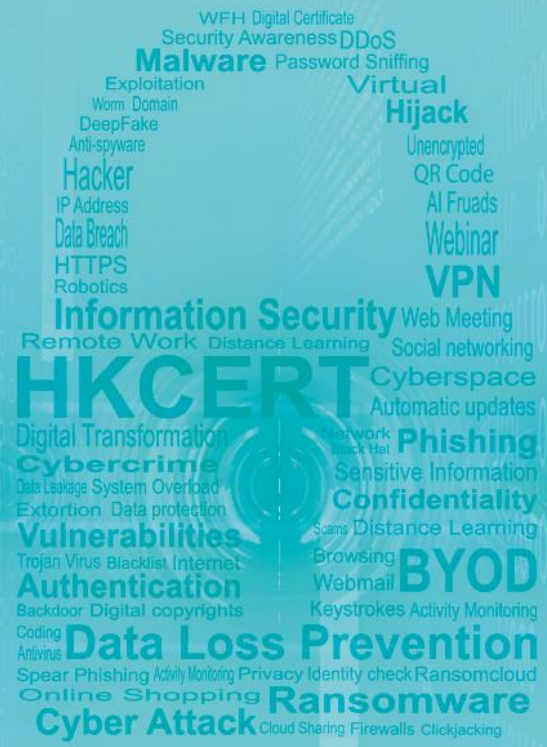
Hong Kong Computer
Emergency Response Team
Coordination Centre
HKCERT 香港電腦保安事故協調中心

香港保安觀察報告
2023 第二季度

發佈日期: 2023年8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	2023-07

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

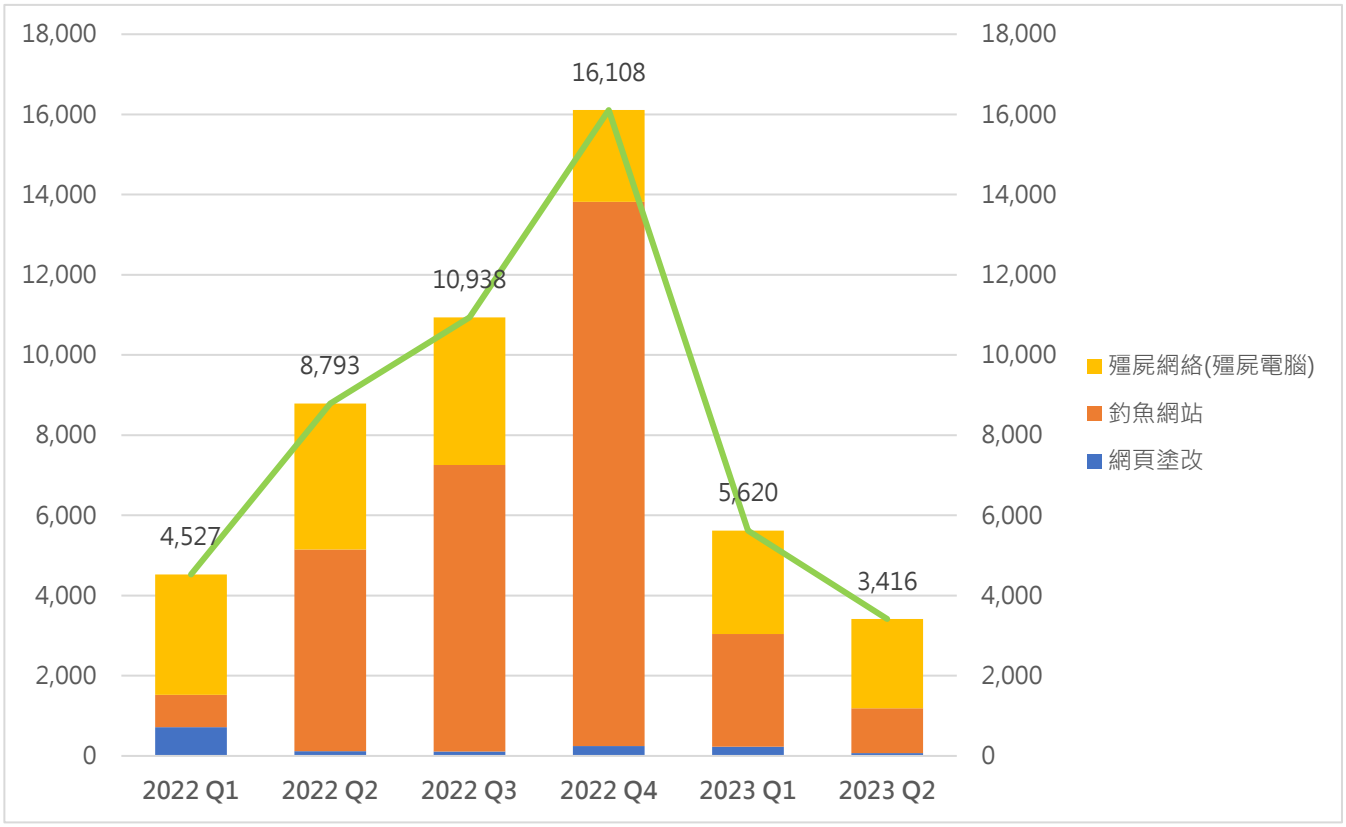
2023 第二季度報告概要

涉及香港的單一網絡保安事件宗數

3,416

按季下跌

39.2%↓



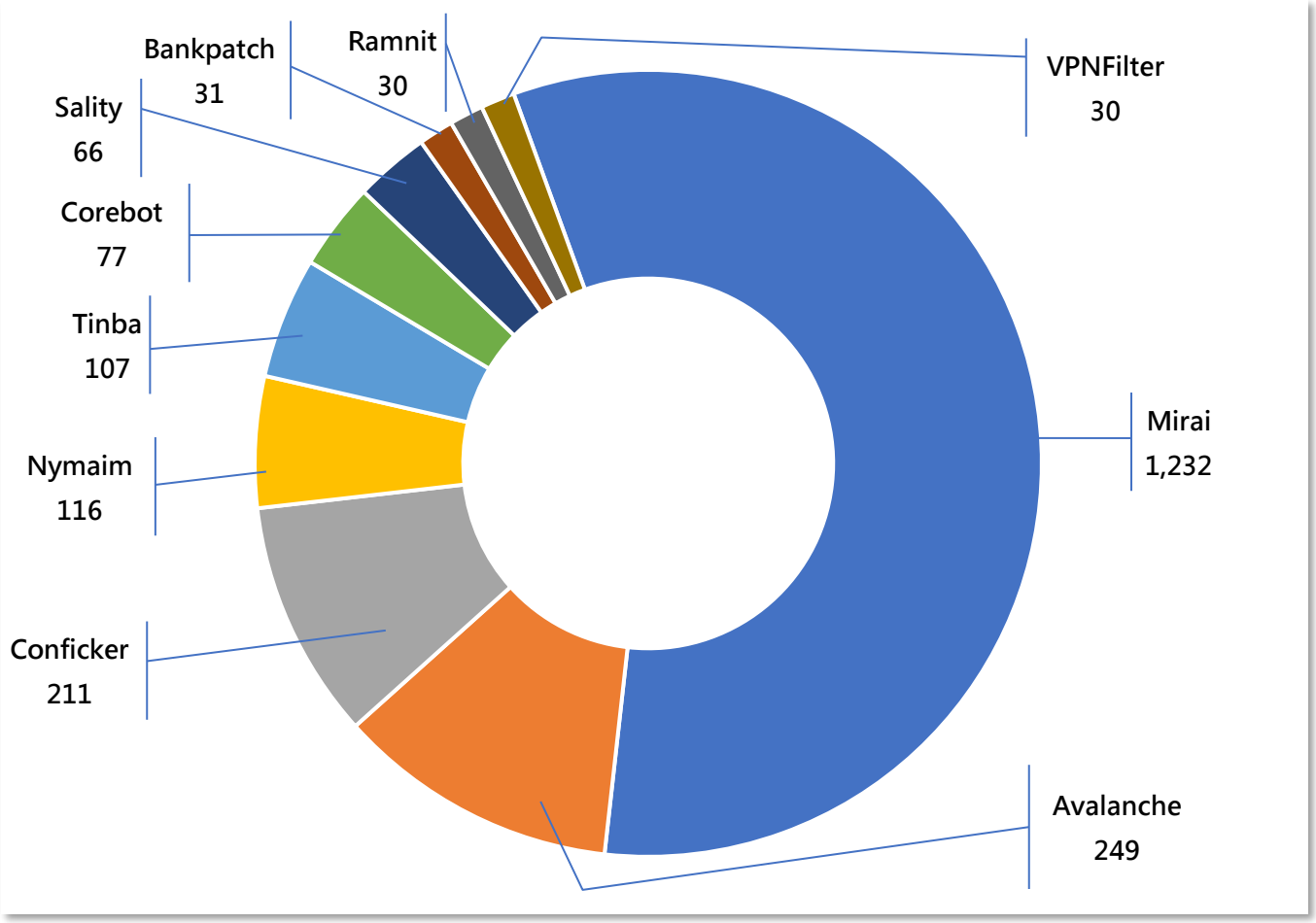
事件類別	2022 Q2	2022 Q3	2022 Q4	2023 Q1	2023 Q2	按季
網頁塗改	118	113	249	233	69	-70.4%
釣魚網站	5,033	7,141	13,574	2,804	1,120	-60.1%
殭屍網絡(殭屍電腦)	3,642	3,684	2,285	2,583	2,227	-13.8%
總數	8,793	10,938	16,108	5,620	3,416	-39.2%

香港網絡內的主要殭屍網絡

Mirai
1232
↑ 53.8%

Avalanche
249
↓ 61.4%

Conficker	211	+9.9%
Nymaim	116	-54.5%
Tinba	107	+114%
Corebot	77	-74.5%
Sality	66	+32%
Bankpatch	31	+47.6%
Ramnit	30	+500%
VPNFilter	30	-14.3%



** 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。*

網絡釣魚連跌兩季！公眾仍需提防受騙！

2023年第二季網絡事件數字正式出爐。今季網絡釣魚較上季下跌60.1%，較去年同期跌77.7%。值得注意的是，有關數字只反映寄存於香港系統內的網站情況，並不包括海外。換句話說，黑客可以將釣魚網站寄存海外伺服器，但攻擊香港用戶。另外，HKCERT亦觀察到近期有不法分子會利用社交媒體，如WhatsApp、Facebook、LinkedIn及Instagram進行欺詐，藉此騙取用戶資產及個人資訊。

為了保護公眾免受釣魚攻擊及利益，HKCERT亦為公眾提供一些網絡安全建議：

1. **避免點擊可疑連結：**不要隨意點擊來自未知來源或可疑的電子郵件、社交媒體消息、短訊或彈出窗口中的連結。在點擊連結之前，先仔細檢查其連結，確保正確。

2. **提高密碼安全性：**使用強式密碼，定期更換密碼，不要在不安全的網站上使用相同的密碼。使用雙因素驗證（2FA）來增加帳戶的安全性。

3. **更新和保護設備及軟件：**定期更新操作系統、應用程序和安全軟件，以確保它們具有最新的安全修補程序和防護措施。

4. **謹慎處理個人資訊：**不要隨意在不信任的網站上輸入個人敏感訊息。當提供個人資訊時，應先了解提交的資料用途。

5. **應對懷疑釣魚攻擊：**如果收到可疑郵件或連結並懷疑涉及釣魚攻擊，不要點擊其中的連結，也不要提供任何個人或敏感訊息。同時應報告該郵件或連結給相關的機構或組織，以協助他們採取適當的行動。

這些建議可以幫助公眾保持警惕，減少成為釣魚攻擊受害者的風險。保持良好的資訊安全意識和行為習慣是網絡保安的關鍵。

圖片來源：癲噹 DinDong Facebook 專頁
https://www.facebook.com/100044634960219/posts/pfbid02WBrHHP6DDJPYwtn9eUzghTbrGjsrrWZJckG5knNk8ondudzNBrWj4cYcF7KeVbX2l/?mibextid=cr9u03

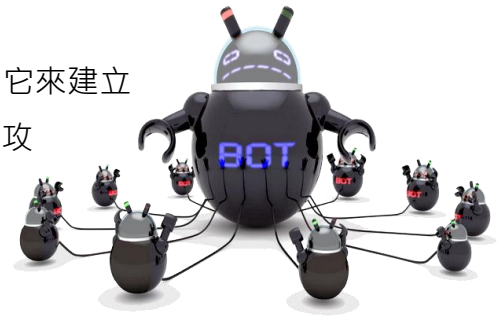
Mirai 有關殭屍網絡數字急升53.8%！專家分析箇中原因

Mirai是一款惡意軟件，它的主要功能是感染物聯網（IoT）裝置，例如攝像頭、路由器和汽車等，並將這些裝置轉變成用於發動大規模分散式阻斷服務攻擊（DDoS）的殭屍裝置或殭屍網絡（Botnet）。Mirai於2016年首次被發現，當時重大事故包括它針對了Dyn域名解析服務商，使許多大型網站無法造訪。

Mirai攻擊上升的原因

至於Mirai個案上升的原因，可能與物聯網裝置的普及和安全意識不足有關，例如設置在家中的IP Camera。許多物聯網裝置的安全性較低，例如預設密碼弱、未更新軟體等問題，使它們容易成為殭屍網絡攻擊的目標。此外，大多數物聯網裝置的用戶並不了解它們的漏洞，也不知道如何保護自己的裝置，因此它們容易被感染並被攻擊。

另一個原因可能是Mirai的源代碼已經公開，令任何人都可以使用它來建立自己的殭屍網絡，進一步擴大了它的威脅範圍。此外，殭屍網絡攻擊已經成為一個龐大且有利可圖的黑色產業，這也可能促使更多不法分子使用Mirai進行攻擊。

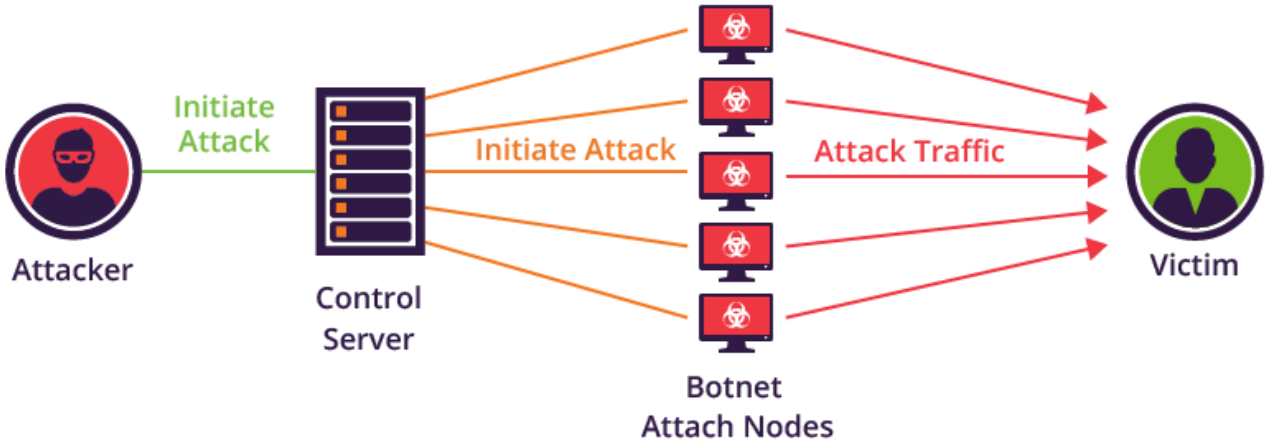


除了剛才提到物聯網裝置普及和安全意識不足之外，還有其他原因如Mirai的變異體開始被使用。Mirai變異體例子有IZ1H9、Satori、Miori 、PureMasuta、IoTrooper 及Reaper等。

Mirai攻擊原理

當Mirai感染一個裝置時，它會使用預先定義好的一組用於攻擊的指令，例如HTTP請求和TCP SYN洪水攻擊，來發動DDoS攻擊。這些攻擊指令會向目標網站或服務發送大量的請求，使其無法正常運作並停止服務。由於Mirai可以感染大量的IoT裝置，使它可以發動非常大規模的攻擊，對網際網路基礎設施造成嚴重的損害。

Mirai感染裝置的方式通常是利用未修復的漏洞或較弱的密碼進行遠程訪問，並在裝置上安裝惡意軟件。一旦受到感染，Mirai會與控制中心建立連接，以便接收攻擊指令並執行攻擊。控制中心可以通過匿名網路，例如Tor設置，使其更難被追踪或被關閉。此外，電郵中的附件也成爲被感染的途徑之一。



近期與Mirai有關的網絡事故

今年四月中，根據Palo Alto Networks 威脅研究團隊Unit 42研究指出一個名為IZ1H9的Mirai惡意軟件變異體正在感染Linux物聯網設備，並創建一個大型的殭屍網絡以進行惡意活動。該惡意軟件會先檢查目標IP，避免向政府網絡、互聯網服務供應商和較大型科技公司發動攻擊，藉此隱藏自己位置。此外，IZ1H9的另一特性是如果目標設備已成為殭屍網絡的一部份，它會把設備已進行的程序終止，並啟動新程序。

另外，在今年五月，Mirai殭屍網絡正積極利用漏洞CVE-2023-28771向Zyxel 防火牆發動大規模攻擊，並允許未經身份驗證的攻擊者於目標系統觸發遠端執行任意程式碼。

HKCERT保安建議

為了保護用戶的物聯網裝置免受Mirai和其他殭屍網絡攻擊的影響，HKCERT建議用戶：

- **使用及定期更新複雜性高的密碼（例如混合使用符號、數字、大階及細階英文字母，及建議長度不少於12個字元）**
- **更新設備的軟體和韌體**
- **限制設備的遠程訪問和關閉不必要的端口等安全措施**
- **定期進行安全檢查**
- **保持網路安全意識**

教育活動：「落區」宣傳防釣魚訊息

第一季「網絡釣魚 全城防禦」 宣傳車活動完滿結束！

HKCERT在六月二十六日至七月二日舉辦「網絡釣魚 全城防禦」宣傳車活動，旨在提高市民對於網絡釣魚的認知和防範能力，並強化大眾的網絡保安意識。這次活動亦與本地插畫家DinDong聯乘合作，透過多元化的宣傳方式，讓更多人了解網絡釣魚的危害，並學習如何保護自己及身邊家人。活動期間「網絡釣魚 全城防禦」宣傳車覆蓋全港多個地區，包括灣仔、觀塘及大埔，讓市民可以近距離了解網絡釣魚的手法、危害及防範方法。同時，現場設置互動遊戲，讓參加者以更有趣的方式學習網絡安全知識，並有機會贏取獎品。

總括而言，「網絡釣魚 全城防禦」宣傳車活動是一次旨在提高市民網絡安全防範能力的重要活動，協助大眾認識網絡釣魚危害，掌握相關防範知識，進一步加強大眾對於網絡安全的意識。第二季宣傳車活動即將舉行，詳情可以稍後留意HKCERT 網站及Facebook / LinkedIn公佈。

「智慧城市」：HKCERT同你洞悉「釣魚」玩番轉!

由政府資訊科技總監辦公室（OGCIO） 舉辦的「智慧城市」巡迴展覽第四季已圓滿結束。HKCERT好榮幸再一次作為其中一間參與機構為各位市民介紹網絡釣魚及如何防範網絡釣魚。是次HKCERT分別於元朗、中環、屯門、柴灣同大埔與公眾見面！除有上一季受市民歡迎的智破「釣魚」小遊戲外，更特別加入洞悉「釣魚」玩番轉小遊戲，希望透過有趣而且生動方式藉此令更多市民明白科技除為社會帶來便利外，亦需要了解當中的潛在風險。避免成為黑客下一個目標。

網絡分析：數碼時代IoT安全 保護你的物聯網世界

物聯網（IoT）指一個相互連接的系統，包括物理設備、車輛、建築物和其他嵌入了感應器、軟件和網絡連接的物體，使它們能夠收集和交換數據。物聯網的目標是創建一個更高效、更連接的世界，在這個世界中，設備和系統可以相互通信，自動化任務，提高整體性能。物聯網設備的例子包括網絡攝影機、智能恆溫器、可穿戴式健身追踪器，以及連接的家電，如冰箱和洗衣機等。

物聯網有什麼例子？

其中一種普及化的應用是無人駕駛飛機（UAV），簡稱無人機，它是一種可以在沒有人類飛行員在機艙內受控飛行的飛行器。它們可以由電腦或控制器控制。無人機已廣泛用於各個領域，如軍事武器裝備、貨物運輸或搜索和救援行動。這個領域的市場規模顯然巨大。它吸引政府和商業產業加入並投資於無人機開發。這有利於技術的發展和無人機成本的降低。結果，一些商業產業開始探索無人機市場，從專業市場轉向經濟市場，為公眾提供低成本的無人機。由於逐漸普及使用，黑客可以透過無人機進行惡意行為，對公眾安全及私隱帶來潛在風險。

HKCERT 已將針對 IoT 的攻擊列為 2023 年五大資訊保安風險之一，早前更夥拍香港理工大學電子計算學系副教授羅夏樸博士及其本科生沈詠聰同學，共同進行一項針對無人機的網絡安全研究，藉此喚起大眾對無人機及物聯網安全的關注。

消費品級無人機的應用

消費品級無人機有兩種：單純的「飛行器」和安裝了拍攝鏡頭的「航拍機」，他們通常都是經由遙控器和電腦程式遠端控制，有不同的用途、形狀和大小，例如攝錄、協助搜索救援行動、科學研究、農業監測等等。由於技術進步和成本降低，它們在近年來變得越來越受歡迎，適合任何年齡層的人士操作。除此以外，黑客可能會控制無人機並使用它進行物理攻擊，例如投放負載或將無人機撞擊目標。這可能會對人員或財產造成嚴重傷害，所以特此揀選此類設備進行研究。

保安風險

黑客攻擊手法普遍會針對系統的漏洞、用戶的個人憑證及加密方法。而一般無人機是經由控制器發送指令給機體，機體會接收並執行指令，並回傳系統狀態及影像至控制器。兩者都是獨立系統，中間透過既定的網絡通訊協定和指令操作。如要「騎劫」無人機，黑客便可以從這幾方面著手，例如：

- 植入惡意軟體至控制器或機體，或
- 透過網絡通訊連接入侵機體

由於大部分物聯網設備的網絡通訊連接方式大同小異（如 Wi-Fi 及藍芽），所以今次會從這一點上進行研究探討，希望用無人機做例子，令大眾了解到其他使用類似連接方式的物聯網設備都有機會發生的保安風險。

測試目標及預期結果

市面上大部分無人機會利用 Wi-Fi 作為通訊方式。Wi-Fi De-authentication 攻擊是一種針對 Wi-Fi 網絡中客戶端設備和接入點之間通信的無線網絡攻擊。攻擊包括向接入點發送取消認證的請求，使客戶端從網絡中斷開連接。方法是於無人機的 Wi-Fi 網絡接收範圍內，利用特定工具向其發送取消認證的幀。這種攻擊可以用來破壞 Wi-Fi 網絡的正常運作，強制客戶端重新連接到網絡，並可能揭示敏感信息，例如登錄憑據，或者發起其他類型的攻擊。

目標： 透過 Wi-Fi De-authentication 中斷用戶裝置對無人機的連接。
預期結果： 控制無人機移動及實時查看當時影像。

測試方式

模擬一般用戶正在使用無人機的情景，另一名扮演黑客的研究人員在附近遙距奪取無人機的控制權。

測試環境及設備

測試在普通室內場景進行，使用的設備都保留在原廠的設定上，設備包括：

用戶

- 無人機
- 安裝了無人機操控程式的 Android 智能電話

黑客

- 安裝了 2 個網絡連接卡的手提電腦，電腦安裝了 Windows 11 和 Kali Linux（VirtualBox）作業系統

測試方法及步驟

用戶

1. 啟動無人機
2. 用智能電話操控無人機飛行及攝錄

黑客

1. 利用網絡掃描工具掃描現場的所有無線網絡以獲取無人機 MAC 地址
2. 執行 Wi-Fi de-authentification 指令來中斷用戶裝置與無人機的連接
3. 用特定程式連接無人機
4. 完全操控無人機及截取攝錄到的影像

經測試，黑客只需約30秒便可完成以上述攻擊，並完全取得無人機的控制權，包括關閉無人機引擎。詳細測試片段可參考以下影片。

影片示範

保安建議

使用複雜性高的密碼（例如混合使用符號、數字、大階及細階英文字母，及建議長度不少於 12 個字元），並盡可能設定雙重驗證 / 多重驗證為用戶認證方式，這將有助於防止未經授權的訪問進入用戶的無人機控制系統。研究亦嘗試在一分鐘內成功 Brute Force 簡短密碼，所以複雜的密碼能減少被入侵的機會；另外，使用無人機或其他物聯網設備前盡可能更改其 SSID，因為黑客能透過預設 SSID 推斷所使用產品的品牌及型號。

其他建議

個人用戶：

1. 保持無人機韌體維持最新狀態
   定期更新無人機的韌體，以修補已知漏洞並確保無人機的軟體是最新的。

2. 停用非必要的功能
   減少黑客透過其他渠道進行攻擊。

生產商：

1. 加密無人機的數據
   使用加密來保護在無人機和其控制系統之間傳輸的數據。這將有助於防止數據被盜或截取。

2. 為用戶設置雙重驗證 / 多重驗證為用戶認證方式
   有助於防止未經授權的訪問您的無人機控制系統。

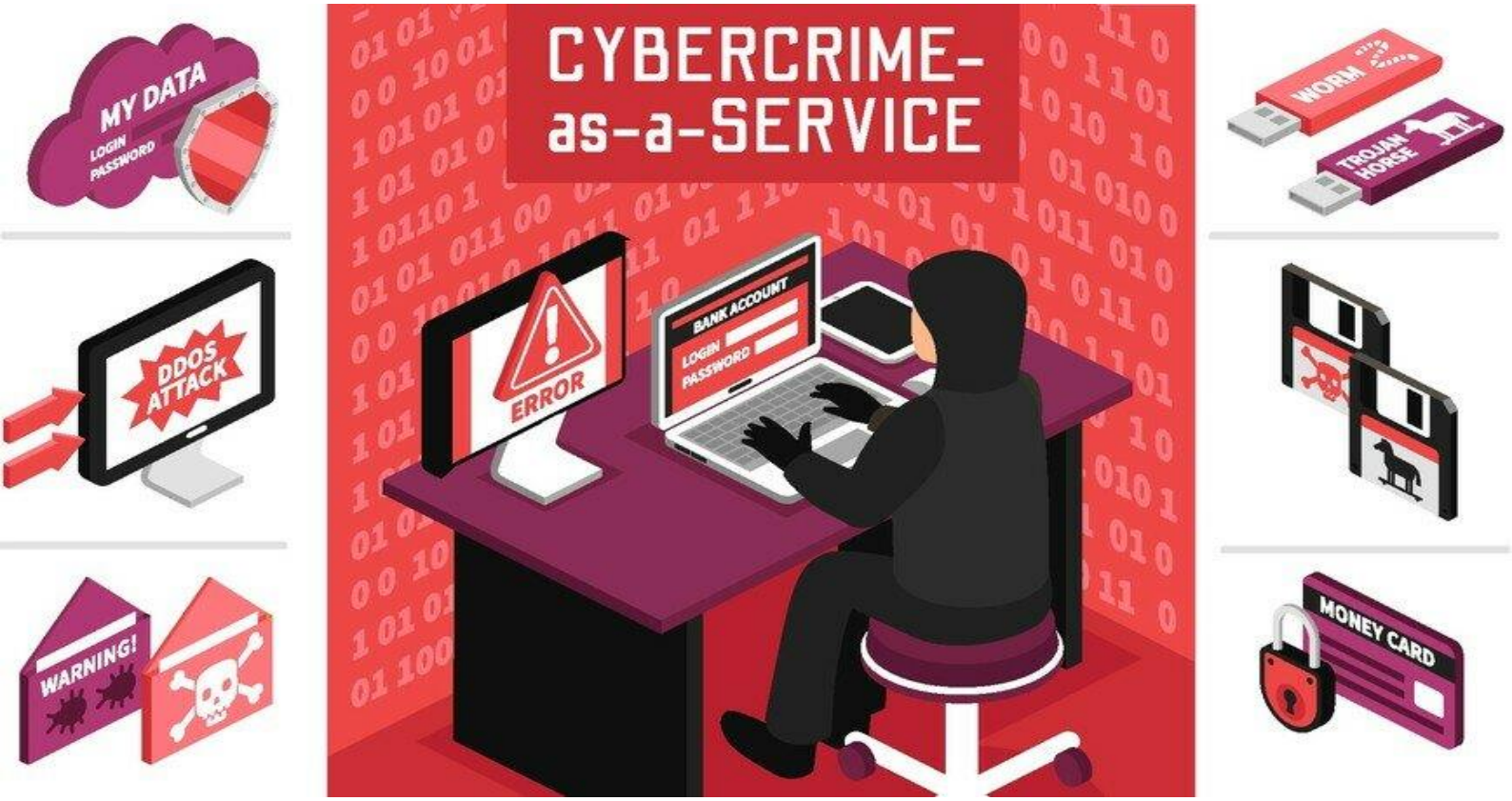
總結

現今物聯網的高速發展為用戶的生活帶來便利，但同時也帶來網絡安全隱患，例如可能導致惡意攻擊、數據洩露、侵犯隱私等安全問題。因此，確保物聯網設備的安全至關重要。為確保物聯網設備的安全，需要採取一系列措施。首先，需要使用安全性能較佳的物聯網設備，這些設備要有完善的安全防護措施；其次，物聯網設備需要定期更新和維護，以確保其系統和軟件是最新的，以避免已知的安全漏洞；此外，還需要加密技術來保護物聯網設備的通信，以防止數據被盜或被篡改。

最後，用戶還應注意保護自己的私隱和安全。用戶應使用強式密碼保護物聯網設備，避免使用公共無線網絡連接物聯網設備，並定期檢查物聯網設備是否正常工作。HKCERT 在 2020 發佈了《物聯網保安最佳實踐指引》，內容涵蓋應用 IoT 設備時要注意的網絡保安事項。大家亦可以此作為參考。

詳細資料可參閱HKCERT保安博錄
https://www.hkcert.org/tc/blog/iot-security-in-the-digital-age-protecting-your-connected-world

網絡小貼士：揭開網絡犯罪服務的神秘面紗 數碼便利的陰暗面



在今天的數碼時代，我們已經習慣依賴互聯網，為我們提供無與倫比的便利，讓我們輕鬆獲取豐富的資訊和無數的服務。不幸的是，並非每個人都將互聯網用於正當用途，有些人甚至在網上出售網絡犯罪服務。HKCERT已將網絡犯罪服務列為2023年五大資訊保安風險之一。本篇文章中，我們將深入探討網絡犯罪服務（CaaS）的概念、其商業模式以及如何興起。我們還將提供CaaS的例子，並討論如何保護自己，防止成為這些網絡犯罪服務的受害者。

什麼是網絡犯罪服務（CaaS）？

網絡犯罪服務（CaaS）是指不法分子或組織向其他罪犯提供網絡犯罪工具、基礎設施和服務來換取收費。實質上，CaaS使即使技術能力有限的人也可以從事複雜的網絡攻擊和其他非法的網絡活動。這導致網絡犯罪快速增長及演進，因為網絡犯罪門檻變得越來越低和變得越來越有利可圖。

網絡犯罪服務的商業模式

網絡犯罪服務的運作方式與其他合法企業的業務類似，向不同的客戶提供各種產品和服務。然而，主要的區別是 CaaS 的客戶是其他罪犯，提供的服務都是用來進行犯罪活動。CaaS 市場上一些常見的產品和服務種類有：

- Malware-as-a-Service:
  包括開發、分發惡意軟件和技術支援，例如勒索軟件、間諜軟件或木馬程式，可用於感染設備和系統、竊取敏感數據或勒索。
- Exploit-as-a-Service:
  網絡罪犯提供未被發現的保安漏洞（也稱為「零日漏洞」），或提供自動化工具攻擊軟件或系統中已知的漏洞。
- Infrastructure-as-a-Service:
  提供被惡意軟件感染和被其操控的用戶電腦或伺服器（也稱為「殭屍網絡」），可用於發起分散式阻斷服務（DDoS）攻擊、發送垃圾郵件或儲存惡意內容。
- Hacking-as-a-Service:
  專業黑客提供受僱服務來入侵僱主指定的系統或網絡，竊取數據或破壞系統等。

為什麼網絡犯罪服務會興起？

網絡犯罪服務的興起可以歸咎於多個因素。首先，互聯網的快速增長和廣泛應用為網絡罪犯提供了「發揮機會」。網絡世界的匿名性使他們能夠隱藏身份並逃避法律制裁，而互聯網的全球覆蓋範圍使他們可以在世界任何地方攻擊受害者。

其次，科技不斷演進，網絡保安技能缺口擴大，創造了網絡犯罪服務的需求。企業投放大量資源加強網絡保安措施，普通網絡罪犯的技術跟不上，要倚靠較專業的網絡罪犯幫助他們繞過這些保安措施並實現其惡意目標，於是這種「供求關係」發展成一個網絡犯罪服務的市場。

網絡犯罪有利可圖，加上地下交易市場匿名化，已經吸引了越來越多個人和組織從事這些非法活動。網絡犯罪服務使他們能夠通過將自己的技能和資源商品化來獲取最大利潤，同時也使其他網絡罪犯因付出的成本較低(如技能和設備等)，而更容易加入網絡罪犯的行列。

網絡犯罪服務的詳細例子

為了更好地了解網絡犯罪服務所帶來的威脅，讓我們探討一些實際的例子：

- 勒索軟件服務（RaaS）：CaaS 最著名的例子之一是勒索軟件服務。 這種模式中，網絡罪犯開發並分發勒索軟件，該軟件加密受害者的數據並要求贖金才能解密。

  RaaS 提供者通常提供簡單易用的平台，允許罪犯定制勒索軟件、自定贖款金額以及管理勒索軟件攻擊。 RaaS 平台的示例包括 GandCrab、REvil 和 Cerber。

- DDoS 出租服務：分散式阻斷服務（DDoS）攻擊是一種常見的網絡攻擊形式，向目標網站或網絡投放過量的流量來使其癱瘓。

  DDoS 出租服務提供殭屍網絡，可隨時發動這些攻擊。 其中一個 DDoS 出租服務，被稱為 LizardStresser，是由臭名昭著的 Lizard Squad 黑客組織經營的，曾對遊戲服務和網站發動了多次引人注目的攻擊。

- 釣魚攻擊服務（PhaaS）：網絡罪犯為非技術人員提供了一個完善的界面，創建和管理釣魚攻擊活動。這些服務通常提供預先構建釣魚攻擊攻擊範本、釣魚網站的托管服務以及收集受害者數據的工具。 PhaaS 平台包括 BulletProofLink 及 EvilProxy 等等。

- 暗網市場：暗網是互聯網的一個部分，不會被傳統搜索引擎索引，需要特殊軟件才能訪問。

  暗網集中眾多市場，網絡罪犯可以在其中買賣各種 CaaS 產品和服務，例如惡意軟件、漏洞利用或被盜數據。其中最著名的暗網市場之一是 Silk Road (已被關閉)，罪犯們都以加密貨幣進行交易，雖然主要以販賣毒品而聞名，但也促進了非法數碼商品和服務的貿易。

保護自己免受網絡犯罪服務的侵害

隨著網絡犯罪服務的不斷增長和演進，個人和企業應採取積極措施來保護自己免受這些威脅。以下是保護自己的數碼資產的保安建議：

- 不要參與任何網絡犯罪活動和到訪暗網及其市場。
- 保持你的軟件和系統最新版本，減低已知漏洞被攻擊的風險。
- 為帳戶設置強度高和獨立的密碼，盡可能啟用多重身份驗證。
- 定期備份數據，以防被勒索軟件攻擊或遭遇其他數據丟失事故時，仍可以還原數據。
- 小心處理釣魚攻擊電子郵件和訊息，避免點擊可疑的連結或下載可疑的附件。
- 投放資源加強全方位網絡保安措施，例如防病毒軟件、防火牆和入侵檢測系統。

通過了解 HKCERT 最新的網絡保安威脅並遵循保安建議，可以大大減少成為網絡犯罪服務受害者的風險，並為每個人創建更安全的互聯網。

詳細資料可參閱HKCERT保安博錄
https://www.hkcert.org/tc/blog/unmasking-cybercrime-as-a-service-the-dark-side-of-digital-convenience

-完-

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