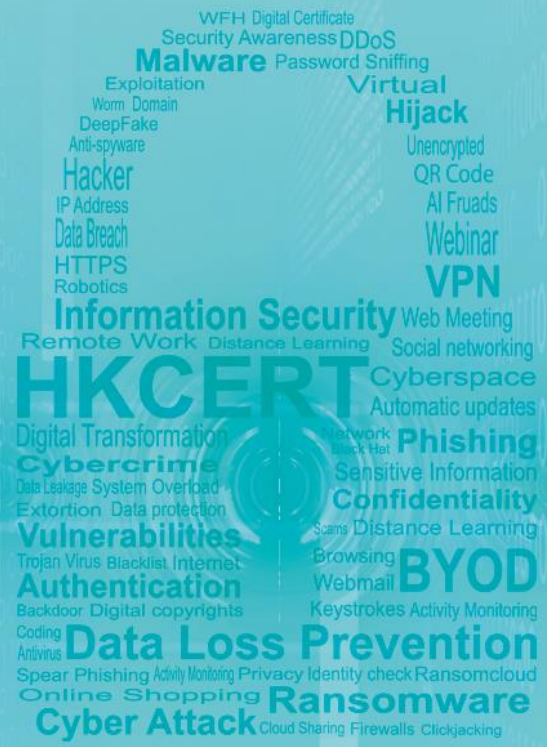
Hong Kong Computer
Emergency Response Team
Coordination Centre
HKCERT 香港電腦保安事故協調中心

香港保安觀察報告
2023 第四季度

發佈日期: 2024年2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	2023-11

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

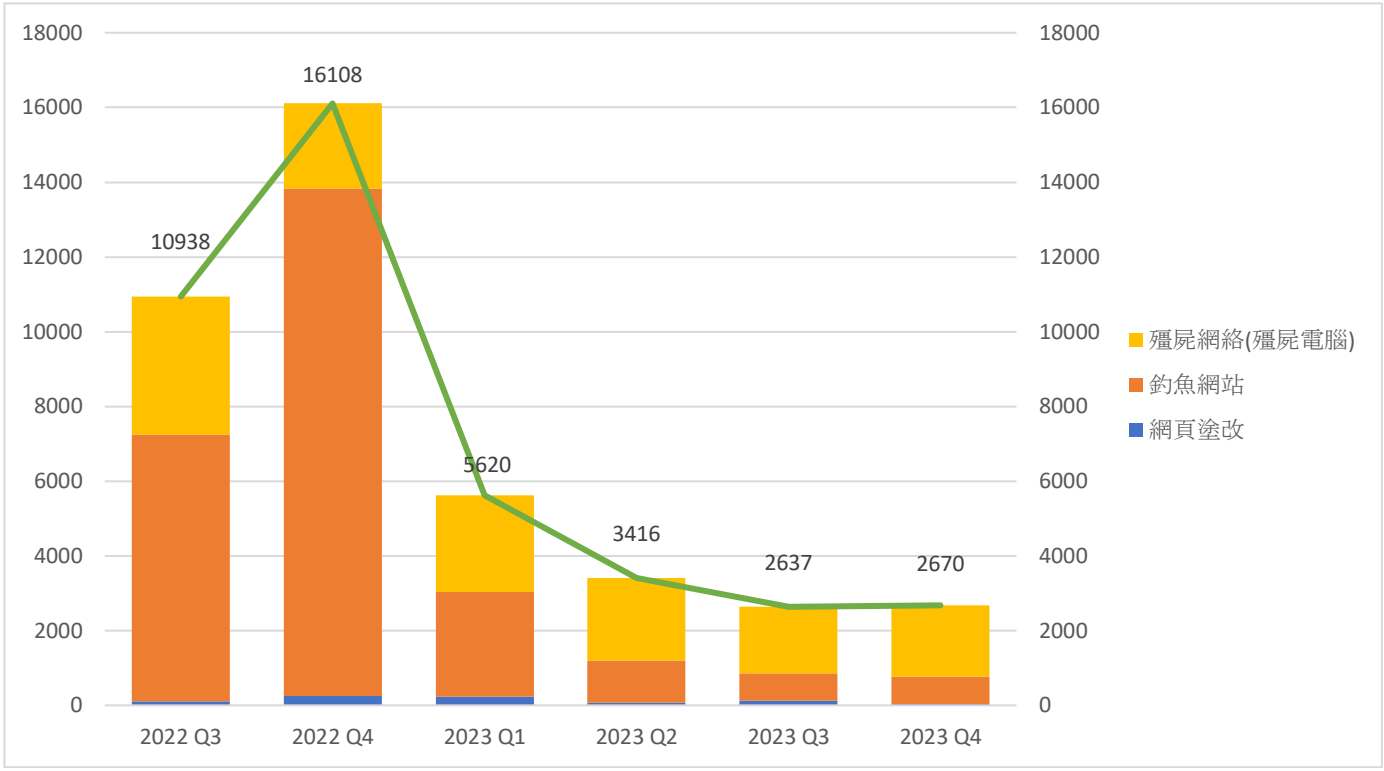
2023 第三季度報告概要

涉及香港的單一網絡保安事件宗數

2,670

按季下跌

1.3%↑

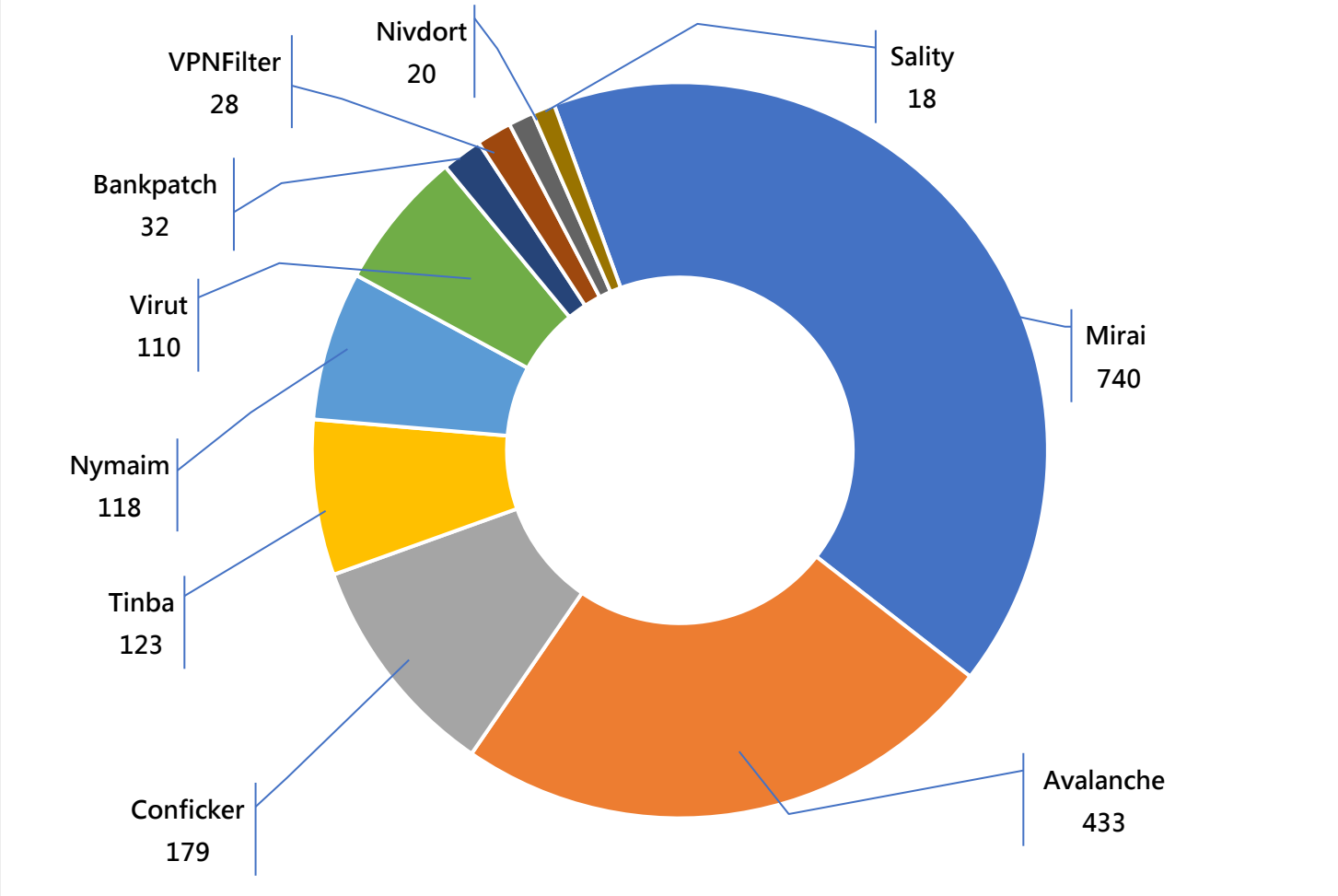


事件類別	2022 Q4	2023 Q1	2023 Q2	2023 Q3	2023 Q4	按季
網頁塗改	249	233	69	132	31	-76.5%
釣魚網站	13,574	2,804	1,120	722	742	+2.8%
殭屍網絡(殭屍電腦)	2,285	2,583	2,227	1,783	1897	+6.4%
總數	16,108	5,620	3,416	2,637	2670	+1.3%

香港網絡內的主要殭屍網絡

Mirai	740	↓25.1%
Avalanche	433	↑111.2%

Conficker	179	+1.7%
Tinba	123	+15%
Nymaim	118	+68.6%
Virut	110	+3.8%
Bankpatch	32	+113.3%
VPNFilter	28	-3.4 %
Nivdort	20	+233.3%
Sality	18	-5.3%



** 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。*

網絡攻擊按季稍微回升，公眾需警剔注意！

2023年第四季網絡事件數字正式出爐。今季網絡釣魚較上季稍微上升2.8%，而殭屍網絡 (殭屍電腦) 亦錄得6.4%上升。值得注意的是，有關數字只反映攻擊源頭寄存於香港的情況，並不包括海外。黑客若果將攻擊源頭寄存海外伺服器，但攻擊香港用戶。這類網絡攻擊並不反映在數字上面，實際數字會更高。HKCERT第四季處理的網絡保安事故同樣錄得升幅，顯示黑客活動依然活躍於香港，公眾需加緊防範。

2023年已經完結，回顧香港過去一年所發生的重大網絡攻擊事件。2023年3月至4月期間，有不分法子假冒香港公司積分計畫及電訊商，以釣魚SMS去誘騙受害人填寫敏感資料，部分受害人更遭受金錢上的損失。2023年8月至9月期間，香港有兩間公營機構的系統先後遭受黑客入侵，盜取大量敏感訊息。其中一間受害機構更遭受黑客公開勒索，要求繳交巨額贖金，否則公開竊取數據。最終，受害機構拒絕繳交贖金，黑客「撕票」洩漏內容，大量的敏感資料在「暗網」流出。市民則面對不法分子利用釣魚攻擊結及搜尋優化功能，大量假冒即時通訊軟件網頁出現，並置頂搜尋引擎結果。不少市民的即時通訊軟件帳號被騎劫。香港的網絡安全響起警號。2023年11月期間，不分法子更將釣魚攻擊伸展到社交平台，假冒本地知名品牌的專頁。有不分法子更透過社交平台的即時通訊功能散播惡意App，偷取受害人的銀行敏感訊息。

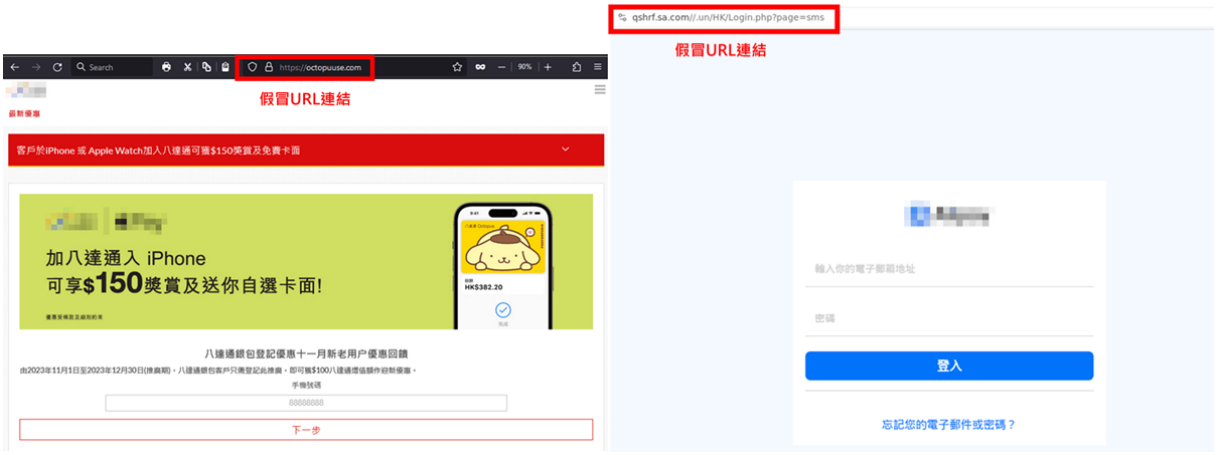
2023年在網絡安全方面也實施了不少措施。2023年2月23日往後，所有電話卡都需要向所屬電訊商進行實名登記，未完成登記則不能繼續使用。2023年12月28日，首階段「短訊發送人登記制」正式實施。電訊商、銀行及個別政府部門已經相繼參與。措施將會擴展至其他行業。兩行措施都是為了打擊電話騙案。

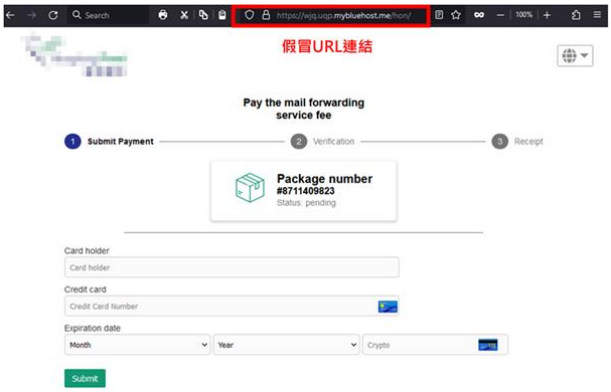
在節慶期間採取網絡保安最佳實踐

隨著網上服務越來越普及， 在享受便利的同時，我們也應就節慶期間的網路保安風險保持警惕。

釣魚攻擊

除了購買商品作為節日禮物外，大家還可以在網上支付旅行費用，以從互聯網上領取機票和酒店的優惠和折扣。黑客亦會把握這個機會對網路用戶發動攻擊。從黑客的角度而言並與其他類型的網路攻擊相比，發動釣魚攻擊是一種較低成本且省力的方法。由於黑客製作釣魚內容與目標的官方網站非常相似亦不易辨別的釣魚內容，大家在日常情況下容易受騙和墮入釣魚攻擊陷阱。 黑客透過發送釣魚訊息或電郵來誘騙目標用戶打開惡意URL連結，甚至是可能包含惡意軟體的附件。據觀察，最近黑客針對香港用戶而創建一些冒充本地會員平台的釣魚網站。他們會欺騙用戶在釣魚網站上輸入登入資訊，並在成功登入後從帳戶中竊取敏感資訊，例如信用卡資訊。 以下是最近發現的釣魚網站例子，它們都是在冒充普及香港的會員平台。





除了偽冒網站，社交平台專頁亦湧現不少偽冒旅行社，並推出大量標榜「勁減」、「低至三折」、「限時/限量推廣一折」等優惠吸引市民查詢，從而騙取受害人金錢及大量個人資料，包括姓名、身份證、信用卡資料、電話號碼以及家人的資料。就著這些社交平台專頁，市民怎樣分辨該專頁是否屬實及廣告訊息內容的真假？除了可以留意專頁是否有藍剔、讚好及追蹤人數的多寡外，還可以注意以下要點，提防網上購物騙案：

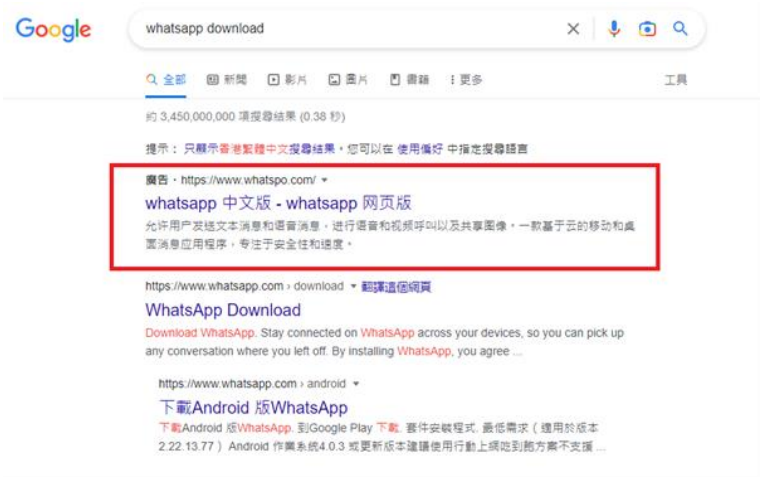
1. 公司商標（Logo）或圖片不清晰：大多數黑客所選用的圖片都是截圖取得或從其他網頁盜取，並非使用原圖，所以像素較低。另外，可以使用谷歌圖片搜尋來搜尋是否在其他網站上找到了類似的照片。
2. 聯絡資訊不詳細：專頁所顯示的聯絡資訊並不詳細，或會以個人電郵或電話作聯絡方式。
3. 管理人員所在地在國外：市民可透過專頁上的「關於」 > 「專頁透明度」查詢相關管理人員的所在地，若一些管理人員的所在地與專頁所在地有出入，就要警剔該專頁的真偽。
4. 專頁名稱是否經常更改以及建立時間：由於每次的詐騙手法不同，所以專頁會經常更改名稱，建立的時間亦很短暫。

市民可透過專頁的「關於」 > 「粉絲專頁透明度」查詢管理人員所在地及專頁建立時間

5. **專頁內只有小量貼文：偽冒專頁內的貼文大多只有近期一至兩個月抄襲而來的貼文。**
6. **異常大量的讚好/留言：留意讚好 / 留言是否來自專頁目標群以外的國家及留言內容是否大致相同。**

身份/憑證盜用

除了發動釣魚攻擊來引誘用戶提供個人資料外，黑客一旦成功盜取使用者的登入憑證還可以擴大攻擊規模，繼而冒充目標用戶身份針對他的家人和朋友進行攻擊。尤其是在節日期間，收到平時甚少聯絡的朋友的祝賀訊息亦不足為奇，因此警覺性或會降低。黑客會透過多種方式發動身份攻擊，包括中間人攻擊（AiTM）、偽裝廣告、社交工程攻擊等。大多數黑客的目標是得到用戶的帳戶登入，並在帳戶內執行惡意活動。有發現指最近黑客會創建虛假的 WhatsApp 登入頁面進行身份攻擊，並將惡意網頁在搜尋引擎結果內置頂。 如果用戶不小心瀏覽惡意網頁並進行登入，黑客就可以騎劫帳戶並存取 WhatsApp 帳戶中的所有資訊，從而發動進一步攻擊。



保安最佳實踐

如要在數碼時代裡體驗安全的旅行和在購物時無憂無慮，大家應考慮採取以下保安最佳實踐。

有關出外旅行時的保安最佳實踐：

1. **使用私人裝置去登入個人帳戶，避免使用公眾共享的裝置；**
2. **連結到可信的 Wi-Fi 熱點，避免連接到保安設定較低的 Wi-Fi 熱點；**
3. **檢查你的網上帳戶會否有任何可疑發入；**
4. **在使用流動支付方式購物時加謹小心，在確認和進行付款前先核對收款人和金額；**
5. **如需要瀏覽網頁或掃描 QR Code，在輸入任何資訊前先驗證 URL 連結的真確性；**
6. **不要點擊或打開使海外 SIM 卡接收的連結或附件，它們可能與釣魚攻擊相關；**
7. **如有需要，只從官方網頁和應用程式平台中安裝應用程式；**
8. **不要使用不明來歷的公眾充電插頭，以防受到「Juice Jacking」攻擊；**
9. **不要將您的裝置放在無人看管的地方； 及**
10. **將在家中和辦公室內不需使用的裝置關閉，在旅行時當你在晚間不再使用隨身裝置時亦將它關閉。**

有關網上購物時的保安最佳實踐：

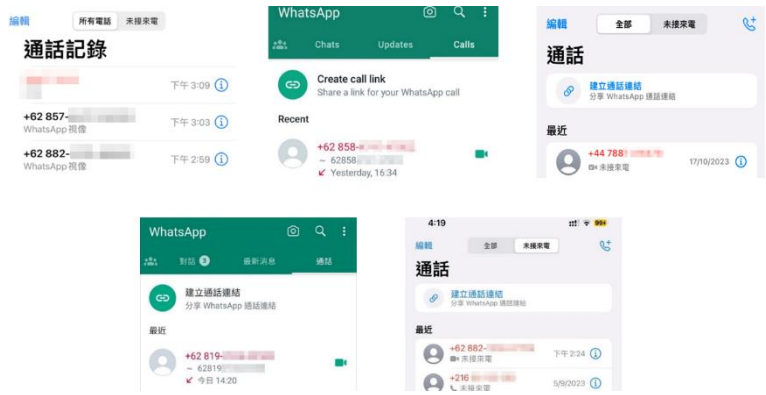
1. **切勿隨便點擊來歷不明的連結或附件。盡量在瀏覽器直接輸入網購平台網址或使用瀏覽器書籤。檢查連結及電郵的合法性，例如檢查清楚網址有否拼寫錯誤、文法錯誤或寄件人是否可信。若網站並非使用 HTTPS 加密，應倍加小心，不要在沒有加密的情況下輸入敏感資訊；**

2. 定期轉換網購平台賬戶密碼，於不同的帳戶使用不同的密碼，以防止其中一個資料被外洩後牽連其他帳戶；
3. 如果購物平台支援多重認證，用戶應將其啟用以加強保安；
4. 只經官方網站或手機應用程式購物或查看訂單情況；
5. 不要在平台的網上帳戶裡上儲存任何敏感資料，例如信用卡資訊等；
6. 定期檢查自己的網上付款記錄，查看是否有可疑交易；
7. 收到可疑電郵或訊息後，可以向官方渠道查詢詳情，切勿向不明來源發送者提供敏感訊息；
8. 在瀏覽器上設定反釣魚網站功能以助阻擋釣魚攻擊； 及
9. 使用用「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。

詳細資料可參閱HKCERT保安博錄
https://www.hkcert.org/tc/blog/taking-security-best-practice-during-festive-season

提高市民網絡安全意識：
防範陌生WhatsApp視像通話的風險

隨著科技的發展，網絡安全已成為我們生活中不可忽視的重要議題，網絡攻擊手法也變得越來越狡猾。有市民向香港電腦保安事故協調中心（HKCERT）查詢，報稱收到陌生人士發出的可疑WhatsApp視像通話（如+62及+44地區編號），對方自稱公安或銀行機構並可以說出事主名字。這引起了公眾對陌生視像通話的風險的關注。本文旨在提高市民對於網絡安全的警覺意識，並提供一些防範陌生視像通話的實用建議。



為什麼攻擊者會利用視訊通話，而不是正常的語音通話？

只要個人身份辨識：攻擊者可以透過視像通話擷取市民的外貌，並透過 Google 搜尋、社交媒體文章或網路相簿將視訊或圖片內容和可識別個人士聯繫。同時也可以觀察目標的背景或外表上的個人細節，協助未來的社會工程或身份盜用攻擊。

取得面部資料製造深偽造影像：攻擊者可以透過視像通話取得市民的外表和聲音以製作高度真實的深偽造影像，藉此進一步向您的家人或朋友進行其他詐欺活動。

身分假冒用作非法目的：當攻擊者的視頻和聲音都清晰可見時，攻擊者更容易利用虛假場景、背景或服裝製造假象，假冒執法機構或銀行組織，以加強真實感和具壓迫感，隨後進行財務詐騙。

感覺需迅速回應：視像通話使目標感覺需要迅速回應，減少審慎思考的時間。這有利於欺詐者控制詐騙的互動過程。

陌生視像通話有什麼風險？

詐騙手法：攻擊者可能試圖利用視像通話來進行詐騙活動，例如冒充公安機關或銀行職員，試圖獲取您的個人資訊或金錢。

個人私隱洩露：陌生人可能通過視像通話偷窺您的私人生活，並將視頻或照片錄製下來，進行不當使用或散佈。另外，不慎使用 WhatsApp 中的分享螢幕功能（右圖），增加資料外洩風險，如用戶正在使用銀行服務或正在輸入密碼。

防範陌生視像通話的實用建議

謹慎接聽：對於來自陌生人的視像通話，應該保持謹慎態度。如果您不認識來電者，可以選擇不接聽或直接拒絕通話。

不透露個人資訊：切勿在陌生視像通話中透露個人敏感信息，如密碼、銀行賬戶號碼等。合法的機構或機構工作人員不會通過視像通話要求您提供這些信息。

下載檔案的審慎：如果陌生人要求您下載或打開視像通話中的檔案，請保持謹慎。請僅下載來自可信來源的檔案，並使用安全的防病毒軟件進行掃描。

與家人和朋友討論：與家人和朋友討論這些風險，增加彼此對陌生視像通話的警覺，並相互提供支持和建議。

設定隱私選項：檢查您的設備和應用程式的隱私選項，確保只有授權的人可以向您發起視像通話，或者可以將不明來電者返為靜音（開啟 WhatsApp「設定」>「私隱」>「通話」> 啟動「將未知來電設為靜音」）。

網絡安全變得日益重要，防範陌生視像通話的風險是我們必須面對的挑戰之一。通過遵循本文提供的實用建議並保持警覺，個人可以增強網絡安全，保護自己免受潛在的威脅。謹慎接聽來自陌生人的視像通話，避免透露個人敏感信息，審慎下載檔案，設定隱私選項，並與家人和朋友討論這些風險，共同提高對陌生視像通話的警覺意識。只有通過這些努力，我們才能建立更安全的網絡環境，保護個人和社會的利益。

詳細資料可參閱HKCERT保安博錄
https://www.hkcert.org/tc/blog/raise-public-awareness-of-cyber-security-guard-against-risks-of-unknown-whatsapp-video-calls

保護重要基礎設施：
IT / OT融合 vs 中間人攻擊（MITM）

本文將詳細說明融合IT和OT系統的風險和介紹中間人攻擊的相關知識，並提供減輕風險的最佳保安實踐。我們亦重點提及採用保安架構以保護網絡保安威脅的重要性，以及對物聯網裝置實施保安措施的必要性。如果用戶將上述之保安實淺納入新常態，他們就可以深入了解IT/OT融合的挑戰和風險，並採取可行的措施來減輕這些風險。

什麼是中間人攻擊（Man-in-the-Middle Attack – MITM）？

中間人攻擊（MITM攻擊）是指黑客攔截兩個裝置之間的通訊並獲得控制權以執行惡意操作，例如讀寫數據，甚至執行命令。MITM攻擊可以從不同手法進行，例如ARP偽造、DNS偽造、SSL剝離等。

IT/OT融合

在保安角度而言，IT 和 OT 系統會優先考慮不同的因素。IT 系統的保安重點在於保護用戶的數據，然而 OT 系統主要強調系統的可用性、操作期間的物理安全性和數據的完整性。由於大多數 OT 系統的生命周期比 IT 系統長，這可能令一些舊 OT 系統仍在工廠中運行。由於 OT 系統一般處於一個與世隔絕的網絡環境，因此在網絡設計階段尚未充分考慮其保安，令其缺乏保安措施和網絡防禦。

IT/OT融合的網絡保安案例研究

早前，香港電腦保安事故協調中心（HKCERT）與香港理工大學電子計算學系教授羅夏樸博士及其本科生鄧浩添先生合作，對普遍的可編程邏輯控制器（Programmable Logic Controller – PLC）作出網絡保安案例研究，以提高公眾在重要基礎設施加強物聯網的保安的重要性，特別是針對中間人攻擊。

測試目標與預期結果

本測試以建造一個小型交通系統作一個測試環境。此中間人攻擊的模擬能夠展示黑客如何截取並更改 PLC 和其組件之間的通訊，導致未經授權的訪問和系統妥協。

測試目標

此測試重點放在 PLC 系統的網絡伺服器上而不是 PLC 本身，並假設網絡伺服器功能已預設啟用。

預期結果

此測試預期會在系統中發現一些漏洞並測試其保安弱點，例如緩衝區溢出或命令注入。這些漏洞可以讓黑客在目標裝置上執行惡意程式碼以進行中間人攻擊。

測試環境與裝置

此測試以模擬通過網絡環境使用 PLC 並遠程控制它的情況。測試環境中使用的裝置包括：

預設環境

- 將已開啟的 PLC 設置與交通燈燈膽和網絡交換器連接
- 使用網絡管理功能設定 PLC，將其設定保持為原廠預設

黑客

- 將筆記型電腦與網絡交換器連接（與 PLC 網絡環境相同）
- 已安裝並執行 Windows 11 作業系統和 Burp Proxy 軟件的筆記型電腦

假設

- 黑客騎劫了 PLC 所在的內部網絡並獲得了最初的存取權限。

模擬中間人攻擊的測試方法和步驟

此黑客發動中間人攻擊的模擬會分為兩個階段使用 Burp Proxy 軟件 – 偵察和武器化：

偵察 – 竊聽和分析網絡流量

1. 黑客會先設定一個代理程式並引誘使用者透過它進行連線，以準備發動中間人攻擊。
2. 駭客使用 Burp Proxy 攔截使用者瀏覽器和網絡伺服器之間的流量。 當使用者嘗試再次登入時，POST 請求會發送至網絡伺服器。

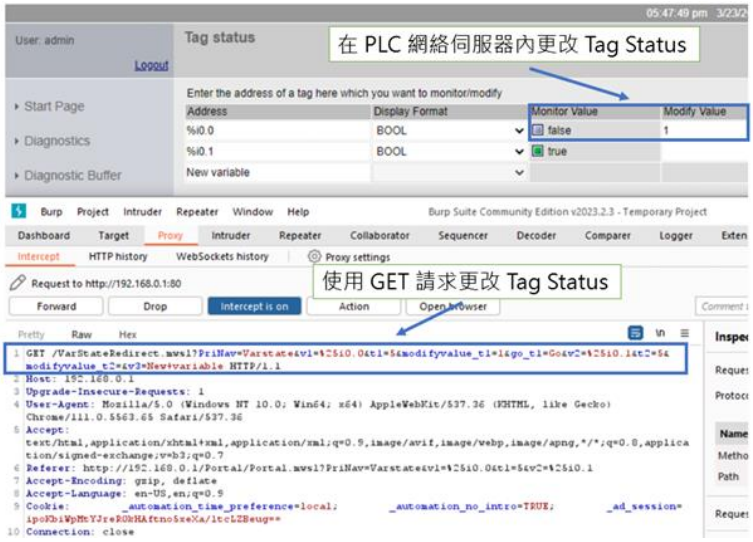
3. 黑客在 Burp Proxy 中檢視顯示的登入資訊，瀏覽器和 PLC 之間在發送登入資訊之前進行了加密。

武器化 – 修改竊聽的網絡流量並發送回 PLC

1. 黑客可以透過丟棄或發送來更改攔截的網絡流量。 透過 Burp Proxy，黑客可以複製攔截的請求並操縱其 Session Cookies 來獲取 PLC 的控制權。

2. 黑客會使用 CURL（一種用於發送自訂網絡請求的簡單命令發送工具）發送一些受自訂的請求以控制 PLC。一些自訂的網絡請求經過測試並成功更改了 PLC 的設置，如下所示：

   - 黑客可以透過發送 GET 請求來更改 Tag Status 列表以監視或更改 PLC 系統的操作



   - 黑客可以透過發送 POST 請求將已上載的檔案更改其名稱或內容，導致它們不能使用或感染其他設施或裝置。

   - 黑客可以透過發送 GET 請求將檔案名稱更改為另一個檔案名稱或強行透過字典攻擊以刪除檔案。

以上中間人攻擊的模擬有顯著發現，證明黑客能夠使用 Burp Proxy 獲取敏感資料，甚至更改 CPU 操作和上傳惡意代碼到裝置。從而可見，黑客可以在 IT/OT 融合的情況下使用 Burp Proxy 軟件進行中間人攻擊。

研究中發現的其他風險

本研究亦得出成功和有風險的發現。一方面，本研究對其網絡伺服器進行重放攻擊（Replay Attack），亦對其網絡應用程式進行字典攻擊。然而，該研究還發現進行測試的 PLC 存在幾個嚴重漏洞。這些漏洞包括黑客能夠使用工業利用框架（Industrial Exploitation Framework）對測試的 PLC 進行重放攻擊的能力。此外，本研究證明黑客如何使用注入器工具對 PLC 進行阻斷服務（DoS）攻擊。

保安最佳實踐以減輕IT/OT融合的風險

機構應採取積極態度來應對網絡保安問題，以減輕 IT/OT 融合帶來的風險，特別要重視減輕中間人攻擊的風險。以下是機構應該考慮的一些保安最佳實踐：

1. 定期進行網路和保安評估，以發現潛在的漏洞和風險；
2. 制定風險評估報告，找出 IT/OT 融合環境中與 中間人攻擊相關的風險；
3. 制定嚴格的實施計劃，率先解決和預防已識別的保安風險和漏洞，例如實施保安通訊協定、加密以及強大的身份驗證和存取控制措施；
4. 更新營運政策，以反映新的保安措施和偵測的最佳實踐，以防止攻擊的可能性；
5. 採用保安架構，如普渡參考模型或「零信任」架構，並用清晰的邊界和嚴格的存取控制，防止未經授權的訪問，減少能夠進行的渠道；
6. 使用入侵偵測和防禦系統監視網路流量，並檢測和預防中間人攻擊對 IT/OT 融合系統潛在損害；
7. 管理修補程式，以確保 IT/OT 融合系統定期安裝修補程式和更新，以修補已知的漏洞；
8. 參考 HKCERT 的《物聯網保安最佳實踐指引》，在使用物聯網裝置時採用保安最佳實踐，並參考 HKCERT 的《中小企保安事故應變指南》制定其環境中的事故應變計畫。

總結

在融合 IT 和 OT 系統之前，有充分的準備是必需以降低風險。如果技術專業人員對所有系統缺乏理解，可能會使 IT 和 OT 系統的融合具有挑戰性。因此，公司的保安、營運和維護政策有必要在融合後進行更新。本研究重點關注 PLC 系統的網絡伺服器而不是 PLC 本身，假定網絡管理功能已設定為默認啟用。總括來說，這個案例研究提醒大家保護 IT/OT 融合系統的重要性，免受特別是中間人攻擊的網絡保安事故。

詳細資料可參閱HKCERT保安博錄
https://www.hkcert.org/tc/blog/protecting-critical-infrastructures-it-ot-convergence-vs-mitm-attacks

完

香港電腦保安事故協調中心
電話：8105 6060
電郵：hkcert@hkcert.org