112年12月號

公務機密
資訊安全維護

農業部林業及自然保育署臺東分署

公務機密 資訊安全維護

目錄

曾勒索台積電供應商22億 波音、名古屋港全遭LockBit毒手

2023/11/12

〔財經頻道／綜合報導〕根據趨勢科技統計，今年上半年遭網路勒索病毒攻擊的企業、組織，較去年下半年增加47%，勒索軟體組織LockBit就佔了26%。這個具有俄羅斯背景的駭客組織最新盯上的目標，竟是中國最大銀行-中國工商銀行在美子公司，害慘中國工銀緊急拿出90億美元（約台幣2907億），支付拖欠美國梅隆銀行的款項。今年年中還曾爆出勒索台積電供應商擎昊科技7000萬美元（約台幣22.6億），美商波音及日本名古屋港也慘遭LockBit下毒手。

俄國背景駭客臭名昭彰 受害者遍及全球

LockBit 勒索軟體在2019年9月首次現身，前身為「ABCD」，2020年1月正名為LockBit，具有俄羅斯背景，是最近幾年最活躍的勒索軟體即服務（RaaS），苦主遍及全球。從2020年至今年第一季，受害組織1653個，光是美國地區支付的贖金就超過9100萬美元，其攻擊佔勒索市場的 40%。這個駭客組織2022年6月推出「LockBit3.0」版本，還引入漏洞賞金計劃，宣稱廣邀地球上所有安全研究人員、道德和不道德的駭客參與漏洞賞金計劃，報酬從 1000 美元到 100 萬美元不等，這票人正在努力找出加密程式碼漏洞、公共基礎設施漏洞。

Lockbit會先竊走組織資料並予以加密，若不給付贖金就將資料公布於TOR暗網上，這導致資料恐被競爭者買走，Lockbit藉此達到雙重威脅，台灣超過一半的攻擊就是來自Lockbit。

今年6月Lockbit在暗網網站公布台積電是受害者，並勒索7000萬美元，結果虛驚一場，遭攻擊的應該是台積電供應商擎昊科技。

台積電供應商成肥肉 中國金融機構也遭毒手

今年6月30日Lockbit在暗網網站公布台積電是受害者，並勒索7000萬美元，威脅如果不在8月6日前支付贖金，將公開竊取資料。結果發現虛驚一場，遭攻擊的應該是台積電供應商擎昊科技。

擎昊科技證實，測試環境遭到外部團體的攻擊，攻擊者成功竊取設定檔和其他參數資料。因遭竊資訊與客戶實際應用無關，僅為出貨時的基本設置，目前客戶（台積電）沒有遭受任何損害，客戶也並未遭駭。

除了護國神山台積電供應商成為Lockbit眼中肥肉外，波音、日本名古屋港今年都被Lockbit盯上。日本最大貨運量之一的名古屋港口，7月4日疑遭LockBit 3.0勒索軟體攻擊，造成運貨處理作業停擺，直到7月6日才恢復運作，這次事件影響約260家船運公司。同時，名古屋港運協會電腦被加密，約100台印表機遭到劫持，以英文列印出系統感染勒索軟體的通知，還要求協會支付贖金。

波音則在今年11月初坦言，駭客取得內部資料，正配合執法機構調查，並通知客戶及供應商。LockBit聲稱擁有這家飛機製造商的大量敏感資料，並使用了零日漏洞來存取資料，但沒有具體說明從波音竊取多少數據，也沒有提供贖金的詳細資訊。

LockBit最新受害者就是中國金融機構，中國工商銀行在美子公司，美東時間11月8日遭勒索軟體攻擊，部分系統中斷，導致美國公債市場出現混亂，部分交易無法結算，中國工銀暫時拖欠紐約梅隆銀行（BNY Mellon）90億美元，該行緊急對在美子公司注資，支付積欠梅隆銀行的款項。

全球資安拉警報，台灣2023上半年的惡意威脅數量急遽成長。（Fortinet提供）

中小企業組織及校園留意！Roundcube Webmail爆零日漏洞已被用來攻擊

2023 / 10 / 26

Roundcube 是一種免費的開源網路郵件解決方案，特別受校園或中小企業組織歡迎。外媒報導，俄羅斯駭客組織Winter Vivern（又名 TA473）一直利用 Roundcube Webmail 伺服器中的零日漏洞，針對歐洲的政府組織和智庫發起惡意電子郵件攻擊、

國外資安研究人員觀察到Winter Vivern發送了特製的電子郵件，該電子郵件使用包含精心製作的 SVG 文檔的 HTML 電子郵件來遠端注入任意 JavaScript 程式碼。

Winter Viver的網路釣魚郵件冒充 Outlook 團隊，試圖誘騙潛在受害者打開惡意電子郵件，自動觸發利用 Roundcube 電子郵件伺服器漏洞的第一階段有效負載。此漏洞為跨站點腳本(XSS) 漏洞，追蹤為 CVE-2023-5631。攻擊中投放的最終 JavaScript 有效負載說明攻擊者從受害者的網路郵件伺服器竊取電子郵件，並將電子郵件洩露到 C&C 伺服器。

CVE-2023-5631影響Roundcube 1.4.15 之前的版本、1.5.5 之前的1.5.x 以及1.6.4 之前的版本。目前Roundcube發布了安全更新，新版本為1.6.4、 1.5.5 、和 1.4.15來解決 CVE-2023-5631。

Winter Vivern 的活動經常被安全研究人員低估，但該組織自 2020 年 12 月起一直活躍。該組織通常使用惡意文件、網路釣魚網站和自訂 PowerShell 後門來危害其目標。

攻擊活動首先從地址team.managment@outlook.com向目標發送一封網路釣魚電子郵件，主題行為「開始使用 Outlook」。該郵件聲稱來自 Microsoft 帳戶團隊，旨在指導使用者使用 Outlook 帳戶，看起來很無害。

然而，只要查看電子郵件，就會啟動由電子郵件 HTML 原始碼末尾的 SVG 標籤（包含 Base64 編碼的有效負載）。根據研究，解碼有效負載會產生 JavaScript 程式碼，該程式碼在受害者的瀏覽器中的 Roundcube 會話上下文中執行。

攻擊中的最終JavaScript 負載可以列出目前Roundcube 帳戶中的資料夾和電子郵件，並透過向「https://recsecas[.]com/controlserver/saveMessage」發出HTTP 請求，將電子郵件訊息洩漏到Winter Vivern的命令和控制伺服器。

除了立即更新Roundcube版本外，也建議採取的端點防禦實踐是停用自動JavaScript 有效負載載入以及部署端點安全解決方案。

用鄰居個資瘋狂檢舉違規218次　害她變「檢舉魔人」台中女要賠6萬

記者白珈陽／台中報導 2023年11月10日

台中市洪姓女子與張姓女子長期有糾紛，洪因常看到違規車輛停放，想檢舉卻又怕被報復，竟盜用張的個資，在半年內向警方檢舉交通違規高達218次。刑事一審張獲判無罪，但二審依違反個資法改判3月確定；張另提民事損害賠償，對洪求償50萬餘元，法官審酌洪侵害隱私權、對張造成精神痛苦，判賠6萬元，可上訴。

判決指出，洪女與張女是鄰居，長期因房屋加蓋等問題產生糾紛，洪見住家附近、台中市大雅區雅潭路一帶常有違規停車，想檢舉又怕被報復，在未經張女的同意下，自2021年2月15日至同年7月10日間，盜用她的電話、地址，於台中市警局交通違規檢舉網頁，檢舉218件交通違規。

洪女一審獲判無罪，但二審時，被依個人資料保護法，判處有期徒刑3月確定。

張女再提民事告訴，主張她因洪的檢舉行為，害她要到警局接受偵訊，同時引起媒體關注報導，更屢遭不明來電質疑她就是檢舉人，造成她名譽受損，內心承受巨大壓力、睡眠失調等症狀，目前仍持續接受憂鬱症門診及藥物治療。張女就名譽權、隱私權受損，以及醫療費用，共求償50萬5810元。

洪女抗辯，她輸入的地址、電話，都是張女張貼於其經營的商店看板或PO在網路上的公開資訊，且她填載的資料無法直接或間接辨識所有人的身分，她雖冒用張的地址及電話號碼進行檢舉，但真實姓名、身分證字號、電子郵件仍是填寫她本人的資料，受理機關可明確知悉檢舉人是誰，並未對張造成損害。

民事庭認為，張女至警局接受偵訊，是為維護自身權益的行為，警方基於偵查不公開原則，偵訊內容不會被社會大眾所知道，未造成張女損害；另新聞報導並未記載張女姓名，主要呈現張收到多張罰單、導致生活困難等情形，也不會讓讀者對張的人格產生負面評價。但洪女冒用張女個資，半年內檢舉高達218次，造成張女精神上痛苦，要賠6萬元，全案還可上訴。

▲洪女冒用張女個資檢舉交通違規高達218次，民事判賠6萬元，可上訴。（圖／資料照）

為郭台銘連署涉不法 屏檢偵辦已收押6人

（中央社記者李卉婷屏東縣20日電）鴻海創辦人郭台銘連署取得獨立參選總統資格，屏檢獲報有連署站涉不法，以新台幣200元換連署書，包含潮州鎮長周品全及屏東市邱姓里長，共已收押6人，並持續調查中。

台灣屏東地方檢察署今天發布新聞稿指出，日前接獲情資指出，屏東市邱姓里長涉嫌於今年9月底，指示吳姓民眾、張姓民眾向選民交付空白連署書，並要求為郭台銘連署即可獲得現金200元報酬。

檢察官經蒐證後於17日傳喚，訊後認為邱姓里長、吳姓民眾、張姓民眾涉嫌違反總統副總統選舉罷免法第87條第1項第2款，犯罪嫌疑重大，有事實足認有勾串共犯、證人之虞，向台灣屏東地方法院聲請羈押禁見，地院裁定邱姓里長、吳姓民眾羈押禁見，張姓民眾以2萬元具保。

另外，屏檢在10月26日查獲陳姓被告等3人，為郭台銘連署涉嫌交付賄賂，日前3人已收押，並持續追查共犯，發現潮州鎮長周品全涉協助收購，昨天到周品全工作地點、居住所等處搜索，查扣相關證物，經檢察官複訊後，也遭聲押獲准。

屏檢指出，全案目前已經收押6人、1人交保，並持續調查中。

（編輯：郭諭儒）1121120

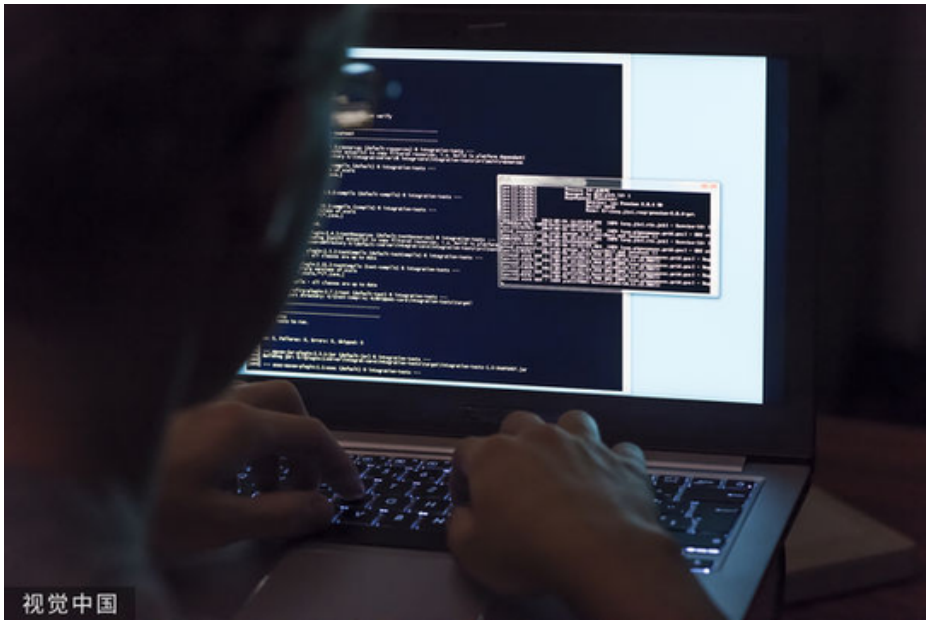
快改掉！台灣人最愛「10組爛密碼」　當心1秒被駭

密碼管理公司NordPass最近公布了2023年全球最受歡迎密碼排行榜，同時揭曉了台灣人最喜愛的前20個密碼。台灣最常使用的密碼首選不再是「123456」，而是改為「admin」，不過，資安專家警告，這些密碼仍然只需要不到1秒就能被駭客輕易破解。

根據NordPass對國人常見密碼的分析，排名第一的是「admin」，過去曾經名列前茅的「123456」則跌至第二名。這兩組密碼都有超過8千個帳戶在使用。接下來的前五名包括「a123456」、「12345678」和「1qaz2wsx」，其中「a123456」有超過6千人使用，而「12345678」和「1qaz2wsx」則分別被超過3千人使用。對於有心盜取帳戶的駭客來說，這些密碼只需要不到1秒的時間就能迎刃而解。

台灣最常使用密碼前10名組合：

1、admin
2、123456
3、a123456
4、12345678
5、1qaz2wsx
6、123456a
7、janejane123
8、password
9、a123456789
10、abc123



▲資安公司公布2023年常見密碼排行。（圖／CFP）

▲這組詐騙貼圖近日在網上瘋傳。（圖／翻攝自Dcard）

LINE「萬聖節免費貼圖」是詐騙！苦主崩潰洗版：+1　5步驟自保

記者周亭瑋／綜合報導 2023年10月31日

最近不少人都收到朋友轉傳的「LINESTORE萬聖節快樂」免費貼圖，只要點入連結，就可從780萬組貼圖中，隨意選擇喜歡的下載，然而這其實是詐騙集團新招，許多網友得知後崩潰表示，「我已經點了，還按了下載」、「因為不同朋友傳，手機和筆電都點了」。

隨著萬聖節的到來，這幾天一個「萬聖節免費貼圖無限量下載」的活動在網上瘋傳，上面聲稱有超過780萬組的貼圖，任你隨機獲得。就有網友在Dcard貼出截圖，驚喊這是詐騙，更懊惱表示「不小心點這個連結按了下載，後來認真看才發現網址怪怪的，超煩的...有誰知道這個詐騙會怎樣嗎？」

PO文掀起熱烈回響，一票網友焦急表示，「我也是...哭呀」、「+1，還加好友了，好怕會被盜手機內的資訊」、「傳給10個好友就可以再扭蛋一次，傳完之後他就會叫你加好友」、「真的詐騙都給我去死」、「想請問一下，點擊下載之後手機會不會被植入什麼後門軟體，好怕手機裡面的資料被盜用阿」、「我甚至還加好友了」、「我也不小心按了，不知道會怎麼樣」。

據事實查核中心MyGoPen指出，平台近三天已收到806次關於「萬聖節假貼圖詐騙」的回報，站長就提醒，想取得免費貼圖只有兩種管道，一是「加入官方頻道，取得贈送的免費貼圖」，再來就是「LINE購物頻道與廠商的限時贈圖活動」，而其餘都是詐騙陷阱。

值得一提的是，若想加強LINE帳戶的安全性，以下5步驟能自保：

1.進LINE後台更改密碼。
2.加強設定「二次驗證」，凡是在其他裝置登入，就會跳出通知。
3.檢視有無其他裝置登入。
4.關閉「LINE ID允許被加入好友」功能。
5.LINE隱私設定內，開啟「阻擋非LINE好友訊息」。

另外，科技網站「iPhone 瘋先生」也指出，該活動要求「加入好友」，主要是用來收集用戶IP位置和居住縣市，也能夠讓對方取得你在LINE上顯示的個資，像是生日、LINE發布動態圖文、個人大頭照與ID資料等。

如果「已點選領取LINE Store萬聖節詐騙貼圖，又該怎麼辦呢？」瘋先生表示，單純點選網址或下載貼圖按鈕，其實不用擔心手機被植入惡意程式碼或信用卡資料被盜，在沒有填寫資料或登入帳號密碼動作的情況下，並不會出現帳號被盜用的資安風險，這算是近年常見的LINE假貼圖跳出式網址詐騙。