



# Good habits to enhance cyber hygiene for the SMEs

## 中小企 - 養成良好習慣， 加強網絡衛生



A large, semi-transparent pink hexagonal shield is positioned on the right side of the slide. Inside the shield, there is a dense grid of cybersecurity-related terms and acronyms, all in white or light blue text. The terms include: WFH, Digital Certificate, Security Awareness, DDoS, Malware, Password Sniffing, Virtual Hijack, Unencrypted QR Code, AI Frauds, Webinar, VPN, Exploitation, Virus Scan, Deepfake, Antivirus, Hacker, IP Address, Data Breach, HTTPS, Robotics, Information Security, Web Meeting, Remote Work, Distance Learning, Social networking, Cyberspace, Automatic updates, Network Blacklist, Phishing, Sensitive Information, Confidentiality, Some Distance Learning, Browsing, BYOD, Keystrokes Activity Monitoring, Digital Transformation, Cybercrime, Data Leakage, System Overload, Extortion, Data protection, Vulnerabilities, Trojan Virus, Backdoor, Internet Authentication, Backdoor, Digital copyrights, Coding, Coding, Mitigation, Spear Phishing, Anti-Malware, Privacy, Identity check, Ransomcloud, Online Shopping, Ransomware, Cyber Attack, Cloud Sharing, Firewalls, Clickjacking.



# Agenda 程序

1. Security Incident Data 網絡保安事故數據
  2. Past Security Incidents 過去網絡保安事故及分析
  3. Advice 建議



# HKCERT

- Hong Kong Computer Security Incident Coordination Centre  
香港電腦保安事故協調中心
- Affiliated to the Hong Kong Productivity Council and funded by the Hong Kong SAR Government  
由香港生產力促進局管理，並由香港特別行政區政府資助
- To provide Hong Kong enterprises and Internet users with information and defense guidelines on information security incidents, incident response, and to raise cybersecurity awareness  
為香港企業及互聯網用戶提供資訊保安事故的消息和防禦指引、事故回應及支援服務，及提高網絡保安意識
- Responsible for liaising with Hong Kong organizations, collecting, distributing information and coordinating computer security incident response  
負責聯絡香港組織，收集、發放訊息及協調電腦保安事故的應變





# A point of contact for cross-border cyber security incidents 作為香港跨境網絡保安事件的聯絡點

## International 海外



Exchange Incidents and Information  
交換網絡保安資訊

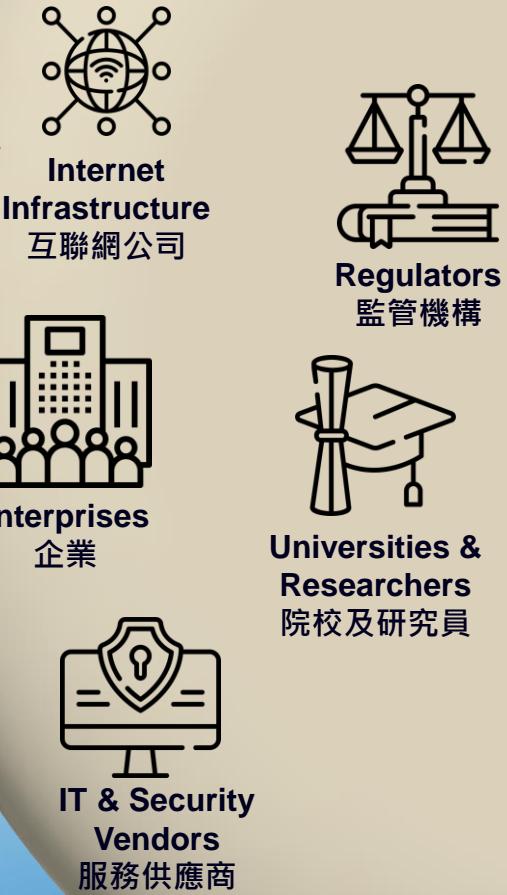
Coordinate incidents and publish alerts  
協調保安事故及保安預警



## GovCERT.HK



## Local 本地



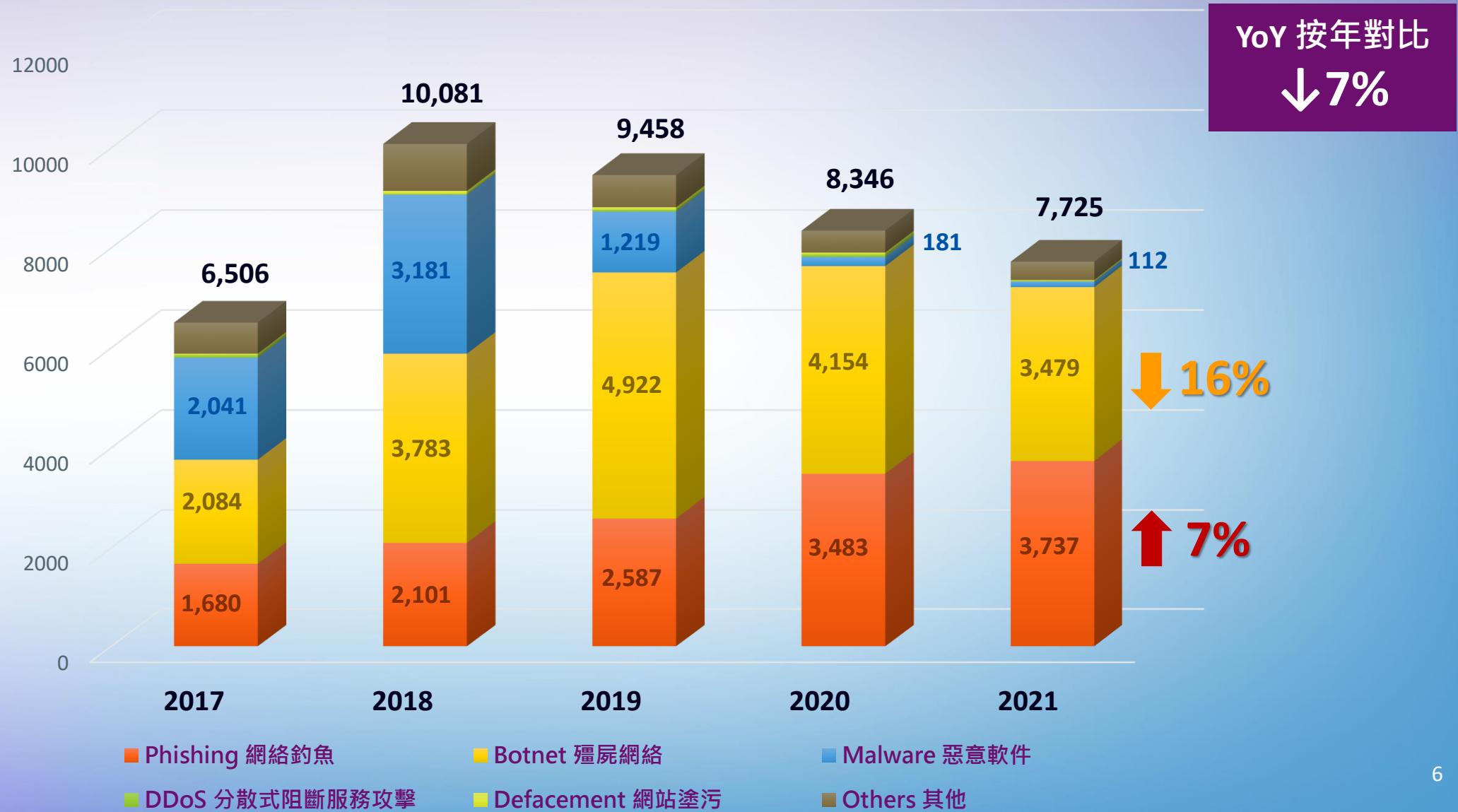
1

# Security Incident Data 网络安全事故數據



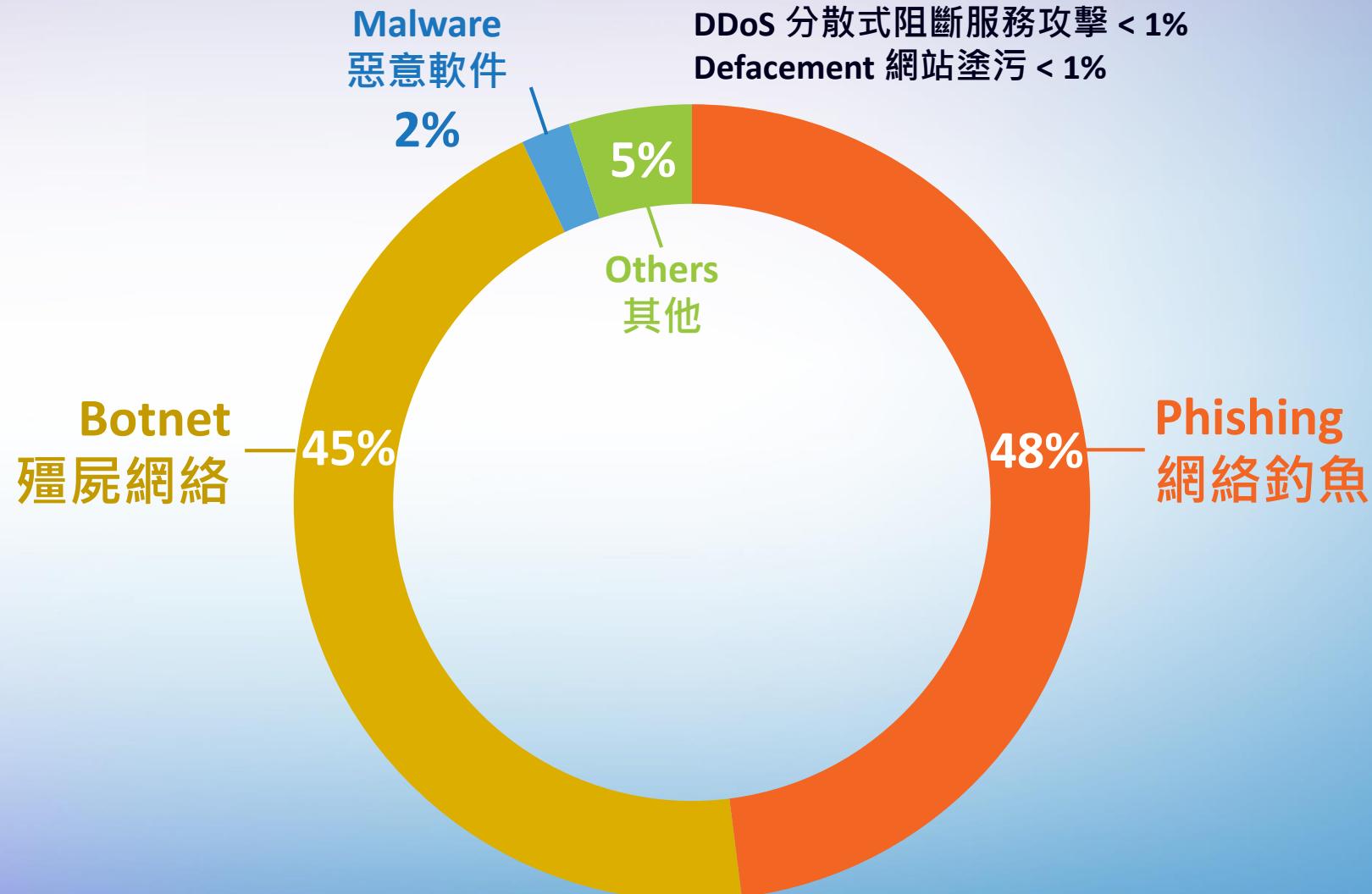
# Trend of Security Incidents

## 保安事故走勢



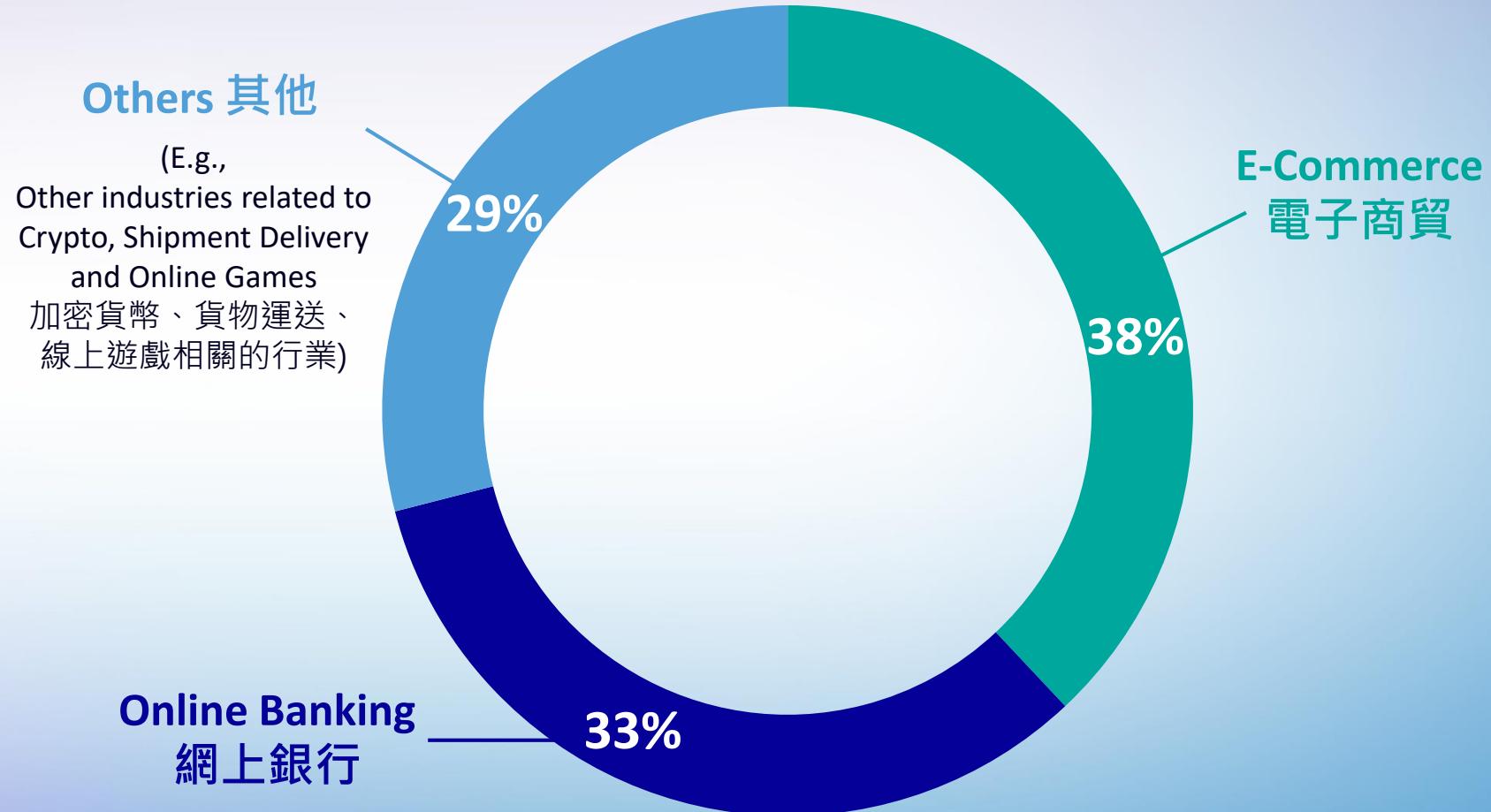
# Categories of Security Incident 2021

## 2021保安事故類別



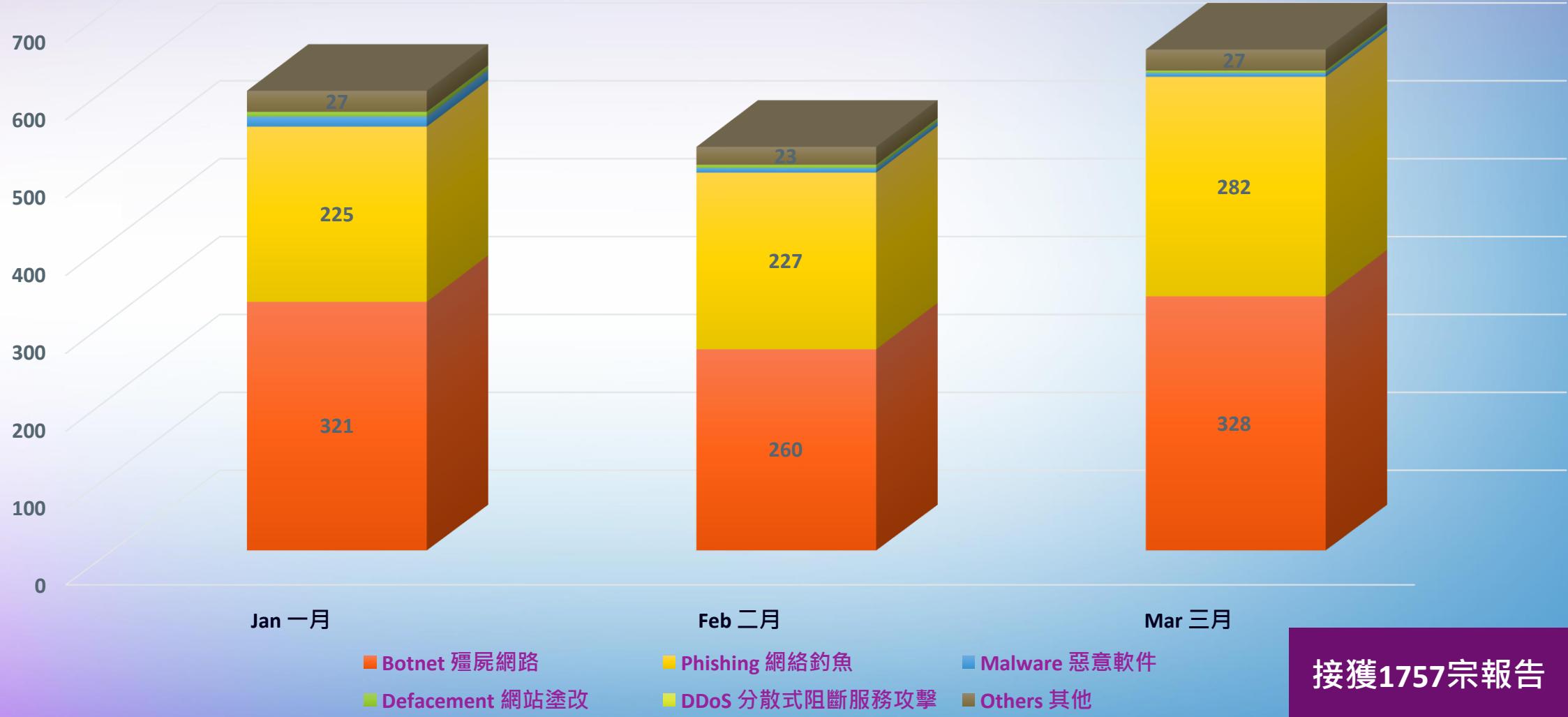
# Types of Phishing Attacks in 2021

## 2021釣魚攻擊種類



# Incidents reported from Jan to Mar 2022

## 2022年1月至3月事故報告



# HKCERT's Responses to Information Security Challenges

## HKCERT 針對資訊保安挑戰的回應



### Beware of Flash Phishing Attacks

Release Date: 7 Jun 2021 | 4441 Views

清理及防範QSnatch惡意軟件



### Ransomware Keep Evolving: Multiple Extortion

Release Date: 22 Jun 2021 | 4626 Views

Protect sensitive information in the use of social media and beware of potential cyber attacks arising from data leakages

Release Date: 27 Apr 2021 | 6250 Views



### Introducing the New "Fight Ransomware" Webpage

Release Date: 19 Nov 2021 | 3757 Views



Ransomware attacks are current cyber threats nowadays. More According to a ransomware report (172 million), up 43% from 2021



### 提防網購及長假期的網絡保安風險

發佈日期: 2021年12月21日 | 2050 閱讀次數



### Patch Vulnerabilities in Remote Access and Remote Storage Now

Release Date: 1 Sep 2021 | 7967 Views

### HKCERT Urges Users of Remote Access Tools and NAS Devices to Beware of Ransomware Attacks

Release Date: 21 Oct 2021 | 1591 Views



### HKCERT Urges Local IT Users to Patch Apache "Log4j" Vulnerability ASAP

Release Date: 16 Dec 2021 | 3214 Views

(Hong Kong, 16 December 2021) The Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) of the Hong Kong Productivity Council is urging local IT users to patch their systems as soon as possible in light of the discovery of a critical vulnerability in Apache "Log4j" and an upsurge in related exploit attempts globally.

Apache "Log4j" is an open-source logging application commonly used in a wide range of IT equipment and software products, such as web servers, network devices, database servers, etc. For the current issue, systems running Apache Log4j version 2.14.1 or below are most vulnerable. Attackers can exploit the vulnerability to seize control of the system and turn it into part of a botnet with updated version of Mirai and Moshikai malware, or even launch ransomware attacks such as Korsair. As HKCERT believes the situation will continue to worsen with more new malware and ransomware attacks related to the "Log4j" vulnerability on the horizon, it urges both individuals and organisations to pay extra attention to related attacks and promptly apply security patch.



### OWASP Top 10-2021 is Now Released

Release Date: 4 Oct 2021 | 6669 Views

### Business as Usual under COVID-19 with Sound "Work from Home" Cyber Security

Release Date: 10 Jan 2022 | 2148 Views

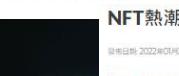


### Secure Use of QR Code

Release Date: 7 Jan 2022 | 1676 Views

### Introduction of QR code attacks and countermeasures

Release Date: 20 Jan 2022 | 878 Views



### NFT熱潮下，如何保護自己的NFT資產

Release Date: 20 Jan 2022 | 250 閱讀次數



### 什麼是NFT

NFT全名是「非同質化代幣」( Non-Fungible Token )，是基於以太坊ERC721標準推出的代幣。有別於貨幣或資本，每一枚NFT都具有唯一獨特的數位ID，所以不會重複，而且交易將不可分割出售。

## 2

# Past Security Incidents 過去網絡安全事故及分析

# 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

#### 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

#### Multiple Extortion Ransomware 多重勒索軟件

Example 例子：

- 1<sup>st</sup>: Distributed Denial of Service (DDoS) 分散式阻斷服務攻擊
- 2<sup>nd</sup>: Contact victims' customers and partners 聯繫受害者的客戶和合作夥伴
- 3<sup>rd</sup>: Short sell victims' stock 賣空受害者的股票

# Common Types of Phishing Attacks 常見釣魚攻擊手法

- Send messages and/or URLs via fake emails or instant messaging / SMS  
透過偽冒電郵或即時通訊軟件/短訊發出訊息及網址
- Use voice or malicious USB  
利用語音方式或USB以偷取用戶資料
- Put malicious QR Code of phishing website  
釣魚網站的惡意二維碼



# Send messages and URLs via fake emails or SMS 透過偽冒電郵或手機短訊發出訊息及網址

- Hackers send bogus messages and links via email or mobile. When the user links to the fake website, they will enter their bank details. Hackers use this to obtain login information.

黑客會透過電郵或手機電訊發出偽冒訊息及連結。當用戶連結該偽冒網站後，會輸入銀行資料。黑客藉此偷取登入資訊。

- When we point to the location to be linked by sliding the mouse cursor, the bottom left of the browser will display the real URL, which is not the bank's official website

當我們透過滑鼠標浮標指著要連結的位置，瀏覽器左下方會顯示出連結的網址並不是該銀行網站

verify your HSBC card to activate the weekly cash back bonus via the following link:  
<https://bit.ly/3b2ZVab>

HSBC: A payment of HKD100,000 was attempted to Mr C Ying on 25/06/2021. If this was NOT you, log-on and cancel immediately via: [hsbc.hk.transfer-ref72019.com](http://hsbc.hk.transfer-ref72019.com)



# Browser In The Browser (BITB) Phishing Attack

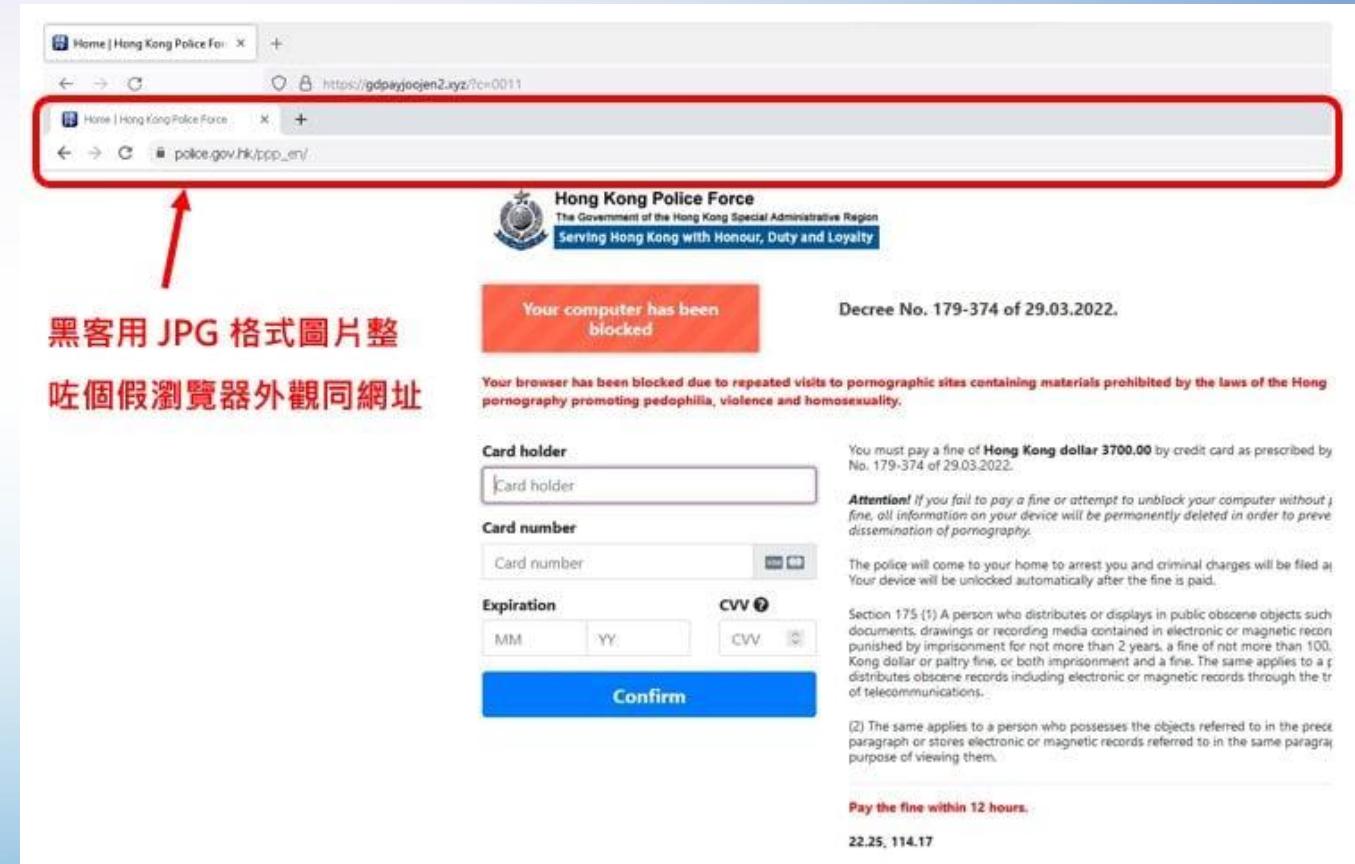
## 嵌入式瀏覽器釣魚攻擊

- When in full screen mode, the URL and logo are the same as the real Hong Kong Police website

當進入全屏幕模式，網址和標誌與真香港警察網站無異

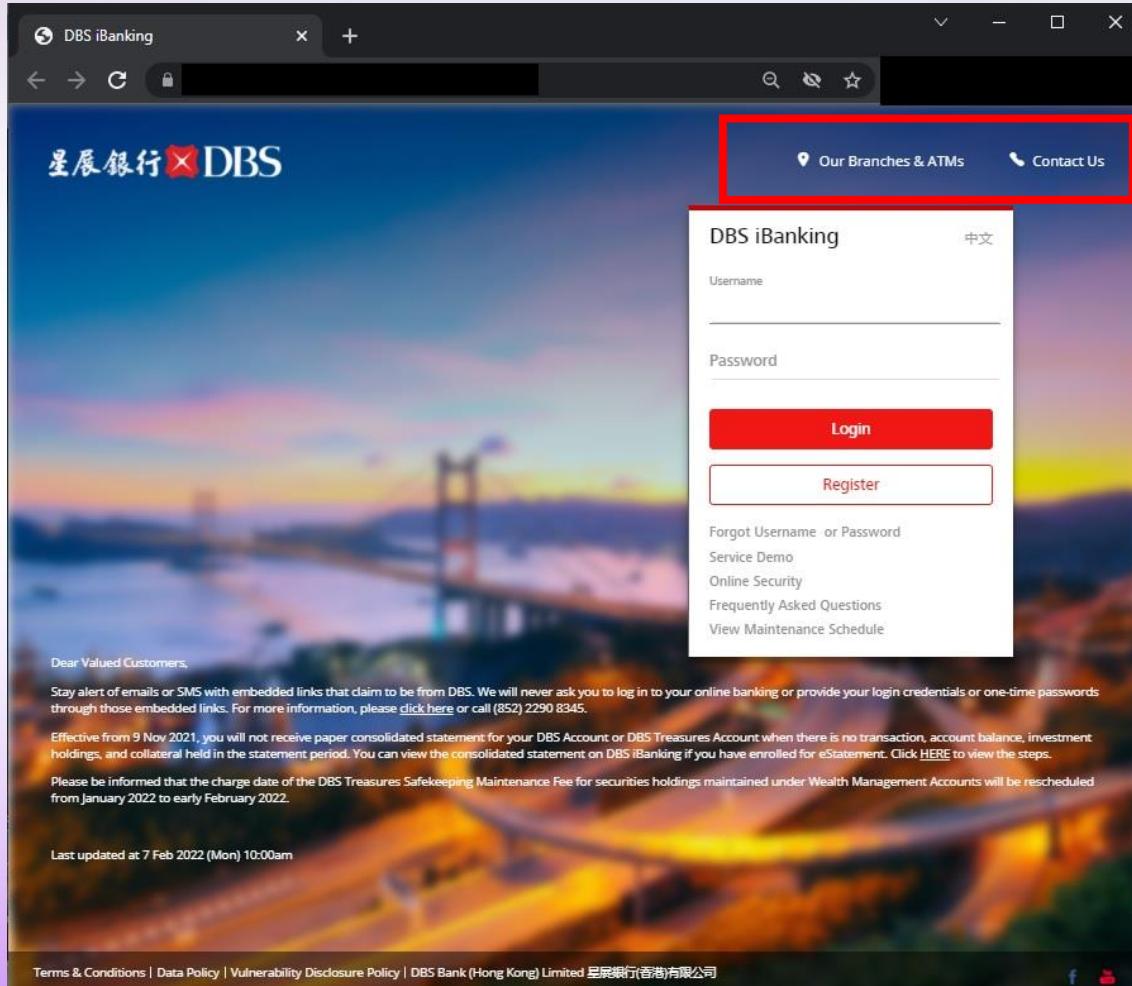
- Hackers make fake websites through JPG. Enter full screen mode, thereby hiding the real URL

黑客透過JPG整作虛假網站。進入全屏幕模式，藉此隱藏真正的網址。

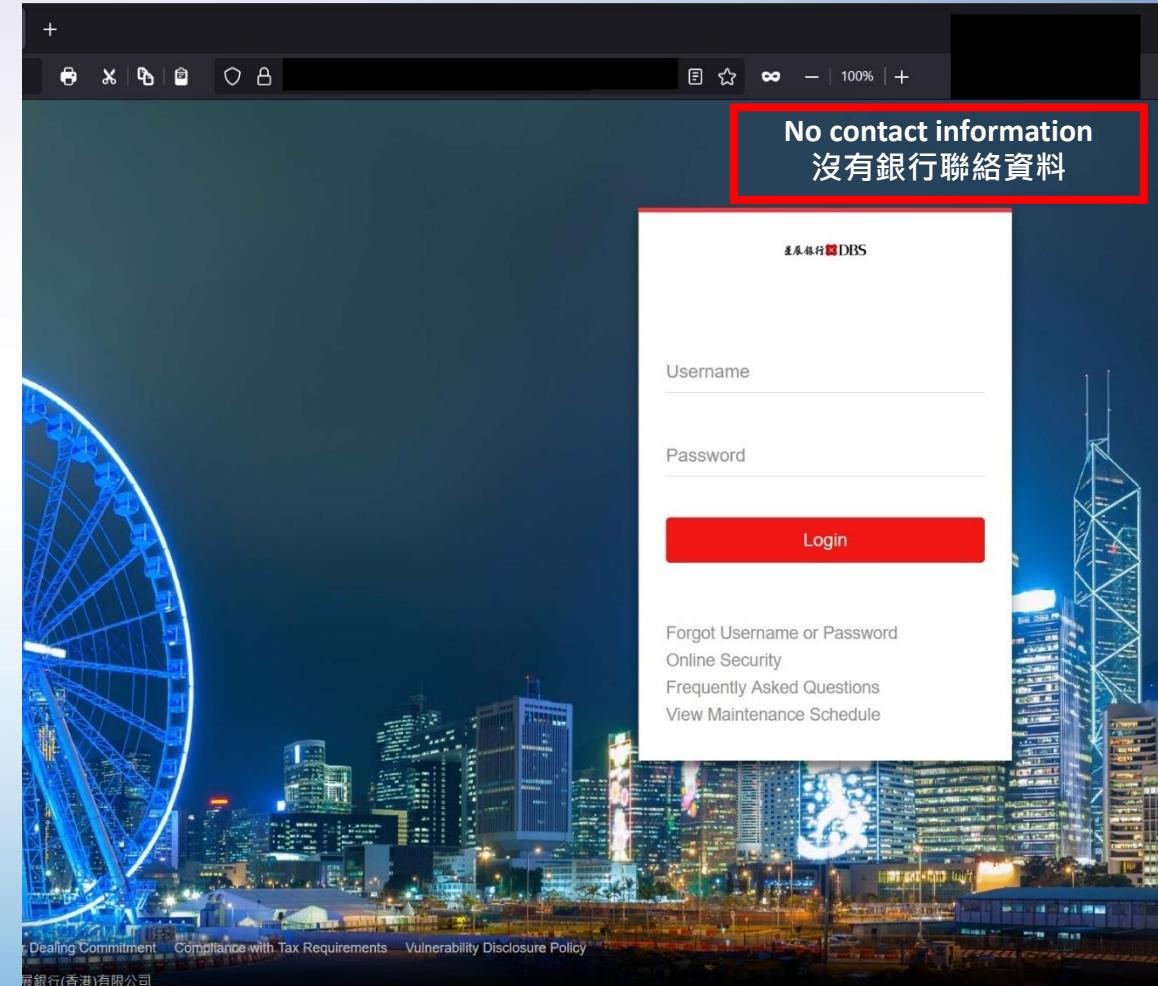


# Example Sharing: Phishing Website

## 例子分享：釣魚網站



Real 真



Fake 假

# Use voice or malicious USB to steal user information 利用語音方式或惡意USB偷取得用戶資料

## A Voice Deepfake Was Used To Scam A CEO Out Of \$243,000

Jesse Damiani Contributor @

I run Postreality Labs, a new media art advisory & curatorial studio.

Follow

Sep 3, 2019, 04:42pm EDT

### 小心公共USB充電站讓惡意程式上身，美政府籲勿使用

黑客可能在公共USB充電站設置充電陷阱，在充電站或充電線中植入惡意程式，讓路過充電的旅客因為充電而被感染，可能鎖住裝置或竊取使用者的資料。

文/ 林妍瀟 | 2019-11-15 發表



- In 2019, the British energy company thought it had received a call from the CEO of the German head office. Because the other party spoke an authentic German accent and the tone was almost the same as the CEO of the German head office he was familiar with, he transferred the money and was defrauded of 220,000 euros. This is due to "voice fishing" synthesized by AI.  
在2019年，英國能源公司以為接到德國總公司CEO來電。因為對方操著一口地道的德國口音，語調也跟他熟悉的德國總公司CEO幾乎一模一樣，於是就把款項轉了過去，被詐騙了22萬歐元。這是由於AI合成的「語音釣魚」。

- In the same year, a woman in the United Kingdom was infected with a mobile phone after a malicious program was implanted by hackers for using a public USB.  
同年，英國一名女士由於使用公用USB而被黑客植入惡意程式，導致手機被感染。

# Put malicious QR Code of phishing website 釣魚網站的惡意二維碼

Services & Software

## QR code scams are on the rise. Here's how to avoid getting duped

Cybercriminals are increasingly using malicious QR codes to trick consumers.



Bree Fowler

Jan. 25, 2022 10:42 a.m. PT

5 min read



The screenshot shows a news article from CNET. The title is "QR code scams are on the rise. Here's how to avoid getting duped". Below the title, it says "Cybercriminals are increasingly using malicious QR codes to trick consumers." The author is Bree Fowler, and the date is Jan. 25, 2022 10:42 a.m. PT. The article has a 5-minute read time. At the bottom, there's a red banner with the text "新興 Quishing 二維條碼成網絡釣魚新手法" (New trend: QR codes become a new method for network phishing). The date is 2022-05-04, and the update date is 2022-05-03. There are social sharing icons for Facebook, Twitter, Pinterest, LinkedIn, and Email.

- Can appear in both physical and virtual environment  
接觸面廣：日常生活及網上活動都有機會接觸到
- Hacker targets mobile user as security protection and user's security awareness of mobile devices are relatively weaker compared with computer  
黑客攻擊流動裝置用戶，因為裝置的保安及用戶的保安意識通常比電腦系統低
- Bypass email security system  
能避開電郵保安系統的偵測

# 「何不直接 盜取資料」

Threat  
Actor  
黑客

Crime-as-  
a-Service  
網絡罪行  
服務

Data  
Exfiltration  
偷取數據

Data Lock  
Up by  
Encryption  
鎖上檔案

Multiple  
Extortion  
Techniques  
多重勒索  
手段

Ransom  
Payment in  
Bitcoin  
用加密幣  
支付續金

# Ransomware Evolution 勒索軟件手法

- Human-operated ransomware 人為操作
- Ransomware as a Service 勒索軟件服務

# Victims

## 受害人案例



1. Critical Infrastructure

關鍵基礎設施

**Colonial Pipeline**

2. Retail 零售

**Dairy Farm**

3. Manufacturer 製造業

**JBS Foods**

4. Insurance 保險

**AXA**

5. Technology 科技

**Acer**

6. SMEs 中小企

(Affected by Kaseya incident  
受 Kaseya 事件影響)

**\$4.4m**

**\$30m**

**\$11m**

**Amount Not Known**  
**沒有公佈**

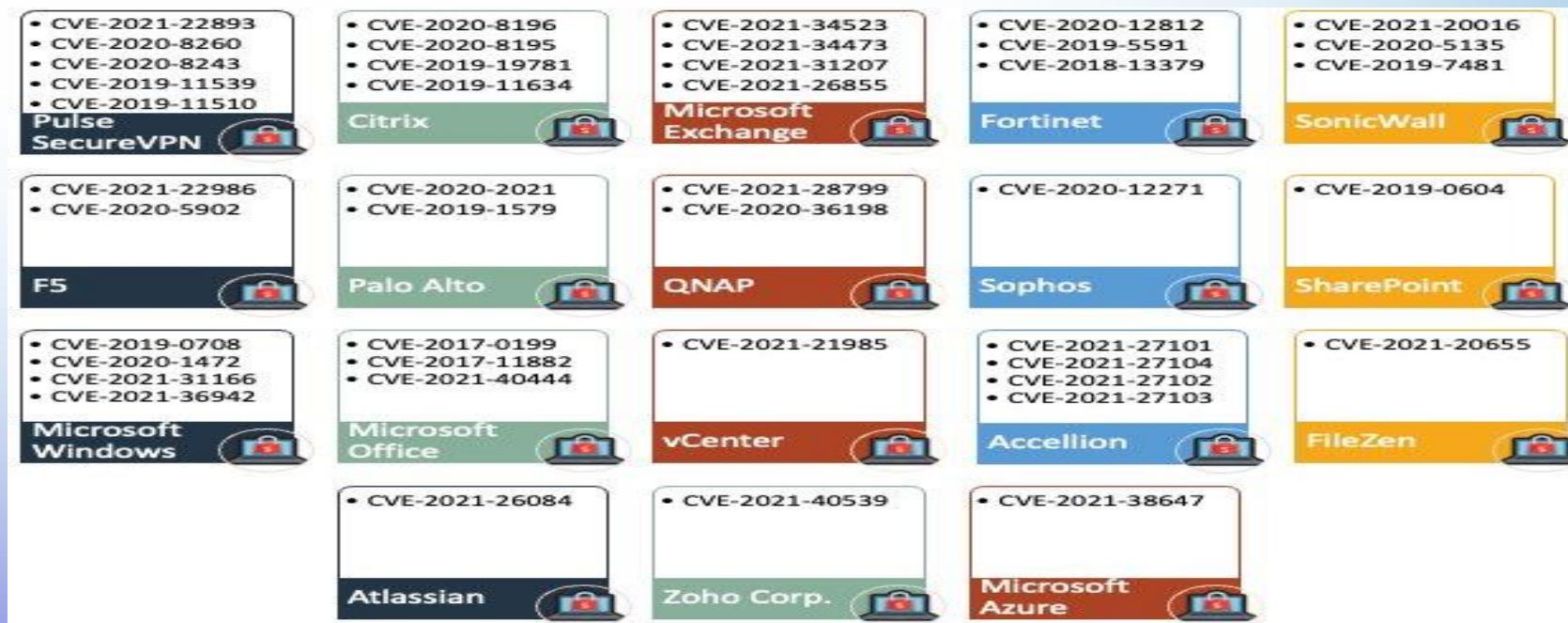
**\$50m**

**\$5m**

# Major Attack Vectors

## 攻擊途徑

1. Phishing email (link/attachment)  
釣魚電郵
2. Unsecure remote connection, e.g. RDP  
遠端連接系統
3. System vulnerabilities  
系統漏洞



# Technique/Channels to Gain Initial Access

## 其他常用作入侵的手法/途徑

- Exploit Public-Facing Application, e.g. SQL Injection  
攻擊直接連至互聯網的系統，如SQL Injection
- Trusted Relationship  
受信任第三方的存取權限(如服務供應商)
- Valid Accounts  
外洩的用戶帳號

# Weak Security Controls

## 保安問題

- Lack of Multifactor authentication and password policies  
缺乏MFA及密碼政策
- Incorrect access control list  
錯誤或過多的存取權限
- Software is not up-to-date  
沒有更新軟件
- Use of default configuration, e.g. password  
使用預設的配置，如預設密碼
- Lack of control to prevent unauthorised access  
缺乏防止入侵的保安系統
- Misconfigured services exposed on Internet  
在互聯網上的服務沒有正確的保安配置
- Poor phishing and endpoint protection  
保護電腦及防釣魚攻擊的機制不足

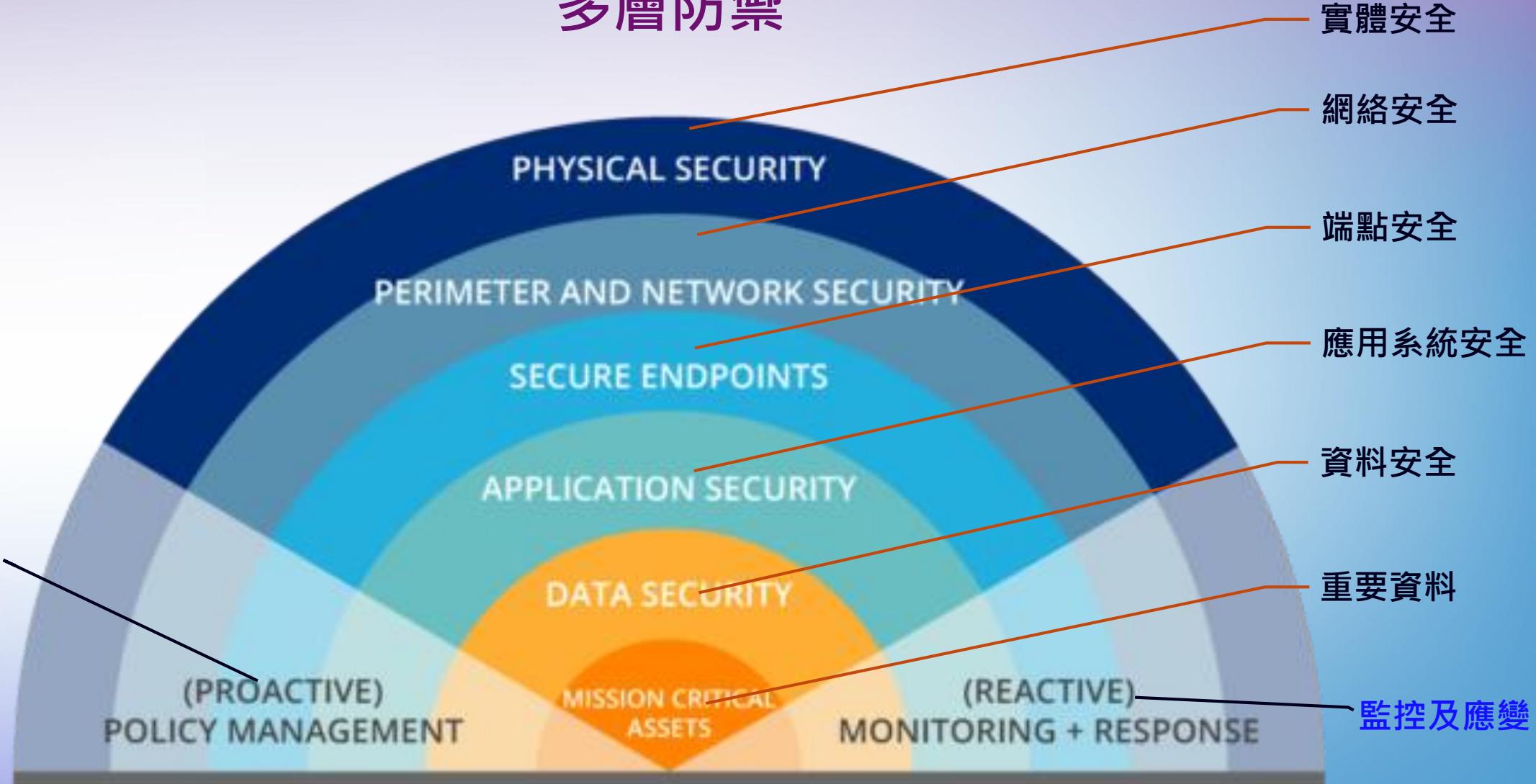
# 4

## Advice for SMEs 中小企網絡保安建議



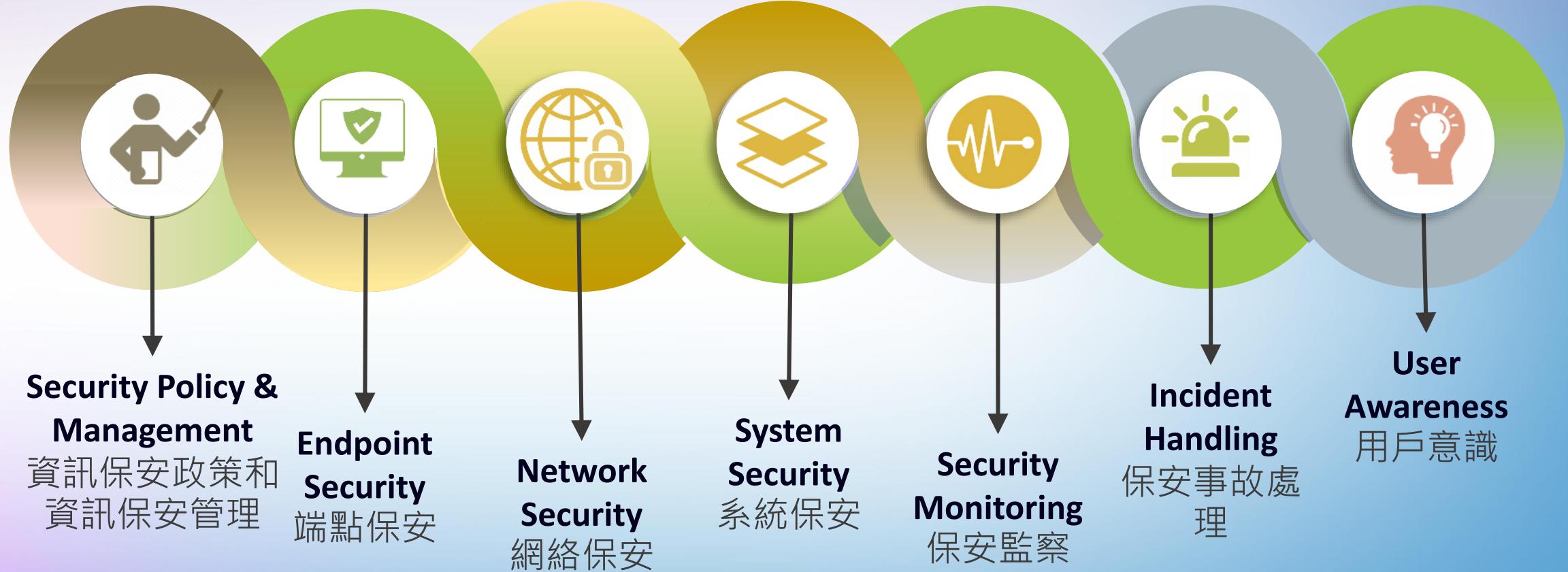
# Multiple Layers of Defense

## 多層防禦



# The Seven Habits of Cyber Security for SMEs

## 中小企網絡安全七大攻略



# Endpoint Security

## 端點保安

1

Endpoint computers should be protected by security software like **anti-virus** and **anti-malware**  
端點電腦應受到**防病毒**和**反惡意軟件**等保安軟件的保護

2

Anti-virus signatures, security software and operating system should be **kept up-to-date** to  
protect the endpoint from most recent threats  
病毒特徵檔、保安軟件和電腦操作系統應**保持最新**，以保護端點免受最新威脅。

3

User accounts on endpoint should be **non-privileged** (not “Administrator”)  
端點上的用戶帳戶應該是普通**非特權用戶**（**非**“管理員”）

# Network and System Security

## 網絡及系統保安

1

Firewall should be **configured properly** that minimize network ports of organization network exposing to the Internet

應正確配置防火牆，盡可能減少企業暴露於互聯網的網絡端口

2

**Do not allow** remote access (e.g. RDP) from Internet to internal servers

不允許從互聯網到內部伺服器的遠程訪問（例如 RDP）

3

Password policy should be configured such that passwords of server should meet **minimum length and complexity requirement**

應設置密碼政策，使伺服器密碼滿足最小長度和復雜性要求

4

For critical systems serving the public and performing critical missions, **periodical penetration test** should be performed by professional parties

對於服務公眾及執行關鍵任務的系統，應由專業人員定期進行滲透測試

# Incident Handling

## 保安事故處理

1

Logs should be **centralized** somewhere within the organization for **periodical review and monitoring**  
日誌記錄應集中儲存在某個位置，方便進行定期審查和監控

2

Incident response plans (including different kinds of security incidents) are developed  
**according to different scenarios**  
根據不同的情況制定事件應對計劃（包括不同類型的保安事件）

3

Systems and data are **backed up regularly**, the backups are taken offline (and even  
offsite)  
定期備份系統和數據，並且離線儲存（甚至異地儲存）

4

Restore procedures are drilled to make sure that the backup can be restored properly  
演練恢復程序以確保可以正確恢復備份

# Remind Staff for the Roles & Responsibility in Security

## 提醒員工保護機構訊息資產的角色和責任

1

Enable **Multi-factor Authentication**. Do Not provide your one-time-password to anyone  
啟用**多重身份驗證**，切勿向任何人提供一次性密碼

- Password must at least 8 characters long and avoid using common words and predictable characters  
密碼長度必須至少為 8 個字符，並避免使用常用詞和可預測字符, e.g. qwerty

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

# Online Cyber Security Self-assessment Tool & Incident Response Guideline

## 線上自我評估工具 & 事故處理指南



ENG 事故報告/求助

主頁 > 資源

### 評估你的網絡保安狀況。

此自我評估是根據香港電腦保安事故協調中心的【[中小企網絡安全十大攻略](#)】製作而成。它將讓你更了解你的網絡安全狀況，並會提供建議助你改善整體網絡保安能力。

請點擊開始按鈕，立即進行評估。

開始



<https://www.hkcet.org/blog/introducing-check-your-cyber-security-readiness-online-self-assessment-to>



INCIDENT RESPONSE  
GUIDELINE FOR SMEs

# HKCERT Official Website “Fight-ransomware”

## HKCERT官方網站「齊抗勒索軟件」

- HKCERT launches "Fight-ransomware" platform to provide the public with information on dealing with ransomware, such as ransomware decryptor
- HKCERT推出「齊抗勒索軟件」平台，為大眾提供有關處理勒索軟件資訊，如勒索軟件解密器



**什麼是勒索軟件？**

什麼是勒索軟件？ 感染途徑 勒索軟件的運作 預防方法 處理方法 勒索軟件種類



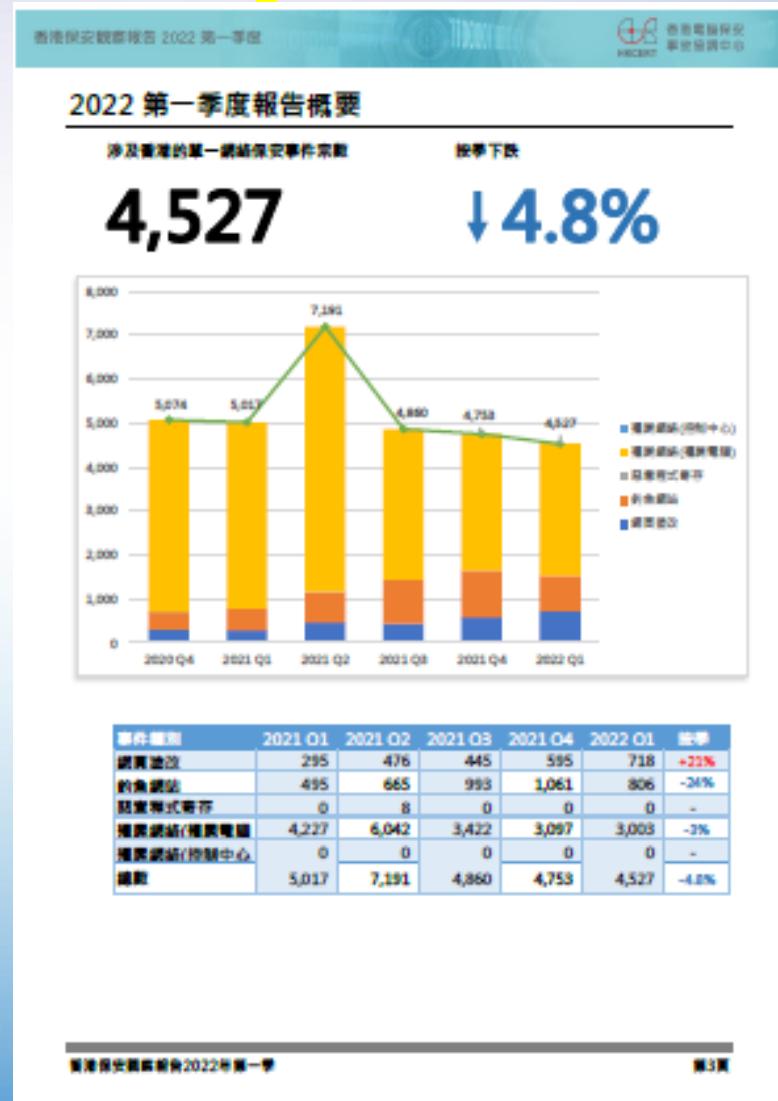
索信息	加密文件副檔名	主要傳播途徑	可解密版本*
ackByte的勒索信息是在 ackByte_restoremyfiles.hta，要求受害按照黑客提供的聯繫方式交付贖金。	副檔名為「.blackbyte」。	利用電子郵件漏洞入侵傳播	BlackByte [解密工具連結]
V1-V3為「.cerber」，其餘為多位隨機字符串。	Magniber 副檔名為「.ypkwwmd」、「.ndpyhss」、「.wmfixdqz」、「.faxlgsbrms」、「.nhsajfee」、「.mqpdbn」、「.damdzv」、「.qmdjtc」、「.mftzmxqo」、「.demffue」、「.dxjay」、「.fbuvkngy」、「.xhsphythnx」、「.dlenggrl」、「.skvtb」、「.vbdrij」、「.fprgbk」、「.ihsdj」、「.mlwzuufcg」及「.kgpvwnr」。	惡意郵件附件 惡意網頁廣告 含有惡意軟件的合法程式 利用 Apache Struts 2 漏洞 利用 Magnitude 漏洞 利用工具包入侵	Cerber V1 [解密工具連結] Magniber: 部分副檔名有解密工具。 [解密工] [解密工]
求受害者通過Tor瀏覽器購買 Cerber/My Decryptor 解密。	加密的文件目錄會有「FILES	暴力破解 Windows遠端桌面服務	部分副檔

**勒索軟件種類.**

QR code

# HKCERT 《Hong Kong Security Watch Report》 2022 Q1

## HKCERT 《香港保安觀察報告》2022年第一季度報告





# 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的社交媒体平台（例如Facebook, LinkedIn及YouTube）



**Take Action Now!**  
**立即行動！**

SUBSCRIBE

<https://www.hkcet.org/tc/form/subscribe/entry>



## 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](http://www.hkpc.org)

WFH Digital Certificate  
Security Awareness DDoS  
Malware Password Sniffing  
Virtual Hijack  
Exploitation Unencrypted QR Code  
Antispyware AI Frauds  
Direct attack Webinar  
Hacker IP Address Data Breach  
Data Breach HTTPS  
Robotics

**Information Security** Web Meeting  
Remote Work Distance Learning Social networking  
**HKCERT** Cyberspace Automatic updates  
Digital Transformation Network Blacklist Phishing  
Cybercrime Sensitive Information Confidentiality  
Data Leakage System Overload Extortion Data protection  
Vulnerabilities Trojan Virus Backdoor Internet Authentication  
Backdoor Digital copyrights Keystrokes Activity Monitoring  
BYOD Cloud Computing Data Loss Prevention  
Browsing Webmail Ransomware  
Spear Phishing Multi-layer Privacy Identity check Online Shopping  
Cloud Sharing Firewalls Clickjacking  
Cyber Attack Ransomware