insights on global Internet traffic, attacks, and technology trends. Cloudflare Radar includes drill-down and filtering capabilities to zoom in on specific countries, industries, and networks. There is also a free API allowing academics, data sleuths, and other web enthusiasts to investigate Internet trends across the globe. To learn how we prepare Cloudflare's DDoS reports, please refer to our Methodologies.

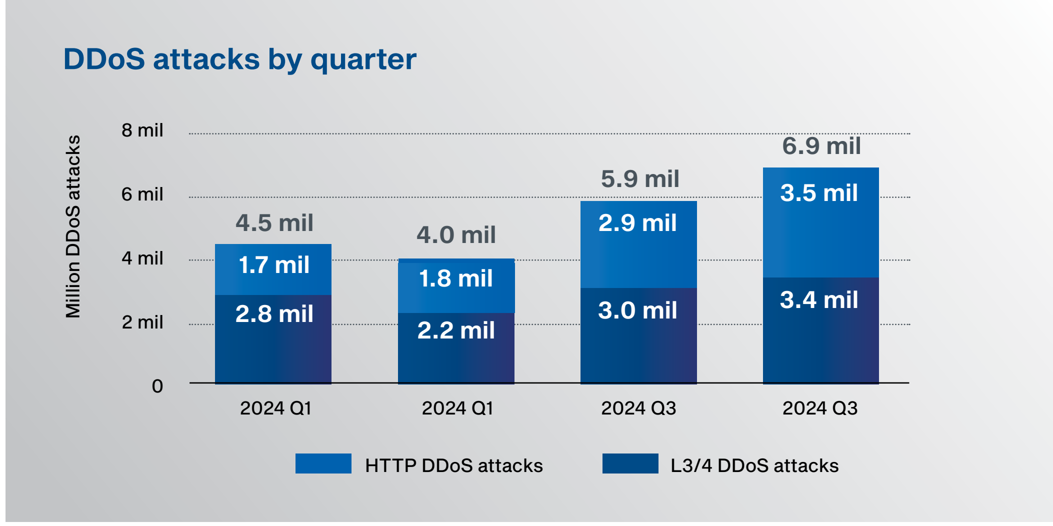


DDoS Attacks Increased in 2024

Throughout 2024, Cloudflare's automated defense systems blocked 21.3 million DDoS attacks, marking a 53% increase from 2023. On average, 4,870 attacks were blocked every hour. Of these, 11.4 million were Layer 3/4 attacks (a 30% increase from 2023), while 9.9 million were HTTP-based attacks (up 90%).

Q4 2024 saw a surge in hyper-volumetric Layer 3/Layer 4 DDoS attacks, with a record-breaking DDoS attack peaking at 5.6 terabits per second (Tbps) in late October 2024. This rise in attack size renders capacity-limited cloud DDoS protection services or on-premise DDoS appliances obsolete.

Q4 2024 saw Cloudflare mitigate 6.9 million attacks, representing a 16% increase quarter-over-quarter and 83% year-over-year.



A Closer Look at Singapore

7TH During Q4 2024, Singapore was the seventh most attacked country globally — down three spots since the previous quarter.

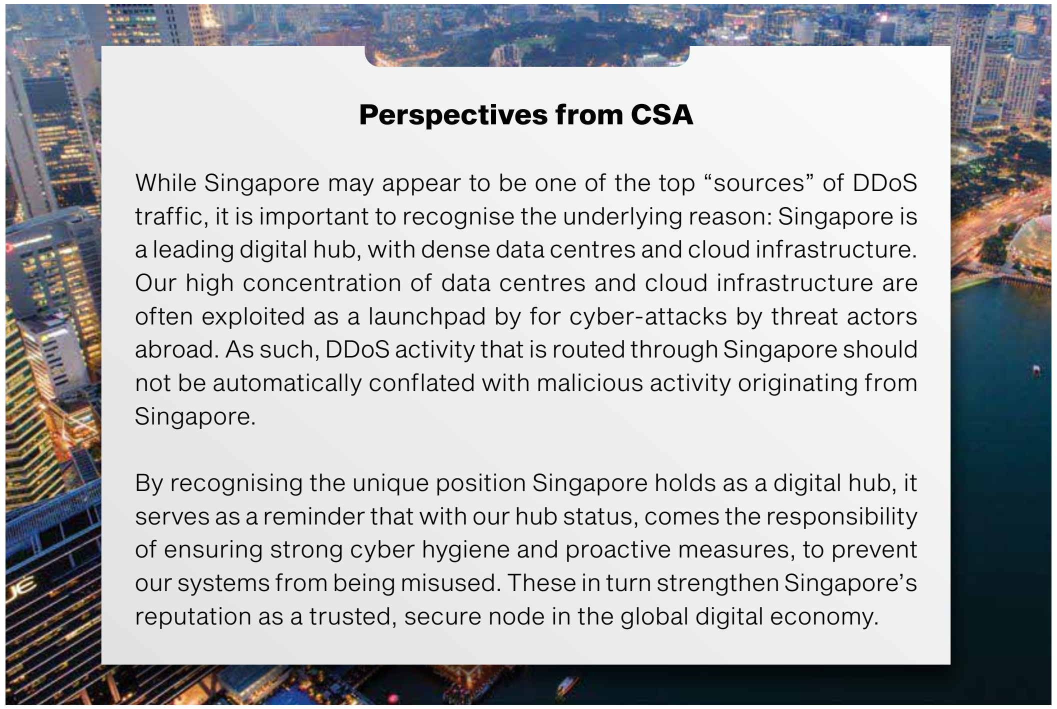
10TH Diving deeper, Singapore was the 10th most attacked country by network-layer DDoS attacks. Over 4% of all Singapore-bound traffic were part of network-layer DDoS attacks.

11TH Singapore was also the 11th most attacked country by HTTP DDoS attacks. Two out of every 100 HTTP requests towards Singapore were part of DDoS attacks.

3RD Singapore ranked as the third-largest source of DDoS attack traffic. As a highly connected technology and data centre hub, it corresponds with the overall high traffic levels and illustrates how threat actors target and exploit infrastructure in digitally advanced countries, rather than attacks being orchestrated by the nation itself. This highlights the increased need for vigilance and proactive measures against threats.

5TH Looking specifically at HTTP DDoS attacks, Singapore was the fifth largest source. Over 5% of all HTTP DDoS requests that Cloudflare mitigated worldwide originated from Singaporean IP addresses – equivalent to around 12% of all Singapore-outbound traffic.

5TH When looking at network-layer DDoS attacks, Singapore was also the fifth largest source with around 4% of all DDoS bytes worldwide originating from Singapore.



Perspectives from CSA

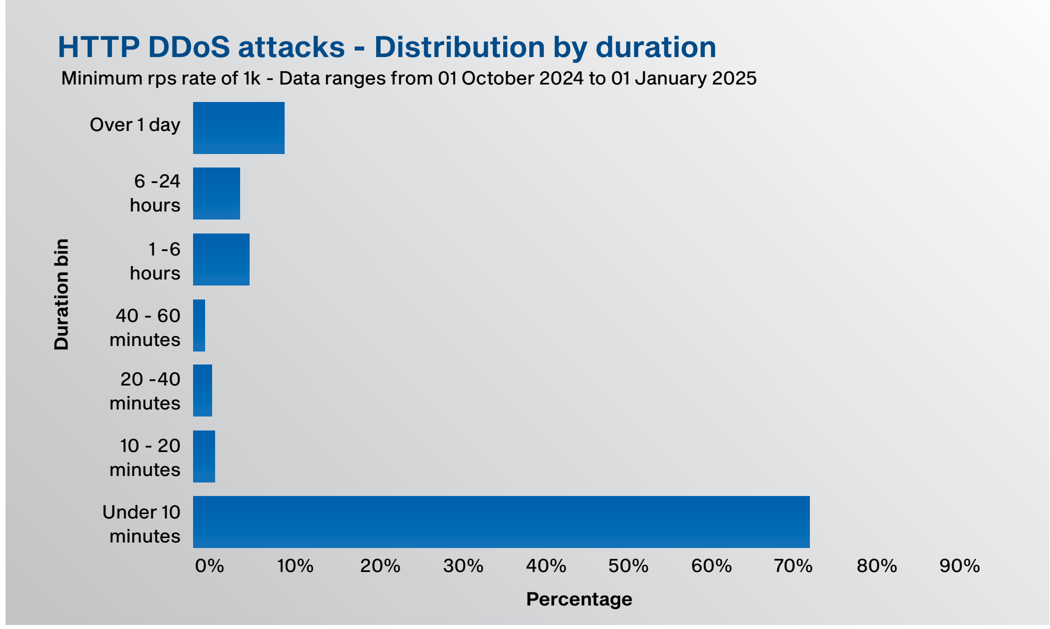
While Singapore may appear to be one of the top "sources" of DDoS traffic, it is important to recognise the underlying reason: Singapore is a leading digital hub, with dense data centres and cloud infrastructure. Our high concentration of data centres and cloud infrastructure are often exploited as a launchpad by for cyber-attacks by threat actors abroad. As such, DDoS activity that is routed through Singapore should not be automatically conflated with malicious activity originating from Singapore.

By recognising the unique position Singapore holds as a digital hub, it serves as a reminder that with our hub status, comes the responsibility of ensuring strong cyber hygiene and proactive measures, to prevent our systems from being misused. These in turn strengthen Singapore's reputation as a trusted, secure node in the global digital economy.

Global DDoS Trends in 2024

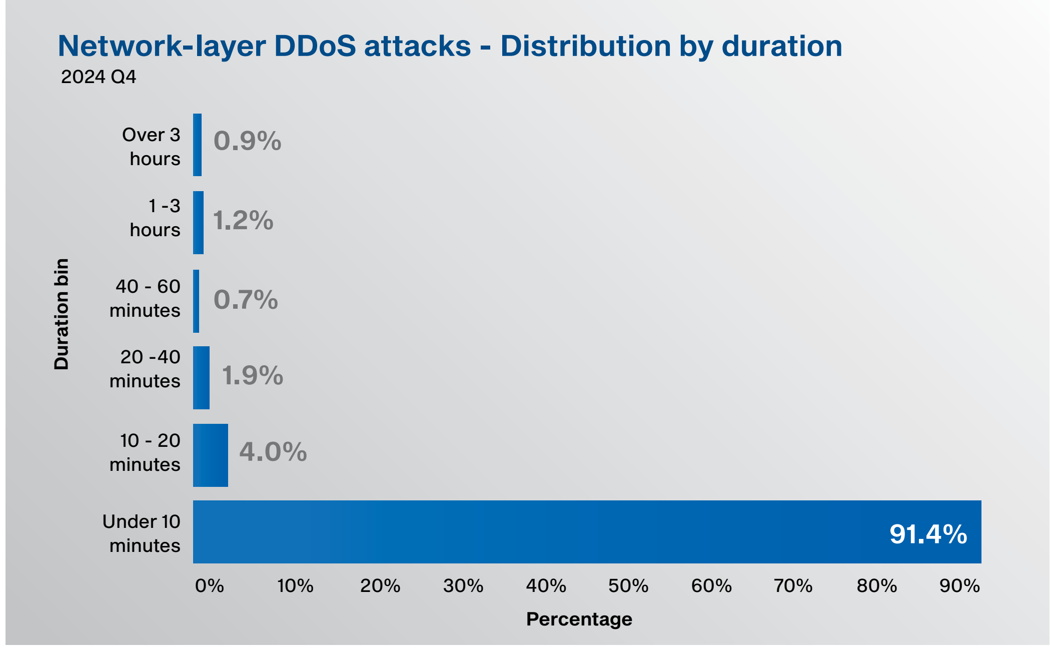
Short Attack Durations Highlight the Importance of Automated DDoS Protection

The majority of HTTP DDoS attacks (72%) lasted under 10 minutes, with 22% lasting more than an hour, and 11% lasting over 24 hours. 91% of network-layer DDoS attacks conclude within 10 minutes.



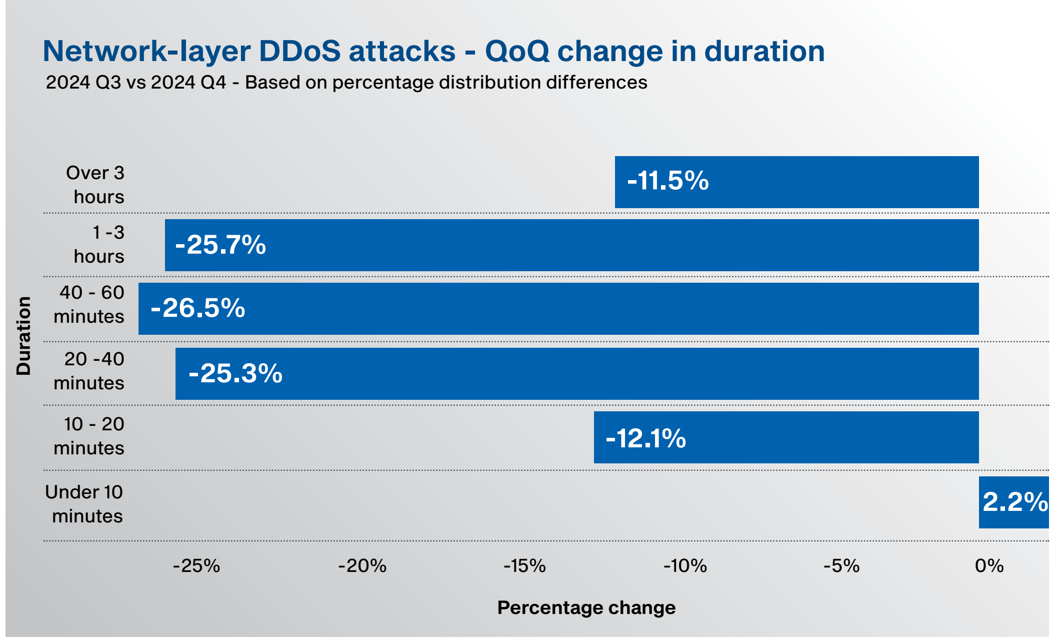
HTTP DDoS attacks - Distribution by duration

Minimum rps rate of 1k - Data ranges from 01 October 2024 to 01 January 2025



Network-layer DDoS attacks - Distribution by duration

2024 Q4



Network-layer DDoS attacks - QoQ change in duration

2024 Q3 vs 2024 Q4 - Based on percentage distribution differences

Average Attack Duration

In Q4 2024, the weighted average duration of a network-layer DDoS attack was approximately 9 minutes. For HTTP DDoS attacks, it was significantly higher, at around 5 hours and 35 minutes.

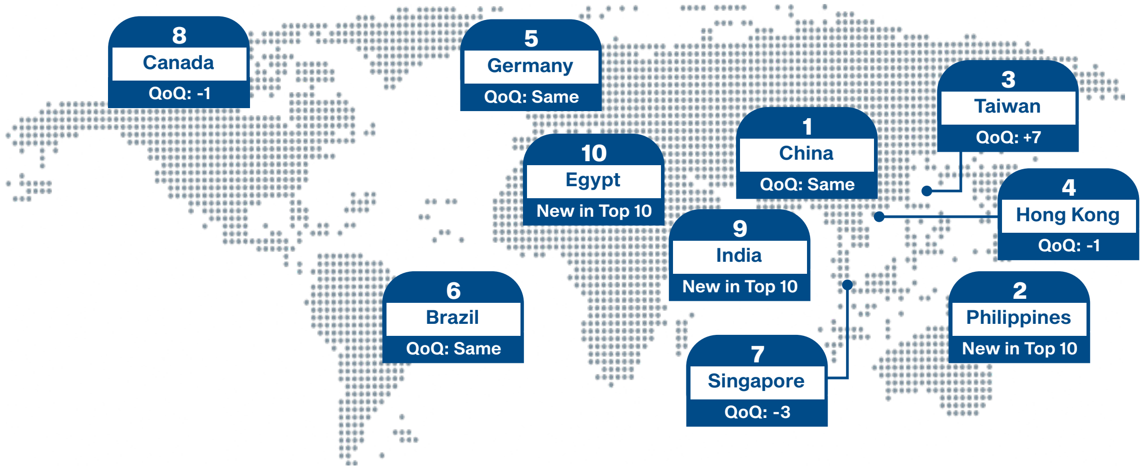
Top attacked industries globally

60% of the most attacked locations are in Asia

Top 10 most attacked industries in 2024 Q4

1	Telecommunications, Service Providers & Carriers	QoQ: +2
2	Internet	QoQ: +3
3	Marketing & Advertising	New in Top 10
4	Information Technology & Services	QoQ: -2
5	Gambling & Casinos	QoQ: +1
6	Gaming	QoQ: +1
7	Retail	QoQ: +3
8	Banking & Financial Services	QoQ: -7
9	Construction & Civil Engineering	QoQ: Same
10	Media, Production & Publishing	New in Top 10

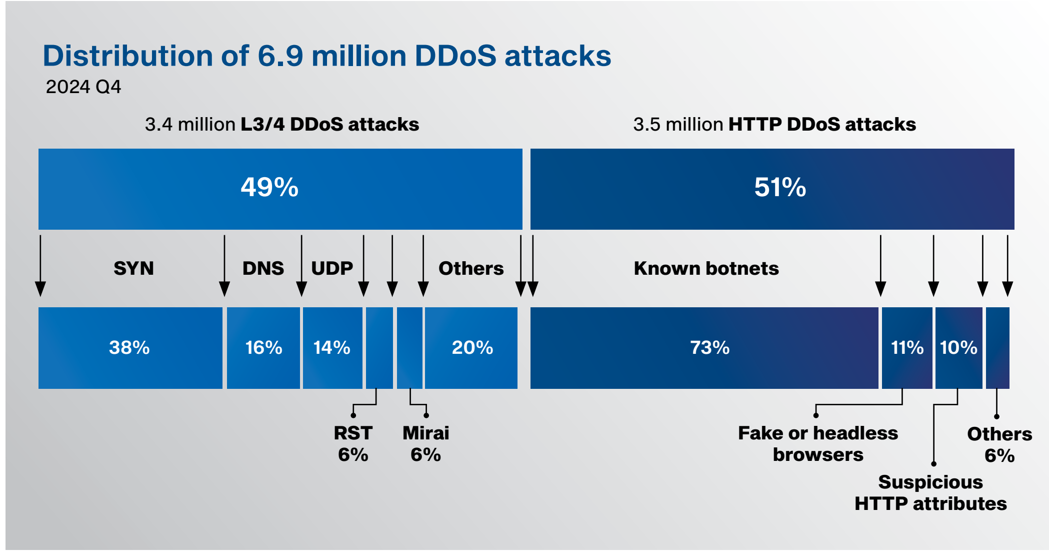
Top 10 most attacked locations in 2024 Q4



The Top Attack Vector Was Botnets

In Q4 2024, 73% of HTTP DDoS attacks were botnet-driven, while 11% attempted to mimic legitimate browsers, and 10% contained suspicious HTTP attributes. Network-layer attacks were dominated by SYN floods (38%), DNS floods (16%), and UDP floods (14%). A significant increase in Mirai botnet activity was also noted,[3] with Mirai variants responsible for 6% of all network-layer attacks in Q4, including the largest attack recorded in 2024.

Cloudflare helps network operators track malicious actors by providing a free DDoS Botnet threat intelligence feed.[4]

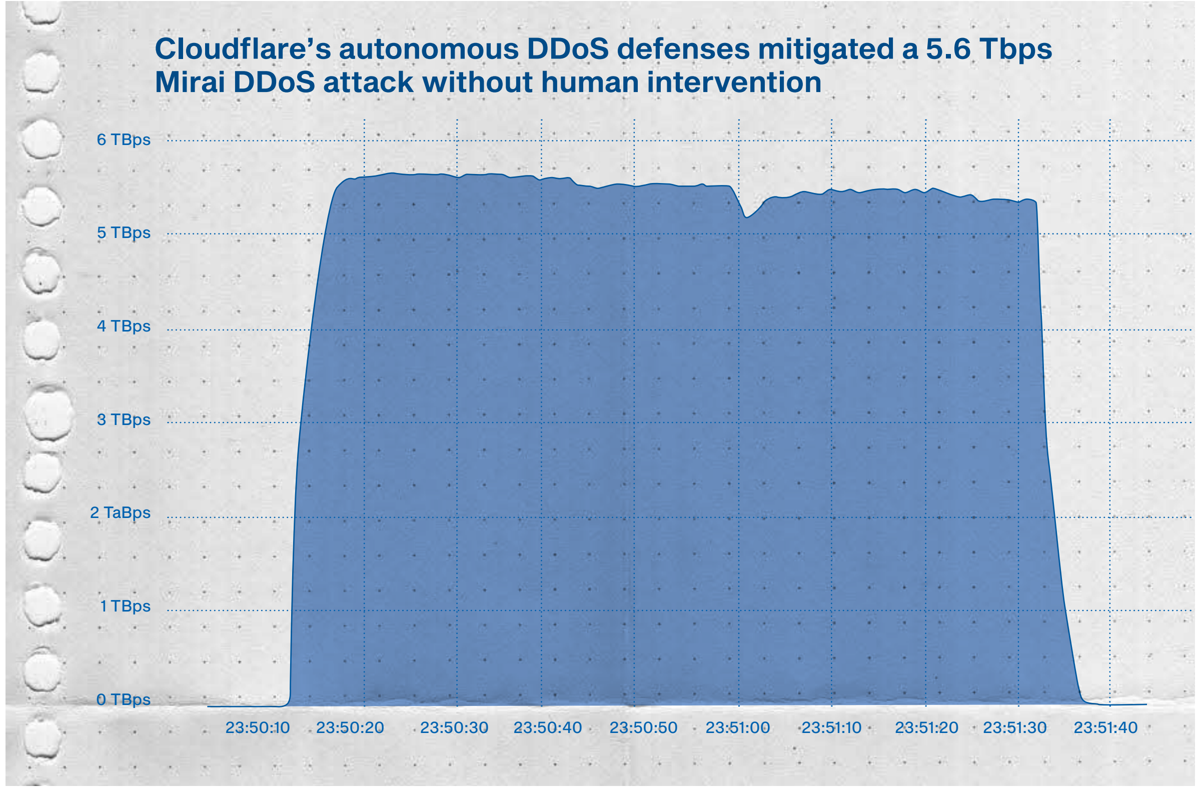


[3] https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/

[4] https://developers.cloudflare.com/ddos-protection/botnet-threat-feed/

Record-breaking 5.6 Tbps DDoS Attack

In late October 2024, Cloudflare's systems mitigated a record-breaking 5.6 Tbps DDoS attack launched by a Mirai-variant botnet. This UDP DDoS attack lasted only 80 seconds, originating from over 13,000 devices. Cloudflare's autonomous systems detected and mitigated the attack without human intervention, avoiding performance degradation.

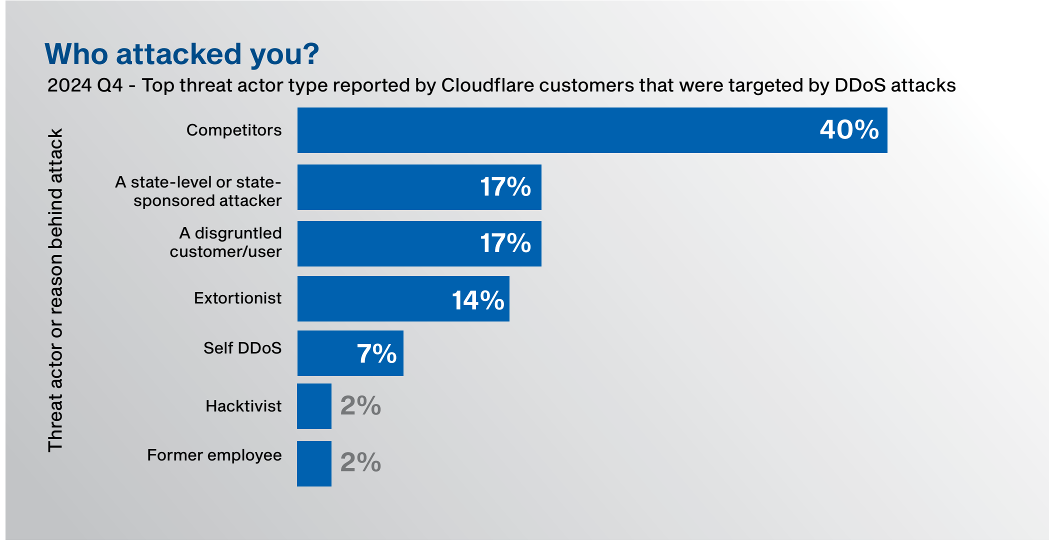


Attack Sizes Are Evolving

Most HTTP DDoS attacks (63%) involved fewer than 50,000 requests per second. However, 3% exceeded 100 million requests per second. Similarly, 93% of network-layer DDoS attacks did not exceed 500 Mbps, and 87% did not exceed 50,000 packets per second. Nevertheless, attacks surpassing 1 Tbps and 1 billion packets per second have become increasingly frequent, with the number of 1 Tbps attacks growing by 1,885% quarter-over-quarter.

Top Threat Actors Perceived To Be Competitors

Cloudflare's survey of targeted customers revealed that most organisations did not know who launched the attacks. Of those who did, 40% attributed the attacks to competitors.



Who attacked you?

2024 Q4 - Top threat actor type reported by Cloudflare customers that were targeted by DDoS attacks

Proactive DDoS Threat Defense

While AI systems are able to enhance the effectiveness of cybersecurity measures across the evolving threat landscape, organisations must play a proactive role, constantly adapting and updating their defense mechanisms to stay one step ahead of malicious activity.

There are several key factors that organisations can consider in the implementation of a proactive DDoS threat defense:

Attack surface reduction to minimise the effect of a DDoS attack. Methods include restricting traffic to specific locations and implementing a load balancer.

An Anycast network helps increase the surface area of an organisation's network, so that it can more easily absorb volumetric traffic spikes and prevent outages by dispersing traffic across multiple distributed servers.

Real-time, adaptive threat monitoring can help pinpoint potential threats by analysing network traffic patterns, monitoring traffic spikes or other unusual activity, and adapting to defend against anomalous or malicious requests, protocols, and IP blocks.

Caching: A cache stores copies of requested content so that fewer requests are serviced by origin servers. Using a content delivery network (CDN) to cache resources can reduce the strain on an organisation's servers and make it more difficult for them to become overloaded by both legitimate and malicious requests.

Rate limiting: Rate limiting restricts the volume of network traffic over a specific time period, essentially preventing web servers from getting overwhelmed by requests from specific IP addresses. Rate limiting can be used to prevent DDoS attacks that use botnets to spam an endpoint with an abnormal number of requests.

The State of Operational Technology (OT) Security

Contribution by **Liz Martin, Global Technical Lead Threat Intelligence, Dragos**

The industrial threat landscape has seen many shifts over the years, and most notably what we have seen over the past year is increased threat activity. OT focused threats stem from sophisticated threat groups, ransomware groups and even hacktivist groups. More than half of the threat groups Dragos tracks actively targeted the Asia-Pacific region over the last year. The threats highlighted below are relevant to Asia-Pacific, which includes Singapore.

On a global scale, Dragos saw continued activity from *VOLTZITE*, one of the most alarming threat groups (associated with the group '*VOLT TYPHOON*').[1] Confirmed victims of *VOLTZITE* were initially found in North America, and subsequently across Africa, Guam, Europe and Asia-Pacific when the group expanded its campaign. Key sectors of interest to *VOLTZITE* appear to be the Electric, Emergency Management, Telecommunications, Satellite Services, National Security and Government.

- While this adversary is mainly focused on long-term reconnaissance and does not appear to have any notable capability for targeting Industrial Control System (ICS), it likely has intent to develop such capabilities for future operations.
- *VOLTZITE* continues to exfiltrate sensitive, OT-related data from networks and usually exploits vulnerable firewalls or virtual private networks (VPNs) for initial access.

In addition to the above activity, over the last year, we have seen hacktivists perform multiple open-source scans across industrial organisations' networks to reveal entry-points via exploitable vulnerabilities in programmable logic controllers (PLCs). Dragos officially denoted one of these hacktivist groups as *BAUXITE*. This group has demonstrated significant technical overlaps with the *CyberAv3ngers* hacktivist persona, and proven their ability to reach Stage 2 of the ICS Kill Chain in multiple campaigns from 2023 to the present day.

- If we look at hacktivist groups, these groups have shifted their modus operandi in an interesting but alarming manner.

[1] *VOLTZITE* activity overlaps with those designated as *VOLT TYPHOON* and *BRONZE SILHOUETTE*.

Increasingly, we observe more of these ‘groups’ intentionally targeting OT and, in some cases, successfully impacting OT.

- In one case, we saw a hacktivist group attack internet-exposed PLCs discovered through open-source scanning, and which had easily accessible login credentials.

- We have also seen hacktivists (*CyberAv3ngers* Group) target a known exploitable vulnerability in Unitronics PLCs across multiple regions. Numerous water utilities in North America had operations impacted in OT due to this vulnerability, and a water utility in Ireland fell victim to the same intrusion with 180 residents left without running water for two days.

- We are also continuing to see targeting of this vulnerability from other hacktivist groups (*Hunt3r Kill3rs* Group). *Hunt3r Kill3rs* also reached Stage 2 of the ICS Cyber Kill Chain for the third time, manipulating device data fields and resetting passwords on exposed controllers.

- There is a growing convergence of interests between sophisticated adversaries and hacktivist personas. We have seen them both use shared infrastructure and intelligence to attack OT/ICS targets.

Also worth noting over the past year, Dragos reported an average of 50 or more ransomware intrusions per week that led to industrial organisations being compromised and their data ending up on publicly available data leak sites (DLSs). Ransomware activity against industrial organisations has doubled year on year since 2022, and Dragos saw an overall 87% increase in ransomware activity against ICS/OT organisations over the past year.

- The most active ransomware groups against industrial organisations in 2024 were *RansomHub*, *Fog*, and *LockBit 3.0*.

- More than 50% of the ransomware incidents Dragos responded to in 2024 involved some element of a remote service being leveraged by adversaries, such as a VPN appliance or remote desktop protocol (RDP) server. Furthermore, 25% of the ransomware incidents resulted in a full OT/ICS shutdown, and the other 75% of the incidents resulted in partial disruptions.

- In 2024, an interesting and concerning convergence of hacktivism and ransomware emerged: Hacktivist groups employed ransomware as part of their operations. *Handala*, *Kill Security*, and *CyberVolk* were three notable hacktivist groups observed to actively using ransomware as part of their operations in 2024.

In April 2024, Dragos discovered *FrostyGoop*, the ninth-known ICS malware, and the most alarming attack that year. *FrostyGoop* modified instrument measurements of ENCO controllers, resulting in heating outages for over 600 apartment buildings in Ukraine during the winter. *FrostyGoop* interacts with ICS devices over Modbus TCP/502, a standard ICS protocol used worldwide, combining generic, publicly available Modbus libraries with logging capabilities to adaptively send commands that read and write registers on ICS devices. The January 2024 cyber-attack against a municipal district energy company in Ukraine involving *FrostyGoop* was likely a part of hybrid warfare in support of the Russia-Ukraine conflict. The attack’s exploitation of internet-exposed controllers and insufficient network segmentation highlights the risks of insufficient basic cybersecurity controls.

The activity highlighted stresses a growing trend in which we see normalisation of ICS/OT targeting by threat groups, compounded with geopolitical conflict-driven threats. While there is no one-size-fits-all approach, there are measures that can be undertaken to effectively mitigate against these trending threats and bolster defenses. Organisations can start with implementing appropriate security controls and best practices to build a more robust OT security program. For example, the SANS ICS 5 Critical Controls provide foundational and tangible best practices for ICS/OT asset owners to follow in addressing the challenges brought on by an ever-evolving OT threat landscape.

#1 ICS Incident Response (IR) Plan

- Have an operations-informed IR plan with a focus on system integrity and recovery capabilities when facing a cyber-attack.

- Understand that OT IR is not the same as IT IR — there are legacy systems and devices at play and the way forensics is done can differ quite significantly.

- Adversaries are becoming more OT/ICS aware, and their tactics, techniques and procedures (TTPs) are targeting deeper into industrial environments. Ensure your IR plans are able to respond to, and recover from, a variety of scenarios, such as supervisory control and data acquisition (SCADA) servers being encrypted by ransomware or *BAUXITE* modifying your PLCs.

#2 Defensible Architecture

- Design architectures that support visibility, log collection, asset identification, segmentation, industrial demilitarised zones (DMZs), and process-communication enforcement.

- RDP and secure shell (SSH) protocols are targeted by *BAUXITE*, while *VOLTZITE* has demonstrated living off the land (LoTL) techniques preying on poor cyber hygiene.

#3 ICS Visibility and Monitoring

- Enable continuous network security monitoring of the ICS environment using protocol-aware toolsets and system of systems interaction analysis capabilities.

- In previous years, 61% of Dragos clients struggled with visibility of their OT networks and systems.

- Understand the difference between a security event and an engineering problem.

#4 Secure Remote Access

- Identify all remote access points and allowed destination environments, and implement on-demand access and multi-factor authentication (MFA) where possible.

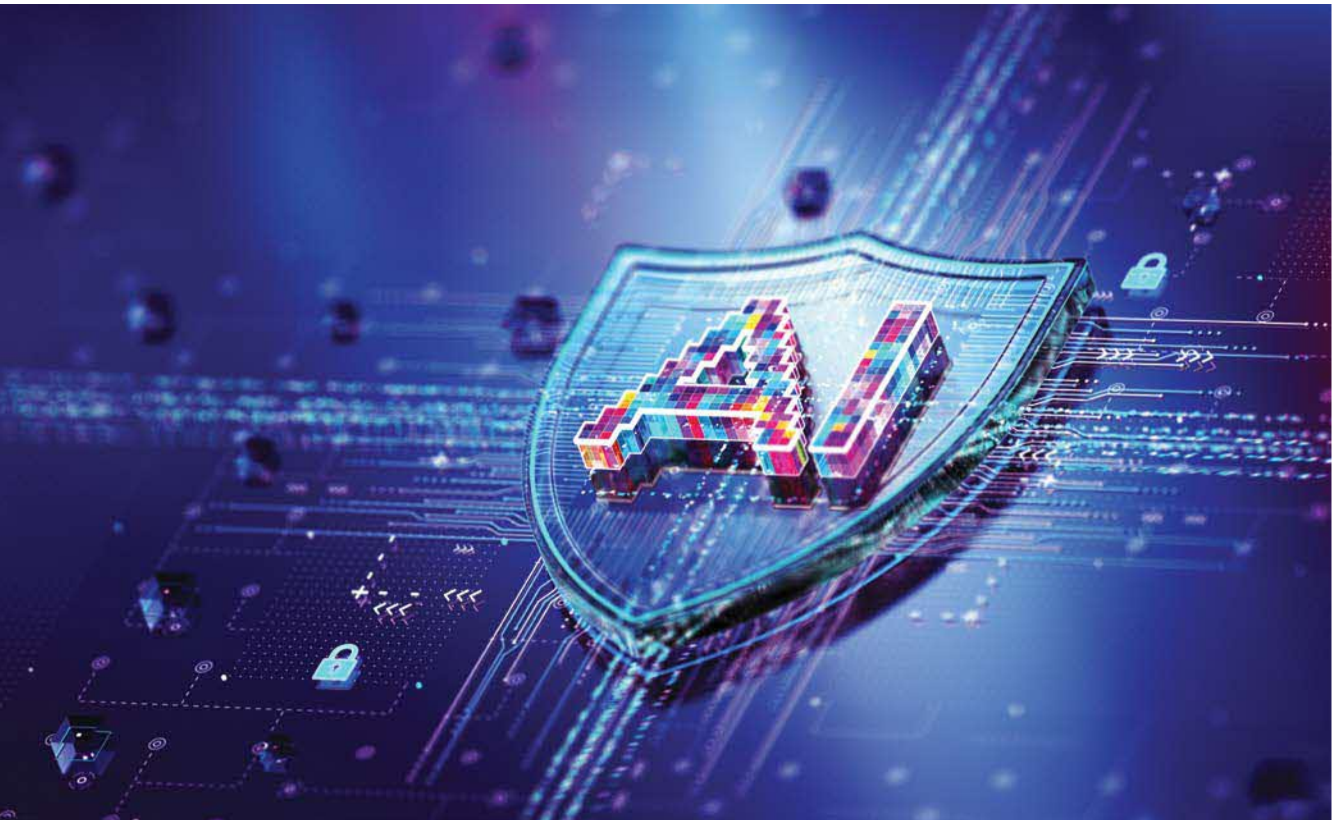
- Dragos’ incident response for its clients has revealed that remote access granted to vendors continues to be an attack vector targeted by threat groups. Ensure that all vendor remote access to your organisation’s systems are accounted for, kept to the minimum privilege necessary, and hardened.

#5 Risk-Based Vulnerability Management

- Understand the cyber digital controls in place and device operating conditions to make risk-based vulnerability management decisions regarding your OT environment.

- When vulnerabilities in OT are discovered to be actively exploitable, remotely exploitable and impact ICS processes (such as loss of view and/or control) or allow for new access to ICS, these are the most critical, high impact vulnerabilities to tackle first.

Artificial Intelligence (AI) in Cybersecurity - More Boon Than Bane

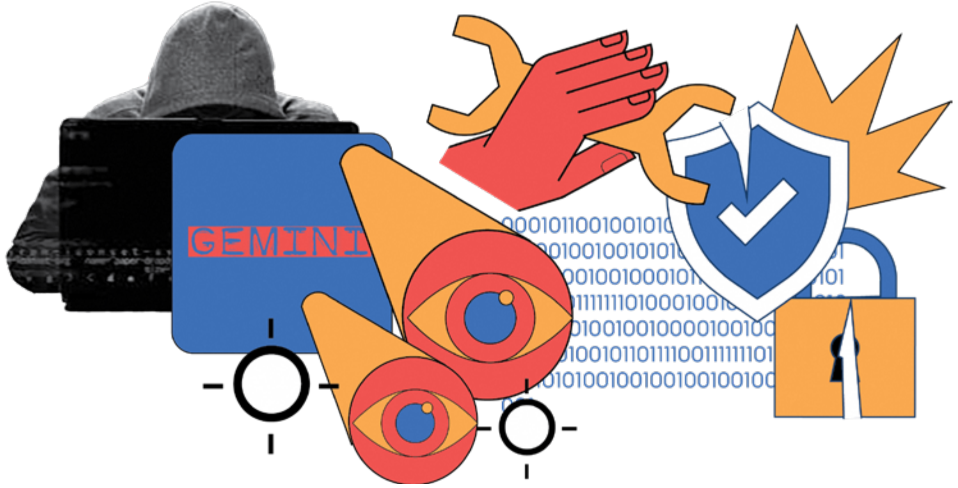


Contribution by **Google Threat Intelligence Group (GTIG)**

AI's transformative potential in cybersecurity is marked by its dual nature: it presents opportunities for enhanced defence while simultaneously creating possibilities to enhance malicious exploitation.

The Two Sides of the Coin: How Adversaries and Defenders Use AI

The AI boom has enabled significant productivity gains in cybersecurity on both sides of the battle. In our blog, "Adversarial Misuse of Generative AI", Google Threat Intelligence Group (GTIG) shared how threat actors are using the Gemini web application to support malicious activities such as hacking and information operations. These various activities seemingly elucidate the Defender's Dilemma - defenders must protect against all possible attacks, while attackers only need to find one vulnerability. While AI can be a useful tool for threat actors, it is not yet the game-changer it is sometimes portrayed to be, and is likely to tip the scales in favour of defenders.



How Adversaries Use AI

- **Enabling Operations:** Threat actors experiment with Gemini to enable their operations, which allows them to find productivity gains, but not yet to develop novel capabilities. Currently, they primarily use AI for research, troubleshooting code, and creating and localising content.

- **Supporting Attack Lifecycle Phases:** Advanced persistent threat (APT) actors used Gemini to support several phases of the attack lifecycle. These phases include researching potential infrastructure and free hosting providers, reconnaissance on target organisations, research into vulnerabilities, payload development, and assistance with malicious scripting and evasion techniques.

- **Content Generation and Translation:** Information Operations (IO) actors used Gemini for research; content generation, including developing personas and messaging; translation and localisation; and finding ways to increase their reach.

- **Experimentation:** In general, the GTIG found that threat actors carried out low-effort experimentation by using publicly available jailbreak prompts in unsuccessful attempts to bypass Gemini's safety controls.

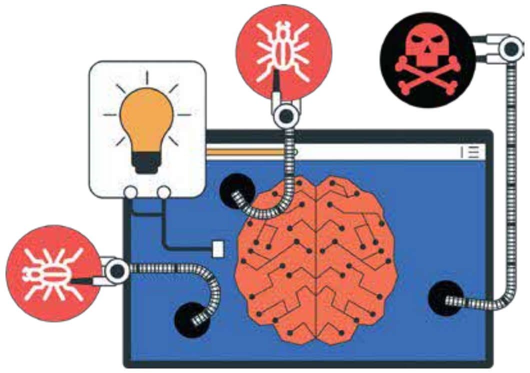
Limitations and Restrictions

- **Safety Measures:** Gemini's safety and security measures restricted content that would enhance adversary capabilities, as observed in GTIG's dataset.

- **Unsuccessful Attempts:** Threat actors attempted unsuccessfully to use Gemini to enable abuse of Google products, including researching techniques for Gmail phishing, stealing data, coding a Chrome infostealer, and bypassing Google's account verification methods.

- **No AI-Specific Threats:** GTIG did not observe any original or persistent attempts by threat actors to use prompt attacks or other AI-specific threats. Instead, threat actors used more basic measures, such as rephrasing a prompt or sending the same prompt multiple times; these attempts were unsuccessful.

GTIG anticipates that the threat landscape will evolve as threat actors adopt new AI technologies in their operations, because the AI landscape is in constant flux, with new AI models and agentic systems emerging daily.



How Defenders Can Use AI

AI offers significant potential to bolster digital security and provide a solution to the Defender's Dilemma. The digital landscape is becoming increasingly complex, and AI can be leveraged to manage this complexity and empower all users of digital technology to become effective defenders.

AI can be utilised to automate threat detection and response, identify and mitigate vulnerabilities, and provide real-time analysis of security threats. By automating these tasks, AI can help to reduce the workload on human security analysts and allow them to focus on more strategic tasks. Additionally, AI can be used to develop more sophisticated security tools and techniques that can help to improve the overall security posture of organisations.

Furthermore, AI can be used to educate and train users of digital technology on how to identify and avoid security threats. By providing users with personalised and adaptive training, AI can help to raise awareness of security risks and empower users to become more competent defenders.

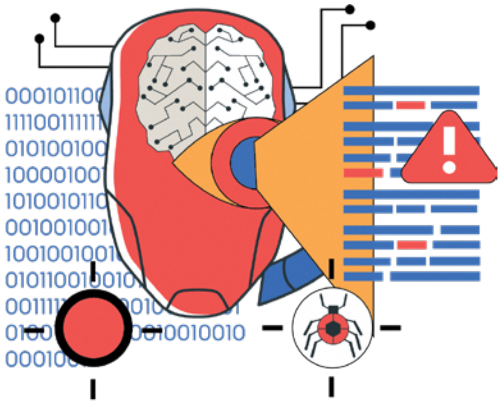
Overall, AI has the potential to revolutionise the field of digital security and provide a much-needed solution to the Defender's Dilemma. By leveraging the power of AI, organisations can improve their security posture, reduce the workload on human security analysts, and empower all users of digital technology to become effective defenders.

AI Capabilities

- **Reasoning:** AI can rapidly analyse information, draw logical conclusions, and make decisions.
- **Scale:** AI uniquely handles diverse data at scale, quickly and autonomously analysing, sorting, and making sense of data sets far larger than any human could handle.
- **Learning:** Machine learning enables an AI system to improve its performance on a given task without being explicitly programmed for every specific scenario.
- **Speed:** AI systems operate at machine speed, which allows them to quickly evolve defenses, apply patches, and detect attacks faster.

AI Cybersecurity Use Cases

- **Classification:** AI can classify malware, identify security vulnerabilities in code, and categorise and prioritise threats.
- **Generation:** AI can generate queries from natural language and create detection rules.
- **Summarisation:** AI can concisely explain the behaviour of suspicious scripts and summarise relevant and actionable threat intelligence and reports.



Roadmap to Digital Security

- **Abstracting Away Complexity:** AI systems can evaluate, generate insights, and make decisions about very large datasets and action spaces. First and foremost, this will help humans understand, and then optimise, the software they are building and the networks they are tasked with defending.
- **Vulnerability Discovery:** AI-powered vulnerability discovery could help in a similar way to the public disclosure of vulnerabilities, on a vast scale. Embedding this technology within build systems can drive not just exploit mitigation but prevention of entire classes of bugs.
- **Scaling Security Expertise:** AI has the potential to relieve the burden on end users and make organisations more capable in cyber defense.

AI-Powered Digital Immune System

- **Vulnerability Discovery Systems:** These systems learn from attacker trends, driving discovery of new vulnerabilities and misconfigurations.
- **Code and Configuration Safety:** Continuous Integration/ Continuous Delivery (CI/CD) systems learn from new vulnerabilities and misconfigurations, and update secure coding and deployment guardrails for developers and administrators.
- **Secure Code Generation:** AI can propose new code and secure-by-default configurations to patch weaknesses.
- **Automated Updates:** AI can test and deploy new patches and configuration changes.
- **Detection and Incident Response:** Systems can learn from baseline endpoint telemetry and user behaviour to detect threats in the environment, summarise alerts and incidents for analysts, and propose remediation steps.
- **Continuous Monitoring:** AI can continuously monitor system performance and controls posture and make recommendations.

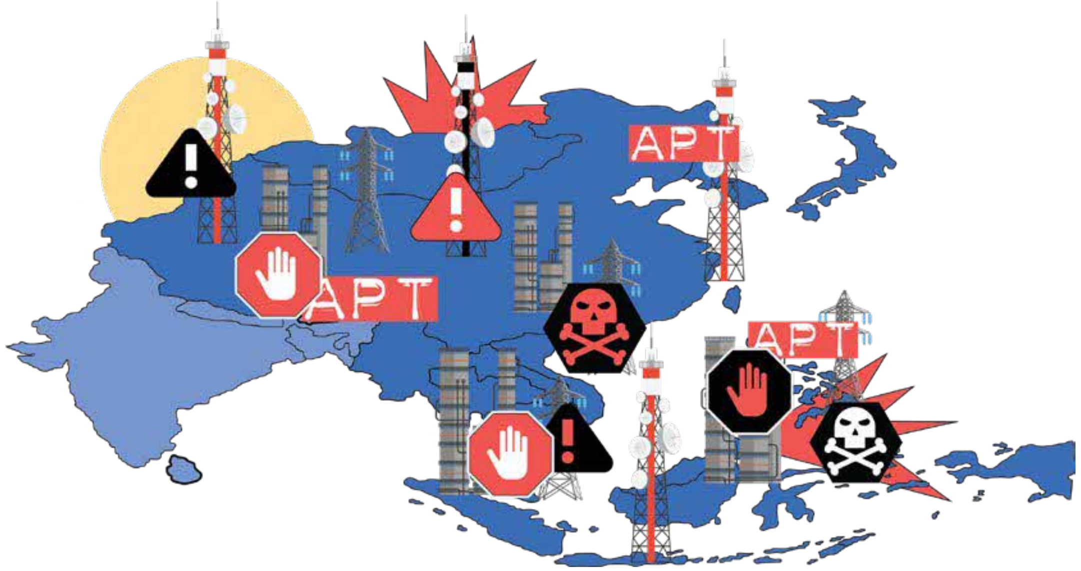
Recommendations

- **Secure AI From the Ground Up:** Prioritise the holistic security and resilience of AI systems. Apply secure-by-design principles throughout the AI lifecycle.
- **Empower Defenders Over Attackers:** Ensure AI governance does not hinder defenders. Preserve the ability to train models on publicly available data. Share and collaborate on security training datasets.
- **Advance Research Cooperation:** Focus on fundamental advancements in protecting AI systems and using AI to protect classic systems. Pursue research in system safety in design and build and system safety in use.

Conclusion

AI's role in cybersecurity is complex and multifaceted. While it empowers adversaries by streamlining operations and enhancing existing capabilities, it offers even greater potential for defenders to manage complexity, automate defenses, and scale security expertise. To realise this potential, stakeholders must prioritise security, collaboration, and research to ensure that AI serves as a force multiplier for cybersecurity.

2024 Threats to Southeast Asia



Contribution by **Recorded Future's Insikt Group**

Advanced Persistent Threat (APT) Activity in Southeast Asia

APT activity in Southeast Asia has primarily targeted government and critical infrastructure, especially telecommunications, likely with the goal of conducting espionage. State-sponsored groups have focused on targeting network edge devices and using relay networks to blend in with existing network traffic to limit detection and complicate attribution.

***RedDelta*:** Throughout 2024, *RedDelta* (*Mustang Panda*) conducted spear phishing attacks targeting government entities in Myanmar and the Vietnamese Ministry of Public Security. The group compromised the Vietnamese Communist Party in November 2024. After gaining initial access through spear phishing lures with political and diplomatic themes, the group ultimately dropped a dynamic-linked library (DLL) search order hijacking triad that delivered the group's customised *PlugX* backdoor.[1] In January 2025, US and international law enforcement took action to remove *PlugX* from thousands of infected devices.

***TAG-43*:** Insikt Group attributed the compromise of the Association of Southeast Asian Nations (ASEAN) and Cambodian government organisations, non-government organisations (NGOs), and a media outlet to a *TAG-43* campaign that started in October 2023 and continued through January 2024. Victims included a Cambodian political party and a nonprofit democracy-focused organisation, with the attacks taking place shortly before the February 2024 Senate elections. *TAG-43* compromised edge devices, including Fortinet FortiGate firewall devices, routers, and network administration devices to carry out the intrusion.

[1] A DLL search order hijacking triad consists of a legitimate susceptible binary, a malicious DLL loader, and an encrypted payload (*PlugX* in this instance).

***RedJuliett*:** *RedJuliett* (*Flax Typhoon*) compromised a government organisation in Laos and conducted reconnaissance activity against two government organisations in the Philippines and a Malaysian airline. The group also targeted perimeter devices to gain access to victim networks.

***RedGolf*:** In April and May 2024, *RedGolf* (*APT41*) compromised a mail server linked to an Indonesian telecommunications company and a web server belonging to the Municipal Government of Hanoi. The group used its *KEYPLUG* custom backdoor and the open-source offensive security tool *Sliver.*

Target Focus: Telecommunications

In 2024, a massive intrusion into US telecommunications networks was made public, impacting at least nine companies, including court-authorised wiretap systems. According to a statement from the US Cybersecurity and Infrastructure Security Agency (CISA), these breaches allowed the threat actors to compromise private communications between a small number of primarily government and political targets, and represent a significant breach of US national security infrastructure. A few months prior to the discovery of the US breach, a major regional telecommunications company was compromised in what sources close to the incident described to Bloomberg news as a "test run" for the attacks on the US. According to analysis from Tenable, *Salt Typhoon* employed at least five Common Vulnerabilities and Exposures (CVEs) to carry out these attacks. While it is unclear if *Salt Typhoon* carried these out as zero-days, the group benefitted from inconsistent vulnerability patching, as scanning data revealed over 91% of devices remain vulnerable to the ProxyLogon vulnerability exploited by this group.

Notable Attack Vectors and Tools

APTs across Southeast Asia were observed using similar tools and attack vectors that facilitate low-impact and long-term operations. Most notably, the revelations from the i-Soon leaks in February 2024 confirmed long-suspected hypotheses about shared tooling and infrastructure across multiple state-sponsored APT groups. Understanding where common infrastructure exists can help defenders track suspicious activity to find the source of the threat.

Tool Development and "Digital Quartermasters"

In February 2024, a trove of documents associated with Anxun Information Technology Co., Ltd., or i-Soon, exposed the inner workings of private sector cybersecurity companies contracted to conduct offensive operations on behalf of state-sponsored group(s). i-Soon was revealed to support and maintain the development of custom tools, including *ShadowPad* and *Winnti* malware. i-Soon is linked to a variety of espionage-focused cyber-attacks, including against government organisations in Vietnam, Thailand, Myanmar, Malaysia, and Cambodia. Despite the exposure, the threat actor groups associated with i-Soon, which include *RedHotel*, *RedAlpha*, and *POISON CARP*, continued operations throughout 2024.

The leaks revealed that i-Soon had obtained call data records from compromised telecommunications companies, indicating a possible motivation for the frequent targeting of these companies by state-sponsored

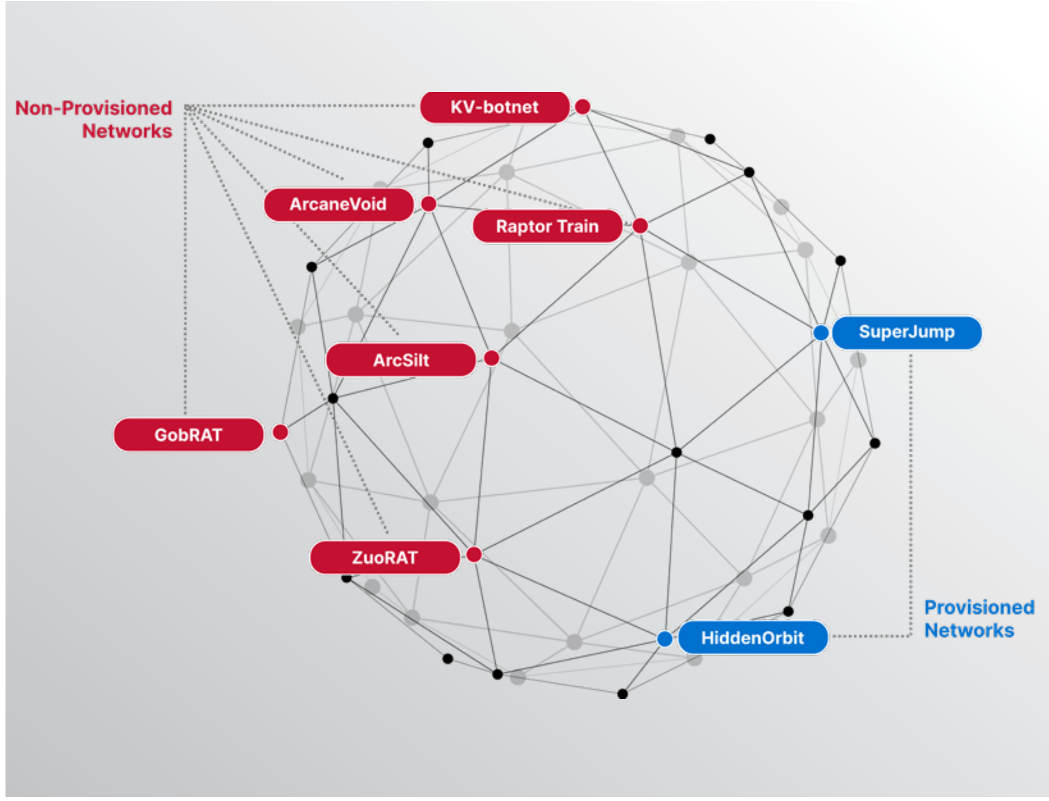


Figure 1: Provisioned vs. Non-Provisioned Anonymisation Networks (Source: Recorded Future)

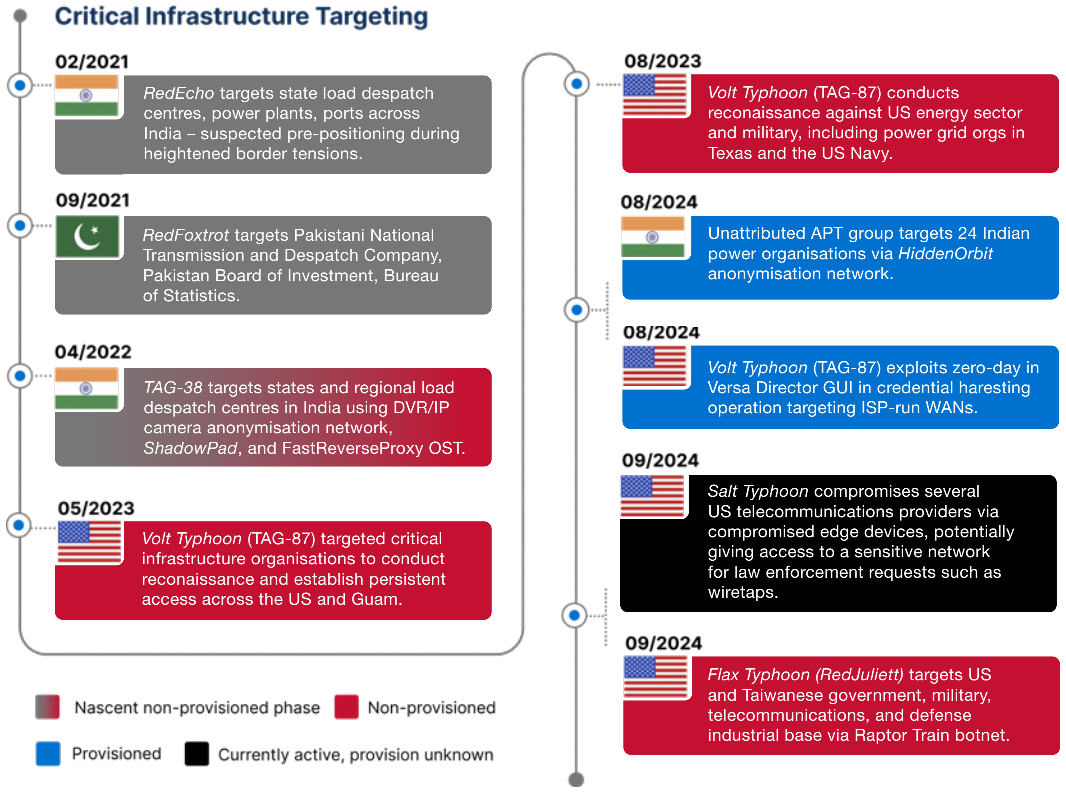
actors throughout 2024. Call data records could enable tracking of a target's pattern of life or communications. While *Salt Typhoon* and *Volt Typhoon*, which were attributed to the telecommunications hacks described above, are not directly linked to i-Soon, the contractor arrangement is likely replicated across multiple state-sponsored threat actor groups and private companies who support tooling, infrastructure, and operations.

Zero-day Exploits on Edge Devices

Since 2021, over 90% of known zero-day vulnerabilities exploited by state-sponsored APT groups have been in public-facing appliances such as firewalls, enterprise virtual private networks (VPNs), hypervisors, load balancers, and email security gateways. Groups target vulnerabilities in internet-facing devices because these edge devices have limited visibility and security solutions available, and targeting them has proven to be an effective way to scale initial access.

Private Relay Networks

Multiple state-sponsored threat actor groups have used relay networks for malicious activity for many years, including to target critical infrastructure. Research has uncovered two types of relay networks: provisioned networks composed of actor-provisioned virtual private server (VPS) infrastructure and non-provisioned networks built from compromised internet-of-things (IoT) devices, including small office/home office (SOHO) routers. According to CISA, these devices are typically compromised via known or zero-day vulnerabilities. Threat actors use malware running on the compromised devices to perform various functionalities that allow them to form part of the network, such as sending information about the infected devices to a command and control (C&C) node, as well as proxy and tunnelling functionality. SuperJump, a provisioned network consisting of several hundred VPS provisioned from a range of hosting providers and a small number of compromised pfSense devices, is one of at least eight identified relay networks that are used to obfuscate malicious activity and hinder attribution and tracking efforts.


Critical Infrastructure Targeting

02/2021
RedEcho targets state load despatch centres, power plants, ports across India – suspected pre-positioning during heightened border tensions.

09/2021
RedFoxtrot targets Pakistani National Transmission and Despatch Company, Pakistan Board of Investment, Bureau of Statistics.

04/2022
TAG-38 targets states and regional load despatch centres in India using DVR/IP camera anonymisation network, *ShadowPad*, and FastReverseProxy OST.

05/2023
Volt Typhoon (TAG-87) targeted critical infrastructure organisations to conduct reconaissance and establish persistent access across the US and Guam.

08/2023
Volt Typhoon (TAG-87) conducts reconaissance against US energy sector and military, including power grid orgs in Texas and the US Navy.

08/2024
Unattributed APT group targets 24 Indian power organisations via *HiddenOrbit* anonymisation network.

08/2024
Volt Typhoon (TAG-87) exploits zero-day in Versa Director GUI in credential haresting operation targeting ISP-run WANs.

09/2024
Salt Typhoon compromises several US telecommunications providers via compromised edge devices, potentially giving access to a sensitive network for law enforcement requests such as wiretaps.

09/2024
Flax Typhoon (RedJuliett) targets US and Taiwanese government, military, telecommunications, and defense industrial base via Raptor Train botnet.

▨ Nascent non-provisioned phase
🟥 Non-provisioned
🟦 Provisioned
⬛ Currently active, provision unknown

Figure 2: Relay networks used in critical infrastructure targeting (2021-2024) (Source: Recorded Future)

Throughout April and May 2024, Insikt Group observed multiple state-sponsored threat actor groups using the "SuperJump" relay network to target Southeast Asia. Via SuperJump, *RedLima* (*APT15*, *Ke3chang*) probed a "Secured Instant Messaging" service for the Philippines Department of National Defense. Additionally, Insikt Group observed suspected browsing activity via SuperJump of military, government, and human rights organisations in the Philippines, Malaysian defence and maritime agencies, and the Indonesian Navy by an unknown actor.

Outlook

Despite exposure from security researchers and government entities alike, state-sponsored activity in Southeast Asia has persisted with minimal operational disruption. Geopolitical developments, including either diplomatic initiatives or increased military activity, could accelerate and further embolden cyber operations. We recommend organisations prioritise patching in edge devices and replace any devices that have reached end-of-life. Finally, monitoring reconnaissance activity from known state-sponsored relay networks can help anticipate targeting for further attacks.

THE CYBERSECURITY SITUATION IN SINGAPORE

In this chapter, we look at the key trends and observations related to four major categories of malicious cyber activity within Singapore's cyberspace in 2024. Our local cyber threat landscape largely mirrored global developments, with an uptrend in all categories except for website defacements. Notably, there was a 49% increase in reported phishing attempts locally to around 6,100 cases last year, with Banking and Financial Services remaining as the most spoofed industry. Ransomware attacks continued to be a concern, with reported cases increasing by 21% to 159 cases in 2024. There was a significant 67% increase in infected infrastructure last year, totalling around 117,300 systems. This was primarily attributed to an increase in botnet drones. Many of these were compromised through months-old or even years-old vulnerabilities, underscoring the importance of good cyber hygiene and timely patching. This chapter also features a deep-dive by our partner, CrowdStrike, into the increasingly used cybercrime tactic of vishing (i.e. telephone-oriented social engineering campaigns), an article by our partner Ensign InfoSecurity on securing hypervisors (i.e. software managing virtual machines and hardware resources), and a look at our counterparts in the Singapore Police Force's (SPF) efforts in combatting cybercrime locally.

INTERVIEW WITH CSA'S FORMER DEPUTY CHIEF EXECUTIVE (NATIONAL CYBER RESILIENCE) NG HOO MING

How Has Singapore's Cybersecurity Grown Since the Formation of CSA in 2015?

1. Why do you think there was a need to form CSA?

Cybersecurity came to the forefront in Singapore's digitalisation journey, as we embarked on building a Smart Nation in 2014 to leverage technology to improve the lives of Singaporeans. Increased digitalisation and increased connectivity meant that there were more cyber threats to be addressed, meaning an increased impetus to create and maintain a resilient and trusted cyberspace.

In light of this, the government saw the need to establish a centralised national cybersecurity agency to ensure a coordinated and holistic response. That was why CSA was established in 2015 under the aegis of the Prime Minister's Office (PMO). Prior to this, cybersecurity efforts were distributed across multiple government agencies. For instance, I was then the Director of the Singapore Infocomm Technology Security Authority (SITSA). My primary focus at that point was on securing critical infrastructure, while other areas such as cybersecurity policy, industry development and international engagements were driven by other agencies.

2. In your opinion, how far has CSA come since its establishment in 2015?

Since its inception in 2015, CSA has made remarkable strides. As I shared earlier, cybersecurity efforts in Singapore were initially decentralised across various government agencies. With CSA's establishment under the PMO, we were given the mandate and the authority to unify these efforts, and that has been transformative.

Today, CSA stands as a benchmark for other countries in establishing a national cybersecurity agency – we have developed a comprehensive national cybersecurity strategy and implemented the Cybersecurity Act to ensure our Critical Information Infrastructure (CII) are well protected. Moreover, CSA's proactive collaboration with both local and international partners has helped Singapore gain recognition as a thought leader in cybersecurity. While there remains more work to be done in face of evolving threats, CSA's journey so far reflects a significant and commendable evolution in securing our cyberspace.

3. As the former DCE in charge of Operations, what was a significant local cybersecurity incident you recalled and how has CSA's role evolved?

One major cybersecurity incident I can think of that affected our CII organisations (CIIOs) was the SingHealth data breach in 2018. In this incident, CSA's role as the national cybersecurity agency was one of swift coordination and provision of technical expertise. The SingHealth breach involved the theft of Personal Identifiable Information (PII) of over 1.5 million patients. CSA worked alongside SingHealth, law enforcement, and other government agencies to quickly assess the situation, contain the threat, and subsequently derive important lessons that would enhance our overall cybersecurity framework. CSA's role in dealing with the SingHealth breach, as well as in other incidents such as the SolarWinds and Log4j vulnerability disclosures, are a testament to the leading role that we have come to play in Singapore's cyber landscape.

4. End users and consumers are usually most impacted by cyber incidents, but the design and implementation of cybersecurity in products have not always been intuitive. How has CSA adopted human-centric approaches towards digitalisation and protection of consumers over the past 10 years?

CSA's mission is to secure Singapore's digital infrastructure while safeguarding the interests of every citizen. We are only as strong as the weakest link, so it's important for organisations and the general public to be more diligent about protecting their digital way of life to improve our collective safety in cyberspace. In this regard, CSA launched the Safer Cyberspace Masterplan, which outlined a blueprint for a safer and more secure cyberspace in Singapore. It comprises three strategic pillars: (i) secure our core digital infrastructure, (ii) safeguard our cyberspace activities, and (iii) empower our cyber savvy population.

CSA also led initiatives that encourage enterprises to adopt a protection of consumers by design mindset. One such initiative is the Internet Hygiene Portal (IHP), which serves as a one-stop platform for enterprises to adopt internet security best practices. The IHP uses non-intrusive internet health lookup tools to assess the internet security of websites, email services and domain configurations, and then provides actionable suggestions on how enterprises can adopt best practices to improve their overall internet security. Through this, enterprises can learn practical ways to safeguard their domains, websites as well as email servers and, by extension, their customers' data.

Another initiative is the Cybersecurity Labelling Scheme (CLS), which aims to enhance the security of internet of things (IoT) and elevate overall cyber hygiene. The CLS helps consumers by making the cybersecurity provisions of IoT devices transparent and enabling consumers to identify poorly secured devices. It also helps developers and manufacturers differentiate themselves in the market, thereby encouraging the production of more secure IoT devices.

5. In the area of cybersecurity thought leadership, are you able to share some of CSA's achievements?

Singapore's strategic position as a global financial and digital hub means that our cybersecurity policies and practices resonate well beyond our national boundaries. In the first year of CSA's formation, the International Telecommunication Union (ITU) ranked Singapore as number one in its annual

Global Cybersecurity Index.[1] I see this as an endorsement of what different government agencies can achieve together when united under one entity.

At the regional level, CSA actively participates in forums such as the ASEAN Network Security Action Council (ANSAC) to promote better cooperation amongst the national computer emergency response teams (CERT) in ASEAN.[2] In 2016, Singapore led the region to establish the ASEAN Ministerial Conference on Cybersecurity (AMCC) to discuss cybersecurity issues at the ministerial and senior official level. Both the AMCC and ASEAN CERT Incident Drill (ACID) continue to be organised during the annual Singapore International Cyber Week (SICW).[3] This is a testament to CSA's commitment to regional capacity-building, particularly in strengthening the region's cybersecurity incident response network.

At the international level, CSA coordinates and develops a whole-of-government approach to support Singapore's participation in the United Nations (UN) international cyber policy discussions under the First Committee (1C), amongst others. Singapore has also had the opportunity to be nominated Chairman of the five-year UN Open-ended Working Group on Security of and in the use of ICTs. Through these engagements, CSA shares insights, learn from global best practices, and help shape international cybersecurity norms to enhance responsible state behaviour in cyberspace.

6. How do you see the local cybersecurity landscape evolving?

In this new and unpredictable era, cyber threats will continue to evolve and become more challenging while threat actors' tactics and techniques increase in sophistication. Despite this, digital transformation will continue being a key driving force in the adoption of new technologies, and some of these new technologies include the shift towards cloud computing and automation through artificial intelligence.

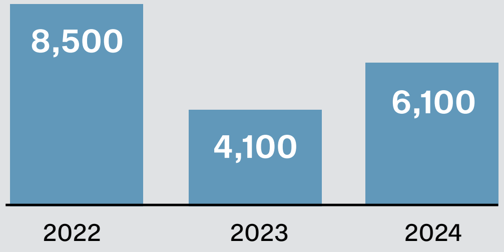
These new technologies will invariably expose both consumers and enterprises to new types of cyber risks. The interdependencies between organisations, their vendors, and third-party suppliers means an incident to one will usually impact the other. Enterprises embarking on digitalisation efforts should consider cybersecurity from a whole ecosystem perspective, including their customers and business partners. This might include implementing security by design when developing solutions or applications to protect the critical data of customers. Enterprises can also consider getting certified with Cyber Essentials and Cyber Trust mark, which will demonstrate their commitment to cybersecurity and enhance trust with customers and partners in their ecosystem. With this as a backdrop, I am confident that CSA will continue its mission to keep Singapore's cyberspace safe and secure, and protect Singapore's digital way of life.

1. The ITU is a specialised agency of the UN responsible for many matters related to information and communication technologies. Its Global Cybersecurity Index measures the commitment of countries to cybersecurity at a global level, to raise awareness of the importance and different dimensions of the issue. Each country's level of development or engagement is assessed along the following five pillars – (i) Legal Measures, (ii) Technical Measures, (iii) Organisational Measures, (iv) Capacity Development, and (v) Cooperation.
2. The ANSAC was established in 2011 under the first five-year ASEAN ICT Masterplan.
3. ACID was launched in 2006 to strengthen cybersecurity preparedness and cooperation among national CERTs. It is organised by CSA's SingCERT.

State of Singapore's Cyberspace

Phishing Attempts

6,100 cases | ▲49% from 2023



Number of phishing attempts reported to CSA

Around 6,100 phishing attempts were reported to CSA in 2024, a 49% increase as compared to 2023 (4,100 attempts). While this was a 28% decrease from the 8,500 cases observed in 2022, the number of phishing cases remained high. Additionally, this number was possibly just a fraction of phishing attempts in Singapore, with majority of phishing attempts being unreported unless there were financial losses involved. CSA's sampling of phishing emails from reported cases found that 12% contained AI-generated content.[1] This suggests continued nascent adversarial exploitation of artifical intelligence (AI) to facilitate phishing, albeit a slight dip from 2023 (13%).

Most spoofed industries

1. Banking and Financial Services
2. Government
3. E-commerce

Globally, the number of phishing attempts increased sharply in 2024.[2] This was likely assisted by the continued exploitation of established generative AI chatbots such as ChatGPT, along with advancements in malware obfuscation techniques to evade detection by antivirus software. Researchers reported that AI-generated phishing emails have become so well-crafted that these emails are increasingly successful at

1. 60 phishing email samples (i.e. around 1% of the reported phishing attempts in 2024) were selected for the testing. Selected samples were all written in English, and in a legible manner. To reduce selection bias, samples that contained common signs of phishing, such as spelling errors or poor grammar, were also included. Only the email subject and relevant content within the emails were analysed as part of the testing.
2. SlashNext's *The State of Phishing 2024* reported a 341% increase in malicious emails.

convincing their recipients to click on the embedded phishing link or execute the attached malware.

Characteristics of Reported Phishing Links

In 2024, CSA observed a continuing trend of threat actors refining their techniques, to make their phishing messages more legitimate and authentic looking.

URL Protocols

In 2024, 69% of phishing websites reported to CSA were served via the HTTPS protocol, marking a rise from the previous year, where just more than 50% of reported phishing websites were served via HTTPS. Correspondingly, the proportion of phishing websites served via the HTTP protocol decreased from 26% in 2023 to 15% in 2024. This reflects the trend where threat actors use HTTPS to add legitimacy and credibility to phishing URLs, as the encrypted HTTPS protocol is generally regarded as more secure than the unencrypted HTTP. Users are therefore encouraged to be vigilant when clicking on any links and to scrutinise the content of the message rather than the form.

Top-level Domains (TLD)

Similar to 2023, the ".com" TLD remained the most prevalent amongst phishing links in 2024, with more than a third of reported phishing attempts using ".com" links. Significantly, the ".cn" TLD rose to second place in 2024, representing 23% of phishing links as compared to 0.32% in 2023.[3] The ".top" TLD rose in its usage in 2024, ranking third in prevalence with 373 reported phishing links as compared to 28 phishing links in 2023, a 13 times increase. On the other hand, the second most prevalent phishing TLD of 2023 – ".sbs" – fell to 29th place. This reflects the dynamic nature of phishing links and campaigns, as threat actors continue to evolve their tactics. The prevalent usage of the ".com" TLD and increase in usage of the ".cn" TLD suggest that threat actors consider these TLDs as more authentic looking. Additionally, the ".top" TLD is noted for its appeal of appearing credible – thereby enhancing the efficacy of attacks.[4]

URL Length

The average URL length increased slightly from 31 characters in 2023 to 37 characters in 2024. While URL length might not be a primary focus, threat actors could be increasingly leveraging generative AI to create URLs that are more obfuscated and more believable. Generative AI could assist threat actors in generating complex and seemingly random URLs, making attribution difficult and harder for spam filters and firewalls to flag out. Additionally, generative AI could assist threat actors in creating URLs that use realistic-looking subdomains, or domain names, including trusted-looking redirectors such as Google Translate and other tracking services. This would result in phishing URLs closely resembling legitimate ones, making them hard to distinguish as fraudulent. Overall, the use of generative AI may enable a shift in the threat actors' tactics. One possible application may be to enhance the pre-built templates used for malicious websites in phishing-as-a-service (PhaaS) kits.[5]

[3] Security vendor Duo Circle noted that ".cn" is one of the most targeted TLDs among cybercriminals. According to the Cybercrime Information Center, during the period of February to October 2024 alone, out of 26,593,444 domains registered in ".cn" TLD worldwide, 38,758 domains (0.16%) were associated with phishing scams.

[4] Cybersecurity researchers have pointed out that the ".top" TLD has been associated with most phishing campaigns and fake e-commerce platforms, and has been labelled as a 'high-risk TLD'.

[5] 'Phishing-as-a-service' is a subscription-based model where cybercriminals can access readily available tools and templates to launch phishing attacks with minimal technical expertise, effectively lowering the barrier to entry for them.

Most Spoofed Industries

The top three spoofed industries were banking and financial services (B&F) in first place, followed by government and e-commerce. While B&F and government have traditionally been among the top three most spoofed industries, this was the first time in three years (since the height of the COVID-19 pandemic) that e-commerce has entered the top three, replacing technology.

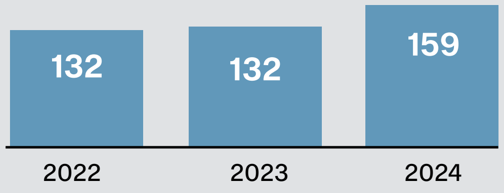
Banking and financial services (B&F) remained the most spoofed industry, with 56% of all phishing attempts observed to impersonate B&F organisations. Phishing attempts targeting B&F entities in Singapore remained highly concentrated on local banks, which accounted for 70% of all phishing incidents in 2024. This is consistent with phishing trends over the past few years. Common lures used by cybercriminals include impersonating internet banking portals and landing pages of banks.

Government accounted for approximately 8% of the phishing cases reported. The most commonly spoofed government agencies were the Ministry of Finance (MOF), Inland Revenue Authority of Singapore (IRAS), and Land Transport Authority (LTA). MOF saw a significant surge in phishing attempts in the months of January, July and December, with cybercriminals exploiting ongoing government support measures like SupportGoWhere and RedeemSG as lures to deceive victims.

E-commerce was the third most spoofed industry in 2024, accounting for 7% of the overall reported phishing attempts. Major platforms like Carousell and Amazon were the primary targets, with Amazon experiencing a noticeable spike in phishing activity in October, likely linked to popular seasonal shopping events. Typical lures for this industry included spoofing of well-known e-commerce platform websites and spoofing of e-commerce payments via email in order to harvest credit card and bank account details.

Ransomware

159 cases | ▲21% from 2023



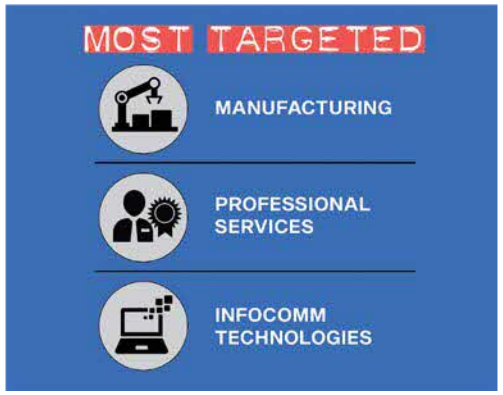
Number of ransomware cases reported to CSA

Ransomware groups targeting Singapore entities included *Akira*, *LockBit*, and *Phobos*.

Global Trends

The ransomware ecosystem has become more complex in 2024. Following law enforcement crackdown on some major ransomware groups, new groups and affiliates have emerged, adopting varied tactics such as targeting smaller markets, and demanding more modest ransoms. Some ransomware groups, such as *FunkSec*, have purportedly experimented with the use of AI to develop malware, indicative of their increasing interest in leveraging AI for nefarious purposes. An increasing number of hacktivists leveraged ransomware for destructive operations and financial gain, with some even purportedly launching ransomware-as-a-service (RaaS) operations to ensure long-term financial stability.[6] Two broad trends that emerged in 2024 were (i) a decrease in ransomware payments and (ii) a surge in initial access brokers (IABs) after a decline in 2023.[7] In 2024, ransomware groups collected approximately US$813.55 million in payments, a 35% decrease from 2023. Cybersecurity experts surmised that this was due to law enforcement taking down prominent ransomware groups, and more victims refusing to pay ransoms, despite the more modest ransom demands by newer groups.

The number of ransomware cases in Singapore rose, with a total of 159 local ransomware cases reported in 2024—an increase of 21% from 132 cases in 2023. This trend mirrored the global surge in ransomware incidents. The most impacted industries were manufacturing, professional services, and infocomm technologies (ICT). Notably, professional services ranked among the top three for the first time since CSA started tracking ransomware trends, highlighting the growing need for stronger cybersecurity in this industry.


MOST TARGETED

MANUFACTURING

PROFESSIONAL SERVICES

INFOCOMM TECHNOLOGIES

Top Affected

The manufacturing and professional services industries were the most affected by ransomware attacks in 2024, accounting for a combined subtotal of 63 cases, more than a third of the total.

The manufacturing industry experienced 35 ransomware attacks in 2024, with more than half targeting multinational corporations (MNCs) and listed firms. Although small and medium enterprises (SMEs) are often perceived as more vulnerable due to limited resources, the sizeable share of attacks on MNCs was particularly notable.

MNCs and large enterprises in the manufacturing industry are increasingly prime targets for cybercriminals due to their complex operations and extensive supply chains. Their handling of valuable intellectual property, proprietary designs, and sensitive data makes them especially appealing. The most impacted sub-industries — precision engineering and electronics engineering — highlight the sector's strategic importance. Although there has been a shift in overall ransomware trends, with some groups moving towards pure data extortion (without encryption), most attacks observed in the manufacturing sector by CSA still involved data encryption.[8] This remains a preferred tactic due to its devastating impact on operations, as it forces companies to prioritise recovery and increases the likelihood of ransom payments.

The professional services industry, encompassing businesses that provide specialised expertise and knowledge-based services – including architecture, engineering, consultancy, accounting, legal and advertising – experienced 28 ransomware attacks in 2024, with majority of the attacks targeting SMEs. This disproportionate targeting highlights the vulnerability of smaller professional service providers, particularly consulting and legal firms, which manage vast amounts of sensitive client data.

Prevalent Groups

In 2024, the top ransomware groups targeting Singapore enterprises were *Akira*, *LockBit*, and *Phobos*. Notably in 2024, a majority of *Phobos* victims in Singapore were impacted by the *Faust* ransomware variant, a trend CSA had been monitoring since December 2023. The proliferation of cracked *Phobos*/*Faust* ransomware versions on the dark web contributed to the group's expanding presence locally, suggesting that Singapore organisations were not being specifically targeted but rather victims of opportunistic attacks.

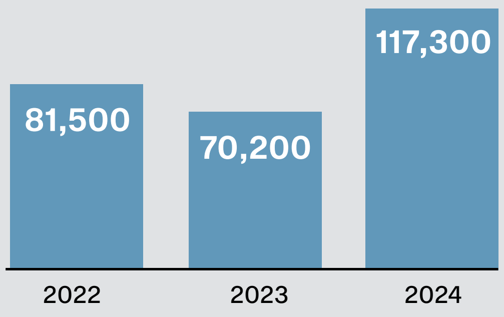
[6] Cybersecurity experts have suggested that adoption of ransomware into hacktivists' arsenal is a convergence of hacktivism and cybercrime.

[7] IABs are cybercriminals who specialise in selling access to compromised networks. They focus on gaining unauthorised access to corporate networks, often through phishing or exploiting vulnerabilities, and have become critical enablers for ransomware groups, allowing the groups to concentrate on the payload delivery and extortion phases. Cybersecurity vendor CrowdStrike noted in its *Global Threat Report 2025* that IAB activity surged in 2024, with advertised accesses increasing by nearly 50% over 2023.

[8] Pure data extortion is a type of attack, typically associated with ransomware groups, where threat actors exfiltrate sensitive data and demand a ransom for its non-disclosure, without encrypting the victims' files or systems.

Infected Infrastructure

117,300 systems | ▲67% from 2023



Number of infected systems observed by CSA

The number of infected systems observed in Singapore rose from around 70,200 in 2023 to 117,300 in 2024, marking a 67% increase. This surge was primarily attributed to a rise in infected botnet drones.[9] The increase could be linked to the continued exploitation of n-day or zero-day vulnerabilities in networking/edge and outdated internet of things (IoT) devices by threat actors, using them to bypass intrusion detection systems and maintain persistent access.[10] In their *2024 Malicious Infrastructure Report*, cybersecurity vendor Recorded Future observed that threat actors were creating botnets and associated infrastructure for malicious purposes by indiscriminately infecting IoT devices, including end-of-life or unpatched small office/home office (SOHO) routers, worldwide with malware.[11]

Top three observed malware associated with locally-hosted command-and-control (C&C) servers:

1. *Cobalt Strike*
2. *Noon*
3. *Sliver*

Top three observed malware in infected botnet drones:

1. *Android.vo1d*
2. *Avalanche – Andromeda*
3. *Sality*

[9] A botnet is a network of compromised devices including personal computers, business servers, mobile devices, and IoT devices like cameras and routers. It is often controlled remotely by an attacker and is used to perform malicious activities such as distributed denial-of-service (DDoS) attacks, data theft, or spam distribution.

[10] Zero-day vulnerabilities refer to previously unknown flaws without available patches or remediation, while N-day vulnerabilities refer to known flaws (i.e. known for N days) for which patches are available but not applied.

[11] In May 2024, Recorded Future identified a malware family that compromised thousands of end-of-life Cisco and ASUS routers, along with QNAP devices. They opined that Ubiquiti, Mercusys, Mikrotik and TP-Link routers were possibly targeted as well.

For the top malware associated with locally-hosted C&C servers, *Cobalt Strike* and *Noon* have maintained their positions as the top two threats since 2022. *Cobalt Strike* continued to be the most prevalent, appearing approximately six times more often than *Noon* and nearly seven times more frequently than *Sliver*.

In contrast, the top three observed malware in locally-hosted botnet drones exhibited a relatively even distribution in terms of prevalence. Dated malware strains dominated this category, with *Android.vo1d* (August 2024) being the sole exception. The oldest malware observed locally, *Sality*, has been around since 2003 while *Avalanche. Andromeda* has been around since 2011. Remediation measures for both malwares are readily available. This trend suggests widespread use of outdated, unpatched and undefended systems, leaving users vulnerable to exploitation.

Top Three Observed Malware Associated With Locally-Hosted C&C Servers:

Cobalt Strike

Mirroring global trends, *Cobalt Strike* remained the most observed malware family in locally-hosted C&C servers. Its continued prominence can be attributed to its versatility. Originally designed for penetration testing, it has been widely repurposed by an array of threat actors – state-sponsored threat actors, cybercriminals, and hacktivists – due to its comprehensive feature set. Ongoing development and the availability of cracked versions has fuelled its use across a variety of attack vectors.

Noon

Noon is a trojan spyware readily available in underground forums. It is distributed in malspam campaigns involving spam emails with product quote inquiry, shipping or delivery inquiries, fake invoice attachments and product order requests. Its versatility and affordability have made it highly prevalent, particularly in cybercriminal activities centred around credential theft and financial fraud by cybercriminals.

Sliver

Since its release in 2020, *Sliver* – C&C framework designed for adversary emulation and red team operations by organisations – has instead gained traction among state-sponsored threat actors and cybercriminals like IABs . Its open-source nature and cross-platform compatibility with OS X, Linux, and Windows made it an appealing alternative to *Cobalt Strike* and *Metasploit*. This is the first time *Sliver* has appeared in the top three malware associated with locally-hosted C&C servers.

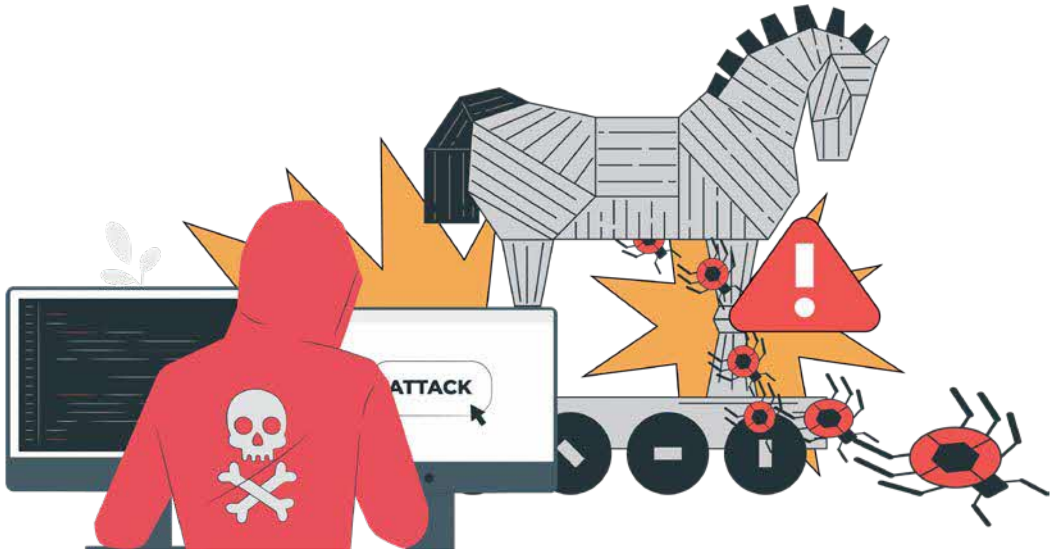
A Close Fourth: *PlugX,* though not ranked among the top three, held the position of the fourth most prevalent malware in this category. Given its association with state-sponsored threat actors, *PlugX* continues to be relevant today. Notably, the dismantling of a cybercriminal syndicate in Singapore in September 2024 brought public attention to the ongoing use of *PlugX* since it was first discovered in 2012.

Top Three Observed Malware in Locally-Hosted Botnet Drones:

Android.vo1d

This sophisticated malware, which targets Android-based TV boxes, emerged in August 2024 and quickly became one of the most prevalent global threats. In less than half a year, it infected approximately 1.3 million devices across 197 countries.[12] Cybercriminals use infected devices as proxy servers to hide the origin of their

[12] Pierluigi Paganini, "Vo1d Malware Infected 1.3 Million Android-Based TV Boxes in 197 Countries", Security Affairs, September 13, 2024, https://securityaffairs.com/168342/malware/vo1d-android-malware-tv-boxes.html.



malicious activities by blending in with seemingly innocuous residential network traffic. This also helps them bypass regional restrictions, security filtering, and other protections. *Android.vo1d* primarily exploits older, unsupported versions of Android, acting as a backdoor for additional malicious software. Its rapid spread and ability to target outdated IoT devices highlight the critical need for improved cybersecurity in the IoT sector. Local observations align with its global prevalence, underscoring *vo1d's* significant impact.

Avalanche-Andromeda

First discovered in 2011, *Avalanche-Andromeda* remained a resilient and adaptable botnet infrastructure. Despite a major takedown operation in December 2017, this modular trojan continued to evolve and remain active. The botnet's modular nature allows it to deliver targeted payloads, adapt to different systems, and spread efficiently. Remotely updatable modules help it avoid detection, while polymorphic components make identification harder. This flexibility enables persistent infections and the introduction of new exploits, ensuring its continued effectiveness across a wide range of systems and therefore appeal to cybercriminals as part of their arsenal. Cybercriminals used it as part of their monetisation schemes to steal passwords from online accounts of infected machines, or install additional malware on the infected machine.

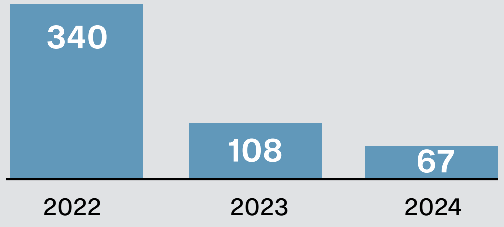
Sality

First discovered in 2003, *Sality* is a polymorphic malware family that continues to pose a significant threat to Windows systems worldwide. It infects executable files and spreads rapidly across networks and removable drives. *Sality's* persistence is largely due to its ability to evade detection and its robust peer-to-peer botnet infrastructure.[13] Its modular architecture also enables it to download additional malicious payloads, adapting to new attack vectors and expanding its capabilities. Cybercriminals have been observed to use *Sality* to steal victim's personal or financial data, send and receive spam emails, and perform computing tasks such as mining cryptocurrency or cracking passwords.

[13] *Sality's* polymorphic engine alters its code with each malware sample generated, making it adept at avoiding signature-based antivirus detection.

Website Defacements

67 websites | ▼38% from 2023



Number of defaced Singapore websites observed by CSA

Threat actors targeting websites with Singapore IP addresses include *kefiex404* and *xzourt*.

The number of website defacements in Singapore decreased from 108 (in 2023) to 67 (in 2024), a 38% decrease that continued the downward trend for website defacements since 2022. This decrease could have been caused by several factors, such as hacktivists opting to make themselves heard on other platforms (such as social media) or shifting methods (e.g. ransomware and DDoS attacks) to advance their agenda, and website owners having mitigated common cyber hygiene issues.

Globally, hacktivists continued to be driven by geopolitical conflicts ongoing in different parts of the world, such as the Russia-Ukraine and Israel-Hamas conflicts. In 2024, electoral processes and infrastructure in particular, were heavily targeted by hacktivists due to the sheer volume of elections taking place globally, with over 100 elections occurring in at least 64 countries.

Historically, websites built using WordPress were prime targets for hacktivists and malicious threat actors, who exploited vulnerabilities for web defacements.

However, a downward trend in such attacks has been ongoing since 2023, and can be attributed to WordPress's significant security improvements over time. Notably, the release of version 6.4.2 on 6 December 2023 introduced automatic updates and strengthened passphrase policies to reduce the risk of common exploits. The increasing adoption of web application firewalls (WAFs) further mitigated attack vectors like cross-site scripting (XSS) and Structured Query Language (SQL) injection.

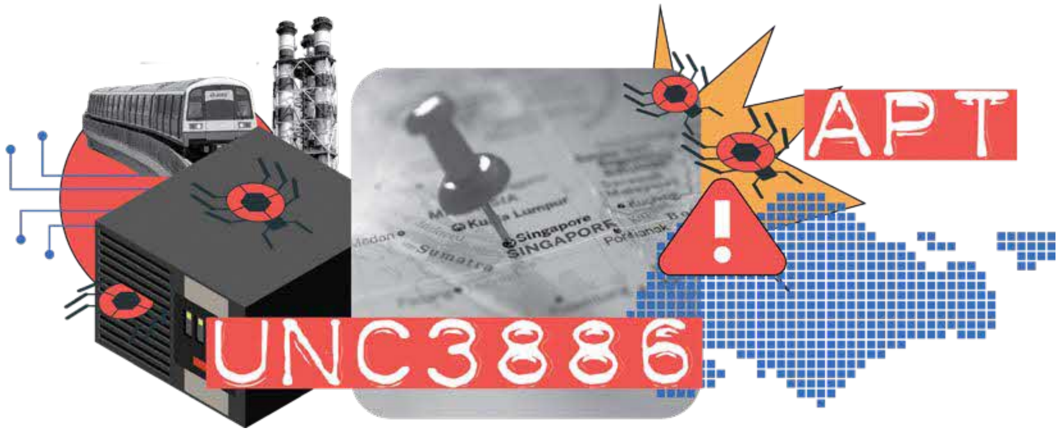
Affected Sites

As in previous years, the majority of the defaced websites belonged to SMEs that generally lacked robust cyber hygiene. Many of these sites were likely built on outdated platforms or used unpatched software, making them easy targets for opportunistic attacks.

Two notable threat actors, *kefiex404* and *xzourt*, emerged with significant activity. Both actors executed coordinated, high-volume defacement campaigns within a single day, suggesting an opportunistic shift towards more aggressive, attention-grabbing cyber operations. *kefiex404* primarily targeted multiple webpages belonging to a single SME, while *xzourt* focused on various unrelated websites. It appears that both actors exploited a vulnerable content management system (CMS), facilitating the mass defacement of these sites. These actors seemed to focus on exploiting specific website vulnerabilities. Their use of automated scripts enabled them to compromise a large number of sites, highlighting the effectiveness and scalability of this approach in executing website defacements.

The observed characteristics of these attacks underscore the importance of implementing robust cybersecurity measures. Regular software updates, comprehensive vulnerability assessments, and website defacement monitoring tools remain critical in mitigating potential risks, particularly for SMEs with limited cyber defence resources.

Advanced Persistent Threat (APT) Activity in Singapore



On 18 July 2025, Coordinating Minister for National Security (CMNS) K Shanmugam gave a speech at CSA's 10th anniversary dinner. A significant focus of his address was the grave and persistent threat posed by APTs in Singapore, with specific mention of APT group *UNC3886*, which was widely reported in local media. The following day, the lottery numbers for "3886" were sold out in Singapore, with CMNS Shanmugam himself sharing about this occurrence in a Facebook post. While this happening sparked widespread humour on social media, the threat posed by *UNC3886* remains a matter of grave concern.

What is *UNC3886*

UNC3886 has been active since at least late 2021, and demonstrates sophisticated tactics, techniques and procedures (TTPs), such as living off the land (LoTL) techniques and zero-day exploits. LoTL refer to techniques whereby the threat actors uses only tools available in the victim's systems. This reduces the attacker's footprint and makes detection of their activities more challenging. Zero-day exploits refer to the threat actor exploiting previously unknown vulnerabilities in systems or software, for which there are no immediate available patches.

An Increasing Cyber Threat and Its Implications on Singapore

CMNS Shanmugam highlighted that from 2021 to 2024, suspected APT attacks on Singapore surged more than four-fold. Among these, *UNC3886* has been identified as one of the APT groups targeting Singapore. Their intent is clear: to focus on high-value, strategic targets, including critical infrastructure that underpins essential services. If successful, such attacks could enable espionage and cause significant disruption to Singapore and its citizens.

Like many countries, Singapore is currently facing persistent and severe cyber threats from APT groups and other foreign actors, posing a substantial risk to national security due to the cascading effects of such attacks. For example, a cyber-attack on the power grid could disrupt electricity supply, which in turn would cripple other essential services such as water, transportation, and healthcare – any system reliant on power would be affected.

The economic repercussions would also be severe, as financial institutions, the airport, and various industries would face operational paralysis, leading to significant economic losses.

Such breaches would impact Singapore's business operations, including its vendors and supply chains, potentially eroding trust and confidence in the nation's systems. Ultimately, if businesses perceive Singapore's systems as unreliable or unsafe, it could deter investment and affect Singapore's overall standing globally.

> **"In four years, from 2021 to 2024, suspected APT attacks on Singapore increased more than four-fold."**
>
> **"*UNC3886* poses a serious threat to us, and has the potential to undermine our national security."**
>
> **Mr K Shanmugam**
> Coordinating Minister for National Security and Minister for Home Affairs

Conclusion

In the face of such threats, a vigilant and unified response is needed. CSA, together with partner agencies, will continue to improve coordinated responses to effectively respond to these threats. It is also crucial to:

1. **Strengthen the Protection of CIIs.** Sustained collaboration with CII owners is vital to ensure robust protection against emerging threats.
2. **Build Up Our Digital Ecosystem.** Recognising that cyber threats extend beyond CIIs to all companies, including vendors and suppliers, it is crucial to work with all stakeholders to bolster their cybersecurity posture.
3. **Improve Crisis Response Capabilities and Readiness.** Cybersecurity exercises, such as Exercise Cyber Star, involving government agencies and CII owners, play a critical role in preparing organisations for potential threats and improving response mechanisms.
4. **International Cooperation.** Continued engagement with the global community is necessary to address transnational cybersecurity issues and contribute to maintaining a secure, rules-based cyberspace for all counties.

The Business of Social Engineering

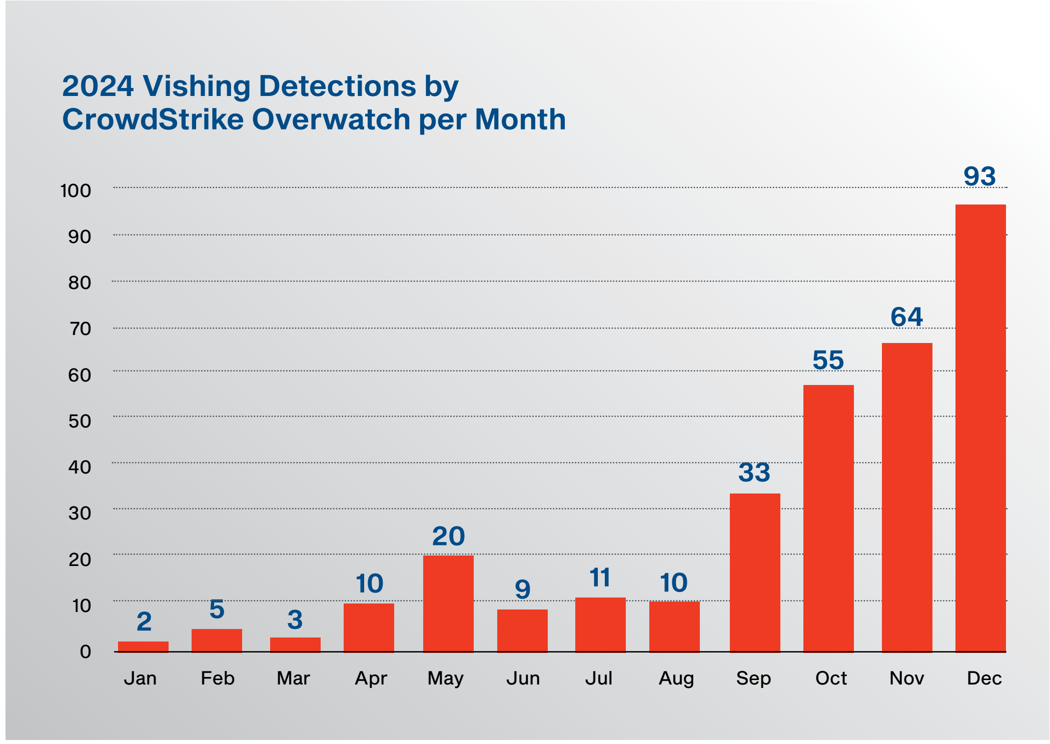
Contribution by **CrowdStrike**

Adversaries are bypassing traditional security measures by exploiting human weaknesses, leveraging stolen legitimate credentials and social engineering to gain access and move laterally within organisations. In 2024, CrowdStrike observed a surge in phone-oriented social engineering campaigns (vishing) and help-desk manipulation, signalling a significant evolution in eCrime tactics.

Vishing

Several eCrime adversaries incorporated vishing into their attack techniques in 2024, amounting to a 40% compounded monthly growth rate in observed vishing operations for the year. The latter half of 2024 saw a significant increase in the use of this tactic.

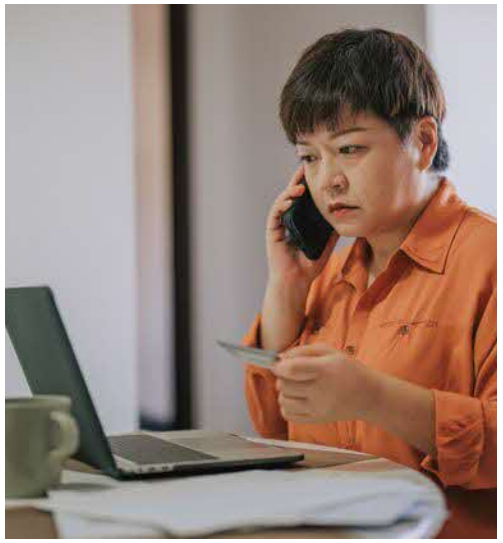
In vishing campaigns, threat actors call targeted users and attempt to persuade them to download malicious payloads, establish remote support sessions, or enter their credentials to adversary-in-the-middle (AITM) phishing pages. In most 2024 vishing campaigns, threat actors impersonated IT support staff, calling targeted users under the pretext of resolving connectivity or security issues.



Why Vishing is So Effective

Similar to other social engineering techniques, vishing is effective because it targets human weakness or error rather than a flaw in software or an operating system (OS). Malicious activity may not be detected until later in an intrusion, such as during malicious binary execution or hands-on-keyboard activity, which can delay an effective response.

This gives the threat actor an advantage and puts the onus on users to recognise potentially malicious behaviour.



Throughout 2024, CrowdStrike tracked at least six similar but likely distinct campaigns in which threat actors posing as IT staff called their targets and attempted to persuade them into establishing remote support sessions, often using Microsoft Quick Assist. In many cases, calls were made via Microsoft Teams from external tenants.

At least four of these campaigns leveraged spam bombing — sending thousands of spam emails to targeted users' email addresses — as a pretext for the vishing call. CrowdStrike observed a significant increase in these campaigns in the second half of 2024, detecting several relevant intrusions each day. eCrime group *CURLY SPIDER* is behind one of these campaigns, with relevant intrusions culminating in *Black Basta* ransomware deployment.

CASE STUDY

CURLY SPIDER's Social Engineering Attack

In 2024, *CURLY SPIDER* emerged as one of the fastest and most adaptive eCrime groups, executing high-speed, hands-on intrusions. In this case, the adversary attempted to achieve their objectives without even needing to break out to another device. The entire attack chain — from initial user interaction and social engineering to introducing a backdoor account to establish persistence — took under four minutes.

How *CURLY SPIDER* Operates

This adversary relies heavily on social engineering for initial access. In some cases, the following will occur:

- A user will receive a large volume of spam emails impersonating charities, newsletters, or financial offers.
- Shortly after, a caller posing as help desk or IT support claims the spam is caused by malware or outdated spam filters.
- The user is instructed to join a remote session using remote monitoring and management software, such as Microsoft Quick Assist or TeamViewer, with the attacker guiding them through the installation if the tool is not already present; in this case, the adversary chose Quick Assist to establish control.

CrowdStrike has seen these tactics directly support ransomware operations, and *CURLY SPIDER* frequently collaborates with *WANDERING SPIDER*, the group behind *Black Basta* ransomware. By combining high-tempo social engineering, legitimate remote tools, and cloud-hosted payloads, *CURLY SPIDER* exemplifies how modern adversaries bypass traditional defences.

Proactive Defence is Essential

The rise in social engineering approaches highlights the urgent need for stronger identity protection. It is difficult for a single security tool to distinguish between a legitimate employee and adversaries using stolen credentials, leaving organisations vulnerable to identity-driven attacks.

To stop these threats, security teams need cross-domain visibility that spans endpoints, identity, and cloud environments. By correlating activity across these domains organisations can uncover suspicious behaviours indicative of compromise. Proactive, intel-driven threat hunting across domains aids rapid detection and disruption of adversary activity before it escalates, delivering stronger protection against modern threats.

Help Desk Social Engineering

In addition to vishing, multiple eCrime threat actors are increasingly adopting help desk social engineering tactics. In these campaigns, threat actors call a targeted organisation's IT help desk and impersonate a legitimate employee, attempting to persuade a help desk agent to reset passwords and/or multi-factor authentication (MFA) for the relevant account.

Since early 2023, *SCATTERED SPIDER* has used this technique to gain access to single sign-on (SSO) accounts and cloud-based application suites. Multiple eCrime actors adopted this technique in 2024. Several relevant cases targeted academic and healthcare entities; in these incidents, threat actors subsequently used the compromised identity to exfiltrate data from cloud-based software-as-a-service (SaaS) applications or modify employee payroll data.

IT help desks often require employees seeking password and MFA resets to provide their full name, date of birth, employee ID, and manager name or answer a previously determined security question. However, eCrime actors attempting to socially engineer help desk personnel often accurately respond to these questions. Much of this information is not necessarily privileged and can be found in public resources and social media sites. Identity data that is typically confidential, such as a government ID number, is often advertised in underground markets.

In most help desk social engineering incidents, calls were made outside the victim's local business hours. This is likely because it enables the threat actor to maintain longer access to the compromised account before the legitimate owner reports suspicious activity.

Threat actors using this technique often register their own device for MFA to enable persistent access to compromised accounts. They also often manually delete emails from compromised mailboxes related to suspicious account activity or configure mail transport rules to redirect relevant emails to a folder other than the main inbox.

Over the past year, several eCrime actors have openly recruited callers on popular eCrime forums. The advertisements are usually for English-speaking callers with knowledge of remote monitoring and management software and experience conducting remote sessions. Some eCrime actors have also sought effective methods for spoofing phone numbers or encrypting calls to ensure caller IDs can be edited and appear more legitimate. This activity suggests phone-oriented social engineering will be a credible threat in 2025 as demand for these capabilities increases.

How to Mitigate Help Desk Social Engineering

- Require video authentication with government identification for employees who call to request self-service password resets.
- Train help desk employees to exercise caution when taking password and MFA reset request phone calls made outside of business hours, particularly if an unusually high number of requests is made in a short time frame or if the caller purports to be calling on behalf of a colleague.
- Use additional, non-push-based authentication factors such as FIDO2 (Fast IDentity Online 2) to prevent account compromise.
- Monitor for more than one user registering the same device or phone number for MFA.

Singapore Police Force (SPF)'s Efforts in Combatting Cybercrime

Contribution by **Singapore Police Force**

Scams and cybercrime continue to be a key concern. In 2024, the number of scam and cybercrime cases increased by 10.8% to 55,810 cases, compared to 50,376 in 2023. Scammers commonly target victims through messaging platforms, social media, online shopping platforms, phone calls, and other websites.[1]

Cybercriminals will continue developing more sophisticated attacks to exploit human and technological vulnerabilities across different levels of digital interaction. Individuals and organisations are at risk of financial loss, data theft, and reputational damage, especially with the growing reliance on digital devices and connectivity.

SPF Cybercrime Command

The SPF Cybercrime Command (CCC) was established in June 2015 to integrate investigations, forensics, intelligence, training, and policy formulation capabilities into a single command, allowing for a comprehensive and coordinated approach to combatting cybercrime. The Command oversees the implementation of the National Cybercrime Action Plan (NCAP), introduced in 2016 to set out the Government's key principles and priorities in combatting cybercrime.

Cybercrime Fighting Capabilities

As cybercriminals continue exploiting new technologies and methods to mask their illicit

[1] For more information, visit https://www.police.gov.sg/Media-Room.

activities, the operating landscape for law enforcement globally will inadvertently have to transform to be ready for the digital future. The SPF has been taking necessary steps to work towards becoming a forward-looking and effective force against cybercrime.

To prepare and upskill SPF officers to better deal with cybercrime related challenges, the SPF CCC instituted the Cybercrime Competency Framework which seeks to equip all officers with the requisite cybercrime knowledge and skills.

The SPF CCC has also been investing in building deep capabilities to tackle the growth of cybercrime. For instance, the SPF uses advanced commercial tools and open-source platforms to trace virtual assets involved in criminal activities. On the digital forensics front, to help identify deepfake audio or video recordings, the SPF has been working with the Home Team Science & Technology Agency (HTX) and other technical agencies to develop and improve AI detection capabilities.

In August 2024, the SPF launched the new National Service Cybercrime Operator (NSCO) vocation, to strengthen our cybercrime response and capabilities. The NSCO vocation allows the SPF to better tap on the expertise of Police Full-time National Servicemen (PNSFs) for deployment in operational roles within the CCC and Anti-Scam Command (ASC) to detect and disrupt cybercrimes and scams.

Collaborative Efforts

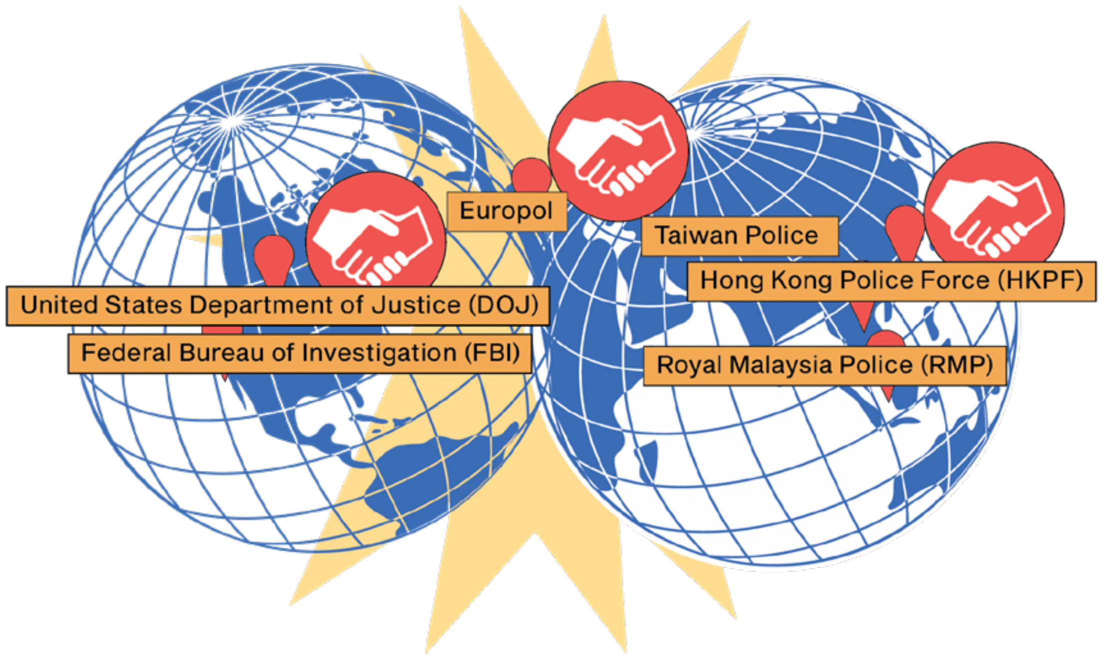
Close collaboration amongst whole-of-government (WoG) agencies is key to an effective cybercrime response. The SPF and CSA maintain an established channel to ensure timely exchange of critical information relating to cyber incidents including ransomware and data breach cases. Depending on the nature of the case, both agencies may conduct parallel incident response and investigation, facilitating case resolution and remedial advisories to victims. On the preventive front, the SPF, in collaboration with the CSA, has rolled-out a one-stop key portal for organisations to access key ransomware-related resources and disseminated joint advisories to provide information on recent cyber threats and trends, as well as mitigation measures.[2]

The **A**lliance of **P**ublic **P**riv**A**te **C**ybercrime s**T**akeholders (APPACT) is a public-private platform established by the SPF CCC in 2017 to facilitate information exchange among the partners. The APPACT community has grown in strength from 40 pioneer partners to a current total of 72 partners across 10 industries.[3] The SPF will continue enhancing collaboration with both APPACT and key stakeholders for a more coordinated response to cybercrime.

Apart from maintaining strong public-private partnerships, the SPF also collaborates with local and foreign law enforcement agencies in information exchange and joint operations. The following cases highlight the resolve of the SPF in fighting cybercrime, and the importance of international partnerships.

In a joint multi-jurisdictional investigation spanning 2023 to 2024, the SPF collaborated with the Hong Kong Police Force (HKPF) and the Royal Malaysia Police (RMP) to take down a syndicate responsible for the spate of malware-enabled scams reported in 2023 (affecting at least 1,899 victims in Singapore with total losses amounting to at least S$34.1 million). With strong cooperation and assistance from the RMP, two men were arrested in Malaysia and handed over to the SPF on 14 June 2024. Both men were subsequently charged in court on 15 June 2024. The HKPF also successfully took down 52 malware-controlling servers in Hong Kong and arrested 14 money mules who had allegedly facilitated the malware-enabled scams. During the course of investigations, the SPF shared information with the Taiwan Police, which in turn, led to the successful takedown of a syndicate operating a fraudulent customer service centre in Taiwan.

In a separate case, the SPF collaborated with the US Department of Justice (DOJ), Federal Bureau of Investigation (FBI) and Singapore's Attorney-General's Chambers (AGC) to dismantle a botnet which was used to compromise millions of computers worldwide that allowed cybercriminals to steal billions of dollars. On 24 May 2024, the SPF arrested a Chinese national responsible for the creation of the 911 S5 proxy service (botnet), putting a stop to the cyber malicious activities. Investigations, led by law enforcement in the US, are ongoing.


Europol
Taiwan Police
Hong Kong Police Force (HKPF)
United States Department of Justice (DOJ)
Federal Bureau of Investigation (FBI)
Royal Malaysia Police (RMP)

The SPF also participated in a Europol-led international operation, leading to the arrests of key figures behind the *8Base* ransomware group. These individuals were suspected of deploying a variant of the *Phobos* ransomware to extort high-value payments from victims across the world, including Singapore. The SPF's timely sharing of investigation findings pertaining to cases involving Singapore victims and technical indicators of compromise crypto-tracing analysis contributed to this successful operation.

Conclusion

To effectively mitigate cyber threats and build a more secure digital future, every one of us has a part to play. Public awareness and vigilance play a crucial role in preventing and deterring cybercriminal activities. The SPF will continue working closely with WoG agencies, public and private stakeholders, and the community to safeguard Singapore against cyber threats.

[2] For more information, visit https://www.police.gov.sg/Advisories/Crime/Cybercrime/Ransomware.
[3] Including social media companies, cybersecurity firms and cryptocurrency businesses.

VIRTUALPITA: A Royal P.I.T.A. A Backdoor With an Attack Path Well Worthy of Its Namesake

Contribution by **Mr Lim Minhan and Mr Melvin Seah, Ensign InfoSecurity**

Note: All server names, software, and tools have been masked to protect the identity of our client.

Virtual Fortress Breached: Hypervisor Attacks on the Rise

Cyber threats are evolving fast. Attackers are increasingly targeting infrastructure with little to no security monitoring. Operational technology (OT) networks and specialised operating systems often lack such comprehensive monitoring and often find themselves at the short end of the stick. A growing concern for this trend is in the rise of attacks against hypervisors, a critical component in server environments.

An Ordinary Day Turns Into Chaos

During a routine server patching operation, a system administrator observed an unexpected lack of internet connectivity. This anomaly was corroborated by reports from colleagues experiencing similar issues. Subsequent troubleshooting efforts determined that network traffic was being obstructed at the perimeter firewall, transforming an initially perceived technical malfunction into a significant security incident.

Unravelling the Incident

First Clues

The organisation's security team collaborated with their firewall vendor, who identified several critical issues. Notably, a superadmin account had been used to access the perimeter firewall via secure shell (SSH) from an administrative virtual machine ("admin VM"). Additionally, a new superadmin user was created on the firewall and was utilised to modify static routes, resulting in the disruption of internet connectivity for internal servers.

Further internal investigations revealed that a rogue internal IP address ("Rogue IP Address") was engaged in suspicious activities, including port scanning and lateral movements within the network. The team also identified the medium access control (MAC) address ("Rogue MAC Address") associated with the Rogue IP Address, aiding in pinpointing the source of the intrusion.

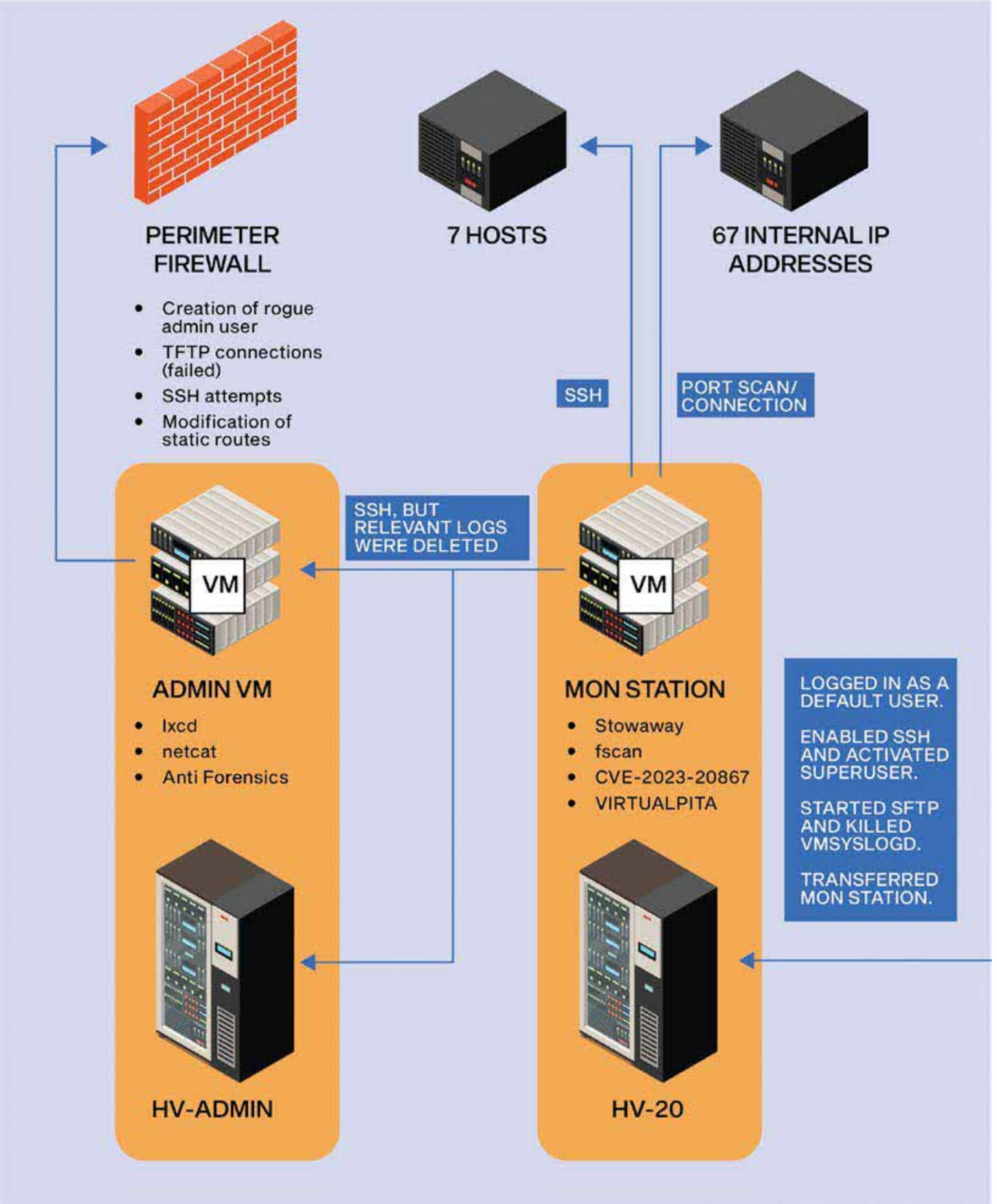
Tracking the Rogue IP

Upon further examination of the admin VM, Ensign traced the Rogue IP address to a hypervisor named "HV-20", which hosts virtual machines (VMs) in the same network range as the Rogue IP address. However, the Rogue IP address cannot be found in HV-20's management interface, raising significant concerns. In response, Ensign team conducted an in-depth analysis of the hypervisor's logs to uncover potential security breaches.

Crouching Attacker, Hidden Virtual Machine

Analysis of the HV-20's logs revealed that a VM named "MON Station" ("Rogue VM") was assigned with the Rogue MAC address. The VM was absent from the HV-20's graphical user interface (GUI) and was only detectable when browsing through HV-20's file system. The attacker had gained access to HV-20's shell, transferred the Rogue VM to HV-20, and started the rogue VM via command line, thereby bypassing the GUI of HV-20. This allowed the attacker to establish a hidden foothold within the network.

Attack Path Diagram



Tactics, Techniques and Procedures (TTPs) Observed

TACTIC	TECHNIQUE(S)	DESCRIPTION
TA0001 Initial Access	T1078.003 Valid Accounts: Local Accounts	The attacker moved around systems using valid local accounts (users) and breakglass accounts.
TA0002 Execution	T1059.004 Unix Shell	Attacker gained access to the hypervisor's Unix shell and performed his activities on the shell.
TA0003 Persistence	T1136.001 Create Account: Local Account	Attacker created a super admin on firewall appliances to update configurations.
	T1554 Compromise Host Software Binary	The firewall vendor reported that the attacker introduced malicious binaries to replace the appliance's legitimate files.
	T1543.002 Create or Modify System Process: Systemd service	The VIRTUALPITA backdoor has peripheral files for it to install as a Systemd service and set the service to start on boot.
TA0004 Privilege Escalation	T1078.001 Valid Accounts: Default Accounts	The attacker used a privileged account to set a password for the superuser on the hypervisor and and used the superuser to perform malicious activities.
TA0005 Defense Evasion	T1564.006 Hide Artifacts: Run Virtual Instance	The attacker introduced his own VM as a staging ground, meaning that tools used for scanning and accompanying results will not be stored on servers.
	T1562.003 Impair Defenses: Impair Command History Logging	Ensign observed that the attacker stopped logging processes on the hypervisor, which stopped the logging of commands issued on the hypervisor.
	T1070.002 Indicator Removal: Clear Linux or Mac System logs	The attacker strategically removed certain entries of login and activities logs on 'admin VM' such that the logs would still appear "complete". There were also other instances of logs being deleted.
TA0007 Discovery	T1046 Network Service Discovery	The attacker performed multiple scans for opened ports across the network. Particularly hypervisor-related ports, SSH, HTTP, and HTTPS.
TA0008 Lateral Movement	T1570 Lateral Tool Transfer	The rogue VM was transferred to the hypervisor using the built-in SFTP server.
	T1021.004 Remote Services: SSH	The attacker moved between machines and appliances using SSH.
TA0011 Command and Control	T1090.003 Proxy: Multi-hop Proxy	Attacker used proxy tools to connect back to attacker infrastructure through the corporate proxy.
TA0040 Impact	T1499 Endpoint Denial-of-Service	Attacker modified a static route on perimeter firewall, causing internal servers to be denied internet access.

Inside the Rogue VM: A Cyber "Attack Submarine"

Forensic examination of the Rogue VM revealed it was running on an Alpine Linux operating system and was configured with the Rogue IP Address, as specified in its network configuration file. The Rogue VM contained several red team tools, including multi-hop proxies, reverse proxies, and scanning tools. Notably, an executable named "lxcd" — identified as "VIRTUALPITA" — was found. The Rogue VM also communicated with several other internal VMs, including the admin VM as talked about earlier.

Upon execution, the "lxcd" backdoor establishes a listening daemon on TCP port 6492, mimicking the behaviour of a standard OpenSSH server process. It enforces certificate-based authentication in addition to password verification, ensuring that only the attacker possessing the requisite certificate could gain access through this discrete channel.

Lessons and Key Takeaways

Recent analysis have identified hypervisors as emerging targets for cyber-attacks. This shift underscores the necessity for robust security and monitoring controls at the hypervisor level to prevent an attacker from gaining control of VMs from an "invisible" source.

The GUIs on hypervisors have proven insufficient in detecting unauthorised VMs, as these hidden VMs can operate undetected within the system.

Moreover, incidents have revealed that attackers can maintain prolonged, covert access within an environment, remaining undetected for extended periods before initiating their primary attack.

Next Steps

This case remains under active investigation. The Ensign team is tracing the full extent of the attacker's activities, identifying other compromised systems, and closing security gaps to prevent a similar attack from happening in the future.

This case highlights the increasing sophistication of cyber threats and underscores the need for proactive hypervisor security and monitoring, and robust incident response strategies to detect and neutralise intrusions before they escalate.

After-Action Review

Due to the ongoing nature of this case, Ensign is unable to provide definitive comments on all mitigation procedures. However, in light of the recent increase in cyber-attacks targeting hypervisors, Ensign recommends implementing monitoring measures for hypervisors. Forwarding hypervisor system logs to a centralised logging server is advisable. For Unix-based hypervisors, tools such as syslog can be utilised, while Windows-based hypervisors can employ Windows Event Forwarder. This centralised approach enables security teams to detect and respond to malicious activities more effectively.

Additionally, standard security practices remain pertinent in this context. Regularly patching systems and applications with the latest updates, routinely changing user passwords, and conducting frequent threat hunts to identify anomalies are essential measures. These proactive steps are instrumental in preventing opportunistic attackers from infiltrating networks.

A COLLECTIVE RESPONSIBILITY

The Singapore Cybersecurity Strategy was first launched in 2016 to set out Singapore's vision, goals and priorities for a resilient and trusted cyberspace. Subsequently, amidst the dynamic and increasingly complex cyber and digital threat landscape, CSA refreshed the Strategy in 2021. This updated Strategy sets forth a comprehensive framework to enhance our nation's cyber resilience and underscores our national commitment to proactively address cyber risks through fostering collaboration with industry and other stakeholders.

The Strategy is built upon three strategic pillars and two foundational enablers:

Strategic Pillar 1: Build Resilient Infrastructure
Strategic Pillar 2: Enable a Safer Cyberspace
Strategic Pillar 3: Enhance International Cyber Cooperation

Foundational Enabler 1: Develop a Vibrant Cybersecurity Ecosystem
Foundational Enabler 2: Grow a Robust Cyber Talent Pipeline

This Chapter highlights key initiatives which CSA, together with our partners, embarked on in 2024, as part of our continued work to implement Singapore's Cybersecurity Strategy 2021.

INTERVIEW WITH CSA'S FORMER DEPUTY CHIEF EXECUTIVE (DEVELOPMENT) TEO CHIN HOCK

How Was the Concept of Collective Responsibility Fostered Among Stakeholders in the Early Days of CSA?

1. What was the cybersecurity ecosystem in Singapore like before CSA was formed?

Before the formation of CSA, we did have groups of dedicated cybersecurity experts in Ministry of Defence (MINDEF), Ministry of Home Affairs (MHA) and Infocomm Media Development Authority (formerly IDA). These professionals were specifically tasked to protect MINDEF/SAF networks, the Critical Information Infrastructure (CII) computer networks and government's IT networks, respectively. In 2014, the then Prime Minister Lee Hsien Loong launched the Smart Nation 1.0 vision for the nation where people live meaningful and fulfilled lives, enabled seamlessly by technology, offering exciting opportunities for all. Beneath the broad vision, we were also convinced that it needs to be underpinned by strong cybersecurity. Yet, the ecosystem then did not have a group dedicated to maintaining the cybersecurity of the nation's cyberspace beyond that of the CIIs.

2. What were your initial thoughts on joining CSA? How did your experience in your prior appointment help to shape your thinking/contribution to CSA?

Before joining CSA as DCE(Development), I was the DCE(Strategic Development) in Defence Science and Technology Agency (DSTA). One of the strategic development initiatives DSTA and MINDEF/SAF undertook was to build up the digital defence capability of the SAF as we believe that the battles of the future will be fought in the digital space. Within DSTA, I set up the Cybersecurity Programme Centre. I also worked with the then Deputy Secretary (Technology), David Koh, to venture into partnership with some strategic partners overseas to build digital defence capability. So it was natural that when CSA was set up, the newly appointed CE (David Koh) and I discussed my transition to CSA as I have done my stint as DCE(Strategic Development) in DSTA.

3. What was the initial strategic focus in response to the cybersecurity threat landscape in the early days of CSA?

While CSA initially concentrated on safeguarding CIIs, we recognised early on that cyber threat actors certainly did not limit their ambitions to attacking CIIs alone. In response, a comprehensive national cybersecurity strategy was formulated and unveiled by the then Prime Minister Lee Hsien Loong during the first Singapore International Cyber Week (SICW) in 2016. This strategy expanded CSA's mandate beyond the protection of CIIs to encompass the broader objective of fostering a safer cyberspace in tandem with Singapore's growing digital way of life.

The strategy necessitated the development of resilient infrastructure, and to step up efforts to enable a safer cyberspace. Additionally, it highlighted the importance of international collaboration in cybersecurity, as cyber threats are not limited by national borders or geographical regions.

4. How was the concept of collective responsibility in cybersecurity fostered among stakeholders in the early days of CSA?

Within CSA, it would be the recognition that our cyber adversaries are not just one group but several groups: cybercriminals, cyber hacktivists, cyber spies and state-sponsored cyber threat actors. We need to know not just what they are doing, but what they are planning to do. This meant that only if everyone in CSA played a part, then only could we stay half a step ahead of these cyber adversaries.

We were also cognisant that the Singapore public perceives all forms of cyber incidents, from network attacks to data theft and ransom demands, as cybersecurity issues. To address these challenges, the collaboration with CII sector leads, the Police, Personal Data Protection Commission (PDPC), and security agencies within MINDEF and MHA has been and still is essential.

5. What were some of the most significant challenges you faced during the initial years, and how were they overcome?

In 2017, the *Wannacry* ransomware incident significantly disrupted global cybersecurity. At that time, our readiness to counter such sophisticated cyber threats was limited, with our SingCERT then operating with a modest team of part-time personnel.

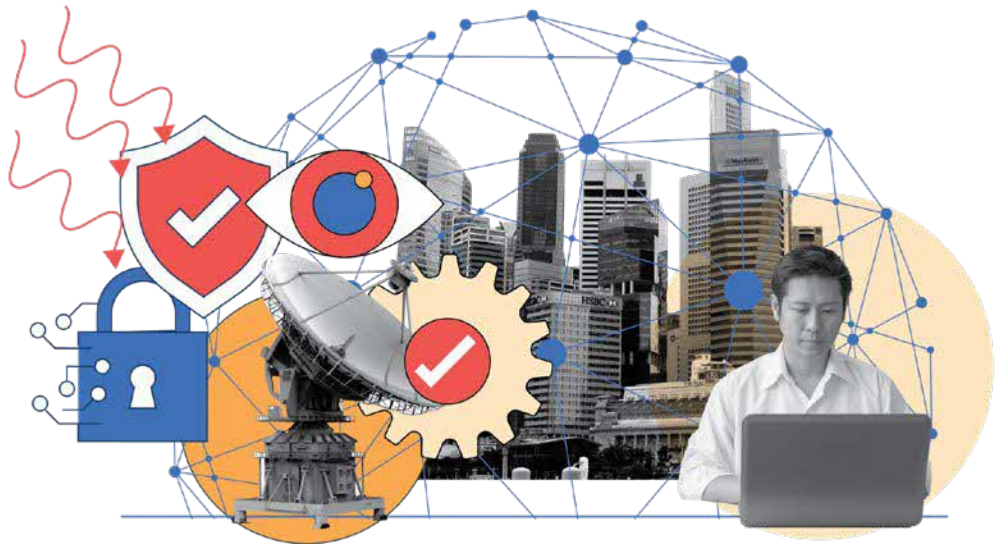
Although our CIIs remained unscathed, some of our small enterprises were hit. Additionally, the ripple effects from the cyber-attack on a major global shipping company had a pronounced impact on Singapore, given our status as a key international transshipment hub.

Despite these challenges, CSA's response was prompt and effective, thanks to our technical expertise and the robust international cyber partnerships we have established with counterparts such as the UK, the Netherlands, and Israel. Such partnerships facilitated a swift and efficient exchange of critical information, which was instrumental in managing the crisis.

6. Do you have any quotes or thoughts that you would like to be highlighted as a prelude to our Chapter on A Collective Responsibility?

"In the realm of cybersecurity, the only constant is change. To stay ahead, we must embrace a culture of continuous learning and adaptability, always anticipating the moves of our adversaries. Our collective responsibility is not just to protect against the threats of today but to prepare for the challenges of tomorrow."

Strategic Pillar 1: Build Resilient Infrastructure



Legislation

Amendment of the Cybersecurity Act – a Legal Framework for the Oversight and Maintenance of National Cybersecurity in Singapore

The Cybersecurity Act has empowered CSA to ensure the cybersecurity of important systems and entities in Singapore's cyberspace. It was first enacted in 2018 with the following objectives:

- Regulate our CIIs for cybersecurity;
- Provide CSA with powers to prevent and respond to cybersecurity threats and incidents; and
- Allow CSA to license some of the more sensitive cybersecurity service providers.

In 2024, the Act was amended to adapt to the use of new technologies, evolving threat landscape and increased attack surface. The amendments included:

- Updating CSA's regulatory powers to account for new business models;
- Expanding the regulatory ambit of the Act to include three new types of systems and entities – Systems of Temporary Cybersecurity Concern (STCC), Entities of Special Cybersecurity Interest (ESCI), and Foundational Digital Infrastructure (FDI); and
- Updating incident reporting obligations to improve our situational awareness and help us stay abreast of the evolving threat landscape.

Chief Executive of CSA and Commissioner of Cybersecurity, Mr David Koh, engaging industry stakeholders at the 26 February 2024 CSA-US-ASEAN Business Council Lunchtime Dialogue on the Cybersecurity Act Amendments.

Moving forward, the amended Cybersecurity Act allows Singapore and Singaporeans to be even more assured of the security of the digital technology, systems and processes that we rely on for our economy and way of life.

Enhancing CII Cyber Resilience

Operational Technology Cybersecurity Expert Panel (OTCEP) Forum 2024

The OTCEP Forum organised by CSA is the largest forum dealing with operational technology (OT) cybersecurity in Asia Pacific. Its 2024 edition involved an impressive turnout of over 1,000 attendees, solidifying its status as Singapore's premier platform for CSA, stakeholders, industry leaders and international OT cybersecurity experts to discuss OT cyber threats, share best practices and collaboratively strengthen the cyber resilience of Singapore's OT sector.

OTCEP 2024 included a carefully curated series of masterclasses to level up participants' proficiency in the OT cybersecurity domain. These masterclasses focused on the fundamentals, ranging from industrial control system (ICS) to supervisory control and data acquisition (SCADA) architecture communication protocols and incident response. The forum's 'capability showcase' also provided a platform for participants to engage with OT vendors and solution providers, gaining insights into practical use cases that can be implemented to strengthen the cybersecurity of their OT/ICS environment.

A hands-on purple teaming workshop was also conducted during the event. Multiple workstations were set up for participants to experience both offense and defence, by executing tactics, techniques and procedures (TTPs), and subsequently detecting the attacks. This allowed them to better appreciate the value of good detection rulesets and more importantly, bring this appreciation back to their own organisations.

Participants working on a purple team exercise during OTCEP 2024.

Minister for Digital Development and Information and Minister-in-charge of Smart Nation and Cybersecurity, Mrs Josephine Teo and former Senior Minister of State for Digital Development and Information, Dr Janil Puthucheary having a photo session with OTCEP members to kick off OTCEP Forum 2024.

Singapore's OT Cybersecurity Masterplan 2024

In 2024, Minister for Digital Development and Information, Mrs Josephine Teo launched the OT Cybersecurity Masterplan at the fourth edition of the Singapore OTCEP forum. This Masterplan serves as a strategic blueprint to bolster Singapore's cyber defence, to ensure a secure and resilient OT cyber environment for both CII and non-CII sectors.

Singapore's OT Cybersecurity Masterplan 2024

Cybersecurity Exercises

A series of cybersecurity exercises were conducted throughout 2024, to enhance Singapore's overall cybersecurity preparedness to deal with contingencies. The exercises aimed to evaluate and validate incident management capabilities of CII sector leads, as well as technical response capabilities of the various national cyber incident response teams (NCIRTs) in Singapore.

Key exercises included:

- **CIDeX** – a joint initiative with the Digital and Intelligence Service (DIS) to provide hands-on training on OT systems for cybersecurity teams in the CII sectors.
- **Cybersecurity Validation Exercise (CVEX)** – a programme to validate key incident management capabilities of CII sector leads and demonstrate their ability to manage multiple incidents and communicate vital information to key stakeholders.
- **Exercise Cyber Knights** – 66 participants comprising NCIRTs from CSA and other governmental agencies were put through realistic, complex scenarios involving eradicating advanced persistent threats (APTs) embedded in targeted systems, with the objective of evaluating their technical response capabilities.

Emerging Tech

Developing Cybersecurity Code of Practice (CCoP) for Cloud

More organisations in Singapore are moving their systems and operations to the cloud. This shift brings significant benefits to accelerate digital transformation, but also introduces new cybersecurity risks.

In 2024 alone, there were three major cloud outages – Alibaba Cloud in September, and Microsoft Azure and Salesforce in November. Furthermore, cyber threats are becoming more sophisticated, and cloud environments are attractive targets for malicious actors.

CSA is developing a CCoP for Cloud, which will provide guidance and a framework for organisations to adopt cloud services securely. It will help organisations understand their responsibilities and implement the appropriate security controls.

The proposed CCoP for Cloud will cover areas such as:

- **Data Security and Privacy:** Protecting sensitive data in the cloud;
- **Access Control:** Ensuring only authorised users can access cloud resources;
- **Incident Response:** Establishing procedures and techniques to handle security incidents in the cloud; and
- **Supply Chain Security:** Assessing and managing risks related to cloud service providers.

CSA Guidelines and Companion Guide on Securing Artificial Intelligence (AI) Systems:

With the rapid development and widespread use of AI, there was a growing need to raise awareness of security risks of AI amongst developers and system owners.

In 2024, CSA engaged 46 AI and cybersecurity practitioners over two rounds of consultations, culminating in the publication of a series of guidelines containing principle-level guidance as an evergreen approach for systems owners to secure AI. These guidelines were further supplemented by a Companion Guide, positioned as a community-driven resource offering practitioners a comprehensive reference when building their own AI security plans.

The guides received positive feedback from practitioners regarding the practical, specific and comprehensive references on how to secure AI systems throughout the lifecycle.

Former Senior Minister of State for Digital Development and Information, Dr Janil Puthucheary's keynote address during SICW 2024, emphasising the importance of securing AI systems.

> *"As such, we strongly support CSA's lifecycle-based approach to security for AI systems, which reflects the need to manage cyber risk at multiple points throughout the lifecycle"*
> Information Technology Industry Council (ITI)

> *"Cybersecurity is a mutual interest for Government and industry, and we commend CSA's continued commitment to engage with industry on key cybersecurity regulations and guidance."*
> US-ASEAN Business Council, Inc.

> *"We applaud CSA for its commitment to transparency and for actively seeking feedback from the business community. We firmly believe that ongoing engagement with industry is vital as technology continues to advance and become increasingly sophisticated."*
> HP Inc.

> *"We appreciate CSA's encouragement for the adoption of risk assessments and risk-targeted measures in AI Governance. We believe the guidelines could expressly recognise the importance of AI Governance."*
> IBM Singapore

> *"AI SIG would like to applaud CSA for their timely and insightful publication of guidelines to secure AI systems. This proactive approach not only addresses emerging risks but also sets a critical benchmark for the industry. By providing clear and forward-thinking standards, the regulator demonstrates a commendable commitment to safeguarding both technological innovation and public trust in an increasingly complex digital landscape. This initiative is a crucial step towards ensuring that AI systems are developed and deployed with robust security measures in place."*
> Association of Information Security Professionals (AiSP) Artificial Intelligence Special Interest Group (AI SIG)

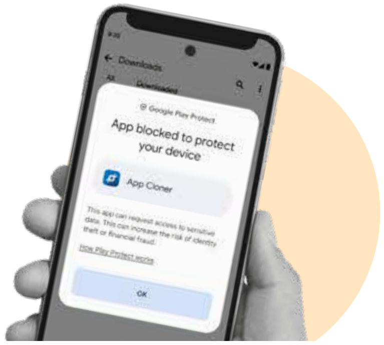
Strategic Pillar 2: Enable a Safer Cyberspace

Empowering a Cyber-Savvy Population

Enhanced Fraud Protection (EFP)

In February 2024, CSA partnered Google to pilot a new Enhanced Fraud Protection (EFP) feature within Google Play Protect (GPP). This feature automatically blocks the installation of potentially malicious applications sideloaded from the internet, that request for excessive permissions.

This feature was rolled out to approximately seven million Android devices registered with Google Play Store. As of December 2024, the EFP has successfully blocked 1.6 million installation attempts of potentially malicious applications across 370,000 devices.



Google Play Protect

App blocked to protect your device

App Cloner

This app can request access to sensitive data. This can increase the risk of identity theft or financial fraud.

How Play Protect works

OK

Enhanced Fraud Protection (EFP) feature within Google Play Protect (GPP).

Cyber Security Awareness Alliance (CSAA)

2024 saw the beginning of the ninth term of the CSAA. The Alliance brought together members from the People, Private and Public sectors to promote and enhance awareness and adoption of good cybersecurity practices. New members in this term included global tech giants Google and Samsung, telecommunications company Singtel, cybersecurity consultancy Lumens, the Singapore Business Federation, and Nanyang Technological University.

Over the years, CSAA members have been actively involved in projects to bolster cybersecurity awareness and adoption of best practices.

For example, CSA worked with Samsung and Google to showcase the firms' *Auto Blocker* and *Play Protect* respectively for an episode of Crimewatch. CSA also worked with Google on a series of social media posts and video collaborations on Google Play Protect Pilot. Finally, SGTech was interviewed by MediaCorp for their expert views on the second reading of the Cybersecurity (Amendment) Bill.

Outreach to Social Service Agencies (SSA)

The findings from CSA's Singapore Cybersecurity Health Report 2023 indicated that non-profit organisations (NPOs) experienced more cybersecurity incidents compared to businesses. As NPOs manage sensitive information related to donors and beneficiaries, they tend to be targeted by cybercriminals.

To address the issue, CSA, in collaboration with the National Council of Social Service (NCSS), doubled efforts to raise cybersecurity awareness within the non-profit sector. Through eight months in 2024, CSA engaged 34 SSA over physical and virtual talks, reaching over 840 participants. Many SSA employees and volunteers expressed appreciation for the sessions, as they found the practical advice and actionable insights very useful in their course of work and daily lives.

> **"AWARE would like to extend our heartfelt gratitude to CSA for providing us with a cybersecurity training session. [The presenters] were knowledgeable and made complex topics accessible and easy to understand. This training has greatly improved our cybersecurity posture and equipped our team with practical skills to handle potential cyber threats effectively."**
>
> Yasmine Tan, Director of Operations, AWARE
>
> National Council of Social Service (NCSS)

SG Cyber Safe Students Programme

In 2024, CSA continued to share cybersecurity messages in assembly halls, classrooms and computer labs through the SG Cyber Safe Students Programme. Its milestones included:

- Collaborating with Microsoft to offer workshops to primary and secondary school students, to convey good cyber hygiene practices through gamification. These workshops leveraged Microsoft's Minecraft education cybersecurity modules, to teach cybersecurity messages using immersive scenarios in the Minecraft world, that were relatable to students.
- Launching CSA's third iteration of the "Be Cyber Safe Pop-up and Be Cyber Safe" drama skit, which continued to receive strong demand and positive feedback from schools and partners. The current Pop-up has travelled to 103 schools and community spaces since its launch in October 2023, while the drama skit has completed 76 shows since January 2024.

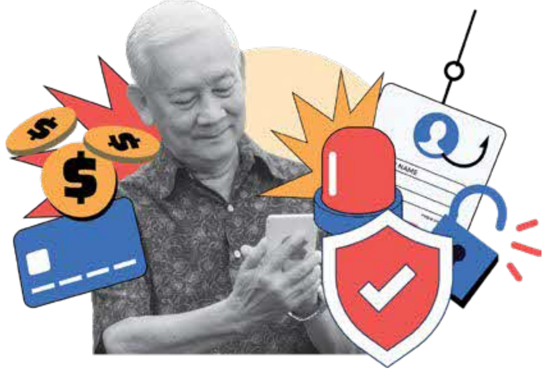
- Conducting school talks to over 40,000 students from 40 schools ranging from primary schools to Institutes of Higher Learning (IHLs), on topics such as the importance of cybersecurity, common cyber threats and tips to stay safe online.
- Working with the Ministry of Education (MOE) through incorporation of content related to cyber threats and Singapore's Cybersecurity Strategy 2021, into the social studies curriculum for upper secondary school students. CSA also co-created videos for MOE's Student Learning Space to deepen educators' and students' understanding of cybersecurity.

SG Cyber Safe Seniors Programme

The SG Cyber Safe Seniors Programme seeks to equip the silver generation with cybersecurity skills that are essential in our digital age. Key milestones included:

- Working with Infocomm Media Development Authority's (IMDA) SG Digital Office to incorporate cybersecurity-related content and resources in the Digital Skills for Life competencies framework, to equip seniors with essential digital skills – including cyber tips to protect themselves from online risks such as phishing scams and deepfakes. In 2024, more than 90,000 seniors have benefitted from this initiative.

- Conducting the "Be Cyber Safe Workshop" for seniors. Seniors were guided by student volunteers from various IHLs on how to use digital apps safely and confidently. In 2024, more than 400 seniors participated in the workshops, which was supported by partners from other government agencies and banks.



- Piloting the "Be Cyber Safe: Train-the-Trainers" workshops. As grassroot leaders and community volunteers are often at the frontlines engaging seniors and residents, the workshops aimed to equip them with essential cybersecurity knowledge and skills. This initiative empowered trainers to effectively share cyber threat trends and cyber hygiene practices with seniors during their daily interactions and community engagements. In 2024, this initiative has trained over 430 volunteers.

- Working with public and private sector partners such as Singapore Police Force (SPF), the People's Association, IMDA, the Central Provident Fund Board (CPFB), the Monetary Authority of Singapore and major local banks, to co-develop and disseminate content on scam trends and good cyber hygiene practices. The partners amplified the content at community spaces such as community centres and bank branches.

Recommended Security Apps List 2024

In 2023, CSA published a list of security applications that members of the public can use to protect their mobile devices against common threats. Since then, CSA has reviewed and refined the criteria for this list of security applications, in order to address evolving attack techniques.

The number of overall scam cases increased in 2024, with attackers exploiting mobile devices to perform unauthorised transactions.

In an effort to stay updated on the evolving attack techniques such as the use of mobile malware-enabled scams, CSA continued to engage various security application vendors to work on enhancing their solutions. These enhancements include the ability to detect and defend against mobile threats such as malware, phishing and network attacks, so as to ensure device integrity. Subsequently, CSA published an infographic featuring the refreshed Recommended Security Apps List 2024.

Cybersecurity Labelling Scheme for the Internet of Things (CLS-IoT)

The Cybersecurity Labelling Scheme (CLS-IoT) aims to enhance the security of internet of things (IoT) and elevate overall cyber hygiene. The scheme aims to incentivise IoT manufacturers to adopt a security-by-design approach by assigning a security rating according to their levels of cybersecurity provisions. As of 2024, this initiative has resulted in more than 550 labelled products across leading global brands such as Google, Asus, TP-Link, D-Link, Netgear, Nokia and Signify Philips.

The scheme utilises a three-pronged approach:

- **To make cybersecurity provisions transparent to consumers,** and enable them to differentiate against poorly secured devices.

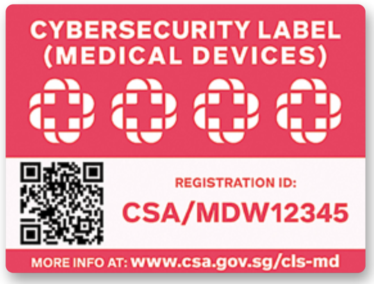
- **To enable developers and manufacturers to differentiate themselves in the market,** hence encouraging the production of more secure devices within the industry.

- **To collaborate with like-minded international partners** to establish Mutual Recognition Arrangements (MRA) of the CLS. Aside from reducing duplicative testing, the MRA formalises mutual recognition of IoT devices with national cybersecurity labels. Singapore has signed MRAs with Germany and the Republic of Korea, in 2022 and 2024 respectively.

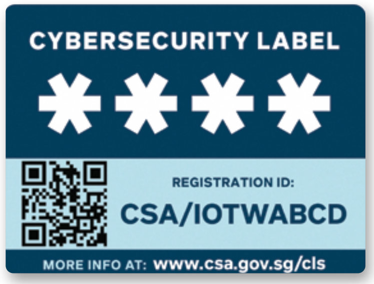
In 2024, CLS for medical devices (CLS-MD) was launched – a voluntary scheme where medical devices are rated according to their levels of cybersecurity provisions. Since its inception, this initiative has received positive support from both leading global medical device manufacturers such as Boston Scientific, Johnson & Johnson, Abbott Medical, and local SMEs such as TIIM Healthcare.

Signing of MRA with National Coordination Centre for Cybersecurity – Federal Office for Information Security (BSI) - Germany on 16 October 2024.

Signing of MRA with Korea Internet & Security Agency (KISA) on 16 October 2024.


CYBERSECURITY LABEL (MEDICAL DEVICES)
REGISTRATION ID:
CSA/MDW12345
MORE INFO AT: www.csa.gov.sg/cls-md

CLS-MD label.



CLS-IoT label.

Fifth National Cybersecurity Campaign – The Unseen Enemy

Through 2023 and 2024, CSA continued its push to raise awareness of good cyber hygiene practices with our "*The Unseen Enemy*" campaign. Through a mix of physical interactions such as roadshows, out-of-home and digital platforms touchpoints, the campaign drove adoption among the public to adopt the refreshed Cyber Tips. There were several notable points:

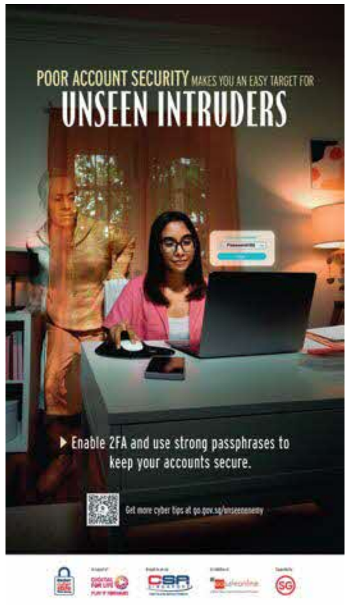
- Around 16,000 people visited our two campaign roadshows at Heartbeat@ Bedok and Toa Payoh Hub, featuring interactive booths to spread public awareness on how to stay cyber-secure and scam-safe. These were supported by our partners – SPF, National Crime Prevention Council, IMDA, and Singtel.

- The campaign received strong support from ecommerce platforms Lazada, Shopee, Carousell, and Zalora. These platforms collaborated with CSA to host our campaign themed microsite, co-develop infographics and share our campaign video and key visuals to amplify our campaign messages to the public.

CSA SINGAPORE
Cyber Security Agency of Singapore
HOME IN ON CYBER SECURITY
JOIN US AT
OUR CYBERSECURITY ROADSHOW
Date: 24 & 25 Feb
Time: 11am -6pm
Location: Toa Payoh Hub
Toa Payoh
Better cyber safe than sorry

- CSAA members, such as Singtel and SPF, supported CSA's "Home in on Cybersecurity" roadshows with booth setups. This included Singtel's "Scam Smash" game machine which allowed users to win prizes while learning about cybersecurity as they took on anti-scam challenges.

OUTDATED SOFTWARE OPENS YOU UP TO
UNSEEN THREATS
Update software promptly to protect your devices from bugs and security flaws.
Get more cyber tips at go.gov.sg/unseenenemy


POOR ACCOUNT SECURITY MAKES YOU AN EASY TARGET FOR
UNSEEN INTRUDERS
Enable 2FA and use strong passphrases to keep your accounts secure.
Get more cyber tips at go.gov.sg/unseenenemy

UNSECURED DEVICES LEAVE YOU VULNERABLE AGAINST
UNSEEN CRIMINALS
Add the ScamShield app to detect scam SMSes and block scam calls.
Install anti-virus apps to prevent malware.
Get more cyber tips at go.gov.sg/unseenenemy

A Shared Responsibility - Playing Our Part

Cyber Threat Information Sharing With the Wider Singapore Community

In the last few years, CSA has established meaningful public-private partnerships to enhance visibility of cyber threats and associated developments in Singapore. Aside from deriving actionable insights to secure Singapore's CII, CSA also recognised the importance and value of sharing threat information with other Singapore-based organisations in the wider community. In 2025, CSA will start sharing machine-readable cyber threat indicators with selected Singapore-based organisations. This initiative will supplement organisations' security operations, enabling them to proactively detect, block and respond to emerging cyber threats.

Director of CSA's Safer Cyberspace Division, Ms Veronica Tan, at the launch of the CSA Cyber Trust and Cyber Essentials Marks certification schemes on 29 March 2022.

Revision of Cyber Essentials and Trust Mark in 2025

CSA launched the Cyber Essentials and Cyber Trust mark in 2022 to help small and medium enterprises (SMEs) in Singapore implement cyber hygiene measures and attain cybersecurity certification. Intended to help improve Singapore's national cyber resilience, Cyber Essentials and Cyber Trust accommodates the resource constraints of small organisations, resulting in more than 300 organisations being certified in cybersecurity.

As organisations progressed in their digital transformation journey, the pace of new tech adoption also picked up. In 2024, the typical SME adopted two digital technologies whilst multinational corporations (MNCs) adopted four to five digital technologies.[1] The utilisation of new digital technologies, while reducing costs and raising efficiency, also expanded the attack surface of the organisations. To this end, CSA will be revising and expanding the Cyber Essentials and Cyber Trust in 2025, to go beyond classical cybersecurity and include Cloud, AI and OT security.

[1] Infocomm Media Development Authority, "Singapore Digital Economy Report 2024," 2024, 9, https://www.imda.gov.sg/-/imda/files/infocomm-media-landscape/research-and-statistics-/sgde-report/singapore-digital-economy-report-2024.pdf.

Onboarding of CSA as a Cyber Emergency Response Team (CERT) CVE Numbering Authority (CNA)

A CNA is an organisation responsible for the assignment of Common Vulnerabilities and Exposure (CVE) IDs, and for creating and publishing information about these vulnerabilities. In 2024, CSA was onboarded as a CERT CNA to centralise the reporting of zero-day vulnerabilities in Singapore. With this, CSA is now able to issue CVE IDs aside from just relaying information regarding zero-day vulnerabilities to affected entities. CSA will also manage the vulnerability disclosure policy, which provides the guidelines and describes in detail how Informers, System Owners, and SingCERT, can contribute to the process of responsible vulnerability disclosure (RVD).

Distributed Denial-of-Service (DDoS) Mitigation Advisory

In view of the rising number of DDoS attacks, CSA published the DDoS Mitigation Advisory in August 2024. Developed in consultation with industry experts and partners such as Cloudflare, Singtel, DSTA and GovTech, this advisory comprises a set of best practices which focuses on ensuring a holistic, layered defence strategy against DDoS incidents, and encourages a cyclical and iterative approach to identify, contain and mitigate DDoS threats.

Safe App Standard (SAS) 2.0

CSA first launched the SAS in January 2024 to provide app developers and owners with comprehensive guidelines to fortify the security of mobile applications that deal with high-risk monetary transactions. SAS 2.0 was subsequently released in December 2024, introducing four new key areas – network communication, cryptography, code quality and exploit mitigation.

Aside from referencing established industry standards such as those set by Open Web Application Security Project (OWASP), the European Union Agency for Network and Information Security (ENISA), Payment Card Industry Data Security Standard (PCIDSS) and the National Institute of Standards and Technology (NIST), SAS 2.0 was refined through consultations with a diverse range of stakeholders including local government agencies, financial institutions, cybersecurity firms, academic institutions and technology companies.

CSA

SAFE APP STANDARD 2.0

Internet Hygiene Portal (IHP)

Since its launch in October 2022, the IHP has been used to scan more than 50,000 unique websites and email domains to assess their security and hygiene levels. Approximately 50% of these unique domains showed improvement in their internet hygiene after following recommendations provided by CSA. At the end of 2024, more than 2,400 website and email domains have also attained the 'Hall of Fame' status (i.e. domains scoring 100% in website and email hygiene scans).

Strategic Pillar 3: Enhance International Cooperation

Cyberspace is borderless. Hence, it is imperative for CSA to continue advocating for a secure, stable, and resilient cyberspace. We need to keep up our efforts at the global, regional, as well as bilateral levels, which are vital for the security and economic well-being of all nations.

Multilateral Engagements

At the global level, CSA continued to engage with international partners on various digital trust and security issues, ranging from cybercrime to cybersecurity threats, to build a multilateral, rules-based cyberspace we can trust.

CSA's commitment to bolstering global cybersecurity was evident in our participation in key international initiatives, such as the Counter Ransomware Initiative (CRI) and the UN Open-Ended Working Group (UN OEWG) on the Security of and in the Use of ICTs (2021-2025).

The CRI brings together 68 states and international organisations, with Singapore and the UK co-leading the CRI Policy Pillar to develop and share best policy practices to build cyber resilience, and disrupt the criminal ransomware industry. In 2024, Singapore and the UK held a table-top exercise to support CRI members in identifying gaps within their ransomware response processes, and to develop best practices within the healthcare sector.

These engagements have been instrumental in fostering international cooperation and enhancing collective cyber resilience.

Chief Executive of CSA and Commissioner of Cybersecurity, Mr David Koh, alongside other Head of Delegations at the CRI Summit held in 2024.

Director of CSA's International Cyber Policy Office, Mr Sithuraj Ponraj, delivering Singapore's national intervention at the UN OEWG.

ASEAN/Regional Engagements

Within ASEAN, CSA actively engages in regional platforms and foster closer cooperation among ASEAN Member States (AMS) to address cybersecurity challenges in the region. CSA is committed to advancing practical cooperative initiatives that enhance collective cyber resilience and security, leading to a more stable and secure international cyber environment in the region.

Such initiatives include conducting capacity building programmes through the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) and hosting the annual ASEAN Ministerial Conference on Cybersecurity (AMCC) on the sidelines of the Singapore International Cyber Week (SICW) since 2016.

Inaugural ASEAN Regional CERT Taskforce Meeting, held in August 2024.

5th iteration of UN-Singapore Cyber Fellowship in August 2024.

9th ASEAN Ministerial Conference on Cybersecurity held on the sidelines of SICW in 2024.

Bilateral Engagements

CSA actively engages with a wide range of international and regional partners across various bilateral platforms to foster the exchange of cyber policy, operational, technical, and diplomatic issues between Singapore and individual countries. Bilateral engagement efforts include hosting meetings with key international personalities, and conducting cyber exchanges and dialogues with various countries, where officials come together to discuss cyber cooperation.

Some key cyber exchanges in 2024 included the inaugural India-Singapore Cyber Dialogue and continued runs of the Malaysia-Singapore Cybersecurity Roundtable, New Zealand-Singapore Cyber Exchange, UK-Singapore Cyber Dialogue (UKSCD) and the US-Singapore Cyber Dialogue (USSCD).

3rd USSCD held in Singapore, on 18 October 2024.

2nd UKSCD held in Singapore, on 13 June 2024.

The inaugural India-Singapore Cyber Dialogue held in Singapore, on 17 October 2024.

Foundational Enabler 1: Develop a Vibrant Cybersecurity Ecosystem

Integrated Approach to Catalyse Talent, Innovation and Growth

Talent, Innovation and Growth (TIG) Plan

For the past 10 years, CSA has sought to develop a vibrant cybersecurity ecosystem. Under the Cyber Talent, Innovation and Growth (TIG) plan, the CyberSG TIG Collaboration Centre, in collaboration with NUS Enterprise, was officially opened in July 2024 as a nexus to bring government, academia and industry together.

From left to right: Chief Executive of CSA and Commissioner of Cybersecurity, Mr David Koh, former Senior Minister of State for Digital Development and Information, Dr Janil Puthucheary, President, National University of Singapore, Professor Tan Eng Chye and Executive Director, Transformation, Innovation and Growth (TIG) Collaboration Centre and Vice President (Ecosystem Building), National University of Singapore, Professor Benjamin Tee, officially launched the CyberSG TIG Collaboration Centre on 15 July 2024.

Supporting Growth of Cyber Start-ups

CyberBoost Programme

CyberBoost helps cybersecurity firms at important stages of growth and development, by providing them with tailored support to scale their solutions in Singapore and beyond. The initiative, consisting of the CyberBoost Build and CyberBoost Catalyse programmes, was launched with key partners Plug and Play and Plexal in 2024. A total of 16 companies hailing from Singapore, the UK, the US and other regional counties have been supported through the initiative.

Group photo of CyberBoost Catalyse Cohort 1, together with CSA and Plexal.

Cybersecurity Industry Call for Innovation (CyberCall)

Since 2018, CyberCall has awarded close to S$24 million to support cybersecurity companies in developing more than 40 solutions, in areas such as cloud security, AI, IoT/OT security and privacy-enhancing technologies such as quantum-safe technologies.

Notable projects included the following:

- Protos Labs developed an AI-enabled risk analytics platform that empowered businesses to create risk management programmes encompassing cyber, data and project risks.
- SecureAge developed an AI phishing-training and endpoint solution that integrated with email clients to identify phishing emails. The solution uses machine learning technology with self-improving AI engines, to provide realistic and adaptive simulation training for companies.
- S2T developed a software solution that supports digital forensics investigations. The solution automates the tamper-proof extraction and processing of artifacts from websites and logs from cloud infrastructure.

Additionally, one of the CyberCall 2021 recipients, CyberOwl, was acquired by DNV, the world's top maritime classification society.[1]

Chief Executive of CSA and Commissioner of Cybersecurity, Mr David Koh, engaged with end users (from public and private entities) and industry technical experts, who participated in CyberCall programme.

[1] Lloyd's List, "Top 10 Classification Societies 2024,", Lloyd's List, December 4, 2024, https://www.lloydslist.com/LL1151134/Top-10-classification-societies-2024

Internationalisation of Singapore Cyber Companies

CyberGrowth Programme

CyberGrowth is a cybersecurity-focused export programme that facilitates the international expansion of promising cybersecurity firms. In 2024, a total of 27 companies participated in business missions to Malaysia, the UK and Thailand. This included the first-ever Singapore Pavilion held at CyberDSA (one of Malaysia's largest cybersecurity conferences) in collaboration with Enterprise Singapore and SGTech. A playbook for doing business in Malaysia was also published, to provide a practical guide for companies to understand the cybersecurity opportunities and landscape for doing business there.

splashtop
SPLASHTOP (SINGAPORE) PTE LTD 6704H
INSPIRE-TECH PTE LTD 6704A
eastshare

TIG Centre, together with SGTech, led the inaugural Singapore cybersecurity companies' delegates to Kuala Lumpur, Malaysia for business mission and exhibited at CyberDSA from 5 to 9 August 2024.

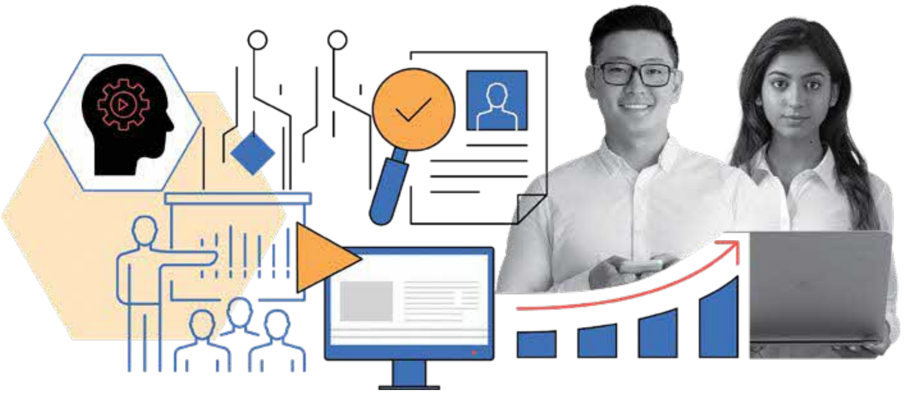
Deepening Industry Partnerships

Deepening Partnerships With Industry

As part of our multi-stakeholder approach towards cybersecurity, CSA has continued to deepen partnerships with industry stakeholders to ensure the safety and security of our digital domain. Over the past decade, CSA has substantially expanded our network of partnerships, encompassing 'Big Tech' companies, cybersecurity firms and others through signing of Memorandum of Understandings (MOUs).

In 2024, CSA entered into MOUs with Cisco, Fortinet, Recorded Future and SANS to take these respective partnerships further forward, and work together on areas of strategic interest including cyber threat intelligence sharing, securing of emerging technologies, workforce development and regional capacity building. A tripartite MOU was also signed with NTT Security Holdings Corporation and NTT Singapore Pte Ltd covering five areas: (i) Cyber Intelligence sharing, (ii) Joint cyber investigation, (iii) Technical collaboration, (iv) Capability and Research Development, and (v) Review for Enhancement.

Foundational Enabler 2: Grow a Robust Cyber Talent Pipeline



To Develop and Sustain a Skilled Cybersecurity Workforce

Cybersecurity Development Programme (CSDP)

CSA introduced the CSDP in 2020 to address the shortage of trained cybersecurity professionals. The programme equips fresh graduates and mid-career professionals with cybersecurity skills and knowledge, to contribute to Singapore's digital economy and digital government.

Officers in the 12-month programme undergo classroom training at the Singapore University of Technology and Design, Ngee Ann Polytechnic and CSA Academy. Thereafter, they will undergo the specialisation phase where they will gain real life work experiences in CSA.

As of February 2025, a total of 191 individuals have graduated from the programme, with 64 of them deployed to 24 government agencies.

CSA's 9th batch of CSDP officers.

SG Cyber Talent Initiative

Since 2015, CSA has collaborated with key partners from government agencies, associations, industry partners and academia to grow and develop the cybersecurity workforce and create job opportunities for Singaporeans. The SG Cyber Talent initiative was established in 2020 to nurture cybersecurity enthusiasts from a young age and help professionals deepen their skills. As of 2024, the initiative has helped over 22,000 individuals through cybersecurity bootcamps, mentoring, career conversion programmes and leadership education. Key programmes included:

- **Cybersecurity Education and Learning Guidebook:** The demand for skilled cybersecurity professionals continues to increase as Singapore digitalises. To increase awareness of the cybersecurity career ecosystem, CSA released the Cybersecurity Education and Learning Guidebook in 2024. The guidebook provides a comprehensive overview on industry trends, prospective career pathways and a structured learning roadmap for students, mid-career professionals as well as employers, educators and career counsellors.

- **SG Cyber Olympians:** Launched in 2022, the SG Cyber Olympians programme aims to nurture a pool of young Singaporeans with exceptional cybersecurity talent, to support Singapore's growth as a cybersecurity hub. CSA works with the cybersecurity community and educators to identify young talent and equip them with advanced cybersecurity skills, complementing the more structured educational approach in polytechnics and universities. The programme provides opportunities for these young talent to take part in cyber sparring, mentorship programmes, specialised training, and overseas competitions. As of 2024, over 50 young Singaporeans have participated in the programme.

- **SG Cyber Leaders:** In 2022, the Cybersecurity Strategic Leadership Programme (CSLP) was rolled out to equip leaders with a deep level of understanding of key global drivers shaping cybersecurity strategies and innovation, and to lead their organisations' cybersecurity functions effectively. The participants also embarked on an overseas immersion trip to the US and the UK to engage in deeper discussions with cybersecurity leaders and organisations there. Since its inception, more than 70 senior cybersecurity leaders have participated in the well-received programme.

The Project for Enhancing ASEAN-JapanCapacity Building Programme for Cybersecurity and Trusted Digital Services
NO.1 CHAMPIONS CYBER SEA GAME

In the annual Cyber SEA Games 2024, the SG Cyber Olympians participants achieved 1st placing.

CSLP participants in the UK for an overseas immersion trip to engage with cybersecurity organisations from the public and private sector.

United for Cyber Resilience: How DCCOM Strengthens Singapore's Cybersecurity

Contribution by **Digital and Intelligence Service (DIS), MINDEF**

Digital vulnerabilities, and the malicious cyber actors that prey on them, are unbounded. Across sectors and nations, they present threats to our economies, critical services and way of life. In response, we need to seamlessly coordinate our cyber defence and responses. The Ministry of Defence and the Singapore Armed Forces (MINDEF/SAF) are committed to working with CSA, government agencies, industry, and other partners to establish a secure and stable cyber environment for MINDEF/SAF and Singapore.

Former Minister for Defence Dr Ng Eng Hen officiated the inauguration of the Digital & Intelligence Service's Defence Cyber Command and SAF C4 & Digitalisation Command on 18 March 2025.

The new units inaugurated under the Defence Cyber Command, including the Cyber Protection Group.

Inauguration of DCCOM

The Defence Cyber Command (DCCOM) represents MINDEF/SAF's commitment to our collective digital security. As part of the Digital and Intelligence Service (DIS), DCCOM was newly inaugurated on 18 March 2025. By consolidating the SAF's cybersecurity operations and capabilities from across the Defence Cyber Organisation and the Cybersecurity Task Force, DCCOM will deal with hostile digital threats against Singapore from both state and non-state actors. The Cyber Protection Group (CPG) was also established under DCCOM to actively partner whole-of-government (WoG) agencies and Critical Information Infrastructure (CII) sectors and organisations, in areas such as operations, training and sharing of technical expertise to enhance overall national cyber resilience.

> **"CSA has close, longstanding collaboration with the DIS in Singapore's cyber defence. The establishment of the two Commands will further strengthen the SAF's support of Singapore's efforts."**
>
> Chief Executive of CSA and Commissioner of Cybersecurity, Mr David Koh

National-level Cyber Training

A key example of DCCOM's contribution in strengthening cross-agency partnerships and training is the Critical Infrastructure Defence Exercise (CIDeX). CIDeX is co-organised with CSA as part of the National Cyber Exercise Programme. The third iteration in 2024 saw over 200 participants from WoG, the CIIs and industry partners exercising our collective responses towards real-world cyberattack scenarios, across seven indigenously-developed testbeds. This helps to sharpen our participants' skills and readiness against ever-evolving cyber threats, and build trust and relationships across different organisations. DCCOM will continue to build upon this strong foundation, to integrate emerging technologies for greater realism and complexity of exercise scenarios. To this end, the SAF Digital Range aims to provide realistic, high-fidelity simulations of sophisticated cyber threats, for effective training of our national cyber defenders.

Group photo of CIDeX 2024, comprising MINDEF/SAF, CSA, WoG, CIIs, industry and academia participants.

Foreign Partnerships

Beyond forging local partnerships, DCCOM is also committed to deepening ties with other military cyber forces, to improve our collective resilience in the borderless cyber domain. In 2024, the DIS formed a joint team with Germany's Cyber and Information Domain Service (CIDS), for Exercise Locked Shields (XLS) organised by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). As the world's largest live-firing cyber defence exercise, 4,000 experts from over 40 countries participated in XLS 2024. Through the exercise, we were able to validate and enhance our incident response protocols, as well as benchmark ourselves against leading international cyber forces.

In our inaugural participation in Exercise Locked Shields 2024, we formed a joint team with our German Cyber and Information Domain Service (CIDS) counterparts, defending against real-time cyber threats in a live-firing environment.

Developing the Talent Pipeline

DCCOM is also committed to growing Singapore's military cyber expertise. This begins with identifying and nurturing the next generation of cyber defenders through the Sentinel Programme - a structured youth talent development initiative that works closely with educational institutions, industry partners and government agencies to develop promising cyber talents from an early age. Full-time National Servicemen in our Cyber Work-Learn Schemes perform operational cyber roles while attaining academic credits to their cyber-related polytechnic diploma or university degree. Through the SAF's Enhanced Expertise Deployment Scheme, Operationally Ready National Servicemen with cyber expertise may opt to be redeployed to relevant roles within the DIS, to deploy their cyber skills for national security.

Senior Minister of State for Defence Mr Zaqy Mohamad at the launch of the Sentinel Programme in 2024 with DIS partners in the Defence Technology Community and Ministry of Education.

Students put their cybersecurity skills and knowledge to the test at the inter-school Sentinel Challenge 2024.

Securing Singapore's Digital Future

DCCOM's establishment contributes to Singapore's ability to address the complexities of modern cyber threats. By fostering partnerships across WoG and international partners, and through initiatives like CIDeX, DCCOM embraces the need for unity, innovation, and preparation alongside our valued ecosystem partners to ensure that the nation's critical systems remain resilient. Together with our partners, DCCOM is committed to safeguarding Singapore and enhancing its readiness to face evolving cyber challenges.

> **"Cyber Defence is a team sport – we look forward to contributing as part of Team Singapore."**
>
> Defence Cyber Chief/Comd DCCOM,
> COL Clarence Cai

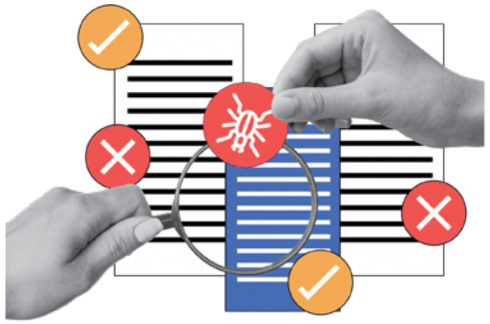
Beyond the Firewall: The Essential Role of Red Teaming in Government Cybersecurity

Contribution by **Government Technology Agency of Singapore (GovTech)**

The Singapore Government's digitalisation drive has made accessing Government services easier and more seamless for businesses and citizens. However, as these digital services become more accessible and ubiquitous, cyber threats also become correspondingly more prevalent. While traditional cybersecurity measures – such as firewalls, intrusion detection systems, and antivirus software – help defend against known threats, they often fall short against sophisticated adversaries who exploit zero-day vulnerabilities and use social engineering tactics. This is because these solutions rely on detecting familiar attack patterns, making them less effective against novel and highly targeted threats. To stay ahead, Government must adopt a proactive approach, simulating real-world attacks to uncover weaknesses before threat actors can exploit them. Red teaming is one such cybersecurity capability which can strengthen overall cybersecurity.

What is Red Teaming?

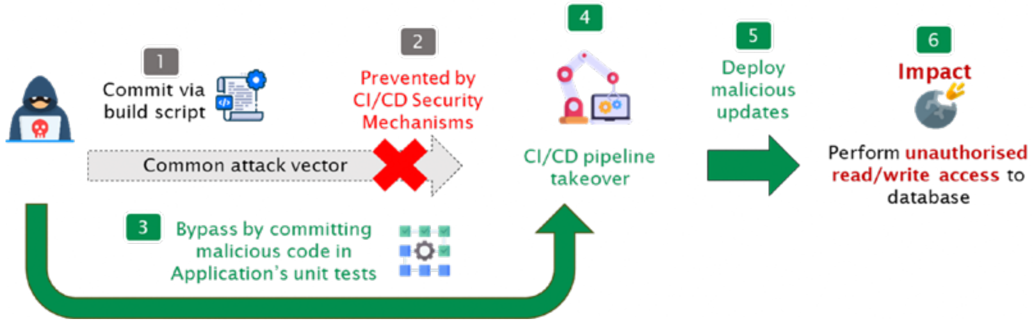
Red teaming is a specialised form of cybersecurity testing designed to help organisations identify vulnerabilities, test response capabilities and strengthen security posture. Unlike penetration testing, which primarily identifies technical vulnerabilities, red teaming simulates the modus operandi of actual threat actors - mimicking their objectives, behaviour and tactics, techniques and procedures (TTPs). Red teaming, therefore, aims to exploit weaknesses in an organisation's security through means such as spear phishing, code injection and process alteration to demonstrate proofs of data exfiltration, system disruption, and unauthorised access to systems. The outcome of a successful red team exercise is to provide organisations with a good sense of its state of cybersecurity. Through this, the organisation will have a better understanding of where the weaknesses are in its people, processes and technologies.



The Collaborative Nature of Red Teaming

Effective red teaming is not only about identifying vulnerabilities – it is a consultative and collaborative effort between the red team and system owners to improve overall security. The process begins with a structured engagement, where both parties define clear objectives and agree on the parameters of the exercise to ensure alignment with business needs.

To achieve robust testing, the red team simulates the most relevant TTPs that adversaries might use. This may involve several weeks of reconnaissance to gather intelligence on the target system or network architecture and identify potential weaknesses which could serve as entry points. Once inside, the red team leverages its understanding of the network to escalate privileges, move laterally across systems, and work towards its objectives. The goal is therefore not to "break" the system but to test its security under realistic attack scenarios, providing actionable insights to help agencies strengthen their defences.


1
Commit via build script
Common attack vector
2
Prevented by CI/CD Security Mechanisms
3
Bypass by committing malicious code in Application's unit tests
4
CI/CD pipeline takeover
5
Deploy malicious updates
6
Impact
Perform unauthorised read/write access to database

Schematic of Red Team's Test that uncovered the weakness, which was remediated by the affected agency.

Throughout the exercise, system owners receive updates on attack progress and collaborate with the red team to implement remediation measures. Findings are documented in a final report, detailing the vulnerabilities discovered, attack paths used and the potential impact of a successful attack. This report serves as a roadmap for the organisation to strengthen its security posture, prioritising remediation efforts based on the severity and likelihood of exploitation.

Delivering Value to Agencies and Citizens

GovTech supports Government agencies in the conduct of red teaming on systems and services including those which are used to deliver e-services to our citizens and businesses. These red teaming exercises help agencies uncover potential vulnerabilities in Government systems which are not obvious to normal users. In one such collaboration with a Singapore Government agency, the Red Team was able to uncover a potential weakness in the agency's development pipeline which allowed potential attackers to embed malicious code in their system's automated test unit – the mechanism which verified software quality – to manipulate the code-checking process. Such a weakness could have been exploited by a threat actor to deploy unauthorised updates and gain illicit access to sensitive data. The discovery prompted the agency project team to modify the identity and access management (IAM) rules of the automated test unit, ensuring that only authorised users can access the unit.

Tapping on the Wider Ecosystem

Protecting the Government's vast and diverse digital infrastructure requires an expansion of testing capacity beyond GovTech's internal red teams. To leverage the expertise of the global white-hat hacker community, GovTech runs the Government Bug Bounty Programme (GBBP), inviting researchers from around the world to identify security flaws in public-facing Government systems. These researchers contribute a wide array of skills and attack techniques, significantly enhancing the Government's ability to detect and address vulnerabilities. Over the years, this responsible disclosure programme has played a crucial role in uncovering potential vulnerabilities across Government systems and digital services.

Conclusion

Securing Government systems against cyber threats continues to be an ongoing race with increasing digitalisation and evolving cyber threats. To stay ahead of cyber threats, we employ a range of strategies, including the use of red teaming and the GBBP, to provide a proactive and realistic approach to identify vulnerabilities and strengthen cybersecurity postures of Government systems. As the cyber landscape continues to evolve, these proactive cybersecurity measures ensure that Government systems remain resilient and capable of withstanding emerging threats.

TOMORROW'S DIGITAL SECURITY CHALLENGES

The cyber threat landscape has evolved dramatically since CSA's inception a decade ago. This chapter looks at its evolution from the varied perspectives of academia, as well as the private and public sectors. This chapter begins with a reflection from the private sector by Mr Huang Shao Fei, Group Chief Information Security Officer of SMRT Corporation (SMRT), on Singapore's cybersecurity manpower development over the years and what he envisages is the future of our cybersecurity talent ecosystem. Next, Mr Benjamin Ang, Head, Centre of Excellence for National Security (CENS), and Future Issues and Technology at the S. Rajaratnam School of International Studies (RSIS) of Nanyang Technological University (NTU), shares his perspectives on the increasingly prevalent problem of supply chain cyber-attacks through the analogy of heavily locked doors with weak hinges. The chapter then concludes with an article by Mr Willis Lim, Director of the National Cyber Threat Analysis Centre (NCTAC) at CSA, titled "Looking Back to See Ahead", reflecting on CSA's forecasts of key cybersecurity trends and emerging issues over the past five years, and analysing how those predictions have panned out.

Reflecting on Singapore's Cybersecurity Progress

Contribution by **Mr Huang Shao Fei,** Group Chief Information Security Officer, SMRT Corporation (SMRT); Vice-Chair, Cybersecurity Committee, International Association of Public Transport (UITP); Immediate Past-President, Cybersecurity Chapter, Singapore Computer Society (SCS)

Having spent the last 25 years in the trenches of cybersecurity, I have had the privilege of witnessing the remarkable journey of Singapore's cybersecurity ecosystem. It is a story of unrelenting dedication to fostering and sustaining partnerships between the public and private sectors, alongside communities of cybersecurity hobbyists, enthusiasts, and professionals. This ecosystem plays a critical role in reinforcing Singapore's position as a global digital and cybersecurity hub, while simultaneously elevating the world's recognition of our expertise and capabilities in this field.

Reflecting on Singapore's Cybersecurity Progress

One of the evolving threats in Singapore, and indeed the world, is the ongoing battle with ransomware. This form of malicious software, which encrypts a victim's data and demands ransom for its release, has been a persistent threat since the 1980s. Despite the evolving technology behind ransomware, the fact that this issue has endured for decades suggests that we may be missing a key aspect of the solution.

What could that be?

In my view, cybersecurity is not merely a technical issue – it is a broader, systemic challenge that requires the collective effort of the entire ecosystem. This means that the public and private sectors, as well as the broader community, must work together to improve cybersecurity.

The Singapore Cybersecurity Ecosystem's Roles and Progress

In the 1990s, the only avenue for obtaining a cybersecurity education was self-study through the limited resources available, acquiring experience on the job, or learning from others with a similar interest in the field. Since then, the landscape of cybersecurity education has transformed dramatically, with numerous academic programmes, certifications, and online courses now available to aspiring professionals. However, communities of cybersecurity hobbyists, enthusiasts, and professionals remain a crucial nexus of learning for those committed to mastering the craft.

Beyond providing a platform for education, these communities play an important role in advancing professional development. They offer opportunities for individuals to meet, network, and grow professionally. In some cases, these communities give their members a voice, providing valuable industry feedback during public consultations on cybersecurity issues or offering advice to the general public. It is indeed heartening to see how our communities have expanded and strengthened over the years. For instance, in the past two decades, we have seen the formation of a growing number of professional associations dedicated to the cybersecurity ecosystem. A testament to the increasing importance of community partnerships is the formation of the Singapore Cyber Security Inter-Association (SCIA) by the Association of Information Security Professionals (AiSP). This collaborative body fosters closer cooperation across professional and industry associations, including the (a) Centre for Strategic Cyberspace + International Studies (CSCIS); (b) Cloud Security Alliance (CSA) Singapore Chapter; (c) Information Systems Audit and Control Association (ISACA) Singapore Chapter; (d) International Information System Security Certification Consortium (ISC2) Singapore Chapter; (e) Law Society of Singapore; (f) Singapore Computer Society (SCS); (g) SGTech, and (h) Operational Technology Information and Sharing and Analysis Center (OT-ISAC).

In addition, many volunteer-run cybersecurity communities have emerged and grown in recent years. One such example is Division Zero (Div0), which boasts over 4,300 members in its Meetup community. Other noteworthy communities include Cyber Youth Singapore (CYS) – a youth-led national movement – and N0H4TS, another youth-oriented cybersecurity group. There are also numerous other communities such as null Singapore and the OWASP Singapore Chapter.

It is an exciting time to be part of Singapore's cybersecurity landscape, and we can expect our communities to continue becoming more inclusive and diverse as we look to the future!

The Future of Singapore's Cybersecurity Ecosystem

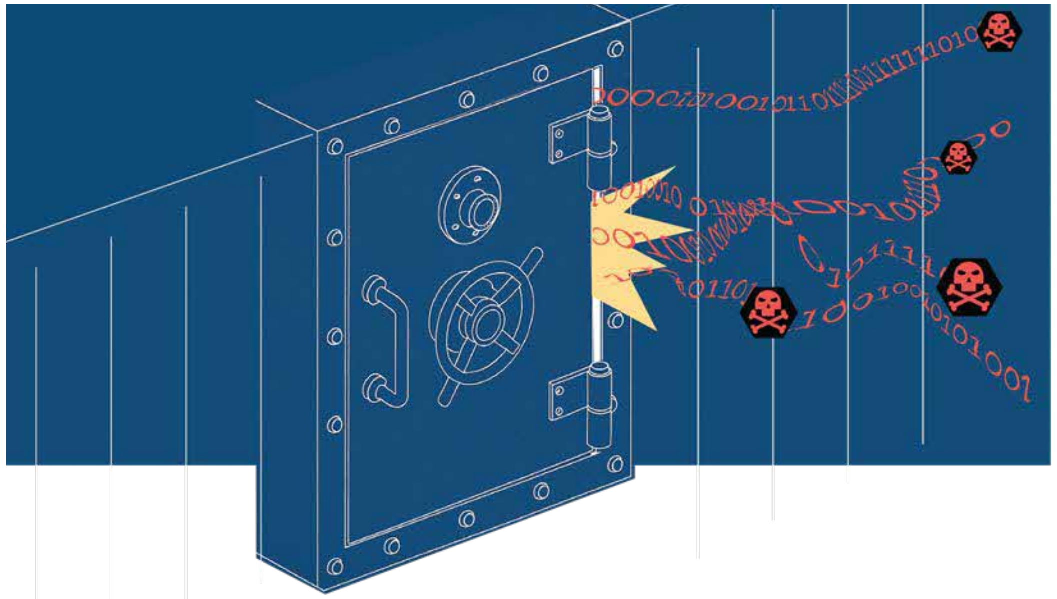
Looking ahead, the Singapore cybersecurity ecosystem will need to anticipate and address new and emerging challenges. As the saying goes, "to go far, go together." Building and maintaining strong partnerships between the public and private sectors, alongside nurturing collaboration with cybersecurity communities, will be essential in creating and sustaining a resilient cybersecurity future.

In November 2024, the Cyber Security Agency of Singapore (CSA) launched a study aimed at enhancing the productivity and professionalism of cybersecurity workers, including the feasibility of developing a professional framework for the sector. It is encouraging to note that CSA formed a tripartite advisory group, comprising industry players, training institutions, and certification bodies, to contribute to this important study. Moreover, the challenges in cyberspace are not limited to large enterprises and government organisations alone. From the average person to every industry, both large and small, cyber threats are indiscriminate. The rapid adoption of generative AI and the corresponding rise in new cyber threats serve as a stark reminder that we must act collectively as an ecosystem to combat these dangers.

Facing the Future Together

In conclusion, even if we may not be able to fully stay ahead of all emerging cyber threats, the cybersecurity ecosystem established and led by CSA will play a critical role in strengthening Singapore's position as a global digital and cybersecurity hub, while simultaneously enhancing global recognition of our expertise and capabilities in this vital field.

Heavily Locked Doors With Weak Hinges – The Problem of Supply Chain Cyber-Attacks



Contribution by **Mr Benjamin Ang**, Head, Centre of Excellence for National Security (CENS), and Future Issues and Technology, S. Rajaratnam School of International Studies (RSIS) of Nanyang Technological University (NTU)

As we read various annual cyber threat landscape reports and are reminded of the dire state of cybersecurity, most of us also know some of the recommended best practices to improve our cyber hygiene: We should regularly (preferably automatically) update our software applications and operating systems to patch vulnerabilities. We should implement firewalls to control network access and monitor our networks for suspicious activity. We should install antivirus and anti-malware software on our devices.

But what should we do when the tools that we use to secure ourselves become the threats?

Solarwinds Breach and CrowdStrike Outage

For example, thousands of high-value organisations, government agencies, and major corporations, including Microsoft and FireEye, used the Orion software by SolarWinds to monitor their networks, and they dutifully downloaded updates to Orion. But in 2020, they discovered that attackers had gained access to them through malicious code planted in a routine Orion software update.

Airlines, airports, hospitals, and hundreds of other organisations trusted the Falcon software by CrowdStrike to keep their devices safe, but in 2024, a faulty update to Falcon caused a worldwide outage and widespread disruption. Airlines had to delay or cancel flights, affecting hundreds of thousands of passengers. This was not a cyber-attack, but it illustrated how a mistake by a trusted supplier can disrupt the services that depend on it, as well as the lives of countless people.

Third Party Vendors and Supply Chain Risks

Any organisation that depends on third party vendors (i.e. every organisation in the modern world) is therefore vulnerable to supply chain attacks. This extends to those carried out through physical means, where attackers infiltrate commonly used hardware to insert security flaws. Former US National Security Agency (NSA) contractor Edward Snowden leaked documents which alleged that the NSA had intercepted deliveries of hard drives, routers, and other devices from companies such as Cisco, Dell, Western Digital, Seagate, Maxtor, Samsung, and Huawei to plant backdoors to enable access to thousands of computer systems that used those devices.

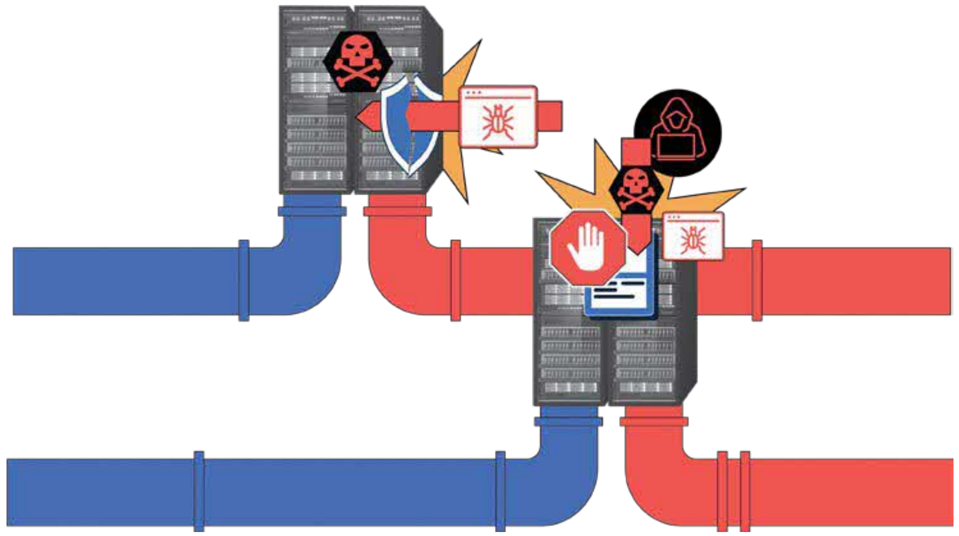
These supply chain attacks are insidious and cascading because the adversary does not need to directly attack the end target(s), which may be too well-protected or geographically dispersed. Instead, the attacker goes further upstream, to infiltrate a trusted supplier which is less secure, then uses this access to compromise the target(s), which could be the organisations we transact with every day, or even ourselves.

We can think of supply chain cyber-attacks as targeting heavily locked doors with weak hinges; attackers bypass an organisation's strong security (strong locks) by going through vendors that have weak security (weak hinges).

Reducing Supply Chain Risks

There are several recommended practices to reduce the supply chain attack risks: Organisations can limit or monitor the access that vendors have to critical parts of their networks, implement zero trust architecture, and train staff to observe good cyber hygiene – just as we might add more locks or additional layers of doors in a building. They can also try to reinforce the "weak hinges" by evaluating vendors for cybersecurity risk and imposing contractual obligations on them. But this is where we see how deeply embedded supply chain vulnerabilities can be.

One example is the vulnerability discovered in the very commonly used open-source software Log4j in 2021, which could give attackers complete control of any system that uses software containing Log4j. This includes widely used Apache web servers, and even security products from Cisco, Symantec, Amazon, F-Secure, McAfee, TrendMicro, and dozens more. Unfortunately, Log4j has been ubiquitous to software development for many years, so it has been embedded into countless software components, and deeply integrated into numerous applications, making it challenging to identify all instances where it has been used. Although the vulnerability



was discovered four years ago, many systems remain unpatched today, because organisations do not know if or where Log4j has been used in their systems.

Software Bill of Materials (SBOM) and CSA's SBOM Advisory

This indicates a need for developers to provide SBOMs, which list and provide full visibility of all software components, so that organisations who use the software can identify their vulnerabilities better, and developers can fix components faster. Unfortunately, generating SBOMs is a laborious process. Recent studies suggest that about 60% of developers are not generating SBOMs, while only 10% of customers are asking for them!

No wonder that the Cyber Security Agency of Singapore (CSA) saw the need to issue an "Advisory on Software Bill of Materials and Real-time Vulnerability Monitoring for Open-Source Software and Third-Party Dependencies" in February 2025 to provide guidance to software developers on how to use automated tools from the start and throughout the development process to generate SBOMs. This is crucial because studies suggest software development projects have an average of 68.81 third-party dependencies per project, and 5.12 critical vulnerabilities per application, which make it unfeasible for humans to manually create SBOMs. Automation may be the most sustainable way to mitigate the supply chain risks from vulnerabilities in open source and third-party software.

However, the advisory also acknowledges the practical limits of SBOMs. For example, if the codebase includes obscure languages, then automated tools may not detect some dependencies; developers may have difficulty obtaining SBOM from software-as-a-service (SaaS) vendors and closed-source software; and developers may find many false positives that are not exploited in their environments, instead wasting time on unnecessary remediation.

Multiple Mitigation Measures for Resilience

Since there is always a possibility of a breach or disruption, while we need strong locks (strong cybersecurity posture) and ways of identifying weak hinges (through SBOMs), we also need incident response plans and business continuity plans for times when the doors, locks, or hinges fail. This may include endpoint detection and response, to spot intruders who have entered; redundant systems and backups, to replace what has been tampered with; and alternative suppliers, to step in where one has failed.

In an extreme case, during the CrowdStrike outage, dozens of airlines switched to manual paper-based check-ins. Although netizens initially laughed at this simple offline method, these airlines got passengers to their destinations more effectively than other airlines which had no contingency plans at all. In our complex, interconnected world, sometimes a simple plan can help build resilience too.

Looking Back to See Ahead

Contribution by **Mr Willis Lim**, Director of National Cyber Threat Analysis Centre (NCTAC), Cyber Security Agency of Singapore (CSA)

Over the past five years, CSA has traditionally forecasted what we believe to be key cybersecurity trends and emerging issues that will have a large impact in the years to come. These forecasts have proven insightful, but not all of our 'predictions' have materialised as expected. This article analyses six trends forecasted in previous Singapore Cyber Landscape (SCL) reports for the accuracy of their predictions.

Top Prize

Ransomware: An Escalating Threat (SCL2020)

In 2020, we highlighted ransomware as an increasingly serious cyber threat, expecting it to evolve beyond simple file encryption into more sophisticated extortion tactics. This prediction proved highly accurate. The years that followed saw the rise of ransomware-as-a-service (RaaS), double extortion models where stolen data is leaked publicly, and even triple extortion, where attackers pressure victims through additional means, such as distributed denial-of-service (DDoS) attacks.

Singapore was not spared, with ransomware incidents affecting various sectors, including healthcare and manufacturing. The continued rise of these attacks reinforces the need for strong cyber hygiene, timely patching, and robust backup strategies to mitigate risks.

Runner Up

Supply Chain Attacks: A Growing Concern (SCL2019)

In 2019, we pointed to the increasing risk of supply chain attacks, where adversaries compromise third-party vendors or software providers to infiltrate their targets. This concern became a reality in major incidents such as the SolarWinds breach in 2020 and the Kaseya ransomware attack in 2021.

In Singapore, we observed a growing number of incidents where attackers exploited third-party relationships to bypass traditional defenses. As organisations become more reliant on cloud services and external vendors, this remains a key area of concern. It is clear that supply chain security must be a priority, with stronger vetting of vendors, better monitoring of software updates, and more stringent cybersecurity requirements across interconnected ecosystems.

2nd Runner Up

Internet of Things (IoT) Vulnerabilities (SCL2019)

In our 2019 report, we anticipated that the rapid proliferation of IoT devices would present new cybersecurity challenges. This trend has continued to unfold, with a surge in IoT-related vulnerabilities and the growing use of botnets such as Mirai to exploit unsecured devices.

While IoT security has improved with better regulations and industry standards, many devices remain vulnerable due to weak authentication, outdated firmware, and a lack of visibility into connected networks. As 5G adoption expands and smart cities become more interconnected, the need for robust IoT security frameworks will only become more pressing.

Best Newcomer Award

Artificial Intelligence (AI) in Cybersecurity: A Double-Edged Sword (SCL2022)

AI was identified in SCL2022 as a transformative force in cybersecurity – both as a defence mechanism and as a tool for attackers. This prediction has largely held true. AI-driven security solutions have improved threat detection and automated responses, but at the same time, cybercriminals have leveraged AI for more convincing phishing campaigns, deepfake social engineering attacks, and automated malware generation.

As generative AI tools become more accessible, we expect to see more sophisticated cyber threats leveraging AI capabilities. Organisations must balance the advantages of AI-powered security with the need to defend against AI-enabled attacks.

"Not Quite What We Anticipated" Award

The Targeting of Remote Workforce (SCL2020)

When remote work became the norm during the COVID-19 pandemic, we anticipated a surge in cyber threats targeting home networks and personal devices. This proved to be an accurate forecast, with a significant rise in phishing attacks, business email compromise (BEC) scams, and virtual private network (VPN) exploits. However, one unexpected development in recent years has been the emergence of fake North Korean IT workers infiltrating global companies.

These threat actors disguise themselves as freelance developers or remote employees, gaining access to company networks while covertly funneling funds to the North Korean regime. This highlights the evolving nature of threats in remote work environments, reinforcing the importance of identity verification and continuous monitoring of remote access.

Supply-Chain Attacks: A Growing Concern (SCL2019)
...supply chain attacks grew by almost 80 percent in 2018...
RUNNER UP
Ransomware: An Escalating Threat (SCL2020)
The pervasiveness of ransomware was never more pronounced... as ransomware cartels innovated their tactics at an accelerating pace...
TOP PRIZE
Internet of Things (IoT) Vulnerabilities (SCL2019)
Additionally, the versatility of 5G and its wide range of applications is expected to bring about a surge in IoT devices...
2ND RUNNER UP

Wide Off the Mark (For Now)

The Emergence of Web3 and Metaverse Security Risks (SCL2021)

In SCL2021, we explored the cybersecurity implications of Web3 and the metaverse, acknowledging that while these technologies were still developing, they could introduce new attack vectors. So far, we have seen some early indicators of these risks, such as blockchain-based scams, vulnerabilities in decentralised finance (DeFi) platforms, and security flaws in smart contracts.

However, large-scale metaverse-related cyber threats have yet to materialise. It remains too early to determine the full extent of security challenges in these spaces, but as adoption grows, cybercriminals will likely explore new ways to exploit virtual environments. We continue to monitor this area closely, particularly in terms of identity security and financial fraud in decentralised systems.

Conclusion

Our forecasted trends have been a mix of Nostradamus-level predictions and forward-looking guesses. The rise of ransomware, supply chain attacks, IoT-related threats, and targeting of remote work vulnerabilities were spot-on, while the cybersecurity implications of Web3 and the metaverse are still brewing.

Recent twists, like fake North Korean IT workers and generative AI's dark side, show just how unpredictable the cyber landscape can be. The interconnectedness of our digital lives means that staying ahead of these trends is no longer optional but essential. The future will always be unpredictable, but that's no reason to stop preparing for it. Here's to staying one step ahead of the hackers — or at least giving them a run for their (stolen) money.

CSA's journey continues at

PUNGGOL DIGITAL DISTRICT

In 2026, CSA will move to our new premises and permanent home at the Punggol Digital District. Join us there to help secure cyberspace, collaborate on groundbreaking achievements, and shape tomorrow's digital landscape.

CSA SINGAPORE | 10 YEARS OF SECURING OUR CYBERSPACE

We value your thoughts

To provide feedback on the Singapore Cyber Landscape publication, please scan the QR code or go to the following URL: https://go.gov.sg/scl2024-25

CSA SINGAPORE
Cyber Security Agency of Singapore

10 YEARS OF SECURING OUR CYBERSPACE

www.csa.gov.sg