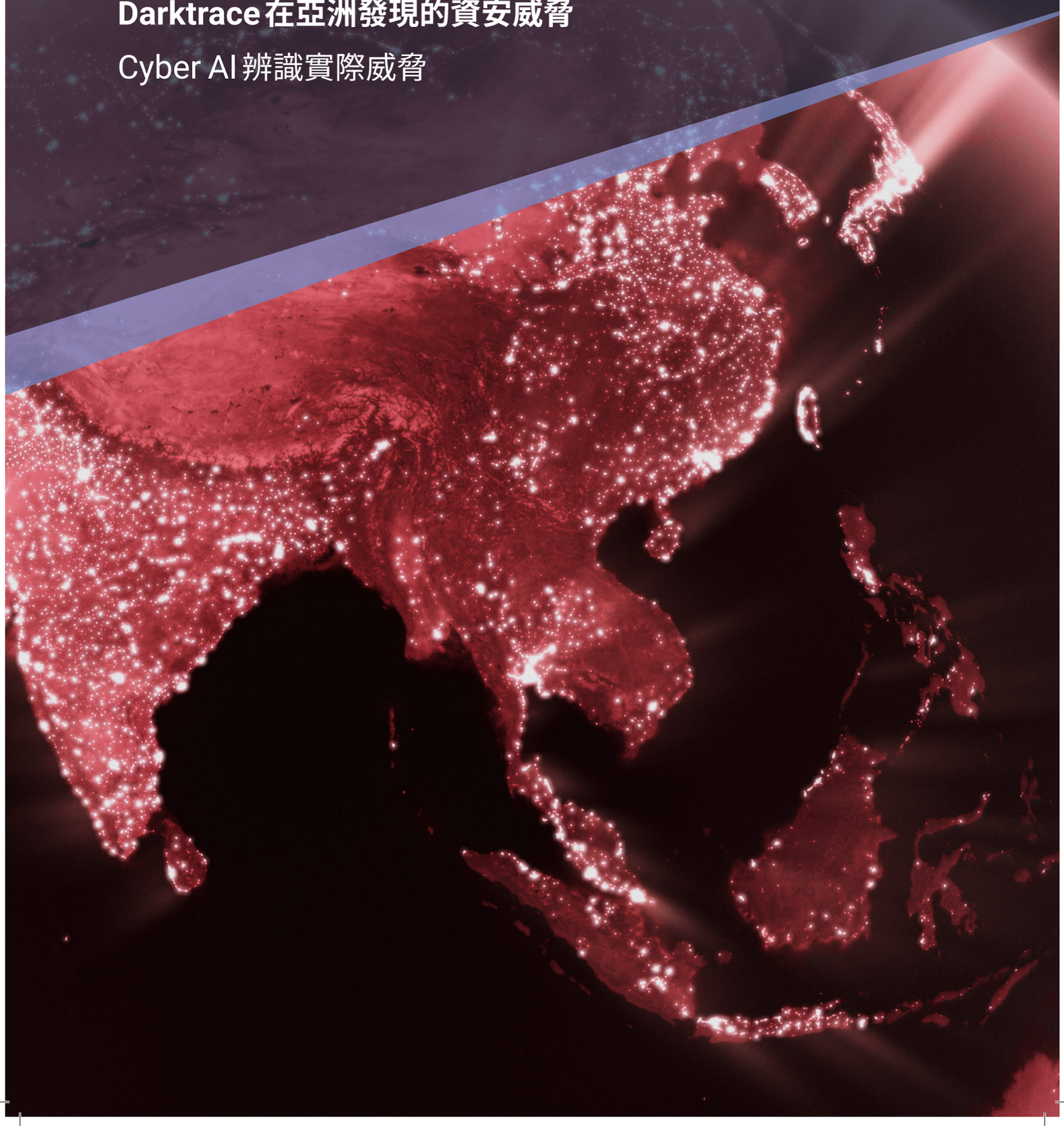
DARKTRACE

Darktrace在亞洲發現的資安威脅

Cyber AI辨識實際威脅



介紹

由新加坡輪值主辦的 2018 年東協峰會、將資安韌性列為第一要務。東協網路安全能力提升計畫 (ASEAN Cyber Capacity Program, ACCP) 及東協資安合作策略等倡議、均指向日益擴大的資安威脅、而同時不致動搖數位經濟開創的商機。資安策略、立法及研究能力極其重要。

企業組織必須先發制人、保護自己的數位業務、否則落在後面的風險高。工商企業在互聯能力推動下持續變革、但此一進步發展卻也連帶提高了網路風險。即使在較不發達的國家地區、物聯網裝置廣為使用也使實體與數位之間的界限變得愈來愈模糊、進而導致這些環境及其中的裝置極易遭受攻擊。

現今的威脅已有能力繞過網路的傳統防禦技術。要打造聯合資安策略、就必須先深刻了解這一點。只有這種方法才能解決威脅的廣度和復雜性; 快速移動的攻擊能在數秒內破壞企業，在人類安全團隊可以響應之前及緩慢而隱秘的攻擊能在雲或網絡系統中未被發現數月，甚至數年。

人工智慧正好能勝任防禦的任務、也是打擊資安攻擊的必須仰賴的盟友。自主防禦技術是一個改變遊戲規則的因素、因為它能即時反擊威脅。機器設備對戰的時代已經降臨、能否避開大規模危機爆發、自主防禦能力至關重要。

以人工智慧為基底、Darktrace 可以辨識並自動回應繞過網路防禦設備侵入企業基礎架構的威脅。這項技術向人體免疫系統的運作取經、學習揣摩每個用戶和裝置的「生活形態」。藉由不斷加深對「正常行為」的理解、Enterprise Immune System能辨識其它错过的新式威脅。接著、Darktrace Antigena 數秒之內就能鎖定目標自主採取行動、在新威脅蔓延之前將之瓦解。

隨著我們進入網路戰爭的新時代、防禦者不能再消極布防、而須佔據主動。亞洲各地企業一旦採用領先全球的資安人工智慧技術、在與層出不窮的威脅交鋒時將能首度扭轉乾坤、進而贏得勝利。

1. 安全監控攝影機遭侵入

產業：金融服務

進入點：連接網際網路的閉路監視系統

明確目標：侵入一台物聯網攝影機、以此進入網路

日常裝置之間的連接程度日益提高、為資安團隊帶來了極大的可見性問題。物聯網裝置通常只有未經整合的基本安全控制措施、因此往往成為攻擊者的目標、將它們當作進入公司網路的跳板。

在一家日本投資顧問公司、Darktrace 發現連接網路的閉路監視系統已被不明攻擊者滲透。犯案者因此得以進入網路、可以竊看攝影機的所有錄像。為了監控整個辦公室空間（從執行長辦公室到會議室）而安裝的攝影機、反而構成資安風險。

Darktrace 的人工智慧系統很快便發現事情不對勁。為了竊取機密、攻擊者在過程中收集數據、有大量數據被觀察進出未加密的閉路監視系統伺服器。

Darktrace Antigena 的反擊

在攻擊者企圖竊取數據之際、Antigena AI 展開快而準的防禦行動。自主防禦技術攔下了從裝置轉移至外部伺服器的數據、同時不妨礙閉路監視系統如常運作。

人工智慧高速反擊、阻止了一次嚴重侵害市場機密的事件。有了 Antigena 助陣、人類組成的安全團隊就能贏得寶貴時間、在損害發生之前進行調查及補救。

2. 鎖定資深主管的針對性攻擊

產業：金融服務

進入點：集中針對重要主管展開攻擊

明確目標：竊取機密

在一家新加坡金融服務公司、Darktrace發現有個可能造成數百萬美元損失的嚴重網路漏洞。Darktrace的人工智慧系統察覺到網路流量被引向異常外部目的地。事實上、這是受感染的設備與位於韓國的攻擊者設備之間的直接指揮及控制(Command and Control, C&C)通道。

網路犯罪已經鎖定一名資深經理、並集中展開高度性蓄意攻擊。在收集了有關這位主管的信息後、攻擊者製作了一個網絡釣魚郵件、其中包含特定及詳細信息、例如最近的工作行程、會議和相關人名。當郵件的附件一打開、網路犯便潛入公司網路、藉機取得電腦上的遠程程式碼執行權。資深主管通過網絡釣魚郵件遭到入侵、但自己卻毫無察覺。

攻擊者測底控制資深主管的電腦及存取權限、並利用該裝置作為切入點、在公司的網路基礎設施之間橫向擴展。在幾分鐘之內、他們已經掃描了網路的多個裝置、企圖搜尋漏洞。網路犯罪隨後更破解了落後的軟體、安裝遠端存取木馬程式。

攻擊者竊得頗高的存取權等級、足以造成系統性破壞並破壞信任。例如、他們可以藉機竊取或篡改分享受限之檔案中的機密資訊、發送電子郵件詐欺客戶、甚至執行銀行交易。如果不是Darktrace的人工智慧系統及早發現犯行、公司或將遭受沉重的財務及聲譽損失、甚至可能嚴重打擊其營運能力。

雖然駭客已避開邊界防禦系統、但Darktrace的人工智慧系統仍將其活動與公司的正常「生活模式」比對、將其鑑識為惡意行為。Darktrace能夠即時偵測出威脅、破解攻擊行動、避免重大損害發生。

3. 網路釣魚詐騙截奪製造商網路

產業：製造業

進入點：透過電子郵件發送的惡意附件

明確目標：鑽企業網路的漏洞、進行隱藏式網路釣魚攻擊

雖然大多數網路攻擊者的目的是竊取或破壞數據、但有越來越多的駭客企圖奪取公司網路基礎設施、從中獲利。這種攻擊通常與加密貨幣挖礦有關、而網路截奪手法層出不窮、花樣也不斷翻新。

在一家香港建材製造公司、Darktrace 發現公司的內部網路已被網路犯罪分子侵入、用來進行大規模、侵略性的網路釣魚攻擊。

入侵由公司一名員工打開內含惡意代碼的電子郵件附件開始。這種侵入手段很常見、可讓犯罪者破壞員工的電腦、並寄居在系統的電源及網路連線系統中。

然後、犯罪分子可以隱藏他們的活動、防止他們的 IP 地址曝光、並且更容易規避偵測及可能的檢控。

攻擊者試圖使用所奪取的裝置向俄羅斯數千個不同的地址發送惡意電子郵件。這些電子郵件看起來正規而合法、且以收件人的母語撰寫、引發受害者提供銀行帳戶資料。

如果未被檢測出來、這類垃圾郵件活動將會導致該製造商的 IP 地址被列入黑名單、妨礙其電子郵件通信。對供應鏈的影響將會削弱其營運功能、商業信譽及收益。所幸 Darktrace 具備學習每個用戶及裝置的「生活模式」的能力、得以立即將此行為辨識為重大偏差。

Darktrace Antigena 的反擊

Darktrace Antigena 在數秒鐘之內便做出反應、自動限制受感染裝置的流量、阻止發送電子郵件。

在攔阻惡意行為的同時、公司仍能維持正常營運。由於 Darktrace Antigena 高速反擊、讓安全團隊爭取到足夠的時間、在破壞發生之前解決感染威脅。

4. IT公司的重大攻擊受挫

產業： 技術
進入點： 軟體錯誤
明確目標： 竊取公司機密資訊

一家台灣IT公司的網路防禦系統頗為先進、但Darktrace的Enterprise Immune System 部署不到一週、就發現該公司網路的資安威脅。

在安裝時、Darktrace 發現網路已有惡意活動。人工智慧系統偵測出活動屬於異常行為、並向公司發出警告。

網路攻擊者當時準備利用緩衝區溢位入侵、這是在一台伺服器上運作的應用程式內嚴重但廣為所知的軟體錯誤、可讓攻擊者盜取相鄰的記憶體並存取應用程式所使用的大量暫存員工資料。

這樣的漏洞可能造成嚴重的損害。高價值的敏感數據已透過例行攻擊洩露、數據如果持續被竊也可能令公司客戶陷入風險。

Darktrace 的人工智慧系統在確認攻擊者對應用程式執行程式碼的異常行為之後便向公司發出警告。Enterprise Immune System 快速、精準偵測出入侵事件、讓公司得以立即採取行動。公司資安團隊因此得到關鍵的資訊和寶貴的時間、得以防止危害加深。

5. 阻止5、000份文件被加密

產業： 金融服務

進入點： 透過網路釣魚電子郵件發送的惡意附件

明確目標： 加密關鍵文件並以解密金鑰勒索贖金

勒索軟體仍然是目前最嚴重的資安威脅之一。新的病毒株幾乎天天出現、企業的資安長絕不能掉以輕心。歐盟GDPR個資法等新法規的發佈、使得對敏感資訊的全面可見性與控制的需求變得更為迫切、企業所面臨的挑戰也更加艱鉅。

在一家技術與媒體投資公司、一名投資助理打開了一封惡意電子郵件的附件、無意中下載了勒索軟體檔案。受感染的裝置隨即被連接至GandCrab勒索軟體的基礎架構、並立即企圖出手加密近5,000份內部文件、還加入文件、包含勒索解鎖贖金的聲明。在裝置下載可執行檔案的那一刻、Darktrace便已將該威脅識別為精密的勒索軟體。

Darktrace Antigena 的反擊

Darktrace Antigena攔阻受感染裝置的所有對外通信、鎖住感染的蔓延路徑、並防止數據繼續遺失。

如果Darktrace的人工智慧系統未在數秒鐘內做出反應、大量高度敏感的財務資訊可能已被加密。可對抗機器速度攻擊的快速自自主防禦、讓公司免於遭受巨大的經濟損失及聲譽損害。

Darktrace 簡介

Darktrace 是全球首屈一指的人工智慧資安防禦公司。公司旗下的 Enterprise Immune System、全球數以千計的客戶、是企業在即時偵測及抵禦網路攻擊的強大後盾。具備自學能力的人工智慧系統可保護雲端、SaaS、企業網路、物聯網及工業系統免受內部威脅、勒索軟體、潛伏性攻擊及無聲攻擊等各種網路威脅及資安漏洞的傷害。Darktrace 在全球各地共設有 40 個辦事處及超過 800 名員工。Darktrace 總部分別設於美國舊金山及英國劍橋。

Darktrace © Copyright 2018 Darktrace Limited 版權所有。保留一切權利。Darktrace 為 Darktrace Limited 的註冊商標。Enterprise Immune System 及 Threat Visualizer 為 Darktrace Limited 的未註冊商標。
本文中包含的其他商標均為其各自所有者的財產。

聯絡我們

亞太地區：+65 6804 5010
台北: +886 2 8729 5868
北美：+1 (415) 229 9100
歐洲：+44 (0) 1223 394 100
info@darktrace.com
darktrace.com