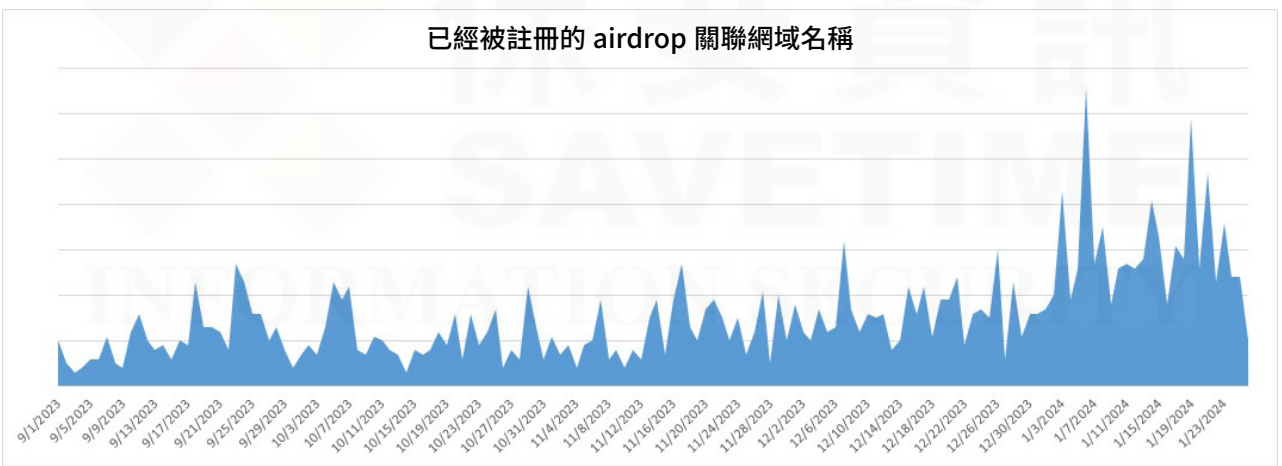
如何避免空投(Airdrop)騙局？賽門鐵克發現以加密貨幣熱門流行語為幌子的惡意網域名稱

2024 年 1 月 30 日發布

利之所在、趨之若鶩～隨著加密貨幣孳生的網路犯罪的日益增加，在我們對威脅環境的持續監控過程中，賽門鐵克發現一大批可疑的網域名稱 (800 多個)，它們的名稱中使用『airdrop(*空投)』。Airdrop一詞通常與更廣泛的加密貨幣領域相關聯，加密貨幣空投是指將數位資產從加密貨幣專案轉帳分發至多個錢包位址。這種分發可以出於各種原因，例如：推廣新專案、獎勵現有加密貨幣持有者或鼓勵用戶採用。Airdrop 通常被用作一種行銷策略，以提高知名度並吸引更多用戶。

不幸的是，那些心懷不軌的人也注意到這些熱門流行語，並在他們的網域名稱或計畫中使用 Airdrop(包括些許的變化) 一詞，以利用該詞在加密貨幣社群的流行和熟悉程度。在過去 6 個月中，已有 2700 多個黑心網域名稱使用這個熱門流行語。



加密貨幣和 Airdrop 的關聯造成合法的假像，吸引對接收免費代幣或貨幣感興趣的人。事實上，網域名稱資料庫目前紀錄有 5,800 多個網域名稱包含『airdrop-』、『-airdrop』或『aiirdrop』字樣。賽門鐵克已對這些網域名稱進行審查和適當分類，並對惡意或可疑的網域名稱進行特別警示。

在最近觀察到可疑網域名稱中，大部分都是透過 Cloudflare 或 DDoS-Guard Ltd (俄羅斯) 的IP所代管的，還有一些分佈在熱門的社交媒體平臺上。一些案例包括仿造已知區塊鏈平臺 (例如：Manta Network) 和加密交易服務所 (例如：Binance 和 Coinbase) 的網域名稱。雖然有些網域名稱是活躍的，但許多網域名稱目前還不是，但以後可能會與網路釣魚、詐騙或惡意軟體偷渡式下載有關。

賽門鐵克已經於第一時間提供多種有效保護**(SEP/SESC/SMG/SMSMEX/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：

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。

賽門鐵克端點防護(SEP)的瀏覽器延伸功能：

- 根據我們 2023 年 1 月發佈的瀏覽器延伸公告，如果瀏覽器延伸偵測到某個網址是惡意的，SEP 就會將用戶轉導向到賽門鐵克的預設封鎖頁面，通知已攔截 (注意，該瀏覽器延伸功能現在也適用於 Microsoft Edge 瀏覽器)。

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。
欲瞭解有關賽門鐵克端點防護 (SEP) 瀏覽器擴展的更多訊息，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**。