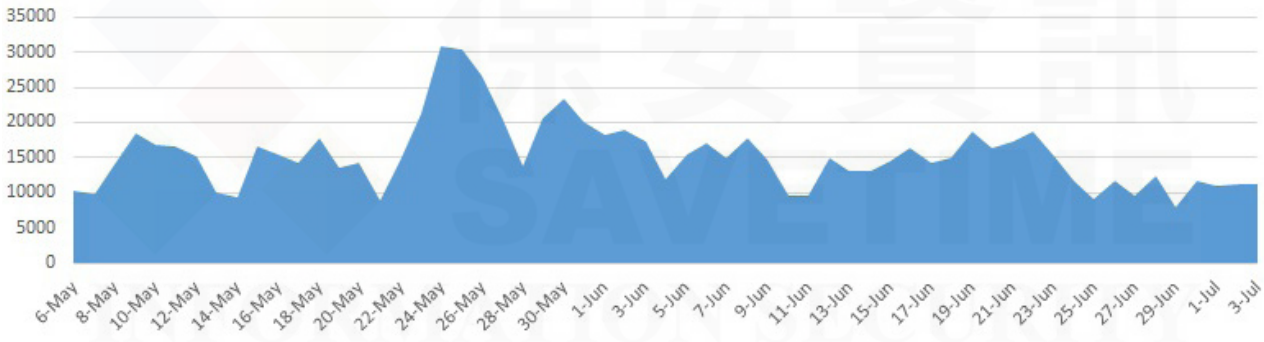
加密貨幣挖礦劫持

2023 年 7 月 3 日發布

透過瀏覽器也可以進行加密貨幣挖礦，它是在瀏覽器核心，運行腳本語言。這種方法與更常見的加密貨幣開採程式的方法不同，後者需要下載和運行一個專用的挖礦程式。如果網頁中被注入了一個加密貨幣挖礦腳本，那麼只要瀏覽該網頁的用戶處於瀏覽狀態，他們電腦上的運算效能就會被暗中用來挖掘加密貨幣。一些網站可能改絃易轍以加密貨幣挖礦取代廣告來增加營利，只要告訴客戶在瀏覽該網站時，他們的 CPU 效能將被用於挖掘加密貨幣，這就可以。然而，一些網站在客戶不知情或不同意的情況下，暗中利用瀏覽網站的電腦或手機／筆電等行動裝置的運算資源來挖掘加密貨幣。這被稱為加密貨幣挖礦劫持。賽門鐵克每天都會阻止成千上萬的此類攻擊。

IPS 阻止網頁式加密貨幣挖礦劫持



典型的藉由瀏覽器的挖礦劫持場景中，攻擊者駭入一個網站，並在網站中注入幾行 JavaScript 的惡意程式。這個被注入的惡意程式碼會讓瀏覽該網站的電腦為駭客挖掘加密貨幣 (挖礦)。門羅幣 (Monero) 就是一個可藉由瀏覽器來挖礦的典型案例，該加密貨幣使用RandomX 演算法，這是一種適用於某些 PoW 區塊鏈的演算法。從過往的案例來看，加密劫持要麼利用基於 JavaScript 的加密劫持服務，例如：2017 年引起軒然大波的 Coinhive，要麼依靠遭駭的外掛程式或惡意的瀏覽器擴充功能來提供惡意的 JavaScript。

與勒索軟體等威脅不同，勒索軟體會立即中斷受害者對其設備的存取，而加密貨幣挖礦劫持可以在受害者意識到發生什麼之前，在其設備上悄悄進行很長時間的運算效能盜用。即使是完全安裝最新修補程式的設備也可以透過基於流覽器的挖礦成為受害目標。這種加密貨幣挖礦劫持的主要影響與電腦效能有關。潛在的影響包括設備性能變慢，電池過熱，設備變得無法使用，以及在雲端運行的企業因用電量增加而導致成本增加，這些企業是根據 CPU 的使用量來收費的。此外，客戶和商譽的損失也是對網站所有者和企業的潛在影響。

一些加密劫持的案例包括：

- 2023年2月，針對 Kubernetes Cluster 進行 Dero 挖礦的加密劫持行動。
- RapperBot DDoS 惡意軟體將加密劫持作為新的收入來源。
- 暴露在網際網路上的 Linux 和物聯網（IoT）設備在暴力攻擊中被劫持，這是最近觀察到的加密劫持行動的一部分。

賽門鐵克的入侵預防系統（IPS）技術透過使用多種檢測來阻止相關的惡意網路活動，保護客戶免受基於流覽器的加密劫持，其已識別方式如下：

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- Web Attack: JSCoinminer Download*
- Web Attack: JSCoinminer Website*

*星號代表多個類似名稱的檢測，例如：Web Attack: JSCoinminer Download 1、Web Attack: JSCoinminer Download 2……等等。

欲瞭解更多有關於賽門鐵克端點安全入侵防護系統 (IPS) 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**。