
●位於弗吉尼亞州蘭利的美國中央情報局總部。網上圖片

AI黑客工具Artex橫行 美網絡安全保障惹憂

美CIA遭黑客入侵 敏感開源訊息外洩

香港文匯報訊 美國聯邦機構接連遭遇網絡安全入侵事件。《紐約時報》11月24日引述美國官員消息稱，最新一次的安全事件涉及美國中央情報局（CIA）、美國國家地理空間情報局（NGA）與美國國家情報總監辦公室（ODNI），它們的系統分別遭到黑客入侵，導致部分非機密的開源訊息外洩。報道並未說明是次入侵如何發生，但指出這一事件再次凸顯美國網絡安全保障不佳等問題。

報道引述知情人士稱，是次入侵影響了一個開源情報分析系統，這是美國情報部門旨在從公開的非機密資料中，搜尋情報信息的計算機網絡。調查人員相信黑客使用了人工智能（AI）黑客工具Artex，該工具早前由匿名途徑於Github開源發布，原作網絡防衛，其後遭黑客改作攻擊用途，與全球多宗企業遭受網絡襲擊的個案有關。

全球或有上千系統被Artex鎖定

聯邦調查局（FBI）早前亦被揭捲入網絡安全事件，當局發警報指出，黑客利用Artex可在不到3小時內，完成由初步目標鎖定、到獲取系統高權限的自動化滲透，相較其他的黑客手段更加迅速，相信全球有上千個外露的電子系統遭到Artex偵測，成為潛在目標。知情人士稱，目前尚不清楚CIA等情報機構外洩了哪些信息，只能確定其機密資料暫未受到波及。

路透社同日報道，消息指CIA與情報機構內部已經解決是次問題，被問及相關報道時，ODNI方面回應稱，該機構的關鍵能力或機密系統沒受到任何干擾。

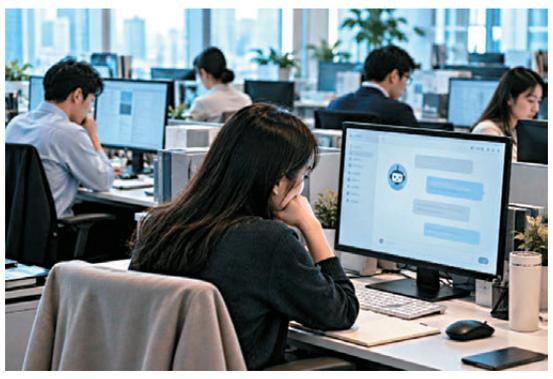
開源情報可助黑客分析信息源

不過《紐時》指出，開源情報外洩同樣敏感，因為開源情報包括大量的商業數據、社媒內容、衛星圖像和其他在線材料。這些大部分公開的內容，可能包括數據供應商出售的信息，這些信息可能具有高度的外露性，特別是與其他數據組合時，或導致機密資料或個人信息外洩。黑客會嘗試將這些數據與其他情報來源結合，綜合分析潛在的信息源。

美國聯邦機構遭受網攻的情況並不少見，但部分機構頻繁遭到入侵，已引起美國情報官員的高度關注。路透社指出，這也是美國國內近期連串技術故障和網絡安全事件中的最新一宗。例如本月12日，微軟Microsoft 365發生全球性服務故障，影響企業和政府機構服務。美國聯邦航空管理局（FAA）翌日電信故障，導致空中交通管制系統通訊不暢，導致全美停飛近5小時。摩根大通與蘋果公司也接連發生系統故障，影響客戶交易和在線服務等。

在美國政府機構中，FBI、國家安全局（NSA）、國防部、國土安全部和農業部等機構，都被揭捲入連串網絡安全事件中。美國總統特朗普多次試圖淡化政府部門遭遇的網絡危機，不過CIA等機構最新的被入侵事件，無疑令情況雪上加霜。

AI降低網攻門檻 黑客目標轉向基建


●分析指全球企業和機構的安全資源配置失衡。網上圖片

香港文匯報訊 伴隨人工智能（AI）技術加速普及，黑客發起網攻的目標正從企業和機構的IT系統，蔓延至工廠、電網和供水設施等關鍵基建。韓媒Digital Times引述專家分析，AI顯著降低了部分網絡攻擊所需的專業知識和技術門檻，從歐洲的雪櫃升溫事件，到美國的排水系統被攻擊，外界對公共設施遭網絡入侵的擔憂正在升溫。

近期網攻針對運營技術

專家指出，這些網攻針對的是運營技術（OT），OT主要指用於監測和控制工廠生產設備、電網和稅務設施等現時設備的系統。目前全球企業和政府機構的網絡安全預算中，約有95%投入IT系統領域，OT的投入僅佔5%，安全資源配置失衡，意味OT遭網攻的風險更高。全球工業設備標準化提高，也放大了相關風險。由於各國廣泛部署廠商統一標準的設備，意味一旦黑客掌握某類系統的攻擊方式，相似方法很易複製到不同國家和行業。

OT遭受網攻的個案今年顯著增加。法國早前發生大規模網攻事件，多間超市和零售商的製冷設備溫度被調升，導致大量冷藏食品報廢，這一情況其後迅速蔓延至歐洲多國。今年年初，墨西哥蒙特雷一間排水供應商也遭到黑客攻擊，黑客試圖使用AI模型Claude編寫攻擊代碼，控制供應商的供水系統。這一事件表明，即使攻擊者缺乏專業知識，也可藉助AI將目標轉向工業設施。

企業端應對危機能力不足

分析認為，企業端目前應對此類網攻的能力不足。OT設備與IT系統構造不同，現有管理體系並不完備。OT安全防護的專業人才短缺，也限制了防護能力。

報道引述專家建議，如今網絡安全的影響已不再局限於信息保護，還會直接關係到公共安全及基建的穩定運行，除強化身份認證等基礎安全措施外，各企業還要建立實施威脅檢測與應對體系。

日本京王電鐵遭網攻 逾1100萬個人資料外洩


●京王電鐵傳出個人資料大規模外洩事件。網上圖片

香港文匯報訊 日本傳出個人資料大規模外洩事件，京王電鐵24日表示，該集團企業今年9月遭到網絡攻擊。公司最新估計，事件導致1,100萬宗顧客與集團企業員工的個人資料外洩，包括身份證明文件、護照、完整信用卡號碼等資料。

共同社報道，京王電鐵表示，公司9月26日遭勒索軟件攻擊，資訊外洩對象包括京王集團顧客及業務夥伴約1,063萬人、求職者約36萬人、退休員工及其家屬約7.7萬人。內容涵蓋姓名、住址、電話號碼等，人數或有重複。公司正在外部專家協助下，調查確切的資訊外洩範圍。

含遊客護照及信用卡資料

是次資訊外洩涉及鐵路、巴士、食肆與百貨公司等眾多與消費者密切相關的行業。公司表示其員工及退休人士約1.2萬人的姓名及資料外洩，曾入住京王廣場酒店等集團旗下酒店的外國住客，約有160萬份護照副本資料可能外洩。京王百貨店可能有消費者的信用卡資料外洩，涉及約兩萬張信用卡號碼。集團地產公司在簽約時收取的身份證明文件，以及類似日本身份證的日本國民個人編號卡（My Number Card）亦包括在內。

京王電鐵呼籲顧客，對可疑郵件和電話提高警覺。公司強調認真看待是次資訊外洩事件，會致力徹底防止類似事件再次發生，調查結果已於24日報告日本個人資料保護委員會。受事件影響，公司旗下的京王Presso Inn酒店暫停接受新預訂，預計下月恢復，10月至12月的住宿收入料減少約18億日圓（約8,800萬港元）。

兩油輪霍峽觸雷起火 伊：一切手段應對美封鎖


●一名聯合國人員早前影到一艘油輪在霍峽冒煙。法新社

香港文匯報訊 伊朗伊斯蘭革命衛隊海軍25日發表聲明說，兩艘「違規」油輪當天凌晨在霍爾木茲海峽水域觸雷發生爆炸並起火。伊朗外交部發言人巴加埃表示，伊朗會動用一切手段應對美國的海上封鎖。美國總統特朗普24日受訪則表示，美國對伊朗軍事行動的經費可以支撐到明年1月底。

伊斯蘭革命衛隊聲明稱，兩艘油輪試圖取道未經許可的航道通過霍爾木茲海峽時，分別在海峽南部和東部沿岸水域觸碰水雷。革命衛隊海軍再次向關閉導航和定位系統的船隻發出警告，「不要輕信美國，以免觸雷發生爆炸和火災。」

伊朗原油出口近零

受美國針對伊朗相關石油出口的封鎖影響，伊朗可觀測的原油出口最近數月已降至接近於零。巴加埃強調，伊朗方面絕不會容忍封鎖：「海上封鎖被視為軍事侵略，在這一方面，伊朗有權使用任何可用手段進行自衛。我們將動用一切手段應對美國的侵略行徑。」伊朗方面也強調，其仍掌控具有戰略意義的霍爾木茲海峽通行權，只有當美方滿足其條件，包括停止敵對行動、解除封鎖，伊朗才會重新開放該海峽。

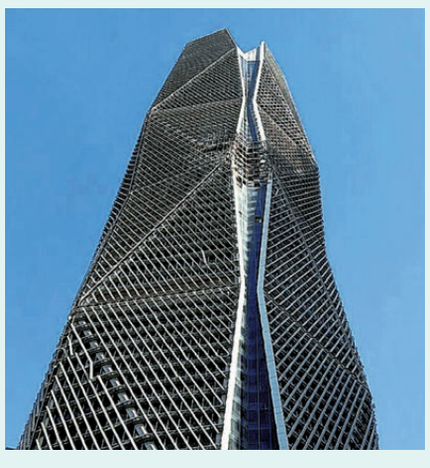
特朗普在白宮受訪時表示，民主黨明年1月掌控國會後，他對伊朗的軍事選項可能受到制約，但他希望民主黨不要將這場衝突倉促收場。「如果（民主黨人）那樣做，他們就會將勝局弄成敗局。」他也表示讓伊朗政權更迭並非他的目標：「我只是不想讓他們擁有核武，我既不支持也不反對政權更迭，那從來不是我的標準。」

胡塞襲沙特主權基金總部11傷

香港文匯報訊 沙特阿拉伯主權基金總部位於首都利雅得的商業大樓，24日遭也門胡塞武裝無人機攻擊，造成至少11人受傷。今次是這座樓高80層、合共385米高的公共投資基金大樓一周以來第二次遇襲，沙特領導的聯軍譴責是次行動屬於恐襲。

沙特民防部門表示，傷者除沙特公民外，還包括印度、尼泊爾與埃及籍人士，有兩人受到嚴重燒傷，情況嚴重。該大樓本月19日首次遇襲，今次再度遇襲時，有數名人員正在內部修復早前襲擊造成的損壞。沙特國營石油巨擘沙特阿美石油公司一座大樓，與今次事發大樓同樣坐落在阿卜杜拉國王金融區，該大樓本月稍早也曾遇襲。

沙特聯軍發言人馬里奇表示，阿卜杜拉國王金融區一座大樓遭到卑劣的恐怖襲擊，相關機構正在勘查遇襲現場，不過未有說明具體是哪座大樓。


●沙特主權基金總部遇襲受損。新華社

韓國首爾地鐵罷工前夕 勞資「臨崖」達協議

香港文匯報訊 韓國營運首爾地鐵1至8號線的首爾交通公社工會，原本預告將全面無限期罷工。不過勞資雙方的薪酬及集體談判於當地時間25日凌晨達成協議，工會宣布撤回罷工計劃，避免早晨通勤交通陷入大混亂。

韓聯社報道，隸屬韓國最大工會全國民主勞動綜合總聯盟（民主勞總）的首爾交通公社工會（即第一工會），自24日上午與資方代表展開新一輪談判。歷經馬拉松式協商，雙方於25日凌晨2時15分進行最終協商，最終達成協議。資方隨後分別與民主勞總旗下的第二、第三工會談妥，三大工會協議的核心內容基本一致。

資方暫緩管理層重組

協議內容包括暫緩資方原有的管理層重組計劃，避免牽涉約2,200名職員的職務，資方同意新聘用500名員工，致力紓緩約800人的人手短缺問題。今年度的員工加薪幅度為2025年度總人事費用的2.4%，資深工齡加薪另計。勞資雙方同意成立聯合專案工作組，應對延後退休年齡、縮短工時等勞動政策變化，共同研究改善列車乘務、車站站務及技術等一線工作制度，強化安全管理。雙方還就改善育兒假等兼顧工作與家庭的制度達成共識。


●首爾交通公社工會原計劃罷工。網上圖片

對於是次達成協議，第一工會會長金正燮表示，雖然協議沒能滿足工會的所有訴求，但暫緩實施爭議最大的人力精簡計劃是工會的勝利，在加薪等方面，工會也爭取到一定成果。為盡可能減少全面罷工對市民造成的不便，工會決定達成協議。第二工會首爾交通公社統合工會，以及第三工會正確勞動工會，均於25日凌晨就薪酬與資方達成協議。

首爾交通公社社長金泰均強調，為避免罷工影響市民日常生活，資方持續與工會對話，最終達成協議，企業未來會在勞資雙方的信任與合作基礎上，全力確保地鐵穩定營運。