個案分析-

Smominru 挖礦攻擊事件

分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

107 年 4 月

I. 事件簡介

1. 2018 年 1 月底安全研究公司 Proofpoint 發現從 2017 年 5 月開始美國國家安全局外流的 EternalBlue 攻擊工具變身惡意程式 Smominru，專門攻擊 Windows 漏洞(CVE-2017-0144)來入侵 Windows 伺服器，使受害主機加入殭屍網路，進而讓受害主機挖掘門羅幣（Monero）。該公司研究人員判斷 Smominru 感染了超過五十萬台以上的 Windows 主機來建立殭屍網路，其中多半為伺服器，這些機器分佈世界各地，但密度最高地區依序為俄羅斯、印度及台灣。

2. 在學術網路中，從 2018 年 3 月開始也陸續出現 Smominru 的資安事件，經統計在 2018 年 3 月觸發的 Smominru 資安事件共有 71 件。從這些資安事件所偵測到的佐證資料中發現，可能礦池有 3 個(如下所列)，通常受害主機會連線一到兩個礦池。

   礦池 1: 78.142.29.152（xmr.xmr5b.ru:8888）保加利亞

   礦池 2: 170.178.171.162（170.178.171.162:8888）美國

   礦池 3: 170.178.171.173（64.mymyxmra.ru:8888） 美國

No	偵測規則	件數
1	Botnet:Smominru.Botnet	37
2	MALWARE-CNC Win.Trojan.Smominru outbound call	34

事件單編號:AISAC-[redacted]9

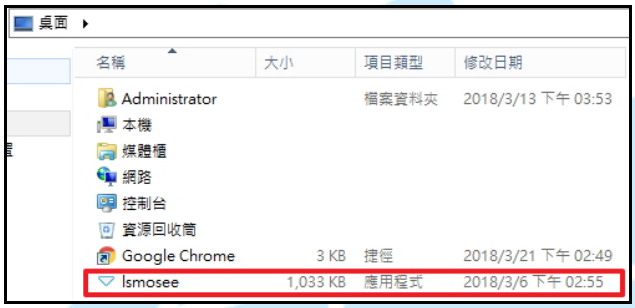
原發布編號	ASOC-INT-201803[redacted]1	原發布時間	2018-03-12 [redacted]:23
事件類型	對外攻擊	原發現時間	2018-03-11 [redacted]:42
事件主旨	通報:[[redacted]大學]140.[redacted].103 Botnet: Smominru.Botnet,		
事件描述	ASOC發現貴單位([redacted]大學)所屬 140.[redacted].103 疑似對外進行 Botnet: Smominru.Botnet, 攻擊		
手法研判	貴單位疑似對外進行非法攻擊，Smominru Botnet為美國國家安全局外流的永恆之藍（EternalBlue）攻擊工具，變成入侵 Windows 伺服器的有害程式「Smominru」。Smominru 使用「Windows Management Infrastructure」來散播並使受害電腦加入殭屍網路，進而讓受害主機挖掘門羅幣（Monero）。		
建議措施	惠請貴單位： 1.檢查防火牆紀錄：查看內部是否有開啟異常的連接埠，並查看內部是否有對外大量不同目的 IP 之異常連線 2.利用工具程式(如:TCPview、procexp)於來源主機觀察，找出實際執行連線的程式，確認該程式是否為惡意程式。 3.若連線並非預期行為，則來源主機可能已遭植入惡意程式，建議利用木馬或後門清除程式掃瞄該主機，並手動檢測是否有惡意程式執行。 4.參考資料： https://www.proofpoint.com/us/threat-insight/post/smominru-monero-mining-botnet-making-millions-operators		

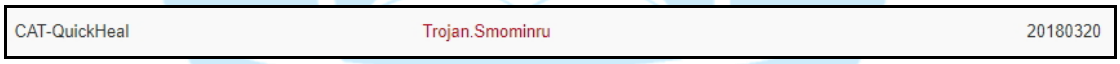
3. 為了瞭解該類型資安事件的觸發原因與攻擊行為，本中心取得樣本後進行檢

測。

II. 事件檢測

1. 首先，在開始檢測前，我們將 Smominru 的樣本 lsmosee.exe 送至 Virustotal 網站檢測，發現它被防毒軟體公司檢測出為惡意的比例高達 50/63，仍有 13 家公司無法檢測出的它的存在，其中只有 2 家公司稱它為 Smominru，其餘大多數的公司稱它為 Miner 或 CoinMiner。





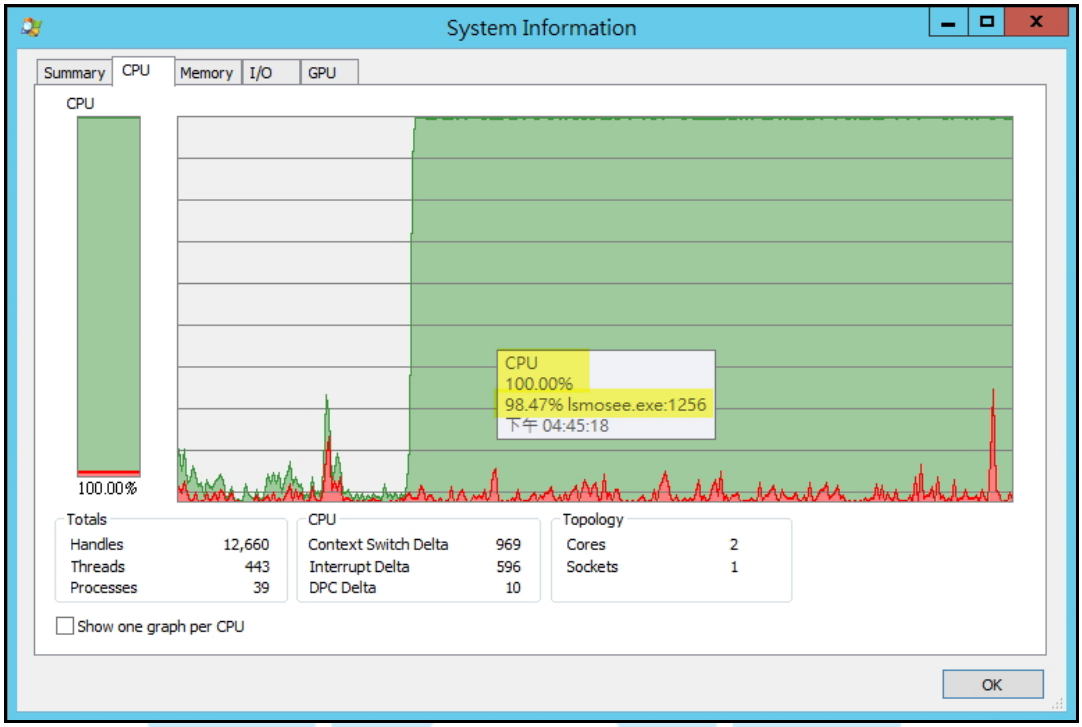
2. 在 Windows Server 2012R2 作業系統環境下，我們進行環境隔離檢測。在執行惡意程式 lsmosee.exe 後，檢視其對外連線狀況，發現會連至下列 IP 位置:

No	目的 IP	目的 Port	目的 IP 所屬國家
1	78.142.29.152	8888	保加利亞
2	78.142.29.152	13000	保加利亞
3	107.191.99.95	5555	美國
4	118.184.176.15	80	中國

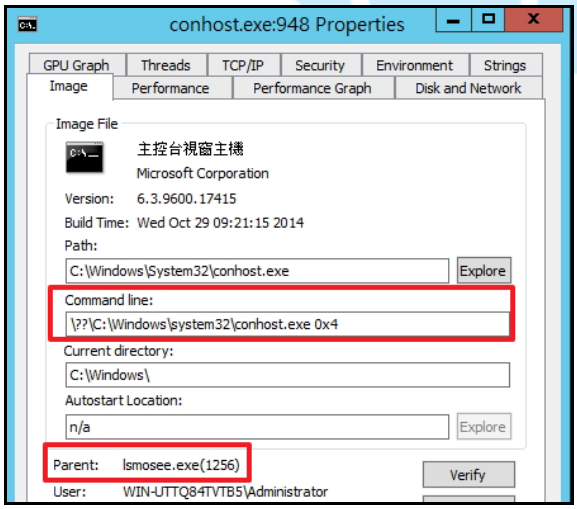
Process Name	Proces...	Protocol	Local Port	Local Address	Remote ...	Remote Addr...	State	Added On
lsmosee.exe	1256	TCP	49253	192.168.195.159	80	118.184.176.15	Syn-Sent	2018/3/21 下午 04:45:55

lsmosee.exe	1256	TCP	49246	192.168.195.159	8888	78.142.29.152	Syn-Sent	2018/3/21 下午 04:44:19
lsmosee.exe	1256	TCP	49250	192.168.195.159	13000	78.142.29.152	Syn-Sent	2018/3/21 下午 04:44:47
lsmosee.exe	1256	TCP	49249	192.168.195.159	5555	107.191.99.95	Established	2018/3/21 下午 04:44:47

3. 檢視受測主機的 CPU 效能，發現程式 lsmosee.exe 執行時 CPU 效能衝高，將近 100%，疑似挖礦行為。

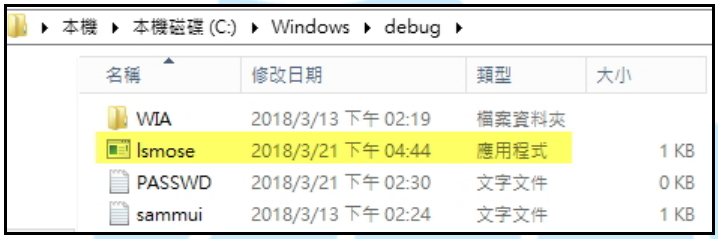


4. 檢視受測主機背景程式運作情形，發現程式 lsmosee.exe 執行後會呼叫程式 conhost.exe。



5. 在惡意程式程式 lsmosee.exe 執行後，會在與它所在的資料夾內出現一個名為「cudart32_65.dll」的檔案，經 Virustotal 網站檢測，惡意比例為 0/55。

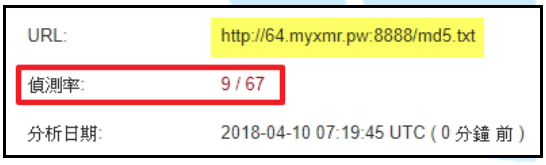
6. 檢視受測主機內各資料夾，發現在 C:\Windows\debug 資料夾內，有新增一個執行檔 lsmose.exe，將它送至 Virustotal 網站檢測，發現其為惡意之比例為 0/56。

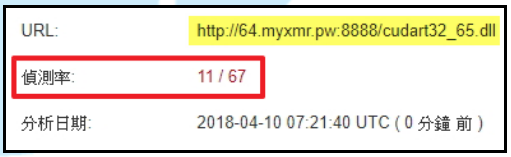


7. 檢視所側錄的封包內容，發現該受測主機會連線至美國 IP:104.155.224.46:8888 想取得 md5.txt、cudart32_65.dll 與 64.rar 等檔案，而目的主機回應「sinkholed by abuse.ch」訊息，可以得知 abuse.ch 已透過 sinkholing 技術介入處理，攔截連線到此 IP 的所有連線。

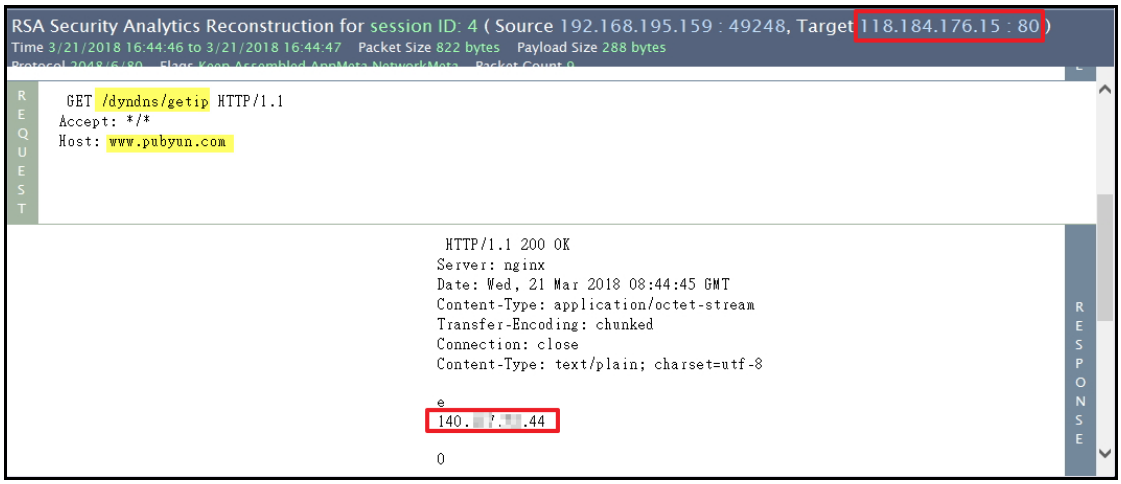
8. 將受測主機連線網址 http://64.myxmr.pw:8888/送至 virustotal 網站進行 URL 檢測，得到下列結果，顯示該網址為惡意網址。

No	URL	視為惡意網址之比例
1	http://64.myxmr.pw:8888/md5.txt	9/67
2	http://64.myxmr.pw:8888/cudart32_65.dll	11/67
3	http://64.myxmr.pw:8888/64.rar	11/67

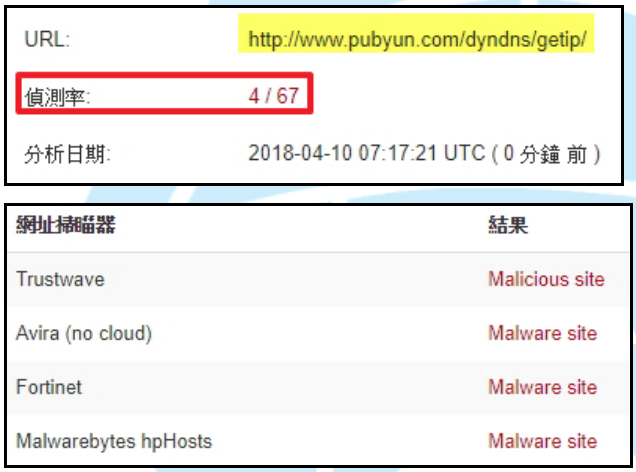




9. 檢視連線至目的 IP: 118.184.176.15 (port:80)的封包內容，發現受測主機與該 IP 進行 IP 報到驗證，取得受測主機當下實體 IP 位置。

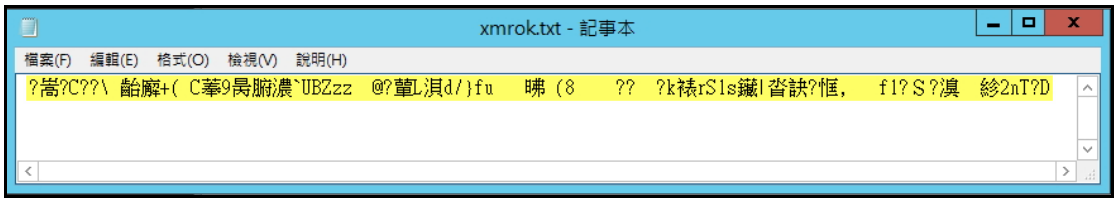


10. 將受測主機連線網址 http://www.pubyun.com/dyndns/getip/送至 Virustotal 網站進行 URL 檢測，得知其為惡意網址之比例有 4/67。



網址掃瞄器	結果
Trustwave	Malicious site
Avira (no cloud)	Malware site
Fortinet	Malware site
Malwarebytes hpHosts	Malware site

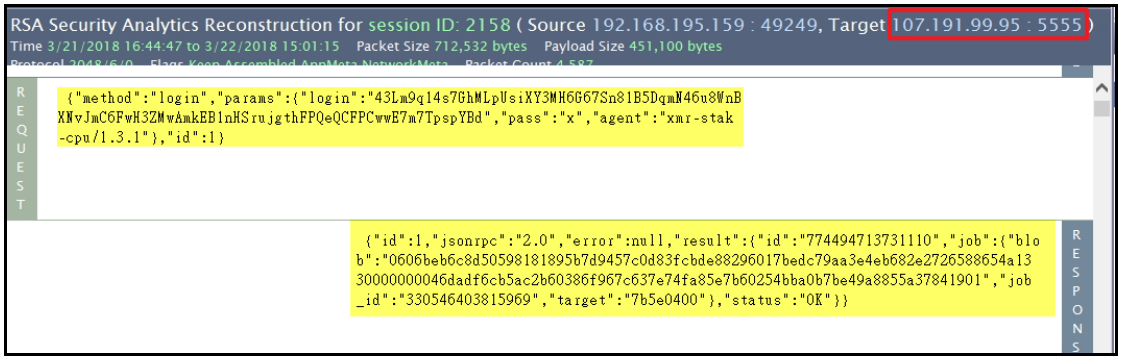
11. 檢視連線至目的 IP:78.142.29.152(port:8888)的封包內容，發現受測主機連線礦池 xmr.5b6b7b.ru:8888 下載 xmrok.txt 檔案。開啟 xmrok.txt 檔案，發現無法識別內容，而其惡意比例經 Virustotal 檢測為 0/58。



12. 將受測主機連線網址 http://xmr.5b6b7b.ru:8888/xmrok.txt 送至 virustotal 網站進行 URL 檢測，得知其為惡意網址之比例有 5/67，有 5 家防毒軟體公司視它為惡意網址，而有 2 家公司認為它是可疑網站。

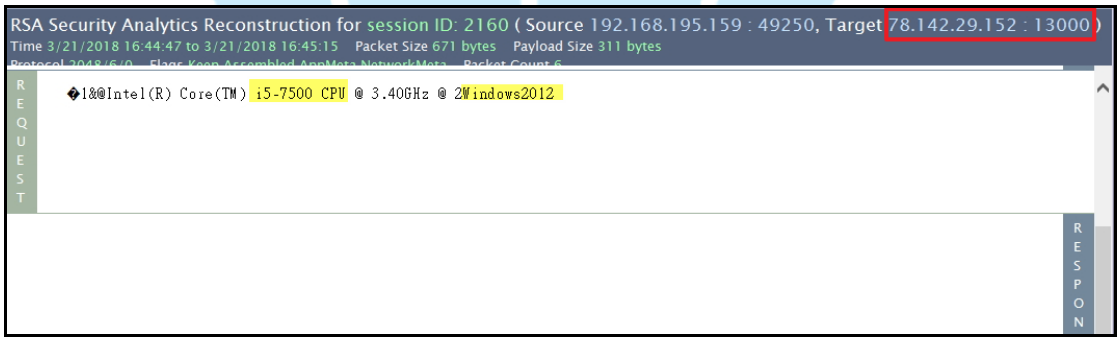
網址掃描器	結果
CyRadar	Malicious site
Dr.Web	Malicious site
Avira (no cloud)	Malware site
ESET	Malware site
G-Data	Malware site
DNS8	Suspicious site
Forcepoint ThreatSeeker	Suspicious site

13. 檢視連線至目的 IP:107.191.99.95 (port:5555)的封包內容，發現受測主機以錢包帳號「43Lm9q14s7GhMLpUsiXY3MH6G67Sn81B5DqmN46u8WnBXNvJmC6FwH3ZMwAmkEB1nHSrujgthFPQeQCFPCwwE7m7TpspYBd」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。

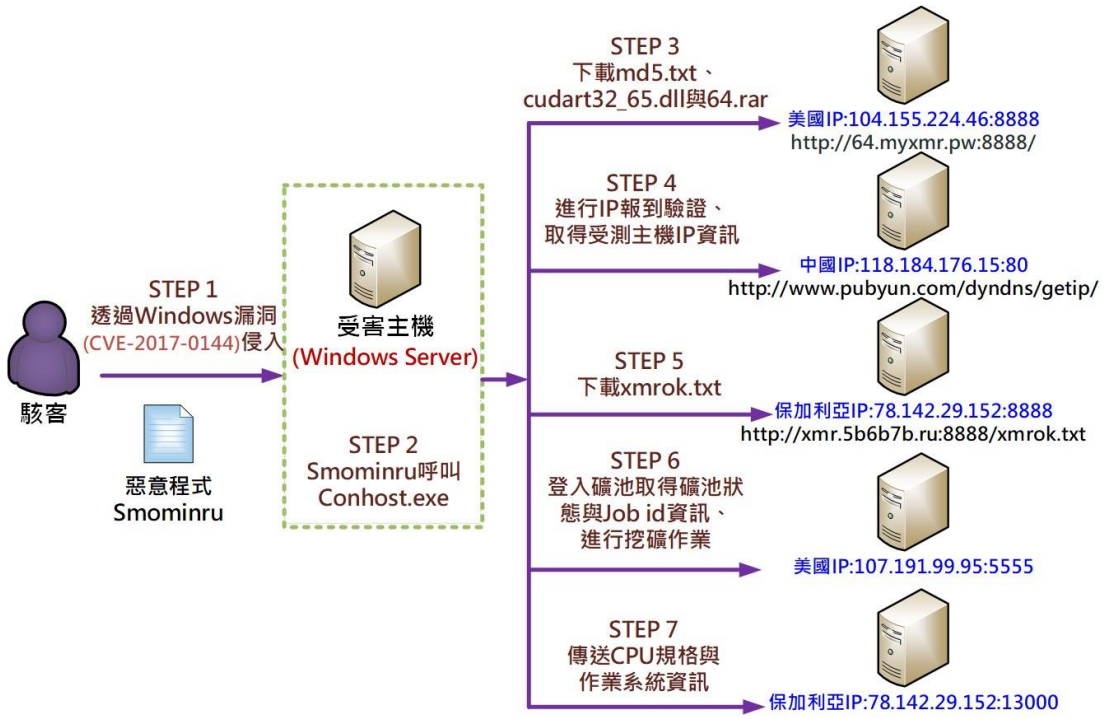


目的 IP 主機指派一次挖礦作業(含 job id)回傳給受測主機後，受測主機 submit 上傳一次挖礦作業執行成果給目的 IP 主機，最後目的 IP 主機回應目前礦池狀態 ok 給受測主機，如此重複該項動作，進行挖礦。

14. 檢視連線至目的 IP:78.142.29.152(port: 13000)的封包內容，發現受測主機傳送 CPU 規格與作業系統資訊給 IP:78.142.29.152:13000。



III. 網路架構圖



1. 惡意程式 Smominru 透過攻擊 Windows 漏洞(CVE-2017-0144)來入侵 Windows 伺服器。
2. 惡意程式 Smominru 入侵後呼叫程式 Conhost.exe。
3. 受害主機連線 IP:104.155.224.46:8888 下載 3 個檔案(md5.txt、cudart32_65.dll 與 64.rar)。
4. 受害主機連線 IP:118.184.176.15:80 進行 IP 報到驗證、取得受測主機 IP 資訊。
5. 受害主機連線 IP:78.142.29.152:8888(礦池)下載 xmrok.txt 檔案。
6. 受害主機登入礦池(IP:107.191.99.95:5555)取得礦池狀態與挖礦作業 id 資訊，並且開始挖礦作業。
7. 受害主機傳送 CPU 規格與作業系統資訊給 IP:78.142.29.152:13000。

IV.建議與總結

Smominru 最喜歡攻擊的對象就是 Windows 伺服器，因為它是市場上最理想的主機之一，不僅總是處於「打開」狀態，而且擁有比個人電腦更強的處理

能力，能增加挖礦的速度與效能。它通過 EternalBlue（CVE-2017-0144 SMB）進行攻擊，以感染新節點並增加殭屍網路的大小。目前來自安全研究公司 Proofpoint、abuse.ch 和 ShadowServer Foundation 等組織的網路安全人員試圖用「sinkholing」的技術來消滅這個殭屍軟體，但結果並不成功，Smominru 惡意軟體在短暫停止之後，很快又恢復了攻擊。為了預防 Smominru 攻擊事件的發生，建議下列幾點措施。

1. 修補 Windows(CVE-2017-0144)漏洞、執行 Windows Server 系統與應用程式的更新作業。
2. 關閉 Windows 系統的 445 通訊埠。
3. 針對容易受到攻擊的 Windows 伺服器，如電子郵件與網站等，加強安全機制、監控 Windows 系統 CPU 效能。
4. 利用應用程式控制機制防止可疑檔案被執行，可阻擋程式遭受不正當的修改。
5. 應用網路分割的網路佈線規劃，降低內部網路的電腦遭受攻擊和損害的風險。
6. 確認防毒軟體已更新至最新版本病毒碼與偵測程式碼，並定期執行電腦掃毒作業。

V. 相關報導

1. 逾 50 萬台 Windows 伺服器淪為 Monero 挖礦機，台灣為第三大受災區

   https://www.ithome.com.tw/news/121078

2. Smominru Monero mining botnet making millions for operators

https://www.proofpoint.com/us/threat-insight/post/smominru-monero-mining-botnet-making-millions-operators