香港仔
LION ROCK DAILY

Facebook

lionrockdaily香港仔 www.lionrockdaily.com | 2024.3.25 | 星期一

P.2 維港基層墟市 婦女手作織夢

P.4 先導受歡迎 醫療券使用率98%

警揭逾17萬項安全漏洞 通知網絡供應商修補

港企電腦不設防 黑客入侵飆54%

香港企業電腦系統去年被黑客入侵案件較前年飆升54%，包括消委會遭黑客入侵勒索50萬美元，導致近八成電腦系統受破壞，更有調查指港企已成黑客主要網絡攻擊目標之一。警方數月前展開代號「神將」行動，透過分析網絡威脅情報，打擊指揮及控制伺服器、殭屍網絡、釣魚網站，發現全港有逾17萬項嚴重網絡安全漏洞及4萬項網絡威脅，遂通知持份者及網絡供應商修補漏洞及清除網絡安全威脅。

根據「2023香港企業網絡保安準備指數及私隱認知度」調查報告顯示，近四分三受訪企業過去12個月內曾遇到最少一類網絡安全攻擊，按年增8%至歷來新高，反映企業成為黑客主要攻擊目標之一。企業電腦系統一旦遭入侵，黑客會以不同形式進行勒索，包括上載盜取數據到暗網出售及將檔案加密勒索解鎖費，甚至橫向攻擊公司網絡上其他電腦系統。去年香港電腦保安事故協調中心共收到逾7,700宗網絡安全事故報告，當中四分之一涉網絡釣魚。

警方網絡安全及科技罪案調查科署理高級警司陳純青表示，去年本港錄得37宗涉企業系統被黑客入侵案件，包括勒索軟件攻擊，較2022年的24宗急升54%，而去年總損失金額約210萬元，主要因為企業接受警方建議拒付贖金。不過警方相信企業實際的損失被大幅低估，因為企業受網絡攻擊後，除業務受阻及商譽受損外，更需要花費巨款作事故應變及系統提升。

根據市場數據，企業約要花費100萬元用於系統復原，警方估算案件總損失可能高達3,700萬元。去年損失最大一宗企業系統入侵案，涉事公司因疏忽網絡安全問題，被一名前員工持續進入公司電腦系統，於14個月內在未經授權下分數次轉走合共71萬元，直至去年1月公司始揭發報警。

警方網絡安全及科技罪案調查科網絡安全分組總督察劉傲松表示，警方在去年9月至今年2月期間，展開代號「神將」的淨網行動，與本地網絡持份者進行情報交流，收集並分析約300萬項網絡安全威脅情報，發現香港網絡存在超過17萬項嚴重網絡安全漏洞，以及有近4萬項網絡威脅。警方主動聯絡80間互聯網服務供應商要求修正相關漏洞，包括超過10萬項高危端口遙距控制、近6.3萬台終止支援的電腦系統及超過4,800台未更新的網絡儲存伺服器（NAS）等，並提供一系列的網絡安全建議。

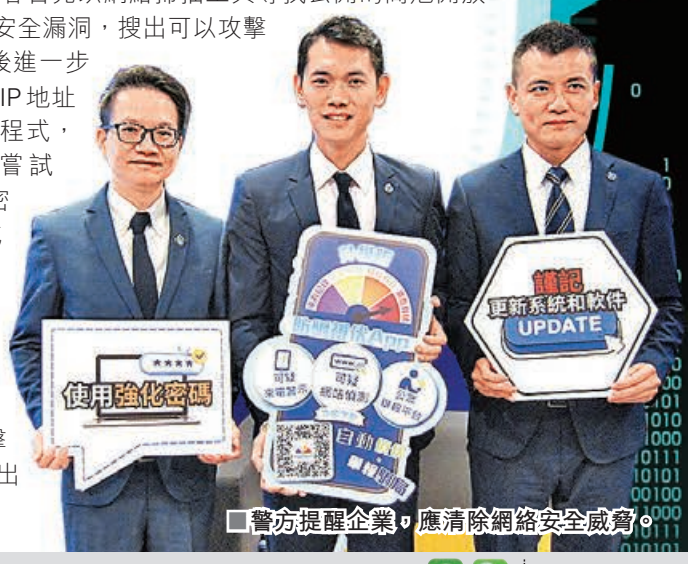
另外，警方亦從源頭堵截攻擊鏈，互聯網服務供應商應警方要求移除接近4萬項網絡威脅，包括成功移除60台指揮及控制伺服器（C2 Server）、超過4,000部已被操控的殭屍網絡設備（Botnet）及超過3.5萬個釣魚網站（Phishing Website）。

警方提醒，不當設置高危端口或採用弱密碼，會讓黑客有機會遙距控制受害人的電腦；終止支援的電腦系統由於無作安全更新，用家容易受到黑客攻擊；而未更新的網絡存儲服務器存在不同已知漏洞，增加資料被盜竊的風險；以上種種問題也會讓黑客有機可乘，用家應盡快作出修補。

攻擊工具分五類 伺服器變武器庫

在「神將」行動中，警方檢取涉及網絡攻擊的C2 Server進行數碼法理鑑證，發現黑客會利用伺服器作「武器庫」下載不同網絡攻擊工具。警方在其中一個「武器庫」發現107種常用網絡攻擊工具， 主要分為五大類，包括木馬程式、掘礦軟件、網絡掃描工具、清除日誌軟件及密碼爆破工具。

「網絡安全特別行動小組」成員之一、深信服科技（香港）有限公司系統工程主管曾祥輝拆解黑客攻擊流程，他指黑客首先以網絡掃描工具尋找公開的高危開放端口或網絡安全漏洞，搜出可以攻擊的目標，然後進一步深入了解目標IP地址是使用何種應用程式，再用密碼爆破工具嘗試「撞中」目標的用戶名和密碼，再上傳「後門程式（backdoor）」以取得電腦控制權，過程中受害人全不知情，黑客更可悄悄開啟受害人電腦鏡頭進行窺視，偷偷錄影及拍照外，同時可偷取資料作日後攻擊之用，包括勒索或放暗網出售。



■警方提醒企業，應清除網絡安全威脅。

網絡安全小貼士

- 使用高強度密碼
- 謹慎點擊連結
- 安裝升級版「防騙視伏App」
- 定期更新系統及軟件
- 謹慎使用遠端桌面連線
- 企業加強員工培訓
- 數據備份
- 定期進行漏洞掃描

資料來源：網絡安全及科技罪案調查科

編輯部: 2873 8233 傳真: 2552 6161 廣告部: 2873 9888 3708 3888 發行中心: 2873 9889 承印: 三友印務有限公司 地址: 香港仔田灣海旁道7號興偉中心2-3樓