


# 賽門鐵克領先業界的ScriptNN神經網路模型機器學習技術，有效拆解日新月異的網路釣魚伎倆

2025 年 4 月 1 日發布



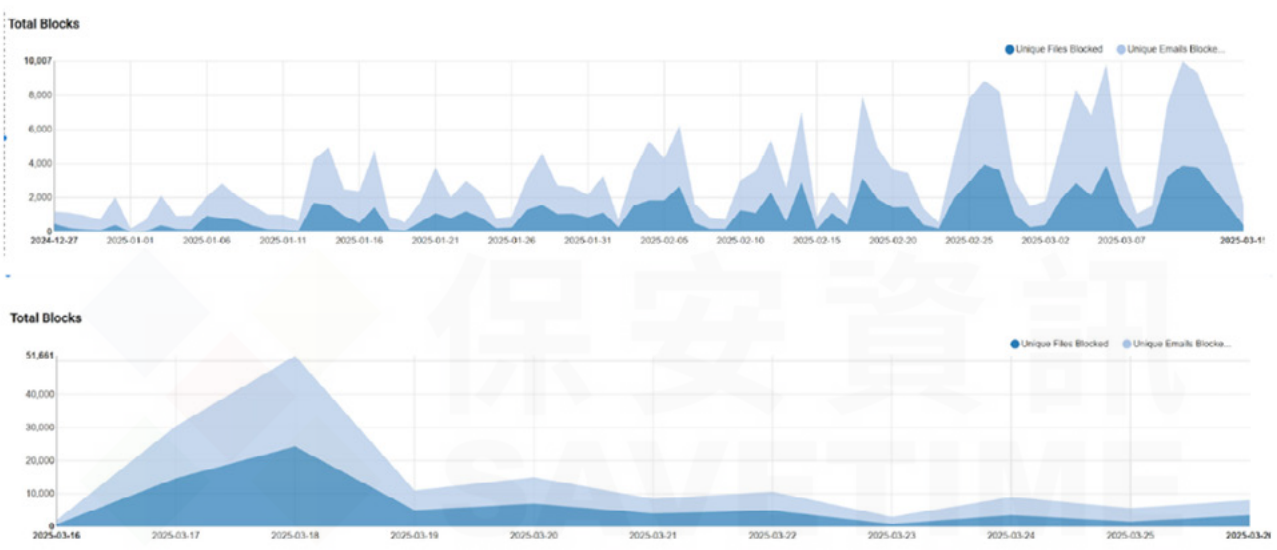
網路釣魚是一種非常常見的社交工程攻擊手法，它試圖透過發送欺詐性通訊 (通常透過電子郵件或簡訊) 來竊取使用者資料，這些通訊來源看起來出於合法。網路釣魚主要在惡意軟體攻擊的第一階段使用，其最終目標是偵察或入侵。惡意軟體作者製作的網頁看起來與不知情的使用者日常會提交個人或敏感資訊 (通常稱為「PII」或「個人識別資訊」)的網站相似甚至相同，例如：電子郵寄地址、帳號名稱、密碼、信用卡號碼等。一旦這些資訊遭竊取，就很容易滲透到該用戶的機器或企業網路中，並根據攻擊的性質和意圖引入額外的惡意軟體、竊取資料或造成更嚴重的損害。傳播網路釣魚頁面最常用手段是透過電子郵件，賽門鐵克的使命是持續創新以保護我們的企業電子郵件客戶免受惡意行為者攻擊，我們採用一種稱為 ScriptNN 的進階機器學習 (SML) 技術來掃描電子郵件並攔截阻擋此類型的網路釣魚頁面。

## 什麼是 ScriptNN

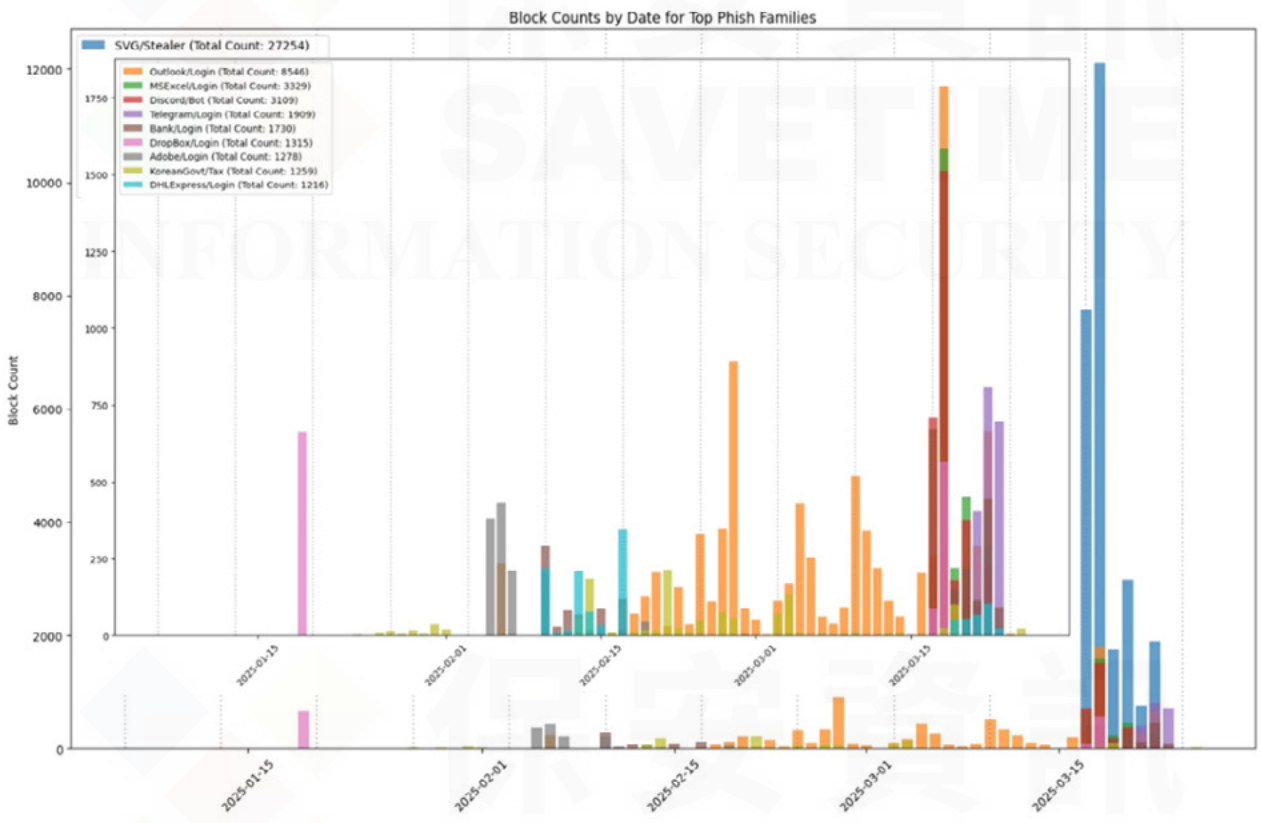
ScriptNN，即「HTML 和 JavaScript 神經網路模型 (Neural Network-based)」的縮寫，可掃描電子郵件附件中的 HTML 和 JavaScript 內容，並使用基於深度神經網路的機器學習 (Deep Neural Network-based Machine Learning (ML)) 模型，該模型經過訓練以通過分析數百萬個頁面 (包括乾淨頁面和已被識別為網路釣魚嘗試的頁面) 來區分網路釣魚企圖和合法網頁，使其能夠偵測與攔截零日攻擊，同時避免對有效電子郵件的錯誤阻止 (誤攔)。ScriptNN 模型採用最先進的工程架構，在磁碟和記憶體上的佔用空間極小，並採用極快的掃描和檢測模型 (每次掃描只需微秒)，確保我們的電子郵件伺服器和電子郵件終端使用者，不會因為這項技術的導入而感受到任何明顯的時間落差。此類模型的挑戰性任務在於如何將誤報幾乎降至可忽略的程度--這意味著不應阻止任何乾淨的附件，以免接收者未能收到電子郵件。我過去幾個月來，我們的 ScriptNN 模型的誤判次數都是零。

## ScriptNN 的優點

下面的圖表顯示由 Symantec 保護的電子郵件伺服器上，ScriptNN 在過去 3 個月內對釣魚頁面的偵測與攔截實績。圖表分為兩個部分，分別是 3 月 16 日之前和之後，以顯示常規趨勢和激增趨勢。在 3月 17 日和 3 月 18 日，出現顯著的激增。




在封鎖網路釣魚網頁的同時，我們也會追蹤網路釣魚家族和釣魚手法的趨勢。如今，除了舊的假登錄頁面 (如：Microsoft／Adobe／Dropbox 登錄) 外，還使用各種新的網路釣魚技術。二進位格式的 SVG 圖檔，能夠輕鬆在瀏覽器中呈現，越來越多被用來繞過基於文本的掃描器。我們最近經歷一次巨大的激增，保護我們客戶環境內的數千個企業端點 (請參閱下文)。Discord 機器人也被大量使用來欺騙使用者，讓他們誤以為有來自授權或已知角色的直接訊息 (DM)，要求他們點選連結或在與某些優惠、贈品、服務續訂或付款驗證等相關的連結上提供憑據，有時甚至會讓用戶經歷一個假驗證碼。類似的技倆也套用在 Telegram 的即時訊息。在某些情況下，被盜取的憑證直接張貼到 Telegram 上。我們定期看到針對特定客戶在特定地區發送有針對性的網路釣魚，有時使用假政府授權頁面。快遞送貨的網路釣魚驗證頁面也在上升。一些網路釣魚是自動化的，通過機器人在特定的星期幾發送 (垂直虛線表示的星期一)。所有這些網路釣魚攻擊呈波浪式出現，如下所示。




在電子郵件伺服器上安裝賽門鐵克 ScriptNN 防護的最大好處，在於以深度學習為基礎的進階機械學習技術可辨識零日攻擊，而無需不斷自我重新訓練。相較之下，我們注意到上述的網路釣魚波在零日時，大多數其他廠商都無法偵測到。

欲深入瞭解更多有關賽門鐵克端點安全完整版(SESC)的詳細資訊--Symantec Endpoint Security Complete，請點擊此處。

欲深入了解賽門鐵克的端點多層次防護解決方案中「進階機器學習」防護技術，請點擊此處。

## 關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 已於 2019/11 併入全球網通晶片巨擘--博通 (BroadCom，美國股市代號 AVGO，全世界網際網路流量有 99.9% 經過博通的網通晶片 ) 軟體事業部的企業安全部門 (SED)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性，有著脫胎換骨並超越業界的長足進步。博通 (Broadcom) 是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec 持續創新的技術能為日新月異的資安問題提供更好的解決方案，近三年 Symantec 很少出現在由公關機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前，增長幅度也領先其他競爭對手，是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。( 美籍華人王嘉廉創辦的企業軟體公司，組合國際電腦（CA Technologies）以及雲端運算及「硬體虛擬化」的領導廠商--VMware， 也是博通軟體事業部的成員 )。2021 年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署（CISA）宣布聯合民間科技公司，發展全國性聯合防禦計畫 JCDC(Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵招的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

## 關於保安資訊 www.savetime.com.tw

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力專注在賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更孰悉用戶使用情境的優勢能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。許多顧客樂意與我們建立起長期的友誼，把我們當成可信任的資安建議者、可以提供良好諮商的資安策略夥伴以及總是第一個被想到的求助暨諮詢對象。

保安資訊連絡電話：**0800-381-500**。