


# 應對惡意XMRig挖礦應用程式 賽門鐵克游刃有餘

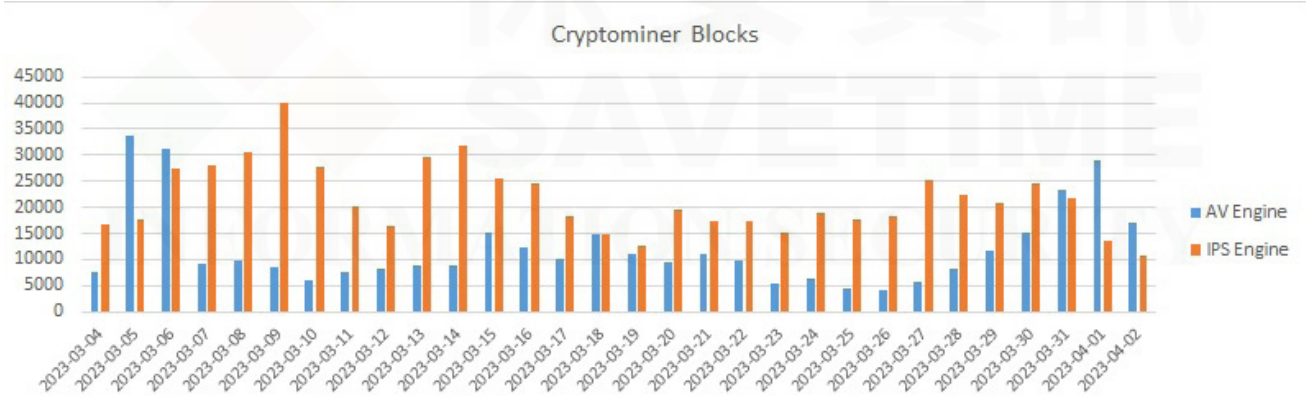
2023 年 4 月 3 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

XMRig 是一種占用 CPU 的熱門的開放原始碼密貨幣挖礦應用程式，常用於開採門羅幣 (XMR)。雖然 XMRig 是一種合法工具，但它經常被惡意軟體作者用來在遭駭入的系統未經用戶同意的情況下使用（即竊取）其運算能力來開採門羅幣。這種做法稱為加密劫持。從這點上，當我們提到 XMRig 時，我們指的是加密劫持之案例。

XMRig 雖然很流行，但它只是眾多不受歡迎的加密挖礦程式中之一種，其中一些會先被我們的防毒--AV (檔案分析) 引擎技術阻止，而另一些則被我們的 IPS (網路流量分析) 技術捕獲，具體取決於特定的感染方式。這裡用『先』是因為大多數都會被這兩種防護技術攔截，但一旦威脅被移除，它通常不會觸發後續防護技術，所以績效會列入先攔截。也就是說，威脅的某些元件可能會被一種防護類型攔截，而同一威脅的其他元件可能會被不同的技術攔截。這其實凸顯『多層式安全』的重要性。

下圖顯示過去一個月所攔截的 AV／IPS 分類。




*此處包含的 XMRig 只是賽門鐵克阻止眾多不需要的加密挖礦程式之一。*

XMRig 可能會使用造駭入電腦的中央處理單元 (CPU) 和／或圖形處理單元 (GPU) 70% 到 80% 的效能。當 XMRig 執行時，用戶可能會注意到他們的電腦執行速度比平時慢，遊戲或應用程式運作不順暢或停頓。根據當時電腦的狀況，它也可能會變得很熱，進而可能對硬體元件造成損壞。長時間使用也會比平時消耗更多的電量，所以可能會增加電費。

XMRig 成為惡意軟體作者的熱門選擇有以下幾個原因：

- XMRig 相對易於使用和設定，即使是新手網路犯罪份子也可以使用它。
- XMRig 是開放原始碼，這意味著它的程式碼可供任何人免費修改和散播。惡意軟體作者可以輕鬆修改程式碼以試圖逃避檢測並增加利潤。
- 門羅幣 (Monero) 是一種廣受歡迎的加密貨幣，因為它被設計成使用 CPU 的效能進行挖礦，進而更容易使用遭駭入系統的殭屍網路進行大規模挖礦。
- XMRig 效率高，可以在不消耗過多系統資源的情況下，以相對較高的速率挖掘門羅幣，使其成為加密貨幣劫持的理想選擇。

XMRig 挖礦程式透過多種方式傳播，包括網路釣魚和其他類型的電子垃圾郵件、惡意廣告、惡意植入程式、漏洞利用、破解軟體、潛在有害應用程式 (PUA)、網頁瀏覽時的順道下載等。

賽門鐵克對 XMRig 進行長期檢測，並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 **零時差**防護技術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：**

- CL.XMRig!gen1
- Miner.XMRig
- Miner.XMRig!gen*
- OSX.Miner.XMRig!g1

**基於行為偵測技術(SONAR)的防護：**

- SONAR.Suspdrop!g61

**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)。

**基於機器學習的防禦技術：**

- Heur.AdvML.*

* 這表示存在多個類似名稱的檢測，例如：Heur.AdvML.B, Heur.AdvML.C 等

要了解有關賽門鐵克端點安全安全完整版更多資訊，請點擊此處。
要了解賽門鐵克行為安全性技術如何防禦就地取材攻擊的威脅，請點擊此處。
要了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。
要了解 Symantec Endpoint Protection 如何使用進階機器學習，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**。