

挪用存款掃高「搭棚」獲利30%即拋售 黑客侵股民戶口炒仙股

網絡黑客「大時代」來臨，投資股票散戶亦要提防戶口被入侵利用「托市」。跨國黑客集團先鎖定某「仙股」，透過入侵香港銀行或證券行的股票戶口，擅自挪用他人存款大手掃貨「搭棚」，炒高股價兩至三成即拋售獲利。香港警方自去年下半年起，接獲多宗未經授權的股票交易舉報，涉及八間銀行或證券行合共56個戶口，涉及交易款項超過5300萬元。弔詭的是，部分戶口被侵入的受害人實際並無金錢損失，有個別戶主更因股價炒高而獲意外之財。

大公報記者 陳卓康

警方今年截至上周五，共接獲四間網上銀行26個戶口、三間證券公司共七個戶口，懷疑曾被未獲授權第三者入侵作出的股票交易，涉及戶口內款項合共5300萬元，較去年全年數目多出一倍（詳見附表），至今未有人被警方拘捕。網絡安全及科技罪案調查科總督察許綺惠昨稱，黑客集團入侵股票戶口後，自行操作以大手買入某特定股票，炒高股價後賺取差價，戶主直至收到銀行就交易發出的手機短訊而起疑，或因股價大幅波動引起證監會注意，始揭發案件。

東歐過江龍來港搵食

網罪科行動組高級督察葉卓譽解釋，犯罪集團多看中一些市值低於三億元、創業板上市公司的股票，特點是價值低和流通量少，俗稱「仙股」，公司的業務性質並非考慮因素。股民戶口款項實際並無被提走或減少，只是被用作購買股票，有個別被入侵戶口的股民，反因股價被推高又及時賣出而獲利。

警方與證監會去年揭發一個來自東歐國家的犯罪集團，先透過中介公司在香港合法開戶，持有某低價股票後，以海外IP地址電腦侵入20個股票戶口，將股價炒高20%至30%後便放售，務求「密食當三番」，並避免大幅波動引起證監會注意。探員



▲金管局指出，股民戶口被黑客入侵用作炒股，不用承擔損失
資料圖片

比對交易紀錄發現，每次某一公司股票被接連大手購入，中介公司總能及時從高價賣出，揭發時集團已運作約兩星期，曾沾手約10隻股票。

每日炒作不同公司股票

葉卓譽指，從集團多次犯案模式可見，所有交易均於同一時段上午或下午完成，同一時間只控制一間公司的股價，「星期一做A公司，星期二做B公司……」由於因港股奉行「T+2」制度，警方利用兩個交易日後交收的時間，成功凍結犯罪集團戶口款項，案件正等候律政司意見決定起訴。據悉，涉案的黑客除佷大機會干犯「有犯罪意圖或不誠實取用電腦」刑事罪行，視乎案情更可能干犯欺詐、造市、操控價格等罪行。

警方仍在了解黑客入侵的手法，許綺惠估計，黑客是透過假扮事主熟人發出電郵，誘騙其按下附有惡意程式的超連結，令事主電腦無形感染「keylogger」或木馬電腦病毒，從而截取事主電腦按鍵輸入的所有紀錄，取得銀行或證券行股票戶口的登入帳號和密碼。

她呼籲市民不要打開不明來歷電郵附件，特別是當對方用語有異，或突然傳送特大附件的電郵，亦不應隨便使用公眾網絡登入銀行戶口。



▲金管局及警方網絡安全及科技罪案調查科講述黑客入侵股民戶口的個案
大公報記者何嘉敏攝

未經授權股票交易案件				
涉及機構數目*	2016年 (截至6月24日)	2015年	2016年 (截至6月24日)	2015年
	網上銀行		證券交易公司	
涉及機構數目*	4間	1間	3間	1間
涉及戶口數目	26個	1個	7個	22個
涉及交易總額	4100萬港元	80萬港元	1200萬港元	2600萬港元
涉及戶口（網上銀行+證券交易）			2016年 (截至6月24日)	2015年
涉及總交易金額（網上銀行+證券公司）			33個	23個
*因有同一機構涉及不止一案，2015年及2016年間實際涉及4間銀行及4間證券公司			5300萬港元	2680萬港元
資料來源：香港警務處				

新勒索軟件CryptXXX襲港

【大公報訊】記者陳卓康報道：加密勒索軟件接連襲港，繼早前Locky之後近日又出現「CryptXXX」，網民登入惡意網站或網上廣告即中招，一旦被入侵，電腦所有檔案被加密無法打開，黑客勒索Bitcoin（比特幣）作贖金。據了解，「CryptXXX」近期「變種」，能夠偵測電腦內的Bitcoin帳戶，自動偷去戶主的Bitcoin。警方提醒，電腦用戶應經常把重要資料備份，不要把備份資料連接電腦，不要瀏覽可疑網站，或從可疑網站下載任何檔案。

網罪科總督察許綺惠指出，被「CryptXXX」加密的電腦的檔案被加上「.crypt」、「.crypz」或「.crypt1」副檔名，被「CryptXXX」版本3.0或以上版本

加密的數據將無法復原，大部分個案均透過到訪被入侵網站受感染，主要是使用過時或未修補的瀏覽器(如IE)或插件(如Flash Player)，某些附載於正常網站的橫額廣告亦可導致使用者裝置受感染。

「CryptXXX」的傳播途徑有別於Locky，不是依賴發送垃圾電郵，而是利用被入侵的網站和網上惡意廣告載入漏洞攻擊包，如帶有Angler漏洞攻擊套件進行感染。漏洞攻擊包是一種上載及執行惡意程式碼的軟件系統，當受害者電腦的瀏覽器被引導至寄存漏洞攻擊包的網站後，漏洞攻擊包便會攻擊瀏覽器及相關應用程式插件，例如Adobe Flash及Reader等，使系統不知不覺地感染惡意程式。

警拘七黑漢涉襲上市公司執董

【大公報訊】本月中一名上市公司執行董事在灣仔出席飯局後，突然被十多名大漢在街頭打傷，警方接手調查後，昨在



▲涉嫌襲擊上市公司執行董事的疑人被探員押走

灣仔及將軍澳拘捕七名男子，他們全部有黑幫背景，警方初步相信案件涉及商業糾紛，正追捕其餘同黨及幕後主腦歸案。

遇襲男子姓張（49歲），是一間上市公司執行董事，與其一同遇襲男友人則姓施（25歲），據悉兩人均從事融資生意。本月十六日晚上十時許，兩人在灣仔謝斐道近杜老誌道出席一個飯局後，擬登上一輛七人車離開時，突遭十多名大漢包圍襲擊。灣仔反黑組接手調查，警方昨日先後在灣仔及將軍澳拘捕七名男子（17至67歲），全部有黑幫背景，當中六人涉嫌參與當日的襲擊行動，一人則參與襲擊策劃，案件仍在調查中，相信稍後會有更多涉案人士被捕。

警破三公屋外圍波賭檔

【大公報訊】警方在歐洲國家杯賽事期間持續採取代號「戈壁」的行動，打擊非法外圍賭博，昨五小時內先後在沙田、天水圍及大埔，破獲三個以公屋單位收受外圍波賭注的賭檔，拘捕三名涉案男子，



▲警方在博康邨內帶走一名涉嫌非法收受波賭男子

合共檢獲1900萬元的波籤記錄。警方呼籲市民切勿參與非法賭博。

新界南總區重案組昨早十一時許突擊搜查博康邨一個單位，檢獲約100萬元「波籤」記錄及約五萬元現金，姓蘇（64歲）男子涉嫌非法收受賭注被捕扣查。中午12時許，新界北總區重案組人員亦掩至天水圍天慈邨一單位搜查，當場拘捕一名涉嫌非法收受賭注的黎姓（31歲）男子，檢獲約200萬元「波籤」記錄及約8700元現金、兩部手提電話及兩本帳簿等。下午三時許，新界北總區重案組人員再掩至大埔富亨邨亨泰樓一公屋單位搜查，檢獲約1600萬元「波籤」，拘捕姓何（35歲）男子。

新購氣體爐爆炸 女戶主危殆印傭重傷

【大公報訊】深水埗一住宅單位，昨日發生懷疑煮食爐爆炸意外。單位內女戶主及印傭被炸傷，幸爆炸未引起火警，主僕兩人送院救治，女戶主危殆，機電工程署到場調查證實涉事氣體煮食爐有「GU」標誌，合乎標準，已將之連同配件檢走作進一步調查。

疑氣體積聚 撻火即爆炸

被炸傷兩主僕送往瑪嘉烈醫院救治時仍清醒，女戶主姓莊（55歲），面及手部燒傷，其後被轉送到瑪麗醫院留醫，情況危殆，一同受傷的女傭ANITA（33歲），手及腳部有燒傷，轉送廣華醫院留醫，情況嚴重。

事發於北河街179號龍安大廈五樓一

單位，屋主是一對姓莊兩姊妹，兩名傷者是大姊及家中印傭。據悉，莊家剛在前日更換了新的氣體煮食爐，並由技工上門安裝及更換新一罐10.5公斤的石油氣。

昨早十一時許，印傭入廚房使用該具新購置的煮食爐，其間懷疑積聚氣體，在「撻火」期間發生爆炸，她與女戶主首當其衝被燒傷，驚動莊妹報警。警方接報與消防員趕至，發覺爆炸並未引起火警，由救護員將受傷兩主僕送院。警方與消防初步調查懷疑發生氣體泄漏，印傭操作煮食爐時發生氣體爆炸，事件無可疑。

換氣罐一日只剩一半氣體

稍後，石油氣代理商及機電工程署人員先後到場。據悉，代理商證實該罐10.5

黑客炒股犯案手法

- 1) 藉載有惡意程式的欺詐網站、詐騙電郵等，盜取受害人股票戶口登入帳號及密碼
- 2) 在海外透過中介公司開設的股票戶口，從低價位購入X公司大量股票（如50萬股，每股0.2元）
- 3) 一小時內先後入侵多名受害人帳戶，各買入數十萬股X公司股票，令股價極速攀升（如0.27元）
- 4) 收市時以高價拋售手上所有X公司股票，賺取約20%至30%差價

戶口被入侵 股民毋須承擔損失

【大公報訊】記者陳卓康報道：股票戶口被非法入侵作交易，損失會否仍由不知情的股民承擔？金融管理局指出，根據《銀行營運守則》，除非客戶作出欺詐或嚴重疏忽行為，否則毋須就未經授權交易而蒙受的直接損失負責。

香港金融管理局業務操作、科技及財務風險監理處主管李偉文昨日表示，今年各銀行接獲46宗未經授權股票交易報告，其中11宗報稱沒有損失，有12宗仍在核證中，23宗證實錄得損失，涉款430萬元，有關銀行已全數賠償予客戶。銀行會就所有未授權股票交易通知警方，金管局上月已發信要求業界採取加強措施，例如採用雙重認證登入，設定所有交易以SMS短訊通知客戶等。

網罪科總督察許綺惠指出，雙重認證登入方法相對安全，暫未有採用此方法的機構戶口被入侵。高級督察葉卓譽指出，銀行必須就懷疑被入侵作未授權交易的個案報警，警方會按銀行資料聯絡受影響客戶，但客戶或因沒損失甚至有賺，並未報警或向警方落口供，因此金管局及銀行的損失統計數字與警方的數字有出入。

投資者教育中心教育計劃及統籌經理潘淵淳亦提醒，客戶應定期查閱交易紀錄，如有不明交易，應盡快通知銀行或報警，銀行不會以電話及電郵要求客人提供個人資料。



▲機電署職員檢走爆炸的煮食爐作深入調查



▲北河街發生氣體煮食爐爆炸現場