奪臉合成不雅片 侵手機勒索贖金

威脅放片給苦主親友「綁架App」挾持案件倍增

新聞追蹤

資訊發達的年代，都市人幾乎是手機不離身，通訊軟件更是生活必需品，有沒有想過這些通訊軟件戶口可以成為不法分子綁架你的「肉參」（人質）？警方過去兩年接獲有關網上勒索、電腦被盜用等案件多達1,255宗至近1,500宗，比2019年及2018年勁升1至3倍。一名深受手機勒索案困擾的苦主近日向香港文匯報講述，早前有不法分子挾持她的WhatsApp戶口，又用她的名義開設WhatsApp群組，將她手機上所有聯絡人拉入群，然後將苦主的肖像以合成方式偽造一段不雅影片，要求苦主支付「贖金」，否則便將不雅影片發到群組上，或逐個朋友發放影片，使苦主身敗名裂。雖然事件最後報警處理，警方介入調查疑負責收取贖金的銀行戶口持有人，但該不雅影片仍是苦主的「痛腳」，擔心不法分子隨時廣發影片報復。

◆香港文匯報記者 劉明

◆都市人幾乎手機不離身，通訊軟件更是生活必需品，然而，近年網上勒索、電腦被侵入盜用等案件倍增，市民須高度警惕。 香港文匯報記者 攝

不法分子挾持市民手機WhatsApp賬戶的常用手法主要有三種，包括冒認是事主朋友要求轉發賬戶的驗證碼、誘騙事主在手機輸入「飛線」的 指令，或者向事主發送虛假的WhatsApp 網頁連結，然後用各種方法誘騙事主按下連結，內含的木馬程式便在不知不覺間入侵事主手機，方便騙徒盜取手機內資料，包括電話號碼、SMS、密碼、通訊錄等。

冒苦主名義拉所有聯絡人入群組

本身是iPhone用戶的Amy（化名）早前手機便遭犯罪分子入侵，她接受香港文匯報訪問時說：「我懷疑手機中了木馬病毒，被犯罪分子取得手機內的資料，但我不清楚中毒的經過，連幾時中毒都不知道！」中毒不久後，她才如夢初醒。

有天，其WhatsApp賬戶突然用她的名義開設一個通訊群組，一口氣加入手機內的所有聯絡人，但群組成立後「綁匪」一直沒有動靜，不少朋友在群組上問Amy將他們拉入群的原因，但Amy根本無法控制WhatsApp賬戶更無法解釋，其後有朋友不耐煩便退群，可惜不久後又被拉入群。未幾，Amy打電話向群組上的朋友解釋及求助，朋友便在群組上留言指Amy賬戶被挾持，提醒其他朋友不要打開群組內發出的任何連結。

不雅片先傳事主「不想影片出街就畀錢」

正當Amy一籌莫展之際，她收到「綁匪」傳來的一條以合成技術製造的虛假不雅影片，片中「主角」正是Amy的模樣，「他們給我看一段影片，說你不想影片出街就給他們錢，然後亦都給我看他們已經拿到了我的我通訊錄。」

「綁匪」更來個下馬威，根據通訊錄知道Amy母親的聯絡電話，於是給母親也發不雅影片，似是警告Amy不要以為他們說說而已，然後「綁匪」提出要一萬多港元的贖金，「他們給我一個本地銀行的戶口轉賬，（戶口）有名，但他們聲稱有時限，說15分鐘內戶口就失效。」

Amy思前想後還是決定報警處理，警方馬上協助重奪WhatsApp賬戶的控制權，但由於不雅影片仍在「綁匪」手上，隨時會報復，「警方都說阻止不了他們發布（影片）。我都不知道是不會send（發布影片）還是遲點會send。」事後，Amy到手機店「洗機」重置手機，「不過其實都還會擔心木馬是否還在。」

黑客騎劫WhatsApp賬戶途徑

騙取WhatsApp認證碼

▶WhatsApp規定，若以新手機登入原有賬戶，需要在舊有手機上輸入認證碼。

黑客用手上的手機登入事主WhatsApp賬戶，當被要求在舊手機輸入認證碼時，便假冒是事主的朋友或自稱是WhatsApp團隊，誘騙對方事主的WhatsApp賬戶便成功轉到黑客手上的手機中

有毒連結

▶發放虛假的WhatsApp 網頁連結，要求事主按下連結，木馬程式隨即植入事主手機內，騙徒便能輕易取得手機內所有資料

▶騙徒以各種方法誘騙事主在手機輸入由*、#以及數字組成的短碼，其實這組數字是電訊商供用戶「飛線」的 指令，輸入後所有來電都轉至騙徒手機中

特稿

多屬跨境犯罪 警破案難度高

「綁匪」勒索贖金時曾向Amy提供一個本地銀行戶口收取贖金，但與「綁匪」周旋過程中，從用語、字眼及簡體字來看，Amy懷疑「綁匪」是非香港本地人。面對跨境罪案，增加香港警方的破案難度，「不知道最後能否拘捕有關的幕後犯罪分子。」

對於Amy表示犯罪分子以合成技術製作虛假影片，香港智慧城市聯盟資訊科技管理委員會主席龐博文接受香港文匯報訪問時直言，其實該技術並不高深，利用換臉技術就能製作虛假影片，「在手機內取得受害人的照片後，以人工智能技術將其樣貌合成到色情影片中，外國也有不少名人和影星成爲換臉技術的受害人。」

專家建議追查借出賬戶者

犯罪分子提供本地銀行戶口給Amy過數付款，但由於事件涉及跨境罪犯，要揪出幕後黑手有一定難度。大律師陸偉雄建議，警方可循此追查戶口持有人，「當然不少戶口持有人是借出戶口收錢，未必追查到幕後的犯罪分子，但借戶口也會觸犯洗黑錢罪行，就算只捉到借戶口的蝦毛，打不到眞正老虎，都要抓人，抓十個蝦毛，可能找到線索抓背後的大老虎。」

◆香港文匯報記者 劉明

專家之言

冒認親友扮大師 最終目標是騙錢

有電腦保安專家指出，近年入侵手機的情況以盜用社交程式WhatsApp最多，不法分子騙取手機用戶的WhatsApp驗證碼後，會取得手機用戶的聯絡人資料及假扮事主行騙，例如冒認事主向「朋友圈」內人士要求購買點數卡、開設投資群組行騙，以至用裸聊或虛假影片勒索事主等，故手機用戶要小心不法分子冒認是相識的親友行騙。

木馬程式可控制對方手機裝置

香港智慧城市聯盟資訊科技管理委員會主席龐博文接受香港文匯報訪問時表示，手機遭入侵的情況時有發生，他個人每月也接獲近20宗求助，而入侵手機的方法包括利用木馬程式以及盜取用戶的WhatsApp，「用木馬程式比較複雜，主要是騙取用戶按其發出虛假訊息的連結，以植入病毒，而木馬程式可控制對方的手機或電腦等裝置，盜取其電子裝置內所有的資料，如聯絡人及銀行賬戶密碼等。」

至於盜用WhatsApp賬戶則簡單得多，「例如犯罪分子假扮WhatsApp團隊，用短訊或WhatsApp聯絡你要求提供驗證碼，如果拿到了你的驗證碼，犯罪分子就可以盜用你的賬戶。」他表示犯罪分子因此可假扮事主向「朋友圈」內的親友行騙，其中包括騎劫事主的WhatsApp賬戶，要求親友幫其購買點數卡並提供點數卡的密碼，另外有犯罪分子則入侵一些財經名人的賬戶，以其名義開設投資群組，「扮個大師騙人投資」，又或以事主名義開群組提供「炒散」工作，騙取他人提供銀行戶口等資料。

手機內有裸聊影片更易被勒索

他又指，犯罪分子除可用人工智能技術製作合成的虛假不雅影片勒索外，若用戶手機內有裸聊影片，亦可能遭犯罪分子作勒索用途。

「其實好多人都可能有裸聊，我都收過10多個涉及裸聊勒索的求助，而製作虛假影片都要花時間，但如果找到你手機已有裸聊影片就簡單好多，直接用來勒索你，不給錢就發給WhatsApp內的聯絡人。」

龐博文說，若使用iPhone手機，其iOS系統較其他手機使用的安卓系統安全程度高，但若然iPhone用戶「越獄」，即突破iOS系統的限制安裝遭官方禁止上架的應用程式，則會降低手機的安全性。

此外手機會不時提供更新，以修補一些漏洞，用戶應按要求更新手機，減低手機被入侵的機會。

◆香港文匯報記者 劉明

警方接獲裸聊勒索、網上勒索及盜用電腦案件宗數

年份	裸聊勒索	網上勒索（不包含裸聊勒索）	盜用電腦	合共
2018年	281	223	224	728
2019年	171	129	71	371
2020年	1,009	135	111	1,255
2021年	1,159	158	142	1,459
2022年（1-3月）	348	39	37	424
總數	2,968	684	585	4,237

四大自保方法

▶切勿開啓來歷不明的連結

▶啓用雙重認證功能——於WhatsApp「設定」功能中，找「賬號」內的啓用「雙步認證功能」功能。啓動後，若在另一手機登入該WhatsApp賬戶，除了需要使用電話號碼（SMS / 語音）認證外，還要輸入自訂的密碼

▶切勿安裝非官方App

▶安裝防毒軟件

資料來源：香港警務處

整理：香港文匯報記者 文森