保安資訊有限公司--賽門鐵克解決方案專家--原廠防護亮點分享

加密貨幣挖礦攻擊不斷

2023 年 8 月 8 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

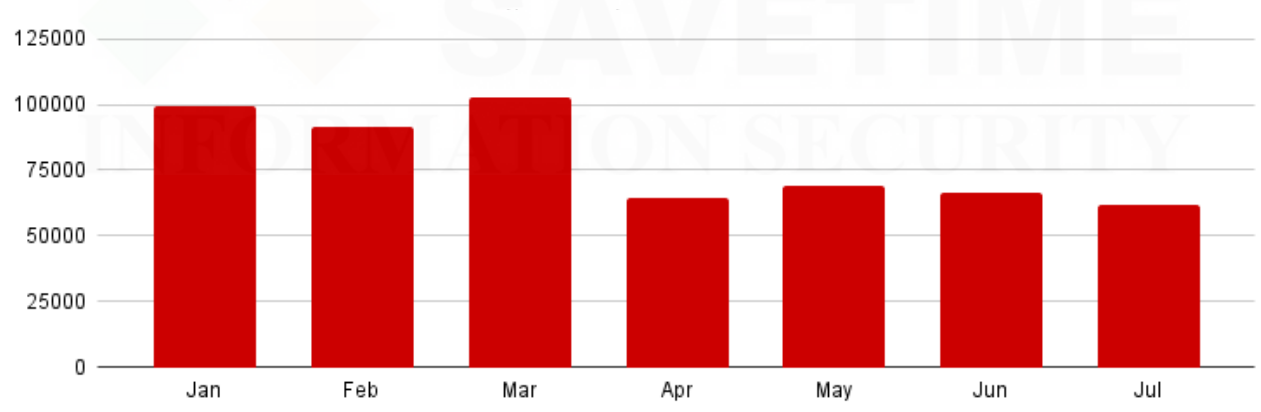
自從比特幣騰空出世以來，加密貨幣挖礦生態就在網路世界佔有一席之地。多年來，隨著數位金融的普及和市場的擴大，加密貨幣挖礦活動也穩步增長。許多個人和組織將加密貨幣挖礦視為一個前景可期的投資機會，利用他們的運算能力來挖掘加密貨幣並期待致富發財。

然而，隨著加密貨幣日益主流化，該領域也引起了網路犯罪分子的覬覦。許多消費者和企業不知道的是，他們的電腦和基礎設施成為了加密貨幣挖礦攻擊的主要目標。

這些惡意加密貨幣挖礦程式背後的網路犯罪分子設計了各種複雜的技術來感染系統並秘密入侵運算資源。他們利用惡意電子郵件、遭入侵的網站、偷渡式下載和漏洞開採利用等伎倆來取得機器的存取權限（以及常駐和橫向移動），隨後神不知鬼不覺地剝削它們的運算資源默默地成為挖礦電腦。

這些網路掏金客總會使用客製化挖礦程式和合法化挖礦程式如吸血鬼般地拼命挖礦。儘管存在對合法挖礦程式的潛在濫用，賽門鐵克長期以來一直對其進行檢測。賽門鐵克每個月都偵測到數萬次以上的挖礦攻擊。

賽門鐵克攔截的挖礦攻擊達數萬次 / 月



這些挖礦攻擊活動的影響甚鉅。對消費者而言，常見的症狀包含電腦運行速度緩慢、電費意外飆升以及設備電池壽命縮短的情況。對於企業來說，後果更為嚴重，包括關鍵運營中斷和潛在的資料外洩。

賽門鐵克提供的單一解決方案內建多層級防護技術，個別技術多能在第一時間就具備**零時差**防護的能力並有明確的定義，僅就不同防護技術說明如下：

基於行為偵測技術(SONAR)的防護：

- SONAR.Bluwimps*
- SONAR.CoinMiner*
- SONAR.Coinbitminer!g1
- SONAR.GhostMiner!gen1
- SONAR.Gosopad!gen5
- SONAR.Miner*
- SONAR.Suspdrop!g61

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.XMRig!gen1
- Linux.Coinminer
- MSH.Gosopad
- Miner.Bitcoinminer
- Miner.Burst
- Miner.Cpuminer
- Miner.Jswebcoin*
- Miner.Neoscrypt
- Miner.Wasmwebcoin
- Miner.XMRig*
- Miner.Zcash!gen1
- Miner.Zcashminer
- OSX.Coinminer
- OSX.Miner.Coinminer
- PUA.Bitcoinminer
- Trojan.Adylkuzz
- Trojan.Coinbitminer
- Trojan.Coinminer*
- Trojan.Madominer
- Trojan.Minjen*
- Trojan.Shminer
- W32.Coinbitminer
- W32.Mysracoin
- W32.Rarogminer
- W32.Rarogminer!G1
- W32.XiaobaMiner

基於機器學習的防禦技術：

- Heur.AdvML.*

欲深入瞭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。

欲深入瞭解更多有關於賽門鐵克端點安全完整版(SESC)的詳細資訊--Symantec Endpoint Security Complete，請點擊此處。

欲深入瞭解賽門鐵克端點防護 (SEP) 的進階機器學習防護技術，請點擊此處。

欲深入瞭解賽門鐵克 (DCS：Data Center Security～資料中心安全的更多訊息，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**。