香港警務處
網絡安全及科技罪案調查科
Hong Kong Police Force
Cyber Security and Technology Crime Bureau

CYBERSECURITY REPORT
網絡安全報告
2024

創新引領　護網守城
共築防線　賦能未來

Leading with Innovation

Securing the Cyberspace

Forging United Defence

Empowering the Future

目錄 TABLE OF CONTENTS

序言 Foreword

香港警務處網絡安全及科技罪案調查科（網罪科）踏入十周年，標誌了一個重要的里程碑，藉此本人首先衷心感謝網罪科人員及各界持份者過去的貢獻及支持。與此同時，本人謹代表網罪科發表首份網絡安全報告2024，簡報香港過去一年的網絡安全形勢，以及未來將面對的挑戰與機遇。過去十年，網罪科與時並進、積極創新、持續推動香港網絡安全生態發展，應對不斷演變的網絡威脅，致力守護香港的網絡安全環境，為香港繼續是世界上其中一個最安全及穩定的社會作出重要貢獻。

回望2024年，國際間的地緣政治令全球局勢變幻莫測。維護國家安全的工作尤其重要，而網絡安全更是密不可分的重要一環。去年，有網絡安全機構估計全球因網絡犯罪而導致經濟損失高達9.5兆美元。香港作為開放型經濟體，全方位與全球國家地區城市互聯互通。面對全球網絡安全威脅持續上升，香港亦不能置身事外。

就本港情況而言，網罪科於2024年錄得超過33 000宗科技罪案，佔香港整體罪案率三成五。相關累計損失金額超過51億港元，較2023年稍為回落，但依然處於近年歷史高位，當中超過八成為網絡詐騙。同年，網罪科網絡安全中心處理及分析逾2 500萬項網絡威脅情報，當中針對香港的攻擊有超過44萬項。儘管網罪科能透過嚴謹的網絡防禦機制進行適時通報及攔截，但數字高企反映網絡威脅風險絕對不容忽視，亦提醒各界持份者必須持續提升網絡防禦能力，應對時刻來襲的網絡攻擊。

宏觀過去幾年，網絡威脅以幾何級數增長，背後主要原因離不開創新科技武器化及網絡犯罪產業化。為應對未來威脅，網罪科早年已引入新世代創新科技，並強化網絡情報蒐集與共享能力。有見及此，網罪科過去兩年已先後成立「科技罪案警政顧問小組」及「網絡安全特別行動小組」。於2024年下旬，網罪科更成立了「網絡安全行動中心聯盟」，以新世代創新科技作支撐，匯聚大型及重要基礎設施，為香港建立全面化網絡威脅情報交流平台。來年，網罪科將融合更多創新技術於智慧警政，推進未來預測性警務工作，並持續深化香港網絡安全生態發展。

同樣地，國際合作對打擊跨境網絡犯罪活動極為重要。去年，國際刑警組織網絡犯罪總局委任本人為亞洲及南太平洋網絡犯罪聯合工作小組副主席，推動與其他24個國家及地區的執法機構共同制訂打擊網絡犯罪的策略，深化情報交流及提升跨境聯合行動能力。多年間，網罪科亦多次與網絡犯罪總局合辦網絡犯罪首長級工作坊、雙邊及多邊會議、網絡指揮官課程，以及執行跨國跨境聯合行動及網絡安全演練。

This year marks a significant milestone – the 10th anniversary of the Cyber Security and Technology Crime Bureau (“CSTCB”). I would like to take this opportunity to express my heartfelt gratitude to CSTCB officers and stakeholders from various sectors for their contributions and support over the years. It gives me great pleasure to launch the first CSTCB Cybersecurity Report 2024, which outlines the cybersecurity landscape in Hong Kong over the past year as well as the challenges and opportunities ahead. Over the past decade, CSTCB has kept abreast of the developments, proactively innovated, and continuously strengthened Hong Kong’s cybersecurity ecosystem to combat the ever-evolving cyber threats. Through this, CSTCB has made a significant contribution to safeguarding Hong Kong’s cyberspace and maintaining its position as one of the safest and most stable societies in the world.

Looking back at 2024, the international geopolitical situation has been unceasingly dynamic. Safeguarding national security is more crucial than ever, with cybersecurity being an integral part of this effort. A cybersecurity organisation estimated that the global economic losses from cybercrime in 2024 reached a staggering US$9.5 trillion. As an open economy, Hong Kong is interconnected with countries and cities around the world on all fronts. In the face of growing global cybersecurity threats, Hong Kong cannot afford to stay aloof.

In 2024, Hong Kong recorded over 33,000 technology crime cases, accounting for 35% of the overall crime rate in Hong Kong. The total financial losses exceeded HK$5.1 billion, reflecting a slight decrease compared to 2023 but still remaining at a record high in recent years. More than 80% of these technology crimes cases were online deception. At the same time, the Cyber Security Centre of CSTCB handled and analysed over 25 million pieces of cyber threat intelligence, more than 440,000 of which targeted Hong Kong specifically. Despite CSTCB’s ability to give timely notifications and take preventive measures through robust cyber defence systems, these figures reflect that the risk of cyber threats must not be taken lightly. This serves as a reminder that we must continually enhance our cyber defence capabilities to respond to the constant threat of cyberattacks.

In a broader sense, cyber threats have been growing exponentially over the past few years, largely due to the weaponisation of innovative technologies and the industrialisation of cybercrime-as-a-service. To cope with future threats, CSTCB has, for years, adopted next-generation innovative technologies and strengthened its cyber intelligence gathering and sharing capabilities. In response, CSTCB established the Cybercrime Policing Advisory Panel and the Cyber Security Action Task Force in the past two years. In late 2024, CSTCB launched the Security Operation Centre Alliance (SOCA) to build a comprehensive cyber threat intelligence exchange platform for Hong Kong, underpinned by next-generation technologies. This platform has integrated large-scale and critical infrastructures, providing a unified approach to cybersecurity. In the coming year, CSTCB will further integrate innovative technologies into smart policing to enhance predictive capabilities in policing efforts and strengthen Hong Kong’s cybersecurity ecosystem.

Simultaneously, international cooperation remains pivotal in combating cross-border cybercrime. Last year, I was appointed Vice-Chairperson of the Asia and South Pacific Joint Operations on Cybercrime Working Group by Cybercrime Directorate of INTERPOL to develop strategies to combat cybercrime with law enforcement agencies from 24 other member jurisdictions, deepen the exchange of intelligence and enhance the capability of cross-border operational collaboration. Over the years, CSTCB has also co-organised with the Cybercrime Directorate several Cybercrime Directors’ workshops, bilateral and multilateral meetings, cyber command courses, as well as transnational and cross-border joint operations and cybersecurity exercises.

與此同時，法律基礎更是打擊網絡犯罪中不可或缺的部份。經過警務處、保安局、數字政策辦公室及律政司的緊密合作，《保護關鍵基礎設施（電腦系統）條例》亦於2025年3月獲立法會三讀通過，預計於2026年1月1日生效。除此之外，本人亦積極參與法律改革委員會的工作，透過電腦網絡罪行小組委員會進行研究，找出電腦網絡迅速發展帶來的挑戰，檢討現有法例和其他相關措施，參考其他司法管轄區的相關發展，並作出適當的法律改革建議，為未來更有效打擊新型網絡犯罪奠下堅實基礎。

為提升整體網絡安全實踐能力，網罪科去年舉行了多項大型演練，包括代號「戰風行動」、由國際刑警組織、新加坡及澳門當局，以及多家重要基礎設施參與的網絡及實體反恐聯合演練，以及超過70個政府部門參與的跨部門網絡安全演練。此外，與業界緊密合作同樣是成功應對網絡威脅的重要基礎。網罪科透過定期舉辦網絡安全研討會，釣魚電郵演習、狩網運動、網絡攻防精英培訓暨攻防大賽等活動，成功凝聚各界持份者提高系統安全意識，主動查找系統安全漏洞，增強整體網絡韌性，以提升香港整體網絡安全水平。

提高公眾網絡安全意識，及早介入更是防範網絡犯罪的深層工作。網罪科於2024年大幅提升「防騙視伏器」及應用程式的功能，包括自動檢測詐騙電話及網站、公眾舉報平台及人工智能分析工具等功能，來年亦會持續推出新功能保護公眾免於網絡陷阱。此外，網罪科亦聯動過百家公私營機構合作參與「守網聯盟」宣傳計劃，並舉辦「大灣區青少年人工智能及網絡安全挑戰賽」和「全城反詐嘉年華」，培養市民大眾、尤其是年青人的網絡素養及網絡安全意識。

展望未來，網罪科將繼續以堅韌不拔的精神，以創新引領網絡安全生態發展，以護網守城為目標與持份者共築網絡安全防線，為智慧城市發展提供堅實安全保障，以實現賦能未來的願景。最後，本人再次感謝各界持份者的鼎力支持，亦期望未來共同持續守護香港網絡安全。

At the same time, a solid legal foundation is an indispensable part of the fight against cybercrime. Through close collaboration between the Hong Kong Police Force (HKPF), the Security Bureau, the Digital Policy Office and the Department of Justice, the Protection of Critical Infrastructures (Computer Systems) Bill passed its third reading in the Legislative Council in March 2025 and is expected to come into effect on 1 January 2026. Apart from that, I have also actively participated in the work of the Law Reform Commission by conducting comprehensive research through the Cybercrime Sub-committee. This initiative aims to identify the challenges brought about by the rapid development of information technology, review existing laws and measures, and propose necessary reforms with reference to the relevant developments in other jurisdictions to ensure Hong Kong’s legal framework remains robust against emerging cyber threats.

To enhance overall cybersecurity capabilities, CSTCB conducted several large-scale exercises throughout the year. This included the cross-border “BATTLEAIR” Counter Cyber and Physical Terrorism Joint Exercise, in collaboration with INTERPOL, Singapore, and Macao authorities, as well as the Inter-departmental Cyber Security Drill involving more than 70 government bureaux and departments. Additionally, close co-operation with all sectors is also an important foundation for tackling cyber threats successfully. Through regular cybersecurity seminars, Ethical Phishing Email Campaign, BugHunting Campaign, and Cyber Attack and Defence Elite Training cum Tournament, CSTCB has successfully rallied stakeholders from various sectors to raise their awareness of system security, proactively identify system vulnerabilities and enhance overall cyber resilience, thereby enhancing Hong Kong’s overall cybersecurity posture.

To raise public cybersecurity awareness, early intervention is essential for preventing cybercrime. In 2024, we significantly upgraded the Scameter and its mobile application, introducing new features such as automatic detection of scam calls and websites, a public intelligence reporting platform, and AI-powered analytic tools. Moving forward, we will roll out new functions to enhance the protection of the public from cyber pitfalls. Moreover, CSTCB joined hands with over 100 public and private organisations to launch the CyberDefenders’ Alliance, a publicity initiative, and hosted the Greater Bay Area Youth Artificial Intelligence and Cyber Security Challenge as well as the Anti-Scam Carnival, effectively enhancing cybersecurity awareness among the general public, particularly the youth.

Looking forward, CSTCB will continue to lead the development of the cybersecurity ecosystem through innovation with resilience and determination, and build a robust cybersecurity defence community with the goal of securing the cyberspace. We will provide solid security for the development of the smart city to realise the vision of empowering the future. Finally, I wish to express my heartfelt gratitude to all stakeholders for their unwavering support, and I look forward to safeguarding Hong Kong’s cybersecurity sustainably in the future.

林焯豪
Raymond LAM
香港警務處
網絡安全及科技罪案調查科總警司
Chief Superintendent of Police
Cyber Security and Technology Crime Bureau
Hong Kong Police Force

專業見解

Key Insights

國際刑警組織網絡犯罪總局認同，打擊網絡犯罪最有效的應對措施，需結合私營機構夥伴、司法當局及全球執法部門的協調行動。

INTERPOL's Cybercrime Directorate recognises that the most impactful response to combat cybercrime will require coordinated efforts between relevant private sector partners, judicial authorities, and the global law enforcement community.

INTERPOL

Mr. Neal JETTON
國際刑警組織 網絡犯罪主管
Director of Cybercrime, INTERPOL

執法機關之間的合作至關重要。透過資訊共享、結合專業知識、促進公私夥伴關係及聯合行動，我們可增強該地區的網絡韌性和能力。國際刑警組織亞洲及南太平洋工作小組致力於促進多方合作、提升執法能力並推動各執法機關建立伙伴關係，及共同打造更安全的網絡環境。

Collaboration among law enforcement agencies is crucial. By sharing information, leveraging collective expertise, fostering public-private partnerships, and participating in joint operations, we can enhance the region's cyber resilience and capabilities. The INTERPOL Asia and South Pacific Working Group is committed to facilitating joint efforts, capacity building, and fostering partnerships to create a safer cyber environment for all.

羅家偉助理警察總監 Assistant Commissioner of Police Kah Wai LOH

國際刑警組織亞洲及南太平洋網絡犯罪聯合工作小組 主席
Chairperson, INTERPOL Asia and South Pacific (ASP) Working Group on Cybercrime

新加坡警察部隊刑事偵查局科技罪案調查署 助理局長
Assistant Director, Technology Crime Division, Criminal Investigation Department, Singapore Police Force

隨着各行業加速數字化，人工智能、雲計算、物聯網、開放源碼和低空技術的應用日益增多，黑客和不法分子有了更多可利用的機會，造成隱蔽且迅速的重大危害。應對這些挑戰需要社會各界的共同合作。

With industries accelerating digitalisation and increasing applications of AI, cloud computing, IoT, open-source, and low-altitude technologies, hackers and malicious actors have more opportunities to exploit, causing significant, concealed, and swift harm. Addressing these challenges requires joint efforts from all sectors of society.

數碼港 Cyberport

鄭松岩博士 Dr. Rocky CHENG
數碼港 行政總裁
CEO, Cyberport

技術狂飆，威脅暗湧。人工智能呼喚內生安全！
AI boom sparks critical demand for built-in security.

奇安信

齊向東先生 Mr. QI Xiangdong
奇安信科技集團 董事長
Chairman, QAX Technology Group

2025年的網絡威脅並非單一事件，對手將不斷精進其戰略並大規模利用保安漏洞，形成日益增長且互相連結的網絡犯罪鏈。建立網絡韌性，需要依靠情報主導的網絡保安、主動式防禦措施，以及私營企業、政府與執法機構之間的緊密合作。

The cyber threats of 2025 are not isolated incidents but part of a growing, interconnected web of cybercrime, where adversaries refine their tactics and exploit vulnerabilities at scale. True resilience requires intelligence-driven security, proactive defences, and strong collaboration between private enterprises, governments, and law enforcement.

GROUP-IB

Mr. Dmitry VOLKOV
Group-IB 行政總裁及技術總監
CEO & CTO, Group-IB

為提升用戶安全，必須強化公私營協作、國際合作，以及犯罪預防與警務教育。各持份者的參與至關重要。
There is a critical need for enhanced public-private collaboration, international cooperation, and education in crime prevention and policing to keep users safer. Every stakeholder's involvement is essential.

BINANCE

鄧偉政先生 Mr. Richard TENG
幣安 行政總裁
CEO, Binance

在全球網絡安全形勢持續變化下，必須掌握新興技術和落實數據保護，才能有效對抗日益普遍且精密的威脅。

In the evolving landscape of global cybersecurity, a commitment to emerging technologies and data protection is essential for effectively combating increasingly pervasive and sophisticated threats.

黃志光先生 Mr. Tony WONG
數字政策辦公室 數字政策專員
Commissioner for Digital Policy,
Digital Policy Office (DPO)

中華人民共和國香港特別行政區政府
數字政策辦公室
Digital Policy Office
The Government of the Hong Kong Special Administrative Region
of the People's Republic of China

培養全機構性的安全思維。
Cultivating an organisation-wide security mindset.

夏其才先生 Mr. Eugene HA
國際信息系統審計協會(中國香港分會) 會長
President, ISACA China Hong Kong Chapter

ISACA China Hong Kong Chapter

抵禦新一代威脅不僅需要人工智能驅動工具，更需實現典範轉移至公私營協作，以整合情報資源及強化集體防禦韌性。

Countering next-gen threats demands not only AI-driven tools but a paradigm shift toward public-private collaboration to pool intelligence and strengthen collective resilience.

顏國定先生 Mr. Kok Tin GAN
羅兵咸永道網絡安全及私隱服務 合夥人
Partner, PwC Cyber Security & Privacy
DarkLab 聯合創辦人
Co-founder, DarkLab

pwc

2025年香港數碼轉型加速，網絡安全威脅加劇，企業需採用人工智能技術、零信任架構及安全存取服務邊緣（SASE）方案，同時加強法規以應對挑戰及抓住機遇。

By 2025, Hong Kong faces rising cyber threats, driving adoption of AI-driven security, Zero Trust, Secure Access Service Edge (SASE) architectures, tighter privacy laws, and strengthened legislation to ensure digital resilience and opportunities.

賈磊先生 Mr. Jeremy JIA
深信服 國際市場部總裁
President of International Market Department, Sangfor Technologies

SANGFOR 深信服科技

2025年，人工智能將成為協作者，大幅提升生產力的同時也帶來風險。企業需要採取健全的網絡保安策略和全面的資訊科技基礎設施，以應對與人工智能相關的挑戰並增強韌性。

In 2025, AI becomes a collaborator, boosting productivity while posing risks. Companies need robust security strategies and holistic IT infrastructure to manage AI-related challenges and enhance resilience.

Mr. Dave WEST
思科 亞太、日本和大中華區 總裁
President, Cisco Asia Pacific, Japan and Greater China

CISCO

在香港2025年網絡安全形勢中，人為失誤仍是關鍵弱點，使攻擊者有機可乘，利用弱密碼、未修補系統、詐騙性人力資源入職程序及深度偽造詐騙等手段，繞過先進防禦系統。

Human error remains a critical vulnerability in Hong Kong's 2025 cybersecurity landscape, enabling attackers to exploit weak passwords, unpatched systems, deceptive HR onboarding, and deepfake scams, bypassing even sophisticated defences.

歐勝傑先生 Mr. Chad OLSEN
畢馬威諮詢法證會計服務 香港主管合夥人
Forensic Leader, Hong Kong, KPMG Advisory

KPMG

關於本報告
About the Report

這是網罪科發表的首份網絡安全報告，從警務政策角度處理網絡安全工作，旨在提高公眾以至網絡安全專才等各界人士和機構的網絡安全意識及防禦能力。透過結合警方行動、內外情報以及來自網絡安全領域合作夥伴的貢獻，網罪科致力提供對全球及香港網絡安全威脅形勢的全面性概述，並提供可行的建議，以幫助所有相關持份者在保護其資訊科技系統方面作出更明智的決策。

This is the first Cybersecurity Report published by CSTCB, which approaches cybersecurity from a policing perspective. The report aims at raising cybersecurity awareness and cyber defence capabilities among both individuals and organisations, ranging from the general public to cybersecurity professionals. By integrating police operations, internal and external intelligence, and contributions from cybersecurity practitioners, CSTCB strives to provide a comprehensive overview of the cybersecurity threat landscape both globally and in Hong Kong. The report also offers practical recommendations to support all stakeholders in making informed decisions to better protect their information systems.

背景 Background

我們生活在一個科技時代，警隊的工作也隨著科技發展而擴展，不僅要維護社會秩序，還需加強打擊網絡犯罪，確保整體公共安全。而隨著數碼化進程加快，網絡安全成為保障個人、企業甚至國家安全的重要課題。

近年來，網絡威脅及網絡攻擊不斷增加。黑客針對電腦系統、網絡設施或電子數據進行惡意行為及攻擊，這些行為往往利用科技漏洞或人為疏忽而造成重大損失。有見及此，政府已開始就網絡安全問題進行立法，制定相關法律來加強對網絡犯罪的防範和執法能力。

在現今數碼時代中，網絡威脅不僅頻繁，更是持續不斷。在2024年，網罪科分析了超過2 500萬項網絡威脅情報，即每日超過6萬8千多項。網絡威脅以不同的形式悄然來襲，但卻可以影響深遠。網罪科觀察到，隨着科技迅速發展、互聯互通程度提升，加上攻擊者日益採用自動化工具及人工智能技術識別和利用系統漏洞，網絡威脅以幾何級數倍增，變得頻繁而且精密。

隨着公眾日漸依賴數碼科技，網絡威脅已成為一個逼切的全球性問題，香港亦不例外。我們必需採取主動且創新的措施來確保系統安全、保護敏感信息，並為不斷演變的攻擊技術做好充分防險準備。

We live in a technological era where the role of the police force has evolved alongside technological advancements. In addition to maintaining social order, law enforcement must strengthen efforts to combat cybercrime and safeguard overall public safety. As digitalisation accelerates, cybersecurity has become a crucial issue in protecting individuals, businesses and even national security.

In recent years, cyber threats and attacks have been surging. Hackers engage in malicious activities and attacks targeting computer systems, network infrastructure, and electronic data. These attacks often exploit technological vulnerabilities or human negligence, causing significant losses. In view of this, the government has begun introducing legislation on cybersecurity issues, formulating relevant laws to enhance the prevention of and enforcement against cybercrime.

In today's digital age, cyber threats are not only frequent but relentless. In 2024, CSTCB analysed over 25 million pieces of cyber threat intelligence, i.e. more than 68,000 pieces every day. Cyber threats strike silently in different forms, but their impact can be far-reaching. CSTCB observed an exponential growth in the frequency and sophistication of cyber threats, driven by rapid technological advancements, increased interconnectivity, and attackers' increasing use of automated tools and artificial intelligence to identify and exploit system vulnerabilities.

As society becomes increasingly reliant on digital technologies, cyber threats have become a pressing global concern, and Hong Kong is no exception. Proactive and innovative measures are essential to ensure system security, protect sensitive information, and stay ahead of constantly evolving attack techniques.

致謝 Acknowledgements

本報告由網罪科撰寫，並得到以下合作夥伴的寶貴貢獻：

This report was prepared by CSTCB with invaluable contributions from the following partners organisations:

ISACA
China Hong Kong Chapter
SANGFOR
深信服科技
GROUP-IB
奇安信
kaspersky
CISCO
pwc
KPMG
ThreatBook

本報告得以完成，有賴各方攜手合作。

The successful completion of this report was made possible through the collaborative efforts of all parties involved.

免責聲明 Disclaimer

本報告旨在為網絡安全從業者及日常需落實網絡安全措施的資訊科技專員提供實用參考。針對企業高層管理人員，報告提出具操作性的建議，協助其制定更周詳的決策以強化機構整體防護能力。儘管報告內容技術性較強，公眾仍可透過此報告掌握基礎防護知識，培養個人網絡安全意識與良好習慣，從而有效保障個人及網絡安全。

本報告提供的資訊僅供參考。報告中對威脅者的描述僅基於技術分析，不涉及政治歸因。網罪科及香港特別行政區政府對本報告內任何不準確、錯誤或遺漏，或因使用本報告的資訊或根據該資訊提供建議而引致的任何損失、行動或不作為，概不負責。

This report offers practical insights primarily for cybersecurity practitioners and IT professionals implementing cybersecurity measures in daily operations. For senior corporate management, this report provides actionable recommendations to support informed decision-making and strengthen organisational resilience. While the report is technical in nature, members of the public may also benefit by gaining basic protective knowledge, developing greater cybersecurity awareness, and cultivating good online habits to better safeguard their personal information and online safety.

The information provided in this report is for reference only. Descriptions of threat actors in this report are based solely on technical analysis and do not constitute political attribution. Neither CSTCB nor the Government of the Hong Kong Special Administrative Region (HKSARG) is responsible for any inaccuracies, errors or omissions in this report, or for any loss, action or inaction arising from the use of, or for advice based on, any information therein.

面對網路威脅，無人能置身事外

No one is immune to cyber threats

全球網絡威脅形勢

Global Cyber Threat Situation

因應科技急速發展、地緣政治局勢日益緊張以及威脅者的攻擊技術越趨複雜，全球網絡威脅形勢正經歷着劇烈的轉變。有網絡安全機構估計，2024年針對機構的全球網絡攻擊數字大幅上升至平均每星期1 673次攻擊，比2023年上升44%[1]。2024年全球因網絡犯罪而導致每年經濟損失估計高達9.5兆美元，在2025年更可能達到10.5兆美元[2]。綜觀全球網安形勢，威脅者主要透過以下幾種攻擊形式及手法，當中包括：透過網絡滲透活動竊取敏感資料；同時亦透過供應鏈漏洞大規模入侵系統；利用人工智能提升網絡攻擊的破壞；利用社交工程手段騙取個人資料及登入憑證；使用勒索軟件加密數據以勒索贖金牟利。科技發展在促進社會聯通的同時，亦無可避免地擴大了網絡犯罪的攻擊面。

The global cyber threat landscape is undergoing dramatic transformation, driven by rapid technological advancements, escalating geopolitical tensions, and the increasingly sophisticated tactics by threat actors. A cybersecurity organisation had estimated that in 2024, the average number of weekly cyberattacks targeting organisations worldwide surged to 1,673, which is 44% higher than in 2023[1]. The global economic losses resulting from cybercrime were estimated to reach US$9.5 trillion in 2024 and may rise to US$10.5 trillion in 2025[2]. An overview of the current global cybersecurity situation reveals that threat actors are primarily exploiting the following methods: stealing sensitive data through cyber espionage activities; exploiting supply chain vulnerabilities for large-scale system intrusions; using artificial intelligence to enhance the destructiveness of cyberattacks; deploying social engineering tactics to obtain personal information and login credentials; and using ransomware to encrypt data and extort ransom payments. While technological development has strengthened global connectivity, it has also inevitably expanded the attack surface available to cybercriminals.

[1] Check Point The State of Cyber Security 2025 (2025年網路安全報告), March 2025 (2025年3月), https://www.checkpoint.com/security-report/

[2] “Cybercrime To Cost The World $9.5 trillion USD annually in 2024” (2024年網路犯罪的每年成本將達到9.5兆美元), October 25 2023 (2023年10月25日), https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/

網絡滲透 Cyber Espionage

數碼世界的無聲入侵者 Silent Intruders in the Digital World

隱匿與耐心

網絡滲透活動是最危險的網絡攻擊之一，一般也被認為與國家級網絡攻擊相關。他們行動有條不紊、資源充足，並專注於長期戰略目標。這類組織運用龐大資源與專業技術維持長期網絡滲透，同時規避偵測。他們追求隱匿性和長期成效，而非短期利益，其攻擊手法亦展現了極高的精確部署：包括定制開發的惡意軟件、利用零日漏洞，以及將惡意活動與合法系統操作融合的「離地攻擊」技術。

Stealth and Patience

Cyber espionage is among the most dangerous forms of cyberattack and is often associated with nation-state cyberattacks. They operate in a methodical manner, with ample resources and a focus on long-term strategic objectives. They leverage substantial resources and advanced technical skills to maintain persistent network access while evading detection. Rather than pursuing short-term gains, they prioritise stealth and sustained impact. Their methodologies display exceptional precision, often involving custom-developed malware, exploitation of zero-day vulnerabilities, and living-off-the-land (LOTL) techniques that camouflage malicious activities within legitimate system operations.

「離地攻擊」技術

離地攻擊是一種利用目標系統中已有工具和資源來進行網絡攻擊的技術。由於所使用的合法工具已經存在於目標系統中（如微軟視窗操作系統中的PowerShell），這種方法使攻擊更難被偵測。

Living-off-the-land (LOTL) techniques

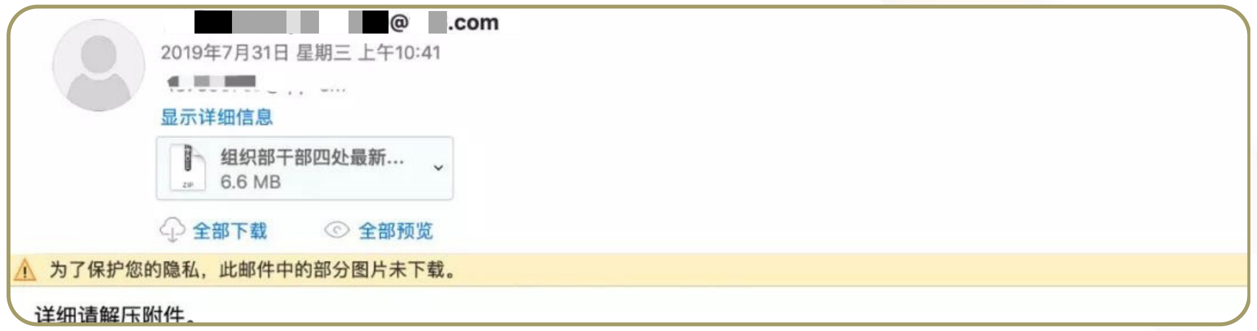
Living-off-the-land (LOTL) refers to a cyberattack technique where attackers use tools and resources that are already present in the target systems. Since these are legitimate utilities (e.g. PowerShell in Microsoft Windows OS), their usage makes the malicious activity harder to detect.

國家級網絡攻擊者

具備國家級能力的威脅者通常從事戰略性網絡情報收集活動，其操作目標可能涉及獲取情報、知識產權和戰略優勢。例如，一個名為「海蓮花」（OceanLotus或APT32）的進階持續性攻擊（APT）組織長期以來針對中國政府和研究機構發起了有組織、計劃性和針對性的魚叉式網絡釣魚攻擊[3]。除了教育機構、軍事、能源和研究開發行業外，近年來「海蓮花」亦被發現以更先進的技術，針對大型科技公司和本地安全研究人員進行攻擊。

Nation-State Threat Actors

Nation-state threat actors typically conduct strategic cyber intelligence collection operations, with objectives that may include gathering intelligence, intellectual property, and strategic advantage. For instance, an Advanced Persistent Threat (APT) group known as "OceanLotus" or "APT32" has launched organised, planned and targeted spear phishing attacks against the Chinese government and research institutions for a long period of time[3]. Apart from education institutions, the military, energy as well as research and development sectors, "OceanLotus" has also been found in recent years to be targeting large technology companies and local security researchers using more advanced techniques.



[redacted]@[redacted].com
2019年7月31日 星期三 上午10:41
[redacted]
显示详细信息
组织部干部四处最新...
6.6 MB
全部下载 全部预览
⚠ 为了保护您的隐私，此邮件中的部分图片未下载。
详细请解压附件。

圖一、 由APT組織「海蓮花」發出的包含惡意軟件的釣魚郵件 (來源：微步在線 2024年威脅情報年報)
Figure 1. Phishing email containing malware sent by APT group "OceanLotus" (Source: ThreatBook 2024 Threat Intelligence Report)

[3] QAX Threat Intelligence Centre (奇安信威脅情報中心), "APT Group: OceanLotus" （"APT組織: 海蓮花"）, February 2025 (2025年2月), https://ti.qianxin.com/apt/detail/5aa0eed8d70a3f07e3f73891?name=%E6%B5%B7%E8%8E%B2%E8%8A%B1&type=listt

經濟目標

除了政治動機外，國家級網絡攻擊者亦把區塊鏈技術和加密貨幣行業視為攻擊目標，通過盜取加密貨幣以獲取經濟利益。例如，一個名為"Lazarus"的APT組織自2009年以來一直活躍於攻擊加密貨幣行業。該組織長期在社交媒體平台上發佈加密貨幣相關的虛假招聘廣告或項目，以引誘目標人士上釣。當受害者上釣後，他們會被進一步誘導安裝帶有惡意軟件的視像面試工具或加密貨幣項目，該組織再盜竊其虛擬資產[4]。

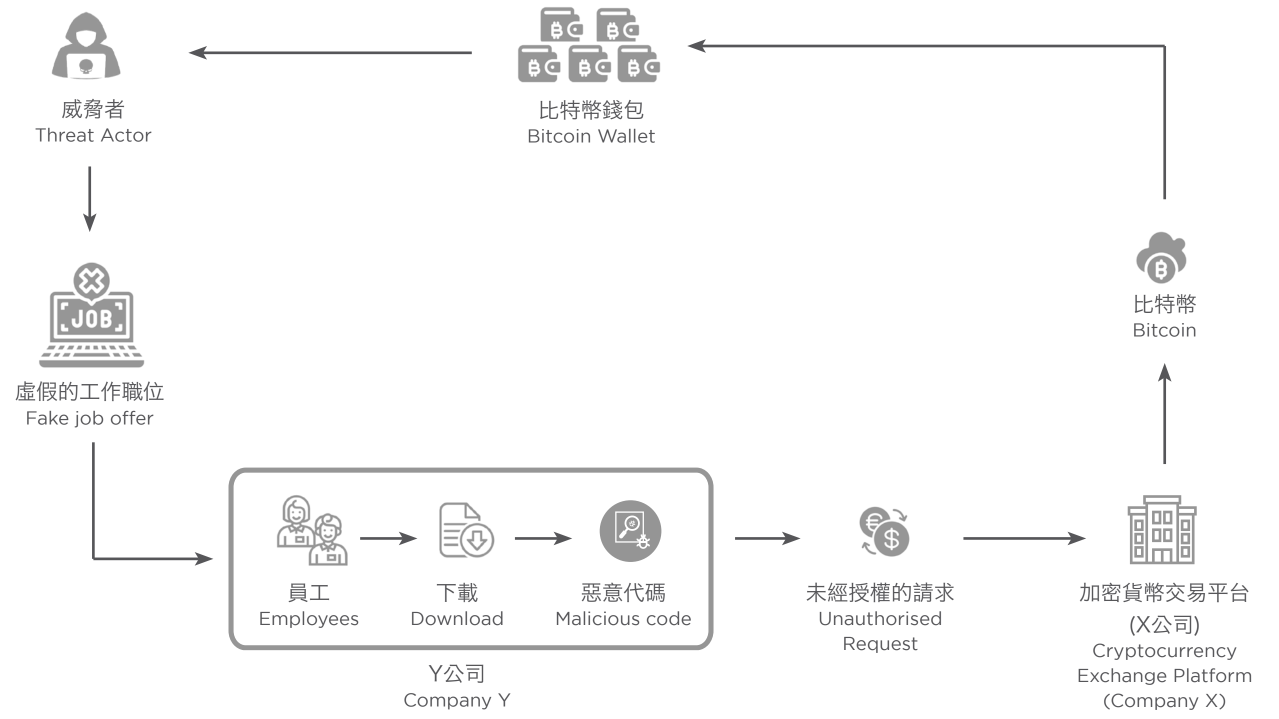
Financial Objectives

Apart from political motivations, nation-state threat actors also target blockchain technology and the cryptocurrency industry, conducting cryptocurrency heists to pursue financial objectives. For instance, a notorious APT group known as "Lazarus" has been actively targeting the cryptocurrency industry since 2009. The group has long been posting fake cryptocurrency-related job advertisements or projects on social media platforms to lure target individuals. Once the victims take the bait, they are further enticed to install malware-laden video interview tools or infected cryptocurrency projects, enabling the group to steal their virtual assets[4].

個案一 Case Study 1

在2024年，一個APT組織成功針對日本一個加密貨幣交易平台（X公司）盜竊加密貨幣，使其損失超過4 000枚比特幣，以當時市值計算超過3億美元[5]。這個APT組織透過冒充獵頭公司，向一間位於日本的加密貨幣錢包公司(Y公司)的員工提供虛假的工作職位，並以入職測試為名誘騙其下載帶有惡意程式碼的文件。成功入侵Y公司系統後，黑客獲得內部通訊系統的接達權限，並操縱Y公司的交易請求，將X公司比特幣轉移到由黑客控制的加密貨幣錢包。此次大規模安全漏洞，導致X公司被迫結束營運。

In March 2024, a notorious APT group stole 4,000 Bitcoin, valued at over US$300 million at the time, from a Japanese cryptocurrency exchange platform (Company X)[5]. Posing as a headhunter, the APT group offered a fake job position to an employee at a Japan-based cryptocurrency wallet company (Company Y), and tricked him into downloading a malware-laden file disguised as a pre-employment test. After successfully infiltrating Company Y's system, the hackers gained access to its internal communication system and manipulated a transaction request, transferring Bitcoin from Company X to cryptocurrency wallets controlled by the hackers. The large-scale breach ultimately forced Company X to shut down.



[4] Qianxin Cybersecurity Threat Annual Report 2024 (奇安信網路安全威脅2024年度報告), February 21, 2025 (2025年02月21日), https://www.qianxin.com/threat/reportdetail?report_id=335

[5] Group-IB High Tech Crime Trends 2025 (Group-IB 高科技犯罪趨勢報告2025), February 26, 2025 (2025年2月26日), https://www.group-ib.com/landing/high-tech-crime-trends-2025/

供應鏈攻擊 Supply Chain Attacks

以隱秘途徑進行大規模入侵 A Stealthy Pathway to Mass Compromise

從上游入手

2024年供應鏈攻擊呈上升趨勢，並已發生多宗重大事件。與其直接攻擊個別機構，攻擊者更傾向於入侵被信任的開發流程，利用獲授權的更新機制留下後門或傳播惡意程式。由於惡意更新中帶有真實的數碼簽署，會被安全工具解讀為合法的更新，繞過常規的安全機制。

Targeting the Upstream

Supply chain attacks were on the rise in 2024 with several major incidents recorded. Instead of directly targeting organisations, attackers compromised trusted development pipelines, transforming authorised update mechanisms into systems for backdoor creation or malware delivery. As malicious updates carried authentic digital signatures, they were interpreted by security tools as legitimate, bypassing conventional security measures.

非對稱優勢

攻擊者在2024年積極探索新的攻擊面，不論是針對邊緣設備的零日攻擊，還是對開放源碼項目的供應鏈攻擊。供應鏈攻擊具有驚人的經濟效益，通過自動化分發機制，單次入侵即可影響數千名下游受害者。供應鏈攻擊已不再局限於單純入侵程式碼庫，而是擴展到雲端服務供應商、開發工具，甚至硬件組件，使機構面臨腹背受敵的困境。

Asymmetric Advantage

A notable characteristic of 2024 was attackers' exploration of new attack surfaces, whether zero-day attacks targeting edge devices or supply chain attacks on open source projects. Supply chain attacks offer adversaries remarkable economy efficiency, enabling a single compromise to affect thousands of downstream victims through automated distribution mechanisms. The attack methodology has expanded beyond simple code repositories to include cloud service providers, development tools, and even hardware components, placing organisations in a position of being attacked from all directions.

精密部署

供應鏈攻擊顯示出攻擊者的縝密與耐性。威脅者通常會在行動前進行數個月的偵察，精心挑選能夠對下游帶來最大連鎖效應的目標。透過長期潛伏使攻擊者能夠徹底了解開發流程、安全控制和程式碼簽署協議，然後再植入其惡意程式碼。攻擊者藉着融入開發者的日常開發工作，暗度陳倉。

Sophisticated Execution

The execution of supply chain attacks demonstrates attackers' meticulousness and patience. Threat actors typically conduct months of reconnaissance before acting, carefully selecting targets that will generate the greatest downstream impact. This prolonged presence allows attackers to thoroughly understand development processes, security controls, and code signing protocols before implanting their malicious code. By blending into the daily development work, attackers can silently carry out their plans.

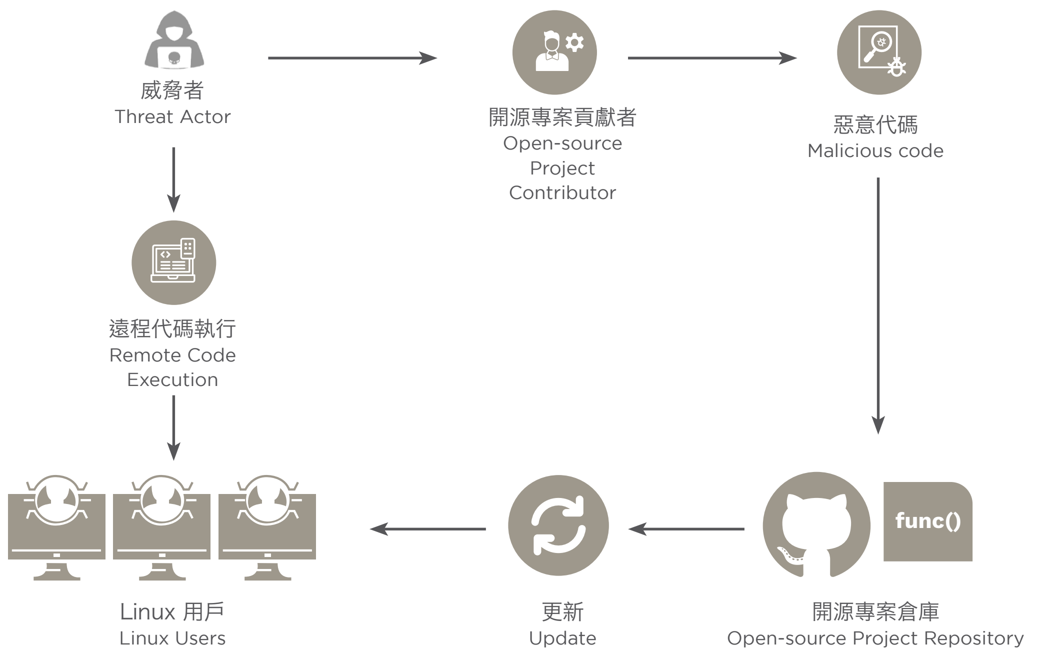
個案二 Case Study 2

2024年3月，美國一名軟件開發者發現一個惡意後門被嵌入於一個常見於Linux發行版本的數據壓縮庫XZ Utils的 5.6.0及5.6.1版本。未通過認證的遠端攻擊者可利用該後門，未經授權而接達受影響的系統。該後門被追蹤為CVE-2024-3094，擁有最高的CVSS嚴重性評分10分。一位名為“JiaT75”的用戶通過精心策劃，以長達兩年時間滲透該開源項目，直至獲得維護者權限，再植入後門。這個後門可以通過被騎劫的安全外殼協議守護程序（SSH daemons），令受影響的Linux系統提供遠端執行程式碼功能，從而讓攻擊者能夠創建殭屍網絡、部署勒索軟件或竊取數據[6]。

假如此次漏洞在廣泛散播之前未被察覺，恐怕會影響幾乎所有嵌入XZ Utils的Linux系統，令全球數百萬台伺服器岌岌可危。這次事件暴露了軟件供應鏈的致命弱點，尤其是作為無數系統基礎組件的開源軟件。

In March 2024, a software developer in the US discovered a malicious backdoor embedded in versions 5.6.0 and 5.6.1 of XZ Utils, which is a data compression library commonly found in Linux distributions. An unauthenticated remote attacker could exploit the backdoor to gain unauthorised access to affected systems. Tracked as CVE-2024-3094, the backdoor received the highest Common Vulnerability Scoring System (CVSS) severity score of 10. The backdoor was planted through a meticulous two-year infiltration by a threat actor known as "JiaT75" who gained maintainer privileges in the open-source project before implanting the backdoor. The backdoor allowed remote code execution on affected Linux systems through hijacked Secure Shell Protocol (SSH) daemons, enabling attackers to create botnets, deploy ransomware or steal data[6].

Had this vulnerability remained undetected before widespread distribution, it could have affected virtually all Linux systems embedding XZ Utils, jeopardising potentially millions of servers worldwide. This incident exposes the critical weakness of the software supply chain, especially open-source software that serves as the foundational component for countless systems.



[6] Qianxin Cybersecurity Threat Annual Report 2024 (奇安信網路安全威脅2024年度報告), February 21, 2025 (2025年02月21日), https://www.qianxin.com/threat/reportdetail?report_id=335

人工智能 Artificial Intelligence | 重塑網絡安全形勢 Reshaping Cybersecurity Landscape

從理論風險到實際威脅

在2024年，人工智能驅動的網絡攻擊迅速從理論上的安全風險，演變為實際威脅。過去僅限於專業黑客的攻擊能力，因人工智能工具降低了技術門檻而變得觸手可及。在2024年，APT組織“UTG-Q-015”發起的一次攻擊中，就發現了疑似由人工智能生成的源碼[7]。此外，攻擊者還會利用生成式人工智能打造針對目標特徵的高仿真釣魚詐騙，繞過傳統偵測機制。

From Theoretical Risk to Actual Threat

In 2024, AI-powered cyberattacks rapidly evolved from theoretical security risks to tangible, operationalised threats. The democratisation of attack capabilities, once exclusive to skilled hackers, became more accessible as AI tools lowered the technical barrier. In 2024, suspected AI-generated source code was found in an attack launched by APT Group “UTG-Q-015”[7]. Attackers also leverage generative AI to craft highly convincing phishing scams tailored to target profiles, bypassing traditional detection methods.

黑灰科技產業

人工智能網絡犯罪經濟已演變為一個泛專業化的市場，從外洩的雲端憑證、大型語言模型(LLM)服務、自動化工具、客製化大型語言模型接達權限以及被入侵的人工智能系統，皆可明碼實價交易。「惡意人工智能即服務」平台的出現大幅降低了技術門檻，使技術水平較低的威脅者也能利用人工智能工具協助進行網絡攻擊。

Dark Technology Market

The AI cybercrime economy has evolved into a broad and specialised marketplace, where leaked cloud credentials, Large-Language-Model (LLM) services, automated tools, custom LLM access rights, and compromised AI systems are openly traded. The emergence of Malicious-AI-as-a-Service platforms has significantly lowered technical barriers, enabling even low-skilled threat actors to leverage AI tools to conduct cyberattacks.

人工智能與數據安全

人工智能工具如今被廣泛用於提升生產力和競爭優勢，但同時也帶來了數據安全方面的新風險。據網絡安全公司思科統計，86%的機構在過去十二個月內曾面對與人工智能相關的安全事件[8]。其中，資料投毒正成為日益嚴重的威脅，攻擊者通過污染訓練數據，破壞其人工智能系統，影響系統生成的結果。另一種風險是數據盜竊。隨着公司投入具價值的資訊發展人工智能系統，攻擊者可以通過特定方式繞過傳統安全措施查閱這些模型，從而竊取底層數據或知識產權。因此，採用人工智能的機構必須實施強而有力的人工智能風險管理措施，推動人工智能設計層面的保安。

Artificial Intelligence & Data Security

AI tools are now widely used to enhance productivity and competitive advantages, but also introduce new risks to data security. According to statistics from cybersecurity company Cisco, 86% of organisations experienced AI-related security incidents in the past 12 months[8]. One growing threat is data poisoning, where attackers contaminate training data to sabotage AI systems and distort their outputs. Another risk is data theft through model extraction. As companies feed valuable information into their AI systems, attackers can bypass traditional security controls and query the models in specific ways to steal underlying data or intellectual property. Organisations adopting AI must therefore implement strong AI risk management practices and promote security-by-design in AI development.

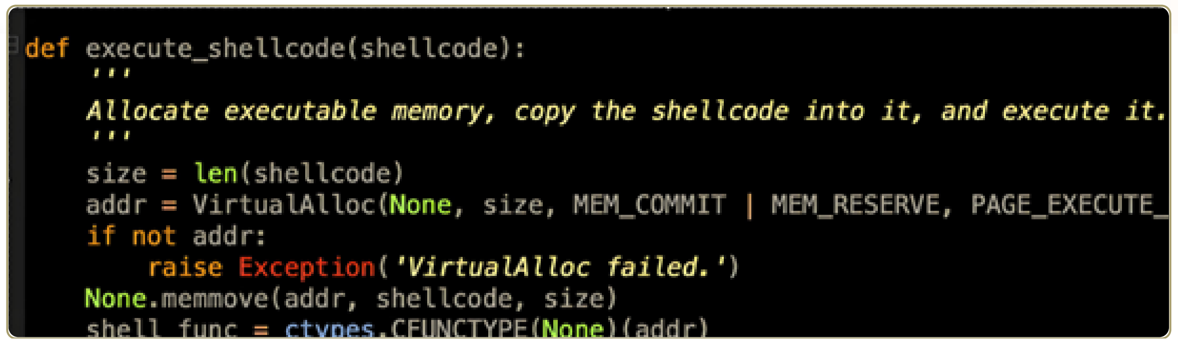
[7] Qianxin Cybersecurity Threat Annual Report 2024 (奇安信網絡安全威脅2024年度報告), February 21, 2025 (2025年02月21日), https://www.qianxin.com/threat/reportdetail?report_id=335

[8] Cisco 2025 Cybersecurity Readiness Index (思科2025年網絡安全準備度指數), April 28, 2025 (2025年4月28日), https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2025/m04/cisco-security-reimagine-ai-rsac.html

個案三 Case Study 3

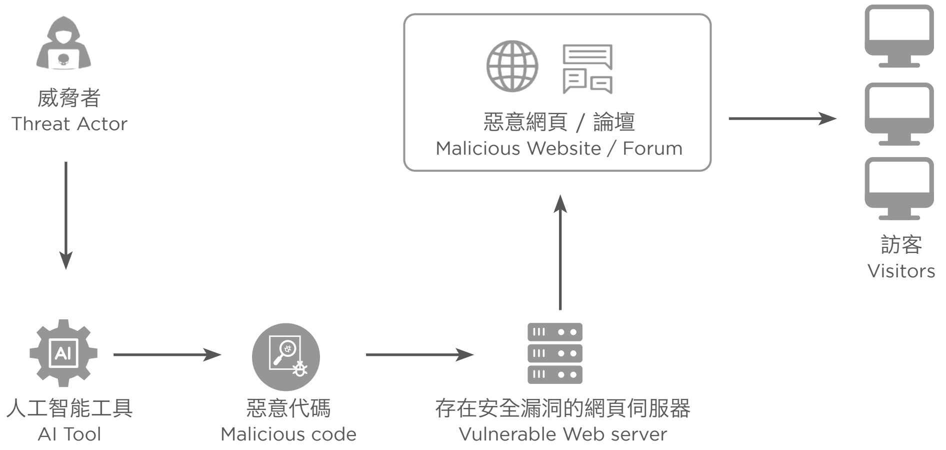
儘管我們難以偵測在網絡攻擊過程中使用人工智能的完整攻擊鏈，但仍可能發現到人工智能生成程式碼的線索。在2024年12月，一個名為“UTG-Q-015”的組織發動水坑攻擊，通過入侵伺服器加入惡意JavaScript程式碼，並攻陷一個網頁應用插件工具，可能影響中國數百萬個網站，包括資訊科技群組、政府網站以及科技論壇。研究人員對惡意軟件的分析顯示其Python惡意程式碼疑似由人工智能生成[9]。

Although it is hard to detect the full kill chain involving AI during cyberattacks, traces of AI-generated code may still be identified. In December 2024, a group known as “UTG-Q-015” launched a watering hole attack, by compromising the servers to inject malicious JavaScript, which then infected a web application plugin tool. The attack potentially affected millions of websites in China, including IT communities, government portals, and technical forums. Malware analysis revealed that the malicious Python scripts were suspected to have been generated by AI[9].



```
def execute_shellcode(shellcode):
    '''
    Allocate executable memory, copy the shellcode into it, and execute it.
    '''
    size = len(shellcode)
    addr = VirtualAlloc(None, size, MEM_COMMIT | MEM_RESERVE, PAGE_EXECUTE_
    if not addr:
        raise Exception('VirtualAlloc failed.')
    None.memmove(addr, shellcode, size)
    shell_func = ctypes.CFUNCTYPE(None)(addr)
```

圖二、圖示顯示由黑客組織“UTG-Q-015”發起的水坑攻擊中使用的疑似由人工智能生成的Shellcode惡意程式碼
Figure 2. Diagram showing suspected AI-generated scripts in shellcode used in a watering hole attack launched by a hacker group named “UTG-Q-015”



水坑攻擊

水坑攻擊是一種針對特定目標的網絡攻擊策略，攻擊者通過入侵特定目標常用的網站，植入惡意代碼，從而在目標使用這些網站時自動執行惡意程式碼。

Watering hole attack

A watering hole attack is a targeted cyberattack strategy in which attackers compromise websites frequently visited by specific targets. By injecting malicious code into these websites, the attackers ensure that the code execute automatically when the target accesses them.

[9] Qianxin Cybersecurity Threat Annual Report 2024 (奇安信網絡安全威脅2024年度報告), February 21, 2025 (2025年02月21日), https://www.qianxin.com/threat/reportdetail?report_id=335

社交工程 Social Engineering | 在數碼時代將信任變為武器 Weaponising Trust in Digital Age

從程式碼到心理操控

現今黑客不僅是技術專家，更是人性操縱者。隨着網絡防禦技術的日漸精良和高效，他們被迫從傳統攻擊方法（如利用系統安全漏洞和暴力破解）轉向更複雜且基於心理操縱的策略，尤其是利用社交工程。此轉變凸顯了一個日益明確的共識：

From Code to Coercion

Nowadays, hackers are no longer just tech wizards but also masters of human manipulation. As cybersecurity defences grow increasingly sophisticated and effective, attackers have been forced to shift from traditional methods, such as exploiting system vulnerabilities and brute force attacks, to more psychologically driven tactics, particularly social engineering. This transition underscores a growing consensus:

> 人為因素往往是網絡安全中最脆弱的一環
>
> Human element is often the weakest link in cybersecurity

依靠信任，而非科技

社交工程是通過利用人類心理(例如信任、貪婪、恐懼、好奇心或衝動)，誘使他們有意與無意間洩露機密資料或授予對受限系統的接達權限。以釣魚郵件為例，此類攻擊透過偽裝成可信人士(如同事、銀行職員或政府部門)，以誘使受害者點擊惡意連結或分享敏感資料。

Thrives on Trust, not Technology

Social engineering works by exploiting human psychology, such as trust, greed, fear, curiosity, or impulsivity, to trick individuals into knowingly or unknowingly disclosing confidential information or granting access to restricted systems. Phishing emails, for instance, impersonate trusted entities like colleagues, bank staff, or government departments to lure victims into clicking malicious links or sharing sensitive data.

經濟實惠，卻具高度可擴展性

攻擊者偏好於社交工程，因為其成本低廉且覆蓋範圍廣。網絡安全公司深信服發現，有APT組織自2023年初起，利用即時通訊軟件、郵件及釣魚網站，針對中國國內金融、教育、電商、貨運、設計等行業發起大規模釣魚攻擊，以進行詐騙活動或竊取敏感信息[10]。遠程遙距工作的興起亦擴大了攻擊面，例如虛擬私有網絡（VPN）和網上通訊平台（電子郵件、即時通訊應用程式和社交網絡）增加大量入侵路徑，讓攻擊者可以利用自動化釣魚工具同時針對數以千計目標，從而提高成功率。

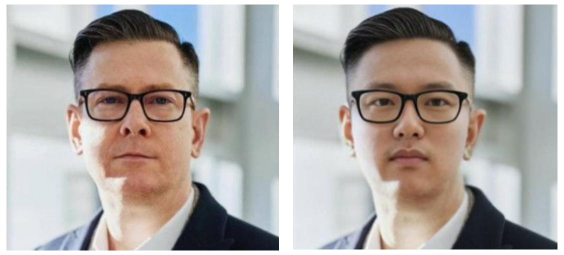
Budget-friendly, yet Highly Scalable

Attackers favour social engineering for its low cost and broad scalability. Cybersecurity company Sangfor reported that, since early 2023, an APT group has been using instant messaging apps, emails and phishing websites to launch large-scale attacks on various industries in Mainland China, including finance, education, e-commerce, logistics, and design, for fraud and data theft[10]. The rise of remote work has further expanded the attack surface, with Virtual Private Networks (VPNs) and online communication platforms (such as email, instant messaging apps, and social networks) offering numerous entry points. Attackers can utilise automated phishing tools to target thousands simultaneously, greatly increasing their success rates.

個案四 Case Study 4

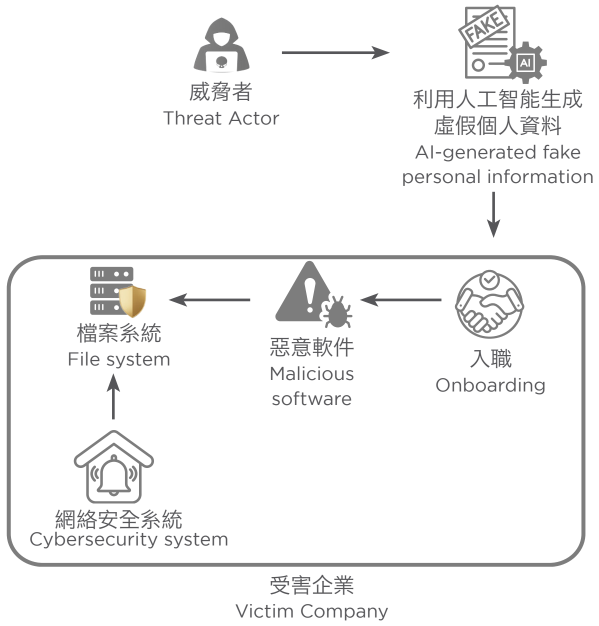
2024年7月，國外一間網絡安全培訓平台通過網上面試，聘請一名軟件工程師進行遙距工作。但其後發現該名假員工原來利用人工智能技術，偽造個人相片及通過人事部門數次遙距面試，成功冒認他人身份通過整個遙距招聘過程。該名假員工在入職後，即時嘗試在公司系統中植入惡意軟件，但其可疑活動觸發內部網絡安全系統的警報。該名假員工被揭發後，隨即失去蹤影。此次事件顯示出黑客能夠利用複雜的社交工程技巧，進行網絡攻擊[11]。

In July 2024, an overseas cybersecurity training platform hired a software engineer for remote work through an online interview process. However, it was later discovered that the individual was a fake employee who had successfully impersonated someone else, using AI to forge resume photo and complete several remote interviews with the HR department. After being hired, the fake employee immediately attempted to install malicious software into the company's system, which triggered alerts from the internal cybersecurity system. Upon discovery, the fake employee disappeared without a trace. This incident highlights how hackers can leverage sophisticated social engineering techniques to launch cyberattacks[11].



圖三、左方為網上圖片，右方為黑客利用人工智能生成的偽造個人照片

Figure 3. Left: Online image. Right: Fraudulent personal photo created by the hacker using AI.



[10] Sangfor 2024 APT Insight Reports (深信服2024年APT洞察報告), March 12 2025 (2025年3月12日), https://www.sangfor.com.cn/document/a85065d9607f4a66be8c8d84676c0425

[11] Qianxin Cybersecurity Threat Annual Report 2024 (奇安信網路安全威脅2024年度報告), February 21, 2025 (2025年02月21日), https://www.qianxin.com/threat/reportdetail?report_id=335

勒索軟件 Ransomware | 從入侵系統中獲利 Monetising System Compromise

從加密到勒索

勒索軟件已轉變成網絡犯罪的主要牟利工具。有網絡安全機構指出，2024年全球已公開發布的企業勒索軟件攻擊逾 5 000 宗，較2023年增長11%[12]。然而，已報告的事故僅僅是冰山一角。

From Encryption to Extortion

Ransomware has transformed into cybercrime's premier profit engine. A cybersecurity organisation recorded over 5,000 disclosed ransomware attacks on enterprises worldwide in 2024, representing an 11% increase compared to 2023[12]. However, reported incidents are only the tip of the iceberg.

精心設計的毀滅性攻擊

勒索軟件攻擊手法極具效率：滲透、加密和勒索。攻擊者會根據特定或隨機目標，試圖通過多種攻擊方法（如暴力破解、社交工程或釣魚攻擊）來獲得受害者網絡的初始接達。一旦成功滲透，他們可能潛伏數星期甚至數個月，才會在關鍵伺服器和數據庫上部署加密工具。

現代勒索軟件團伙採用「雙重勒索」策略，在加密數據前先竊取敏感資料，並威脅受害者如果拒絕支付贖金，將會在暗網上公開這些資料。更甚，勒索軟件團伙採用「三重勒索」以及「四重勒索」策略，進一步迫使目標公司繳付贖金。這種精心策劃的手法使受害者進退兩難：無論是否支付贖金，都可能面臨業務運作癱瘓、商譽受損與財務損失的多重打擊。

Devastating by Design

Ransomware attacks follow a brutally effective methodology: infiltrate, encrypt, and extort. Attackers attempt to gain initial access to a victim's network, whether targeted or opportunistic, through various techniques such as brute force, social engineering or phishing. Once inside, they may remain undetected for weeks or even months before deploying encryption tools across critical servers and databases.

Modern ransomware gangs employ "double-extortion" tactics, exfiltrating sensitive data before encryption and threatening to publish it on the dark web if ransom demands are not met. Even more aggressively, some gangs now adopt "triple extortion" or even "quadruple extortion" strategies to further pressure target companies into paying. These calculated methods leave victims facing impossible decisions: whether or not they pay the ransom, they risk operational paralysis, reputational damage, and financial loss.

單一勒索 Single Extortion	雙重勒索 Double Extortion	三重勒索 Triple Extortion	四重勒索 Quadruple Extortion
攻擊者加密數據庫，發出勒索訊息要求付款以解鎖文件檔案系統。 The attackers encrypt the database and issue a ransom note demanding payment for the decryption of system files and data.	攻擊者不僅加密受害者的資料，還竊取敏感資料，並威脅受害者如果拒絕支付贖金，將會在暗網上公開這些資料。 The attackers not only encrypt the victim's data but also exfiltrate sensitive information, threatening to publish it on the dark web if ransom is not paid.	攻擊者除了威脅目標公司外，還會向其客戶或生意伙伴進行勒索，以獲取更多的贖金。 In addition to targeting the victim company, the attackers also extort its customers or business partners to obtain additional ransom payments.	攻擊者會進一步要脅針對目標公司的系統網絡弱點發動分散式阻斷服務攻擊，透過制造大量網絡流量癱瘓目標公司的網絡，以迫使目標公司繳付贖金。 The attackers further threaten to exploit system vulnerabilities in the target company's network by launching a Distributed Denial-of-Service (DDoS) attack, generating massive traffic to paralyse the company's network and force the target company to pay the ransom.

[12] "Ransomware Yearly Report 2024" (勒索軟件年度報告2024), January 13, 2025 (2025年1月13日), https://cyberint.com/blog/research/ransomware-annual-report-2024/

勒索軟件黑灰產業

勒索軟件已經演變成一個龐大的地下產業，包括「勒索軟件即服務」的興起、數據洩露網站的出現，以及協助進入目標網絡的初始訪問代理的參與[13]。正如國際刑警組織的觀察所得，初始訪問代理在勒索軟件即服務生態系統中扮演關鍵角色，透過提供初始接達以支援更複雜的攻擊[14]。這種犯罪生態系統大幅降低了犯罪入場門檻，同時提高了運作效率。而加密貨幣的匿名交易機制，能夠繞過傳統金融監控體系，進一步推動了此犯罪模式跨地域進行。

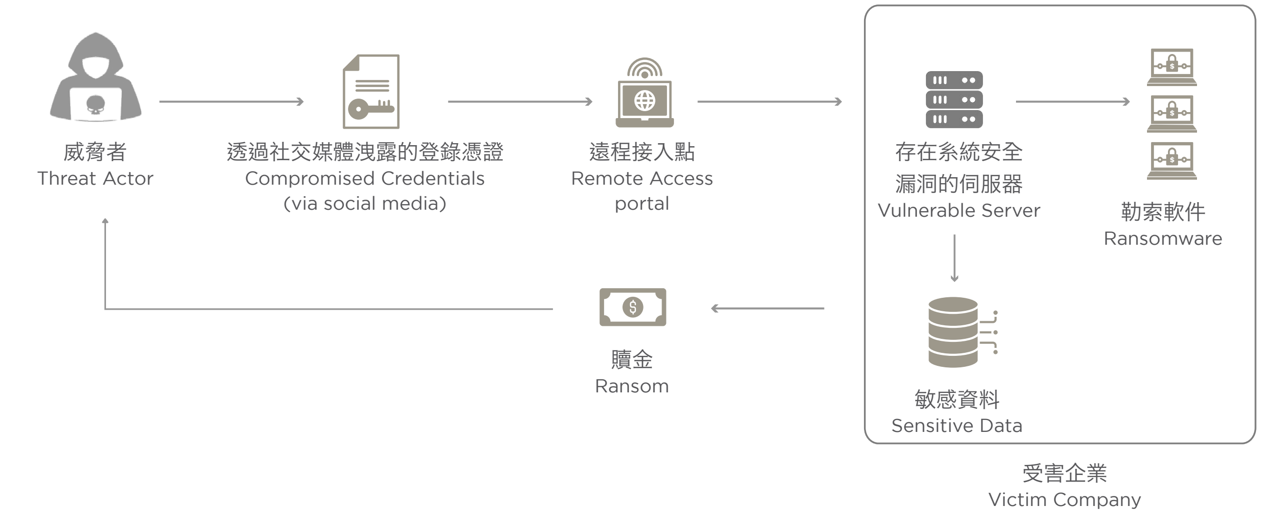
Ransomware Underground Industry

Ransomware has evolved into a sprawling underground industry, characterised by the rise of Ransomware-as-a-Service, the emergence of dedicated leak sites that publicly expose stolen data, and the involvement of initial access brokers who facilitate entry into targeted networks[13]. As observed by INTERPOL, initial access brokers play a critical role in the Ransomware-as-a-Service ecosystem by providing the initial access needed to support more sophisticated attacks[14]. This criminal ecosystem has significantly lowered the barriers to entry while increasing operational efficiency. The relatively anonymous nature of cryptocurrency transactions, operating outside traditional financial oversight, has further propelled this model across geographic boundaries.

個案五 Case Study 5

2024年2月，一間美國大型醫療技術供應商遭受ALPHV/BlackCat勒索軟件團伙的攻擊後，被迫中斷業務運作數星期，導致醫療服務供應商和保險公司無法使用其核心系統[15]。根據相關訴訟法律文件顯示，攻擊者透過Telegram群組取得客服人員遭盜用的登入憑證，入侵未啟用多重認證的遠端入口，並潛伏長達9日。期間不僅建立特權管理帳號、部署惡意程式，更竊取數TB敏感資料後才加密系統。此次數據洩露事件最終導致逾億民眾個人資料外洩，亦令受害機構支付數百萬美元的贖金，及面對因數據外洩和長期服務中斷而引發的多宗訴訟。

In February 2024, a major healthcare technology provider in the US fell prey to the ALPHV/BlackCat ransomware gang, forcing a weeks-long disruption of operations that left healthcare providers and insurers unable to access core systems[15]. According to legal documentation filed in a lawsuit against the organisation, the attackers gained access using stolen customer support employee credentials obtained via a Telegram group. They infiltrated a remote portal that lacked multi-factor authentication and remained undetected in the network for nine days. During which, they created privileged administrator accounts, deployed malware, and exfiltrated several terabytes of sensitive information before finally encrypting the systems. The breach ultimately compromised the personal data of over 100 million individuals and resulted in the payment of millions of US dollars in ransom, along with multiple lawsuits triggered by the data breach and prolonged service outage.



[13] Group-IB High Tech Crime Trends 2025 (Group-IB高科技犯罪趨勢報告2025), February 26, 2025 (2025年2月26日), https://www.group-ib.com/landing/high-tech-crime-trends-2025/

[14] INTERPOL Asia and South Pacific Cyberthreat Assessment Report (國際刑警組織亞洲及南太平洋網絡威脅評估報告), Aug 2024 (2024年8月), https://www.interpol.int/content/download/22308/file/Asia%20and%20South%20Pacific%20Cyberthreat%20Assessment%20Report%202024-4.pdf

[15] "Attorney General Mike Hilgers Files Lawsuit Against Change Healthcare for Critical Failures to Protect Consumer Data and Prevent Against Harm from a Widespread Cyberattack" [總檢察長邁克・希爾格斯（Mike Hilgers）對Change Healthcare 提出訴訟，指控其在保護消費者數據和防止大規模網絡攻擊造成傷害方面存在嚴重缺失], December 16, 2024 (2024年12月16日), https://ago.nebraska.gov/news/attorney-general-mike-hilgers-files-lawsuit-against-change-healthcare-critical-failures

網罪科是香港應對網絡威脅和科技罪案的重要防線

Serving as a key line of defence, CSTCB safeguards Hong Kong against cyber threats and technology crimes

香港網絡安全形勢

Hong Kong Cybersecurity Situation

自2015年成立以來，網罪科採取了多管齊下的策略維護香港網絡安全。在進行刑事調查的同時，網罪科積極收集網絡威脅情報，維護重要基礎設施網絡安全，並主導公眾教育活動，提高網絡安全意識。

網罪科致力透過廣泛收集及分析多維度的網絡威脅情報，包括開源情報、專屬威脅情報源、前沿技術監控系統，以及強大的合作夥伴網絡，以掌握香港整體網絡安全形勢。

網罪科轄下的網絡安全中心全年無間斷運作。除了收集相關情報分析網絡攻擊，網絡安全中心亦會監察重要基礎設施系統的正常運作及全天候提供不同等級的網絡防禦及行動支援。

自2024年起，網罪科正式成立一個名為「網絡安全行動中心聯盟」（SOCA）的核心網絡威脅情報交流平台，串聯香港大型及重要基礎設施。通過分析來自各個來源的情報，網罪科全面了解針對香港的網絡安全威脅，並適時發出預警及作出適時應對。

Since its establishment in 2015, CSTCB has pursued a multi-pronged approach to safeguarding Hong Kong's cybersecurity. While conducting criminal investigations, CSTCB also proactively gathers cyber threat intelligence, secures critical infrastructure networks, and leads public education initiatives to raise cybersecurity awareness.

CSTCB endeavours to enhance its visibility of the overall cybersecurity landscape in Hong Kong by extensively collecting and analysing cyber threat intelligence from diverse sources. These include open source intelligence, proprietary threat intelligence feeds, cutting-edge technology monitoring systems, and robust network of strategic partners.

The Cyber Security Centre under CSTCB operates round-the-clock throughout the year. In addition to collecting and analysing intelligence related to cyberattacks, the Centre also monitors the smooth operation of critical infrastructures' systems and provides round-the-clock defence and operational support at various levels.

The Security Operation Centre Alliance (SOCA), established by CSTCB in 2024, connects large-scale and critical infrastructures across Hong Kong, serving as a core cyber threat intelligence exchange platform. By analysing intelligence from multiple sources, CSTCB maintains a comprehensive view of cybersecurity threats targeting Hong Kong and issues timely alerts with appropriate countermeasures.

主要網絡安全數據
Key Cybersecurity Figures

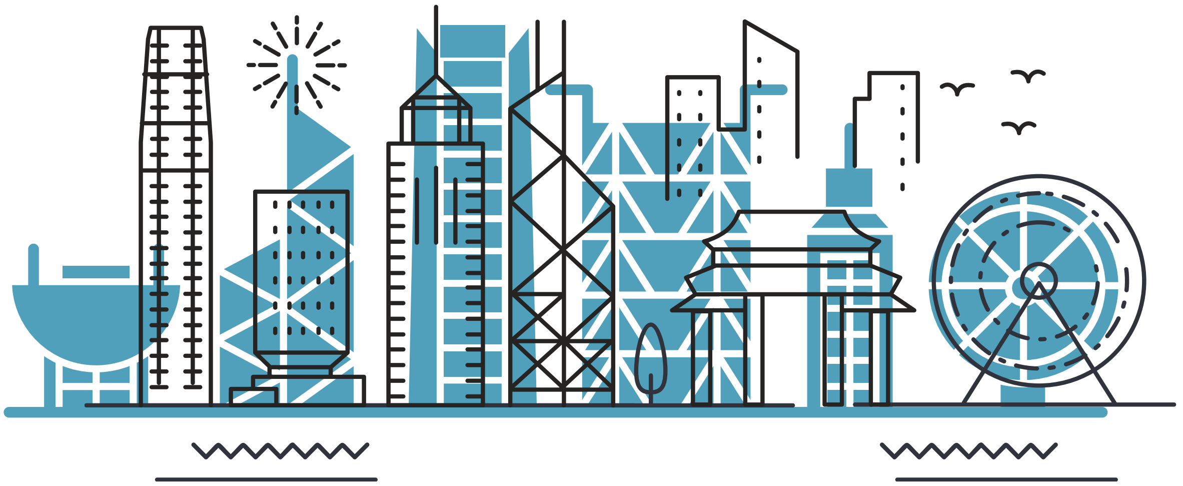
2 500萬項網絡威脅情報
25 million pieces of cyber threat intelligence

在2024年，網罪科處理超過2 500萬項網絡威脅情報，即平均每日處理超過68 000項情報。

In 2024, CSTCB processed over 25 million pieces of cyber threat intelligence, averaging over 68,000 pieces per day.

超過44萬項網絡威脅情報直接針對香港

Over 440,000 pieces of cyber threat intelligence directly targeting Hong Kong



具破壞性的網絡攻擊手段
Destructive Cyberattacks

1 入侵系統活動 Hacking Activities

2024年按年增加65%至61宗
Increased by 65% year-on-year to 61 cases in 2024

造成總損失達2 550萬港元
Causing total losses of HK$ 25.5 million

2 勒索軟件 Ransomware

2024年按年增加一倍至46宗
Doubled year-on-year to 46 cases in 2024

最高勒索金額達到3 880萬港元
The highest ransom demand reached HK$ 38.8 million.

Lockbit、Phobos、ALPHV/Blackcat 和 Trigona 是2024年在香港最活躍的勒索軟件家族
Lockbit, Phobos, ALPHV/Blackcat and Trigona were the most active ransomware families in Hong Kong in 2024

3 分散式阻斷服務攻擊 Distributed Denial-of-Service (DDoS) Attacks

報案數字從2023年的零宗案件上升至2024年的5宗
Increased from zero reported case in 2023 to 5 cases in 2024

損失金額達到460萬港元
Causing losses of HK$ 4.6 million

網絡釣魚 PHISHING

280,000+

網罪科發現超過440 000項針對香港的網絡威脅情報，當中有超過280 000項與網絡釣魚有關，佔所有香港網絡威脅情報超過65%。

CSTCB detected over 440,000 pieces of cyber threat intelligence specifically targeting Hong Kong, of which 280,000 were phishing-related, accounting for over 65% of all local threat intelligence.

約78%參與「釣魚電郵演習2024」的機構有至少一名員工曾點擊釣魚連結，有機會導致其網絡受到入侵。

Around 78% of organisations participating in the Ethical Phishing Email Campaign 2024 had at least one employee clicked the phishing link, potentially compromising the organisation's network.

重要基礎設施漏洞測試
Vulnerability Testing for Critical Infrastructures

90,000+

網罪科評估了超過90 000個香港重要基礎設施的網絡資產，發現當中5%存在不同程度的系統安全漏洞。

CSTCB assessed over 90,000 Internet-facing assets belonging to critical infrastructures in Hong Kong and found that 5% had varying degrees of system vulnerabilities.

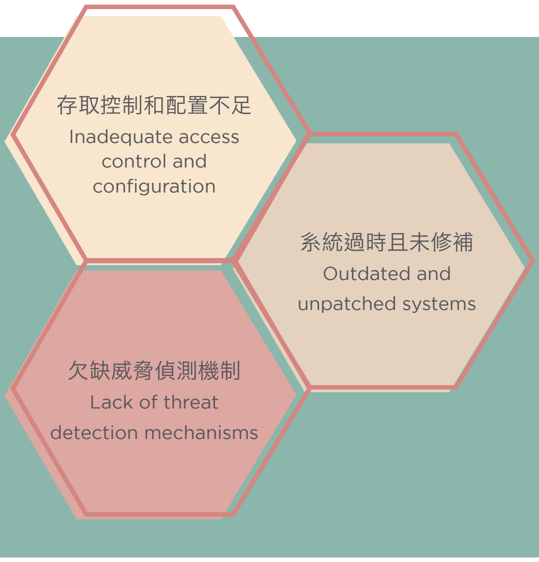
在已識別的系統安全漏洞中，89%被歸類為中低風險，而11%屬極高及高風險級別，主要包括憑證外洩或遭盜用、可被騎劫的子域名，以及被暴露的雲端儲存服務。

Among the identified system vulnerabilities, 89% were classified as medium and low risk, while 11% were deemed critical and high risk, including credentials leakage/compromise, hijackable subdomains, and exposed cloud storage.

在2024年，銀行與金融行業是面對網絡攻擊的重要基礎設施中受攻擊最頻繁的行業，其次是通訊業和政府。

In 2024, the banking and finance sector was the most frequently targeted industry among critical infrastructures facing cyberattacks, followed by the communications sector and the government.

網罪科分析網絡安全事故，重複發現三個問題：
CSTCB's analysis of cybersecurity incidents consistently identified three recurring problems:

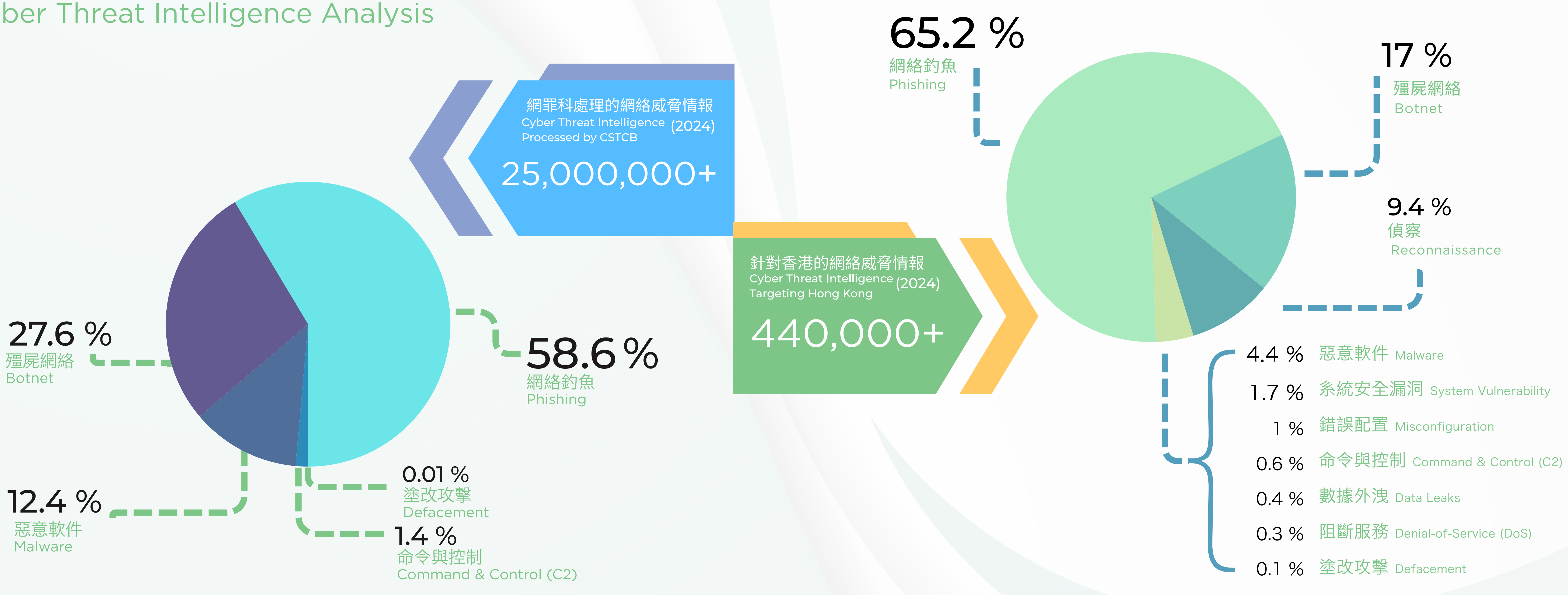


存取控制和配置不足
Inadequate access control and configuration

系統過時且未修補
Outdated and unpatched systems

欠缺威脅偵測機制
Lack of threat detection mechanisms

網絡威脅情報分析
Cyber Threat Intelligence Analysis



網罪科處理的網絡威脅情報 Cyber Threat Intelligence Processed by CSTCB (2024)

25,000,000+

58.6 % 網絡釣魚 Phishing

27.6 % 殭屍網絡 Botnet

12.4 % 惡意軟件 Malware

1.4 % 命令與控制 Command & Control (C2)

0.01 % 塗改攻擊 Defacement

針對香港的網絡威脅情報 Cyber Threat Intelligence Targeting Hong Kong (2024)

440,000+

65.2 % 網絡釣魚 Phishing

17 % 殭屍網絡 Botnet

9.4 % 偵察 Reconnaissance

4.4 %	惡意軟件	Malware
1.7 %	系統安全漏洞	System Vulnerability
1 %	錯誤配置	Misconfiguration
0.6 %	命令與控制	Command & Control (C2)
0.4 %	數據外洩	Data Leaks
0.3 %	阻斷服務	Denial-of-Service (DoS)
0.1 %	塗改攻擊	Defacement

網絡釣魚

攻擊者冒充成可信賴的個體，誘騙他人透露敏感資料，如密碼或信用卡資料。

Phishing

Attackers impersonate trusted entities to trick individuals into revealing sensitive information, such as passwords or credit card details.

系統安全漏洞

由於設計或編碼錯誤而存在於軟件、硬件或流程中的內在弱點或缺陷，攻擊者可以利用這些漏洞來獲取未經授權的接達或造成損害。

System Vulnerability

Weaknesses or flaws inherent in software, hardware, or processes that exist due to design or coding errors, that can be exploited by attackers to gain unauthorised access or cause harm.

殭屍網絡

由攻擊者控制的一個受感染的設備網絡，用於執行網絡攻擊，例如分散式阻斷服務攻擊（DDoS）或濫發電郵。

Botnet

A network of compromised devices controlled by attackers to perform cyberattacks, such as DDoS attacks or spamming.

錯誤配置

由於系統、網絡或應用程序的不正確配置而產生的系統安全風險，通常由人為錯誤導致。

Misconfiguration

System security risks arising from incorrect configuration of systems, networks, or applications, often caused by human error.

惡意軟件

專為破壞、干擾或未經授權地接達系統的惡意軟件，包括病毒、蠕蟲、勒索軟件和間諜軟件。

Malware

Malicious software designed to damage, disrupt or gain unauthorised access to systems, including viruses, worms, ransomware, and spyware.

偵察

收集有關目標系統、網絡或機構的資訊，以識別系統安全漏洞，並策劃潛在的攻擊。

Reconnaissance

Gathering of information about a target system, network, or organisation to identify system vulnerabilities and plan potential attacks.

命令與控制

由攻擊者用作與受感染設備或惡意軟件通訊和控制的指揮中心，用於協調網絡攻擊。

Command & Control (C2)

A control hub used by attackers to communicate with and control compromised devices or malware to coordinate cyberattacks.

阻斷服務

通過耗盡系統或服務的資源以削弱其可用性，從而阻止合法用戶的接達。

Denial-of-service (DoS)

Deplete the resources of a system or service to undermine its availability, preventing access from legitimate users.

塗改攻擊

未經授權修改界面(包括網頁或電子屏幕)的外觀或內容，以展示惡意或不受歡迎的圖片和訊息。

Defacement

Unauthorised modification of the visual appearance or content of an interface (including webpage or electronic screen) to display malicious or unwanted graphics and messages.

數據外洩

敏感或機密資料被意外地暴露或洩露予未經授權人士。

Data Leaks

Sensitive or confidential information unintentionally exposed or disclosed to unauthorised individuals.

網罪科的觀察所得
What CSTCB Observed

在收集的2 500萬項網絡威脅情報中，網罪科識別出約440 000項（1.76%）針對香港的情報

Among the 25 million pieces of cyber threat intelligence collected, CSTCB identified approximately 440,000 (1.76%) specifically targeting Hong Kong

網絡釣魚

網罪科所處理與香港相關的網絡威脅情報中，超過65%與網絡釣魚活動有關。換言之，全年共偵測到超過28萬項針對香港的網絡釣魚威脅情報。這類攻擊手法既可被用於詐騙活動，亦能製造網絡攻擊的入口。除了高成功率外，網絡釣魚攻擊的盛行有多種原因：低廉開發成本、低技術門檻、容易進行大規模攻擊，以及人工智能技術的出現。

Phishing

Over 65% of Hong Kong specific cyber threat intelligence handled by CSTCB in 2024 was related to phishing related activities. In other words, over 280,000 phishing-related threats targeting Hong Kong were detected over the year. Phishing techniques can be used to conduct scams or serve as entry points for broader cyberattacks. Beyond their high success rate, phishing attacks continue to thrive due to multiple factors: low development costs, minimal technical barriers, ease of large-scale deployment, and the emergence of AI technologies.

香港網絡安全事故協調中心(HKCERT)在2024年共處理12 536宗保安事故，其中網絡釣魚佔整體個案超過六成（7 811宗，佔62%），對比2023年上升108%，共增加4 059宗[16]。

In 2024, Hong Kong Computer Emergency Response Team (HKCERT) handled 12,536 security incidents. Phishing accounted for over 60% of all cases (7,811 cases, or 62%), representing a 108% increase from 2023, i.e. an increase of 4,059 cases[16].

[16] "HKCERT Unveils Hong Kong Cyber Security Outlook 2025" (HKCERT 發表「香港網絡安全展望 2025」), January 20, 2025 (2025年1月20日), https://www.hkcert.org/press-centre/hkcert-unveils-hong-kong-cyber-security-outlook-2025-phishing-hits-five-year-high-vulnerabilities-in-supply-chain-and-ai-content-hijacking-emerge--as-key-risks-over-half-of-enterprises-fear-cyber-attacks-on-iot-digital-signages

釣魚電郵演習2024

由網罪科及香港互聯網註冊管理有限公司（HKIRC）合辦的「釣魚電郵演習2024」中，約78%的參與機構有至少1名員工曾點擊了釣魚連結，此舉足以令機構網絡面臨潛在入侵。當中，假冒人力資源部門發出的郵件最為有效，成功誘使超過3 300名員工點擊釣魚連結，其中逾330名員工更在釣魚網站上上載了敏感資料。

Ethical Phishing Email Campaign 2024

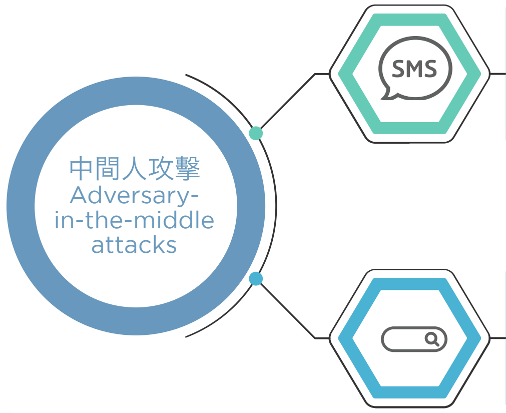
In the Ethical Phishing Email Campaign 2024, co-organised by CSTCB and the Hong Kong Internet Registration Corporation Limited (HKIRC), around 78% of participating organisations had at least one employee clicked a phishing link, potentially exposing the organisation's network to intrusion. Among the simulated phishing emails, those impersonating Human Resources departments were the most effective, successfully luring over 3,300 employees to click the phishing link, with more than 330 of them uploading sensitive information to the phishing website.

WhatsApp帳戶騎劫

由2023年底至2024年初期間，本港WhatsApp帳戶騎劫案件顯著上升。 在2 989宗「帳戶盜用」個案中，涉及WhatsApp的騎劫案件多達2 547宗，總損失金額更高達7 350萬港元。騙徒主要會以網絡釣魚的兩種「中間人攻擊」手法入侵帳戶：

WhatsApp Hijacking

From late 2023 to early 2024, WhatsApp hijacking cases saw a significant surge in Hong Kong. Among the 2,989 "Account Abuse" cases, 2,547 involved WhatsApp hijacking, with total losses reaching HK$73.5 million. Scammers primarily used two types of phishing-based adversary-in-the-middle attacks to compromise user accounts:



釣魚短訊詐騙 Smishing

發送附有虛假網站連結的釣魚短訊，並誘使受害人在欺詐網站上輸入手機號碼及WhatsApp驗證碼。

Scammers sent phishing text messages containing links to fake websites, tricking victims into entering their phone numbers and WhatsApp verification codes on these fraudulent sites.

搜尋器優化（SEO）中毒
Search Engine Optimisation (SEO) Poisoning

建立假冒的WhatsApp登入頁面，並在搜尋器投放廣告。當用戶搜尋WhatsApp時，欺詐網站會出現在搜尋結果中，用戶進入虛假網站後會被要求掃描惡意二維碼。一旦掃描後，騙徒可以騎劫用戶帳戶，再向其親友騙取金錢。

Scammers created fake WhatsApp login pages and promoted them through advertisements on search engines. When users search for WhatsApp, the fraudulent sites appeared in search results. Upon entering these fake websites, users were prompted to scan a malicious QR code. Once scanned, scammers could hijack the user's accounts and impersonate them to defraud their friends and family.

殭屍網絡

殭屍網絡活動位居第二，佔針對香港的網絡威脅情報約17%。殭屍網絡通過利用被C2伺服器所控制的受感染設備來牟利，既可隱藏網絡犯罪分子的身份，同時亦可執行濫發郵件、DDoS攻擊和網上詐騙等大規模攻擊。缺乏安全性的物聯網（IoT）設備不斷增加，亦顯著擴大了潛在攻擊面，為威脅者提供可供利用的資源。

Botnet

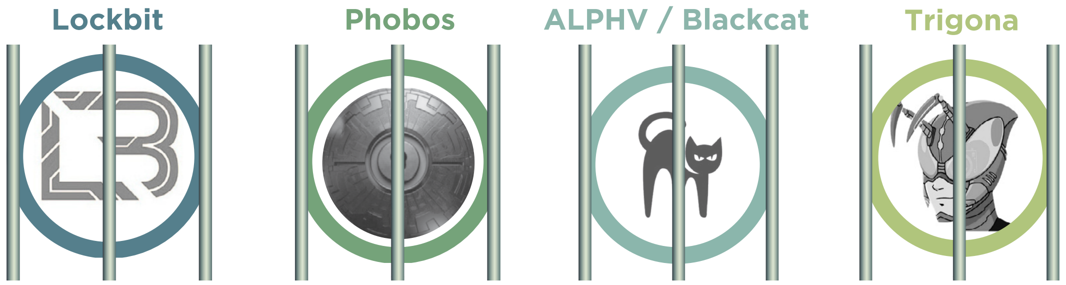
Botnet activity ranked second, accounting for approximately 17% of cyber threat intelligence targeting Hong Kong. Botnets generate profit by leveraging compromised devices controlled by Command-and-Control (C2) servers, masking the identities of cybercriminals while carrying out large-scale attacks such as spam distribution, DDoS attacks, and online scams. The growing number of unsecured Internet of things (IoT) devices has significantly expanded the potential attack surface, providing threat actors with exploitable resources.

惡意軟件

惡意軟件相關情報佔2024年針對香港的網絡威脅情報約4.4%。當中，勒索軟件是香港以至全球最令人擔憂的網絡攻擊之一。進行勒索軟件攻擊的網絡犯罪分子採用越來越具侵略性的手法，滲透機構網絡，加密重要數據，並要求高額贖金。網罪科在調查中經常發現以下幾種勒索軟件家族：

Malware

Malware-related threat intelligence accounted for approximately 4.4% of cyber threat intelligence targeting Hong Kong in 2024. Ransomware remained one of the most concerning forms of cyberattack, both globally and in Hong Kong. Cybercriminals deploying ransomware have adopted increasingly aggressive tactics, infiltrating organisational networks, encrypting critical data, and demanding hefty ransom payments. The following ransomware families were frequently identified during CSTCB investigations:



網罪科強烈建議受害者不要支付贖金，原因有兩點：支付贖金後不但無法保證數據能夠成功復原，而且提供營運資金，會助長犯罪集團

CSTCB strongly advises victims not to pay ransom for two reasons: first, payment does not guarantee successful data recovery; second, it funds and empowers criminal organisations

除了勒索軟件外，攻擊者轉向更精密的方法，如專門設計、具有隱蔽性的惡意軟件、「無檔案攻擊」和「離地攻擊」（LOTL）技術。這些方法留下的可偵測痕跡更少，可能降低一般威脅情報收集機制的偵測率。

Apart from ransomware, attackers are turning to more advanced methods such as specially crafted, evasive malware, fileless attacks and living-off-the-land (LOTL) techniques. These approaches leave fewer detectable traces, potentially reducing detection by standard threat intelligence collection mechanisms.

「無檔案攻擊」

無檔案攻擊是一種不依賴傳統可執行檔案（如“.exe”或“.dll”檔案）的網絡攻擊技術，攻擊者利用系統內建的工具或直接在系統記憶體執行惡意程式碼，而不在硬碟中留下痕跡。

Fileless attacks

A fileless attack is a cyberattack technique that does not rely on traditional executable files (e.g. “.exe” or “.dll” files), but exploits built-in system tools or executes malicious scripts directly in system memory, leaving no trace on the hard disk.

面對頻繁威脅，仍有效防禦

儘管去年網絡攻擊事件有上升趨勢，但仍然保持在可控制的範圍內。2024年，香港警務處錄得61宗「入侵系統活動」事件，按年增加65%，總損失金額達到港幣2 550萬元。同時，「勒索軟件」案件增加了一倍，達到46宗案件，勒索金額高達港幣3 880萬元。「分散式阻斷服務攻擊（DDoS）」雖然從2023年的零宗增加到2024年的5宗，造成高達460萬元損失，但在香港整體網絡安全形勢中仍屬較次要的威脅。

即使網絡威脅情報數量龐大，但成功攻擊的數量相對較少，這個顯著的差異反映出一個令人鼓舞的事實：

Effective Defences Prevail Against Frequent Attacks

Although cyberattacks showed an upward trend over the past year, the overall situation remained within manageable levels. In 2024, the Hong Kong Police Force (HKPF) recorded a 65% increase in "Hacking activities" incidents, with 61 reported cases and financial losses amounting to HK$25.5 million. Concurrently, "Ransomware" cases doubled to 46, with extortion demands reaching up to HK$38.8 million. "Distributed Denial-of-Service (DDoS)" attacks rose from zero cases in 2023 to 5 in 2024, resulting in losses of up to HK$4.6 million. However, DDoS remains a relatively minor threat in the context of Hong Kong's overall cybersecurity landscape.

Despite the large volume of cyber threat intelligence collected, the number of successful attacks remained comparatively low. This notable disparity reflects an encouraging fact:

香港強大的網絡防禦機制持續有效地應對來自威脅者的反覆攻擊

Hong Kong's robust cyber defence mechanisms continue to perform effectively against recurrent attacks from threat actors

這既反映社會對整體網絡安全意識的有效水平，亦顯示各界努力維護良好網絡環境，標誌着由政府、公私營機構與公眾三方協作驅動的集體成果。

This reflects not only the effectiveness of cybersecurity awareness across society, but also the combined effort of various sectors in maintaining cyber-hygiene. It also marks a collective achievement driven by collaboration between the government, the public-private sector, and the general public.

儘管結果令人鼓舞，但網絡安全形勢複雜多變、充滿挑戰。我們必須保持警覺性和韌性，以應對不斷演變的威脅。

While these results are encouraging, the cybersecurity landscape remains complex, dynamic and full of challenges. We must all remain vigilant and resilient in the face of ever-evolving threats.

針對重要基礎設施的網絡威脅
Cyber Threats to Critical Infrastructures

香港是智慧城市、國際商貿和金融中心、國際航運和貿易樞紐，亦是重要和專業服務核心基地，高度依賴其先進運輸、通訊、金融及公共基礎設施系統。一旦核心服務遭受網絡攻擊而中斷，不僅會造成重大經濟損失，更可能引發公共安全危機，損害國際社會對本港的信心。

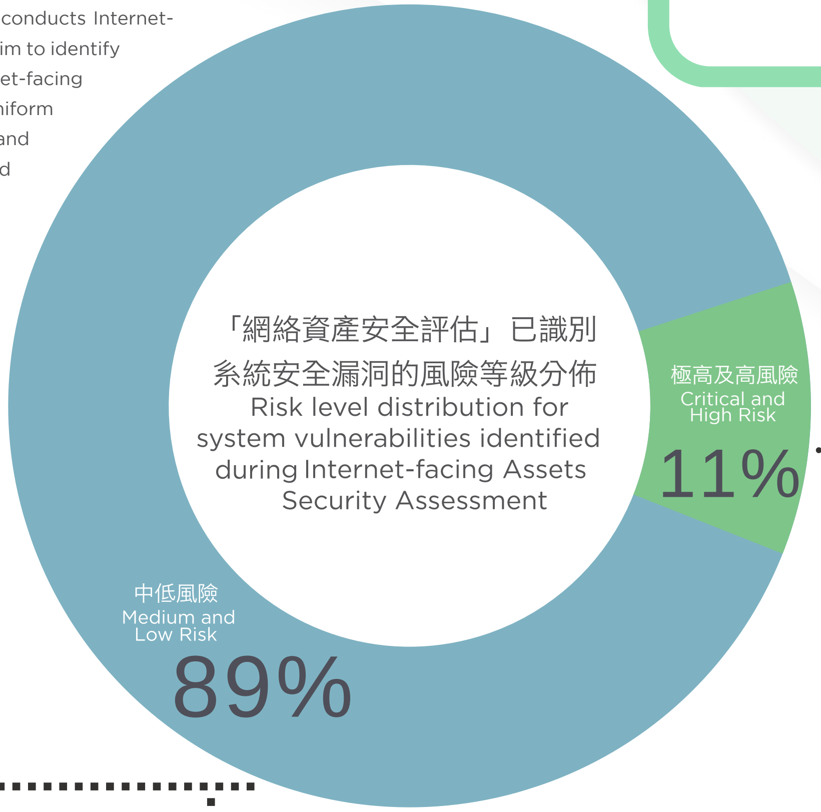
有見全球重要基礎設施持續遭受網絡威脅，網罪科定期進行「網絡資產安全評估」。這項安全評估旨在偵測重要基礎設施面向互聯網的網絡資產中，如劃一資源定位址（URLs）、域名及互聯網規約（IP）地址，可能存在的系統安全漏洞，以確保這些重要網絡資產的保安與韌性。

2024年網罪科評估超過90 000個屬於重要基礎設施的網絡資產，發現當中5%存在不同程度的系統安全漏洞。透過常設通報機制，所有重要基礎設施已適時處理令風險變得可控，同時凸顯持續進行主動評估和監測的重要性。

Hong Kong, recognised as a smart city and a global leader in commerce and finance, serves as a vital hub for international shipping and trade, as well as a centre for essential professional services. These functions rely heavily on its advanced transportation, telecommunications, financial, and utility infrastructures. Any disruption to these core services due to cyberattacks could result in significant economic losses, pose risks to public safety, and undermine international confidence in the city.

In view of the persistent cyber threats targeting critical infrastructures worldwide, CSTCB regularly conducts Internet-facing Assets Security Assessments, which aim to identify potential system vulnerabilities in Internet-facing assets of critical infrastructures, including Uniform Resource Locators (URLs), domain names, and IP addresses, to ensure their security and resilience.

In 2024, CSTCB assessed over 90,000 Internet-facing assets belonging to critical infrastructures in Hong Kong and found that 5% had varying degrees of system vulnerabilities. Through the established notification mechanism, all critical infrastructures addressed the identified risks in a timely manner, emphasising the importance of ongoing proactive assessment and monitoring.



「網絡資產安全評估」已識別系統安全漏洞的風險等級分佈
Risk level distribution for system vulnerabilities identified during Internet-facing Assets Security Assessment

極高及高風險漏洞 Critical and High Risk Loopholes

該漏洞很可能讓威脅者能夠直接發動網絡攻擊，並可能對重要基礎設施的正常營運帶來重大的影響。
These vulnerabilities are likely to allow threat actors to launch cyberattacks directly and may have a significant impact on the normal operation of critical infrastructures.

憑證外洩或盜用
Credential Leakage / Compromise

無論是員工或公眾的登入憑證一旦外洩或被盜用，攻擊者即可藉此未經授權接達關鍵系統，構成重大安全威脅。

Leaked or stolen credentials, whether from staff or the public, pose a major threat, as they allow attackers to gain unauthorised access to critical systems.

可被劫持的子域名
Hijackable Subdomains

閒置的子域名可能遭攻擊者惡意利用於進行釣魚攻擊或詐騙活動，反映機構需加強域名管理措施。

Unused subdomains can be taken over by attackers for malicious purposes, such as phishing or fraud, highlighting the need for enhanced domain management.

被暴露的雲端儲存服務
Exposed Cloud Storage

配置不當的雲端儲存服務容易導致資料外洩及遭受網絡攻擊，必須實施更嚴格的存取管理及加密技術以保護敏感數據。

Misconfigured cloud storage services increase the risk of data leakage and cyberattacks. Stronger access controls and encryption measures are essential to protect sensitive data.

在已識別的系統安全漏洞中，89%被歸類為中低風險，僅11%屬極高及高風險級別，主要包括憑證外洩或遭盜用、可被騎劫的子域名，以及被暴露的雲端儲存服務。

Among the system vulnerabilities identified, 89% were classified as medium and low risk, while only 11% were categorised as critical and high risk, including credentials leakage / compromise, hijackable subdomains and exposed cloud storage.

中低風險漏洞 Medium and Low Risk Loopholes

該漏洞讓威脅者直接發動網絡攻擊的可能性相對較低，但仍然可能被利用作偵察活動，促進一步網絡攻擊。
These vulnerabilities are less likely to enable direct cyberattacks but may still be exploited for reconnaissance activities, which can facilitate further cyberattacks.

郵件伺服器被列入黑名單
Mail server in blacklist

重要基礎設施自身的郵件伺服器被列入黑名單，暗示該伺服器可能已被入侵並成為殭屍網絡的一部分。
Email servers belonging to critical infrastructures that appear on blacklists may indicate compromise and possible integration into a botnet.

證書授權問題
Certificate authority issues

無效或未更新的網絡安全證書。
Invalid or outdated cybersecurity certificates.

保密插口層/傳輸層保安問題
SSL/TLS issues

網絡資產使用較弱加密套件和密鑰。
Use of weak cipher suites or cryptographic keys in Internet-facing assets.

可被利用的端口
Exploitable port

未經限制的端口可能會被利用來達到惡意目的。
Unrestricted ports can be exploited for malicious purposes.

暴露的網頁介面
Exposed web interface

內部或敏感系統托管在網頁上(例如用於系統控制的登入頁面）並且對外公開。
Internal or sensitive systems hosted on a publicly accessible webpage (e.g. login portals for system control).

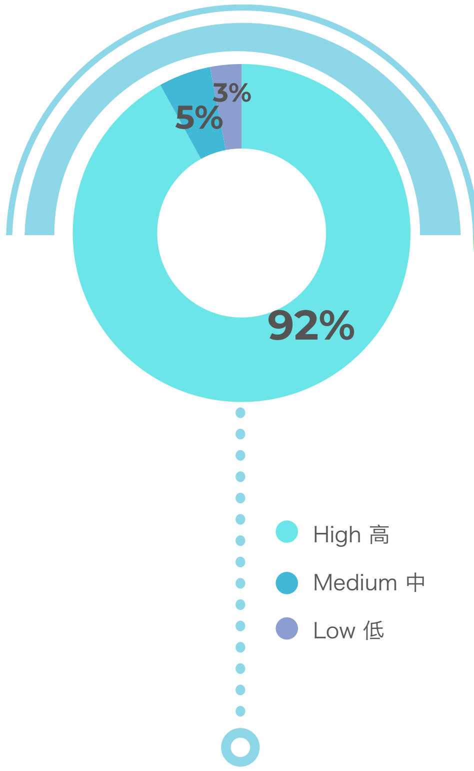
完成漏洞測試後，所有被識別的系統安全漏洞均已適時修補，相關機構亦已全面提升系統防護水平。為有效應對此類網絡安全風險，各機構應：

After the vulnerability testing, all identified system vulnerabilities were promptly patched, and the affected organisations have significantly enhanced their system security levels. To effectively mitigate such cybersecurity risks, organisations should:

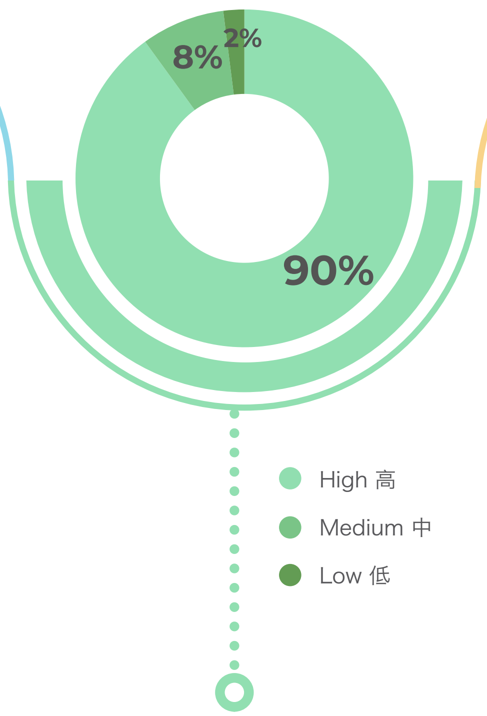
- 定期進行域名配置審查，防止子域名遭惡意劫持。
  Regularly review domain configurations to prevent subdomain hijacking.
- 對雲端儲存服務實施加密，並設立嚴格的存取權限管理。
  Apply encryption to cloud storage and implement strict access control measures.
- 制定更嚴格的密碼政策，並啟用雙重認證。
  Enforce stronger password policies and enable two-factor authentication.

網絡安全意識和應變準備
Cybersecurity Awareness and Preparedness

2024年重要基礎設施對網絡威脅警覺性的調查結果
Survey result of critical infrastructures on alertness to cyber threats in 2024



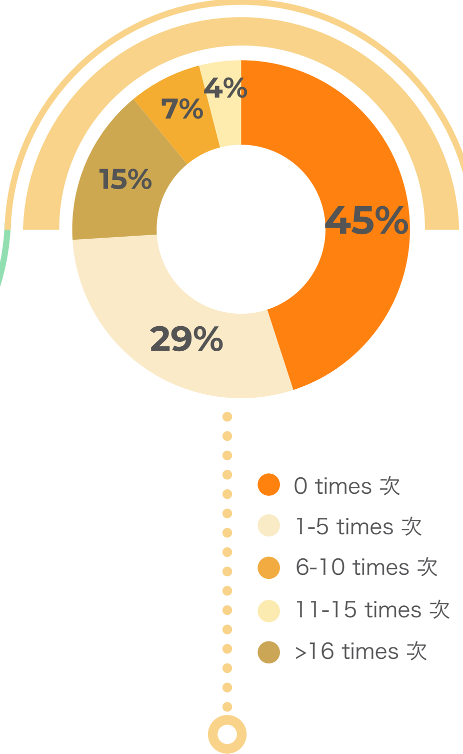
2024年重要基礎設施對網絡安全應變準備的調查結果
Survey result of critical infrastructures on cybersecurity preparedness in 2024



網罪科每年均會進行調查，以評估本港重要基礎設施營運者的網絡安全警覺性及應變準備。2024年度接受問卷調查的重要基礎設施中，約92%自評對網絡威脅保持高度警覺，約90%認為自身具備完善的網絡安全應變準備，結果反映重要基礎設施營運者普遍認為自身保持高度警惕性和前瞻性。

CSTCB conducts an annual survey to assess the cybersecurity alertness and preparedness of critical infrastructure operators. In 2024, among the critical infrastructures responding to the survey, around 92% self-assessed as maintaining high alertness to cyber threats, and about 90% believed they possessed strong cybersecurity preparedness. These results show a general perception among critical infrastructure operators that they remain highly vigilant and forward-looking.

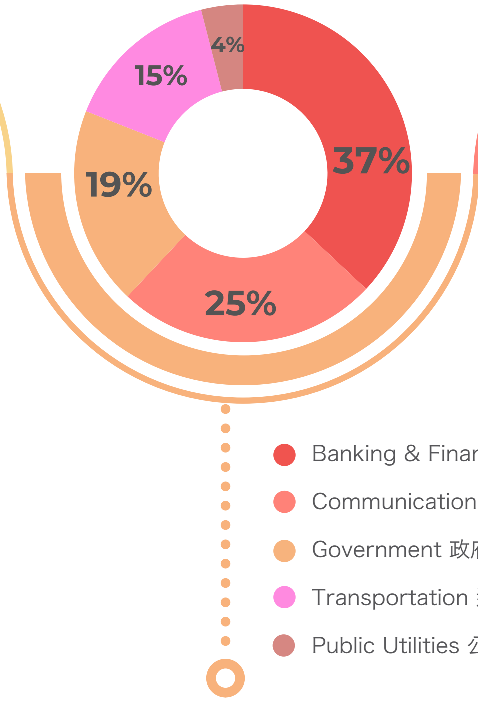
2024年重要基礎設施受到網絡攻擊或發生網絡安全事故頻率的調查結果
Survey result of critical infrastructures on the frequency of cyberattacks or cybersecurity incidents encountered in 2024



調查亦顯示，55%的重要基礎設施在過去一年至少受到一次網絡攻擊或發生網絡安全事故。當中，更有15%受訪機構在2024年內面對超過16次或以上網絡攻擊或發生網絡安全事故。

The survey also revealed that 55% of critical infrastructures (CIs) had experienced at least one cyberattack or cybersecurity incident in the past year. Among them, 15% of respondents reported facing 16 or more such events in 2024.

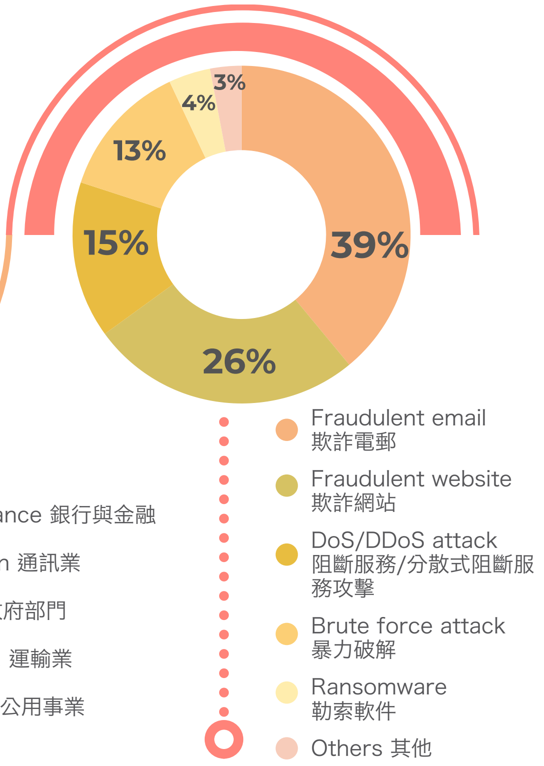
2024年重要基礎設施受到網絡攻擊或發生網絡安全事故的行業分布調查結果
Survey result on distribution of critical infrastructures encountering cyberattacks or cybersecurity incidents by sector in 2024



根據 2024 年調查結果，首三個受網絡攻擊或發生網絡安全事件的行業分別是銀行及金融業（37%）、通訊業（25%）和政府部門（19%）。

According to the 2024 survey results, the top three sectors affected by cyberattacks or cybersecurity incidents were banking and finance (37%), communications (25%), and government departments (19%).

2024年重要基礎設施受到網絡攻擊或發生網絡安全事故性質的調查結果
Survey result on the nature of cyberattacks or cybersecurity incidents encountered by critical infrastructures in 2024



根據2024年調查結果，最常見的網絡攻擊手法依次序為：欺詐電郵（39%）、欺詐網站（26%）及阻斷服務（DoS）或分散式阻斷服務（DDoS）攻擊（15%）。其餘攻擊方式包括透過即時通訊軟件的釣魚活動、惡意軟件、零日攻擊、結構化查詢語言（SQL）插入及殭屍網絡活動。

According to the 2024 survey, the most common types of cyberattacks were: fraudulent emails (39%), fraudulent websites (26%), and denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks (15%). Other attack methods included phishing via instant messaging applications, malware, zero-day exploits, structured query language (SQL) injection attempts, and botnet activity.

《保護關鍵基礎設施（電腦系統）條例》立法進展
Legislative Progress of the Protection of Critical Infrastructures (Computer Systems) Bill

《保護關鍵基礎設施（電腦系統）條例》（下稱「條例」）旨在應對不斷升級的網絡威脅，保障香港的必要服務。隨着這些服務日益依賴互聯網、電腦系統、電訊基建及智能裝置，關鍵基礎設施所面對的網絡攻擊風險亦有增無減。

是次立法為本港建立了實務框架，包括成立專責辦公室以指明關鍵基礎設施營運者，並引領他們落實更嚴格的安全要求。條例借鑒中國內地、新加坡、歐盟等領先司法管轄區的成功經驗，制定了切合本港獨特需求的安全標準。

條例對指定營運者提出明確要求，必須實施嚴密的安全協議，並在指定時間內報告電腦系統安全事故：嚴重事故須於知悉事故後12小時內通報，其他安全事件則須知悉後48小時內呈報。違例者將面臨最高500萬港元的罰款，以及持續違規會按日追加最高10萬港元罰款。

此項立法不僅關乎監管合規，更牽涉加強關鍵基礎設施的網絡韌性，確保必要服務能持續運作，維護經濟穩定，在這個互聯互通的世界中保護香港。

The Protection of Critical Infrastructures (Computer Systems) Bill aims to address the growing cyber threats to Hong Kong's essential services. As the essential services become increasingly dependent on the Internet, computer systems, telecommunications infrastructure, and smart devices, critical infrastructures are facing increasing risks of cyberattacks.

This landmark legislation establishes a practical framework, including the creation of a dedicated Commissioner's Office to designate critical infrastructure operators and guide them in implementing enhanced security requirements. Drawing on successful experience from leading jurisdictions such as Mainland China, Singapore, and the European Union, the Bill sets security standards tailored to Hong Kong's unique needs.

The legislation sets out clear obligations for designated operators to implement stringent security protocols and report computer-system security incidents within specified timeframes: serious incidents must be reported within 12 hours of becoming aware of the incident, while other incidents must be reported within 48 hours. Non-compliance may result in fines of up to HK$5 million, with an additional daily fine of up to HK$100,000 for ongoing violations.

This legislation goes beyond regulatory compliance. It strengthens the cyber resilience of critical infrastructures, ensures the continuous operation of essential services, protects economic stability, and safeguards Hong Kong in today's interconnected world.

經驗總結 Lessons Learnt

主動分析網絡威脅情報對預防潛在網絡攻擊至關重要。透過剖析過去的網絡安全事件，網罪科發現不同香港機構中被重複利用的系統安全漏洞，尤其是存取控制和配置不足、系統過時且未修補，以及欠缺威脅偵測機制。所有企業必須認真處理以下重大系統安全漏洞。

Proactive analysis of cyber threat intelligence is vital for preventing potential cyberattacks. By reviewing past cybersecurity incidents, CSTCB has identified recurring system vulnerabilities across different Hong Kong organisations, particularly inadequate access control and configuration, outdated and unpatched systems, and the lack of threat detection mechanisms. All enterprises must take these critical system vulnerabilities seriously.

1 問題一：存取控制和配置不足 Problem 1: Inadequate Access Control and Configuration

自2020年遙距辦公浪潮以來，虛擬私人網絡（VPN）通訊閘和遠端桌面協定（RDP）連接因其高權限，成為系統入侵者主要的踏腳石。

Since the remote work surge in 2020, Virtual Private Network (VPN) gateways and Remote Desktop Protocol (RDP) connections, due to their high system access privileges, have become key entry points for system intruders.

在2024年，網罪科發現網絡攻擊者持續利用兩個主要媒介來攻擊VPN通訊閘和濫用RDP以獲取未經授權的接達：

In 2024, CSTCB found that threat actors continued to exploit two primary vectors to target VPN gateways and abuse RDP for unauthorised access:

未修補的漏洞
Unpatched vulnerabilities
憑證攻擊
Credential-based attacks

攻擊者迅速利用已公開的通用漏洞披露（CVE）平台來作為武器，去攻擊VPN和RDP基礎設施中未修補的漏洞。從漏洞被公開披露，直至機構修補漏洞之間出現的時間差，仍然存在明顯安全漏洞。

Attackers rapidly weaponise vulnerabilities published on Common Vulnerabilities and Exposures (CVE) platforms to target unpatched VPN and RDP infrastructures. A significant security gap remains in the time window between public disclosure and organisational patching of these vulnerabilities.

攻擊者利用憑證攻擊成功入侵系統，包括：

- 對單一憑證系統進行暴力攻擊;
- 使用外洩數據集進行憑證填充攻擊;
- 使用常見或容易猜測的密碼進行密碼噴灑攻擊；以及
- 專門設計的魚叉式網絡釣魚活動，以獲取特定權限用戶的身份憑證。

Credential-based attacks remain an effective method for compromising systems:

- brute force attacks on single-factor authentication systems;
- credential stuffing using leaked datasets;
- password spraying with common or easily guessable passwords; and
- spear phishing campaigns designed to harvest authentication credentials from privileged users.

憑證填充攻擊 Credential stuffing

憑證填充攻擊是一種網絡攻擊技術，攻擊者利用從其他網站或數據洩露事件中獲得的用戶名和密碼組合，自動嘗試在不同的網站或服務中登錄。

Credential stuffing is a cyberattack technique where attackers use usernames and password combinations obtained from other websites or data breaches to automatically attempt logins across multiple websites or services.

因此，機構必須實施嚴格的系統安全漏洞管理流程，強制執行多重認證和帳戶鎖定政策，並建立全面的監控能力，以減輕網絡安全風險。

Therefore, organisations must implement rigorous system vulnerability management processes, enforce mandatory multi-factor authentication (MFA) and account lockout policies, and establish comprehensive monitoring capabilities to mitigate cybersecurity risks.

個案六 Case Study 6

在2024年7月，一間本地公營機構遭受勒索軟件攻擊，影響了其在兩個不同地點的用戶驗收測試（UAT）系統。調查顯示，攻擊者通過機構的虛擬私人網絡（VPN）通訊閘入侵系統，成功使用預設的「訪客」帳戶進行身份驗證。

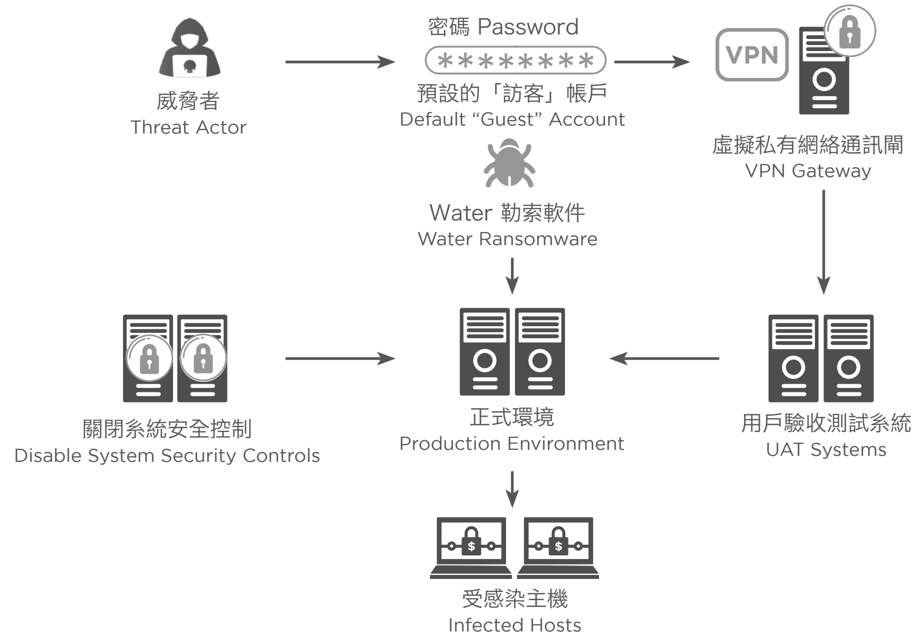
In July 2024, a local organisation fell prey to a ransomware attack that affected its User Acceptance Test (UAT) systems at two different sites. Investigation revealed that the attackers had compromised the system via the organisation's Virtual Private Network (VPN) gateway by successfully authenticating with a default "guest" account.

成功通過驗證後，攻擊者在網絡中橫向移動，關閉系統安全控制，並使用自動化程式，同時執行名為「Water」的勒索軟件（屬於名為「Phobos」的勒索軟件變種）進行加密，使機構營運中斷。

After gaining access, the attackers moved laterally across the network, disabled system security controls, and deployed "Water" ransomware (a variant of "Phobos" ransomware) using automated scripts to execute simultaneous encryption, which disrupted the organisation's operations.

是次事件顯示，針對外部遠程服務實施簡單憑證攻擊，能夠為攻擊者提供網絡存取權限，造成具毀滅性的攻擊。所有機構都應該停用預設帳戶，為遠端服務實施多重認證，並保留足夠的日誌記錄，以進行系統安全監控和保安事故應變。

This incident demonstrates how simple credential-based attacks on external remote services can grant attackers network access and enable destructive attacks. All organisations should disable default accounts, enforce multi-factor authentication (MFA) for remote services, and retain sufficient logging to support system security monitoring and incident response.



Water勒索軟件 "Water" ransomware

Water勒索軟件是臭名遠播的Phobos勒索軟件家族的一個變種。「Water」這個名稱來源於攻擊者加密文件後附加的“.WATER”檔案副檔名。

Water ransomware is a variant of the notorious Phobos ransomware family. The name "Water" likely originates from the ".WATER" file extension appended to encrypted files by the attackers.

Water勒索病毒主要利用弱遠端桌面協定連接進行攻擊，並經常使用虛擬私人網絡或代理伺服器隱藏攻擊者位置，接著加密檔案並刪除復原選項。攻擊者使用高強度加密演算法，並要求以加密貨幣支付贖金，使受害者幾乎無法自行復原數據。

Water ransomware primarily targets weak Remote Desktop Protocol (RDP) connections and often uses Virtual Private Networks (VPNs) or proxy servers to hide attackers' locations. It encrypts files using strong encryption algorithms, disables recovery options, and demands ransom payments in cryptocurrency, leaving victims with limited options for data recovery.

2 問題二：系統過時且未修補
Problem 2: Outdated and Unpatched Systems

未修補的防火牆和舊版系統仍是主要攻擊目標。當製造商發佈安全更新時，實際上等同揭露舊版本中存在的系統安全漏洞，無意間向攻擊者暴露這些系統的弱點。

Unpatched firewalls and legacy systems remain prime targets for cyberattacks. When manufacturers release security updates, they are effectively disclosing system vulnerabilities in older versions, unintentionally exposing these weaknesses to attackers.

兩個重大漏洞
Two critical vulnerability patterns

未修補和過時的安全系統
Unpatched and Outdated Security Systems

過時系統
Legacy Systems

在2024年，網罪科觀察到兩個重大漏洞：

(1)未修補和過時的安全系統

防火牆和安全系統是機構的第一道防線，但假如它們過時，便會失去保護屏障，甚至成為潛在的入侵點。未及時更新保安系統的機構會暴露於這些已知系統安全漏洞的威脅之中。

In 2024, CSTCB observed two critical vulnerability patterns:

(1) Unpatched and Outdated Security Systems

Firewalls and security systems are an organisation's first line of defence. However, if they are outdated or not properly maintained, they can become potential points of intrusion rather than protective barriers. Organisations that fail to apply timely updates leave themselves exposed to well-known system vulnerabilities.

(2)過時系統

過時系統面臨重大網絡安全風險，如欠缺保安更新及維護人員、進階系統安全功能(例如進階加密和硬件保護)不足，以及公開數據庫中已知系統安全漏洞。

(2) Legacy Systems

Legacy systems face significant cybersecurity risks, including a lack of security updates and qualified maintenance personnel, inadequate modern security features such as advanced encryption and hardware protections, and exposure to publicly documented system vulnerabilities in open databases.

個案七 Case Study 7

在2024年5月，一間本地教育機構遭到勒索軟件攻擊。調查顯示，該機構已超過一年未進行防火牆更新，導致已知的系統安全漏洞未得到處理。

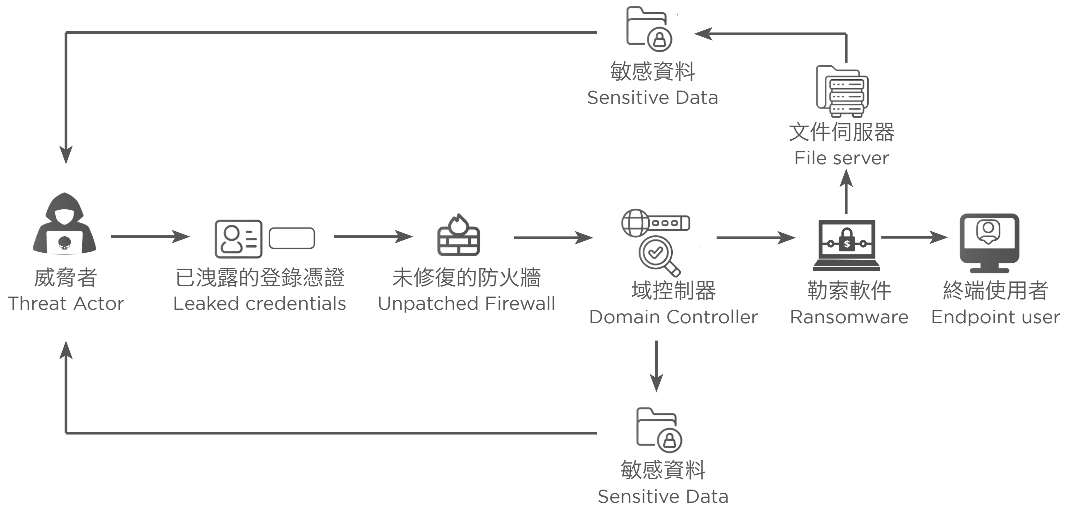
攻擊者利用一個非活躍VPN用戶的已洩露憑證，通過機構的公共VPN入口進入內部網絡。其後攻擊者在網絡中橫向移動，針對域控制器和文件伺服器等重要伺服器進行攻擊。在成功提升權限後，攻擊者嘗試執行勒索軟件，加密數據並要求支付贖金。所幸的是，個別用戶電腦上的端點保護和防毒軟件成功阻止勒索軟件進行加密。

這次事件顯示出未修補的防火牆如何削弱機構的整體防禦能力。機構必須落實健全的資訊保安管理政策，包括修補程式管理，以確保防火牆和其他重要網絡基礎設施獲得及時更新。

In May 2024, a local education institution faced a ransomware attack. Investigation revealed that the institution had not updated its firewall for over a year, leaving known system vulnerabilities unaddressed.

The attackers exploited leaked credentials from an inactive VPN user to gain access to the internal network through the institution's public VPN portal. Once inside, they moved laterally across the network, targeting critical servers such as the Domain Controller and File Server. After successfully escalating privileges, the attackers attempted to deploy ransomware, encrypt data, and demand a ransom payment. Fortunately, endpoint protection and antivirus software on some user computers successfully prevented the ransomware encryption.

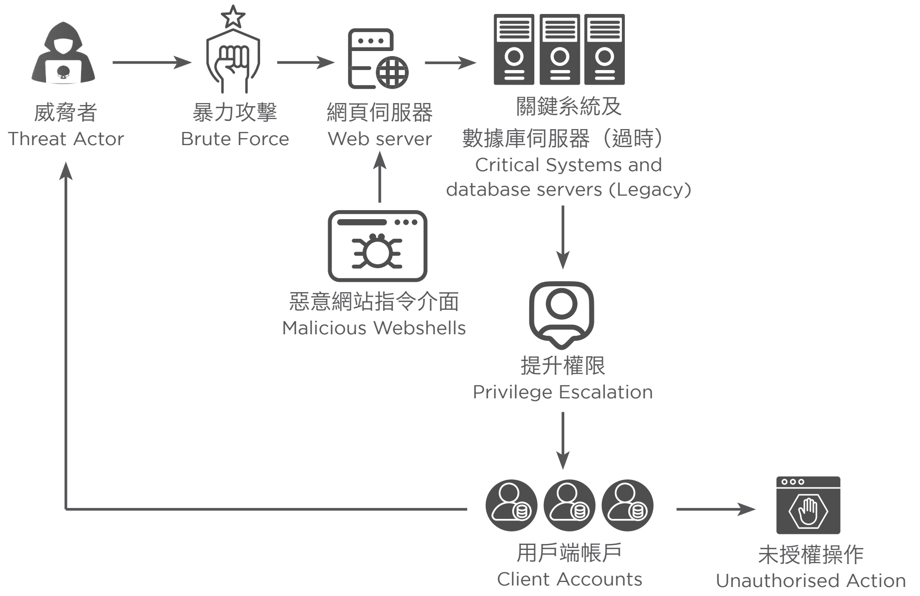
This incident demonstrates how an unpatched firewall can compromise an organisation's overall security posture. Organisations must implement a robust information security management policy, including patching management, to ensure that firewalls and other critical network infrastructure components are updated in a timely manner.



個案八 Case Study 8

在2024年12月，一間本地金融機構發現有超過100個客戶帳戶被入侵，部分帳戶被利用進行未經授權的操作。調查顯示，黑客通過暴力攻擊入侵了該公司的公共網頁伺服器，並執行了惡意的網站指令介面（Webshell）攻擊以獲取存取權限。在初步滲透後，網絡攻擊者對內部網絡進行了偵察，包括端口掃描和提升權限，進一步對重要系統和數據庫伺服器進行橫向移動。調查發現該公司仍然使用多台存在嚴重系統安全漏洞的過時伺服器。

In December 2024, a local financial institution discovered that more than 100 client accounts had been compromised, with some accounts used to carry out unauthorised transactions. Investigation revealed that the hacker had gained access to the company's public-facing web server through a brute force attack and deployed malicious webshells to establish system access. After the initial infiltration, the attacker conducted reconnaissance within the internal network, including port scanning and privilege escalation, enabling lateral movement to critical systems and database servers. Investigation revealed that the company was still using multiple legacy servers with serious system vulnerabilities.



3 問題三：欠缺威脅偵測機制
Problem 3: Lack of Effective Threat Detection Mechanism

根據網罪科觀察，受害公司通常欠缺威脅偵測機制，讓威脅者能夠入侵並潛伏於網絡中，並造成災難性後果。

受害機構平均需要258日才能識別並遏制資料外洩事件，而涉及被盜或外洩憑證的網絡攻擊則需要延長至292日才能被偵測和遏止[17]。遏制資料外洩事故的時間越長，修復其破壞的成本越高。因此，機構必須部署強大的威脅偵測機制，如保安資訊和事件管理（SIEM）系統及端點偵測和回應（EDR）解決方案，以縮短攻擊者潛伏時間並減輕對機構的潛在損害。

According to CSTCB's observations, victim companies often lacked effective threat detection mechanism, allowing threat actors to infiltrate and remain undetected within their networks, sometimes with catastrophic consequences.

On average, it took victim organisations 258 days to identify and contain a data breach. For attacks involving stolen or leaked credentials, the detection and containment period extended to 292 days[17]. The longer it takes to contain a breach, the higher the cost of damage recovery. Organisations must deploy robust threat detection capabilities, such as Security Information and Event Management (SIEM) systems and Endpoint Detection and Response (EDR) solutions, to shorten attacker dwell time and reduce potential harm to the organisation.

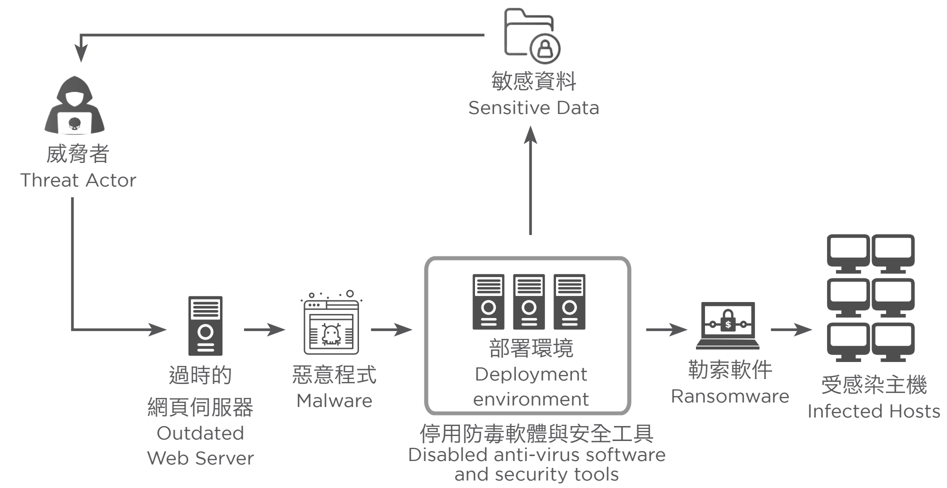
個案九 Case Study 9

在2024年3月，一間本地非牟利機構遭遇了勒索軟件攻擊，導致大量個人數據被洩露。隨後的調查顯示，威脅者最初在2022年獲取了一台連接互聯網的伺服器的接達權限，並潛伏超過兩年未被發現。在這長時間的潛伏時間內，攻擊者得以進行廣泛的偵察、關閉網絡保安控制，並最終將勒索軟體安裝在多個系統上。

調查發現，引致是次嚴重系統安全事故的其中一個原因是受害機構缺乏有效的偵測機制，以識別可疑網絡活動、監控異常登入或檢測可疑內部橫向移動。若能夠事先部署適當的威脅偵測系統，機構便可以在勒索軟件執行之前，及時發現及修補系統安全漏洞，移除潛在威脅。

In March 2024, a local non-profit organisation faced a ransomware attack, resulting in the leakage of a large volume of personal data. A subsequent investigation revealed that the threat actor had initially gained access to an Internet-facing server in 2022 and remained undetected for more than two years. During this prolonged dwell time, the attacker conducted extensive reconnaissance, disabled network security controls, and ultimately deployed ransomware across multiple systems.

The investigation concluded that one of the root causes of this severe cybersecurity incident was the organisation's lack of effective detection mechanisms. The organisation was unable to identify suspicious network activities, monitor anomalous login behaviour, or detect suspicious lateral movement within its environment. Had proper threat detection systems been implemented, the organisation would have been able to identity and remediate the system vulnerabilities in time, eliminating potential threats before the ransomware was executed.



[17] IBM Cost of a Data Breach Report (IBM數據洩露成本報告) 2024, July 2024 (2024年7月), https://www.ibm.com/reports/data-breach

如何評估你的電腦是否被入侵？
How to Assess if Your Computer Has Been Hacked?

1 檢查異常的登入活動，例如不明用戶或不正常的登入位置。
Check for unusual login activity, such as unknown user accounts or logins from unexpected locations.

2 留意系統上是否被安裝不明軟件或有未獲授權程式在系統中運行。
Watch for unfamiliar software installations or unauthorised programmes running on your systems.

3 密切監測可疑的網絡活動或異常數據流量激增情況。
Look out for suspicious network activity or unexplained spikes in data traffic.

4 留意安全設定或系統設置是否在未經授權的情況下被更改。
Watch for changes to security settings or system configurations made without authorisation.

5 注意系統頻繁崩潰、速度變慢或無法訪問的情況。
Pay attention to frequent system crashes, sluggish performance, or sudden inaccessibility to files or services.

如果應對被黑客入侵電腦？
What to Do if Your Computer Has Been Hacked?

1 立即切斷受影響設備的網絡連接。
Immediately disconnect the affected device from the network.

2 立即檢查及清理受影響電腦及終端機。
Immediately inspect and clear compromised computers and terminals.

3 立即更新和修補系統安全漏洞。
Immediately update and patch all identified system vulnerabilities.

4 進行全面的安全掃描，以偵測並移除任何惡意軟件或未經授權的工具。
Run a thorough security scan to detect and remove any malicious software or unauthorised tools.

5 向有關方面和當局報告事件，並從未受影響的備份中復原受影響的系統。
Report the incident to relevant parties and authorities, and restore affected systems using clean backups.

網絡安全專家建議
Professional Advice on Cybersecurity

保護自己，保護您的企業
Protect Yourself, Protect Your Business

個人網絡安全提示
Cybersecurity Tips for Individuals

1 設定高強度及獨特的密碼 Create strong and unique passwords

建議採用包含大小寫字母、數字及特殊符號的複雜密碼組合，切忌於不同帳戶重複使用相同的密碼。考慮使用密碼管理工具，安全儲存及管理各項登入憑證。

Use complex passwords that combine uppercase and lowercase letters, numbers, and special characters. Avoid reusing the same password across different accounts. Consider using a password manager to securely store and manage your login credentials.

5 安裝信譽良好的系統保安軟件 Install reputable security software

於個人裝置上使用可靠的防毒軟件及防火牆。市面上有不少免費或價格相宜的軟件，都能夠提供基本惡意程式偵測和即時保護功能。

Use trusted antivirus software and firewalls on your personal devices. Many free or affordable options are available that provide essential malware detection and real-time protection.

2 採用多重認證 Enable multi-factor authentication (MFA)

啟用多重認證而非依賴簡單密碼，尤其電郵、網上銀行和社交媒體等重要帳戶，務必開啟多重認證功能。使用免費的驗證應用程式亦能夠為帳戶增添多一重保障。

Strengthen your account protection by enabling MFA, especially on critical services such as email, online banking, and social media. Even free authenticator apps can enhance your account's security.

6 加強家居Wi-Fi保安 Secure your home Wi-Fi network

更改路由器出廠的預設密碼，並採用高強度加密技術（如WPA3無線加密）以增強家居網絡安全。定期檢查已連接的裝置，確保未有未經授權的設備接入。

Change your router’s default password and enable strong encryption (such as WPA3) to enhance home network security. Regularly review connected devices to ensure there are no unauthorised users.

3 定期更新軟件及裝置 Regularly update your software and devices

及早安裝作業系統、應用程式與裝置的最新安全更新。可以啟用自動更新功能簡化流程，並及時修補最新發現的系統安全漏洞。

Install the latest security updates for your operating systems, applications, and devices as soon as they become available. Enabling automatic updates can simplify this process and help patch newly discovered system vulnerabilities promptly.

7 定期備份重要數據 Regularly back up important data

定期將重要檔案備份至外置硬碟或加密雲端儲存，提高網絡韌性並確保在發生事故時能夠復原數據。

Create regular backups of important files to external hard disks or encrypted cloud storage to improve cyber resilience and ensure data recovery in case of incidents.

4 提防釣魚攻擊 Be cautious of phishing attacks

對於任何要求提供個人資料或銀行轉帳的可疑電郵或訊息，務必提高警覺。避免點擊不明連結或下載不明附件，並核實來源是否可信。

Stay vigilant against suspicious emails or messages requesting personal information or bank transfers. Avoid clicking unknown links or downloading unverified attachments. Always verify the sender’s identity through trusted channels.

8 加強網絡私隱設定 Strengthen your online privacy settings

盡量減少於社交媒體平台公開個人資料，並定期檢視各項私隱權限設定。

Minimise the amount of personal information shared on social media and routinely review your privacy settings to control who can access your data.

機構網絡安全提示
Cybersecurity Tips for Organisations

1 識別資產及進行分類
Identify and Classify Assets

清晰辨別並分類關鍵資訊系統、數據資產、硬件、軟件和網絡，以評估相關系統安全漏洞。不論機構規模大小，均可使用簡單工具進行資產識別，並隨業務發展逐步採用更完善的資產管理系統。

Clearly identify and categorise your critical information systems, data assets, hardware, software and networks to assess associated system vulnerabilities. Organisations of all sizes can begin asset identification using simple tools and gradually adopt more advanced asset management systems as their operations grow.

5 復原與重置
Recover and Restore

實施可靠的復原策略，包括定期安全備份、災難復原計劃及業務持續運作計劃。無論機構規模大小，均可先採用簡單備份與復原程序，再隨資源與業務複雜度提升擴展功能。

Adopt reliable recovery strategies, such as regular security backups, disaster recovery planning, and business continuity planning. Organisations of any size can begin with basic backup and recovery processes, then enhance them as business scale and complexity grow.

2 保護與預防
Protect and Prevent

針對已識別資產採取主動保安措施，包括嚴格存取控制、多重認證（MFA）、加密技術、安全配置、網絡安全解決方案、端點保護及員工網絡安全培訓。小型機構可從基礎措施入手，逐步加強防護機制。

Implement proactive security measures for the identified assets. These should include strict access controls, multi-factor authentication (MFA), encryption, security configurations, network security solutions, endpoint protection, and cybersecurity awareness training for employees. Small organisations can begin with basic measures and scale up their protective controls over time.

6 管治與風險管理
Governance and Risk Management

採用風險為本的方法，以一致及有效的方式識別資訊系統的保安風險、訂定應對風險的緩急次序和應對有關風險。小型機構可先進行簡單保安審計，隨規模擴大逐步制定資訊保安政策及標準。

Adopt a risk-based approach to identify, prioritise and mitigate information system security risks in a consistent and effective manner. Small organisations may start with simple security audits and gradually develop comprehensive information security policies and standards as they grow.

3 偵測與監控
Detect and Monitor

部署有效的監測與偵測方案，包括網絡入侵偵測系統(NIDS)、保安資訊與事件管理工具（SIEM）平台、網絡監控工具及端點偵測與回應（EDR）系統。早期偵測機制有助及時發現網絡安全威脅及異常活動。機構可從基本監控開始，隨資源增加逐步採用更全面的工具。

Deploy effective monitoring and detection tools, such as Network Intrusion Detection Systems (NIDS), Security Information and Event Management (SIEM) platforms, network monitoring tools, and Endpoint Detection and Response (EDR) solutions. Early detection helps identify threats and anomalies promptly. Organisations can start with basic monitoring and progressively adopt more comprehensive tools as their resources permit.

7 第三方風險管理
Third-party Risk Management

評估及管理供應商或服務供應商等外部利益相關者潛在的網絡安全風險。通過識別依賴關係，各機構可以評估相關網絡安全風險，並採取適當的系統安全措施。

Evaluate and manage potential cybersecurity risks posed by external parties, such as vendors or service providers. By identifying dependencies, organisations can assess and address associated cybersecurity risks with appropriate system security measures.

4 應變與減低風險
Respond and Mitigate

建立明確的事故應變程序，界定事故控制、緩解、通報及復原等工作的具體角色和職責。小型團隊可先建立簡單的應變方案，大型機構則應實施詳細事故應變流程並組建專責應變小組。

Establish clear incident response procedures, including defined roles and responsibilities for incident containment, mitigation, reporting, and recovery. Small teams can begin with a simple, practical response plan, while larger organisations should implement detailed incident response workflows and form dedicated incident response teams.

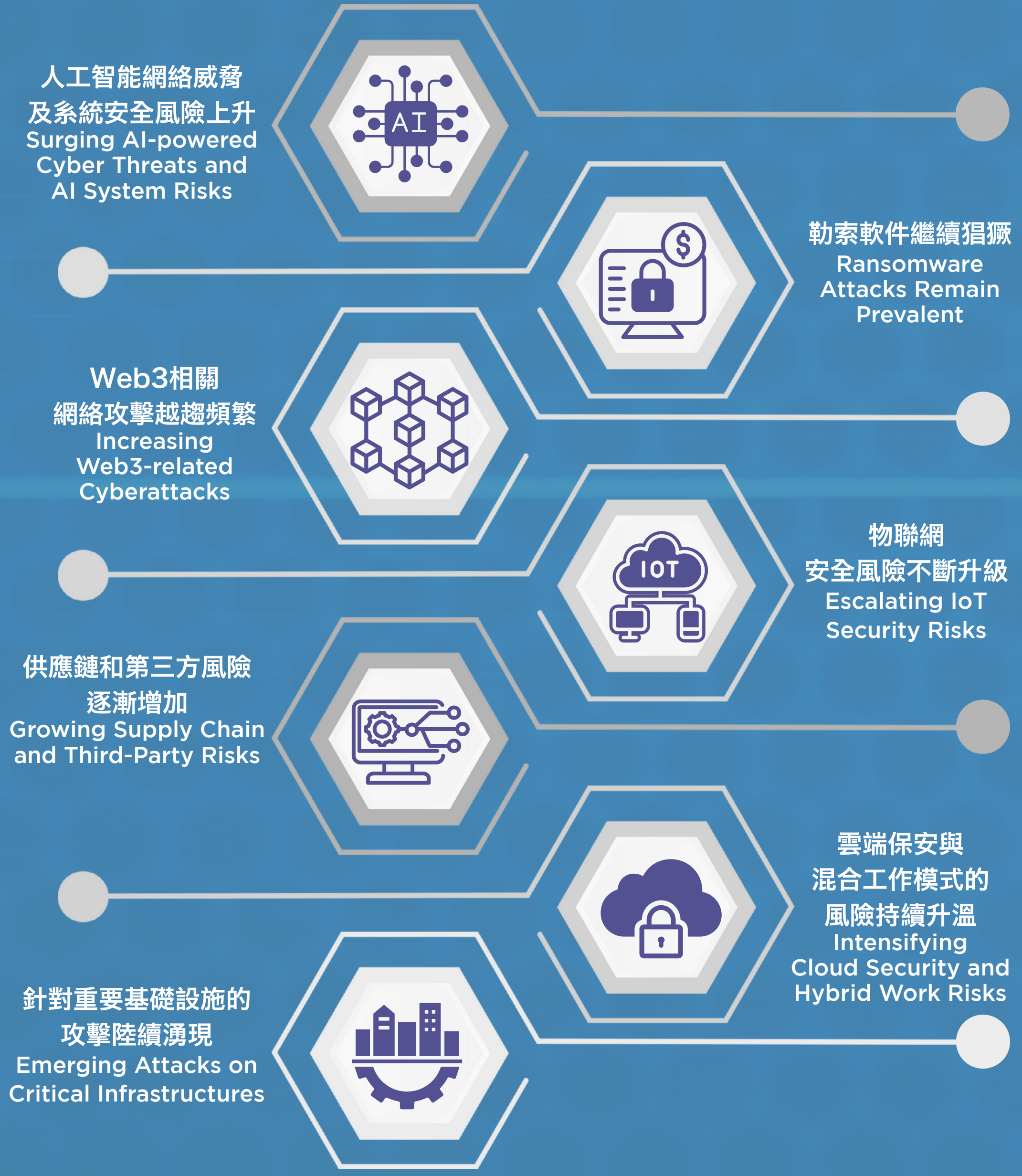
8 持續改進
Continuous Improvement

透過定期進行網絡保安審計、滲透測試、漏洞評估及網絡安全演習，持續檢視網絡安全成效。機構可先利用不同免費資源，尤其是網罪科所提供的不同活動，再按實際情況逐步採用更先進的技術與評估。

Regularly assess cybersecurity effectiveness through audits, penetration testing, vulnerability assessments, and cybersecurity drills. Organisations can utilise free resources, in particular those offered by CSTCB, and scale up to more advanced tools and evaluation techniques as capacity allow.

2025年網絡威脅預測

Cyber Threat Forecast 2025



人工智能網絡威脅
及系統安全風險上升
Surging AI-powered
Cyber Threats and
AI System Risks

勒索軟件繼續猖獗
Ransomware
Attacks Remain
Prevalent

Web3相關
網絡攻擊越趨頻繁
Increasing
Web3-related
Cyberattacks

物聯網
安全風險不斷升級
Escalating IoT
Security Risks

供應鏈和第三方風險
逐漸增加
Growing Supply Chain
and Third-Party Risks

雲端保安與
混合工作模式的
風險持續升溫
Intensifying
Cloud Security and
Hybrid Work Risks

針對重要基礎設施的
攻擊陸續湧現
Emerging Attacks on
Critical Infrastructures

面對日新月異的網絡威脅，必須時刻保持警覺
As cyber threats rapidly evolve, it is crucial to stay vigilant

2025年網絡威脅預測
Cyber Threat Forecast 2025

Web3相關網絡攻擊越趨頻繁
Increasing Web3-related Cyberattacks

隨着香港積極發展成為全球領先的Web3和虛擬資產樞紐，針對區塊鏈、加密貨幣交易所和智能合約的網絡威脅將不斷增加。加密資產盜竊、智能合約漏洞攻擊以及詐騙計劃等攻擊會導致財政損失，同時削弱投資者信心。加強網絡保安協議和遵守監管合規，將是保護香港在Web3和虛擬資產生態系統中領先的關鍵。

With Hong Kong emerging as a leading global hub for Web3 and virtual assets, cyber threats targeting blockchain, cryptocurrency exchanges, and smart contracts are expected to rise. Attacks such as crypto heists, smart contract exploits, and scam schemes could lead to financial losses, and also undermine investor confidence. Enhanced cybersecurity protocols and stringent regulatory compliance will be crucial to maintaining Hong Kong's leading position in the Web3 and virtual asset ecosystem.

勒索軟件繼續猖獗
Ransomware Attacks Remain Prevalent

勒索軟件在2025年將繼續構成重大風險，為攻擊者提供牟利的途徑。香港擁有龐大的資金流及數據流，吸引網絡犯罪分子尋找高價值目標。即使如此，不論機構規模的大小，都有機會面對勒索軟件攻擊。因此，機構必須制定健全的備份策略、保安事故應變計劃以及安全意識培訓，以對抗這些持續威脅。

Ransomware will continue to pose significant risks in 2025, providing attackers a profitable avenue. Hong Kong's massive flow of capital and data makes it a prime target for cybercriminals. Nevertheless, organisations of all sizes remain potential targets for ransomware attacks. Therefore, it is imperative for organisations to develop robust backup strategies, incident response plans, and security awareness training to defend against these persistent threats.

物聯網安全風險不斷升級
Escalating IoT Security Risks

香港擁有全球最先進的物聯網（IoT）生態之一，包括廣泛設置的電視幕牆、智慧燈柱、智能泊車咪錶等設備，也因此面臨獨特的網絡安全挑戰。隨着香港推動低空經濟及推廣大型活動，物聯網技術中的系統安全漏洞，特別是數碼顯示屏系統和無人機控制系統，對香港的數碼基礎設施和公共安全構成了日益嚴重的威脅。全面落實物聯網安全標準並定期評估漏洞，對保護這些互聯互通的系統至關重要。

With one of the world's most advanced Internet of Things (IoT) ecosystems, including large-scale deployments of digital billboards, smart lampposts, and smart parking meters, Hong Kong faces unique IoT cybersecurity challenges. As Hong Kong advances low-altitude economy and promotes mega events, vulnerabilities in IoT systems, especially digital signage and drone control systems, pose growing threats to digital infrastructure and public safety. Adopting comprehensive IoT security standards and conducting regular vulnerability assessments will be crucial.

供應鏈和第三方風險逐漸增加
Growing Supply Chain and Third-Party Risks

香港對全球供應鏈和第三方服務的依賴將增加網絡風險。第三方軟件、供應商以及開源組件中的保安漏洞，可能導致供應鏈攻擊、數據外洩，甚至面臨法律或財政上的責任。本地機構必須加強對第三方服務的安全評估和監控。

Hong Kong's reliance on global supply chains and third-party services will amplify cybersecurity risks. Vulnerabilities in third-party software, vendors, and open-source components could lead to supply chain attacks, data breaches, and legal or financial repercussions. Local organisations must enhance their third-party security assessment and monitoring practices.

雲端保安與混合工作模式的風險持續升溫
Intensifying Cloud Security and Hybrid Work Risks

隨着香港機構加強採用雲端服務和混合工作模式，同時亦擴大了機構的攻擊面。網絡威脅包括錯誤雲端服務配置及遠端存取漏洞等，可能導致數據洩露、監管處罰、客戶資料外洩以及損害機構聲譽。嚴格的雲端管理和安全的遠程工作措施變得尤其重要。

The increasing adoption of cloud services and hybrid work models is expanding attack surface for organisations in Hong Kong. Common cyber threats include cloud service misconfigurations and remote access vulnerabilities, each capable of leading to data leaks, regulatory penalties, customer exposure, and reputational damage. Stringent cloud governance and secure remote work practices will be critical.

針對重要基礎設施的攻擊陸續湧現
Emerging Attacks on Critical Infrastructures

針對重要基礎設施及其運營科技（OT）系統的網絡攻擊將加劇，對香港的必要服務和公用事業構成重大威脅。這些複雜的攻擊可能引發廣泛的服務中斷，並危及公共安全。為應對這些威脅，機構必須優先考慮電腦系統及OT系統網絡安全，加強網絡安全事故偵測能力，並加強公私營合作以保護重要基礎設施。

Cyberattacks targeting critical infrastructures and their operational technology (OT) systems are expected to intensify, posing significant threats to Hong Kong's essential services and public utilities. These sophisticated attacks can cause widespread service disruptions and endanger public safety. Organisations must prioritise cybersecurity for both IT and OT systems, enhance cybersecurity incident detection capabilities, and strengthen public-private collaboration to protect critical infrastructures.

人工智能網絡威脅及系統安全風險上升
Surging AI-powered Cyber Threats and AI System Risks

人工智能驅動的網絡攻擊將在2025年變得更加先進和無處不在。威脅者不但將人工智能融合到他們的戰術中，同時也視人工智能系統為攻擊目標。隨着本地機構採用更多的人工智能應用程式、自動化代理和大型語言模型（LLMs），這些技術亦帶來了新的攻擊面和系統安全漏洞，例如提示詞注入、資料投毒和操縱數據。人工智能安全乃國家安全的重點領域之一，各機構必須實施人工智能安全措施和先進的威脅檢測系統，以減輕這些不斷演變的風險。

AI-powered cyberattacks are expected to become more advanced and widespread in 2025. Threat actors are increasingly incorporating AI into their attack tactics while also targeting AI systems themselves. As local organisations adopt more AI applications, autonomous agents, and large language models (LLMs), new attack surfaces and system vulnerabilities, such as prompt injection, data poisoning, and data manipulation, emerge. AI security is a key component of national security. Organisations must implement AI security measures and advanced threat detection systems to mitigate these evolving risks.

Mr. Neal JETTON

國際刑警組織
網絡犯罪主管
Director of
Cybercrime, INTERPOL

INTERPOL

隨着犯罪分子利用生成式人工智能等新興技術，提升各種網絡犯罪的能力，執法機關打擊網絡犯罪的策略亦必須因時制宜。國際刑警組織網絡犯罪總局認同，打擊網絡犯罪最有效的應對措施，需結合私營機構夥伴、司法當局及全球執法部門的協調行動。然而，我們每個人都應採取預防措施，對於點擊的連結，以及透過電話、視訊、電子郵件或簡訊往來的對象，都應保持謹慎，使網絡犯罪分子更難得逞。

As criminals leverage emerging technologies, such as generative AI, to improve their ability to commit a variety of cybercrimes, law enforcement's strategy to investigate these crimes must also evolve. INTERPOL's Cybercrime Directorate recognises that the most impactful response will require coordinated efforts between relevant private sector partners, judicial authorities, and the global law enforcement community. However, it is incumbent on each of us to take precautionary measures to make it more difficult for cybercriminals - be cautious of what we click and who we communicate with via phone, video, email or text.

由2025年起，全球網絡安全形勢將聚焦於整合新興技術，以應對日益精密的網絡威脅，致力落實數據保護。各國政府及不同機構將積極運用人工智能與機器學習來提升威脅偵測與事故應變能力，對持續演變且日趨普遍的網絡攻擊保持警覺。此外，優先進行全面的員工培訓尤為重要，以強化應變技能，並培養數據保護的意識文化。各國政府、公私營機構、內地與國際夥伴必須互相協作，從而應對不斷變化的網絡威脅形勢，維護整體國家安全，確保數字經濟的可持續發展。

In 2025 and beyond, the landscape of global cybersecurity is expected to focus on the integration of emerging technologies to tackle increasingly sophisticated cyber threats, with a strong commitment to data protection. Governments and organisations are likely to utilise artificial intelligence and machine learning to enhance their threat detection and response capabilities, ensuring their vigilance against evolving and more and more pervasive attacks. Prioritising comprehensive employee training will be crucial to sharpen up the combating skills and cultivate a culture of awareness in data protection. Collaborative initiatives among governments, public and private sectors, the Mainland and international partners play a vital role in effectively addressing the ever-changing landscape of cyber threats and safeguarding our national security as a whole while ensuring the sustainable growth of the digital economy.

黃志光先生
Mr. Tony WONG

數字政策辦公室 數字政策專員
Commissioner for Digital Policy,
Digital Policy Office

中華人民共和國香港特別行政區政府
數字政策辦公室
Digital Policy Office
The Government of the Hong Kong Special Administrative Region
of the People's Republic of China

齊向東先生
Mr. QI Xiangdong

奇安信科技集團 董事長
Chairman, QAX
Technology Group

奇安信

用內生安全驅動人工智能安全將成為行業趨勢。DeepSeek大模型開源引爆了人工智能“應用競賽”，應用的核心是資料，資料安全決定人工智能安全。那些掛接在大模型上資料，不再是“大資料”，而是“小資料”，“小資料”更容易被盜竊、被破壞、被勒索。解決“小資料”安全，必須建設內生安全體系，把安全能力內生到智慧場景、業務流程、資料治理之中，即能防黑客攻擊，又防“三員”內部作案。

As artificial intelligence surges forward, so too does the severity and sophistication of cyber threats. Today's AI race—ignited by the open-sourcing of DeepSeek's powerful foundational models—puts data squarely in the spotlight. But unlike the era of big data, the AI revolution now centres around highly sensitive, proprietary datasets, which are increasingly vulnerable to theft, sabotage, and ransomware attacks. Embedding comprehensive security measures directly into intelligent platforms, operational workflows, and data governance is necessary to safeguard against external cybercriminals but also internal threats posed by developers, operators, and administrators.

羅家偉助理警察總監
Assistant Commissioner of
Police Kah Wai LOH

國際刑警組織亞洲及南太平洋
網絡犯罪聯合工作小組 主席
Chairperson, INTERPOL
Asia and South
Pacific (ASP)
Working Group
on Cybercrime

新加坡警察部隊刑事偵查局
科技罪案調查署 助理局長
Assistant Director,
Technology Crime Division,
Criminal Investigation Department,
Singapore Police Force

隨着人工智能、區塊鏈、雲端服務、5G及量子計算等技術的興起，網絡犯罪分子將利用這些新興技術，使網絡威脅變得更加嚴峻。因此，不論個人還是機構組織都必須落實良好的網絡安全習慣、採取嚴密的安全防護措施、通報可疑活動，並積極推廣網絡安全教育。

執法機關通力合作至關重要，透過資訊共享、結合專業知識、促進公私夥伴關係及聯合行動，我們可增強該地區的網絡韌性和能力。國際刑警組織亞洲及南太平洋工作小組致力於促進多方合作、提升執法能力並推動各執法機關建立伙伴關係，及共同打造更安全的網絡環境。面對持續演變的威脅，我們必須群策群力。

Cyber threats will intensify with the rise of artificial intelligence, blockchain, cloud services, 5G, and quantum computing. Cybercriminals will exploit these technologies, making it imperative for individuals and organisations to practise good cyber hygiene, adopt robust security measures, report suspicious activities, and promote cyber literacy.

Collaboration among law enforcement agencies is crucial. By sharing information, leveraging collective expertise, fostering public-private partnerships, and participating in joint operations, we can enhance the region's cyber resilience and capabilities. The INTERPOL Asia and South Pacific Working Group is committed to facilitating joint efforts, capacity building, and fostering partnerships to create a safer cyber environment for all. A collective approach is essential to stay ahead of evolving threats.

人工智能的快速發展為人們帶來了精彩的機遇，但同時也帶來了新的風險，例如高度逼真的偽造影像、語言和故事。隨着各行業加速數字化，人工智能、雲計算、物聯網、開放源碼和低空技術的應用日益增多，黑客和不法分子有了更多可利用的機會，造成隱蔽且迅速的重大危害。應對這些挑戰需要社會各界的共同合作。

令人鼓舞的是，香港警察高度重視科技和網絡安全，積極擁抱創新技術，廣泛徵詢業界專家意見，不斷提升應對這些挑戰的能力。同時，他們也積極推動全社會各層面對網絡安全的認知與意識，致力於保護公眾和社會的安全。

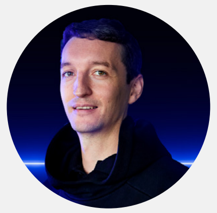
The rapid development of artificial intelligence brings exciting opportunities but also new risks, such as highly realistic fake images, language, and stories. With industries accelerating digitalisation and increasing applications of AI, cloud computing, IoT, open-source, and low-altitude technologies, hackers and malicious actors have more opportunities to exploit, causing significant, concealed, and swift harm. Addressing these challenges requires joint efforts from all sectors of society.

It is encouraging to see the Hong Kong Police prioritising technology and cybersecurity, embracing innovation, consulting industry experts, and continuously enhancing their capabilities to tackle these challenges. At the same time, they actively promote cybersecurity awareness across all levels of society, striving to protect public and community safety.

鄭松岩博士
Dr. Rocky CHENG

數碼港 行政總裁
CEO, Cyberport

數碼港
Cyberport



Mr. Dmitry VOLKOV

Group-IB
行政總裁及技術總監
CEO & CTO, Group-IB

GROUP-IB

2024年的網絡威脅形勢凸顯了Group-IB打擊網絡犯罪的使命的迫切性。隨着人工智能驅動的威脅、勒索軟件以及日益複雜的高級持續性威脅不斷演變，2025年的網絡威脅並非單一事件，而是日益增長且互相連結的網絡犯罪鏈的一部分。對手將不斷精進其戰略並大規模利用保安漏洞，沒有任何組織或國家能夠單獨應對這些挑戰。要建立真正的網絡韌性，需要依靠情報主導的網絡保安、主動式防禦措施，以及私營企業、政府與執法機構之間的緊密合作。通過加強全球協作和瓦解犯罪網絡，我們才可以構建一個更安全、更具韌性的數碼未來。

The 2024 cyber threat landscape reinforced the urgency of Group-IB's mission - to fight against cybercrime - as AI-driven threats, ransomware, and increasingly sophisticated Advanced Persistent Threats continue to evolve. The cyber threats of 2025 are not isolated incidents but part of a growing, interconnected web of cybercrime, where adversaries refine their tactics and exploit vulnerabilities at scale. No organisation or nation can face these challenges alone. True resilience requires intelligence-driven security, proactive defences, and strong collaboration between private enterprises, governments, and law enforcement. By strengthening global cooperation and disrupting criminal networks, we can build a safer and more resilient digital future for all.

鄧偉政先生
Mr. Richard TENG

幣安 行政總裁
CEO, Binance

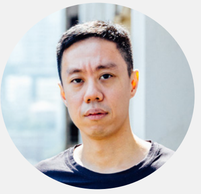
BINANCE

區塊鏈及人工智能等新興技術正重塑網絡犯罪的格局，並為執法工作帶來全新挑戰。儘管這些技術為創新與效率方面帶來巨大的潛力，卻也為不法活動提供了新的途徑。因此，我們迫切需要加強公私營合作、國際協作以及在犯罪預防與警務工作的教育，以保障用戶安全。每一位持份者的參與皆至關重要。

在幣安（Binance），我們積極支持全球反網絡犯罪的行動，並率先推出業界首創的培訓計劃。我們與全球執法機關（包括香港警務處）的緊密合作，充分體現我們對這些行動的承諾。我們有信心這些合作將樹立新的業界標準，大幅強化Web3生態系統的安全性與誠信度。

Emerging technologies such as blockchain and AI are reshaping the landscape of cybercrime, posing new challenges for law enforcement. While these technologies offer immense potential for innovation and efficiency, they also create new avenues for illicit activities. Therefore, there is a critical need for enhanced public-private collaboration, international cooperation, and education in crime prevention and policing to keep users safer. Every stakeholder's involvement is essential.

At Binance, we proactively support anti-cybercrime efforts worldwide and have pioneered industry-first training programmes. Our partnerships with the global law enforcement community, including the Hong Kong Police Force, demonstrate our dedication to these initiatives. We are optimistic that these collaborations will set new industry standards, significantly bolstering the security and integrity of the Web3 ecosystem.



顏國定先生
Mr. Kok Tin GAN

羅兵咸永道網絡安全
及私隱服務 合夥人
Partner, PwC Cyber
Security & Privacy

DarkLab聯合創辦人
Co-founder, DarkLab

pwc

人工智能驅動的惡意軟件和自動釣魚攻擊的興起，標誌着網絡威脅的關鍵性演變，使攻擊者能以前所未有的速度和個人化方式利用漏洞。不但依賴靜態規則的傳統防禦措施難以跟上步伐，孤立的防禦系統亦同樣脆弱。政府和企業必須共同開發實時數據共享框架和標準化保安事故應對協議。只有通過統一及具適應性的策略，我們才能確保攻擊手段的進步能夠以同樣靈活和協作的防禦措施應對。

The rise of AI-powered malware and automated phishing campaigns signals a critical evolution in cyberthreats, enabling attackers to exploit vulnerabilities with unprecedented speed and personalisation. Traditional defences, reliant on static rules, struggle to keep pace. Siloed defences remain vulnerable; governments and enterprises must co-develop frameworks for real-time data sharing and standardised response protocols. Only through unified, adaptive strategies can we ensure that advancements in attack vectors are met with equally agile, cooperative defences.

Mr. Dave WEST

思科亞太、日本和
大中華區 總裁
President, Cisco Asia
Pacific, Japan and
Greater China

CISCO

2025年人工智能將由工具演變為協作夥伴，提高生產力的同時也帶來影子人工智能和安全漏洞等風險。企業應當管理第三方人工智能應用程式並在整個生命週期中確保人工智能模型的安全。同時，企業需要結合硬件、軟件和服務的全面資訊科技基礎設施，以增強韌性應對網絡威脅。思科2025年網絡安全準備度指數顯示，86%的機構近期面對與人工智能相關的安全事件，凸顯了制定穩健安全策略應對人工智能挑戰的必要性。隨着機構為人工智能主導的未來做準備，他們應當利用相關科技來提升運營的生產力和韌性。

In 2025, AI will evolve from a tool to a collaborator, enhancing productivity but also introducing risks such as shadow AI and security vulnerabilities. Companies should manage third-party AI apps and secure AI models throughout their lifecycle. A holistic IT infrastructure approach, combining hardware, software, and services, is essential for resilience against cyber threats. Cisco's Cybersecurity Readiness Index 2025 reveals 86% of organisations faced AI-related security incidents recently, highlighting the need for robust security strategies to address AI challenges. As organisations prepare for a future dominated by AI, they should harness relevant technologies to drive productivity and resilience in their operations.

夏其才先生
Mr. Eugene HA

國際信息系統審計協會
(中國香港分會) 會長
President, ISACA
China Hong Kong Chapter

ISACA
China Hong Kong Chapter

在當今數碼生態系統中，強大且穩健的網絡安全策略對於組織與個人而言至關重要。隨着網絡威脅持續演變，企業必須採取全面的安全架構與保安事故應急響應機制，以有效保護關鍵資產與敏感信息。

為了有效管理漏洞，必須實施嚴格的網絡衛生措施，包括多因素身份驗證、定期修補漏洞、主動偵測安全威脅、實施零信任架構，以及採用先進的自動化安全解決方案。此外，通過針對性的安全意識培訓，促進整個機構的安全文化建設亦為不可或缺。

將網絡安全深度融入組織策略與日常營運，能夠構建具有韌性的數碼環境，有效抵禦新興威脅，並同時維持業務連續性並增強持份者的信任。

In today's digital ecosystem, robust cybersecurity practices are imperative for organisations and individuals alike. Cyber threats continue to evolve, necessitating comprehensive security frameworks and incident response protocols to protect critical assets and sensitive data.

Effective vulnerability management requires implementing stringent cyber hygiene: multi-factor authentication, regular patching, proactive threat hunting, Zero Trust architecture implementation, and advanced security automation. Equally crucial is cultivating an organisation-wide security mindset through targeted education programmes.

By integrating cybersecurity into organisational strategy and operations, organisations can establish resilient digital environments capable of withstanding emerging threats while supporting business continuity and stakeholder trust.

賈磊先生
Mr. Jeremy JIA

深信服 國際市場部總裁
President of International
Market Department,
Sangfor Technologies

SANGFOR
深信服科技

2025年香港數碼轉型加速，企業面對更複雜的網絡安全威脅。為應對挑戰，企業須引入AI技術、零信任架構及SASE方案，加強勒索軟件防禦與遠端工作安全。同時，私隱條例日益嚴格，政府將推新法例應對跨境網絡犯罪，企業必須符合法規要求，以保護數據並維持競爭力。

In 2025, Hong Kong's rapid digital transformation intensifies cybersecurity challenges. Enterprises must adopt AI-driven solutions, Zero Trust architecture, and SASE frameworks to combat ransomware and secure remote work. With stricter privacy laws and upcoming cybersecurity legislation targeting cross-border threats, compliance becomes critical. Businesses need to invest in data protection and intelligent, automated defence systems to ensure resilience, stay competitive, and support Hong Kong's role as a digital hub. Processing procedures comply with regulations to avoid legal and reputational risks.

歐勝傑先生
Mr. Chad OLSEN

畢馬威諮詢法證會計
服務 香港主管合夥人
Forensic Leader,
Hong Kong,
KPMG Advisory

KPMG

在香港2025年網絡安全形勢中，即使最先進的防禦系統也可能因簡單疏忽而失效。儘管組織大量投資於先進技術，攻擊者仍經常利用弱密碼、過時軟件和未修補系統等基本漏洞。在某些情況下，人力資源部門在無意中可能招聘了來自受制裁國家、冒充IT分判商的員工，從內部入侵網絡。犯罪集團如同商業企業般運作，不斷尋求低風險、高回報的方法，其中深度偽造詐騙被用於觸發未經授權的資金轉賬，尤其陰險。這些看似微小的弱點凸顯了人為失誤如何仍是關鍵入侵點，讓網絡犯罪分子能夠繞過最精密的安全措施。

In Hong Kong's 2025 cybersecurity climate, even the most sophisticated defences can falter due to simple oversights. While organisations invest heavily in advanced technologies, attackers often exploit basic vulnerabilities such as weak passwords, outdated software, and unpatched systems. In some cases, HR departments unintentionally onboard workers from sanctioned nations posing as IT subcontractors, exposing networks from within. Criminal groups, operating like commercial enterprises, consistently seek low-risk, high-reward approaches, with deepfake scams emerging as a particularly insidious tactic for triggering unauthorised fund transfers. These seemingly minor weaknesses underscore how human error remains a key entry point, enabling cybercriminals to bypass even the most elaborate security measures.

網絡安全主動措施
Cybersecurity Initiatives

- 國際合作 International Cooperation
- 建立網絡韌性 Building Cyber Resilience
- 策略性諮詢與合作 Strategic Advisory and Partnership
- 立法工作 Legislative Work
- 宣傳及公眾教育 Publicity and Public Education

國際合作
International Cooperation

網絡及實體反恐聯合演練2024
Counter Cyber and Physical Terrorism Joint Exercise 2024

網罪科與國際刑警組織、新加坡警察部隊和網絡安全局、澳門司法警察局在2024年第三季舉辦代號「戰風」的跨地域網絡及實體反恐聯合演練，藉此加強人員的網絡及實體反恐應變能力，並進一步提升各地政府及主要基建設施管理機構在預防、偵測、情報交流和溝通協調的整體能力。演練分為桌上及實地演練兩階段進行，逾370名本港、新加坡及澳門三地的執法部門、國際刑警組織和四個主要基建設施管理機構參與。

In the third quarter of 2024, CSTCB held the cross-border Counter Cyber and Physical Terrorism Joint Exercise, codenamed BATTLEAIR, in collaboration with INTERPOL, the Singapore Police Force (SPF), the Cyber Security Agency of Singapore and the Macao Judiciary Police (MJP). The exercise aimed to strengthen cyber and physical counter-terrorism response capabilities, while enhancing the overall capacity of governments and major infrastructure organisations in prevention, detection, intelligence sharing, and inter-agency coordination. The exercise was conducted in two phases, including a tabletop and on-site exercises, and involved over 370 participants from law enforcement agencies in Hong Kong, Singapore and Macao, as well as INTERPOL and four major infrastructure organisations.

網絡指揮官課程
Cyber Command Course

網罪科於2025年2月舉辦了「網絡指揮官課程2025」，並邀請了30名來自澳門司法警察局及香港警方各刑事單位的指揮官參與。課程除了邀請到律政司、金管局及本地和海外的網絡安全及互聯網監管專家分享專業知識，學員亦參觀了人工智能科技公司商湯集團位於科學園的科技展覽，了解新世代科技發展及應用。

網罪科總警司林焯豪期後率領11位刑事部代表團前往泰國曼谷，與國際刑警組織合作舉辦海外「網絡指揮官課程2025」，並以副主席身份引領國際刑警組織亞洲及南太平洋網絡犯罪聯合工作小組首次針對「資訊竊取惡意程式」的跨國聯合打擊行動工作會議。除了警隊代表團，課程共有30名海外網絡指揮官分別來自22個國家及地區，以及23名來自聯合國毒品及犯罪問題辦公室、世界經濟論壇、英國外交及聯邦事務部、網絡安全及虛擬資產行業的代表參與，共同鞏固國際間的合作關係，打擊網絡犯罪。

In February 2025, CSTCB hosted the Cyber Command Course 2025, bringing together 30 commanders from MJP and various criminal investigation units of the Hong Kong Police Force (HKPF). Apart from expert sharing from the Department of Justice (DOJ), the Hong Kong Monetary Authority, as well as local and overseas cybersecurity and internet regulation experts, participants also visited the technology exhibition of AI company SenseTime Group Inc. at Hong Kong Science Park, gaining insights into the development and application of next-generation technologies.

CSP of CSTCB LAM Cheuk-ho then led an 11-member delegation to Bangkok, Thailand, to co-host the overseas Cyber Command Course 2025 with INTERPOL. As the Vice-chairperson of INTERPOL Asia and South Pacific (ASP) Working Group on Cybercrime, he also chaired a coordination meeting of the group's first transnational joint operation targeting information-stealing malware. In addition to the Hong Kong delegation, the course included 30 overseas cyber commanders from 22 countries and regions, along with 23 representatives from the United Nations Office on Drugs and Crime (UNODC), the World Economic Forum (WEF), the UK Foreign, Commonwealth and Development Office (FCDO), and the cybersecurity and virtual asset sectors. The event served to further reinforce international cooperation in the global fight against cybercrime.

第一屆國際刑警組織亞洲及南太平洋網絡犯罪聯合工作小組會議
The 1st INTERPOL Asia and South Pacific Working Group Meeting in Joint Operations on Cybercrime

網罪科總警司林焯豪於2024年9月，率領代表團到菲律賓馬尼拉出席第一屆國際刑警組織亞洲及南太平洋網絡犯罪聯合工作小組會議，並獲選為該工作小組的副主席，帶領及致力深化亞洲及南太平洋地區共24個國家及地區的執法機關之間的合作、制定打擊網絡犯罪策略、加強情報交流及提升共同打擊網絡犯罪的聯合行動能力。

In September 2024, CSP of CSTCB LAM Cheuk-ho led a delegation to Manila, the Philippines, to attend the 1st INTERPOL Asia and South Pacific Working Group Meeting in Joint Operations on Cybercrime. CSP LAM was appointed the Vice-Chairperson of the Working Group, taking the lead in strengthening collaboration among law enforcement agencies from 24 countries and regions across Asia and the South Pacific. His mandate includes formulating regional cybercrime strategies, strengthening intelligence exchange and enhancing joint operational capabilities in combating cybercrime.

第14屆國際刑警網絡犯罪首長級工作坊
The 14th INTERPOL Cybercrime Directors Workshop

由網罪科與國際刑警組織合辦的第14屆國際刑警網絡犯罪首長級工作坊於2024年10月成功舉行。工作坊匯聚了國際刑警人員及來自五個司法管轄區的網絡犯罪首長人員參與，包括中國大陸、新加坡、南韓和香港，及通過線上方式參與的日本。在網絡犯罪首長會議中，由執法機關代表及來自網罪科網絡安全特別行動小組的專家亦一同參與座談會，重點討論深偽技術、人工智能相關網絡犯罪、勒索軟件和惡意軟件威脅等議題。來自警隊各區和總部的220多名參與調查網絡犯罪人員也出席研討會。是次活動除了讓各地區代表的官員積極交流他們所面臨的網絡犯罪挑戰外，更提供了一個讓執法機關與行業專家互動的平台，達致雙方加強合作，並推動創新解決方案。

The 14th INTERPOL Cybercrime Directors Workshop, jointly organised by CSTCB and INTERPOL, was successfully conducted in October 2024. The workshop brought together INTERPOL officials and cybercrime leaders of five jurisdictions, including Mainland China, Singapore, South Korea and Hong Kong, with Japan participating virtually. During the Cybercrime Directors' Sharing Conference, representatives from law enforcement agencies and experts from CSTCB's Cyber Security Action Task Force (CSATF) joined panel discussions focusing on key topics such as deepfake technology, AI-related cybercrime, ransomware, and malware threats. The workshop brought together over 220 cybercrime investigators from various police districts, regions and headquarters. The event not only created an opportunity for senior officers to exchange insights regarding current cybercrime challenges, but also served as a platform for law enforcement agencies and industry experts to engage directly, strengthen cross-sector collaboration and foster the development of innovative solutions.

跨境聯合執法行動
Cross-Border Joint Enforcement Operations

相片來源: 星島日報[18]
(Source: Singtao)[18]

網罪科於2024年6月中旬與新加坡警察部隊和馬來西亞皇家警察展開名為「遙嶺」的聯合行動，成功瓦解一個以馬來西亞為基地、針對新加坡和香港受害者的跨境詐騙集團。是次行動中拘捕多名人士，成功打擊一個跨境犯罪集團，維護相關司法管轄區的網絡安全。

該集團誘使受害者安裝載有惡意軟件的手機應用程式，使犯罪分子能夠控制受害者的流動裝置、登入受害者網上銀行戶口，並通過未經授權的交易竊取戶口資金。在2023年9月至2024年4月期間，新加坡錄得相關案件共1 899宗，損失達1.97億港元，而香港則錄得41宗案件，損失達1 250萬港元。這些惡意軟件被發現由設在新加坡、馬來西亞和香港的伺服器控制。通過三地聯合情報交流、伺服器、數據流量和資金流向分析，最終確認兩名馬來西亞主腦身份。

於2024年6月中旬，馬來西亞皇家警察聯同新加坡警察部隊在馬來西亞拘捕兩名馬來西亞主腦。兩名主腦其後被引渡到新加坡作進一步調查及檢控。同時網罪科人員在香港以串謀詐騙及洗黑錢罪拘捕26名「錢騾」。此次行動凸顯出國際合作、情報共享及執法部門聯合行動，對打擊跨境網絡犯罪的重要性。

In mid-June 2024, CSTCB conducted a joint operation codenamed Operation DISTANTHILL with SPF and the Royal Malaysia Police (RMP) to successfully dismantle a Malaysia-based cross-border scam syndicate targeting victims in Singapore and Hong Kong. The operation resulted in multiple arrests and effectively disrupted the syndicate's operations, safeguarding the cybersecurity of all jurisdictions involved.

The syndicate lured victims into installing mobile applications embedded with malware, which allowed the perpetrators to remotely control the victims' mobile devices, access their e-banking accounts, and steal funds through unauthorised transactions. Between September 2023 and April 2024, Singapore recorded 1,899 cases involving losses of approximately HK$197 million, while Hong Kong reported 41 cases with losses amounting to HK$12.5 million. The malware was found to be controlled by servers located in Singapore, Malaysia, and Hong Kong. Through joint intelligence exchange, and coordinated analysis of servers, data traffic, and fund flows, the authorities successfully identified two Malaysian masterminds behind the syndicate.

In mid-June 2024, RMP and SPF arrested the two masterminds in Malaysia. They were subsequently extradited to Singapore for further investigation and prosecution. Meanwhile, CSTCB officers in Hong Kong arrested 26 money mules for conspiracy to defraud and money laundering. The successful operation underscores the importance of international collaboration, intelligence sharing, and joint law enforcement efforts in combating cross-border cybercrime.

[18] 港警聯同星馬破跨境木馬應用程式詐騙集團150人被捕受害者逾4 000人, June 14, 2024, https://std.stheadline.com/realtime/article/2004761/

建立網絡韌性
Building Cyber Resilience

第八屆「跨部門網絡安全演習」
The 8th Inter-departmental Cyber Security Drill

為提升政府部門應對網絡威脅的整體能力，網罪科與政府電腦保安事故協調中心於2024年4月合辦第八屆「跨部門網絡安全演習」，吸引超過250名來自70個政府部門的資訊科技人員參與，並設置實戰演練場景，進行事故應變及調查。演習展現了警方與政府跨部門緊密合作，共同應對日益嚴峻的網絡安全挑戰，全面加強預防、偵測及應變能力，致力築起堅實的網絡安全屏障。

To strengthen the government's overall capability in responding to cyber threats, CSTCB and the Government Computer Emergency Response Team Coordination Centre co-organised the 8th Inter-Departmental Cyber Security Drill in April 2024. The event drew participation from over 250 IT professionals across 70 government departments, featuring hands-on simulation scenarios to enhance incident response and investigation skills. The Drill underscored the close collaboration between the Police and various government departments in addressing escalating cybersecurity challenges, reinforcing the government's ability to prevent, detect, and respond to cyberattacks while safeguarding its digital infrastructure.

網絡安全研討會
Cyber Security Seminars

為提升本港企業應對網絡攻擊的防禦能力，網罪科定期舉辦「網絡安全研討會」，吸引數百名來自不同行業及企業的資訊科技同業精英參與。研討會邀得網絡安全業界專家及網罪科代表擔任講者，深入剖析最新網絡威脅趨勢（如勒索軟件攻擊模式及產業鏈動態），並分享實戰事故應變策略與防護最佳實踐方案。活動有效加深業界對網絡風險的認知，促進公私營協作，助力企業建立主動防禦的安全文化。

To enhance the defence capabilities of Hong Kong's business sector against cyberattacks, CSTCB regularly organises Cyber Security Seminars, attracting hundreds of IT professionals from various industries. Featuring expert speakers from both the cybersecurity industry and CSTCB, the seminars provide in-depth analyses of the latest cyber threat trends, including ransomware attack patterns and developments within the cybercrime ecosystem. They also share practical incident response strategies and best practices in cybersecurity. These events have significantly raised industry awareness of cyber risks, fostered public-private collaboration, and empowered enterprises to cultivate a proactive cybersecurity culture.

網絡攻防精英培訓暨攻防大賽

網罪科、數字政策辦公室及香港互聯網註冊管理有限公司於2024年8月合辦為期三日的「網絡攻防精英培訓暨攻防大賽」，為網絡安全從業員提供網絡攻擊及防禦訓練，並透過模擬網絡攻擊的比賽，提升他們的專業水平及網絡事故應變能力，以全面鞏固香港的網絡安全。活動共有超過70間機構，合共160位從業員進行攻防培訓，並吸引超過300支隊伍，合共740名業界與學界精英參與攻防比賽。

釣魚電郵演習

為了提高員工識別可疑電郵的意識，網罪科自2021年起舉辦「釣魚電郵演習」，並於2023年開始與香港互聯網註冊管理有限公司合辦該活動。

「釣魚電郵演習2024」於2024年8月至12月舉行，共吸引了來自216間機構的37 220名參與者。在演習期間，參與機構員工收到四封模擬釣魚電郵，旨在測試員工的網絡安全意識。活動結束後，參與機構會收到一份詳細報告，內容顯示其員工在處理可疑電郵方面的表現。此項活動旨在提高企業員工對釣魚攻擊的防範意識，共同構建一個更安全的香港網絡安全環境。

狩網運動

為了提升企業層面，尤其是中小企業的網絡安全意識，網罪科自2023年起與一家網絡安全初創公司Cyberbay合辦「狩網運動」，並自2024年起加入個人資料私隱專員公署成為戰略夥伴。

「狩網運動2024」於2024年6月至8月期間舉行，共有153間機構參與。在活動期間，已認證的網絡安全專才通過漏洞獎勵制度，為參與機構提供網絡安全漏洞測試、安全報告及一對一的專業諮詢服務。網罪科期望能夠讓企業系統漏洞檢測普及化，共同為香港創造一個更安全的網絡世界。

Cyber Attack and Defence Elite Training cum Tournament (CADET^2)

To enhance attack and defence capabilities of cybersecurity personnel, CSTCB, the Digital Policy Office (DPO), and the Hong Kong Internet Registration Corporation Limited (HKIRC) co-organised a three-day Cyber Attack and Defence Elite Training cum Tournament (CADET^2) in August 2024. Apart from hands-on training, the programme also enhanced participants' professional skills and incident response capabilities through simulated cyberattack competitions, contributing to the overall reinforcement of Hong Kong's cybersecurity. The event provided cyberattack and defence training to a total of 160 personnel from more than 70 organisations, and attracted over 300 teams, comprising a total of 740 cybersecurity talents from both the industry and academia, to compete in the tournament.

Ethical Phishing Email Campaign

To raise staff awareness in identifying suspicious emails and reduce cybersecurity risks for participating organisations, CSTCB has organised the Ethical Phishing Email Campaign since 2021, and has collaborated with the HKIRC since 2023.

The 2024 campaign, held from August to December 2024, attracted 37,220 participants from 216 organisations. During the campaign, employees from participating organisations received four pseudo-phishing emails designed to assess their cybersecurity awareness. At the end of the campaign, each organisation received a detailed report outlining their employees' performance in handling suspicious emails. The campaign seeks to raise awareness among corporate employees against phishing attacks and contribute to building a safer cybersecurity environment in Hong Kong.

BugHunting Campaign

To enhance cybersecurity awareness at the corporate level, especially among small and medium-sized enterprises (SMEs), CSTCB has organised the BugHunting Campaign in collaboration with the cybersecurity start-up Cyberbay since 2023, and partnered with the Office of the Privacy Commissioner for Personal Data (PCPD) since 2024.

The BugHunting Campaign 2024 was conducted from June to August 2024, with participation from 153 organisations. During the campaign, certified cybersecurity professionals provided vulnerability tests, security reports, and one-on-one professional consultations under a bug bounty model. The campaign aims to promote wider adoption of vulnerability testing among enterprises and to foster a safer cyberspace in Hong Kong.

策略性諮詢與合作
Strategic Advisory and Partnership

網絡安全特別行動小組
Cyber Security Action Task Force

香港警務處於2024年成立網絡安全特別行動小組，集合全球資深網絡安全專家及企業，與執法機構緊密合作，共同打擊網絡犯罪。網絡安全特別行動小組旨在加強網絡威脅情報的交流及行動支援，推動專業知識共享，從而有效提升未來應對網絡威脅的整體能力。

In 2024, HKPF established the Cyber Security Action Task Force (CSATF), bringing together leading global cybersecurity experts and firms to work closely with law enforcement agencies in combating cybercrime. CSATF aims to strengthen cyber threat intelligence sharing, enhance operational support, and promote professional knowledge exchange, ultimately enhancing collective capabilities to respond to evolving cyber threats effectively in the future.

科技罪案警政顧問小組
Cybercrime Policing Advisory Panel

香港警務處於2025年3月14日正式成立第二屆「科技罪案警政顧問小組」，委任13位來自網絡安全、人工智能、金融科技等領域的頂尖專家，攜手應對新世代科技罪案所帶來的多重挑戰。顧問小組將就網絡安全、創新科技風險、執法策略及數碼警務發展等議題提供專業意見，協助警隊加強科技應變能力，構建更堅實的網絡安全防線。

On 14 March 2025, HKPF officially launched the second term of the Cybercrime Policing Advisory Panel, appointing 13 distinguished experts from the fields of cybersecurity, artificial intelligence, fintech, and other emerging technologies. The Panel will provide strategic advice on matters including cybersecurity, technological risks, enforcement strategies, and the development of digital policing, empowering the Force in strengthening its technological preparedness and in building a more robust cyber defence framework for Hong Kong.

立法工作
Legislative Work

保護關鍵基礎設施（電腦系統）條例
Protection of Critical Infrastructures (Computer Systems) Bill

香港警務處一直與保安局及數字政策辦公室緊密合作，全力推動《保護關鍵基礎設施（電腦系統）條例》的立法工作。條例旨在向被指定的關鍵基礎設施營運者施加法定要求，確保它們採取適當措施保護其電腦系統，減低因網絡攻擊導致必要服務被干擾或破壞的可能，從而維持香港社會的正常運作和市民的正常生活。有關條例已於2024年12月6日由政府正式刊憲，並於2025年3月19日在立法會順利完成三讀程序並獲正式通過，標誌着香港在保障關鍵基礎設施電腦系統安全的法律建設上取得重大進展。條例預計於2026年1月1日生效。

HKPF has worked in close collaboration with the Security Bureau and DPO to spearhead the legislative process of the Protection of Critical Infrastructures (Computer Systems) Bill. The Bill seeks to impose statutory requirements on designated critical infrastructure operators, mandating appropriate measures to safeguard their computer systems and mitigate disruptions to essential services caused by cyberattacks. This aims to preserve the normal functioning of society and the daily lives of Hong Kong citizens. The Bill was officially gazetted on 6 December 2024, and was passed after its third reading in the Legislative Council on 19 March 2025, marking a significant milestone in Hong Kong's legislative framework for the protection of computer systems of critical infrastructures. The legislation is scheduled to come into effect on 1 January 2026.

加強保護關鍵基礎設施電腦系統安全 - 建議立法框架
Proposed Legislative Framework to Enhance Protection of the Computer Systems of Critical Infrastructures
諮詢報告簡介會
Briefing on the Consultation Report

條例
（中文版）

The Bill
(English version)

電腦網絡罪行法律改革
Law Reform on Cybercrime

鑑於資訊科技、電腦和互聯網發展迅速，加上其有被利用來從事犯罪活動的潛在可能，香港法律改革委員會於2019年成立小組委員會，就電腦網絡罪行這個課題展開研究，而網罪科總警司亦為小組委員會成員之一。小組委員會於2022年7月發表《依賴電腦網絡的罪行及司法管轄權事宜》諮詢文件，經公眾諮詢及小組委員會討論後，建議立法訂明五類依賴電腦網絡的罪行，包括非法取覽程式或數據、非法截取電腦數據、非法干擾電腦數據、非法干擾電腦系統，以及提供或管有用作干犯電腦網絡相關罪行的器材、程式或數據。小組委員會亦正就「借助電腦網絡的罪行」，如網上欺凌、深偽技術詐騙等議題，展開討論。

With the rapid development of information technology, computers, and the Internet, as well as their potential exploitation for criminal activities, the Law Reform Commission of Hong Kong established a sub-committee in 2019 to study the topic of cybercrime. CSP of CSTCB is also one of the sub-committee members. In July 2022, the sub-committee published a Consultation Paper on Cyber-Dependent Crimes and Jurisdictional Issues. Following public consultation and internal discussions, the sub-committee recommended the enactment of new legislation to address five categories of cyber-dependent crimes, including illegal access to programmes or data, illegal interception of computer data, illegal interference with computer data, illegal interference with computer systems, and making available or possessing devices, programmes or data for the purpose of committing a cybercrime. The sub-committee is also exploring the issue of cyber-enabled crimes, including topics such as cyberbullying and deepfake-related scams.

宣傳及公眾教育
Publicity and Public Education

「防騙視伏器」系列
Scameter Series

留意可疑帳號警示
轉數時要醒啲
警示已全面覆蓋轉數快、自動櫃員機及其他網上銀行轉賬
提示！冇警示，都唔等於一定安全㗎！
G.E.M. 鄧紫棋
CyberDefender.hk
立即了解

「防騙視伏器」搜尋引擎於2022年10月推出，讓公眾能夠查證可疑的網址、電郵地址、電話號碼及銀行帳戶。為進一步提升其效用，網罪科推出「防騙視伏APP (Scameter+)」手機應用程式，提供詐騙搜索、防詐騙資訊及即時通知功能，並於2024年2月再新增自動檢測詐騙電話及網站、公眾情報分享平台及人工智能分析工具等功能。這些發展不僅提升了公眾的使用便利性，更聚焦於安全性與私隱，應對不斷演變的威脅。

Launched in October 2022, the Scameter search engine enables the public to verify suspicious websites, email addresses, phone numbers and bank accounts. To further enhance its utility, CSTCB introduced the "Scameter+" mobile application, providing scam search capabilities, anti-scam information and real-time notifications. In February 2024, new features including automatic scam call and fraudulent website detection, a public intelligence-sharing platform and an AI-powered analyser, were added. These enhancements not only improved user convenience, but also prioritised security and privacy in the face of evolving cyber threats.

截至2024年底，「防騙視伏器」已完成近680萬次風險評估，其手機應用程式的下載量超過86萬次，顯著提升了公眾防範詐騙的能力。自2024年12月起，「可疑帳號警示」機制的涵蓋範圍擴展至銀行自動櫃員機交易，將覆蓋絕大部分市民的日常轉帳。不論客戶於銀行分行、自動櫃員機或網上銀行進行轉帳或存款，一旦收款人的戶口號碼、手機號碼、電子郵件地址或轉數快識別碼與「防騙視伏器」內被標記為「高危有伏」的資料脗合，客戶將於確認交易前收到警示，提醒他們相關的詐騙風險。

By the end of 2024, Scameter had completed nearly 6.8 million risk assessments, and the mobile application had surpassed 860,000 downloads, significantly boosting public awareness and prevention of scams. Since December 2024, the Suspicious Account Alert mechanism has been extended to cover ATM transactions, encompassing most of the public's routine fund transfers. Whenever customers transfer or deposit funds via a bank branch, ATM, or online banking, if the recipient's account number, mobile phone number, email address or Faster Payment System (FPS) Identifier matches information flagged as "High Risk" in Scameter, an alert will be triggered prior to transaction confirmation, warning users of potential fraud.

於2024年12月，「防騙視伏器」系列於第四屆亞洲創新發明展覽會中，獲得智慧金融科技與軟件類別銀獎。其後，「防騙視伏器」系列更於2025年4月在瑞士舉辦的「第50屆日內瓦國際發明展」中，榮獲「國際傳媒大獎」及金獎。

In December 2024, the "Scameter series" was awarded the Silver Medal in the Smart Finance Technology and Software category at the 4th Asia Exhibition of Innovations and Inventions (AEII). Subsequently, in the 50th International Exhibition of Inventions of Geneva held in April 2025 in Switzerland, the "Scameter series" garnered the "International Press Prize" and Gold Medal.

守網聯盟

為應對不斷演變的網絡威脅，網罪科聯同其他政府部門、法定機構及私營企業於2024年推出「守網聯盟」。此項計劃旨在透過不同網站、社交媒體平台及實體宣傳活動，打擊網上詐騙並提升網絡安全。透過其協作平台，「守網聯盟」致力於擴大宣傳活動的覆蓋範圍，提升打擊網絡犯罪及網上詐騙的成效。

CyberDefenders' Alliance

In response to ever-evolving online threats, CSTCB, in collaboration with other government departments, statutory bodies, and private corporations, launched the "CyberDefenders' Alliance" in 2024. This initiative aims to combat online scams and strengthen cybersecurity through a range of publicity campaigns conducted via websites, social media platforms, and physical events. By leveraging its collaborative platforms, the Alliance seeks to expand the reach of publicity campaign and enhance the effectiveness of initiatives aimed at tackling cybercrimes and online scams.

守網聯盟
CYBERDEFENDERS ALLIANCE
共築防線 捍衛網安
面對日新月異的網絡陷阱，網絡安全及科技罪案調查科聯同各政府部門、公營機構及各界企業組成「守網聯盟」，以集結社會各界的力量，共同守護網絡安全。
Cyber Defender 守網者
立即下載防騙視伏APP

全城反詐嘉年華

網罪科、商業罪案調查科和財富情報及調查科於2024年12月，在西九文化區首次合辦為期兩日的全城反詐嘉年華，透過主題遊戲攤位、反詐騙體驗館及各種表演，讓市民認識如何防範騙案、洗黑錢及網絡陷阱。是次活動共吸引接近20 000名市民入場。

Anti-Scam Carnival

In December 2024, CSTCB, the Commercial Crime Bureau and the Financial Intelligence and Investigation Bureau co-organised the first-ever "Anti-Scam Carnival" at the West Kowloon Cultural District. The two-day event aimed to raise public awareness of scam prevention, anti-money laundering, and cyber pitfalls through thematic game booths, an interactive "Anti-Scam Hub" and various performances. The event attracted nearly 20,000 citizens.

大灣區青少年人工智能及網絡安全挑戰賽2024
Greater Bay Area Youth Artificial Intelligence and Cyber Security Challenge 2024

由網罪科、澳門司法警察局聯同澳門教育及青年發展局合辦，澳門科學館和香港教育局等機構協辦的「大灣區青少年人工智能及網絡安全挑戰賽2024」是一項旨在提升青少年網絡安全意識及人工智能知識的合作計劃。

Co-organised by CSTCB, MJP, and the Education and Youth Development Bureau of Macao, with support from the Macao Science Centre, the Hong Kong Education Bureau and other institutions, the "Greater Bay Area Youth Artificial Intelligence and Cyber Security Challenge 2024" is a collaborative initiative aimed at raising cybersecurity awareness and promoting AI literacy among youth.

本屆賽事自2024年9月開展，吸引粵港澳三地共126所學校、1 182名學生參與。經過初賽甄選，最終117名學生成功晉級決賽，獲選到澳門參與三日兩夜的人工智能訓練營。訓練期間，參賽者參加工作坊，並走訪澳門科學館，透過互動展覽了解人工智能的應用。參賽者於決賽中運用所學的人工智能及網絡安全技術，在限時內設計出創新的防詐騙模型，展現卓越的科技實踐能力與團隊協作精神。

Launched in September 2024, the competition attracted participation from 126 schools and 1,182 students across Guangdong, Hong Kong and Macao. Following preliminary rounds, 117 students advanced to the finals and were invited to Macao to take part in a three-day, two-night AI training camp. During the camp, participants attended workshops and visited the Macao Science Centre, where interactive exhibitions deepened their understanding of cutting-edge AI applications. In the final round, participants applied their knowledge of artificial intelligence and cybersecurity to design innovative anti-fraud models within a set time limit, showcasing exceptional technical skills and teamwork.

常用詞彙
Glossary

簡稱Abbreviations	English	中文
AI	Artificial Intelligence	人工智能
APT	Advanced Persistent Threat	進階持續性攻擊
C2	Command & Control	命令與控制
CADET[2]	Cyber Attack and Defence Elite Training cum Tournament	網絡攻防精英培訓暨攻防大賽
CSATF	Cyber Security Action Task Force	網絡安全特別行動小組
CSTCB	Cyber Security and Technology Crime Bureau	網絡安全及科技罪案調查科
CVE	Common Vulnerabilities and Exposures	通用漏洞披露
CVSS	Common Vulnerability Scoring System	通用漏洞評分系統
DDoS	Distributed Denial-of-Service	分散式阻斷服務
DoS	Denial-of-Service	阻斷服務
DPO	Digital Policy Office	數字政策辦公室
EDR	Endpoint Detection and Response	端點偵測和回應
HKCERT	Hong Kong Computer Emergency Response Team	香港網絡安全事故協調中心
HKIRC	Hong Kong Internet Registration Corporation Limited	香港互聯網註冊管理有限公司
HKPF	Hong Kong Police Force	香港警務處
HKSARG	Government of the Hong Kong Special Administrative Region	香港特別行政區政府
IoT	Internet-of-things	物聯網
IP	Internet Protocol	互聯網規約
IT	Information Technology	資訊科技
LLM	Large-Language-Model	大型語言模型
LOTL	Living-off-the-land	離地攻擊
MFA	Multi-factor authentication	多重認證
MJP	Macao Judiciary Police	澳門司法警察局
NIDS	Network Intrusion Detection System	網絡入侵偵測系統
OT	Operation Technology	運營科技
PCPD	Privacy Commissioner of Personal Data	個人資料私隱專員
RDP	Remote Desktop Protocol	遠端桌面協定
RMP	Royal Malaysia Police	馬來西亞皇家警察
SIEM	Security Information and Event Management	保安資訊和事件管理
SME	Small and medium-sized enterprise	中小型企業
SOCA	Security Operation Centre Alliance	網絡安全行動中心聯盟
SPF	Singapore Police Force	新加坡警察部隊
SQL	Structured query language	結構化查詢語言
SSH daemons	Secure Shell Protocol daemons	安全外殼協議守護程序
SSL VPN	Secure Sockets Layer Virtual Private Network	保密插口層虛擬私人網絡
UAT	User Acceptance Test	用戶驗收測試
VPN	Virtual Private Network	虛擬私有網絡

方法
Methodology

網罪科通過案件調查、與合作夥伴分享情報和其他可靠來源，收集和分析網絡威脅情報，讓網罪科更全面了解全球及香港的網絡安全形勢。

本報告所呈列的數據來自多個可信來源及業界意見，但並非旨在全面涵蓋或代表全球所有網絡安全趨勢。報告中的結論和觀察旨在提供對新興網絡威脅模式和風險的概括性參考，並非作為權威性或全面性的分析依據。

CSTCB collects and analyses cyber threat intelligence from multiple sources, including case investigations, intelligence sharing with working partners, and other reliable sources. These diverse inputs enable CSTCB to gain a more comprehensive understanding of the cybersecurity landscape, both globally and in Hong Kong.

The data presented in this report are drawn from a range of credible sources and industry insights. However, they are not intended to be exhaustive or fully representative of all global cybersecurity trends. The conclusions and observations herein aim to provide a general reference for understanding emerging patterns and risks, rather than serving as a definitive or comprehensive analysis.

網絡安全及科技罪案調查科
Cyber Security and Technology Crime Bureau

香港灣仔軍器廠街一號警察總部警政大樓
Arsenal House, Police Headquarters, No. 1 Arsenal Street, Wan Chai, Hong Kong

防騙視伏APP Scameter+