http://www.netmag.tw/2017/12/07/%E7%B6%B2%E8%B7%AF%E5%AE%89%E5%85%A8%E5%B7%A5%E5%85%B7%E7%AE%B1%E6%9C%80%E8%81%B0%E6%98%8E%E7%9A%84%E5%B7%A5%E5%85%B7%EF%BC%9A%E4%BA%BA%E5%B7%A5%E6%99%BA%E6%85%A7

網路安全工具箱最聰明的工具：人工智慧

07/12/17

若沒有AI，從行動裝置到雲端服務一切都陷於安全風險。

人類愈來愈力有未逮。惡意程式攻擊、零時差攻擊、網路釣魚、修補程式、更新、弱密碼、勒索軟體、分散式阻斷工具(DDoS)及企業網路內部人士洩密等排山倒海而來，讓人類疲於奔命。資料太多無法消化，而弱點或攻擊的指標跡象又太微弱難以察覺。

人工智慧(AI)這時出現了，它們化身為專家系統、神經網路及機器學習演算法。AI 可用來發現紀錄、交易資料及訊息中的規則模式，判斷電子郵件附件是安全還是有害的，可以進行預測，利用分析結果協助資訊安全長(Chief Information Security Officer, CISO)及團隊跑在駭客前面一步。

行動威脅防護廠商 Zimperium 產品長 John Michelsen 說，若沒有 AI，從行動裝置到雲端服務一切都陷於安全風險。

「你的裝置上可能沒有軟體能偵測裝置是否遭到攻擊，」Michelsen 說，「為解決問題，我們的策略是在裝置端佈上神經系統。它可以感測攻擊，因此從 App、藍牙任何攻擊管道察覺網路連線的異常狀況。這就需要 AI 非決定論的機器學習技術。」

Zimperium 的 z9 能有效防禦零時差裝置和網路攻擊，是唯一一個能即時偵測未知行動惡意程式的機器學習引擎。它整合了 MobileIron 的安全與遵循引擎，可提供整合解決方案。這將有助於解決企業面臨最重大的行動安全問題，即裝置、網路及應用威脅偵測能力，並採取自動化行動來立即防護企業資料。

監控支付卡、保護金融機構

信用卡發行商 MasterCard 執行副總裁暨資安長 Ron Green 就表示，該公司正大力發展 AI。「我們用 AI 或進階分析作為信用卡交易中，包括持卡人或其他使用者的分析。AI 讓我們可以監控有無詐欺交易，使我們能進一步防患未然，在它冒出來之前加以阻止。」結果成績斐然。

「我們可以在攻擊由星火變成燎原大火前加以撲滅。在一家公司阻擋失敗，讓駭客入侵系統時，我們能迅速掌握情況並及時降低該公司曝險程度，」他說：「MasterCard AI 可以依據卡片使用資料判斷信用卡處理機構或其他公司是否也遭到攻擊。」

將人類能做的自動化

AI 也是網路和安全分析與應用效能管理廠商 NETSCOUT 的核心技術，但其目的是為了協助人類專家。

「我們有很多資料，」NETSCOUT 安全技術長 Gary Sockrider 說：「我們將資料拿來分析後，用於防護、勘察，用於瞭解壞人在做什麼勾當、用來協助我們的顧客、客戶、以便在戰爭中勝出。如何辦到的呢？因為我們將大批資料，用真人分析，然後將之自動化。」

為什麼要用 AI 呢？原因是效能。「自動化讓我們得以拓展，且更快回應，」他說：「其中的祕訣是以可擴充、可複製及儘可能迅速自動化應用人類智慧。當然，我們仍持續各種嘗試、持續擴大規模、加快速度、強化演算法，然後持續微調。」

在排山倒海的資料中歸納出規則模式

資料堆積如山，惡意程式找也找不完，這就是為什麼防毒公司 Sophos 援引 AI 的原因，該公司次世代終端策略長 Anup Ghosh 說：「人工智慧和機器學習喊得震天價響，但不是萬能解藥，無法解決我們所有安全問題。可是如果運用得當，效果真的很好。」

他說，「以人類來偵測惡意程式最大的問題是根本不適合。人類擅長做決策，而機器學習則非常適合消化巨量資料、辨識出規則模式。我們人類可以在安全產品上將深度學習發揮得很棒，消費者導向的公司如 Google、Amazon Alexa、蘋果等用得淋漓盡致。我說的很棒，意思是可以很精準偵測未知威脅。未知威脅偵測是我們一直想克服的困難，這正是機器學習的長項。」

偵測上最困難的地方在於誤判—即其實沒有危險，但系統卻認為有攻擊或惡意程式。「少了對誤判的認知，解決方案就不完整，」Ghosh 解釋：「我們的解決方案未知威脅偵測率很高，誤判率又很低。AI 解決方案最關鍵、難度最高的是你能否將誤判情況降到可忽略的程度？」

即時決策

「談到進階攻擊時，不妨談談紅色小組(red team)，它基本是組織內部模擬攻擊，並研判攻擊者行為的團隊。」網路安全公司 Vectra Networks 技術長 Liver Tavakoli 說：「一旦攻擊者進入網路後，他們如何突破關卡、如何移動，如何達成目標？這些聽來好像電影中描述歹徒如何穿越重重迷宮，最後進入銀行金庫竊取財物的情節。」

而這時就需要 AI 來幫忙從資料中找出蛛絲馬跡，他說：「我們坐擁大量資料，有豐沛運算能力來處理資，但叫個人來爬梳資料、從中找出線索是完全不切實際的。機器學習很適合來歸納出規則模式，而且視模式的複雜性而定，你的工具可能小到簡單的 Naïve Bayes，大到深度運算，後者是建立起過去稱為神經網絡網路的系統。」

最後是機器學習，它是一種可從海量資料中找出規則模式，並以精簡方式表達出來，用來即時偵測某種東西、幫你做出決策的工具。

AI 也能傷害攻擊者

別忘了不論好人用 AI 能做什麼，壞人也能，端點安全公司 Ziften 資深副總裁 Roark Pollock 提醒。因此防衛者的目標應該是透過耗損大量資源來重創敵人。

「我們能運用 AI，對我們的敵人造成更大痛苦。AI 許多投資都是關於我如何辨識出已知惡意軟體？如何辨識已知的惡意行為？我們也可以用 AI 來找出基礎架構裡有問題的地方、強化基礎架構、確保漏洞都修補了。如果這些都做到了，就能增加我們敵人的痛苦，使他們要闖進來更困難，同時也增加

他們的成本，或讓成本效益更低。那麼他們可能就無法用簡單技倆，而必須使用更困難、更昂貴的方法來攻擊我們。」

Pollock 說，不久之後，壞蛋也會開始將 AI 用於攻擊中。「機器學習或 AI 未來固然可能發展成一種產業，但 AI 也可能變成我們的敵人。AI 可能為正、反雙方所用，因此我們只是把它用來貓捉老鼠，總有一天會陷入僵局。我認為 AI 真正的希望在於能提升軟體的強度，提升作業系統，所有用於基礎架構的工具、網路、以及用於打造我們基礎架構的一切東西。如果我們能用 AI 來強化這些工具和元素，總有一天我們的基礎架構會變得穩健、安全。」

「AI 對 AI」的網路安全攻防

Sophos 的 Ghosh 同意 Pollock 對惡性 AI 的憂慮。「安全公司被迫要適應 AI，特別是機器學習，主要是因它具備強大識別規則模式的能力。但我認

為，如果需求是科技產業的發明之母的話，那麼錢才是驅使黑暗世界採用 AI 和機器學習的真正原因。」

Ghosh 說幾年內就能看到，「12 到 18 個月內，我們就會看到機器學習快速被用於邪惡目的。例如我們知道許多網路犯罪來自魚叉式網釣攻擊，如果你是壞人，你會有開發傀儡網路的基礎架構、運用微型鎖定手法來發動惡意廣告，並採用流程自動化機制、並觀察轉換率。」

也就是說，「對抗這些壞蛋的安全廠商也必須採用機器學習。現在我們處於 AI 對 AI 的局面，這也會促使我們採用即時機器學習技術。因此以前那種抓出模式之後說『好啦！人類，後面你自己搞定吧！』已經行不通了，你還必須以機器的速度來回應。」Ghosh 表示。

駭客與 AI：一切都是因為錢

到頭來，除了國家贊助的網路犯罪和恐怖主義行動，金錢才是多數攻擊者的目標所在，Zimperium 的 Michelsen 說：「機器學習和其他 AI 技術對於怎麼使用並沒有任何立場。有些人用機器學習來保衛他們的網路，另一些人則是想更有效偷到別的錢而使用機器學習。」

他說，「軟體界已經發展出創新的軟體測試方法，包括機器學習來找出漏洞，因此大型軟體公司會用同樣技術來找出別人家軟體的漏洞，目的是發動攻擊。現在這還不是主流，但我相信那些發展駭客工具的人將來一定會用上 AI，因為可以大幅提高效率。」

預測行動並反擊

Vectra 的 Travakoli 指出 AI 有兩大特性：預測式分析及反制。「所謂預測有雙重含意，一是預測還有哪些漏洞是尚未被開採的，另一層意思是預測攻擊者接下來的一步為何。」

他解釋，「後者比較容易，因為你是把資料集結起來，由已發生攻擊來推斷後續行為，有點像預測對方下一棋怎麼走。你通常根據歷史資料來推斷最有可能的行動。而在 AI 對 AI 的對戰中，現在我們根本還無法預測未來發展。有點像人類的戰爭，對方不僅有很厲害的工具、很先進的科技、懂得怎麼用，它們更厲害的是對於必要時發動毀滅式攻擊毫不遲疑。」

但防衛者就比較處於下風，因為你是在保衛家園，而攻擊者則是在你家攻擊你，Tavakoli 說：「攻擊者通常不擔心造成連帶損壞，但因為是在你家，你就會多所顧忌。傳統戰爭變成網路戰爭後，同樣情形還是會上演。因為你不

知道攻擊者是誰，就不可能在別人家園展開反擊，如果你純粹是自我防禦，就永遠會居下風，而在 AI 戰爭中想獲勝就難上加難。所以想打擊敵人，不只阻止其攻勢，還要制敵機先，做起來相當困難。」

人類還是可以對付 AI—只是要人幫

如今每週全球冒出上萬隻新惡意程式變種，DDoS 攻擊、魚叉式網釣以及摧毀網路的攻擊行為連綿不絕，人類已經力有未逮。問題不是在於智慧高低，而是它的規模太大，而 AI 可以協助人類處理所有資料、面對攻擊執行正確決策，AI 加上人類智慧將是最完美組合。