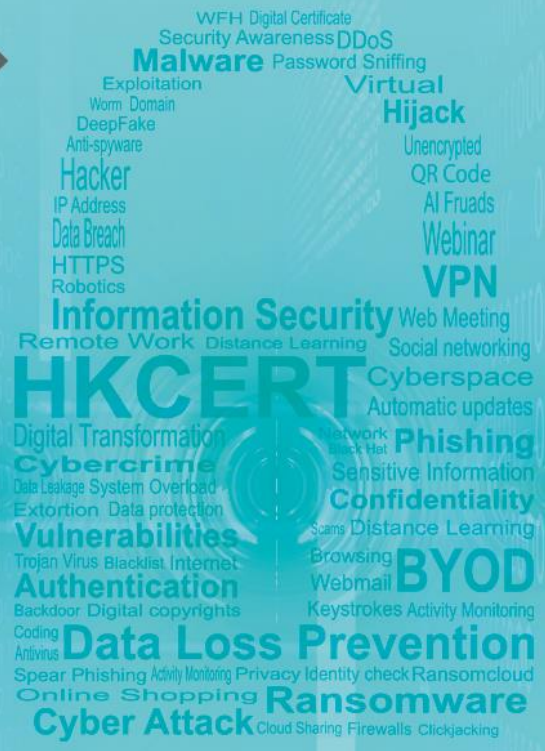
Hong Kong Computer
Emergency Response Team
Coordination Centre
HKCERT 香港網絡安全事故協調中心

# 香港保安觀察報告
# 2024 第三季度

發佈日期: 2024年10月



# 前言

## 提升資訊保安由認知做起

現今，有很多具備上網功能的數碼設備( 例如個人電腦、智能手機、平板裝置等 )，在用戶不知情下被入侵，令儲存在這些設備內的數據，每天要面對被盜取和洩漏，甚至可能被用於進行不同形式的犯罪活動的風險。

《香港保安觀察報告》旨在提高公眾對香港被入侵系統狀況的認知，從而作出更好的資訊保安選擇。這份季度報告提供的數據聚焦在被發現曾經遭受或參與各類型網絡攻擊活動（包括網頁塗改、釣魚網站、殭屍電腦等)的香港系統，其定義為處於香港網絡內，或其主機名稱的頂級域名是「.hk」或「. 香港」的系統。報告亦會回顧該季度所發生的重大保安事件及探討熱門保安議題，並提出易於執行的保安建議，提升公眾的資訊保安認知的水平，增強應對有關風險的能力。

## 善用全球保安資訊力量

本報告是香港電腦保安事故協調中心（HKCERT）和全球各地資訊保安研究人員共同合作的成果。很多資訊保安研究人員具有偵測針對他們或其客戶攻擊的能力，有些會把攻擊來源的可疑IP地址或惡意活動網絡連結的數據資料收集起來，並提供給其他資訊保安機構，以改善互聯網的整體保安。他們會遵守良好的作業守則，在分享數據前，先刪除個人身份資料。

HKCERT 建立Information Feed Analysis System (IFAS) 系統，收集和匯聚這些數據，對有關香港的資料進行分析。數據的來源廣泛和可靠，可以持平地反映香港資訊保安情況。

HKCERT會移除來自多個數據來源的重複報告，並以下面的統計指標來確保統計數據的質量。

| 網絡攻擊類型 | 統計指標 |
|---|---|
| 網頁塗改、釣魚網站 | 在本報告所述期間，錄得有關的單一網址的數量 |
| 殭屍電腦 | 在本報告所述期間，錄得各個殭屍網絡在季度內的同日單一IP 地址數量的最高值的總和 |

以下是IFAS資料的來源:

| 網絡攻擊類型 | 資料來源 | 開始使用 |
|---|---|---|
| 網頁塗改 | Zone – H | 2013-04 |
| 釣魚網站 | CleanMX – Phishing | 2013-04 |
| 釣魚網站 | Phishtank | 2013-04 |
| 殭屍電腦 | Shadowserver - microso _sinkhole_events | 2021-06 |
| 殭屍電腦 | Shadowserver - microso _sinkhole_http_events | 2021-06 |
| 殭屍電腦 | Shadowserver - sinkhole_http_events | 2021-06 |
| 殭屍電腦 | Shadowserver - sinkhole_events | 2021-06 |
| 殭屍電腦 | Shadowserver - honeypot_darknet_events | 2021-06 |

本中心採用以下方法去識別網絡的地理位置是否在香港。

| 方法名稱 | 開始使用 | 最後更新 |
|---|---|---|
| Maxmind | 2013-04 | 2024-10 |

## 更好的資訊帶來更好的服務

HKCERT將來會加入更多有價值的數據來源以進行更深入的分析，持續改善報告內容，亦會探討如何最有效利用這些數據提升 HKCERT 的服務。請發送電郵至*hkcert@hkcert.org* 反饋閣下的意見。

## 報告的局限

本報告的數據來自多個途徑，他們有不同的來源、收集週期和表達方式，各自亦存有局限，因此數據只宜作為參考，不宜用作直接比較或視為反映現實的全貌。

## 免責聲明

本中心可隨時更新或修正報告，恕不另行通知。對於本報告內容及數據中出現的任何錯誤、偏頗、疏漏或延誤，或據此而採取之任何行動，本中心概不負上任何責任。對於因使用本報告內容及數據而產生的任何特殊的、附帶或相應的損失，本中心概不負上任何責任。

## 授權條款

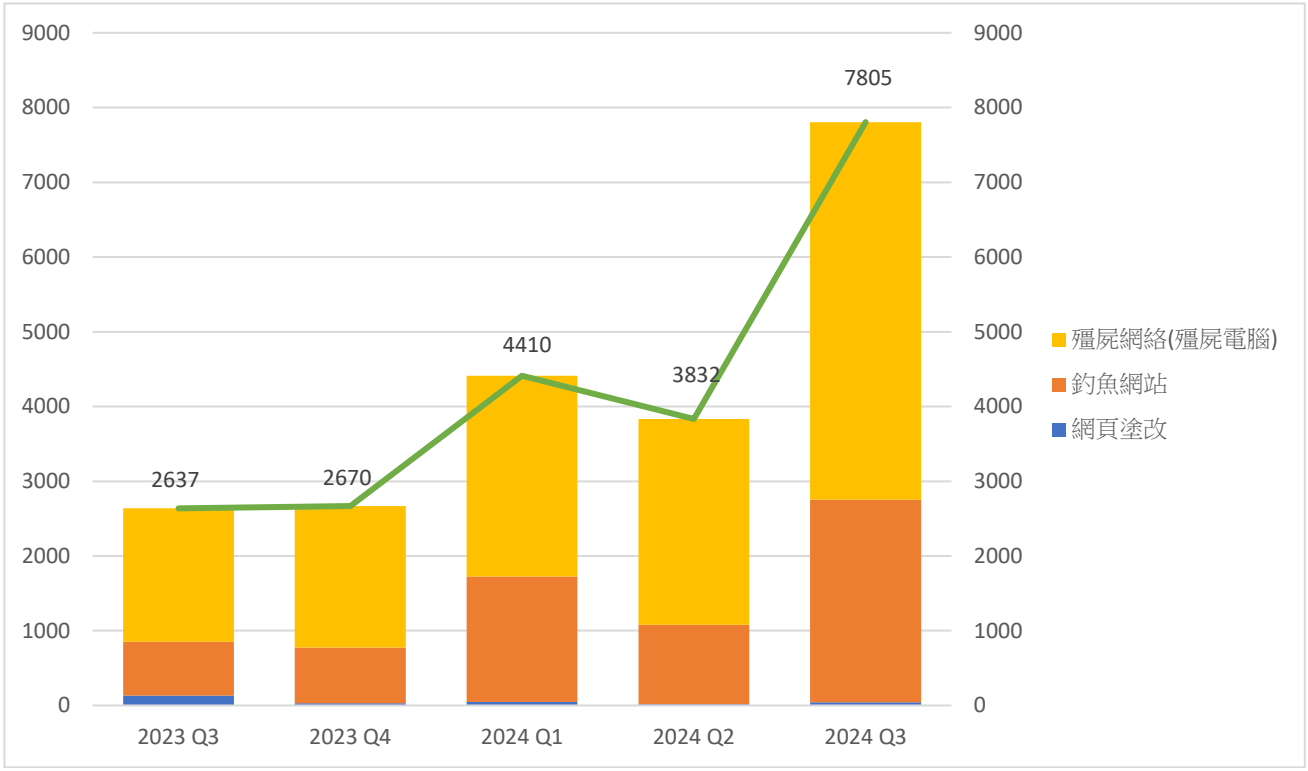
# 2024 第三季度報告概要

涉及香港的單一網絡保安事件宗數

**7,805**

按季上升

**103.6%↑**




| 事件類別 | 2023 Q3 | 2023 Q4 | 2024 Q1 | 2024 Q2 | 2024 Q3 | 按季 |
|---|---|---|---|---|---|---|
| 網頁塗改 | 132 | 31 | 46 | 18 | 42 | +133.3% |
| 釣魚網站 | 722 | 742 | 1,682 | 1,060 | 2,712 | +155.8% |
| 殭屍網絡(殭屍電腦) | 1,783 | 1,897 | 2,682 | 2,754 | 5,051 | +83.4% |
| 總數 | 2,637 | 2,670 | 4,410 | 3,832 | 7,805 | +103.6% |

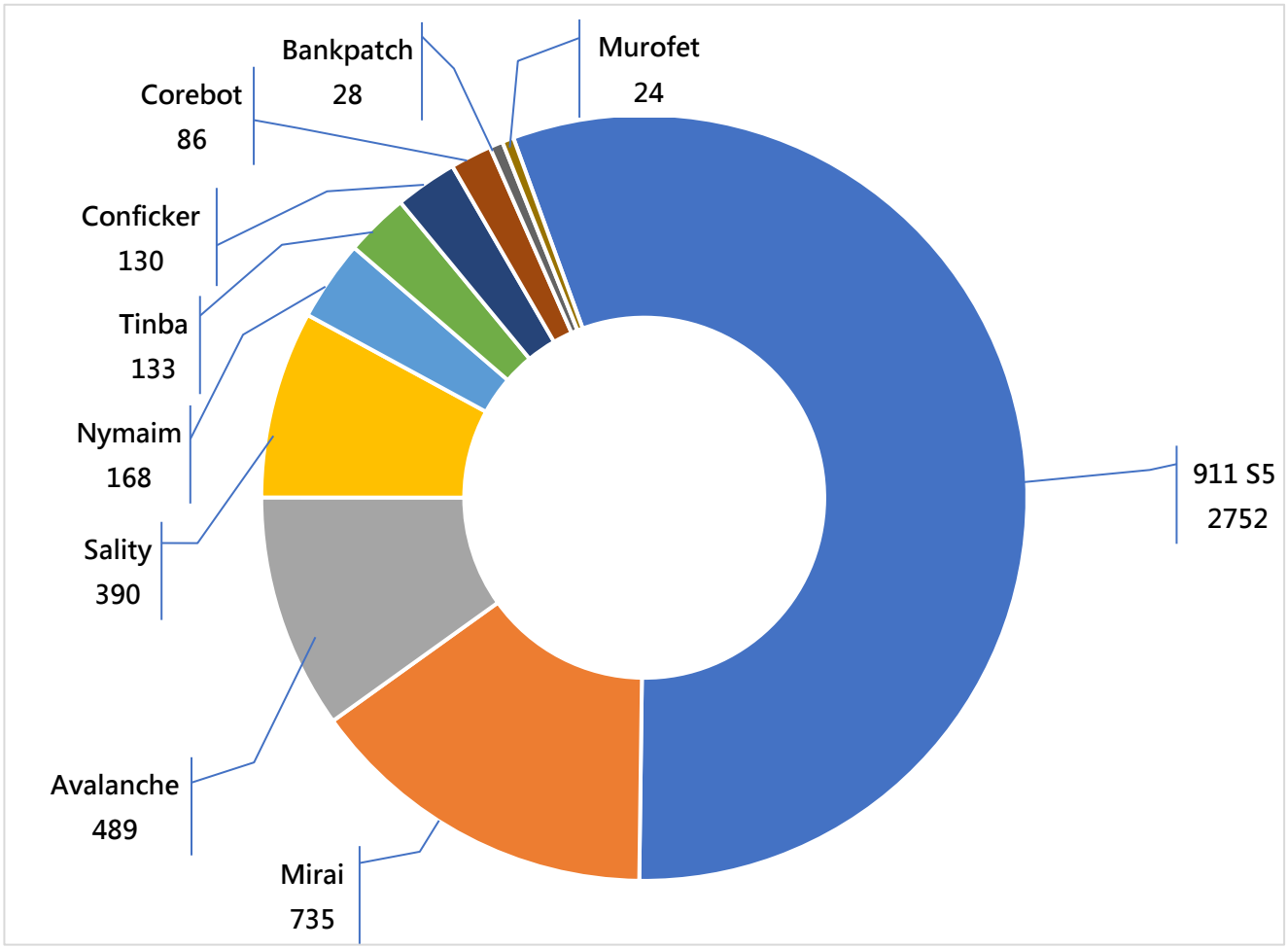
# 香港網絡內的主要殭屍網絡

911 S5
2,752
New

Mirai
735
11.3%

| | | |
|---|---|---|
| Avalanche | 489 | -23.2% |
| Sality | 390 | -26.7% |
| Nymaim | 168 | -29.1% |
| Tinba | 133 | +10.8% |
| Conficker | 130 | -22.6% |
| Corebot | 86 | +68.6% |
| Bankpatch | 28 | -17.6% |
| Murofet | 24 | -17.2% |

111




** 主要殭屍網絡指在報告時間內，透過資訊來源有可觀及持續穩定的數據。殭屍網絡的規模是計算在報告時間內，每天嘗試連接到殭屍網絡的單一IP地址總數的最大值。換言之，由於不是所有殭屍電腦都會在同一天開機，因此殭屍網絡的實際規模應該比以上的數字更大。*

# 殭屍網絡 911 S5

殭屍網絡個案在本港第三季錄得驚人增長，其中超過一半的個案是感染了911 S5病毒。根據HKCERT的威脅情報顯示，首宗報告於2024年5月錄得，源於美國司法部的一次聯合行動成功摧毀了911 S5殭屍網絡的基礎設施，並釋出受感染設備的資訊。本報告所引用的 shadowserver數據源，亦於2024年6月開始提供有關情報。

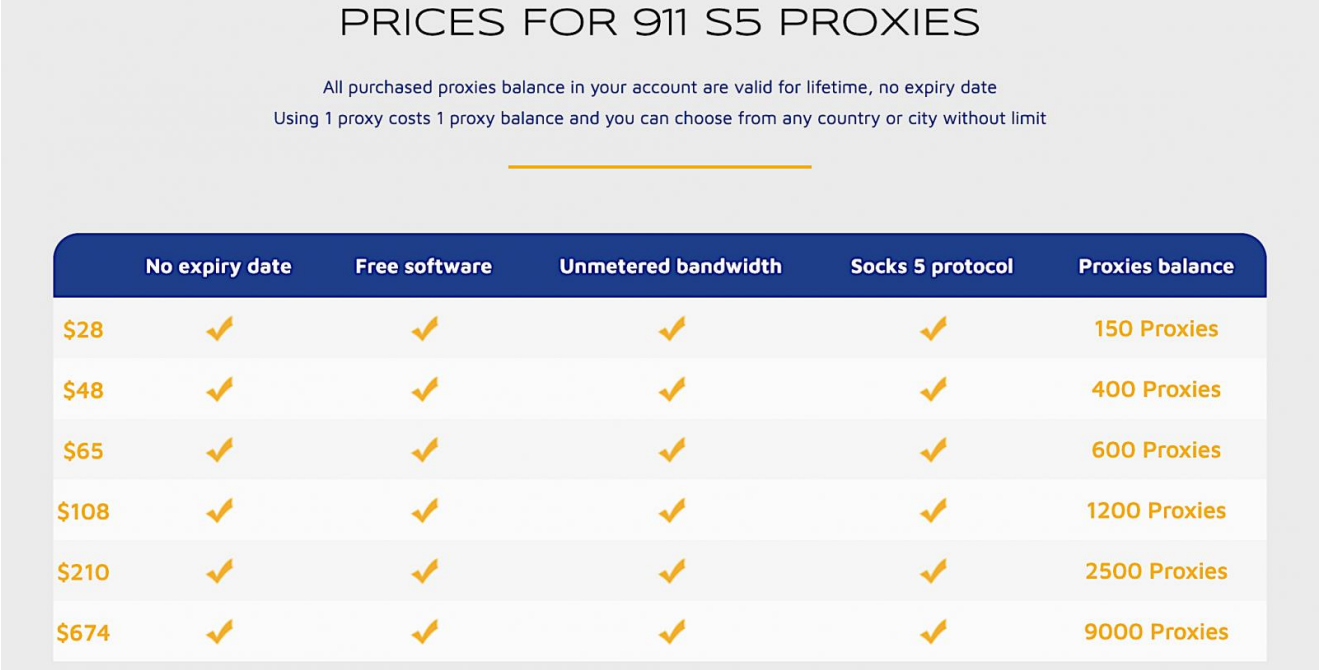
## 什麼是911 S5?

美國司法部於2024年5月宣布成功摧毀「911 S5」殭屍網絡。「911 S5」自2014年開始運作，並於2023年10月更名為CloudRouter，感染了超過1,900萬個IP地址，遍及全球190多個國家。隨著「911 S5」的瓦解，受感染設備的資訊陸續被公開。至於香港方面，HKCERT觀察到2024年第三季有超過2,000個IP地址曾受到「911 S5」的感染。


## 911 S5 / CloudRouter 分析

「911 S5 」透過在 VPN 應用程式中內建惡意後門，使受感染的裝置能被非法存取。這些 VPN 通常被植入到盜版遊戲或軟件中。當受害者下載這些遊戲或軟件後，VPN 應用程式和後門會在未經同意的情況下悄然安裝，讓裝置不知不覺成為 「911 S5 」殭屍網絡的一部分。與「911 S5 」網絡連接的 VPN 應用程式包括：MaskVPN、DewVPN、PaladinVPN、ProxyGate、ShieldVPN 和 ShineVPN。

「911 S5 」殭屍網絡為犯罪分子提供代理服務，通過出租受感染裝置的存取權限，讓犯罪分子可以隱藏自己的網絡足跡，使其活動看似來自受害者的裝置，從而進行各種網絡犯罪活動，例如金融詐騙等。



PRICES FOR 911 S5 PROXIES

All purchased proxies balance in your account are valid for lifetime, no expiry date
Using 1 proxy costs 1 proxy balance and you can choose from any country or city without limit

| | No expiry date | Free software | Unmetered bandwidth | Socks 5 protocol | Proxies balance |
|---|---|---|---|---|---|
| $28 | ✓ | ✓ | ✓ | ✓ | 150 Proxies |
| $48 | ✓ | ✓ | ✓ | ✓ | 400 Proxies |
| $65 | ✓ | ✓ | ✓ | ✓ | 600 Proxies |
| $108 | ✓ | ✓ | ✓ | ✓ | 1200 Proxies |
| $210 | ✓ | ✓ | ✓ | ✓ | 2500 Proxies |
| $674 | ✓ | ✓ | ✓ | ✓ | 9000 Proxies |

911 S5 proxy service prices (BleepingComputer)

## 如何移除「911 S5 」

即使「911 S5」殭屍網絡已經被搗破，受感染設備仍存在網絡安全風險，因此需要立即移除與「911 S5」相關的 VPN 應用程式。以下是美國 FBI 提供的檢查和移除步驟：

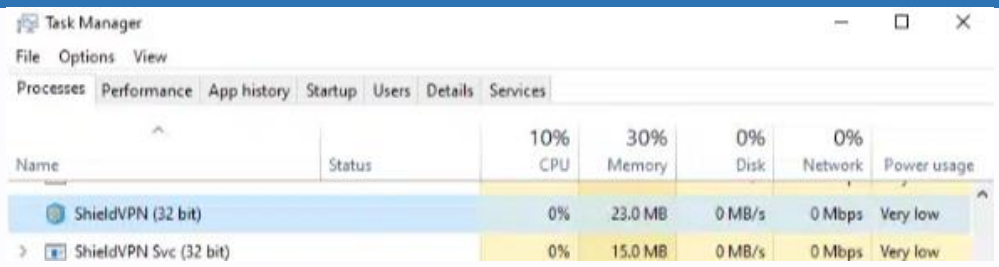
**只提供英文版本**

1. Press **Control+Alt+Delete** on the keyboard and select the "**Task Manager**" option or right-click on the **Start menu (Windows icon)** and select the "**Task Manager**" option.

2. Task Manager should now be running. Under the "**Process**" tab, look for the following:
   - **MaskVPN (mask_svc.exe)**
   - **DewVPN (dew_svc.exe)**
   - **PaladinVPN (pldsvc.exe)**
   - **ProxyGate (proxygate.exe, cloud.exe)**
   - **ShieldVPN (shieldsvc.exe)**
   - **ShineVPN (shsvc.exe)**

   Example of running processes for **ShieldVPN** and **ShieldVPN Svc**:

## 只提供英文版本

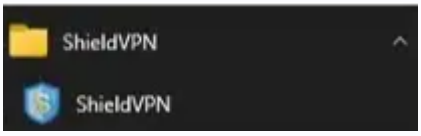



If Task Manager doesn't detect any of these services, verify that by searching the Start menu for any traces of software labeled as "**MaskVPN**," "**DewVPN**," "**ShieldVPN**," "**PaladinVPN**," "**ProxyGate**," or "**ShineVPN**."

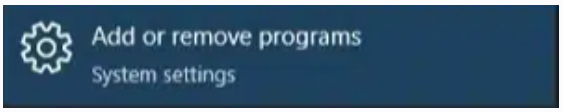
3. Click on the "**Start**" **(Windows Icon)** button typically found in the lower lefthand corner of the screen. Then, search for the following terms, which are the identified names of the malicious software applications:
   - **MaskVPN**
   - **DewVPN**
   - **ShieldVPN**
   - **PaladinVPN**
   - **ShineVPN**
   - **ProxyGate**



4. If one of the VPN applications is found, an **uninstaller** is sometimes located under the Start menu option of the VPN application. **The example image below shows an instance where the uninstall option isn't available.**

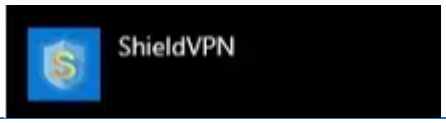



5. If the application **doesn't contain an uninstall option**, then follow the steps below to attempt to uninstall the application:
   a. Click on the **Start menu (Windows button)** and type "**Add or remove programs**" to bring up the "**Add and Remove Programs**" menu.



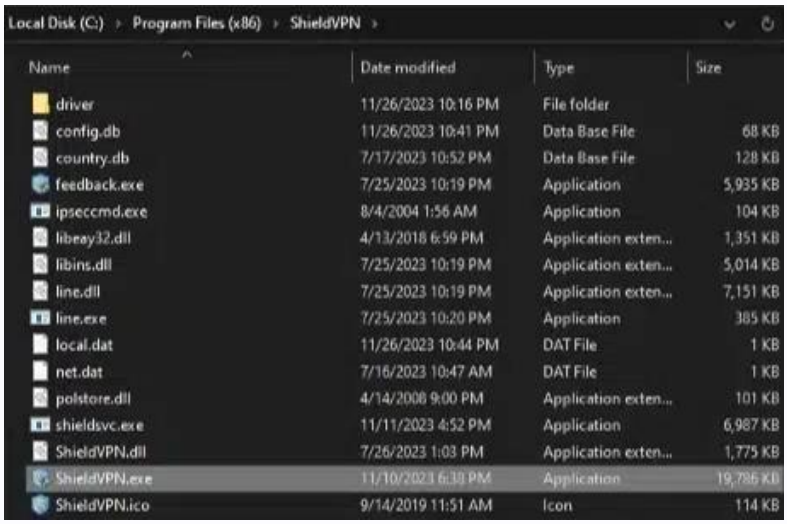

   b. Search for the **malicious software application names**.

   An example image below shows the **ShieldVPN** application found within the "**Add or remove programs**" application list. Once you find the application in the list, click on the application name and select the "**Uninstall**" option.



## 只提供英文版本

c. After the application is uninstalled, you can try to verify that the application has been removed by clicking on "**Start**" **(Windows Icon)** and typing "**File Explorer**."
d. Click on the drive letter "**C:**"—sometimes labeled as "**Windows (C:)**"—and navigate to "**Program Files(x86)**." Then, look for the malicious software application names in the list of files and folders.




e. For **ProxyGate**, navigate to "**C:\users\[Userprofile]\AppData\Roaming\ProxyGate**."
f. If you don't see any folder labeled "**MaskVPN**," "**DewVPN**," "**ShineVPN**," "**ShieldVPN**," "**PaladinVPN**," or "**Proxygate**," then this particular malicious software application may not be installed.
g. If a service was found running, but not found under the **Start menu** or "**Add and Remove Programs**," then:
   i) Navigate to the directories described in directions **5d** and **5e**.
   ii) Open "**Task Manager**."
   iii) Select the service related to one of the identified malicious software applications running in the **process** tab.
   iv) Select the option "**End task**" to attempt to stop the process from running.
h. Right-click on the folder named "**MaskVPN**," "**DewVPN**," "**ShineVPN**," "**ShieldVPN**," "**PaladinVPN**," or "**ProxyGate**."
i. Select the "**Delete**" option.
j. You can also select all files found within the folder and then select the "**Delete**" option.
k. If you try to delete the folder—or to delete all files located inside the folder—and receive an error message, **be sure that you've ended all processes related to the malicious software within in Windows Task Manager, as described in step 5g**.

### 參考資料:


- https://www.ic3.gov/Media/Y2024/PSA240529
- https://www.justice.gov/opa/pr/911-s5-botnet-dismantled-and-its-administrator-arrested-coordinated-international-operation
- https://www.bleepingcomputer.com/news/security/us-dismantles-911-s5-residential-proxy-botnet-used-for-cyberattacks-arrests-admin/

# 第五屆「香港網絡安全奪旗（CTF）挑戰賽2024」


香港網絡安全事故協調中心（HKCERT）及香港生產力局（HKPC）將於2024年11月舉辦第五屆「香港網絡安全奪旗（CTF）挑戰賽2024」。這是本港數一數二的大型網絡安全比賽之一，旨在喚起香港市民的網絡安全意識，提升參賽者的網絡攻防能力，以滿足業界對未來技術人才的需求。 比賽詳情請訪問CTF 2024官網。

## 比賽亮點：

### 對於機構、公司、或企業：

- 增强員工網安意識及參與度：參賽過程中，員工將深入了解網安的重要性，提升安全意識及防範能力，幫助機構、公司、或企業在日益複雜的網絡環境中更有效地保護數據安全，應對潛在的安全威脅。
- 提升公司聲譽及業界知名度： 參加此類大型比賽可提升機構、公司、或企業的知名度，獲得業界的認可，增強企業在網安領域的聲譽。

### 對於個人：

- 網安實戰經驗：參賽者將置身於真實的網絡攻防環境，親自體驗如何識別和利用安全漏洞，提升攻防及實戰技能。對於業內人士，它可以評估您的網絡攻防技術，並在遊戲化的場景中學習新技術，實踐查找漏洞的知識。

- 專業能力提升：比賽涵蓋網頁安全、密碼學、鑑證、及逆向工程等技能，並提供多場工作坊及分享會，為您提供專業指導及前沿的網安資訊，這些都是未來空缺的網安職位（如網安分析員、滲透測試員、道德黑客、紅隊攻擊手等）所需的核心技能。
- 增强職業履歷：參賽者將有機會深入了解網安世界，探索更多職業選擇。另外，每名參賽者均可獲得電子證書，以此展示在網絡安全領域的興趣和能力，增强職業履歷。
- 獎品與業界認可：獎品額度高達港幣15,000元；獲得金、銀、銅獎不僅會獲得業界的認可，亦會有益於未來職業生涯發展。
- 人脈與視野拓展：比賽吸引了來自不同國家的專業人士和技術愛好者，通過訪問我們的Discord交流平台或參加現場決賽，您將有機會結識行業專家和志同道合的朋友，並拓展國際視野。業內人士亦可參加世界各地不同的「道德黑客」社群，鑽研網絡保安，成為該領域的專家。

## 比賽時間線

- 報名截止日期：2024年11月4日
- 初賽：2024年11月8-11月10日（48小时綫上作賽）
- 決賽：2025年1月20-21日（1.5日日間作賽）
- 頒獎典禮：2025年1月21日（緊貼決賽完結）

詳細資料可參閱HKCERT CTF官網
https://ctf.hkcert.org/zh/index.html

# 勒索軟件的新陣線 揭露香港面臨的最新威脅


## 勒索軟件入侵途徑

近幾個月來，香港的勒索軟件攻擊事件激增，多宗事件擾亂了各行各業的企業和機構。攻擊者部署了一系列複雜的攻擊負載，滲透目標系統。香港網絡安全事故協調中心（HKCERT）分析了這些事件，並識別出目前勒索軟件的入侵途徑，現概述如下：

- 釣魚電郵：傳送勒索軟件有效負載的惡意附件或連結。
- 遠端桌面協定(RDP)漏洞：利用薄弱或受損的RDP憑證。
- 漏洞利用：攻擊者通常利用軟件、資料庫和中介軟件中未修補的漏洞。
- 偷渡式下載：透過受損或惡意網站發起的惡意下載。
- 惡意廣告：導致勒索軟件下載的惡意廣告。
- 供應鏈攻擊：破壞第三方供應商以存取目標。
- 暴力攻擊：猜測密碼以取得存取權限。
- 利用設定錯誤的服務：透過錯誤配置的網路服務取得存取權。
- 社會工程：操縱個人以取得存取權限或憑證。

## 勒索軟件攻擊的最新發展

香港網絡安全事故協調中心（HKCERT）在全面分析及近期研究勒索軟件事件後，發現勒索軟件攻擊的演變出現重大轉變。網絡罪犯不但採用新興的攻擊手法，對勒索軟件的部署方法也有新的理解。

- 勒索軟件即服務（RaaS）：越來越常使用RaaS平台，讓較不複雜的攻擊者也能使用勒索軟件（如REvil、DarkSide、LockBit）。
- 多重勒索：一種進階勒索軟件策略，攻擊者利用三種方法進行脅迫。
- 加密資料：鎖定檔案並要求支付解密金鑰。
- 資料竊取和公開發布：竊取資料並威脅如果不支付贖金就公開發布資料。
- DDoS攻擊：對受害者的基礎設施發動分散式阻斷服務（DDoS）攻擊，進一步向受害者施壓，迫使其支付贖金。
- 人工智慧和機器學習：利用人工智慧自動化和增強攻擊策略，提高攻擊效率。
- 漏洞利用：越來越多地利用漏洞繞過傳統安全措施（如CVE-2020-0796、CVE-2021-34527、EternalBlue）。
- 加密創新：攻擊者使用先進的加密技術，在不支付贖金的情況下增加解密難度。

## 預防建議

總而言之，2024 年香港面臨的勒索軟件威脅凸顯出攻擊的廣泛性和多樣性。從公共部門到私人企業，很少有部門能夠免受這些有組織的勒索軟件事件的影響。為了有效應對這些威脅，一般使用者和企業使用者需要加強意識並採取合適的網路安全策略。 HKCERT建議使用者保持警覺並採取適當的保護措施。

### 普通用戶

- 謹慎處理電郵：避免開啟來歷不明或可疑的電郵或附件。在點擊任何鏈接或下載附件前，應核實發件人的電郵地址。
- 使用強密碼：為所有帳號建立強大、獨特的密碼。例如，避免使用生日或常用字等容易猜到的資訊。

## 企業用戶

- 多因素身份驗證（MFA）：對所有帳戶，尤其是具有管理權限的帳戶，實施多因素身份驗證，以增加一層額外的安全防護。
- 風險管理：確保定期更新所有系統和軟件並打補丁，以防範已知漏洞。定期進行安全風險評估、漏洞掃描和滲透測試。
- 加強協定安全：如果不需要，停用遠端桌面協定(RDP)、遠端登入協定(Telnet)、檔案傳輸協定(FTP)等服務。使用虛擬私人網路(VPN)和強身份驗證方法限制訪問。定期進行軟件更新以修補協定服務的漏洞。
- 實施進階電子郵件安全：使用先進的電子郵件過濾和反釣魚解決方案來偵測和阻止惡意電子郵件，然後定期進行釣魚模擬演習來培訓員工。
- 部署端點偵測和回應（EDR）：啟用EDR實時監控和自動化反應措施，偵測包括惡意軟件在內的異常行為。 在所有端點安裝EDR，並根據威脅情報配置合理的檢測策略，在很大程度上提高對勒索軟件攻擊的偵測率，縮短回應時間，減少勒索軟件攻擊造成的損失。
- 網路分割：隔離關鍵系統和數據，限制勒索軟件的傳播。使用防火牆和存取控制來實施網路分割非常重要。
- 數據的加密存儲與數據備份及復原：加密敏感資料以確保其安全性並實施適當的存取控制、身份驗證和授權。定義明確的數據保留期限，並定期進行資料清理。對於重要數據，應定期保存離線備份，並建立必要的測試備份和復原程序，確保資料能夠快速復原。
- 事件回應計畫與使用者訓練與認知：定期制定、更新回應計劃，定期進行以勒索軟件防範為重點的網路安全訓練。

詳細資料可參閱HKCERT保安博錄
https://www.hkcert.org/tc/blog/ransomware-s-new-front-uncovering-the-latest-threats-facing-hong-kong

# 新一代釣魚攻擊：不斷進化的網絡威脅

## 新一代釣魚攻擊的技術

### 進階釣魚電郵

有網絡保安專家指出，有近90%的網絡攻擊是從一封電郵開始，當中就不乏釣魚電郵。傳統的釣魚電郵常常偽裝成來自合法來源，例如使用相似的域名、商標和設計風格，使電郵看起來真實可信。

另外，這些電郵通常使用緊急或誘導性的語氣，要求受害者立即打開電郵中的釣魚連結或惡意附件。為了防止這些電郵流入到用戶郵箱，企業及電郵服務供應商對電郵亦會採取過濾，例如攔截含有釣魚連結或惡意附件的電郵。

若果把釣魚連結直接放在電郵內容，電郵很容易就被攔截，因為連結很輕易被過濾出來進行檢查。相反，若果把連結以其他方式隱藏或加載，大大增加釣魚電郵的存活率。

釣魚電郵開始進化，例如把釣魚連結加載到二維碼（Quishing），然後經由電郵發送。另外，他亦提及把加載後的二維碼封裝到PDF或JPG文件，或加密含有惡意二維碼的文件，可以增加釣魚電郵的生存機會。

縱使現時已有方案把電郵中的二維碼進行檢查，但有研究指出黑客可透過更改二維碼圖片的背景顏色和錯誤比例取代以往使用完整二維碼的釣魚電郵，令相關電郵保安措施更難偵測當中的二維碼。


圖片：以上圖片由Green Radar Limited提供

另一種同電郵相關的新型網絡釣魚 – 複製網路釣魚（Clone Phishing），例如黑客透過複製帶有附件真實電郵，再假冒原始寄件者重新發送，但當中的連結或附件更換成釣魚連結或惡意程式。

## 多重轉跳

不法分子開始不再直接發送釣魚連結，而是發送一些他們即時通訊軟件頻道的連接，引導用戶到他們的頻道展開對話。由於這些連接都是合法，所以基本上是可以通過所有網絡安全措施。當在頻道展開對話時，他們就會發送惡意連結，誘導用戶按下連結。

## 深偽詐騙(Deepfake Scams)

隨著人工智能的迅速發展，深偽技術開始進入「平民化」，互聯網亦出現網上平台讓用戶體驗深偽技術，解決了高運算力的要求，而且所需的訓練素材亦因應技術成熟而減少。

外國一項調查報告，Egress-Email Security Risk 2024，有63%受訪的資訊安全從業員非常擔憂深偽技術帶來的網絡攻擊。為應對攻擊，互聯網出現深偽檢測工具，當中不乏由大型網絡安全供應商開發。一項外國研究指出由人工智能生成的合成照都會殘留人眼看不見的獨特痕跡。透過偵測這些痕跡，可以判別圖片是否由人工智能生成。同時，研究亦指出痕跡會因應人工智能模型有所差異，導致偵測工具難以對所有模型都有效用。

深偽技術亦為社交平台帶來困擾，因為深偽可以生成逼真的音頻及視訊內容，阻礙我們對網絡資訊的判斷。現時社交平台Meta、抖音及小紅書紛紛利用AI來標記由AI生成的內容來提醒用戶。

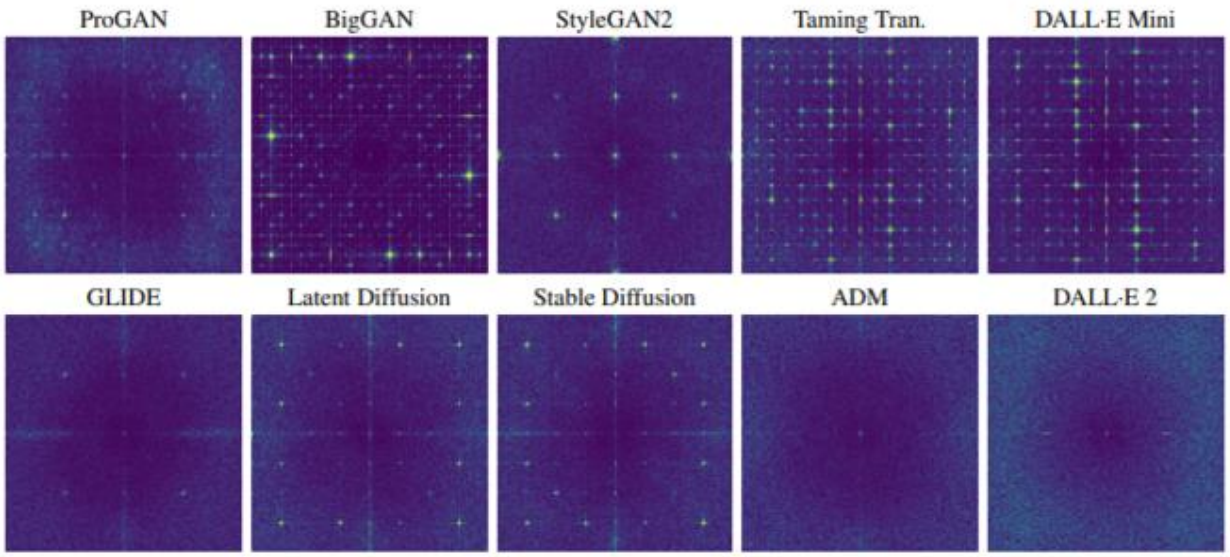



**Fig. 2:** Fourier transform (amplitude) of the artificial fingerprint estimated from 1000 image residuals. Top row: from left to right ProGAN [20], BigGan [21], StyleGAN2 [22], Taming Transformers [23], DALL·E Mini [24]. Bottom row: GLIDE [5], Latent Diffusion [25], Stable Diffusion [4], ADM [26], DALL·E 2 [3]

**HKCERT過去亦刊登過多篇文章分析深偽的保安風險，提及過深偽技術、過往發生的真實例子，以及預防的建議。詳情請參閱文章「人工智能武器化：網絡安全新領域」、「深度偽造：有圖未必有真相」及「人工智能與網絡保安」。**

## 釣魚攻擊結及搜尋引擎行銷（Search Engine Marketing，簡稱SEM）

**搜尋引擎行銷的原意是透過向搜尋引擎支付廣告費用，讓網站可以在相關的搜尋查詢獲得更佳的搜尋結果，而搜尋結果往往高於自然搜尋結果 (Organic Search)。例如，在Google進行搜尋時，會先出現廣告 (網站被標示為贊助)，接著才出現自然搜尋結果。不幸的是，不法分子亦利用搜尋引擎行銷為釣魚網站爭取更佳搜尋結果排名。**

**2023年，即時通訊軟件平台WhatsApp網頁版被人假冒，並利用搜尋引擎行銷成功置頂。當有人使用" WhatsApp網頁版" 等關鍵字，就會搜尋到相關假冒網站。當時有不少香港市民因此WhatsApp帳號被騎劫。**

**2024年1月，一間知名Pizza餐廳網站被同樣手法假冒，有市民被盜用信用卡。**


圖片：星島

## 社交平台上的釣魚攻擊

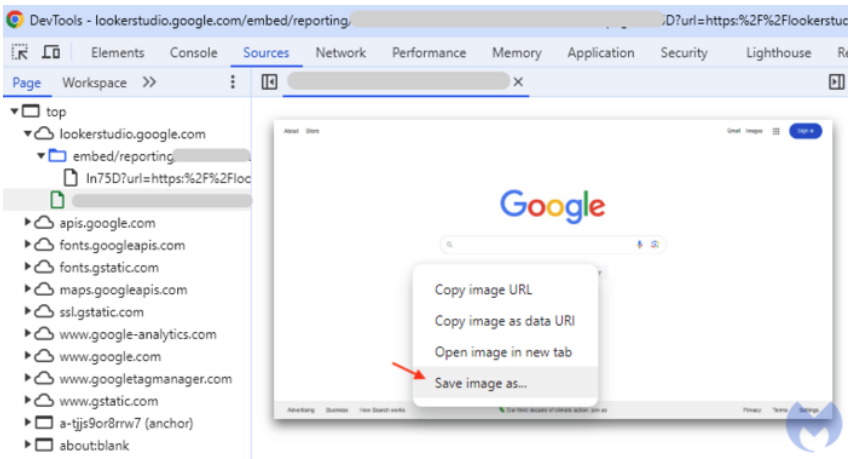
**HKCERT亦發現釣魚攻擊開始延伸到去社交平台，假冒公司專頁，例如2023年一間旅行社公司Facebook專頁被多次假冒。HKCERT在「在節慶期間採取網絡保安最佳實踐」文章中提出過幾點假冒專頁的特徵.**

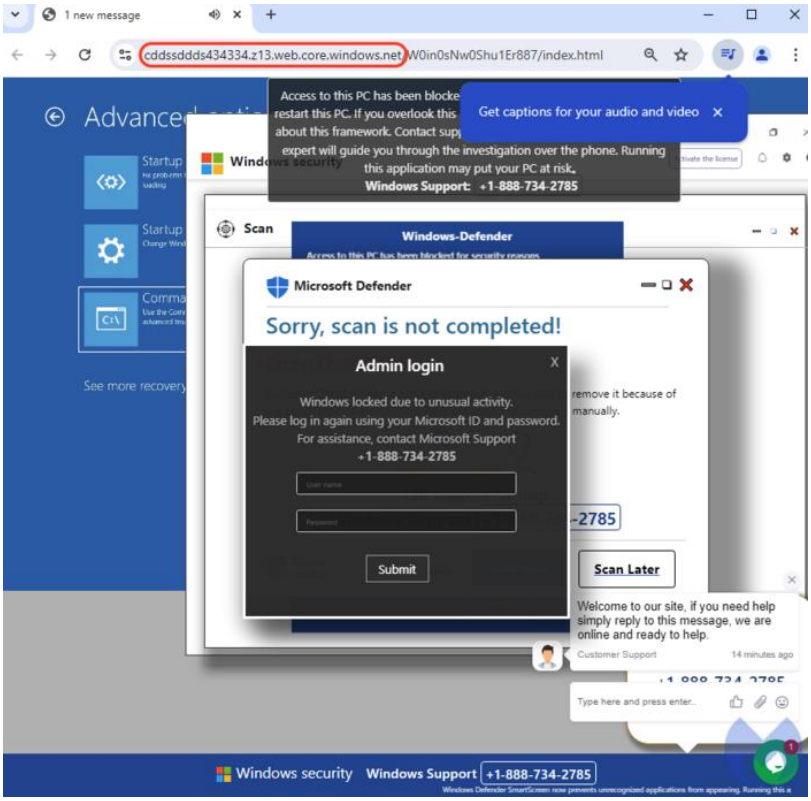
## 假冒客服

近期，WeChat微信「假冒客服」騙案升幅驚人。騙徒假冒WeChat通過短訊 (SMS) 聲稱你之前購買的保險期限已過，如果不取消將自動扣費。短訊附有一個「假冒客服」的網站連接或電話號碼，誘導你聯繫他們。典型詐騙過程例子

1. 收到短訊：短訊內容提到自動扣費，造成恐慌。
2. 點擊鏈接：進入假冒網站，指示你聯繫在線客服。
3. 撥打電話：點擊後自動撥打電話聯繫假冒客服。
4. 增加可信性：假冒客服會指導你開啟微信App內的所謂「官方授權書」。
5. 套取信息：假冒客服以取消續保為藉口，誘導你提供銀行或信用卡資料及密碼。
6. 盜取資金：騙徒利用獲取的信息轉走賬戶存款或盜用信用卡。

WeChat「假冒客服」騙案不斷演變，衍生出不同的詐騙手法。有部分騙案更以WhatsApp、WeChat即時通訊或Cold Call進行類似詐騙，市民需要密切留意最新手法。
除了WeChat假冒客服，國外也發現有不法分子假冒Microsoft和Apple技術支援的詐騙案件。不法分子架設釣魚網站後，濫用 Google工具來制作假頁面，冒充一系列Google產品，再利用搜尋引擎廣告功能，將這些網站置頂。只要在搜尋引擎中搜索“google {產品名稱}”（例如：google Translate），這些網站就會出現在搜尋結果的前幾位。
當用戶點擊這些連結時，會被帶到一個看似google.com的頁面，但實際上這只是一張載有惡意連結的google.com頁面圖片。只要用戶點擊圖片，螢幕就會彈出一個提示電腦出現問題並要求用戶聯絡Microsoft或Apple技術支援的視窗，並進入全螢幕模式。一旦用戶聯絡假冒的技術支援，詐騙行動就開始了。






圖片：Malwarebytes

## 防範措施

### 員工教育和培訓

定期的員工教育和培訓是防範釣魚攻擊的首要措施。企業應該組織釣魚模擬測試，讓員工在實際操作中學習如何識別釣魚訊息。HKCERT在網站提供許多培訓素材，就釣魚攻擊亦開設主題專頁，教導市民分辨及防範釣魚攻擊，詳情請參閱「網絡釣魚 全城防禦」。

### 多重身份驗證（Multi-Factor Authentication, MFA）

實施多重身份驗證可以顯著增加攻擊者獲取帳戶控制權的難度，即使密碼被洩露，仍需通過其他驗證步驟才能登錄。

### 電郵過濾

配備電郵過濾系統，過濾可疑的釣魚訊息，可以在訊息到達收件人之前將其攔截。

### 制定網絡保安事故應變計劃

企業應該制定詳細的網絡保安事故應變計劃，一旦發現釣魚攻擊，能迅速採取措施減少損失。這包括做好定期數據備份、確保溝通渠道暢通以及明確各部門的應對角色和職責。HKCERT亦為企業制定過一份保安事故應變指南，概述在保安事故發生之前、期間和之後要採取的行動，

詳情可參閱「中小企保安事故應變指南」。

## 定期安全審計

定期進行安全審計，識別並修補可能存在的安全漏洞。審計過程中應包括模擬釣魚攻擊，以測試企業現有的防禦措施是否有效。

## 安裝防毒軟件

安裝防毒軟件以防範釣魚攻擊。同時，可以使用「CyberDefender 守網者」的「防騙視伏器」，通過檢查電郵地址、網址和IP地址等，來辨識詐騙及網絡陷阱

## 結論

新一代釣魚攻擊對個人和企業構成了嚴重的威脅。透過了解這些攻擊的特點和技術，並採取有效的防範措施，我們可以降低這些攻擊帶來的風險和損失。持續的警惕、全民教育以及全面的網絡安全措施是應對新一代釣魚攻擊的關鍵。

詳細資料可參閱HKCERT保安博錄
https://www.hkcert.org/tc/blog/next-level-phishing-the-evolving-threat-landscape

香港網絡安全事故協調中心
電話：8105 6060
電郵：hkcert@hkcert.org