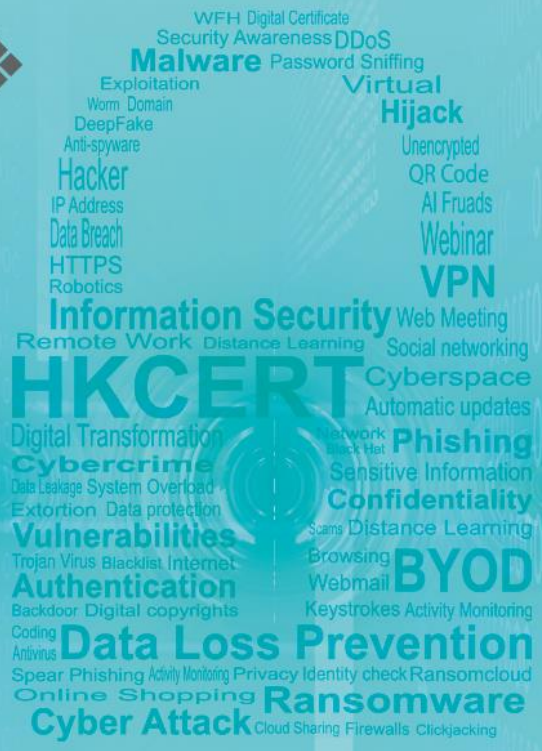
Hong Kong Computer
Emergency Response Team
Coordination Centre
HKCERT 香港電腦保安事故協調中心

香港保安觀察報告
2023 第三季度

發佈日期: 2023年11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

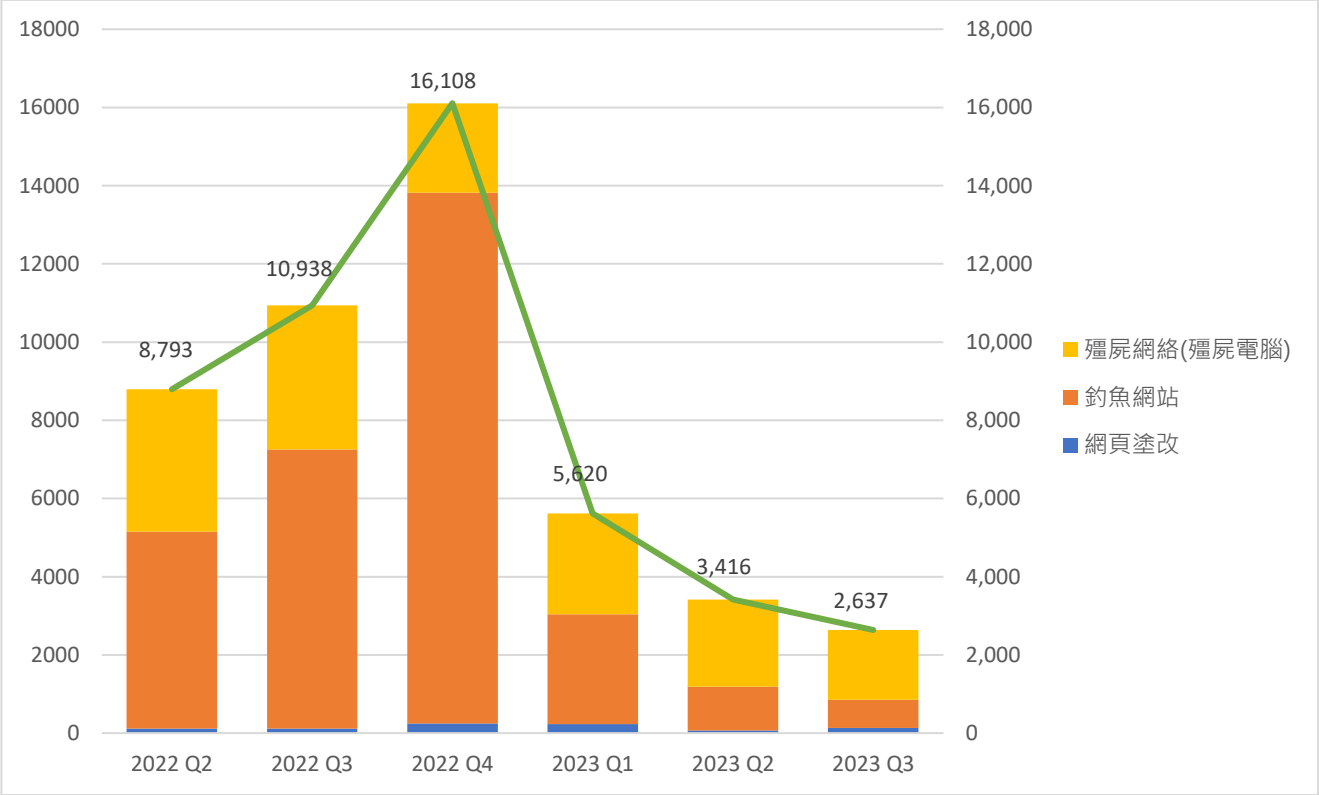
2023 第三季度報告概要

涉及香港的單一網絡保安事件宗數

2,637

按季下跌

22.8%↓

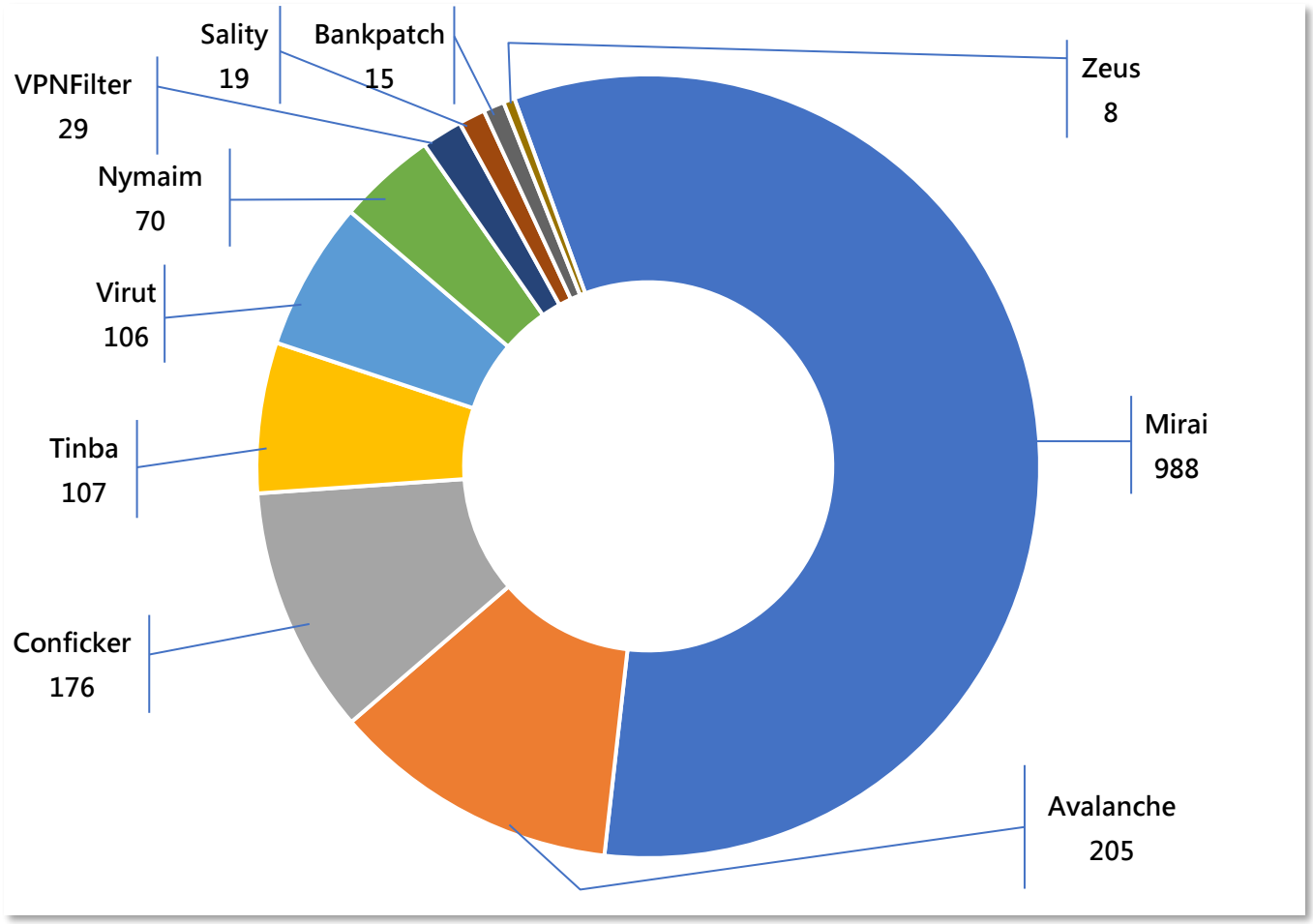


事件類別	2022 Q3	2022 Q4	2023 Q1	2023 Q2	2023 Q3	按季
網頁塗改	113	249	233	69	132	+91.3%
釣魚網站	7,141	13,574	2,804	1,120	722	-35.5%
殭屍網絡(殭屍電腦)	3,684	2,285	2,583	2,227	1,783	-19.9%
總數	10,938	16,108	5,620	3,416	2,637	-22.8%

香港網絡內的主要殭屍網絡

Mirai	Avalanche
988	205
↓19.8%	↓17.7%

Conficker	176	-16.6%
Tinba	107	-7.8%
Virut	106	-0.9%
Nymaim	70	-9.1%
VPNFilter	29	-56.1%
Sality	19	-38.7%
Bankpatch	15	-50.0%
Zeus	8	-73.3%



** 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。*

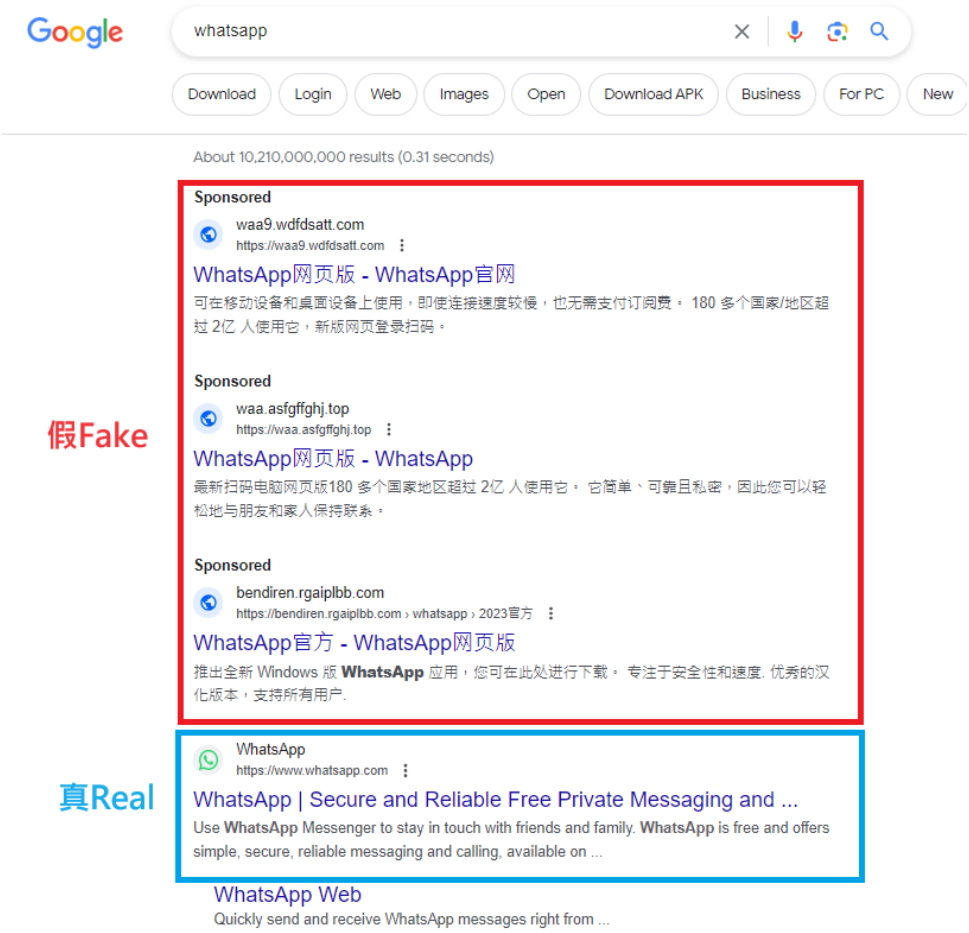
網絡焦點：保護你的WhatsApp帳戶，警惕針對香港WhatsApp騙案

近期，香港出現了一系列WhatsApp帳戶被盜的騙案，對公眾的個人私隱和資訊安全構成了嚴重威脅。為了保護市民的利益，香港電腦保安事故協調中心（HKCERT）特別提醒大家加強對WhatsApp帳戶的保護。以下會介紹騙案的運作方式，並提供一些預防措施，幫助市民提高警覺並保護自己的個人資訊。

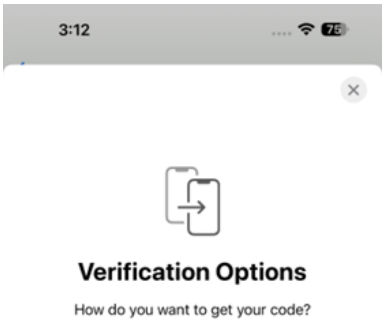
騙徒的目的多是騙財，他們會利用社交工程和技術手段，欺騙受害人掃瞄假WhatsApp網站(釣魚網站)的二維碼，或是盜取受害人帳戶的一次性驗證碼(OTP)，繼而控制其WhatsApp帳戶。一旦控制了帳戶，騙徒就可以冒充受害人，向其聯繫人發送詐騙信息，甚至進一步詐騙其他人。

近期HKCERT留意到騙徒甚至會透過刊登廣告，或搜尋引擎最佳化（Search engine optimization, SEO），將其精心設計的釣魚網站在搜尋引擎置頂，增加用戶點擊及受騙的機會。

於下一章節，HKCERT輯錄了大部份市民關心的問題，並提出解答及保安建議。

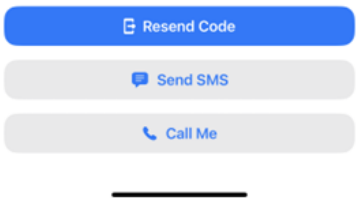


如市民帳戶遭盜用後，是否能即時奪回主導權？



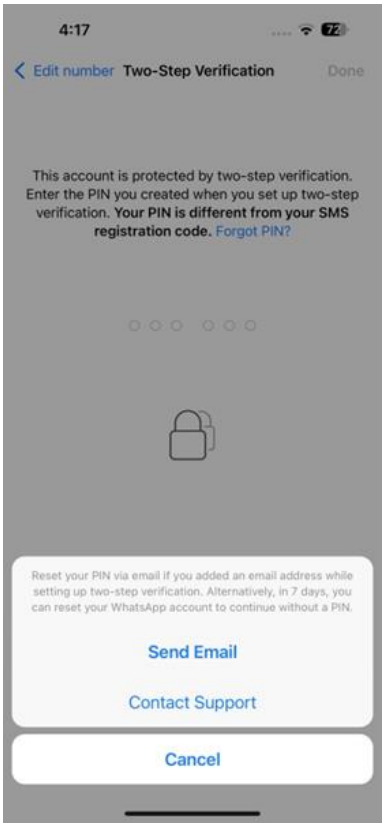
黑客一旦取得受害人的登入驗證碼後，便可以登入及盜用受害人的 WhatsApp 帳戶，與此同時，受害人亦會被強制退出自己的帳戶，WhatsApp 會顯示要求輸入手機號碼的畫面。然而如果此時受害人再以自己的註冊手機號碼登入，便可以奪回帳戶的主導權。

步驟如下：受害人只要再次輸人手機號碼登入，WhatsApp 會要求輸入一次性的驗證碼，此時用戶可等待並選擇透過以手機短訊（SMS）或來電方式，收取及輸入該驗證碼，完成後便可重新奪回帳戶的主導權。



當受害人再次登入帳戶時，會被要求輸入 WhatsApp 戶口的驗證碼。用戶應選取以 SMS 或來電方式收取該驗證碼。

啟動雙重認證功能是否有效保障帳戶？



是，啟動雙重認證能有效阻止黑客登入及盜用用戶的帳戶。

當啟動雙重認證後，用戶需要設定一個六位數字的 PIN 碼。設定完成後，即使有騙徒騙去用戶的登入驗證碼，並成功登入了用戶的帳戶時，騙徒還是會被要求輸入用戶預先設定的雙重認證 PIN 碼，才能使用用戶的 WhatsApp 帳戶。換句話說，設定雙重認證 PIN 碼後，黑客便無法奪取用戶的 WhatsApp 使用權。

騙徒若沒有用戶的雙重認證 PIN 密碼將不能使用用戶的 WhatsApp 帳戶。

假如原有賬戶未有啟動雙重認證，騙徒登入後啟用，是否就無法再奪回主導權？

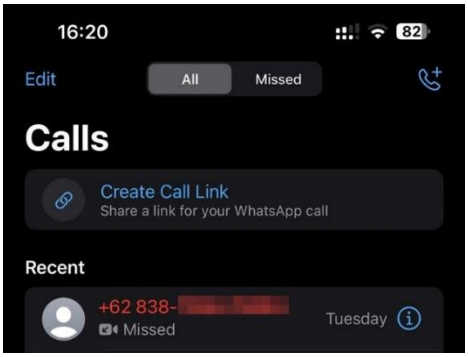
不是。如騙徒盜用了用戶的帳戶後啟動雙重認證，用戶亦可重新奪回主導權。

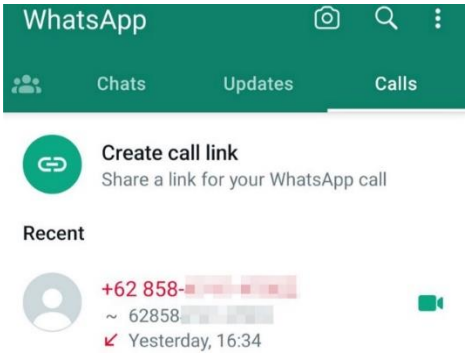
雖然當用戶再次登入帳戶時，WhatsApp 便會要求用戶輸入騙徒所設定的雙重認證 PIN 碼，用戶沒有該 PIN 碼便不能使用 WhatsApp。但是，據 WhatsApp 的官方指引，WhatsApp 會容許用戶七天後重設該 PIN 碼及重新登入。除了等待七天外，WhatsApp 亦允許用戶以預先設定的電郵地址重設 PIN 密碼。

不過無論用戶是否知道該 PIN 碼，只要用戶輸入 SMS 登入驗證碼後，對方便會被強制登出，不能再繼續使用用戶的 WhatsApp 帳戶。

WhatsApp 陌生視像來電頻繁出現

另外，有市民向本中心查詢，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。





為什麼攻擊者會利用陌生視訊通話，而不是正常的語音通話？

- 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。

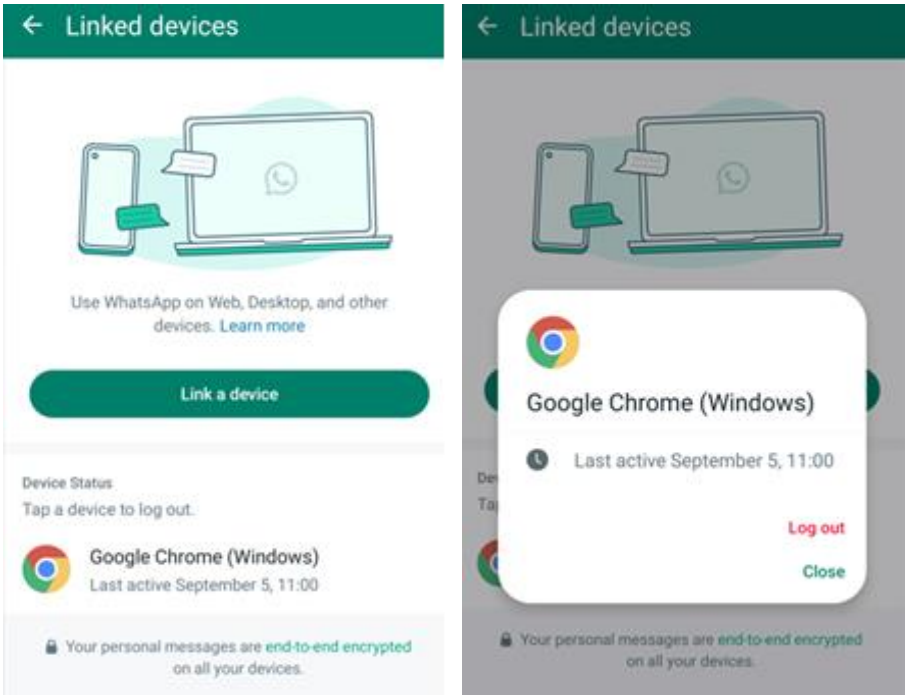
陌生視像通話有什麼風險？

- 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。

預防措施

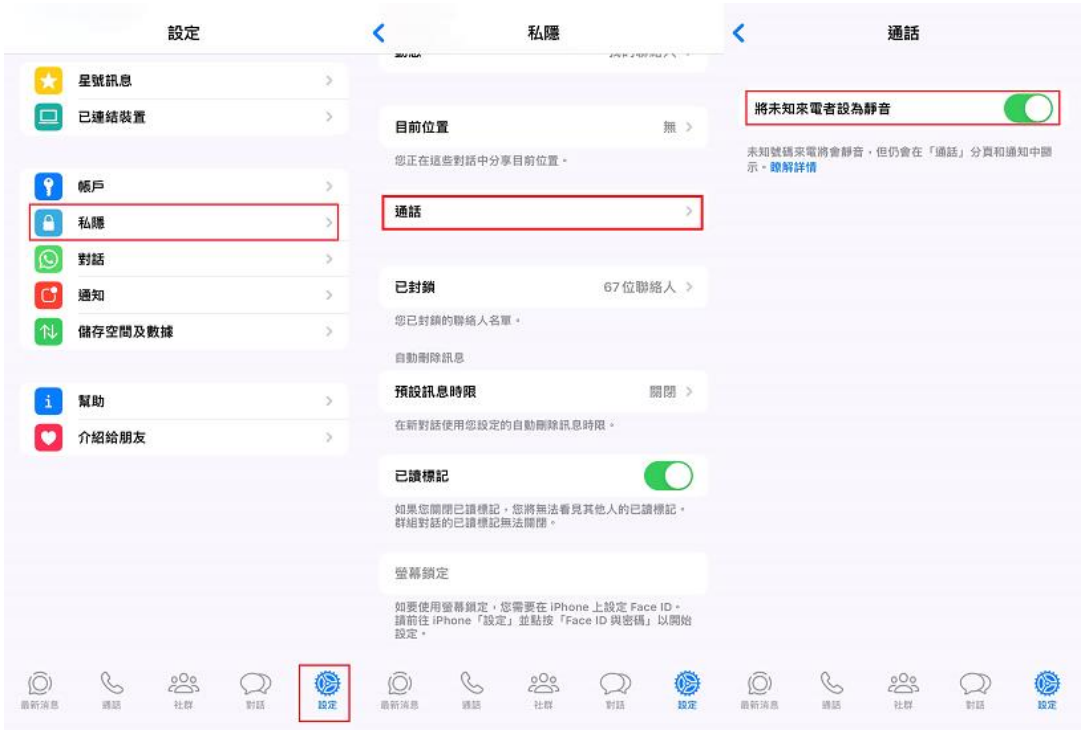
1. 加強帳戶安全性：
    - 設定PIN碼及定期更換：避免使用相同的PIN碼在不同的帳戶中，並可能新增電郵地址作PIN碼重設。
    - 啟用雙重驗證：在WhatsApp設置中啟用雙重驗證功能，這將為你的帳戶添加額外的安全層，需要輸入PIN碼才能登錄。
    - 不要共享驗證碼：不要將收到的驗證碼分享給任何人，包括親朋好友。騙徒可能通過詢問驗證碼來試圖控制你的帳戶。

- 定期在WhatsApp設定中檢查已連結裝置：登出不再使用的裝置連結。



「設定->已連結裝置」內的清單，如發現不明裝置，應立即登出該裝置。

- 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」）。



2. 警惕社交工程攻擊：

- 驗證身份：當收到涉及金錢或緊急情況的信息時，盡量通過其他渠道驗證發件人的身份。可以通過語音或視頻通話確認對方的真實身份。
- 謹慎點擊鏈接：不要隨意點擊來歷不明的鏈接，尤其是在收到不尋常或可疑信息時。這些鏈接可能包含惡意軟體或釣魚網站，這將危害你的帳戶安全。

3. 定期更新和保護設備：

- 更新應用程式：確保你的WhatsApp應用程式和設備操作系統是最新版本，以獲得最新的安全修補程序和功能。
- 安裝官方軟件：在你的手機或設備上安裝可信的安全軟件，以檢測和阻止惡意軟體的攻擊。

4. 提高警覺：

- 學習詐騙手法：了解不同類型的詐騙手法和常見的騙局模式，這樣你就能更容易地識別和避免詐騙。
- 與親朋好友溝通：與你的家人和朋友分享這些騙案的資訊，提醒他們保持警惕，並相互提醒不要輕易相信可疑的信息。

保護個人資訊和私隱是我們每個人的責任。在近期香港出現的WhatsApp帳戶被盜騙案中，我們應該加強對帳戶的保護，提高警覺，並嚴格遵守安全措施。通過使用強密碼、啟用雙重驗證、警覺社交工程攻擊、定期更新和保護設備，以及提高警覺，我們可以更好地保護自己的WhatsApp帳戶免受騙案的威脅。

詳細資料可參閱HKCERT保安博錄
https://www.hkcert.org/tc/blog/hkcert-alerts-the-public-on-preventive-measures-against-whatsapp-account-theft

2023年第二季度勒索軟件趨勢：亞太地區勒索軟件攻擊事故顯著增加，多重勒索持續流行，勒索軟件不斷進化

近年來，勒索軟件的不斷演變給企業帶來了嚴重的影響。最近的趨勢顯示，勒索軟件開發者更傾向於採取多重勒索策略。此外，他們開始針對以往較少關注的平台開發勒索軟件，例如macOS操作系統，並利用不同的技術手段來規避檢測，以及針對不同產品的漏洞進行攻擊，使得勒索軟件攻擊的檢測和防範變得更加困難。

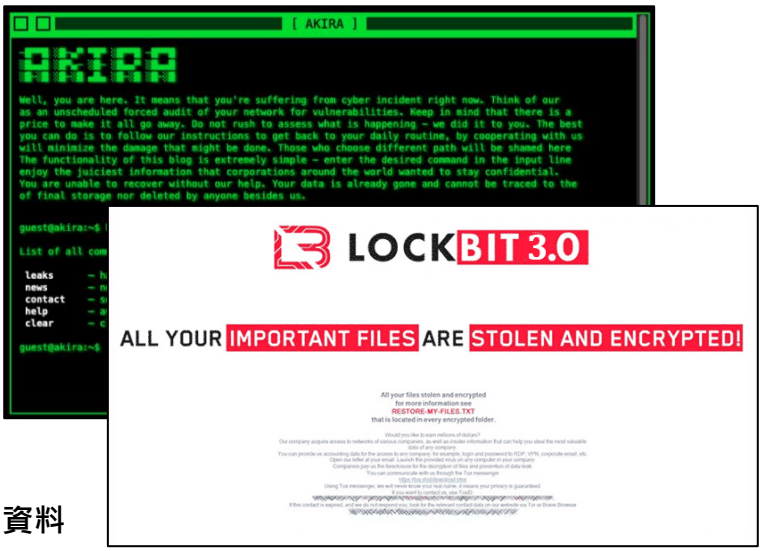
亞太地區勒索軟件攻擊事故顯著增加

針對亞太地區的勒索軟件攻擊事故數量顯著增加。根據網絡保安公司Check Point的研究，於2023年第二季度，全球每44個組織中便有一個組織遭受勒索軟件攻擊，而亞太地區的受攻擊數量相較於2022年同期更增加了29個百分比，顯示勒索軟件攻擊呈現上升趨勢。政府/軍事部門、醫療保健行業和教育/研究行業更是遭受勒索軟件攻擊次數最多的行業。此外，公用事業、保險/法律和顧問機構受勒索軟件攻擊次數也有顯著增加。美國加

> 州一家連鎖醫院近日更因勒索軟件攻擊而被迫暫停大部分資訊科技服務，影響17間醫院及166間診所服務。因此，相關行業及機構應該加強網絡安全措施以保護自身。

最近在香港發生了因勒索軟件而導致資料外洩的事件，例如數碼港、消費者委員會和香港芭蕾舞團等機構都成為受害者。這些事件提醒我們個人資料的重要性，以及保護自己免受勒索軟件攻擊的必要性。本文旨在向公眾提供有關勒索軟件的相關知識，並強調保護個人資料的重要性，以幫助大家提高警覺並採取適當的防範措施。

勒索軟件的威脅



勒索軟件是一種惡意軟件，它可以入侵你的電腦系統並加密你的檔案。攻擊者隨後會要求支付贖金（通常以加密貨幣形式）以解密你的檔案。這種攻擊對個人和組織都造成了極大的損失，包括資料丟失、財務損失和聲譽損害。

資料外洩事件的影響

數碼港、消費者委員會和香港芭蕾舞團等機構的資料外洩事件引起了廣泛關注。這些事件顯示了個人資料外洩的嚴重後果，包括個人私隱被侵犯、身份盜竊和金融詐騙等。這些事件提醒公眾，無論是個人還是組織，保護個人資料是一個迫切的任務。

多重勒索持續流行

根據網絡保安公司 Palo Alto Networks Unit 42 的研究，截至 2022 年底，平均約 70% 的勒索軟件案例發生數據盜竊。與 2021 年中期相比數字顯著增加，當時平均只有約 40% 的勒索軟件案例發生數據盜竊。另外，根據網絡保安公司 Cisco Talos 的研究，與 2023 年第一季度相比，2023 年第二季度的數據盜竊勒索個案數量大幅增加了 25%。可見多重勒索持續及數據盜竊有上升趨勢。在這種類型的攻擊中，勒索軟件團伙會勒索受害者組織，如果不支付贖金，就會在暗網上洩露被盜數據。

而最近，夏威夷社區學院更向勒索軟件團伙支付贖金以防止數據洩露，勒索軟件團伙收到贖金後雖然已將相關機構條目從數據洩露網站中刪除，但無法排除可能將來會繼續勒索受害者或洩露數據。

勒索軟件推陳出新不斷進化

知名的勒索軟件團伙和勒索軟件服務供應商 LockBit 近期推出了針對蘋果 macOS 設備的勒索軟件變種。根據網絡安全公司 Uptycs 的研究發現，勒索軟件服務供應商 Cyclops 開發了可感染三個主要操作系統（Windows、Linux 和 macOS）的勒索軟件。這表明勒索軟件團伙越來越多地以不同的系統為目標。另外，有一種新的勒索軟件 Cactus 會利用 VPN 設備的漏洞來獲取受害組織的網絡初始訪問權限及感染受害組織裝置，而 Cactus 與其他勒索軟件不同之處在於會對勒索軟件自身進行加密。通過對自身進行加密，使其可以逃避防毒軟件和網絡監控工具的檢測，使它能夠繞過這些安全措施並在不被發現的情況下進行惡意活動。

根據網絡安全公司 Cisco Talos 和 Vmware 的研究，2023 年第二季度出現了兩個新的勒索軟件活動，分別為 8Base 和 MoneyMessage。8Base 最早於 2022 年三月被發現，從 2023 年六月開始活動急劇增加。8Base 利用客製化的 Phobos 勒索軟件進行數據盜竊及文件加密勒索，而 Phobos 勒索軟件是在地下市場以勒索軟件即服務（RaaS）的形式販售。而 MoneyMessage 勒索軟件活動於 2023 年三月首次被發現，與 8Base 類似其採用相同的雙重勒索模式。鑑於勒索軟件活動的不斷增加，我們必須積極採取措施來減輕勒索軟件攻擊帶來的風險。

積極利用產品漏洞進行攻擊

不同的勒索軟件團伙正積極利用產品漏洞來竊取數據。例如，Bl00dy、Clop 和 LockBit 勒索軟件被發現針對 PaperCut、GoAnywhere MFT 和 MOVEit Transfer 等產品漏洞發起攻擊，以竊取數據或將其用作橫向傳播的跳板。 其中，PaperCut 是一種廣泛應用於企業和教育機構的打印機和文檔管理解決方案，而 GoAnywhere MFT 和 MOVEit Transfer 是一種企業級文件傳輸和協作平台，提供安全的文件傳輸和共享功能。

採取措施加強防禦

勒索軟件不斷進化，攻擊者不僅關注不同操作系統，還在不斷開發新的技術和手段來規避檢測和加強攻擊效果。這對網絡安全和數據保護構成了重大挑戰，更突顯組織和個人在加強安全意識和採取有效的防護措施的迫切性和重要性。

本中心建議用戶及系統管理員應保持警惕並採取適當的防護措施：

一般用戶：

1. 定期更新和升級系統和應用程序，包括操作系統和防病毒軟件；

2. 定期更改密碼及使用多因素身份驗證（MFA）來增加帳戶的安全性；
3. 定期備份重要文件和數據，並將備份存儲在離線和加密的位置；
4. 定期進行網絡安全培訓，以了解最新網絡威脅及提高員工識別網絡攻擊的能力。
5. 謹慎使用公共 Wi-Fi，避免訪問敏感資料或進行金融交易。使用虛擬私人網路（VPN）來加密你的網路連接，保護你的數據免受攔截。
6. 謹慎對待電子郵件和附件，不要打開來歷不明的電子郵件或附件，以免觸發惡意軟體或勒索軟體。

系統管理員：

1. 儘量減少擁有特權訪問權限（如網域的管理權限）的用戶數量，以限制攻擊範圍及影響。日常的操作亦只應使用沒有特權訪問權限的普通賬戶；
2. 加強網絡基礎架構，減少暴露於互聯網當中的端點；
3. 安裝終端保安解決方案，可以檢查電郵和網絡內容中的惡意下載內容，檢測和隔離惡意程式碼，以防止感染惡意軟件；
4. 架構網絡威脅情報平台，以追蹤最新的威脅，並與同行組織交流信息，預先阻止新出現的攻擊；
5. 設置網絡監控和保安檢測，一旦發現任何異常的網絡活動，立即進行事故響應。

總括而言，近期在香港發生的勒索軟件事件提醒我們保護個人資料的重要性。我們應該增強對勒索軟件的認識，並採取適當的防範措施，例如更新系統、謹慎對待電子郵件和附件、建立強大的密碼、謹慎使用公共 Wi-Fi 和備份重要資料等。保護個人資料不僅關係到個人私隱，還關係到金融安全和聲譽保護。讓我們共同努力，提高警覺並保護我們的個人資料免受勒索軟件的威脅。

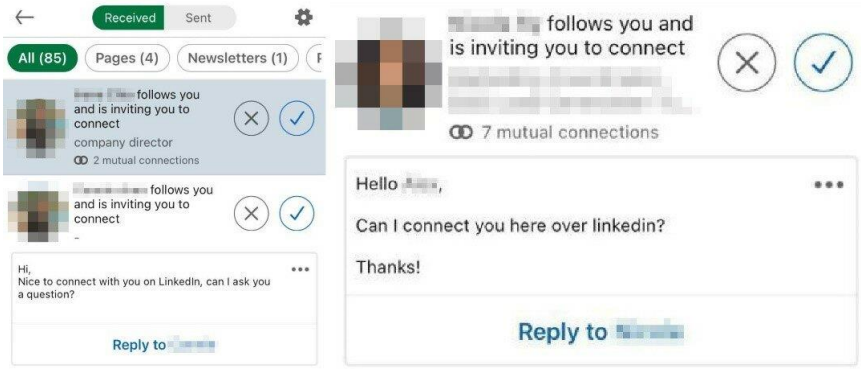
如想了解更多詳情或保安建議，可參考保安博錄「揭開網絡犯罪服務的神秘面紗：數碼便利的陰暗面」或《中小企保安事故應變指南》。

詳細資料可參閱HKCERT保安博錄
https://www.hkcert.org/tc/blog/ransomware-trends-q2-2023-surge-in-attacks-across-asia-pacific-persistent-multiple-extortion-and-evolving-threat-landscape

社交媒體防詐騙全攻略：設定防禦，守護個人資訊

社交媒體已成為人們日常生活不可或缺的一部分，卻也吸引了不法之徒虎視眈眈。香港電腦保安事故協調中心（HKCERT）提醒大眾提防社交媒體詐騙，並時刻保持警覺。在此，HKCERT將深入探討如何提高社交媒體用戶的警覺，從而更有效地遏制網絡詐騙活動。另外，在文章稍後部份亦提供一些使用Facebook及LinkedIn安全設定的示範，藉此減少他人查閱個人用戶資料的機會。

雖然科技發展為公眾帶來便利，但同時增加不法分子的攻擊渠道。用戶有責任保護自己的帳戶及個人資訊。以下是防止社交媒體詐騙的建議：

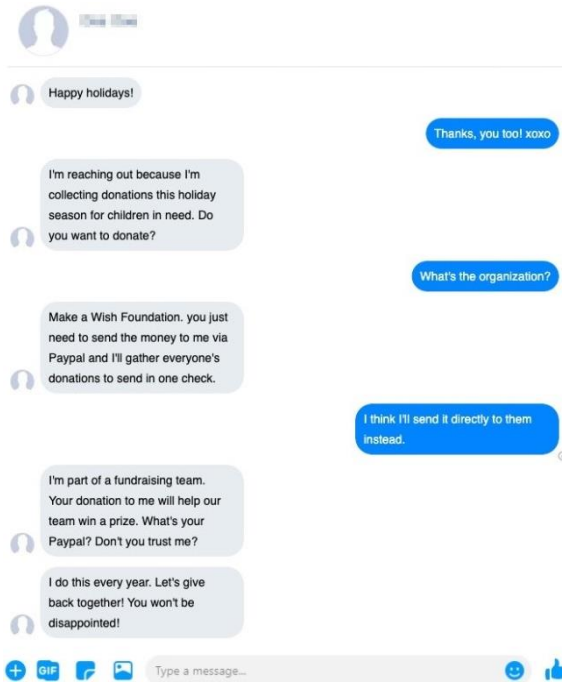


小心處理陌生人的聯繫

只要於網絡上與陌生人互動，就存在風險。應檢視陌生人的個人資料，確定是否可信，再考慮選擇給予回覆。相同頭像但不同姓名人士嘗試發出交友邀請。

切勿分享個人敏感訊息

不要讓陌生人得知你的全名、地址、電話號碼、銀行資料或密碼等敏感訊息。嘗試向用戶提出問題，以獲取資訊。



多加留意可疑「跡象」

如陌生人表現急切、提供不切實際的好處或要求用戶捐款，即可能存在詐騙意圖。對答表現急速，如希望用戶投放資金。

加強帳戶保護

通過強密碼、多重驗證及簡訊驗證碼等方式，加強社交媒體帳戶的安全防護。同時，部分社交媒體會設有網絡保安指南網頁，提供有關設定予公眾參考。

定期檢視帳戶私隱及安全設定

確保社交媒體帳戶的私隱設定配置正確，令上載的資訊只公開予指定用戶。

報告可疑行為

如對詐騙存在懷疑，立即向相關社交媒體平台及執法部門舉報。

社交媒體提供了許多便利，但同時也帶來風險。用戶須學會提高警覺，小心處理所有陌生人的聯繫，並對可疑跡象保持審慎。只有如此，才能享受社交媒體的好處，同時免受網絡詐騙的侵擾。

Facebook 及 LinkedIn 會提供各種安全設定予用戶選用。
以下是其中一些例子：

Facebook安全設定（建議）
如有任何有關Facebook疑問，可參閱：https://www.facebook.com/help

- **定期更改密碼 （培養定期更改密碼習慣。如遇上任何安全問題時應立即變更密碼。 ）**

- **啟用雙重驗證（啟用後，除了登入密碼外，用戶登入時需要使用額外驗證方式用作核實個人身份，減少被黑客入侵機會。例如驗證應用程式、簡訊或安全性金鑰。 ）**

- **限制他人透過其他方式搜尋自己（可以限制其他人用電話、電郵或 Facebook 以外搜尋引擎找到自己。）**

- **限制所有人檢示自己的個人檔案帖子（可以減少更多個人資料外洩）**

LinkedIn安全設定（建議）

如有任何有關LinkedIn疑問，可參閱：https://www.linkedin.com/help/linkedin?lang=zh-hant

- **定期更改密碼（培養定期更改密碼習慣。如遇上任何安全問題時應立即變更密碼。）**

- 啟用雙重驗證（啟用後，除了登入密碼外，用戶登入時需要使用額外驗證方式用作核實個人身份，減少被黑客入侵機會。例如驗證應用程式及簡訊。）

- 限制他人透過其他方式搜尋自己（可以限制其他人用電話、電郵或 LinkedIn 以外搜尋引擎找到自己。）

- **限制所有人檢示自己的個人檔案帖子 （可以減少更多個人資料外洩）**

以上建議只供用戶參考。用戶可以更據自己的喜好及用途自行決定安全設定的設置。希望此文章能為大眾提供更多提高警覺的方法，以有效抵禦社交媒體詐騙。

詳細資料可參閱HKCERT保安博錄
https://www.hkcert.org/tc/blog/comprehensive-guide-to-social-media-scams-setting-up-defense-to-safeguard-your-personal-information

完

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