常見的網頁含挖礦程式判斷與防護指南

重點摘要

- 近年來，加密貨幣興起，虛擬貨幣已成為投資寵兒，市值不斷成長，致使越來越多人投入挖礦熱潮，除自建挖礦機外，有心人更將挖礦程式植入其所有之公開網站或其已掌控弱點的網頁中，利用網路瀏覽者的系統資源協助其挖礦；若使用者不慎瀏覽這些網站，將遭利用成為礦工。
- 使用者在瀏覽網頁時，若發現系統效能異常降低，應有所警覺，並開啟瀏覽器的開發者工具(例如Chrome可透過F12開啟)，檢視該網頁是否含有coinhive.min[.]js之類的挖礦程式。
- 若不想成為別人的礦工，使用者可於瀏覽器中安裝如AdBlock Plus等合法廣告過濾程式，或是諸如AntiMiner、MinerBlock或No Coin等瀏覽器外掛程式，阻擋已知的挖礦程式，封鎖挖礦行為。

防護建議

- 使用者在瀏覽網頁時，若在非預期情況下，發現系統效能持續降低，應提高警覺。使用者若要判斷所瀏覽的網頁是否含有挖礦程式，可在瀏覽網頁時，開啟瀏覽器的開發者工具(例如Chrome可透過F12開啟)，檢視該網頁是否有下列之挖礦程式碼，若有，建議應通報TWCERT/CC。常見的部分挖礦程式碼如下：
  - digxmr[.]com/deepMiner.js
  - coin-hive[.]com/lib/coinhive.min.js
  - crypto-loot[.]com/lib/miner.min.js。
- 使用者可於瀏覽器中安裝防止挖礦程式執行的合法外掛程式，例如AdBlock Plus、AntiMiner、MinerBlock或No Coin，來阻擋已知的挖礦程式。

防護建議

- 網站管理者若發現其網站遭植入挖礦程式，應在確認惡意程式碼所在位置後移除之，並全面檢查與強化系統的安全性，以降低再次被利用挖礦的風險。
- 網站管理者應隱藏網站伺服器、網頁開發框架等系統資訊，避免開啟未使用的通訊埠，及定期更新防毒軟體、作業系統及應用程式，以降低網站被攻擊利用的風險。

參考連結

1. Adblockplus. “Adblock Plus”, Retrieved February 7, 2018, from the World Wide Web: https://chrome.google.com/webstore/detail/adblock-plus/cfhdojbkjhnklbpkdaibdccddilifddb?hl=zh-TW
2. Adguard. “AdGuard廣告阻擋器”, Retrieved February 7, 2018, from the World Wide Web: https://chrome.google.com/webstore/detail/adguardadblocker/bgnkhhnnamicmpeenaelnjfhikgbkllg?hl=zh-TW
3. Tunghobrens. “Anti Miner - No 1 Coin Minerblock”, Retrieved February 7, 2018, from the World Wide Web: https://chrome.google.com/webstore/detail/anti-miner-no-1-coin-mine/ibhpgkhoicjhklmbhdoeikeggbeejonj
4. CryptoMineDev. “minerBlock”, Retrieved February 7, 2018, from the World Wide Web: https://chrome.google.com/webstore/detail/minerblock/emikbbbebcdfohonlaifafnoanocnebl
5. Keraf. “No Coin - Block miners on the web!”, Retrieved February 7, 2018, from the World Wide Web: https://chrome.google.com/webstore/detail/no-coin-block-miners-on-t/gojamcfopckidlocpkbelmpjcgmbgjcl