即使採用混淆技術的的網路釣魚攻擊也不是賽門鐵克Stargate(*星際之門)安全引擎的對手

2022 年 12 月 15 日發布

網路釣魚是最常見的社交工程攻擊之一，用於欺騙警覺性不足的人向攻擊者透露敏感資訊，以竊取機密及值錢的資訊，包括登錄憑證和信用卡號碼，受害者往往已經上鉤自己還不知道，並可能對受害者造成相當大的傷害。網路釣魚也是網路犯罪活動最常見的形式之一，特別是針對企業組織，網路釣魚攻擊在 2022 年顯著增加。地下市場上有大量的網路釣魚工具包可取得且價格便宜，賽門鐵克無時不刻都會攔阻新的網路釣魚攻擊。上周也不例外。

12 月 5 日，我們全天候的監控系統對暴增的惡意電子郵件流量發出警報。

經立即調查發現，我們的 Stargate (*星際之門) 安全引擎（由我們的電子郵件安全服務--Email Security Service 簡稱：ESS 所提供）憑藉其先進的啟發式威脅檢測能力，主動阻斷每一個暗度陳倉的電子郵件攻擊，其中隱匿經混淆化的程式碼（或在這種情況下試圖隱匿），伺機發動攻擊。一旦解除混淆並運行，該程式碼就會以 HTML 為目標，試圖透過網路釣魚來獲取和竊取微軟 Office 365 的登錄憑證和密碼。如果受害者被成功引誘，被盜資訊將被上傳到由攻擊者所控制的 C&C 伺服器，受害者就任人宰割了。

攻擊發動者竭盡全力以隱藏感染媒介以避免被發現，再加上通常會利用看起來完全合法的『釣魚』頁面或快顯視窗，毫無戒心的被攻擊目標幾乎不可能發現。幸運的是，賽門鐵克 ESS 客戶可以安然無恙，因為『星際之門』安全防護的進階啟發式引擎為他們做到這一點，足以讓攻擊者落荒而逃。

賽門鐵克擁有領先業界的 **零時差** 保護技術，以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malscript!gen2

郵件安全防護機制：

不管是地端自建 (SMG／SMSEX) 的郵件過濾／安全閘道及主機防護、雲端郵件安全服務 (E-mail Security.Cloud) 以及郵件威脅隔離 (ETI)，都能提供終端用戶隔絕或隔離威脅於境外的保護 (威脅不落地)。

欲瞭解更多有關 Stargate--基於機器學習、雲知識和深度內容檢查的威脅檢測平臺的資訊，請在此聯繫 賽門鐵克。

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 年起就全心全力於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環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。保安資訊連絡電話：**0800-381-500**。