SMB 暴力破解密碼
攻擊事件分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

2020 年 03 月

一、事件簡介

1. 2020/01/07 某學校有 22 個 IP 在同一天觸發「SMB.Login.Brute.Force」偵測規則，造成該校一天之內被開 22 張資安通報單。

教育機構資安通報平台

事件類型:入侵事件警訊

事件單編號:AISAC-1[redacted]1

原發布編號	ASOC-INT-[redacted]	原發布時間	2020-01-07 08:15:26
事件類型	對外攻擊	原發現時間	2020-01-07 02:52:34
事件主旨	通報:[[redacted]學]140.[redacted]217 SMB.Login.Brute.Force		
事件描述	ASOC發現貴單位([redacted]學)所屬 140.[redacted]217 疑似對外進行 SMB.Login.Brute.Force 攻擊		
手法研判	手法研判		
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或未經許可的連接埠，並查看記錄是否有外界對貴單位內部IP之異常連線。 2.如發現為非授權的連線，建議將該IP於防火牆阻擋。 3.建議針對被攻擊的主機做好相關主機系統服務檢查及弱點修補確認的工作，並關閉不需要的服務。 4.將所使用的密碼複雜度提高。 5.攻擊名稱相關參考資料網站： FortiGuard http://www.fortiguard.com/encyclopedia/vulnerability/#id=12090		
參考資料	無		
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			
如果您對此通告的內容有疑問或有關於此事件的建議，歡迎與我們連絡。			

2. 這些受害 IP 所屬設備皆會對外連線攻擊多個目的 IP 的 445 port 或 1433 port。
3. 由本案 22 個 IP 的事件發現時間點推測，該類攻擊在 2020/01/07 當天凌晨開始。
4. 該事件發生後部分 IP 主機即被緊急處理，無法採證，但為了瞭解這些 IP 主機群的攻擊行為與危害程度，本中心對學校所能提供三台主機(IP: 140.X.X.81、140.X.X.69 與 140.X.X.199)進行鑑識作業。

二、事件檢測

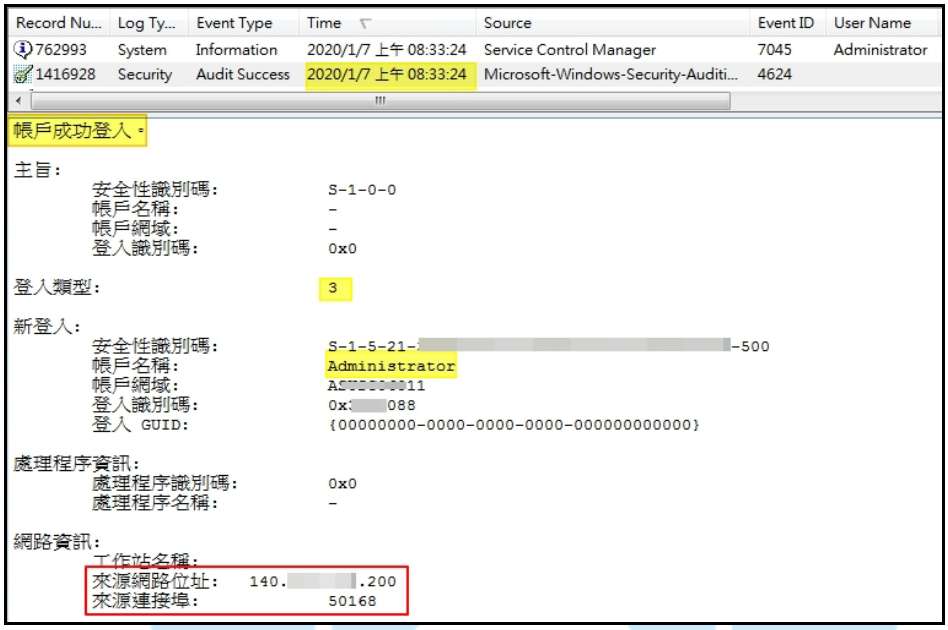
1. 首先，本資安事件所檢測的三台主機之主機資訊與用途說明如下。

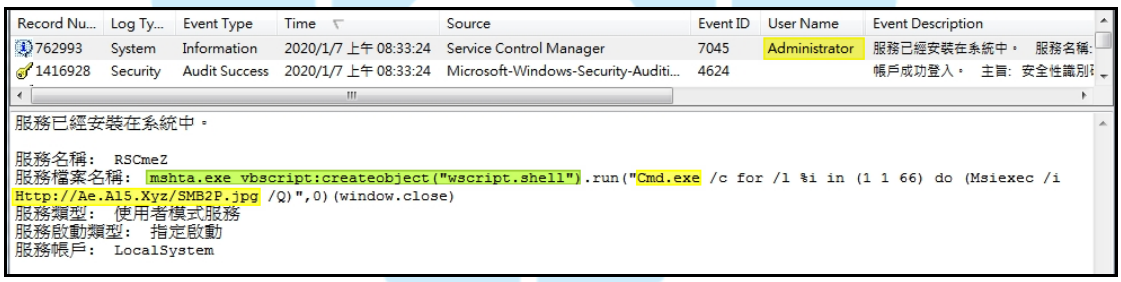
主機簡稱	IP	主機用途	作業系統
81 主機	140.X.X.81	校外遠端連線校內主機用	Windows Server 2008 R2 Service Pack 1
69 主機	140.X.X.69	派車系統	Windows Server 2008

主機簡稱	IP	主機用途	作業系統
199 主機	140.X.X.199	一般行政事務用	Windows 7 Service Pack 1

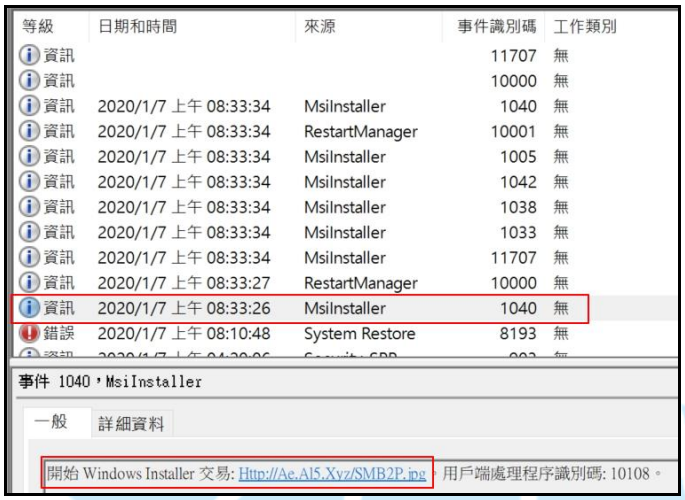
2. 199 主機的檢測資訊如下:

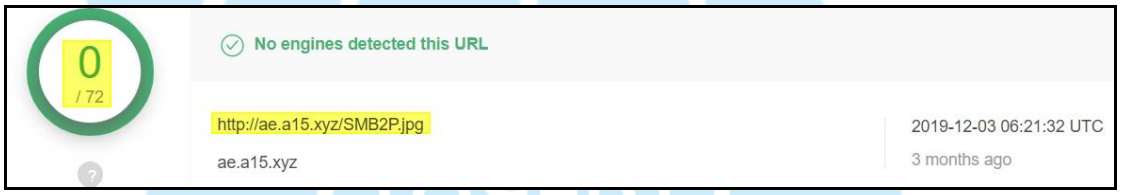
2.1 由系統日誌發現在 2020/01/07 8:33:24 IP:140.X.X.200 使用帳戶 Administrator 登入主機，執行 VB Script 腳本來利用 Windows Installer 程式安裝軟體。

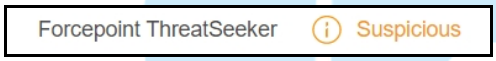




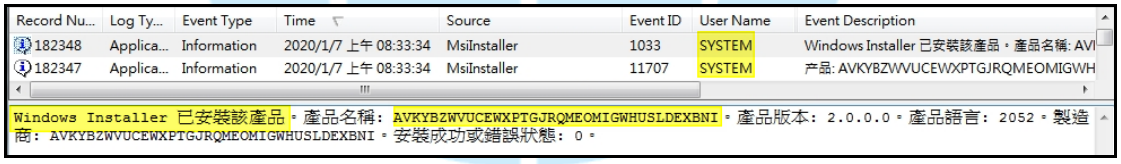
2.2 之後主機在 2020/01/07 08:33:26 開始有一連串安裝軟體與重新開機的動作，而且此類型的 Windows Installer 行為會連到一個網址 Http[://]Ae.A15.Xyz/SMB2P.JPG。該網址經 Virustotal 檢測其惡意比例為 0/72，僅有一家防毒軟體公司認為其為可疑的惡意網址。



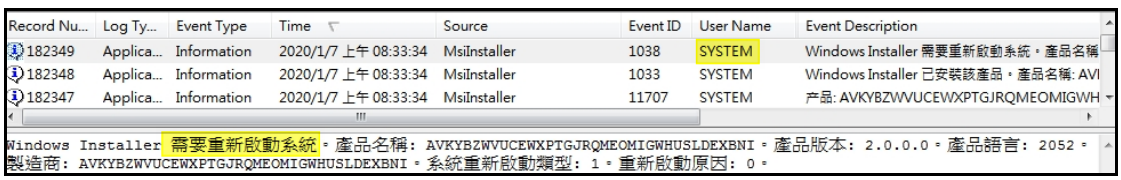




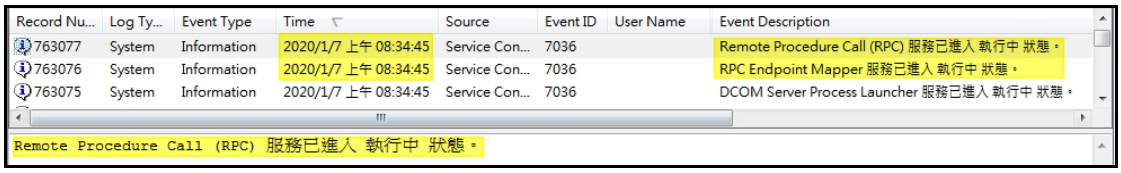
接著系統會告知該產品已安裝完成，從系統日誌可以得知其產品名稱(AVKYBZWVUCEWXPTGJRQMEOMIGWHUSLDEXBNI)為一段亂碼。



在安裝完成後會出現重新開機的訊息。由這一連串的行為得知此產品在一分鐘之內被安裝完成，而且安裝完成後會重新開機。

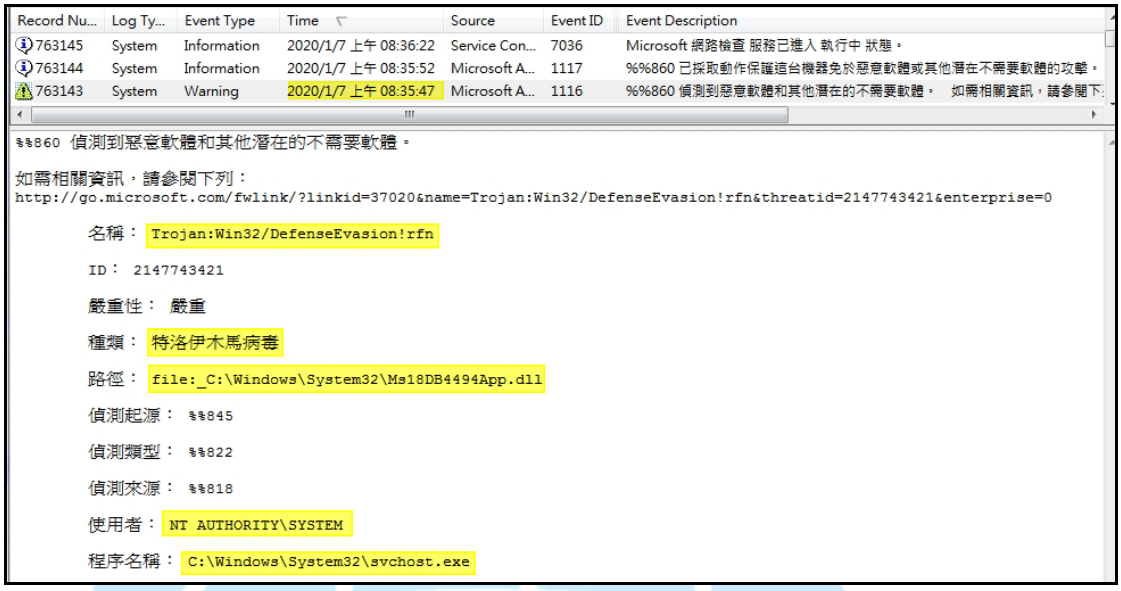


軟體安裝完成重開機後，會啟動 Remote Procedure Call(RPC)服務，而且防毒軟體偵測到特洛伊病毒 Ms18DB4494App.dll 使用 svchost.exe 在執行。



Record Nu...	Log Ty...	Event Type	Time	Source	Event ID	User Name	Event Description
763077	System	Information	2020/1/7 上午 08:34:45	Service Con...	7036		Remote Procedure Call (RPC) 服務已進入 執行中 狀態。
763076	System	Information	2020/1/7 上午 08:34:45	Service Con...	7036		RPC Endpoint Mapper 服務已進入 執行中 狀態。
763075	System	Information	2020/1/7 上午 08:34:45	Service Con...	7036		DCOM Server Process Launcher 服務已進入 執行中 狀態。

Remote Procedure Call (RPC) 服務已進入 執行中 狀態。



Record Nu...	Log Ty...	Event Type	Time	Source	Event ID	Event Description
763145	System	Information	2020/1/7 上午 08:36:22	Service Con...	7036	Microsoft 網路檢查 服務已進入 執行中 狀態。
763144	System	Information	2020/1/7 上午 08:35:52	Microsoft A...	1117	%%860 已採取動作保護這台機器免於惡意軟體或其他潛在不需要軟體的攻擊。
763143	System	Warning	2020/1/7 上午 08:35:47	Microsoft A...	1116	%%860 偵測到惡意軟體和其他潛在的不需要軟體。 如需相關資訊，請參閱下

%%860 偵測到惡意軟體和其他潛在的不需要軟體。

如需相關資訊，請參閱下列：
http://go.microsoft.com/fwlink/?linkid=37020&name=Trojan:Win32/DefenseEvasion!rfn&threatid=2147743421&enterprise=0

名稱： Trojan:Win32/DefenseEvasion!rfn

ID： 2147743421

嚴重性： 嚴重

種類： 特洛伊木馬病毒

路徑： file:_C:\Windows\System32\Ms18DB4494App.dll

偵測起源： %%845

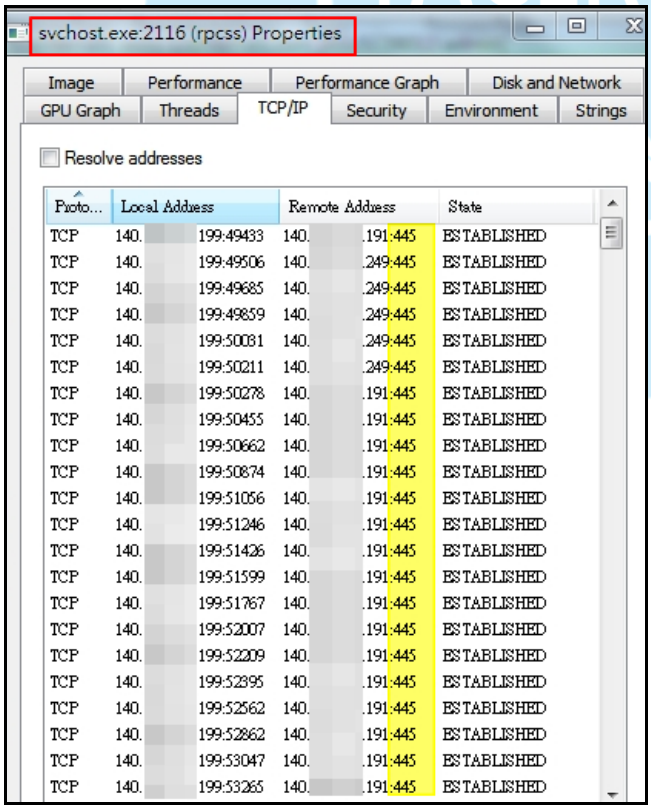
偵測類型： %%822

偵測來源： %%818

使用者： NT AUTHORITY\SYSTEM

程序名稱： C:\Windows\System32\svchost.exe

2.3 檢視執行中的所有 Svchost.exe 程序，發現 Svchost.exe(2116)執行 RPCSS，對外大量建立目的 IP:445port 或 1433port 的連線。



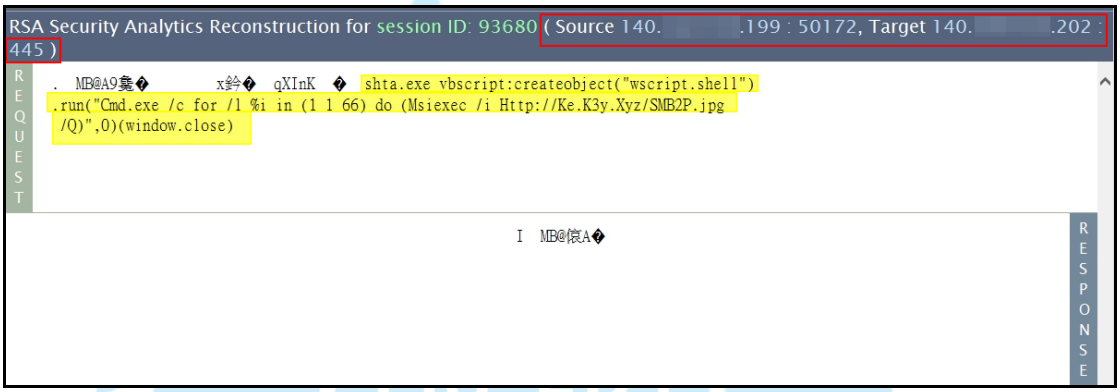
Proto...	Local Address	Remote Address	State
TCP	140. 199:49433	140. .191:445	ESTABLISHED
TCP	140. 199:49506	140. .249:445	ESTABLISHED
TCP	140. 199:49685	140. .249:445	ESTABLISHED
TCP	140. 199:49859	140. .249:445	ESTABLISHED
TCP	140. 199:50081	140. .249:445	ESTABLISHED
TCP	140. 199:50211	140. .249:445	ESTABLISHED
TCP	140. 199:50278	140. .191:445	ESTABLISHED
TCP	140. 199:50455	140. .191:445	ESTABLISHED
TCP	140. 199:50662	140. .191:445	ESTABLISHED
TCP	140. 199:50874	140. .191:445	ESTABLISHED
TCP	140. 199:51056	140. .191:445	ESTABLISHED
TCP	140. 199:51246	140. .191:445	ESTABLISHED
TCP	140. 199:51426	140. .191:445	ESTABLISHED
TCP	140. 199:51599	140. .191:445	ESTABLISHED
TCP	140. 199:51767	140. .191:445	ESTABLISHED
TCP	140. 199:52007	140. .191:445	ESTABLISHED
TCP	140. 199:52209	140. .191:445	ESTABLISHED
TCP	140. 199:52395	140. .191:445	ESTABLISHED
TCP	140. 199:52562	140. .191:445	ESTABLISHED
TCP	140. 199:52862	140. .191:445	ESTABLISHED
TCP	140. 199:53047	140. .191:445	ESTABLISHED
TCP	140. 199:53265	140. .191:445	ESTABLISHED

Process Name	Process ID	Protocol	Local Port	Local Address	Remote Port	Remote Address	State
svchost.exe	2116	TCP	56487	140. 199	1433	140. .63	Syn-Sent
svchost.exe	2116	TCP	56488	140. 199	1433	140. .64	Syn-Sent
svchost.exe	2116	TCP	56489	140. 199	1433	140. .3	Syn-Sent
svchost.exe	2116	TCP	56495	140. 199	1433	194. 181	Syn-Sent
svchost.exe	2116	TCP	56521	140. 199	1433	194. 19	Syn-Sent
svchost.exe	2116	TCP	56552	140. 199	445	140. 226	Syn-Sent
svchost.exe	2116	TCP	56564	140. 199	1433	194. 137	Syn-Sent
svchost.exe	2116	TCP	56575	140. 199	1433	140. 105	Syn-Sent
svchost.exe	2116	TCP	56590	140. 199	1433	140. .177	Syn-Sent
svchost.exe	2116	TCP	56597	140. 199	1433	140. .54	Syn-Sent
svchost.exe	2116	TCP	56608	140. 199	445	140. 189	Syn-Sent
svchost.exe	2116	TCP	56611	140. 199	1433	140. 0	Syn-Sent
svchost.exe	2116	TCP	56618	140. 199	1433	194. .136	Syn-Sent
svchost.exe	2116	TCP	56626	140. 199	1433	194. .49	Syn-Sent
svchost.exe	2116	TCP	56649	140. 199	1433	194. .46	Syn-Sent
svchost.exe	2116	TCP	56652	140. 199	445	140. .152	Syn-Sent
svchost.exe	2116	TCP	56658	140. 199	445	140. .83	Syn-Sent
svchost.exe	2116	TCP	56665	140. 199	1433	194. .255	Syn-Sent
svchost.exe	2116	TCP	56667	140. 199	1433	194. .187	Syn-Sent
svchost.exe	2116	TCP	56670	140. 199	1433	194. .83	Syn-Sent
svchost.exe	2116	TCP	56671	140. 199	1433	194. .244	Syn-Sent
svchost.exe	2116	TCP	56674	140. 199	1433	194. .231	Syn-Sent
svchost.exe	2116	TCP	56675	140. 199	445	140. .183	Syn-Sent
svchost.exe	2116	TCP	56702	140. 199	1433	140. .96	Syn-Sent
svchost.exe	2116	TCP	56745	140. 199	1433	194. .197	Syn-Sent
svchost.exe	2116	TCP	56751	140. 199	445	140. .194	Syn-Sent
svchost.exe	2116	TCP	56765	140. 199	445	140. .126	Syn-Sent
svchost.exe	2116	TCP	56772	140. 199	1433	194. .40	Syn-Sent
svchost.exe	2116	TCP	56807	140. 199	1433	140. .7	Syn-Sent

2.4 檢視連線目的 445port 的封包內容，發現 199 主機對外建立 445port 連線後，目的 IP 主機會回傳該主機的系統資訊，而 199 主機會嘗試破解帳戶 Administrator 的密碼。

```
00000496 : 00 00 FF FF 44 08 00 48 00 00 0C FF 00 00 00 04 [....D..H........]
000004a6 : 11 02 00 01 00 00 00 00 00 62 01 00 00 00 00 44 [.........b.....D]
000004b6 : C0 00 80 6D 01 A1 82 01 5E 30 82 01 5A A2 82 01 [...m....^0..Z...]
000004c6 : 56 04 82 01 52 4E 54 4C 4D 53 53 50 00 03 00 00 [V...RNTLMSSP....]
000004d6 : 00 18 00 18 00 5A 00 00 00 E0 00 E0 00 72 00 00 [.....Z.......r..]
000004e6 : 00 00 00 00 00 40 00 00 00 1A 00 1A 00 40 00 00 [.....@.......@..]
000004f6 : 00 00 00 00 00 5A 00 00 00 00 00 00 00 F8 00 00 [.....Z..........]
00000506 : 00 05 02 88 A0 61 00 64 00 6D 00 69 00 6E 00 69 [.....a.d.m.i.n.i]
00000516 : 00 73 00 74 00 72 00 61 00 74 00 6F 00 72 00 31 [.s.t.r.a.t.o.r.1]
00000526 : 17 53 E6 7E 51 EB D2 B5 FF EE E2 CF A6 C6 38 59 [.S.~Q.........8Y]
00000536 : 58 35 72 74 45 77 54 01 35 79 C8 85 92 BC 8F 02 [X5rtEwT.5y......]
00000546 : 5D 92 DC 11 79 C5 70 01 01 00 00 00 00 00 00 AB []...y.p.........]
00000556 : 4B 09 CE F7 CC D5 01 59 58 35 72 74 45 77 54 00 [K......YX5rtEwT.]
```

比對主機對外連線目的 IP 之 445port 的時間點與所截錄 IP 封包的時間點，發現 svchost.exe 執行時，若 199 主機以帳戶 Administrator 成功登入有開啟 445port 的主機時，會傳送 VB Script 腳本給該 IP 主機。



2.5 檢視背景程式與對外連線，發現 199 主機對同網段 IP 的 445 Port 建立連線，而且使用系統內建 System 程序來建立。該 System 程序對外開啟主機的 139、445 與 5357 port。

Process Name	Process ID	Protocol	Local Port	Local Address	Remote Port	Remote Address	State
System	4	TCP	49182	140. .199	445	140. .247	Established
System	4	TCP	49183	140. .199	445	140. .202	Established

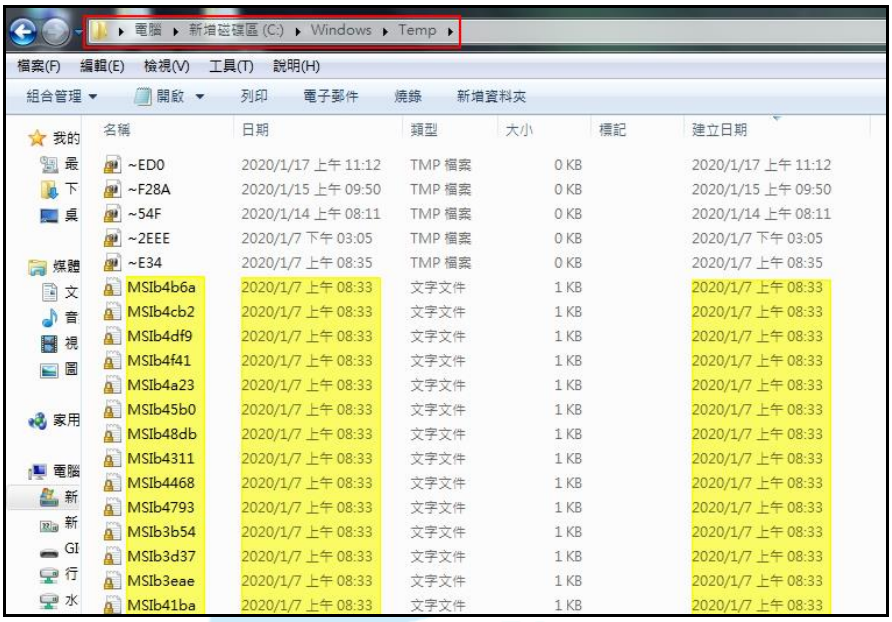
System:4 Properties

Image | Performance | Performance Graph | Disk and Network | GPU Graph | Threads | TCP/IP | Security | Environment | Strings

Resolve addresses

Protocol	Local Address	Remote Address	State
TCP	140. .199:139	0.0.0.0:0	LISTENING
TCP	140. .199:49182	140. .247:445	ESTABLISHED
TCP	140. .199:49183	140. .202:445	ESTABLISHED
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5357	0.0.0.0:0	LISTENING
UDP	140. .199:137	*:*	
UDP	140. .199:138	*:*	
TCPV6	[0:0:0:0:0:0:0:0]:445	[0:0:0:0:0:0:0:0]:0	LISTENING
TCPV6	[0:0:0:0:0:0:0:0]:5357	[0:0:0:0:0:0:0:0]:0	LISTENING

2.6 在 C:/Windows/Temp 資料夾內發現許多與前述所提產品安裝時有關的檔案。這些檔案都是在 2020/01/07 08:33 被建立的。



2.7 「Administrator」為廠商所建立來維護主機用之帳戶，但該帳戶沒有設定密碼。

3. 查看 69 主機與 81 主機的系統日誌，出現與 199 主機一樣的情形，僅執行時間與網址不同。

4. 69 主機在 2020/01/07 01:24 開始安裝軟體與重新開機，其所連線的網址為 Http[://]Ae.A15.Xyz/SMB2.JPG，該網址經 Virustotal 檢測其惡意比例為 0/72。

Time	Source	Categ...	Event ID	Event Description
2020/1/7 上午 01:24:34	Service Cont...	0	7036	
2020/1/7 上午 01:24:34	USER32	0	1074	程序 msiexec.exe 已代表使用者 NT AUTHORITY\SYSTEM，啟動電腦 [redacted] 的重
2020/1/7 上午 01:24:34	Microsoft-W...	0	10001	正在結束工作階段 0 已啟動 2020-01-06T17:24:26.481886200Z。
2020/1/7 上午 01:24:34	MsiInstaller	0	1040	開始 Windows Installer 交易: Http://Ae.A15.Xyz/SMB2.jpg。用戶端處理程序識別碼: 3616。
2020/1/7 上午 01:24:34	MsiInstaller	0	1005	Windows Installer 已經發出系統重新啟動的要求，以便完成或繼續執行 FONDQXIMSYHLISND
2020/1/7 上午 01:24:34	MsiInstaller	0	1042	結束 Windows Installer 交易: Http://Ae.A15.Xyz/SMB2.jpg. 用戶端處理程序識別碼: 3212.
2020/1/7 上午 01:24:34	MsiInstaller	0	1038	Windows Installer 需要重新啟動系統。產品名稱: FONDQXIMSYHLISNDBCFPGGQDFFXNKBAR
2020/1/7 上午 01:24:34	MsiInstaller	0	1033	Windows Installer 已安裝該產品。產品名稱: FONDQXIMSYHLISNDBCFPGGQDFFXNKBARIRJH
2020/1/7 上午 01:24:34	MsiInstaller	0	11707	产品: FONDQXIMSYHLISNDBCFPGGQDFFXNKBARIRJH -- 成功地完成了安装。
2020/1/7 上午 01:24:33	Service Cont...	0	7040	
2020/1/7 上午 01:24:26	Microsoft-W...	0	10000	正在開始工作階段 0 - 2020-01-06T17:24:26.481886200Z。
2020/1/7 上午 01:24:23	Service Cont...	0	7036	
2020/1/7 上午 01:24:23	Service Cont...	0	7036	
2020/1/7 上午 01:24:23	Microsoft-W...	12548	4672	特殊權限已指派給新登入。 主旨: 安全性識別碼: S-1-5-18 帳戶名稱: SYSTEM 帳戶網域
2020/1/7 上午 01:24:23	Microsoft-W...	12544	4624	帳戶成功登入。 主旨: 安全性識別碼: S-1-5-18 帳戶名稱: [redacted]$ 帳戶網域
2020/1/7 上午 01:24:23	MsiInstaller	0	1040	開始 Windows Installer 交易: Http://Ae.A15.Xyz/SMB2.jpg。用戶端處理程序識別碼: 3212。

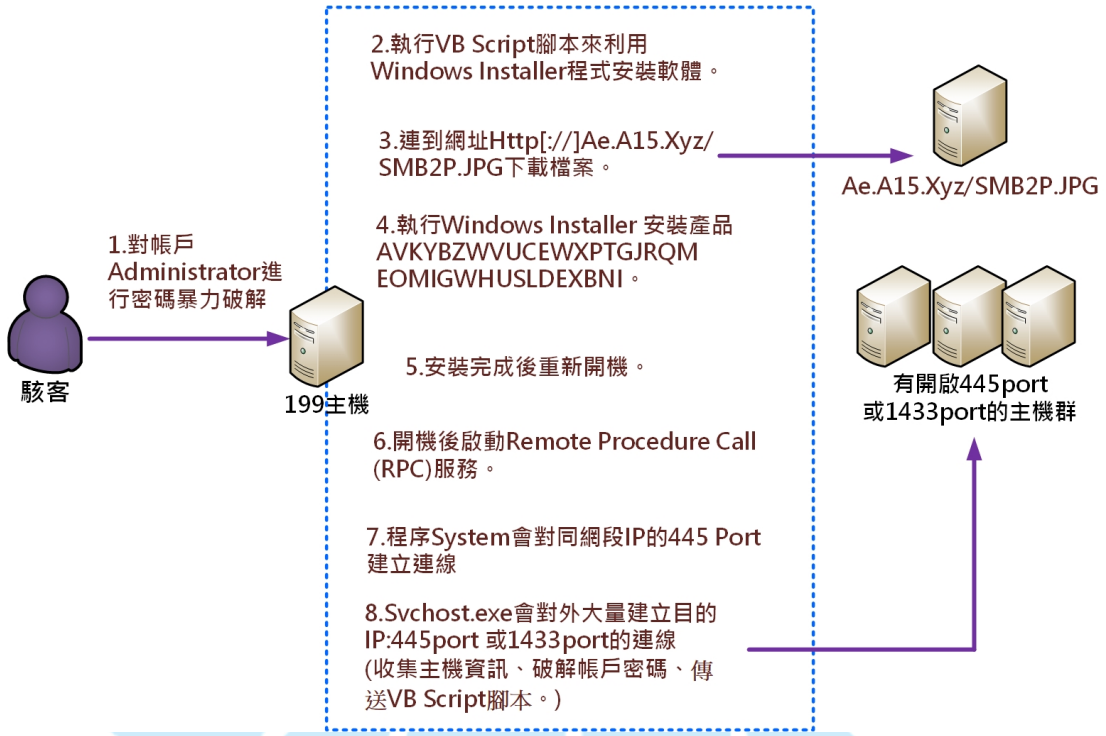
5. 81 主機在 2020/01/07 01:30 開始安裝軟體與重新開機，其所連線的網址為 Http[://]Ae.A15.Xyz/SMB1.JPG，該網址經 Virustotal 檢測其惡意比例為 9/72。

6. 經由檢測三台主機得知這些主機有下列共同的特徵。

項目	81 主機	69 主機	199 主機
有無帳戶 Administrator/ 有無密碼	有/有設密碼	有/未設密碼	有/未設密碼
445 port 是否開啟	是	是	是
3389port 是否開啟	是	是	是
2020/01/07 執行 Windows Installer 時間	2020/01/07 01:29	2020/01/07 01:24	2020/01/07 08:33
其他	系統內建執行程式帳戶 system 於 2020/01/07 01:29 登入、執行軟體安裝。	系統內建執行程式帳戶 system 於 2020/01/07 01:24 登入、執行軟體安裝。	由同一網段 IP:140.X.X.200 於 2020/01/07 08: 33 登入，使用 VB Script 腳本，之後帳戶 system 於 2020/01/07 08:33 執行軟體安裝。

三、事件攻擊行為示意圖

本事件三台主機的攻擊手法皆相同，以 199 主機為例，說明如下圖。



1. 駭客對帳戶 Administrator 進行暴力破解密碼。
2. 執行 VBScript 腳本來利用 Windows Installer 程式安裝軟體。
3. 連到網址 Http[://]Ae.A15.Xyz/SMB2P.JPG 下載檔案。
4. 執行 Windows Installer 安裝產品 AVKYBZWVUCEWXPTGJRQMEOMIGWHUSLDEXBNI。
5. 安裝完成後主機重新開機。
6. 重新開機後，主機會啟動 Remote Procedure Call(RPC)服務。
7. 程序 System 會對同網段 IP 的 445 Port 建立連線。
8. Svchost.exe 會執行 RPCSS，對外大量建立目的 IP:445port 或 1433port 的連線，收集各連線主機的系統資訊，並且嘗試破解帳戶 Administrator 的密碼。當成功登入受害主機後，會傳送 VB Script 腳本給受害主機。

四、總結與建議

1. 本事件的攻擊行為主要是駭客利用 SMB 漏洞進行暴力破解密碼，進而攻

擊有開啟 445port 的目的 IP 主機，造成多台主機感染惡意程式。

2. 維護廠商在安裝學校主機時會習慣性建立帳戶 Administrator，以便維護使用，但該帳戶未設定密碼，讓駭客很容易駭入主機。
3. 當主機被駭入後會使用 VB Script 腳本執行 Windows Installer，連至網址 Http[://]Ae.A15.Xyz/SMB2P.JPG 下載檔案來安裝惡意程式。
4. 當主機安裝惡意程式完成並重開機後，Svchost.exe 會對外進行大量的 445port 或 1433port 的攻擊連線。
5. 關於本事件的預防措施，有幾點建議如下:
   (1) 建議關閉駭客常會攻擊的 445port。
   (2) 如需開啟 3389port，建議限制連線來源的 IP。
   (3) 定期更新防毒軟體的病毒碼，並且定期進行掃毒作業。
   (4) 檢視主機帳戶資訊，並關閉非必要的帳戶。
   (5) 加強帳戶的密碼強度。
   (6) 定期更新作業系統與修補程式的漏洞。
   (7) 定期備份資料。