Hong Kong Computer Emergency Response Team Coordination Centre
HKCERT 香港電腦保安事故協調中心

Hong Kong Information Security Outlook
香港資訊保安展望 2022

HKCERT

Agenda 程序

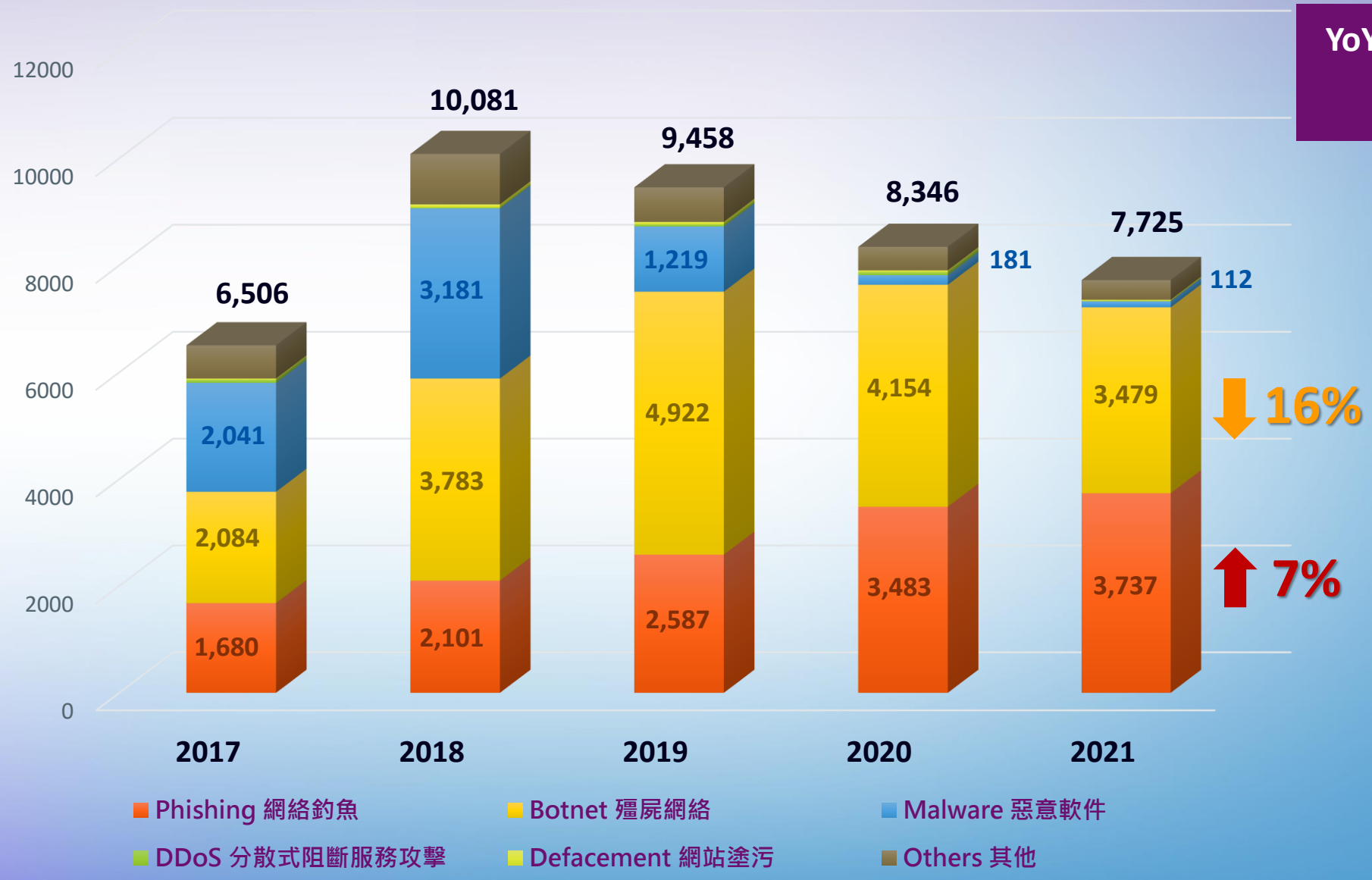
1. Review 回顧 2021
2. Outlook 展望 2022
3. Advice 建議

HKCERT

1

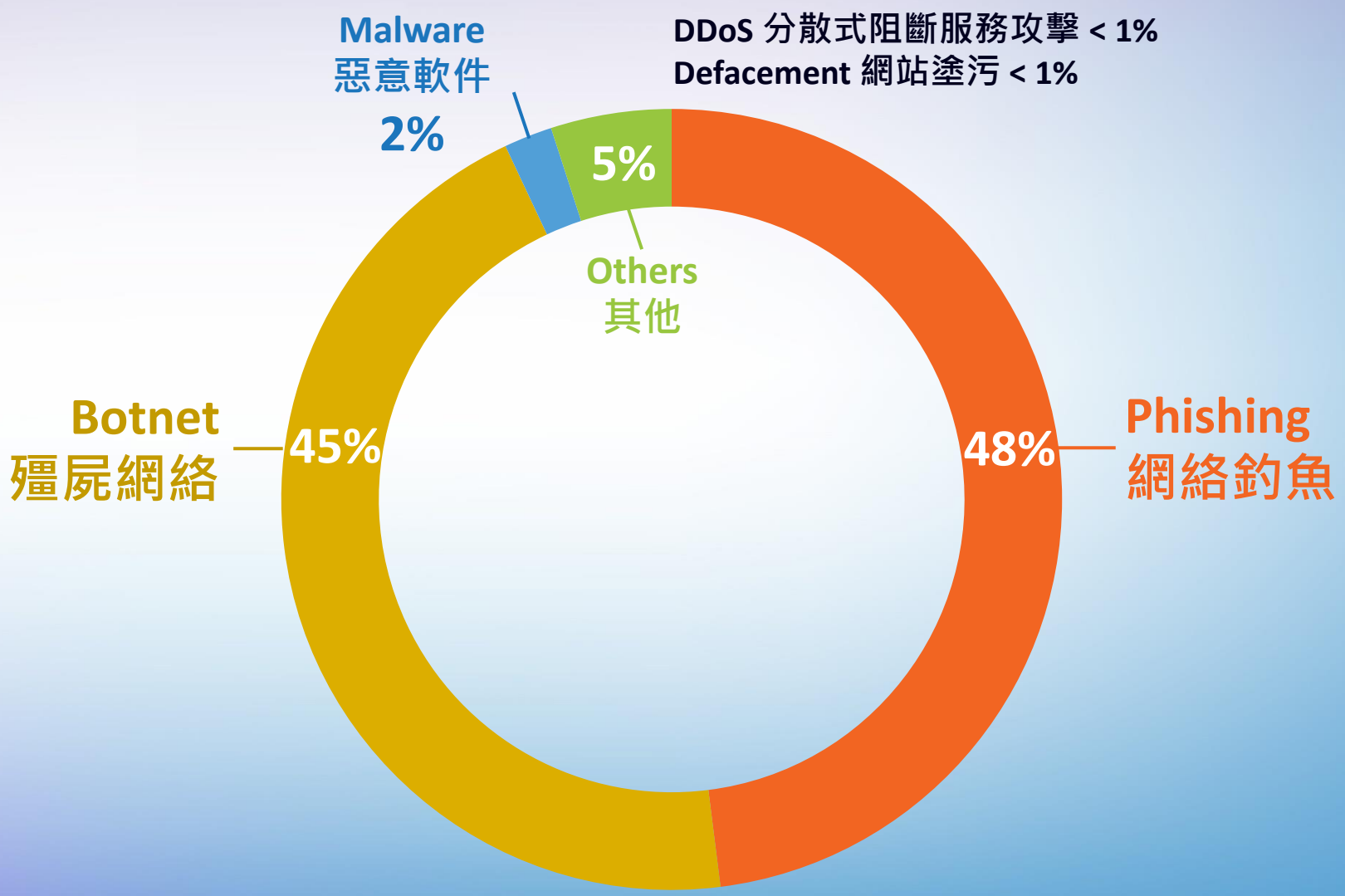
Review 2021
回顧

Trend of Security Incidents
保安事故走勢



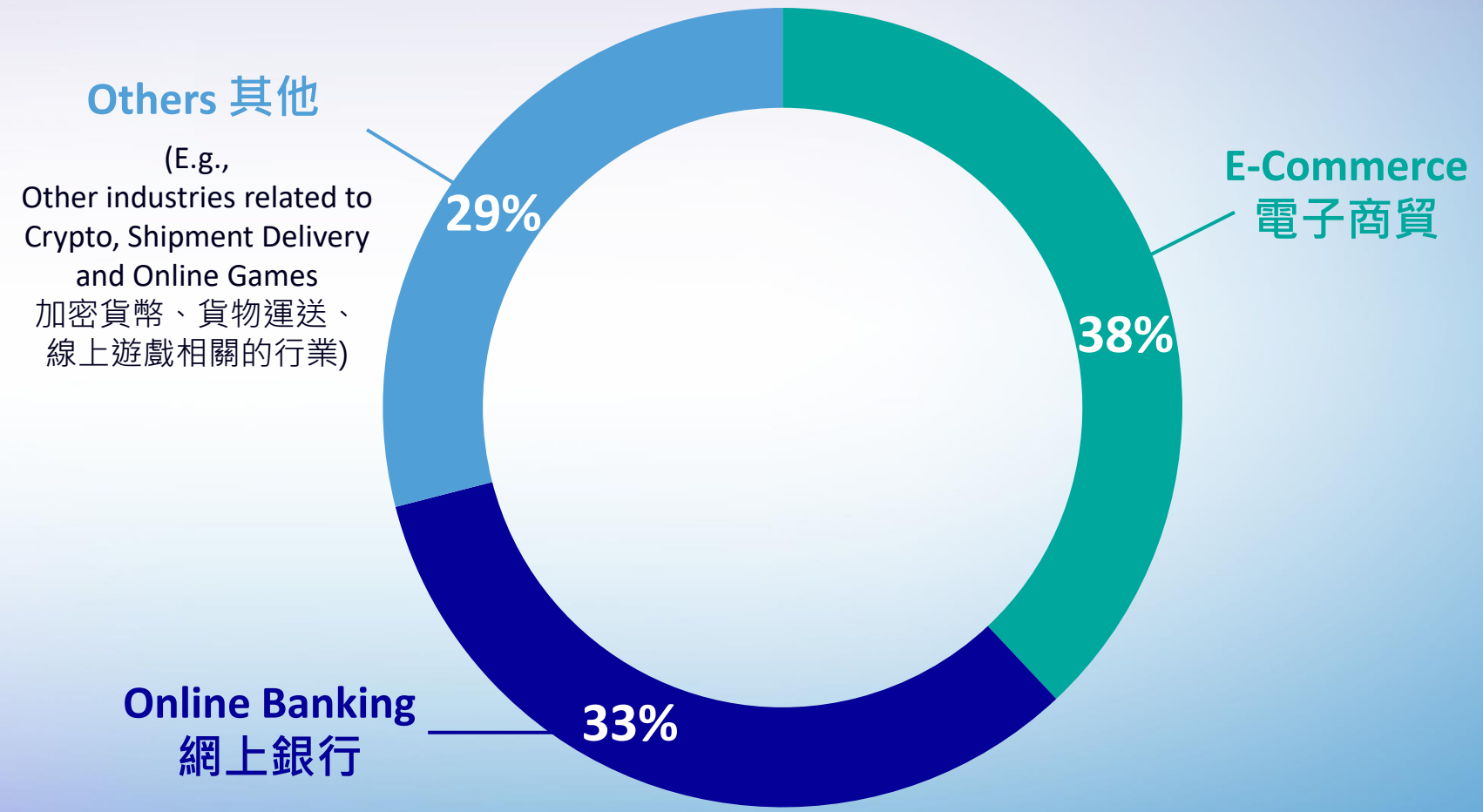
Source 來源：HKCERT

Categories of Security Incident 2021
2021保安事故類別



Source 來源：HKCERT

Types of Phishing Attacks in 2021
2021釣魚攻擊種類



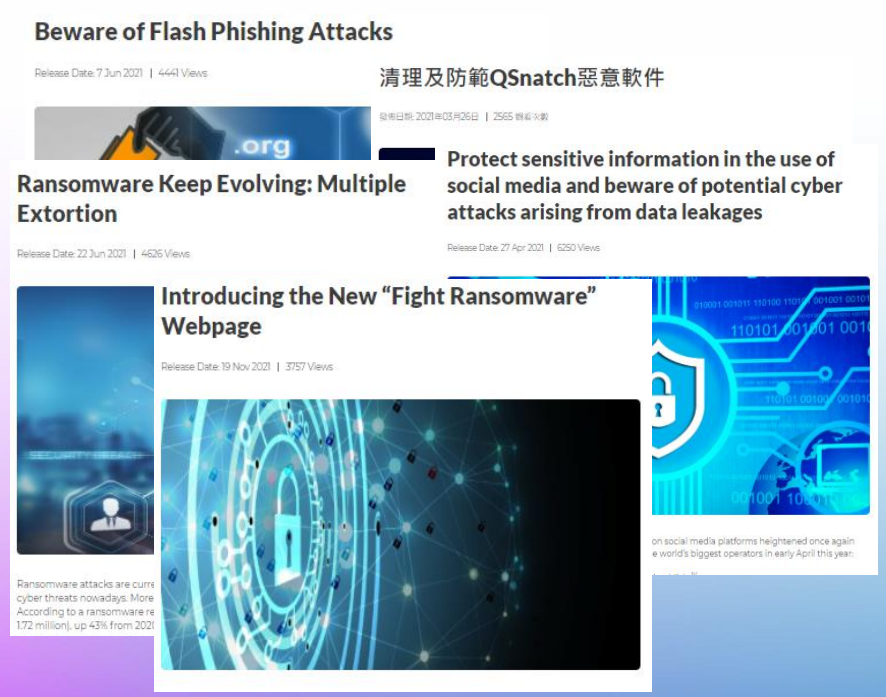
Source 來源：HKCERT

HKCERT's Responses to Information Security Challenges
HKCERT 針對資訊保安挑戰的回應

Preventive Security Advice
預防性保安建議

Cyber Attack Alerts and Reactions
網絡攻擊警報及應變

Emerging Information Security Risks Reminders
新興資訊保安風險提示



HKCERT

2

Outlook 2022 展望

5 Key Information Security Risks in 2022
2022年五大資訊保安風險

1. **Security Risks of Cryptocurrency**
   加密貨幣的保安風險 — NEW!
2. **Security Risks of Metaverse**
   元宇宙的保安風險 — NEW!
3. **Security Risks Brought by Emerging Technologies**
   新興科技帶來的保安風險
4. **Supply Chain Attacks**
   供應鏈攻擊
5. **Targeted and Organised Cyber Attacks**
   有針對性及有組織的網絡攻擊

（In no particular order 排名不分先後）

Security Risks of Cryptocurrency
加密貨幣的保安風險

Cryptocurrency 加密貨幣

Security Risks of Cryptocurrency Wallet 加密貨幣錢包的保安風險

“Hot wallet” 「熱錢包」

- Requires an internet connection 需連接網路
- Vulnerable to **cyber attacks** or **data breach** 易受**網絡攻擊**或**數據洩露**

“Cold wallet” 「冷錢包」

- Does NOT require an internet connection 不需連接網路
- At risk of **physical loss or damage**, **storage device malfunction** 有**物理丟失或損壞**、**存儲設備故障**等風險

Security Risks of Metaverse
元宇宙的保安風險

Metaverse 元宇宙
Security Risks of Non-Fungible Token (NFT) 非同質化代幣的保安風險 • Hackers will compromise user's **NFT accounts** or **sensitive information** 黑客會盜取使用者的**NFT賬戶**或**敏感資料** • Hackers will imitate the promotions of NFT platforms and distribute **fake NFT assets** for **free** 黑客會模仿NFT平台的推廣手法，以**免費名義**發放**假NFT資產**
Fake Identity and Data Security Problems 虛假身份及數據保安問題 • Online **data breach** risks 線上**數據泄露**風險 • **Identity theft** in Metaverse: "Avatar" being hacked 元宇宙中的**身份盜竊**：「虛擬化身」被盜用

Security Risks Brought by Emerging Technologies
新興科技帶來的保安風險

Emerging Technologies 新興科技	Related Security Risks 相關保安風險	Related Development 相關發展
5G Technology (5G) **第五代行動通訊技術**	• **Protocol Security Loopholes 協議保安漏洞**	• **Industry Standard Practice on 5G** **5G行業標準實踐指引**
Internet of Things (IoT) **物聯網**	• **Weak Password 密碼強度低** • **98% Unencrypted IoT Traffic 物聯網通訊未加密**	• **Regulations and Industry Standard Practice on IoT** **物聯網法規及行業標準實踐指引**

Artificial Intelligence (AI) Frauds
人工智能欺詐
	• **DeepFake Identity Theft 深度偽造的身份盜竊**
	  • DeepFake celebrity and politician footages
	  深度偽造的名人和政客錄像
	• **AI Voice Cloning 人工智能語音仿效**
		• **Tools for Fake Face Detection**
		檢測偽造面孔的工具
		• **Regulations and Industry Standard Practice on AI**
		人工智能法規及行業標準實踐指引

Operational Technology (OT) **運營技術**	• **Attacks on Industrial Control Systems (ICS)** **針對工業控制系統 (ICS) 的攻擊**	• **Future Emergence of OT Security Standard** **OT安全標準於未來陸續出現**
Widely Use of QR Code **二維碼的廣泛使用**	• **Phishing Website Spread by Using QR Code** **經二維碼散播的釣魚網站**	• **Security Guideline on Using QR Code** **使用二維碼的保安指引**

Supply Chain Attacks
供應鏈攻擊

- Bypass **enterprises' defence system**
  繞過**企業的保安系統**
- Leverage on **enterprises' trust on their partners** to evade security defence
  利用**企業對合作夥伴的信任**來避開保安防禦
- Use legitimate mechanism to distribute **trojanised software components "downstream"**
  使用合法軟件將**木馬化的軟件組件**發布至「**下游**」

Apache "Log4j" Vulnerability 漏洞 (Dec 2021)

HKCERT's **Responses and Actions** to Apache "Log4j" Vulnerability:
HKCERT針對 Apache "Log4j" 漏洞的**回應及行動**：

- Released **timely security bulletin** → Remind the public to take prompt prevention action
  發布**即時保安公告** → 提醒大眾作出及時防禦
  https://www.hkcert.org/security-bulletin/apache-log4j-denial-of-service-vulnerability_20211220

- Released **press release** and updated **blog post** → Increase public awareness
  發布**新聞稿**及更新**網誌** → 提升大眾意識
  https://www.hkcert.org/blog/hkcert-urges-local-it-users-to-patch-apache-log4j-vulnerability-asap
  https://www.hkcert.org/press-centre/hkcert-urges-local-it-users-to-patch-apache-log4j-vulnerability-asap

Targeted and Organised Cyber Attacks
更具針對性及有組織的網絡攻擊

Cyber Attacks 網絡攻擊
Multiple Extortion Ransomware 多重勒索軟件 Example 例子： • 1st: Distributed Denial of Service (DDoS) 分散式阻斷服務攻擊 • 2nd: Contact victims' customers and partners 聯繫受害者的客戶和合作夥伴 • 3rd: Short sell victims' stock 賣空受害者的股票
Phishing Attacks Targeting Specific Sectors 瞄準個別行業的釣魚攻擊 • Top 2 affected sectors by phishing attacks: **E-Commerce** and **Online Banking** 兩大受釣魚攻擊行業：**電子商貿**、**網上銀行**

HKCERT's Future Initiatives
HKCERT 未來方向

1 **Formulate and Promote Information Security Related Incident Prevention and Response Guidelines**

制定及推廣資訊保安相關的事故防禦及處理指南

2 **Formulate and Promote Emerging Technologies (e.g., Cloud Technologies) Related Best Practice and Guidelines**

制定及推廣新興技術（例如雲技術）相關的最佳實踐和指南

3 **Organise More SME-targeted Seminars to Raise Information Security Awareness and Capability Against Attacks**

舉辦更多針對中小企的研討會以提高資訊保安意識及應對能力

HKCERT

3

Advice
建議

Information Security Advice (Corporate Level)
資訊保安建議（企業層面）

1

Formulate Strategies & Develop Relevant Security Measures to Tackle New Security Risks
制定策略及保安措施以應對新的保安風險

- **Cryptocurrency**, **Metaverse** and **Emerging Technologies**
  加密貨幣、**元宇宙**和**新興科技**

2

Monitor Third-Party Security Risks to Tackle Supply Chain Attacks and Improve Security Defence Mechanism
監察第三方保安風險以應對供應鏈攻擊及改善保安防禦機制

- Vendors and software applications (e.g., Log4j)
  供應商及應用軟體 (e.g., Log4j)

3

Conduct Regular Security Health Check on Network and System
定期進行網絡及系統保安檢查

- Monitor IT assets connected to internet continuously
- 無間斷監察聯繫互聯網的資訊科技配置

Information Security Advice (Individual Level)
資訊保安建議（個人層面）

1

Enable Multi-factor Authentication and Asset Transfer Whitelist to Protect Personal Crypto Assets (e.g., NFT)
啟用多重身份驗證及資產轉移白名單以保護個人加密資產（例如NFT）

2

Turn Off QR Code Scanner's Automatic URL Redirection Function to Prevent QR Code Attacks
關閉二維碼掃瞄器自動瀏覽網頁功能以防範二維碼攻擊

- Do not scan QR Codes from **unknown sources**
  請勿掃描**來源不明**的二維碼

3

Pay Attention to the Spelling of Domain Names of Websites to Avoid Phishing Websites
注意網站域名的英文串法以防範釣魚網站

- Check the **authenticity** of websites
  核實網站**真偽**

Service and Support by HKCERT
HKCERT服務及支援

Monitoring
監察

Collect and Analyse Attack Patterns
收集及分析攻擊模式

Provide Early Information Security Alerts
盡早發出資訊保安警報

Education and Technical Advice
教育及技術性建議

24-hours Free Incident Report Hotline
提供24小時免費事故報告/求助熱線

Organise Free Seminars and Briefings
舉辦免費研討會及匯報會

Collaborate with Local Industry, Government Agencies, and Global CERTs
與業界、政府機構及國際協調中心合作

Research and Insights
研究及洞察力

Offer Best Practice and Guideline
提供最佳實踐及指南

Provide Online Cyber Security Self-Assessment Tool
提供線上網絡保安評估工具

Online Cyber Security Self-assessment Tool & Incident Response Guideline
線上自我評估工具 & 事故處理指南

https://www.hkcert.org/blog/introducing-check-your-cyber-security-readiness-online-self-assessment-tools

Service and Support by HKCERT
HKCERT服務及支援

https://www.hkcert.org/f/page/500014/910613/Seven%20Habits%20of%20Cyber%20Security_Chi.pdf

Subscription to HKCERT Information Security Alert Service
訂閱HKCERT資訊保安警報服務

To stay vigilant against **information security risks**, please subscribe or follow:
要對**資訊保安風險**保持警惕，請訂閱或追蹤：

1. **Free Security Bulletin and Monthly Newsletter**
   免費保安公告及月報

2. **Free SMS Alert**
   免費電話短訊警報

3. **HKCERT's Social Media Platforms (e.g., Facebook, LinkedIn and YouTube)**
   HKCERT的社交媒體平台（例如Facebook, LinkedIn及YouTube）

Take Action Now!
立即行動！

https://www.hkcert.org/tc/form/subscribe/entry

HKCERT

Hong Kong Productivity Council
香港生產力促進局

HKPC Building, 78 Tat Chee Avenue, Kowloon, Hong Kong
香港九龍達之路78號生產力大樓
+852 2788 5678 www.hkpc.org

HKCERT

Incident Response Guideline for SMEs

中小企保安事故應變指南

HKCERT

Contents 內容

1 Importance of Planning Incident Response

保安事故應變計劃的重要性

應對網絡攻擊的困難及痛點

- 發動網絡攻擊的成本和困難度大減
- 趨向自動化
- 愈趨有組織及針對性
- 針對保護較弱的裝置攻擊
- 在有限的資源下難以有效地防禦網絡攻擊

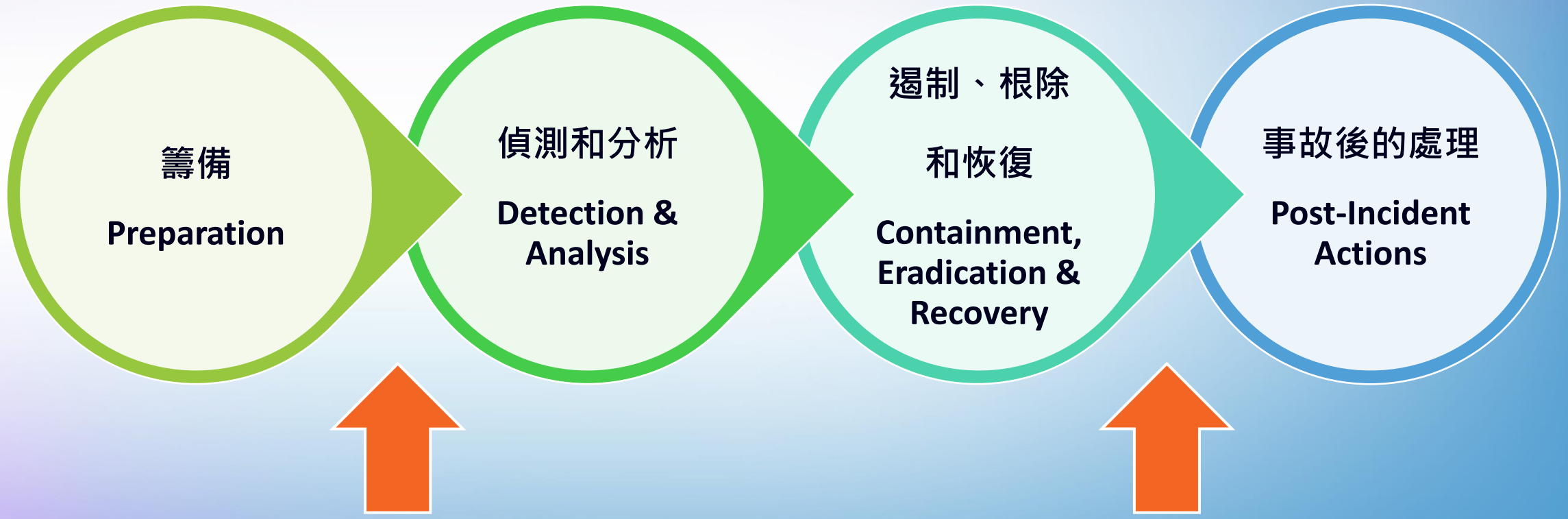
保安事故應變計劃的重要性和目標

- 及時將商業損失和隨之而來的責任減至最低
- 以有限的資源應對保安事故
- 清楚事故應變中不同崗位的職責
- 防止類似的襲擊和破壞再次發生

2 Key Elements of Incident Response Plan and its Handling Cycle

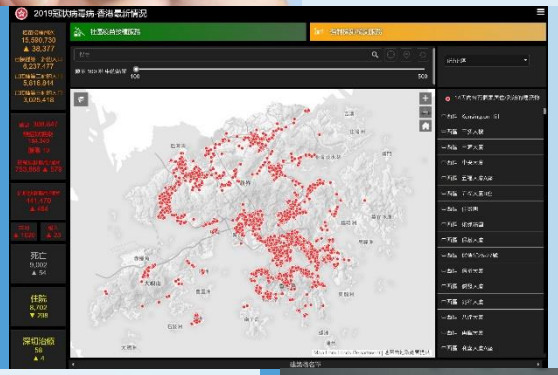
保安事故應變計劃的重要元素及處理周期

保安事故應變計劃的處理周期



偵測和分析 Detection & Analysis

- 來源的先導和指標
  Sources of Precursors and Indicators



- 事故分析
  Incident Analysis

- 事故通知
  Incident Notification

遏制、根除和恢復 Containment, Eradication & Recovery

- 選擇遏制策略
  Choosing a Containment Strategy

- 證據收集和處理
  Evidence Gathering and Handling

- 根除和恢復
  Eradication & Recovery

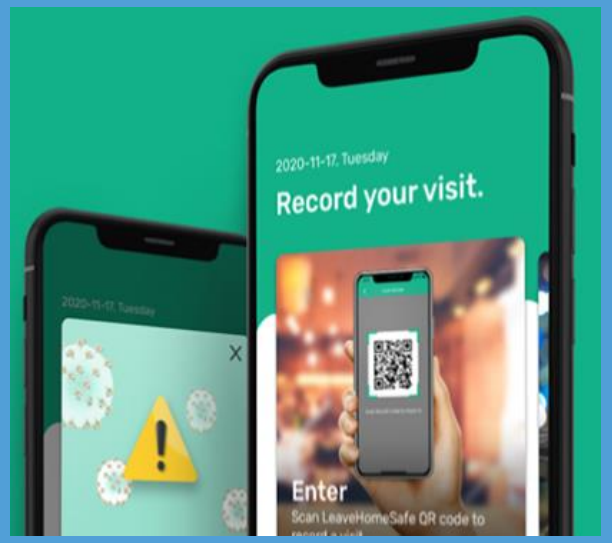
事後行動 Post-Incident Actions

- 證據保留
  Evidence Retention

- 使用收集的事件數據
  Using Collected Incident Data

- 保安改善建議
  Recommendations

籌備 Preparation

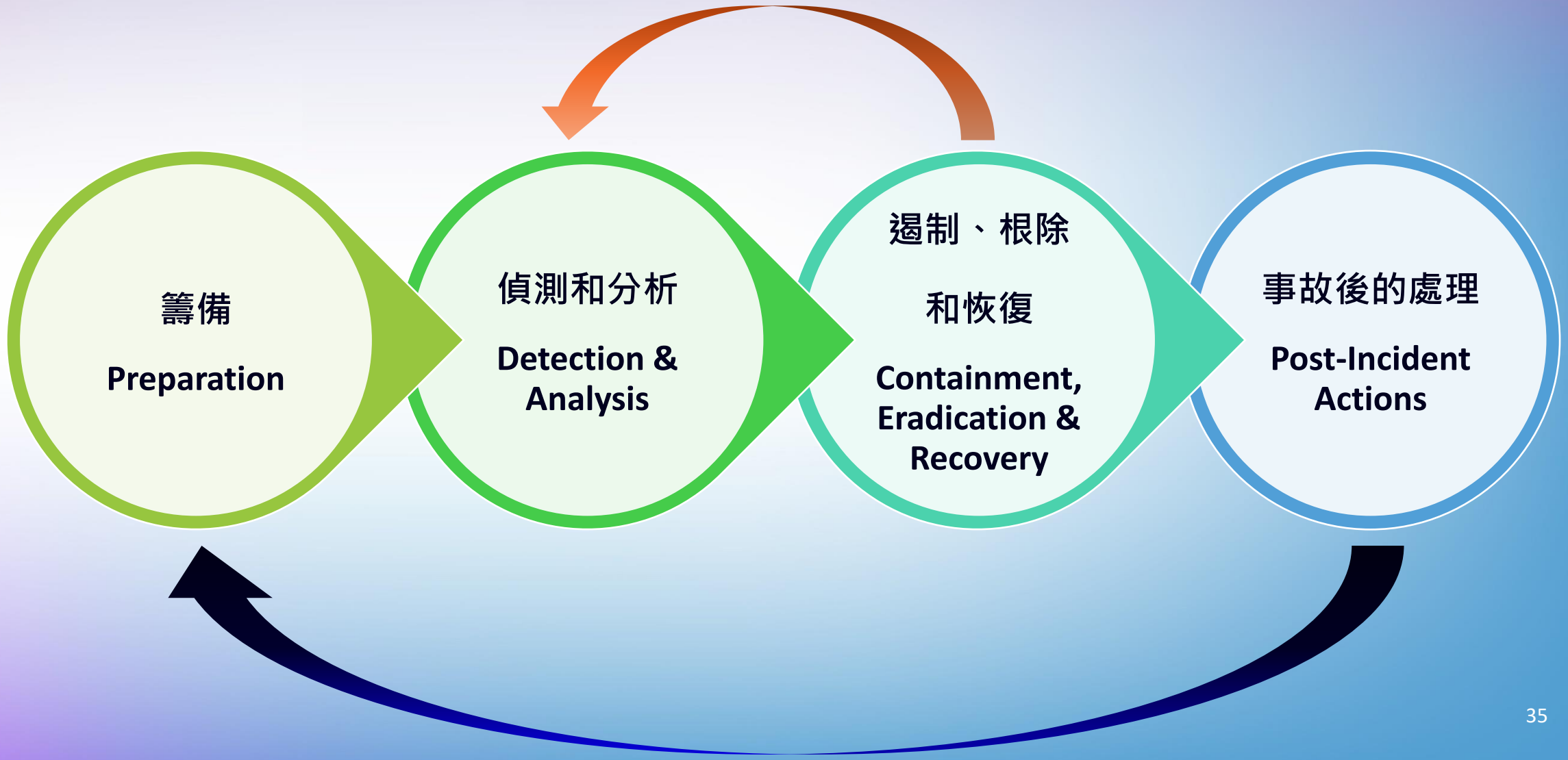


- 識別重要的系統和器材
  Identify Critical Systems and Assets

- 優先考慮和管理風險
  Prioritise and Manage the Risk

- 制定事故應變計劃
  Make an Incident Response Plan

保安事故應變計劃的處理周期



3 Real Case Scenarios in the use of Incident Response Plan

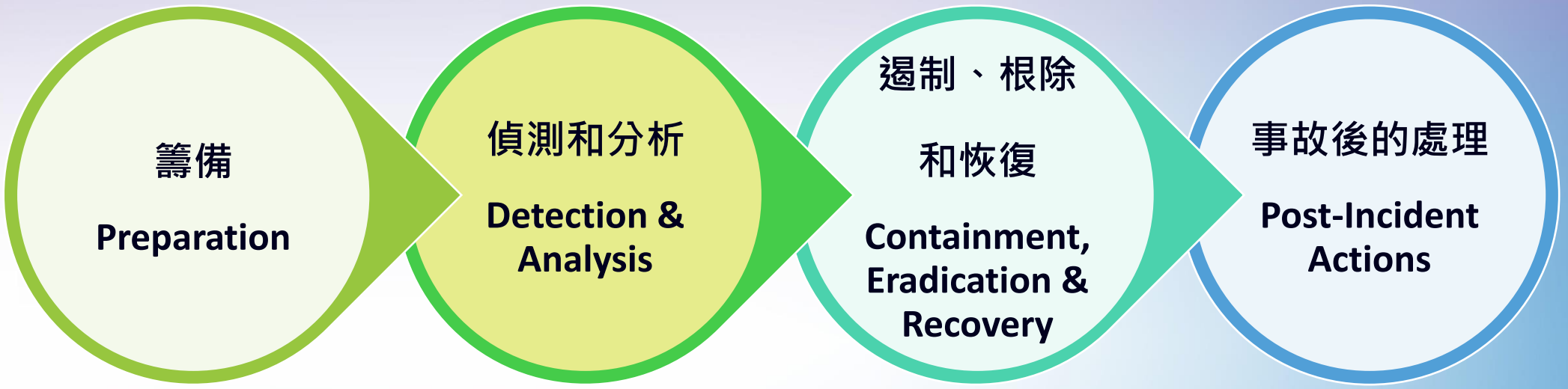
應用在真實個案的保安事故應變計劃

個案研究: HKTVmall 客戶資料未經授權被取覽

- 香港科技探索有限公司於2022年1月26日發現電腦系統出現不正常及可疑活動，未經授權取覽HKTVmall的客戶資料

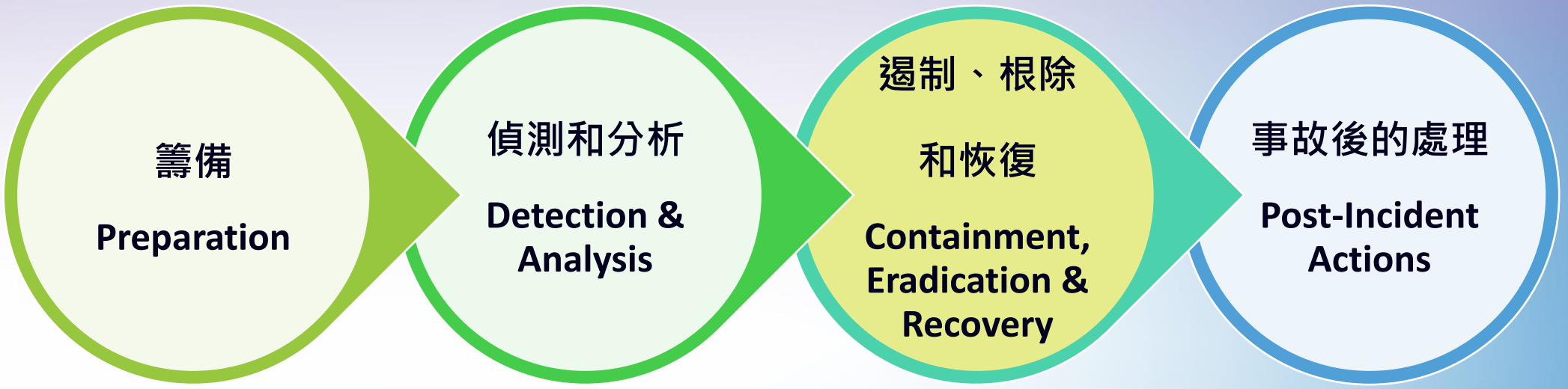
Source 來源：HKTVmall、明報
https://finance.mingpao.com/fin/instantf/20220204/1643967107543/hktvmall-438%E8%90%AC%E7%94%A8%E6%88%B6%E8%B3%87%E6%96%99%E6%9C%89%E5%B0%8F%E9%83%A8%E5%88%86%E8%A2%AB%E6%9C%AA%E7%B6%93%E6%8E%88%E6%AC%8A%E5%8F%96%E8%A6%BD

個案研究: HKTVmall 客戶資料未經授權被取覽



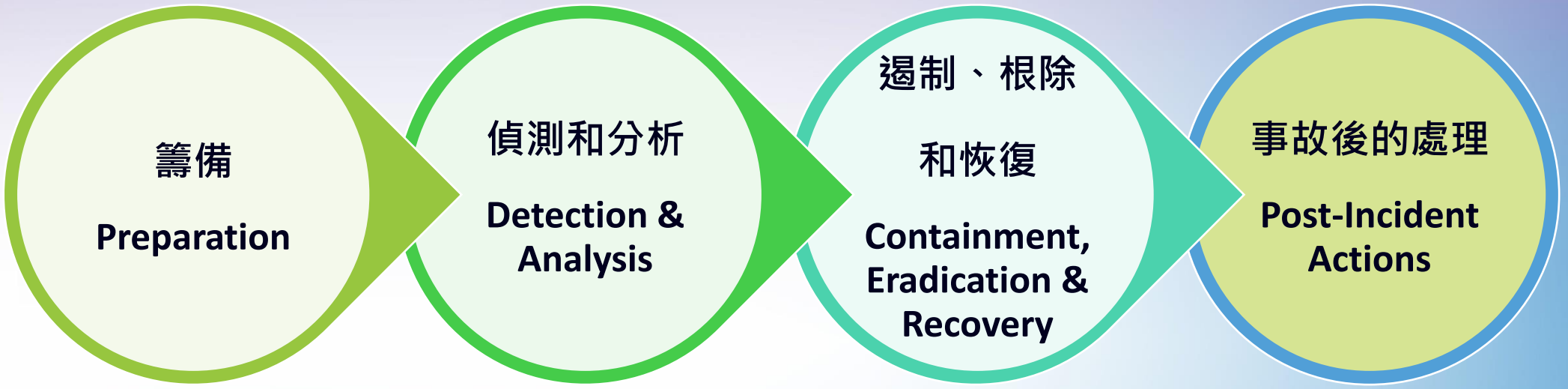
- 未經授權取覽客戶資料的來源/位置
- 被取覽客戶資料的範圍
- 被取覽客戶資料的內容和資料類別

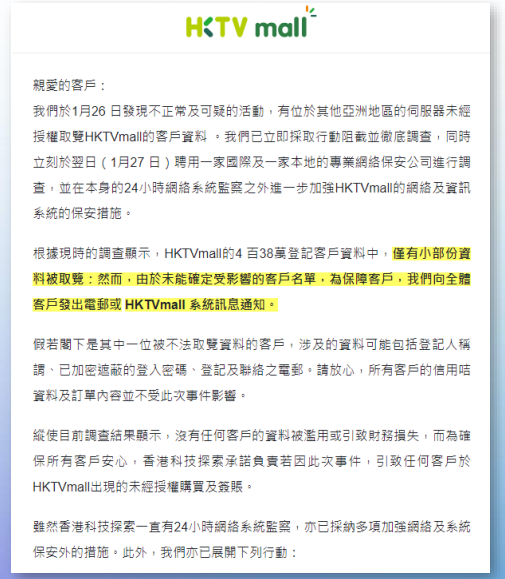
個案研究: HKTVmall 客戶資料未經授權被取覽



- 即時採取阻截事故的行動

個案研究: HKTVmall 客戶資料未經授權被取覽





HKTV mall

親愛的客戶：

我們於1月26 日發現不正常及可疑的活動，有位於其他亞洲地區的伺服器未經授權取覽HKTVmall的客戶資料，我們已立即採取行動阻截並徹底調查，同時立刻於翌日（1月27 日）聘用一家國際及一家本地的專業網絡保安公司進行調查，並在本身的24小時網絡系統監察之外進一步加強HKTVmall的網絡及資訊系統的保安措施。

根據現時的調查顯示，HKTVmall的4 百38萬登記客戶資料中，**僅有小部份資料被取覽；然而，由於未能確定受影響的客戶名單，為保障客戶，我們向全體客戶發出電郵或 HKTVmall 系統訊息通知。**

假若閣下是其中一位被不法取覽資料的客戶，涉及的資料可能包括登記人稱謂、已加密遮蔽的登入密碼、登記及聯絡之電郵。請放心，所有客戶的信用咭資料及訂單內容並不受此次事件影響。

縱使目前調查結果顯示，沒有任何客戶的資料被濫用或引致財務損失，而為確保所有客戶安心，香港科技探索承諾負責若因此次事件，引致任何客戶於HKTVmall出現的未經授權購買及簽賬。

雖然香港科技探索一直有24小時網絡系統監察，亦已採納多項加強網絡及系統保安外的措施。此外，我們亦已展開下列行動：

- 向相關人士/機構通告事故
- 回顧系統使用和資料保存政策

Source 來源：HKTVmall email notification to customer subjected “客戶資料安全事件| Information Security Event on Customer Data”

個案研究: HKTVmall 客戶資料未經授權被取覽

- 增加和改善保安措施

個案分析：HKTVmall 客戶資料未經授權被取覽

恰當的處理	
有充分的事故應變能力	• 即時採取行動防止事故惡化
有充分的事故徵測和分析	• 分析事故發生的詳細情況 • 了解受事故影響的範圍
事故後的處理恰當	• 向相關機構報告 • 通知受影響的用戶 • 對系統的設定和防備作出改善 • 改善及增加監控系統

能改善之處	
• 及早更新系統以堵塞漏洞	• 限制系統存取權限
• 在防火牆只容許必要的流量	• 將敏感資料和系統與互聯網分隔
• 訂立數據儲存規例：儲存時限、儲存位置、清除方案 等等	

處理網絡釣魚 Phishing（詐騙 Scam）的要點

處理周期階段 Handling Cycle Stages	必要步驟 Compulsory Steps
籌備 Preparation	• 準備網絡釣魚事故的溝通渠道 • 採用可行的保安解決方案，例如電郵過濾閘道等
偵測和分析 Detection & Analysis	• 收集網絡釣魚的數據（例如釣魚電郵），調查其標頭並找出發送源
遏制、根除和恢復 Containment, Eradication & Recovery	• 從電腦中刪除相關的釣魚郵件 • 盡可能通過相關通訊閘道攔截相關釣魚來源
事後行動 Post-Incident Actions	• 重新考慮通訊閘道的規則：檢查是否可能提高網絡釣魚的偵測級別等 • 討論改進（經驗教訓）

處理惡意軟件 Malware 或勒索軟件 Ransomware 的要點

處理周期階段 Handling Cycle Stages	必要步驟 Compulsory Steps
籌備 Preparation	• 評估和保護重要系統備份，創建可能的恢復點 • 在系統中安裝防毒軟件並保持最新狀態
偵測和分析 Detection & Analysis	• 檢視防毒軟件警報或懷疑被入侵的跡象 • 了解惡意軟件及其特徵，查證惡意軟件是否仍在運行或與其他裝置溝通
遏制、根除和恢復 Containment, Eradication & Recovery	• 盡快隔離受感染系統，使受感染系統保持通電狀態 • 隔離惡意軟件並確保在恢復系統正常運行之前將其徹底清除 • 當遇到勒索軟件攻擊時，查找是否有可信來源發布的解密器 • 如果沒有可用的解密器，找出可能的離線備份並將數據恢復到不受影響的系統
事後行動 Post-Incident Actions	• 重新考慮系統的安全性：檢查檢查防火牆及防毒軟件設定、應用程式的安全性等

處理分散式阻斷服務 DDoS的要點

處理周期階段 Handling Cycle Stages	必要步驟 Compulsory Steps
籌備 Preparation	• 採用保安解決方案，例如入侵偵測和預防系統（IDPS）等 • 限制防火牆規則，盡可能採用默認拒絕所有流量的原則
偵測和分析 Detection & Analysis	• 確定任何受到影響的系統，從網絡流量日誌中查緝來源 • 檢查網絡和系統日誌，找出可疑活動，分析受影響系統中是否存在用於DDoS攻擊的漏洞
遏制、根除和恢復 Containment, Eradication & Recovery	• 在 IDPS 或防火牆的阻止相關網絡流量 • 禁用可能用於對受影響系統進行 DDoS 攻擊的登入帳號 • 有需要時，聯絡網絡供應商尋求協助
事後行動 Post-Incident Actions	• 重新考慮系統的安全性

如何善用保安事故應變指南

Preparation:	
1.	What measures are in place to prevent this type of incident from occurring or to limit its impact?
2.	Would the organisation consider this activity an incident? If so, which of the organisation's policies does this activity violate?
Detection & Analysis:	
1.	What precursors of the incident, if any, may the organisation detect? Would any precursors cause the organisation to act before the incident occurred?
2.	What indicators of the incident may the organisation detect? Which indicators would cause someone to think that an incident may have occurred?
3.	What additional tools may be needed to detect this particular incident?
4.	How would the incident response team analyse and validate this incident? What personnel would be involved in the analysis and validation process?
5.	To whom and which groups within the organisation should the incident be reported?
6.	How would the team prioritise the handling of this incident?
Containment, Eradication and Recovery:	
1.	What strategy should the organisation take to contain the incident? Why is this strategy preferable to others?
2.	What could happen if the incident were not contained?
3.	What additional tools might be needed to respond to this particular incident?
4.	Which personnel would be involved in the containment, eradication, and/or recovery processes?

	Action	Completed
	Detection and Analysis	
1	Determine whether an incident has occurred	
1.1	Analyse the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g. search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering the evidence	
2.	Prioritise the handling of the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organisations	
	Containment, Eradication, and Recovery	
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	

情景問題

- 制定完整的保安事故應變計劃：
  - 盡量攝取系統環境的資料
  - 應包括及排除的考慮因素

列表清單

- 簡化保安事故應變周期的應用：
  - 列出採取行動的範疇

4 Key Takeaways

要點回顧

保安事故應變計劃

盡可能找出有機會受網絡保安事故影響的系統及裝置，並評估其嚴重性

應訂立能夠做到而有成效的方法

有詳細的計劃來預防和處理安全事件

保安事故應變計劃應定期檢閱並保持更新

向不同機構報告保安事故

香港電腦保安事故協調中心(HKCERT)
惡意程式、網頁塗改、網絡釣魚、網上詐騙、阻斷服務攻擊

香港警務處 網絡安全及科技罪案調查科 (CSTCB)
網絡犯罪行為，例如：網上詐騙和牽涉經濟損失的案件

個人資料私隱專員公署 (PCPD)
涉及個人資料的投訴

香港通訊事務管理局辦公室 (OFCA)
非應邀電子訊息（垃圾郵件）

HKCERT

Hong Kong Productivity Council
香港生產力促進局

HKPC Building, 78 Tat Chee Avenue, Kowloon, Hong Kong
香港九龍達之路78號生產力大樓
+852 2788 5678 www.hkpc.org

Hong Kong Computer Emergency Response Team Coordination Centre
HKCERT 香港電腦保安事故協調中心

安心，放心
居家工作

Yu On Ng | 資訊保安顧問 | 2022年4月

HKCERT

程序

1. 遙距工作注意事項
2. 網上會議注意事項

遙距工作

Image: https://blog.emsisoft.com/en/37028/remote-work-ransomware-protection-guide-for-businesses/

疫情後全球及本港居家工作數字

全球

1. **81%** 企業已經大規模實施居家工作
2. **74%** 計劃永久實行居家工作

本港

1. **60%** 受訪顧主已實施居家工作
2. **超過60%** 顧員享受居家工作及希望公司應加強資訊科技來應付

遠端連接技術

遠端連接軟件

- *普遍是開放免費軟件*
- *安全措施較寬鬆*
- *存在安全風險*

虛擬私人網絡 VPN

- *需要進行身份驗證，限制人員接入及權限*
- *惡意軟件可以透過 VPN 入侵企業網絡*

桌面虛擬化 VDI

- *安全規格較高，用戶經驗證後接入標準規格的虛擬電腦*
- *成本高，需要周邊設備配合*

網絡攻擊數字

1. 2020年，每日發現**100,000**新的惡意網站及**10,000**惡意文件
2. 2021年，勒索軟件攻擊有**93%**上升
3. 於2021年，平均每**10**秒就有一間企業被攻擊

勒索軟件猖獗，造成重大經濟損失

paloalto NETWORKS | UNIT 42

2022 Ransomware Threat Report

144%

AVERAGE DEMAND IN 2021

consultants handled in 2020. The average payment in cases worked by Unit 42 consultants climbed to $541,010, which is 78% higher than the previous year.

cks per minute

Source: Herjavec Group

網絡攻擊 – 釣魚攻擊

釣魚方法

- 冒充Dropbox，O365電郵/網站
- 冒充知名域名或利用受關注主題(例如防疫，消費卷等)
  - 假疾病預防控制中心網站 (海外)
  - 假遙距營商計劃網站 (本地)
- 假娛樂網站，例如遊戲，電影

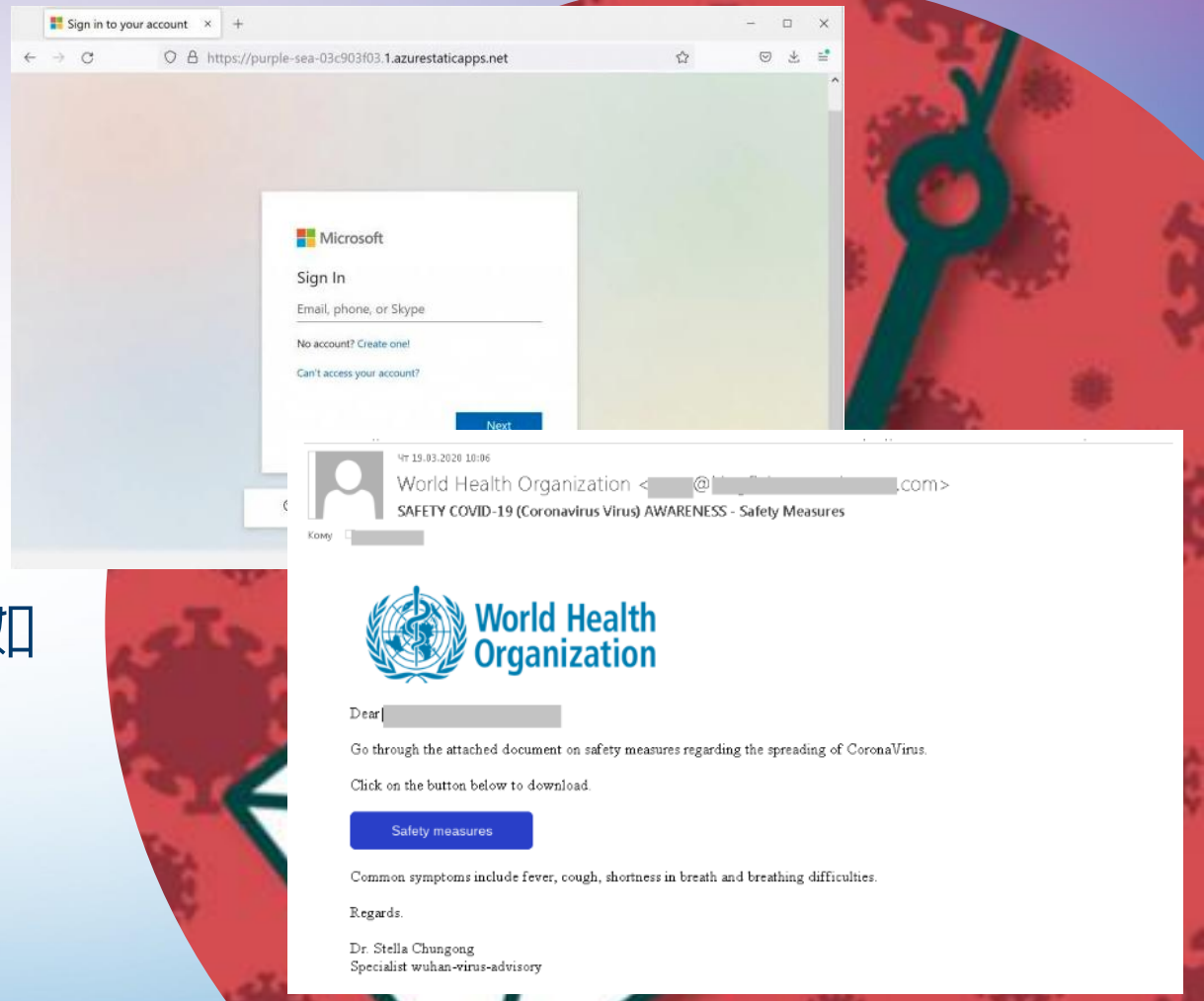


Image source: https://www.clarecomputer.com/blog/covid-19-relief-aid-phishing-attempts-have-increased-by-6000-is-your-business-vulnerable/
https://www.bleepingcomputer.com/news/microsoft/phishing-uses-azure-static-web-pages-to-impersonate-microsoft/
Kaspersky

網絡攻擊 – 遠端連接攻擊

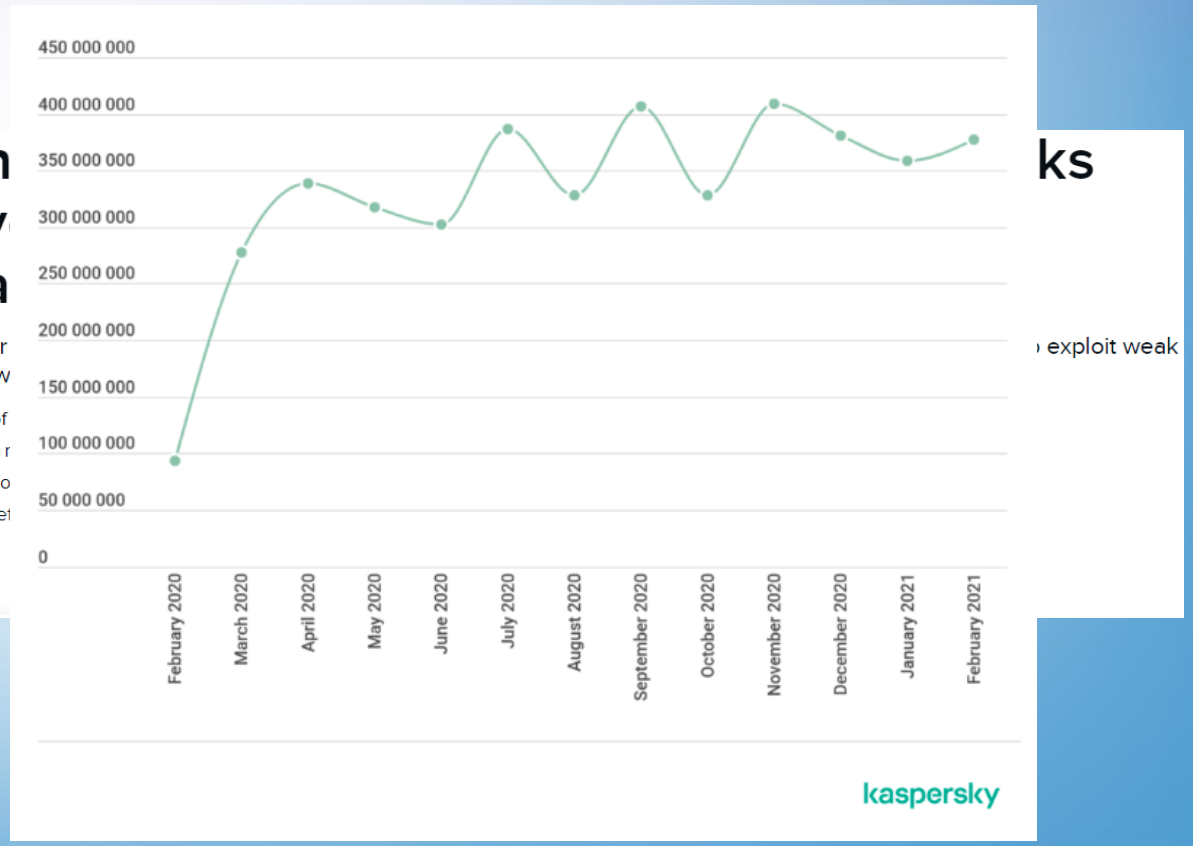
黑客搜尋沒有安全配置的遠端連接設備進行入侵

目標

- 遠程桌面協議
- 虛擬私人網絡

攻擊方法

- 利用未修補的漏洞
- 強行破解登入密碼



資料來源：

- Kaspersky
- https://www.zdnet.com/article/these-systems-are-facing-billions-of-attacks-every-month-as-hackers-try-to-guess-passwords/

居家工作保安問題因由

企業

- 在架設網絡時沒有做足保安措施
- 沒有修復系統漏洞及有效的監控
- 沒有給員工充足培訓

- 沒有開啟多要素驗證(MFA)
- 使用太過簡單密碼，或預設的密碼

員工

- 沒有足夠技術支援
- 辦工設備除了工作用途，還有私人用途
- 要處理大量內部及外部郵件

5項必備保護措施

資料來源：
CheckPoint

1. 防衛來自終端或流動裝置帶來的威脅

- *70% 網絡攻擊源於终端，如筆記本電腦、手提電話. – IDC*
- *接近46%企業，至少一名僱員曾經下載過流動惡意程式*

實施終端保安4原則

- 反釣魚攻擊
- 反惡意軟件，例如勒索軟件，殭屍病毒
- 阻截不良內容
- 自動檢測及修復

2. 啟用多要素驗證 MFA

盡可能在所有賬戶開啟多要素驗證

密碼使用習慣統計

1. 59% 使用自己名字或生日日期作為密碼
2. 43% 用家會同其他人分享密碼
3. 42% 企業會將密碼張貼出來，如張貼到公司桌面
4. IT 從業員比普遍用戶更易重用密碼

資料來源：

- https://www.comparitech.com/blog/information-security/password-statistics/

為何要使用多要素驗證?

- MFA 可以防止 **99.9%** 攻擊 – By Microsoft Manager Alex Weinert
- 只有 **45%** 用戶會在密碼被泄露後修改密碼 – By Google Survey
- 有**2/3**用戶會在多個賬戶使用相同密碼 – By 2019 Google Study

什麼是多要素驗證?

使用多個以下要素

- 你所知道 – e.g. password
- 你所攜有 – e.g. one time password (OTP)
- 你是誰 – e.g. biometric

3. 互聯網安全

在2020年，每日有100,000個惡意網站被發現 - Check Point Research

4 個概念實施互聯網安全

- 有能力預防最新/未知威脅
- 不防阻用戶體驗
- 私隱
- 100% 流量檢視

4. 保護電子郵箱
防止散播惡意程式及釣魚攻擊

起過50%網絡犯罪的損失是由於公司郵件被破解

4項安全建議守護公司郵件

- 實時釣魚攻擊保護
- 防衛惡意程式
- 防止數據洩漏
- 防衛內部攻擊

5. 注意雲服務安全

87% 僱主因應疫情加快把業務轉移到雲 - LogicMonitor

前4項公共雲保安事故因由

27%公司的雲端服務曾遭攻擊

23% 由於錯誤配置

15% 數據或文件不恰當傳送

15% 賬戶被破解

14% 漏洞利用

資料來源：
CheckPoint 2022 cloud security report

雲服務保安建議

- 配置訪問及存取限制
- 採用先進威脅防衛 (ATP)
- 實施應用方面的防護 (e.g., WAF, scanners, etc.)
- 啟用多要素驗證

其他安全建議

1. 設置監控及記錄機制

可疑活動可以被標示及通知相關技術人員。技術人員跟據記錄展開調查。

2. 建立應急預案

e.g. *備份，建立恢復方案，風險檢視*

3. 提供定時網絡安全培訓

定期對員工進行安全意識培訓，如小測、釣魚測試

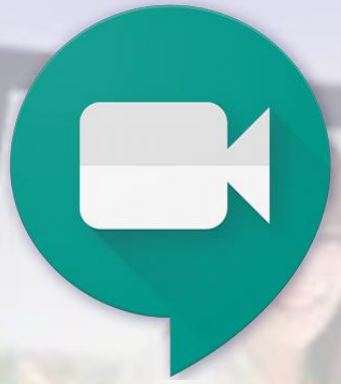
4. 注意網絡保安動向

保持網絡資訊更新。如發現與公司相關網絡保安問題，可與HKCERT聯絡

安全使用視像會議

Source: https://www.smwllc.com/protect-meetings-zoom-teams-webex/

有沒有似曾相識?

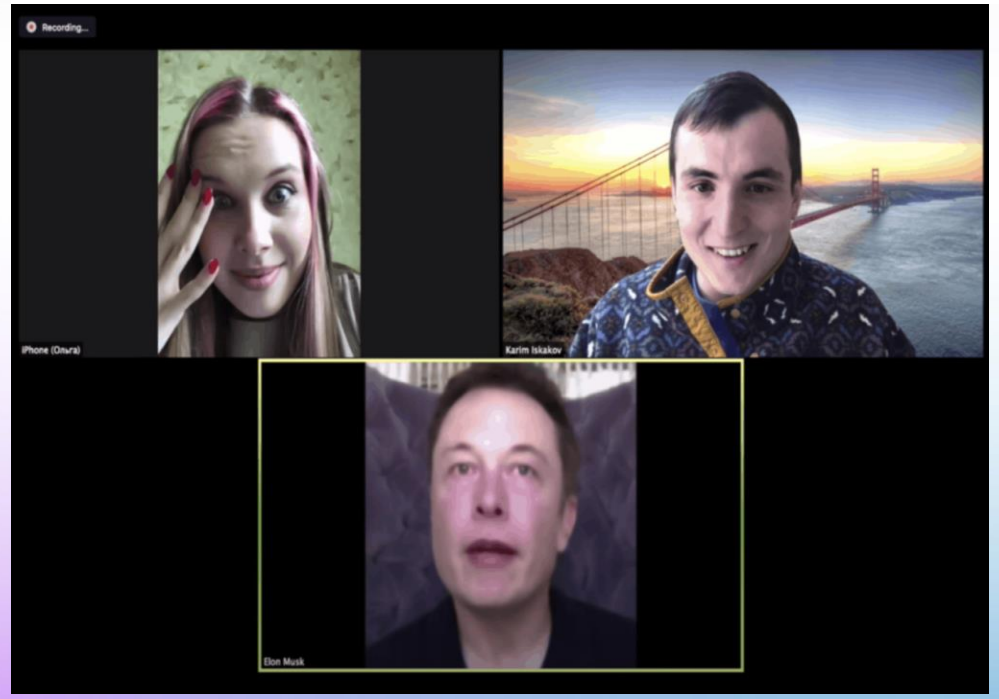


Meet

Microsoft Teams

提防欺詐手法 - Deepfake

This Open-Source Program Deepfakes You During Zoom Meetings, in Real Time



「你是誰？」議員與「俄羅斯反對派成員」Zoom視訊結束後，才驚覺對方可能是Deepfake

他們收到了一些「俄羅斯反對派成員」的視訊會議邀請，還煞有其事地討論了克里米亞問題之類的政治事務，結果發現在這些所謂的「俄羅斯反對派成員」都是別人用Deepfake換臉假冒的。

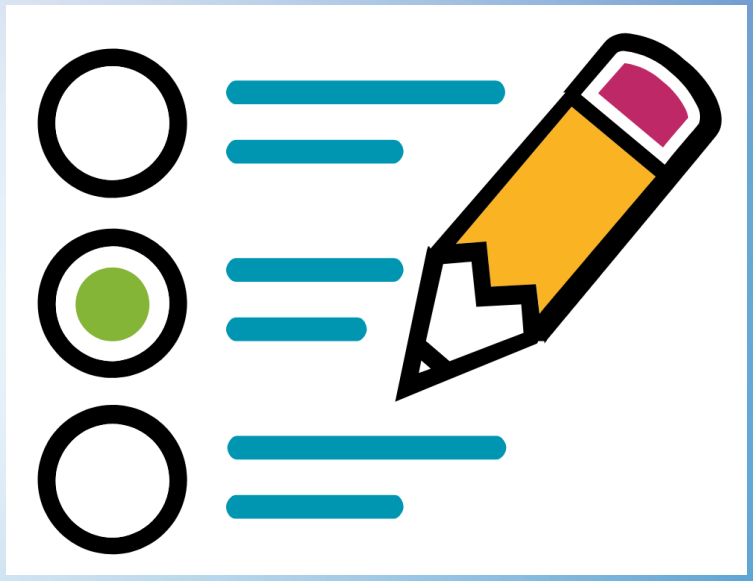
這些受騙者包括拉脫維亞議會外交事務委員會主席Rihards Kols，以及來自愛沙尼亞和立陶宛的議員。英國外交事務特別委員會主席Tom Tugendhat也表示，他也是目標之一。

資料來源：

- https://www.vice.com/en/article/g5xagy/this-open-source-program-deepfakes-you-during-zoom-meetings-in-real-timehttps://securityaffairs.co/wordpress/102495/hacking/covid-19rdp-bruteforce-attacks.html
- https://www.techbang.com/posts/86684-deepfake-zoom-video-conference

使用視頻會議軟件思維

- 風險評估
  - 數據分類, e.g. 敏感資料?
  - 認識風險源頭及成因
    - 系統漏洞
    - 錯誤配置
- 減少風險
  - 選擇一些有技術支援的供應商，會提供更新解決漏洞
  - 建立安全措施, e.g. 設定預防措施，補救措施
  - 定期更新軟件
- 進行測試
  - 確保措施符合預期



3大安全風險

Image credit: **https://economictimes.indiatimes.com/tech/internet/69-indian-firms-face-serious-cyber-attack-risk-study/articleshow/69305216.cms**

#1 未經許可參加會議(e.g. 會議騎劫)

- 未被授權人士進入會議 (e.g. zoombombing)
  - 撞破會議連接及ID，從而非法進入會議
- 後果/影響
  - 展示惡意內容，如暴力影像或不雅照片
  - 進行性騷擾
  - 把會議內容洩露

#2 散播惡意軟件/ 可疑 URL

- 在會議聊天室散播惡意軟件或釣魚網站
  - Zoom曾經出現UNC漏洞 ，容許黑客透過聊天室發放URL奪取Windows login

- 後果/影響
  - 植入勒索軟件
  - 偷取敏感資料
  - 金錢欺詐

#3 私隱問題

- 會議視頻記錄被未授權人士訪問
- 收音在未經許可下打開
- 後果/影響
  - 資料外洩
  - 法律問題
  - 影響聲譽

Your Zoom videos could live on in the cloud even after you delete them

A Zoom Bug Is Recording Mac Users Outside of Calls: Here's the Fix

It sounds scary, but a simple update is all it takes for peace of mind.

BY AYA MASANGO

PUBLISHED FEB 16, 2022

A week ago, Phil Guimond discovered a vulnerability that allowed someone to search for stored Zoom videos using share links that contain part of a URL, such as a company or organization name. The videos could then be downloaded and viewed. Guimond also created a tool, called Zoombo, that exploited a limitation of Zoom's privacy protection, cracking passwords on videos that savvy users had manually protected. He discovered videos that were deleted remained available for several hours before disappearing.

https://www.cnet.com/news/your-zoom-videos-could-live-on-in-the-cloud-even-after-you-delete-them/
https://www.makeuseof.com/zoom-bug-mac-fix-recording-users-outside-calls/

保安建議

Image credit: **https://www.century-it.co.uk/cyber-security-advice-and-help/**

會議前準備

設置用戶指引

把會議軟件更新到最新版本

把會議設置為私人會議，防止入侵者

不要隨意透露會議連接及接入密碼

不要重複使用同一個會議連接及ID

開啟waiting room 功能

會議中措施

限制會議參與者在會議中行為

e.g. video, audio, screen sharing, chat

監控聊天室是否有不當內容

提示會議參與者，會議會被記錄

把會議視頻記錄存放到本地

會議開始後，把會議鎖上，禁止人員再進入會議

HKCERT

Hong Kong Productivity Council
香港生產力促進局

HKPC Building, 78 Tat Chee Avenue, Kowloon, Hong Kong
香港九龍達之路78號生產力大樓
+852 2788 5678 www.hkpc.org