



祝福的季節--謹防禮券和獎勵計畫詐騙

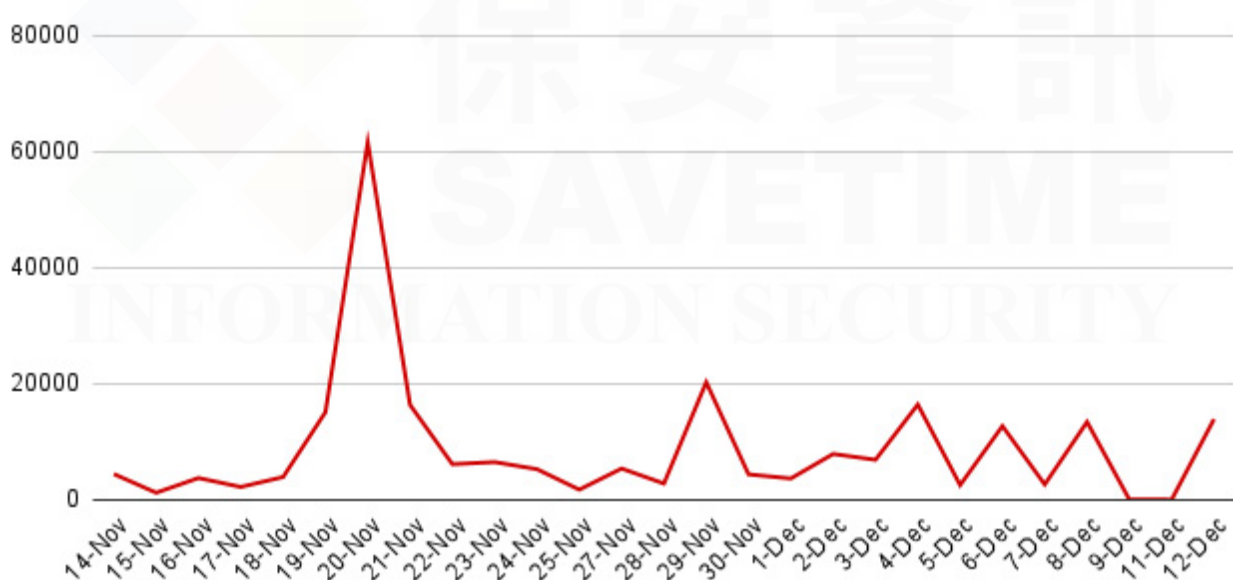
2023 年 12 月 19 日發布

[點擊此處可獲取--最完整的賽門鐵克解決方案資訊](#)

正值年終節慶期間，禮品卡和獎勵計畫詐騙猖獗。這是永遠不會退流行的騙術，至今在全世界仍被廣泛使用，特別是在禮券和禮品銷售旺季前後更是明顯增加。這些惡意禮券和獎勵計畫詐騙通常屬於網路釣魚攻擊的範疇。它們通常利用人性貪圖免費贈品和優厚折扣的弱點。

具體情況如下：網路釣手會傳送誘人的資訊，誣稱你抽中了某知名品牌的免費禮券或某些特別獎勵。一旦有人上鉤，點擊連結或按照他們的指示操作，用戶可能會被要求提供個人資訊或下載含有惡意軟體的檔案。有些人甚至會誘騙用戶先付款以領取他們的『免費』禮物。這是一種典型的誘騙行為，讓受害者兩手空空，敏感資訊也可能洩露。

賽門鐵克掌握大量的攻擊行動，最近幾周出現的大量釣魚網頁數量 (超過28萬~283k) 引起我們的注意。以下是我們觀察到的與該行動相關的釣魚網頁數量。



這些釣魚網頁上架在 294 個最近才註冊的域名的網站，這些域名似乎是運用 DGA(動態網域產生演算法) 來混淆視聽，顧名思義，網域清單會動態不斷的隨機產生。這些域名稱使用不常見的頂層網域名 (TLD)，例如：beauty、boats、bond、cfd、fun、homes、lat、monster、sbs……等。範例如下：

- masonblackwell[.]beauty
- harmonyx[.]cfd
- jayleo[.]bond
- nebulashift[.]boats
- eliwhitestudio[.]monster

這類社交工程騙術和攻擊通常是針對消費者，但企業用戶受到的影響也不小。事實上，私人與公務上的上網界線已變得越來越模糊。員工在辦公時間使用公司電腦，可能也會不小心落入設局圈套，給公司的基礎設施帶來巨大風險。

賽門鐵克已經於第一時間提供多種有效保護 (SEP/SESC/SMG/SMSEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 多重防護技術能在第一時間就偵測到該惡意程式及有效對應零時差攻擊的防護機制及其威脅名稱：

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)。

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類/過濾/安全服務)：

被發現的惡意網域名稱/IP位址已於第一時間收錄於不安全分類列表中。

建議客戶啟用 WebPulse 即時分類功能，以獲得最佳保護。[請點擊此處獲取配置 WebPulse 說明。](#)

欲深入瞭解有關賽門鐵克基於雲的網路安全服務 (WebPulse) 的更多訊息，[請點擊此處。](#)

欲深入瞭解更多有關賽門鐵克郵件安全雲端服務 (Email Security.Cloud) 的詳細資訊，[請點擊此處。](#)

Symantec
A Division of Broadcom

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。

保安資訊
KEEPSAFE
INFORMATION SECURITY

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, 以及基於比原廠更熟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。