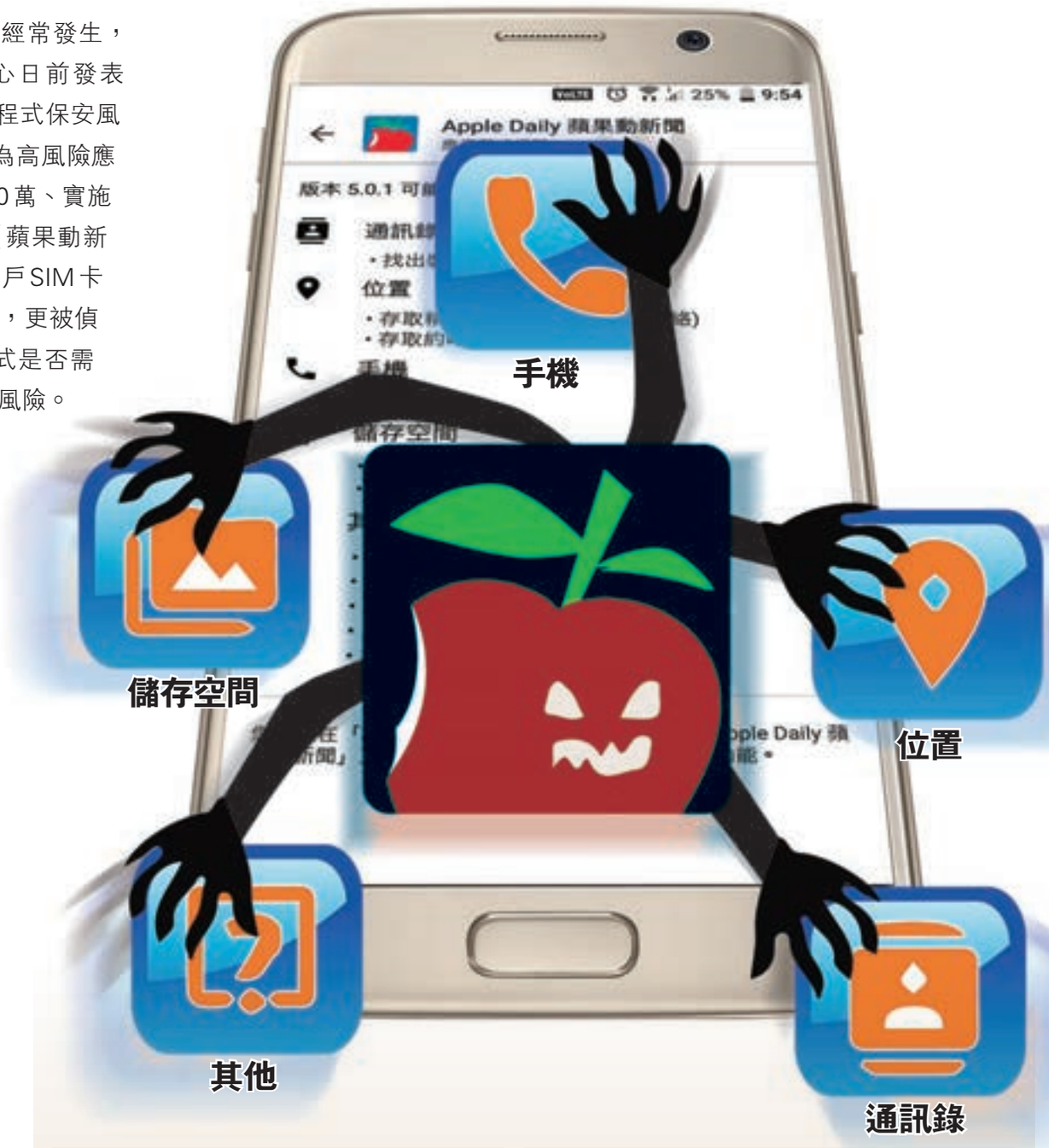
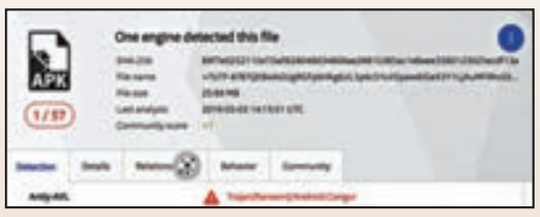
《動新聞》高風險 或中毒洩私隱

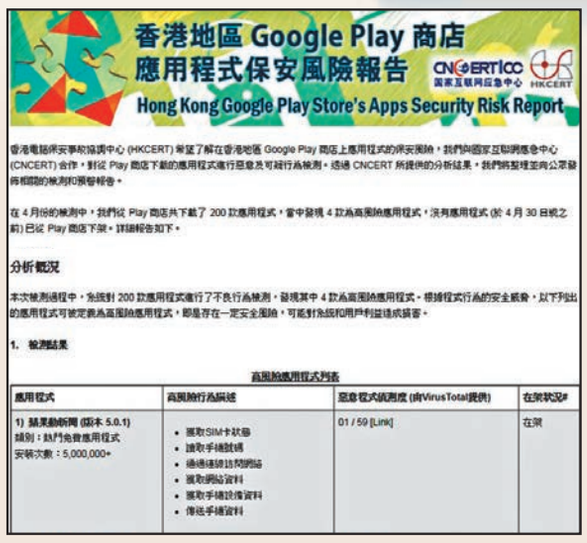
索料多 有木馬 專家籲考慮下載風險

香港文匯報訊（記者 文森）資料外洩事故經常發生，有時防不勝防。香港電腦保安事故協調中心日前發表2019年4月「香港地區Google Play商店應用程式保安風險報告」，將4款港人常用的Android App列為高風險應用程式，當中更包括Android版下載次數逾500萬、實施會員登記制僅3星期已累積277萬名會員的《蘋果動新聞》。報告指出，《蘋果動新聞》存在獲取用戶SIM卡狀態、網絡資料及傳送手機資料等高風險行為，更被偵測出惡意木馬程式。有電腦專家質疑手機程式是否需要獲取那麼多資料，並呼籲市民下載時要考慮風險。





▲根據VirtualTotal的惡意程式偵測度報告，指Antiy的AVL防毒軟件掃描到Android版《蘋果動新聞》程式裡含有一款惡意木馬程式「Trojan[Ransom]/Android.Congur」。



►香港電腦保安事故協調中心日前發表報告，發現Android版《蘋果動新聞》程式會收集大量用戶資料，將其列為高風險。 HKCERT網頁截圖

香港電腦保安事故協調中心與中國國家互聯網應急中心合作，對從Google Play商店下載的應用程式進行惡意及可疑行為檢測，調查範圍包括香港地區排名首50位免費的熱門和最新應用程式及遊戲，總共200款應用程式，當中發現4款屬高風險應用程式/遊戲。該4款被列為高風險的應用程式/遊戲分別為新聞軟件《蘋果動新聞》、動作遊戲《RunRace 3D》、卡牌遊戲《三國殺繁體版》及動作RPG《元氣騎士 Soul Knight》。

報告列《蘋果》程式可疑代碼

其中，《蘋果動新聞》被指獲取用戶SIM卡狀態、讀取手機號碼、通過連線訪問網絡、獲取網絡資料、手機設備資料及傳送手機資料等高風險行為，且根據VirtualTotal的惡意程式偵測度報告，指Antiy的AVL防毒軟件掃描到程式裡含有一款惡意木馬程式「Trojan[Ransom]/Android.Congur」。報告內設「高風險應用程式深度分析」的《附錄》，打開後可看到源代碼(source code)，報告逐項清楚列出《蘋果動新聞》程式的可疑代碼部分。

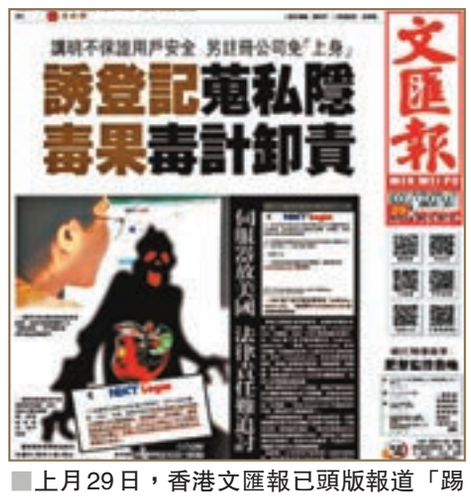
《三國殺》也是許多港人熟識的卡牌遊戲，不論實體遊戲、網絡遊戲時代已深受歡迎，登陸手機之後也有不少捧場客。報告發現它會獲取多項SIM卡資料、通過連線訪問網絡和獲取及傳送手機資料等。VirtualTotal報告亦指它被發現含有兩種廣告型惡意軟件。市民如欲查閱報告，可登入網頁連結：https://www.hkcert.org/my_url/zh/blog/19043001。

專家：下載免費App有代價

香港大學信息安全及密碼學研究中心總監鄒錦沛接受香港文匯報訪問時質疑，新聞程式及手機遊戲是否有需要讀取用家的SIM卡資料(例如網絡供應商)、IMEI(手機機身編號)等資料，甚至將之傳送出去，市民下載該等程式時亦需留意有否授權對方獲取該等資料。他說：「好難講它們獲取客戶該些資料有什麼目的，例如是否作推銷之用？但這世界沒有免費的午餐，免費下載程式總有付出吧！」

他續說，用戶被讀取上述資料不等於即出現資料被盜取或外洩等網絡保安事故，但市民下載時必須特別留心，「我個人向來不會下載會讀取那麼多資料的程式。」

用盡空殼公司「魔鬼條款」避刑責



■上月29日，香港文匯報已頭版報道「踢爆」《蘋果動新聞》實施會員制背後暗藏私隱陷阱。 香港文匯報截圖

話你知

《蘋果動新聞》於上月初起實施會員制，卻被香港電腦保安事故協調中心的風險報告點名列為高風險應用程式。上月29日，香港文匯報已頭版報道「踢爆」《蘋果動新聞》實施會員制背後暗藏私隱陷阱，因其網站存有大量「魔鬼條款」；與會員簽訂使用條款的公司也非壹傳媒，而是一間以港幣1元股本成立的私人公司，令人質疑一旦網站洩露會員資料時，壹傳媒能「金蟬脫殼」避過刑責。

《蘋果日報》網站於上月初實施會員制，市民必須登記個人資料始能閱讀全文及視頻；數天後「巧合地」爆出全城哄動的「安心偷食事件」，一日間進賬40萬登記人數，累積會員數量旋即突破200萬，截至本月2日更已累積超過277萬。

網民如欲瀏覽該網站的新聞內容時，會被要求先透過手機號碼、電郵、facebook或google賬戶註冊與登入，惟香港文匯報在其「使用條款及細則」的連結卻發現，與用戶簽訂條款的公司並非壹傳媒，而是一間名為「OMO Network Limited」的公司。

有關的條款更列明，「我們（OMO）可能將你的個人資料提供給第三方服務供應商（可能位於香港境外）……可能將你的與賬單和付款有關的信用卡號碼和信息提供給代表我們的第三方服務供應商。」OMO之後列出「無法保證且不保證你的賬戶或你的內容的安全性」等大堆免責條款作「免死金牌」。

伺服器放美 出事難追究

香港文匯報記者透過公司註冊處查冊更發現，2015年7月成立的「OMO Network Limited」股本僅1港元，由一間英屬處女島公司持股，時任壹傳媒執行董事丁家裕代表該英屬處女島公司簽署文件，時任壹傳媒行政總裁張嘉聲則為OMO的董事；其後OMO經歷多次人事變動，目前的董事為《蘋果日報》社長張劍虹。

香港文匯報記者同時發現，網站伺服器疑設置於與壹傳媒關係密切的美國，用戶日後若要追究責任時，香港法律未必適用。 ■香港文匯報記者 文森

「讀卡黨」現尖東 製假卡碌走廿萬

香港文匯報訊（記者 蕭景源、劉友光）沉寂一時的「讀卡黨」再現。一個來自保加利亞的假卡集團，疑覷準AEON信貸財務（亞洲）部分信用卡未裝有晶片的保安漏洞，以新式讀卡器及針孔攝錄機加裝在尖東港鐵站內一部櫃員機，套取客戶卡資料及密碼，再複製假卡提取現金或購買比特幣（Bitcoin），最少七人「中招」，合共損失20萬元。警方接報經調查，前日在佐敦一酒店目標房間拘捕三名保加利亞籍男子及檢獲一批證物。

被捕三名外籍男子由26歲至33歲，保加利亞人，於今年3月中以旅客身份來港，為假卡集團骨幹成員，均被暫控一項「管有用作製造虛假文書的設備」罪名，將於今日在西九龍裁判法院提堂。

專覷準AEON磁帶卡保安漏洞

據悉，該假卡集團尚未能破解裝有加密晶片技術的信用卡。其犯案手法是覷準本港的AEON信貸財務（亞洲）並非金管局監管的認可機構，所發出的信用卡部分仍使用較低保安的磁帶功能而非加密晶片的漏洞，在尖東港鐵站一部相關櫃員機加裝新式讀卡器及針孔攝錄機，盜取客戶卡資料及密碼，再複製假卡提取現金、或購買比特幣（Bitcoin）；估計集團已運作一個月，遭盜取資料事主數以十計。

警方商業罪案調查科高級警司鄭麗琪表示，今年四月上旬警方接獲一間發卡機構報案，指人員巡查發現港鐵尖東站內一櫃員機疑被插入讀卡裝置；同月23日，該發卡機構人員再在同一部櫃員機發現被插入讀卡裝置及鍵盤膠蓋上安裝有針孔攝錄機。同月下旬，該發卡機構接獲7名客戶舉報，指信用卡在未經授權下被提走款項，合共損失約20萬元。

警破假卡竇「勇獵」3外籍男

商業罪案調查科人員翻查涉案櫃員機附近閉路電視錄影及深入調查，鎖定一個以遊客身份來港的保加利亞假卡集團，並展開監視。至前日（2日）凌晨約2時，警方認為時機成熟展開代號「勇獵者」行動，突擊搜查佐敦一間酒店目標房間，終偵破該跨境假卡詐騙集團，當場拘捕三名目標外籍男子，檢獲兩個讀卡裝置、一部針孔攝錄機、114張懷疑偽造信用卡、電腦、用作製造假卡器材、及約7萬元現金等證物。

商業罪案調查科署理警司黎偉俊表示，初步調查相信三名被捕男子製造及在櫃員機安裝非法裝置，以套取卡主磁帶資料及密碼，再製造假卡提取現金或用以購買虛擬貨幣。

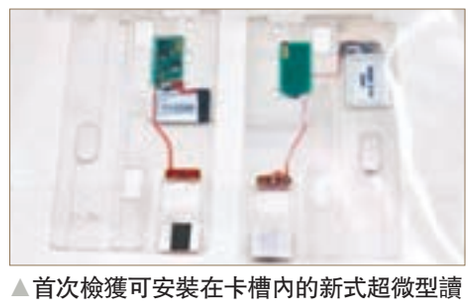
案件揭發後，警方已即時通知金管局和香港銀行公會，要求各銀行巡查旗下櫃員機，確保未受干擾。警方同時加強尖東一帶櫃員機巡邏及與港鐵合作，協助調整港鐵站內閉路電視鏡頭覆蓋櫃員機位置。

AEON將停所有櫃員機

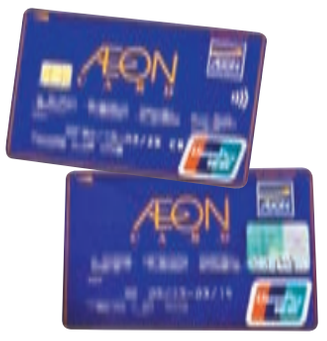
AEON信貸財務（亞洲）發言人表示，公司將負責承擔有關客戶的損失，為加強保安，公司會暫停所有126部櫃員機服務，待完成調查及更新保安措施才重開。香港文匯報記者昨日到尖東港鐵站涉案櫃員機查看，發現該部櫃員機已經暫停服務。

金管局發言人接受香港文匯報查詢時表示，這次事件所涉機構非金管局監管的認可機構，但鑑於事件涉及新的犯罪手法，已盡快通知及要求銀行檢視櫃員機的保安措施，提高警覺和加強巡邏。

發言人補充，本港銀行的提款卡和櫃員機已經全面使用晶片技術，即使提款卡資料被盜取製成假卡，亦不能於本港銀行櫃員機提款。



▲首次檢獲可安裝在卡槽內的新式超微型讀卡器。 香港文匯報記者劉友光 攝



◄AEON新發信用卡已加有晶片(上)，但今年3月到期的舊卡則無晶片(下)。

此外，根據銀行營運守則，除非客戶作出欺詐行為或有嚴重疏忽，他們毋須為未經授權的交易所引致的損失負責。市民應定期查閱交易記錄及銀行月結單，如發現可疑情況應立即與相關銀行聯絡。

慎防櫃員機被「做手腳」

- 留意櫃員機附近範圍是否有可疑鏡頭
- 信用卡或提款卡插入櫃員機前小心留意入卡口有否可疑裝置或凸起異物
- 檢查提款鍵盤護罩底有否隱藏針孔鏡頭
- 在櫃員機輸入提款密碼時用手或物件遮掩，防止被偷看或偷錄密碼
- 盡量避免使用保安程度低的密碼，並定期更改密碼，提高安全性
- 當不需要在海外提款時，可向銀行要求取消海外提款功能，避免卡資料遭人於海外被盜用
- 如發現戶口記錄有未授權交易，應立即向有關金融機構查詢

整理：香港文匯報記者 蕭景源

卡主若涉疏忽 或需承擔損失

專家之言

沉寂一時的「讀卡黨」再現，市民最關心一旦信用卡遭盜用所造成損失責任誰屬。國際專業保險諮詢協會會長羅少雄接受香港文匯報查詢時表示，發卡機構向客戶發出新信用卡時，會附有卡主需要遵守的相關注意事項。基本而言，卡主除必須妥善保管信用卡外，當發現信用卡遭盜用時，卡主有責任盡快通知發卡機構及報警，若延誤通報則必須要有合理解釋，才可免負上損失責任。

接收交易短訊減風險

羅少雄提醒，如果信用卡遭盜用涉及人為疏忽，卡主就可能需要負上損失責任，故市民在收到信用卡月結單應第一時間拆閱核實，若發卡機構有提供一次性交易密碼或電話交易短訊服務，卡主便應該選用以盡量減低風險。同時，提款卡及信用卡在櫃員機的每日提款額亦應設有上限。

大律師陸偉雄接受香港文匯報查詢時表示，在一般情況下，信用卡遭盜用引致損失的責任問題，需要釐清事件屬發卡機構或是卡主的疏忽，再按雙方在事件上所涉疏忽程度，衡量所需要承擔損失的責任。

他以今次案件為例，因為發卡機構在信用卡上未有裝設晶片，以致出現嚴重保安漏洞，加上為免客戶失去信心，發卡機構承擔所有損失亦屬合理。

加密晶片卡可防偷料

有資訊科技專家指出，不法分子只需取得信用卡磁帶資料，或已可複製信用卡冒認卡主進行網購，如果卡主連密碼也遭盜取，不法分子更可以製作假卡進行提款。要防止「讀卡黨」的最有效方法，是信用卡及提款卡全面採用加密晶片代替磁帶，防止「讀卡黨」利用讀卡機複製磁帶資料犯案。 ■香港文匯報記者 蕭景源