賽門鐵克新增掃描／封鎖電子郵件相關的釣魚網頁先進技術：ScriptNN

2024 年 7 月 23 日發布

網路釣魚，簡單但有效的攻擊

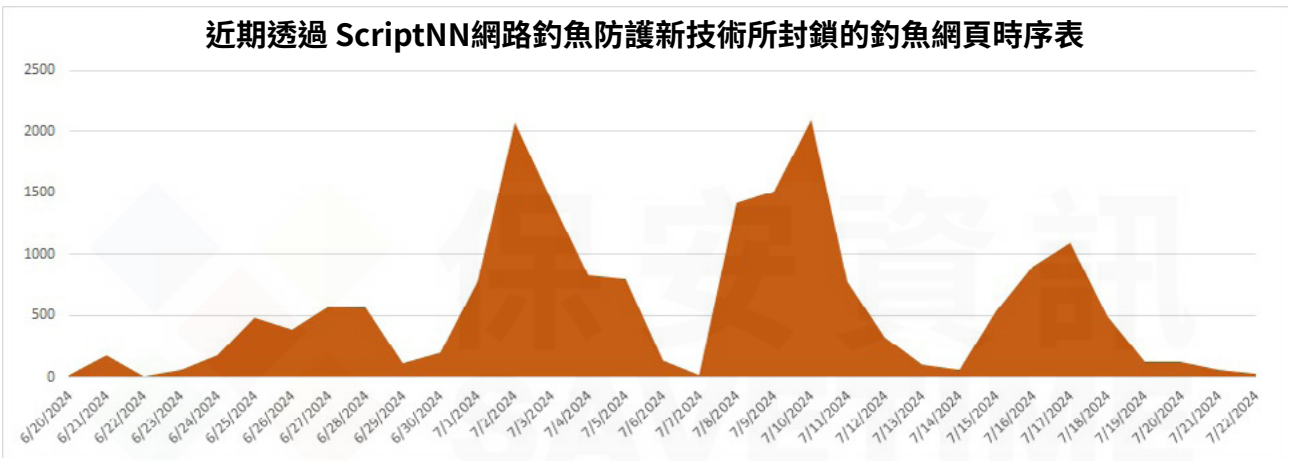
網路釣魚是一種非常常見的社交工程攻擊類型，通常透過電子郵件或簡訊 (SMS) 傳送看似來自合法來源的詐騙通訊，試圖竊取使用者資料。網路釣魚主要在惡意軟體攻擊的第一階段使用，不論最終目的是偵查或入侵。惡意軟體作者製作的網頁看起來與毫無戒心的使用者通常會需要輸入個人或敏感資訊 (通常稱為「PII」或「個人識別資訊」)，例如：電子郵件地址、使用者名稱、密碼、信用卡號碼等的網頁類似或甚至相同。一旦這些資訊被竊取，就很容易潛入使用者的機器甚至企業網路，並根據攻擊的性質和目的，呼叫或導入後續的惡意軟體、滲出資料或造成損害。賽門鐵克不斷創新，以保護我們企業電子郵件客戶免受惡意攻擊者的攻擊，而最常使用的傳播釣魚網頁方式就是透過電子郵件，作為賽門鐵克不斷創新的一部分，我們啟用一項新的先進技術，我們稱之為 ScriptNNto 來掃描電子郵件並封鎖這些釣魚網頁。

先進的網路釣魚偵測技術介紹

ScriptNN 是「HTML 與 JavaScript 神經網路模型」的縮寫，它會掃描電子郵件附件中的 HTML 與 JavaScript，並使用以深度神經網路為基礎的機器學習 (ML) 模型，該模型經過訓練，可透過分析數百萬個乾淨網頁以及已識別釣魚企圖的網頁，區分釣魚企圖與合法網頁。該模型會不斷更新，以便能夠識別零時差攻擊，同時避免誤攔有效的電子郵件。ScriptNN 模型採用最先進的技術架構，在磁碟和記憶體上佔用空間極小，並採用極快的掃描和偵測模式 (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延遲與效能耗損。

ScriptNN 的優點與風險

根據學習階段所收集的資料，我們預期 ScriptNN 初期每天可在我們的電子郵件防護空間中封鎖超過一千封的釣魚郵件。下圖顯示的是初步版本的實際現場攔截情況，隨著分析資料的增加，下圖也將不斷更新和改進。



ScriptNN 在識別通用檢測遺漏方面有很大幫助，而隨後的通用檢測改進實際上是第二層保護。舉例來說，最近的 Telegram Bot API 網路釣魚攻擊就被 ScriptNN 偵測到，並建立和釋出通用特徵來阻擋這些攻擊--補足現有的防護措施。另一方面，HTML 和 Javascript 是用來建立網路釣魚攻擊的主要運算語言，這兩種語言都因未使用強大的程式設計標準而聲名狼籍。這兩種語言也在不斷演進，所以在這個範疇與領域中幾乎不可能有百分之百零失誤的技術。因此，我們不會吹捧 ScriptNN 可以提供 100% 的涵蓋率，不過我們可以據實陳述，在我們廣泛的測試過程中，很少發生錯誤的判斷。即便極少發生的漏攔或誤攔的情況時，我們會有專門的團隊立即進行修正更新，並對引擎採取永久性的補救措施，以避免這些事件再次發生。

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。
欲深入瞭解賽門鐵克端點防護 (SEP) 的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好用資源。
保安資訊連絡電話：**0800-381-500**。