電腦教室主機群體感染
惡意程式攻擊事件分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

2019 年 4 月

一、事件簡介

1. 某學校在 2019/ 3 中旬校園電腦陸續群體觸發「Malicious File Download/Malicious Binary Download」(由遠端下載惡意程式) 的資安事件，兩星期內被開 76 張資安通報單，為了解群體主機觸發資安事件的原因，學校請求本中心協助進行鑑識作業。
2. 所感染的主機群中有大量主機來自校園內某單位之電腦教室，教室內 32 台電腦中有 25 台電腦受感染。
3. 這些電腦教室主機的事件發生時間皆為 2019/3/28 18:23~19:43，當時廠商正進行系統更新維護作業。
4. 從資安通報單的佐證資料得知這些受害主機會連線目的 IP:128.199.64.236 的 80 port。

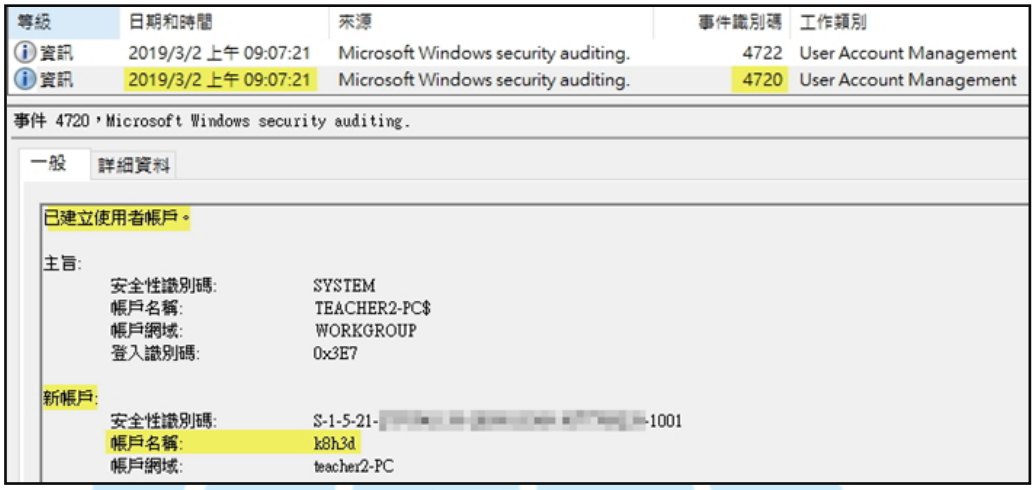
二、事件檢測

1. 首先，該電腦教室有 30 台學員用主機與 2 台教師用主機。檢視電腦教室內各感染主機系統環境設定發現如下表結果。

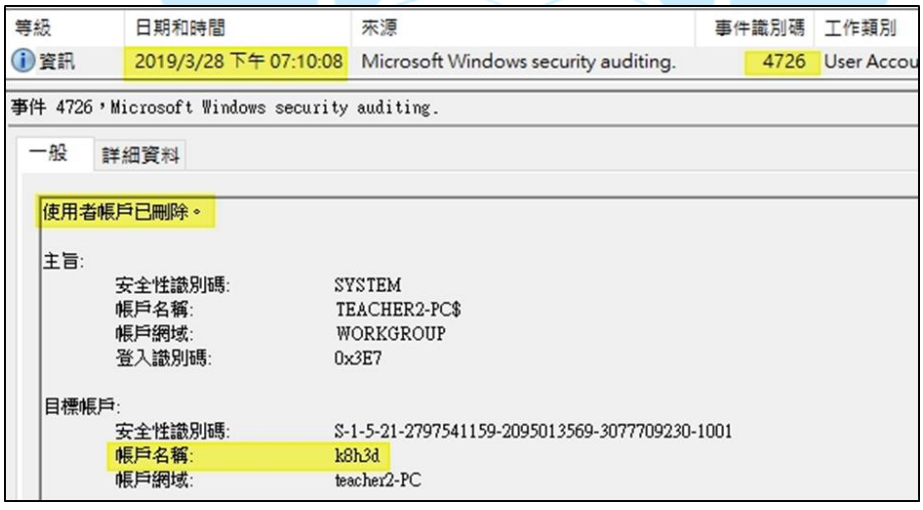
主機	主機系統	主機用途	帳戶是否設定密碼	是否安裝還原卡	防火牆與 port 開啟狀態	系統更新日期	病毒碼更新日期
94 主機 (Teacher 2-PC)	Windows 7 SP1	教師用	否	是	防火牆未開啟、開啟許多 port	2015/9/3	2010/11/19
其他感染主機	Windows 7 SP1	學員用	否	是	防火牆未開啟、開啟許多 port	2015/9/3	2010/11/19

2. 該單位人員表示廠商在 2019/3/27 先對 94 主機進行系統更新作業，之後 2019/3/28 對學員用主機進行系統更新，故本個案將優先檢測 94 主機。

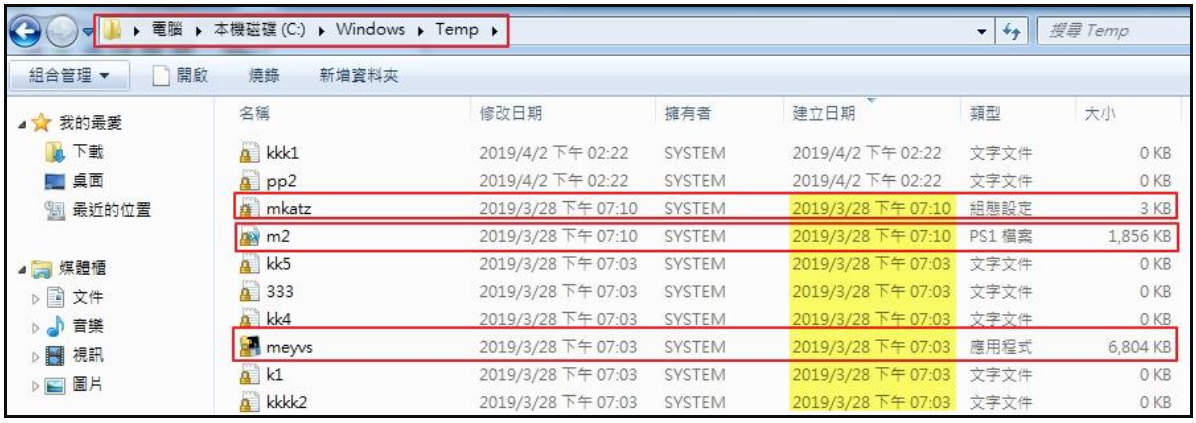
3. 檢視 94 主機之系統登入紀錄，發現駭客在 2019/3/2 曾駭入 94 主機後新增帳戶 k8h3d。從紀錄可以得知校園 IP:140.X.X.53 登入 94 主機的第一筆時間在 2019/3/2 上午 8:57，之後 9:07 新增帳戶 k8h3d，建立帳戶後當天 9:07 起陸續以此 IP 登入帳戶 k8h3d。



4. 在 2019/3/28 19:10 廠商進行系統更新時，帳戶 k8h3d 被刪除。檢測時也發現其他受害主機在惡意程式執行期間，會自動建立帳戶 k8h3d，提供駭客入侵主機的管道。在所有受害主機中，建立帳戶 k8h3d 的時間以 94 主機的時間 2019/3/2 最早。

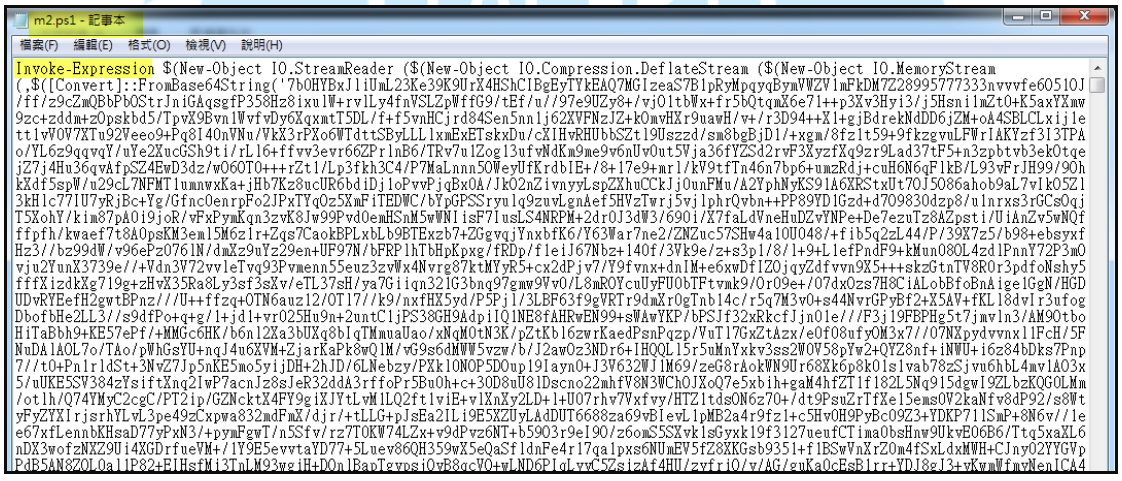


5. 在 94 主機的 C:\Windows\Temp 內發現多個 2019/3/28 建立的惡意檔案，從其中 3 個惡意檔案 mkatz.ini、m2.ps1 與 meyvs.exe 可以得知駭客的攻擊行為，其檔案功能與 virustotal 檢測結果如下表所示。



檔案名稱	功能	virustotal
mkatz.ini	存放 94 主機的帳戶與密碼資訊，為使用 mimikatz 竊取主機帳戶與密碼後存放資訊的檔案	---
m2.ps1	從惡意網址下載到主機內的可用 powershell 執行的程式碼	29/55
meyvs.exe	對外大量連線 445 port 與 1433 port	44/61

檢視 m2.ps1 為 PowerShell Scripts 的檔案，內有一大段程式碼，推測為駭客傳送至主機內要使用 powershell 來執行的程式。



6. 在 94 主機的 C:\Windows 內發現 3 個 2019/3/28 建立的惡意程式 HusSDz.exe、tL4EuCGZ.exe 與 S89PlnBr.exe，其檔案功能與 virustotal 檢測結果如下表所示。

惡意檔案名稱	功能	virustotal
HusSDz.exe	取得 mac address 與呼叫 Q6REQ6.exe 進行挖礦	41/70
tL4EuCGZ.exe	為通過 SMB，MS SQL 或利用 Windows 操作系統中的漏洞傳播的蠕蟲程式。	42/70
S89PlnBr.exe	取得 UUID 與 mac address 資訊	41/71

7. 檢視 94 主機的對外網路連線狀態，發現下列結果:

(1) meyvs.exe 會大量連線校內與校外網段內所有 IP 的 445 port 與 1433 port。

(2) powershell.exe 會連線南韓 IP:27.102.107.137。

(3) meyvs.exe 會連線美國 IP:153.92.4.49。

(4) Q6REQ6.exe 會連線南韓 IP:141.98.213.220 與 27.102.118.147。

Process Name	Process ID	Protocol	Local Port	Local Address	Remote Port	Remote Address	State
powershell.exe	6080	TCP	49389	140.[redacted].94	80	27.102.107.137	Close Wait
meyvs.exe	4068	TCP	64741	140.[redacted].94	80	153.92.4.49	Close Wait
meyvs.exe	4068	TCP	50089	127.0.0.1	50090	127.0.0.1	Established
meyvs.exe	4068	TCP	50090	127.0.0.1	50089	127.0.0.1	Established
Q6REQ6.exe	3884	TCP	55868	140.[redacted].94	443	141.98.213.220	Established
LMS.exe	2636	TCP	49192	::1	49194	::1	Established
LMS.exe	2636	TCP	49194	::1	49192	::1	Established
meyvs.exe	4068	TCP	57521	140.[redacted].94	445	140.[redacted].114	Established
meyvs.exe	4068	TCP	53924	140.[redacted].94	445	140.[redacted].232	Established
meyvs.exe	4068	TCP	54002	140.[redacted].94	445	140.[redacted].35	Established
meyvs.exe	4068	TCP	54008	140.[redacted].94	445	140.[redacted].72	Established
meyvs.exe	4068	TCP	54261	140.[redacted].94	445	140.[redacted].19	Established

Process Name	Process ID	Protocol	Local Port	Local Address	Remote Port	Remote Address	State
Q6REQ6.exe	3884	TCP	60295	140.[redacted].94	443	27.102.118.147	Established
meyvs.exe	4068	TCP	51386	140.[redacted].94	445	140.[redacted].130	Established
meyvs.exe	4068	TCP	51642	140.[redacted].94	445	140.[redacted].130	Established
meyvs.exe	4068	TCP	52399	140.[redacted].94	445	140.[redacted].130	Established

8. 從 94 主機的側錄封包分析得知，程式 meyvs.exe 執行時會大量連線校內、外各網段 IP 之 445 port 與 1433 port，當連線登入成功後，會在主機內建立檔案、上傳惡意程式、刪除惡意程式…等。

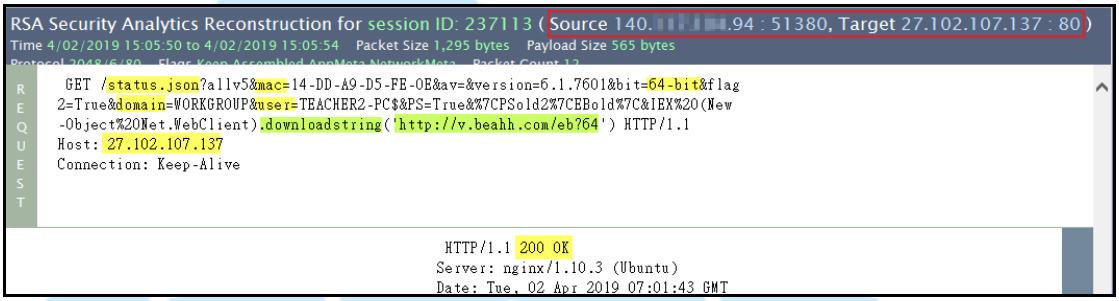
	Time	Source	Destination	Protocol	Length	Info
52	6.644945	140.[redacted].94	140.[redacted].60	SMB	131	Tree Connect AndX Request, Path: \\140.[redacted].60\public
53	6.646765	140.[redacted].60	140.[redacted].94	SMB	107	Tree Connect AndX Response
54	6.912091	140.[redacted].94	140.[redacted].60	SMB	154	NT Create AndX Request, FID: 0x2afe, Path: VtFhoNsO.exe
55	6.913488	140.[redacted].60	140.[redacted].94	SMB	193	NT Create AndX Response, FID: 0x2afe
56	7.118468	140.[redacted].94	140.[redacted].60	TCP	60	60979 → 445 [ACK] Seq=1639 Ack=2109 Win=65196 Len=0
57	7.478141	140.[redacted].94	140.[redacted].60	TCP	1514	60979 → 445 [ACK] Seq=1639 Ack=2109 Win=65196 Len=1460 [TCP segment of a reassembled PDU]
58	7.478151	140.[redacted].94	140.[redacted].60	TCP	1514	60979 → 445 [ACK] Seq=3099 Ack=2109 Win=65196 Len=1460 [TCP segment of a reassembled PDU]
59	7.478157	140.[redacted].94	140.[redacted].60	TCP	1514	60979 → 445 [ACK] Seq=4559 Ack=2109 Win=65196 Len=1460 [TCP segment of a reassembled PDU]
60	7.479188	140.[redacted].60	140.[redacted].94	TCP	60	445 → 60979 [ACK] Seq=2109 Ack=4559 Win=16000 Len=0

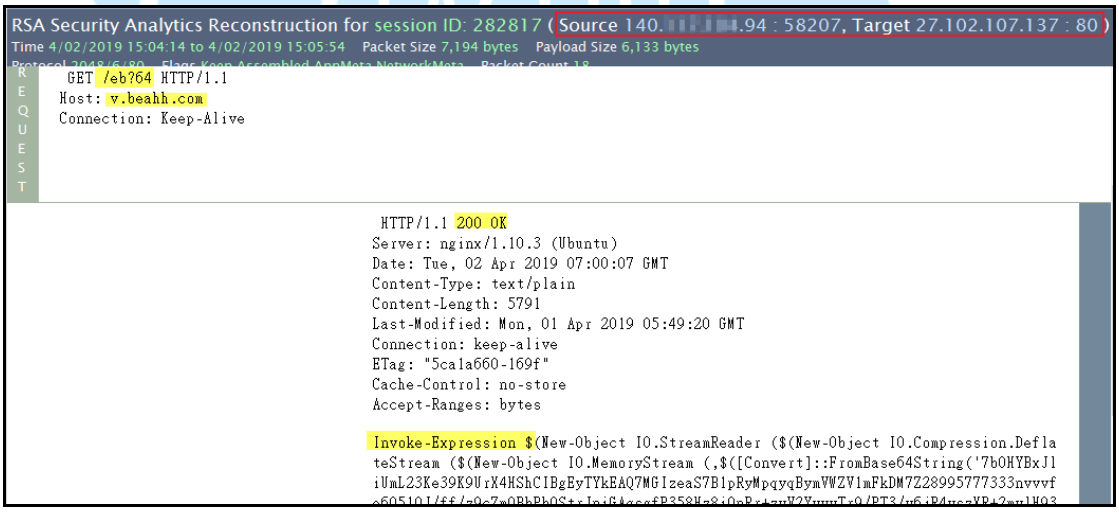
140.x.x.94登入140.x.x.60
並傳送檔案VtFhoNs0.exe

	Time	Source	Destination	Protocol	Length	Info
143	11.128852	140.[redacted].94	140.[redacted]60	SMB	131	Tree Connect AndX Request, Path: \\140.[redacted].60\public
144	11.130719	140.[redacted].60	140.[redacted].94	SMB	107	Tree Connect AndX Response
145	11.416649	140.[redacted].94	140.[redacted]60	TCP	60	60979 → 445 [ACK] Seq=58793 Ack=2824 Win=64484 Len=0
146	11.498722	140.[redacted].94	140.[redacted]60	SMB	149	Trans2 Request, FIND_FIRST2, Pattern: VtFhoNsO.exe
147	11.501001	140.[redacted].60	140.[redacted].94	SMB	234	Trans2 Response, FIND_FIRST2, Files: VtFhoNsO.exe
148	11.728687	140.[redacted].94	140.[redacted]60	TCP	60	60979 → 445 [ACK] Seq=58888 Ack=3004 Win=64304 Len=0
149	11.979679	140.[redacted].94	140.[redacted]60	SMB	93	Tree Disconnect Request
150	11.981098	140.[redacted].60	140.[redacted].94	SMB	93	Tree Disconnect Response
151	12.207182	140.[redacted].94	140.[redacted]60	SMB	131	Tree Connect AndX Request, Path: \\140.[redacted].60\public
152	12.208815	140.[redacted].60	140.[redacted].94	SMB	107	Tree Connect AndX Response
153	12.415184	140.[redacted].94	140.[redacted]60	SMB	110	Delete Request, Path: VtFhoNsO.exe
154	12.415877	140.[redacted].60	140.[redacted].94	SMB	93	Delete Response
155	12.608362	140.[redacted].94	140.[redacted]60	SMB	93	Tree Disconnect Request
156	12.613149	140.[redacted].60	140.[redacted].94	SMB	93	Tree Disconnect Response

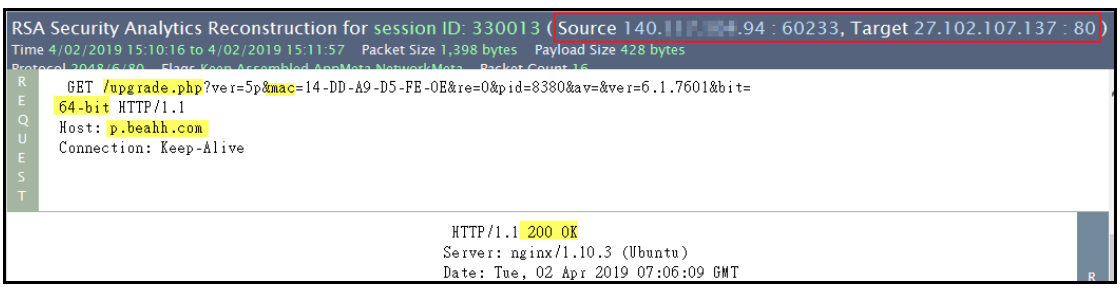
刪除VtFhoNs0.exe

9. 從 94 主機的側錄封包分析得知，程式 powershell.exe 執行時會連線南韓 IP:27.102.107.137/status.json 回傳主機狀態後，再連線 http://v.beahh.com/eb?64 下載惡意程式 m2.ps1。

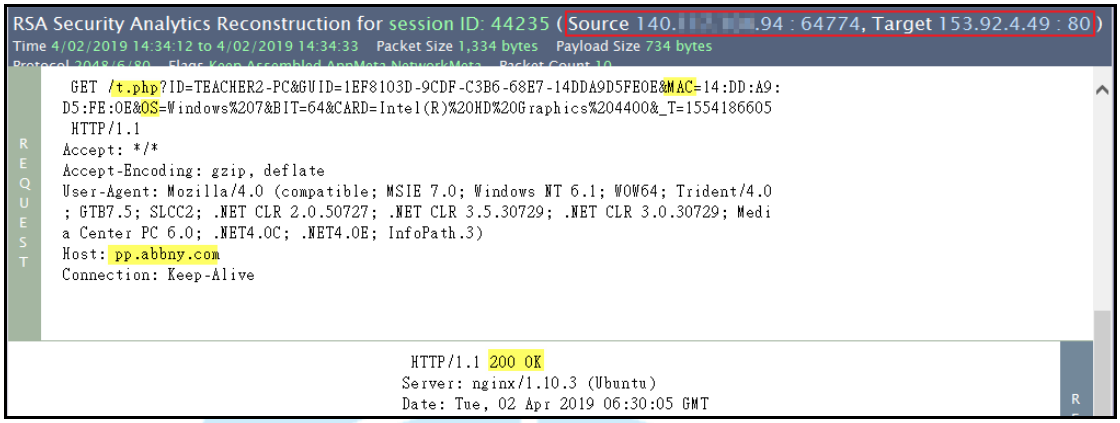




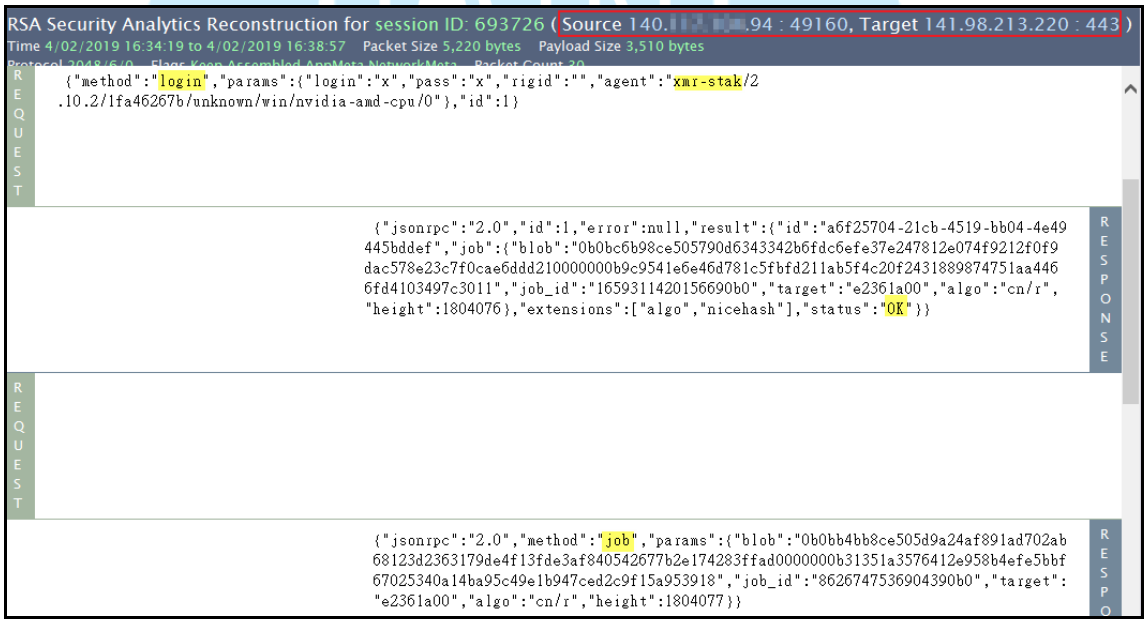
powershell.exe 也會連線南韓 IP:27.102.107.137 之另一個網址 p.beahh.com/upgrade.php 來更新主機狀態資訊。



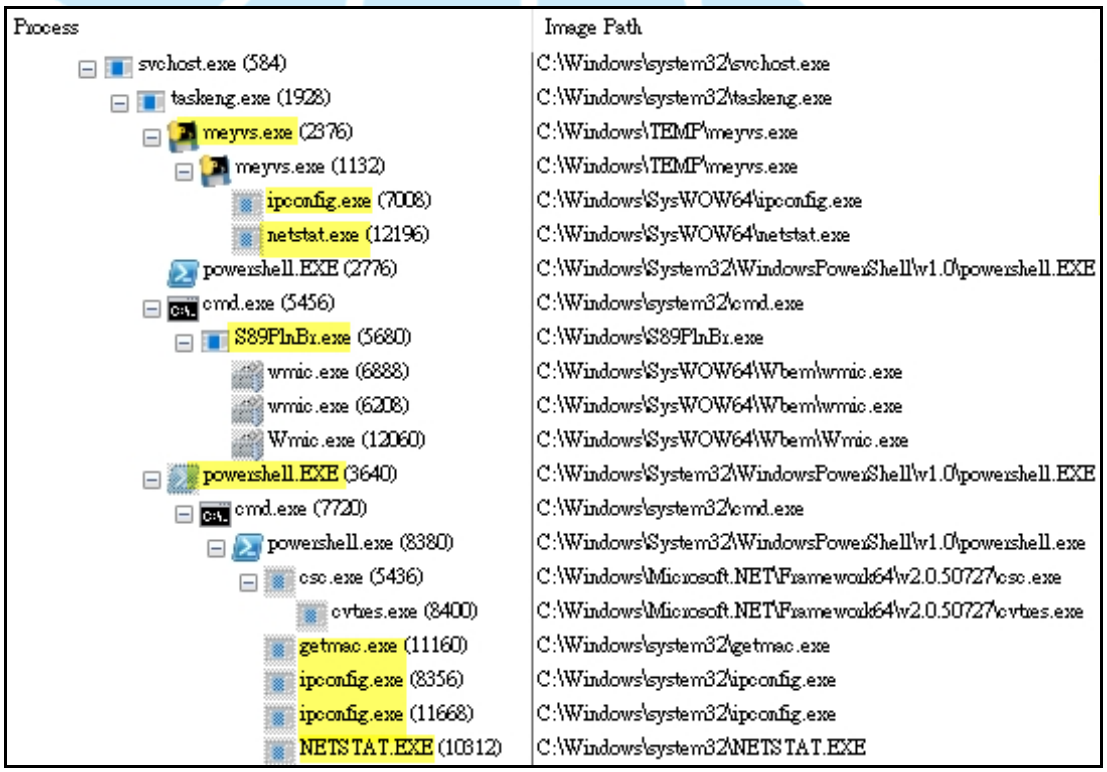
10. 從 94 主機的側錄封包分析得知，程式 meyvs.exe 連線美國 IP:153.92.4.49 (http://pp.abbny.com/t.php)時會傳送主機名稱、mac 值、作業系統資訊...等給對方主機。

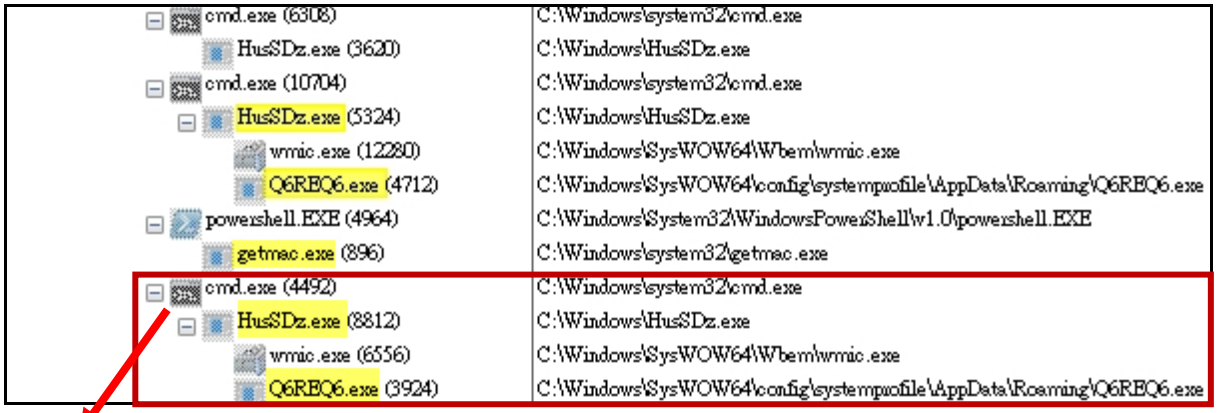


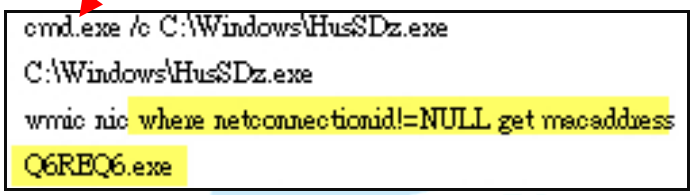
11. 從 94 主機的側錄封包分析得知，程式 Q6REQ6.exe 連線南韓 IP:141.98.213.220 與 27.102.118.147 是登入礦池、進行挖礦作業，推測 Q6REQ6.exe 為一個挖礦程式。Q6REQ6.exe 經 virustotal 檢測，其惡意比例為 36/70，而且有多家防毒軟體公司以 Miner 用字稱呼它。



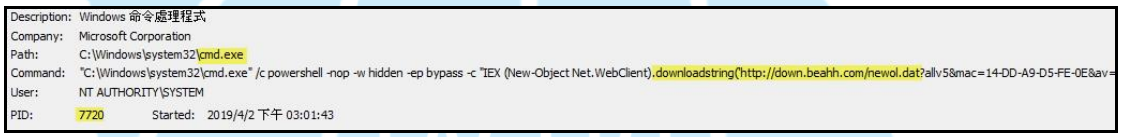
12. 檢視 94 主機的背景程式運作情形，發現 meyvs.exe 會呼叫 ipconfig.exe 與 netstat.exe 進行網路 port 掃描，之後執行 powershell 下載 m2.ps1，接著執行 S89PlnBr.exe 來取得連線 IP 的 macaddress，最後執行 HusSDz.exe 來取得 macaddress 與執行挖礦程式 Q6REQ6.exe，而且程式 HusSDz.exe 會被重複執行著。

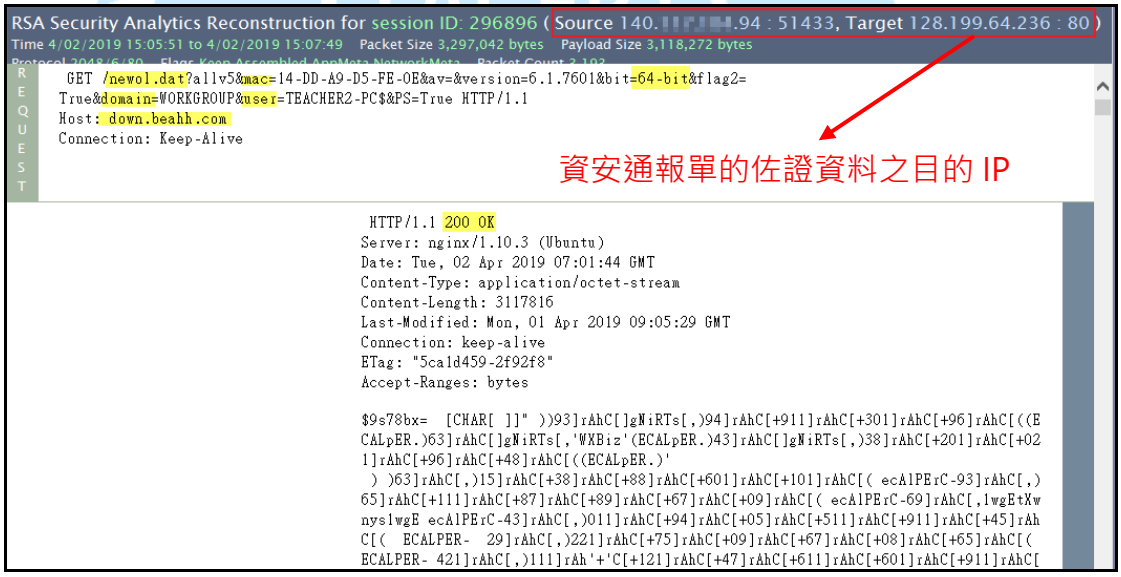






其中一個透過 cmd.exe 呼叫 powershell.exe 來執行的 powershell，則從其 command 內容可以看出會至 http://down.beahh.com/newol.dat 下載惡意程式碼。





13. 探討「94 主機有安裝系統還原卡，為何 2019/3/2 有駭客入侵紀錄存在?」之問題，發現下列現象。

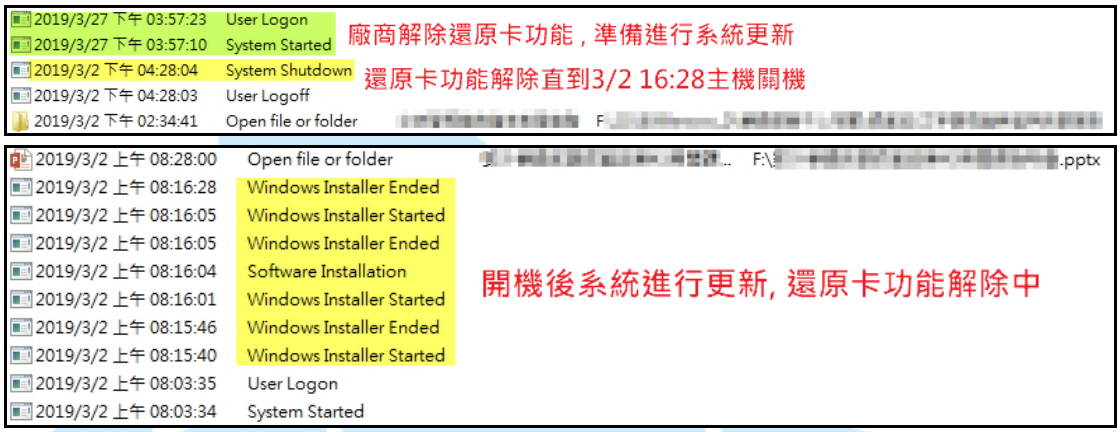
(1) 檢視系統還原卡的設定，發現系統還原卡可設定重開機 N 次後在下一次啟動時才鎖住系統狀態。

(2) 系統還原卡之登入密碼存放於 D:\內，檢視存放密碼的 Word 檔，發現該

內容已被清空。

(3) 94 主機所使用的還原卡為軟體式，當該還原卡的驅動程式被更換存放位置或變更其檔案名稱時，將使還原卡功能喪失。

14. 檢視系統操作執行紀錄，發現在 2019/2/27 廠商更新字型，並且在 2019/3/2 主機重啟後還原卡功能解除，推測因當時還原卡設定為重新開機一次後在下一次啟動時才鎖住系統狀態造成。



15. 檢視其他受害主機之感染狀況，發現下列情形:

(1)在 C:\windows 內皆會有 3 個與 94 主機名稱不同但功能相同的惡意程式。

(2)在 C:\winodws\temp 內皆會有與 94 主機相同的惡意檔案，但是執行檔名稱不同、功能相同。

(3)皆會新增帳戶 k8h3d 於主機內。

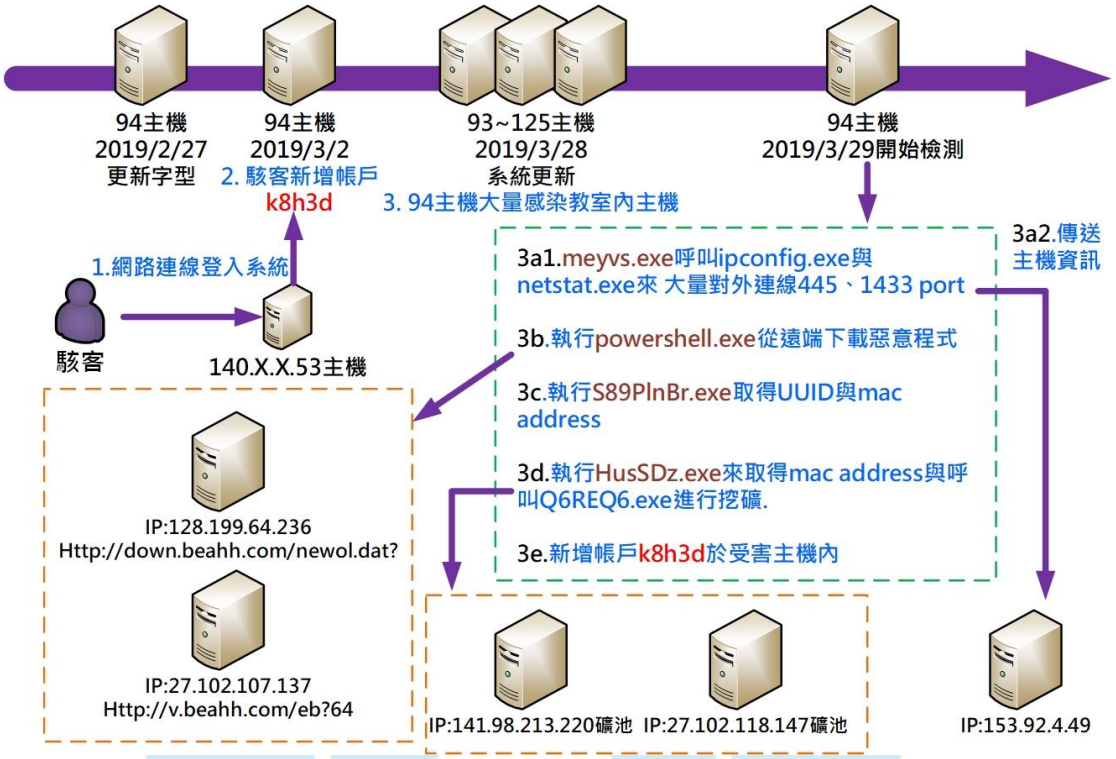
(4)皆會對外大量連線 445 port 與 1433 port。

(5)皆會存在挖礦程式於主機內進行挖礦。

因此可以得知其他受害主機之感染特徵與 94 主機相同，而 94 主機為所有受害主機中第一個建立帳戶 k8h3d 的主機，推測教室內主機受感染來源來自 94 主機。

三、事件攻擊行為示意圖

本個案之事件攻擊行為從 2019/3/2 駭客入侵至 94 主機開始，分別敘述如下。



1.駭客從網路連線登入 94 主機。

2.駭客於 94 主機內新增帳戶 k8h3d。

3.駭客透過 94 主機大量感染教室內主機。

3a1.meyvs.exe 執行後呼叫 ipconfig.exe 與 nestat.exe 來大量對外連線 445 與 1433 port (port scan).。

3a2.meyvs.exe 執行時會傳送主機資訊給 IP:153.92.4.49。

3b.執行 powershell.exe 從遠端下載惡意程式至主機內。

3c.執行 S89PlnBr.exe 取得 UUID 與 mac address 資訊。

3d.執行 HusSDz.exe 取得網域內連線 IP 的 mac address 與呼叫 Q6REQ6.exe 進行挖礦 (連線 2 個礦池)。

3e.新增帳戶 k8h3d 於受害主機內。

四、建議與總結

1. 系統還原卡為一般學校管理電腦教室會安裝的工具，一般認知有安裝還原卡則系統不會中毒。透過本個案的檢測指出系統還原卡會引發下列的資安問題。

   (1)因為有還原卡，系統與病毒碼未定期進行更新。

   (2)主機使用時，系統無防毒能力。

   (3)主機使用時，可能系統中毒去攻擊其他主機，容易變成駭客入侵後對外攻擊的跳板。

   (4)因久未系統更新，一旦進行更新則需花費許多作業時間，容易在更新期間感染病毒。

   由以上問題可以得知「系統還原卡不是永久安全，有安裝的主機也不是一定不會中毒」。

2. 檢視本個案的資安防護措施，有下列幾點缺失:

   (1)電腦教室內所有主機皆未設定密碼即可登入系統。

   (2)因為安裝還原卡，故各主機多年未進行系統與病毒碼更新。

   (3)各主機皆未開啟防火牆，但卻開啟許多個 port。

   (4)將軟體還原卡登入設定之密碼存放於主機內，造成駭客容易取得。

   (5)所安裝的軟體還原卡可被駭客登入主機後，手動使其還原功能失效。

3. 檢視本個案之情況，有下列幾點建議改善措施提供參考。

   (1)教室內各主機須建立登入系統的密碼，並加強密碼強度。

   (2)建議使用硬體還原卡代替軟體還原卡。

   (3)建議將駭客容易使用來攻擊的 port 鎖住，如 445 port。

   (4)使用官方網站下載軟體，來定期進行系統與病毒碼更新作業。

   (5)勿存放帳號與密碼資訊於主機內。

4. 從檢測本個案之受害主機群發現，此類型的攻擊事件在受害主機一旦感染惡意程式後，會在校園區域網路內散播惡意程式，建議優先封鎖惡意程式

的下載網址 IP:27.102.107.137、128.199.64.236 與 153.92.4.49。