銀行木馬 emotet 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 1 月

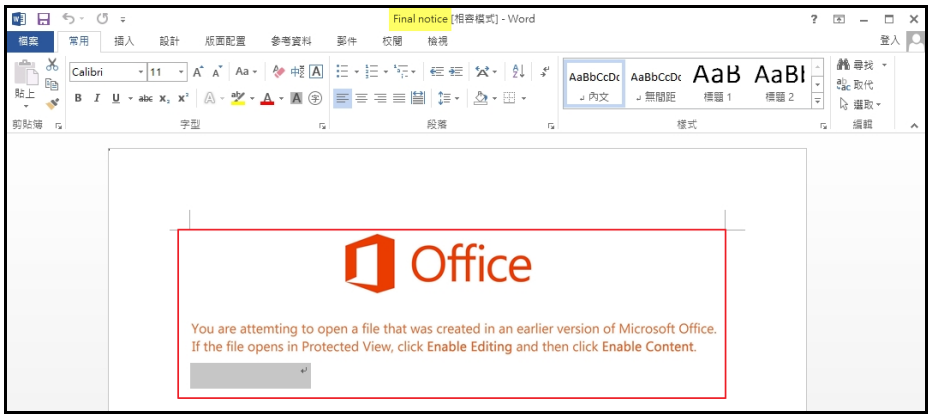
一、 事件簡介

1. 2014 年安全研究人員首次發現了銀行特洛伊木馬 Emotet，它最初被設計為一種銀行惡意軟體，試圖潛入使用者的電腦來竊取敏感和私密信息。
2. 2018 年後續版本的 Emotet 包括向受感染主機安裝其他惡意軟體的能力，此惡意軟體可能包括其他銀行特洛伊木馬或垃圾郵件(malspam)傳遞服務。
3. 趨勢科技在 2018 年 11 月公布知名銀行木馬 Emotet 的蹤跡，發現它在 2018 年 6 月 1 日到 11 月 15 日期間於全球建立 721 個 C&C 伺服器，採用 8,528 個獨立的 URL，使用 5,849 個文件 Dropper 以及 571 個執行檔案。

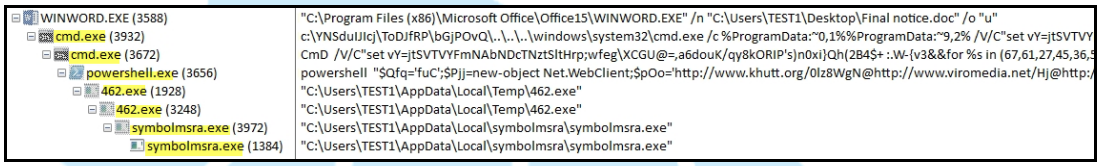
4. 為了解現行的銀行木馬 Emotet 之惡意行為，本中心取得樣本進行檢測。

二、 事件檢測

1. 首先，在 Windows 7 作業系統上，開啟樣本 Final notice.doc。打開後，出現該文件是由早期 office 版本所產生的說明文字，並告知要如何才能看到文檔內容。當該 Word 檔開啟後，若沒有使用檢測工具，一般使用者不會感覺到主機有異常現象。

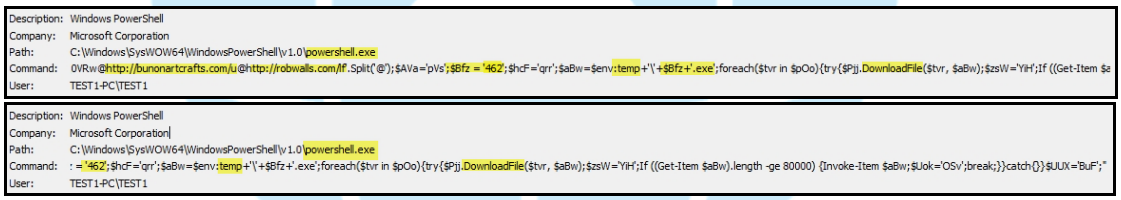


2. 檢視主機背景程式運作情形，發現在 Final notice.doc 開啟後，會直接呼叫 cmd.exe 2 次，之後再陸續執行 powershell.exe、462.exe 與 symbolmsra.exe。



從 Powershell 的命令列可以看到有一些網址的資訊與 DownloadFile 用字，推測該指令可能連線至這些網址下載東西到受測主機內。

從命令列中也可以得知在 temp 資料夾中會產生一個 462.exe 執行檔。

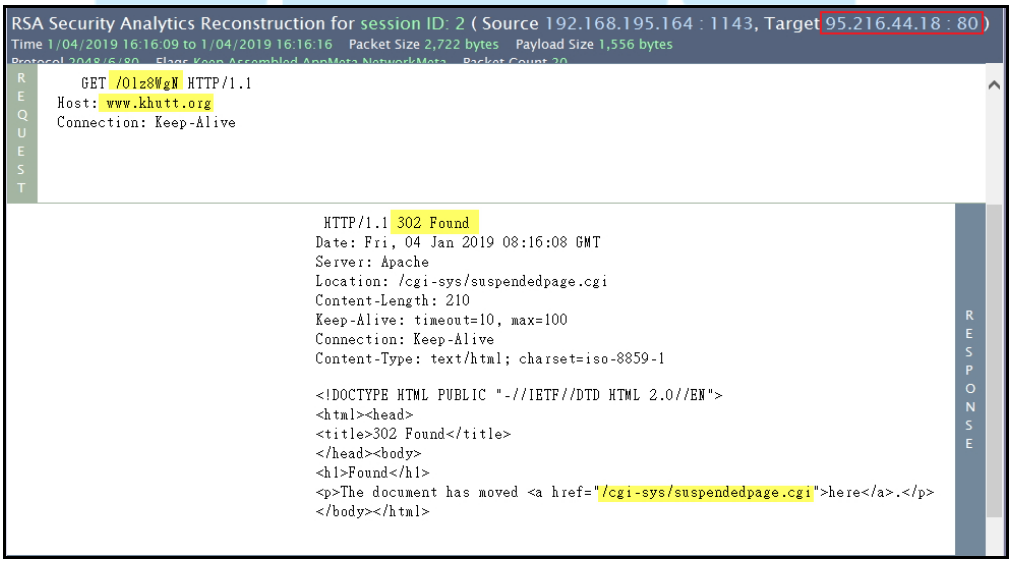


3. 檢視主機對外連線狀態，發現執行 powershell.exe 時會對外連線 3 個固定的目的 IP，分別為芬蘭 IP:95.216.44.18、美國 IP:108.174.147.74 與英國 IP:37.247.116.235，而執行 symblomsra.exe 時會對外連線數個目的 IP，其中英國 IP:95.141.175.240 為常連線的目的 IP。

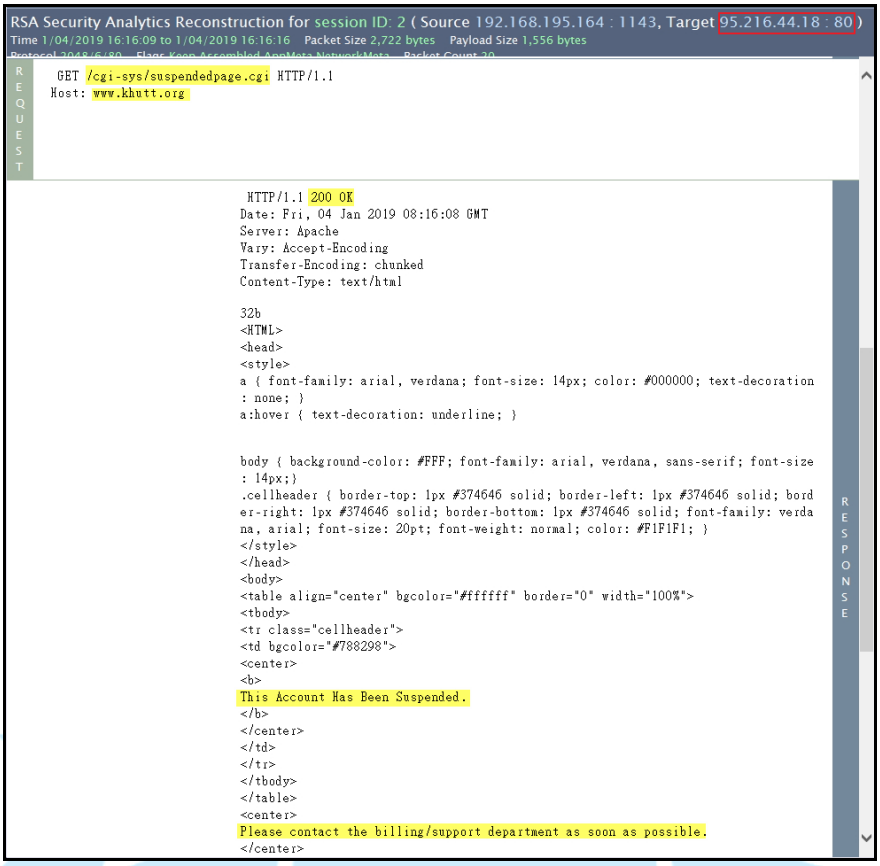
2019/1/4 下午 04:16:06 Added	WINWORD.EXE	TCP 192.168.195.164:1141	203.69.81.50:80
2019/1/4 下午 04:16:06 Added	WINWORD.EXE	TCP 192.168.195.164:1142	163.28.228.10:80
2019/1/4 下午 04:16:06 Added	powershell.exe	TCP 192.168.195.164:1143	95.216.44.18:80
2019/1/4 下午 04:16:08 Added	powershell.exe	TCP 192.168.195.164:1144	108.174.147.74:80
2019/1/4 下午 04:16:12 Added	powershell.exe	TCP 192.168.195.164:1145	37.247.116.235:80
2019/1/4 下午 04:16:14 Added	WINWORD.EXE	TCP 192.168.195.164:1146	117.18.237.29:80
2019/1/4 下午 04:16:33 Added	WINWORD.EXE	TCP 192.168.195.164:1147	117.18.237.29:80
2019/1/4 下午 04:16:33 Added	symbolmsra.exe	TCP 192.168.195.164:1148	105.228.198.254:7080
2019/1/4 下午 04:16:49 Added	WINWORD.EXE	TCP 192.168.195.164:1149	104.18.24.243:80
2019/1/4 下午 04:16:55 Added	symbolmsra.exe	TCP 192.168.195.164:1150	83.110.95.159:990
2019/1/4 下午 04:16:59 Added	WINWORD.EXE	TCP 192.168.195.164:1151	117.18.232.200:80
2019/1/4 下午 04:17:15 Added	symbolmsra.exe	TCP 192.168.195.164:1152	169.0.142.82:8080
2019/1/4 下午 04:17:19 Added	WINWORD.EXE	TCP 192.168.195.164:1153	210.65.144.177:80
2019/1/4 下午 04:17:35 Added	symbolmsra.exe	TCP 192.168.195.164:1154	189.152.183.239:80
2019/1/4 下午 04:17:58 Added	symbolmsra.exe	TCP 192.168.195.164:1155	187.205.170.3:990
2019/1/4 下午 04:18:18 Added	symbolmsra.exe	TCP 192.168.195.164:1156	85.243.49.63:80
2019/1/4 下午 04:18:38 Added	symbolmsra.exe	TCP 192.168.195.164:1157	105.225.199.219:80
2019/1/4 下午 04:19:01 Added	symbolmsra.exe	TCP 192.168.195.164:1158	189.186.19.97:50000
2019/1/4 下午 04:19:21 Added	symbolmsra.exe	TCP 192.168.195.164:1159	189.183.174.174:50000
2019/1/4 下午 04:19:43 Added	symbolmsra.exe	TCP 192.168.195.164:1160	89.211.243.207:80
2019/1/4 下午 04:20:03 Added	symbolmsra.exe	TCP 192.168.195.164:1161	91.236.245.65:8080
2019/1/4 下午 04:20:24 Added	symbolmsra.exe	TCP 192.168.195.164:1162	95.141.175.240:443
2019/1/4 下午 04:34:44 Added	symbolmsra.exe	TCP 192.168.195.164:1163	95.141.175.240:443
2019/1/4 下午 04:49:24 Added	symbolmsra.exe	TCP 192.168.195.164:1187	95.141.175.240:443
2019/1/4 下午 05:03:44 Added	symbolmsra.exe	TCP 192.168.195.164:1216	95.141.175.240:443

4. 查看所側錄的主機對外連線封包，發現到下列資訊。

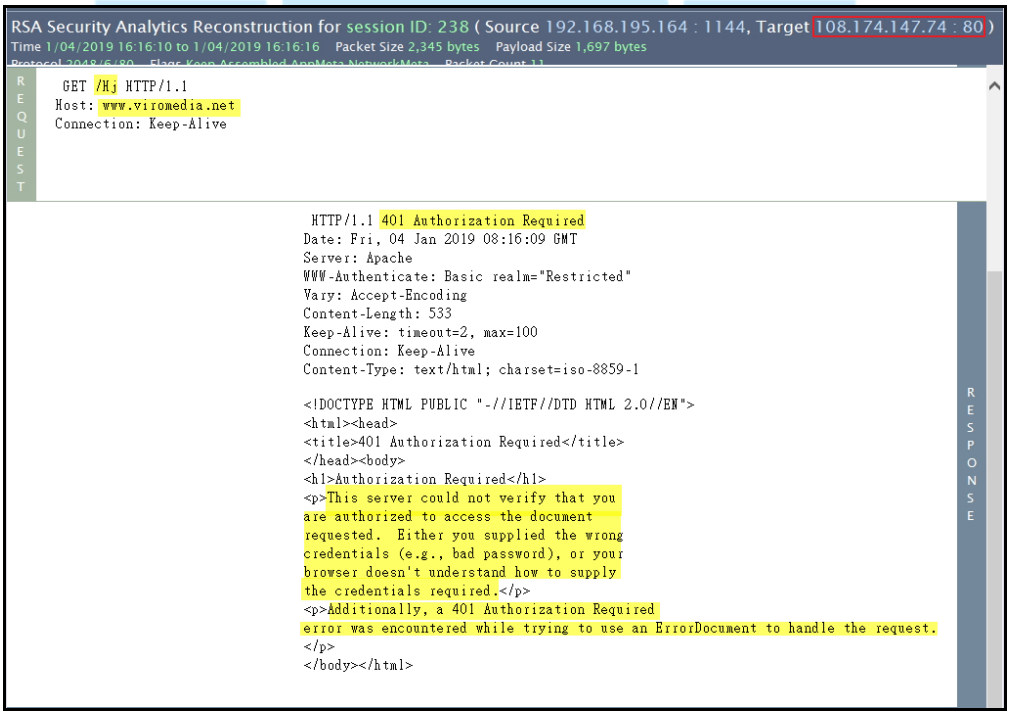
(1) 當執行 powershell.exe 而連線芬蘭 IP:95.216.44.18 時，對方主機回覆 http://www.khutt.org/0lz8WgN 的內容已被移至/cgi-sys/suspendedpage.cgi。



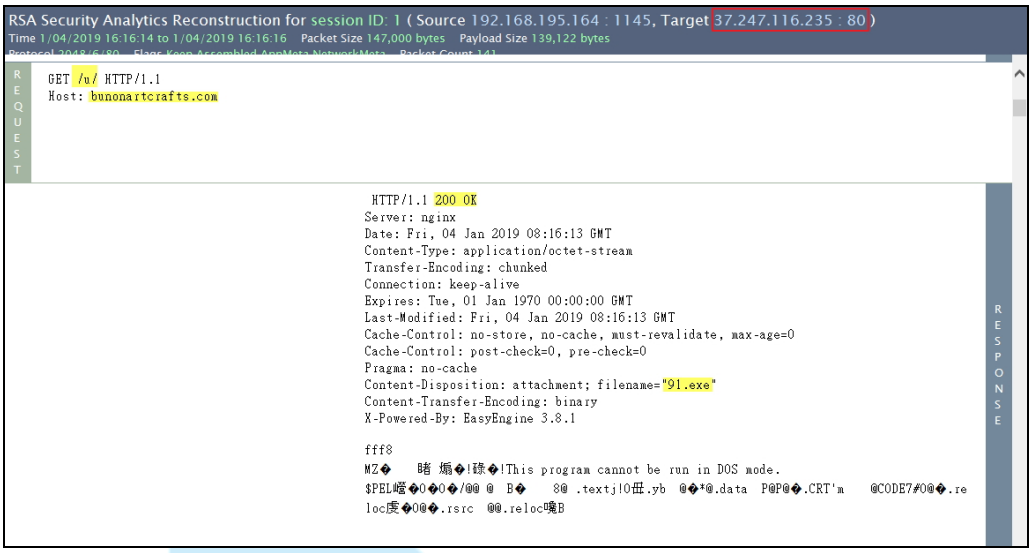
當瀏覽 http://www.khutt.org/cgi-sys/suspendedpage.cgi 網頁時，則被告知該帳號為可疑帳號，請盡速聯絡支援部門。



(2) 當執行 powershell.exe 而連線美國 IP:108.174.147.74 時，主機回覆伺服器無法驗證使用者是否有連線存取文件的權限，需有授權才可以存取。



(3) 當 powershell.exe 執行而連線英國 IP:37.247.116.235 時，會下載檔案 91.exe。



(4) 當執行 symblomsra.exe 而連線英國 IP:95.141.175.240 時，對方主機回覆經加密過的亂碼。該連線行為每隔一段時間便重啟連線，推測為受測主機對遠端主機進行報到動作，告訴遠端主機該主機仍然存活著。

5. 查看 462.exe 與 symbolmsra.exe 兩程式所在的資料夾，發現 462.exe 在它執行後便自我刪除，而 symbolmsra.exe 仍然在該資料夾內。

6. Final notice.doc 與 symbolmsra.exe 經 Virustotal 檢測，其結果如下:

(1) Final notice.doc:惡意比例為 42/59，而且有多家防毒軟體公司將它視為 Downloader 下載器。

SHA256:	6d803fd64139bbee1f626acd3c70bc7161830715b44690129776a0042fc9890f
檔案名稱:	Final notice.doc
偵測率:	42 / 59
分析日期:	2019-01-04 08:47:43 UTC (0 分鐘 前)

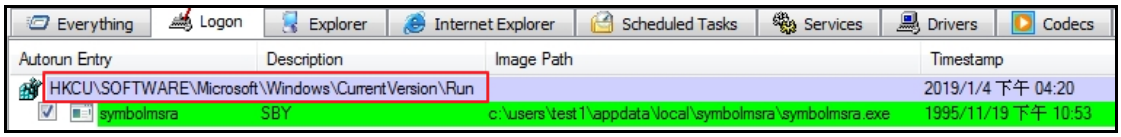
防毒	結果
Ad-Aware	W97M.Downloader.HRE
AhnLab-V3	DOC/Downloader
ALYac	W97M.Downloader.HRE
Antiy-AVL	Trojan[Downloader]/MSOffice.Agent.lrn
Baidu	VBA.Trojan-Downloader.Agent.dwt
BitDefender	W97M.Downloader.HRE
CAT-QuickHeal	W97M.Emotet.33612
ClamAV	Doc.Downloader.Generic-6776294-0
Cyren	W97M/Downldr.E.gen!Eldorado
DrWeb	W97M.DownLoader.3179
Emsisoft	Trojan-Downloader.Macro.Generic.L (A)
ESET-NOD32	VBA/TrojanDownloader.Agent.LRN
F-Secure	W97M.Downloader.HRE
GData	Macro.Trojan-Downloader.Shallow.S
Ikarus	Trojan-Downloader.VBA.Agent
McAfee	W97M/Downloader!34935653BF23
McAfee-GW-Edition	BehavesLike.Downloader.cg
Microsoft	TrojanDownloader:O97M/Donoff
eScan	W97M.Downloader.HRE
Panda	O97M/Downloader
Symantec	W97M.Downloader

(2) symbolmsra.exe:惡意比例為 55/70，有多家防毒軟體公司用 Emotet 命名它。

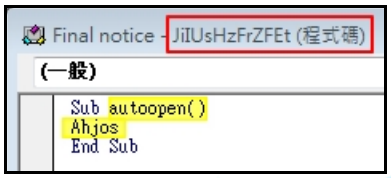
SHA256:	f5f4e7b656f8cfcdef2fa2fb56c9e3825c8b10047408c6020fdf86261c06b067
檔案名稱:	symbolmsra.exe
偵測率:	55 / 70
分析日期:	2019-01-04 08:52:02 UTC (0 分鐘 前)

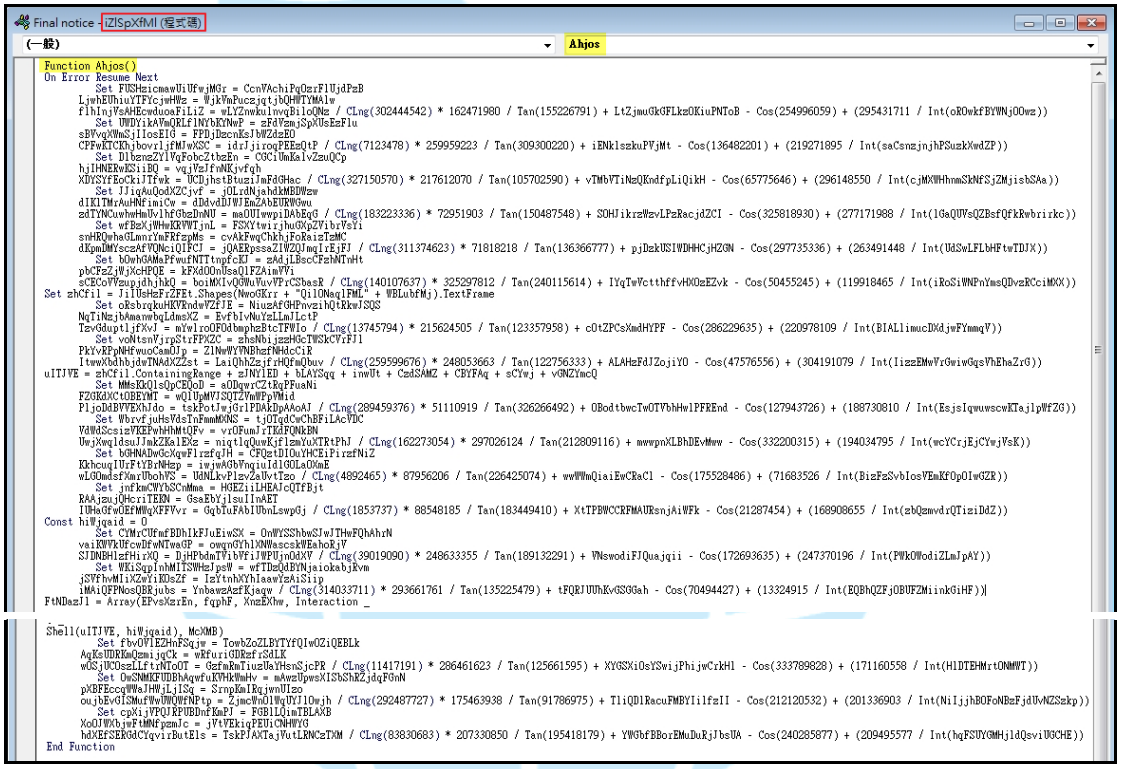
防毒	結果
Acronis	suspicious
Ad-Aware	Trojan.Autoruns.GenericKD.31402830
AegisLab	Trojan.Win32.Emotet.4!c
AhnLab-V3	Trojan/Win32.Emotet.R248220
ALYac	Trojan.Agent.Emotet
Antiy-AVL	Trojan[Banker]/Win32.Emotet
CAT-QuickHeal	Trojan.Emotet.R6
Cyren	W32/Emotet.KT.gen!Eldorado
DrWeb	Trojan.DownLoader27.18661
F-Prot	W32/Emotet.KT.gen!Eldorado
Ikarus	Trojan-Banker.Emotet
Jiangmin	Trojan.Banker.Emotet.eop
Kaspersky	Trojan-Banker.Win32.Emotet.buni
Malwarebytes	Trojan.Emotet.Generic
McAfee	Emotet-FJX!CA37ACC88BF0
McAfee-GW-Edition	BehavesLike.Win32.Emotet.ch
Microsoft	Trojan:Win32/Emotet.BF
NANO-Antivirus	Trojan.Win32.Emotet.flauyi
Panda	Trj/Emotet.C
Symantec	Trojan.Emotet
TACHYON	Banker/W32.Emotet.135168.BI
TrendMicro	TrojanSpy.Win32.EMOTET.THABAOAH
TrendMicro-HouseCall	TrojanSpy.Win32.EMOTET.THABAOAH
VBA32	BScope.Trojan.Emotet
Webroot	W32.Trojan.Emotet
Yandex	Trojan.PWS.Emotet!
Zillya	Trojan.Emotet.Win32.9279
ZoneAlarm by Check Point	Trojan-Banker.Win32.Emotet.buni

7. 檢視主機登錄檔紀錄，發現 symbolmsra.exe 會在主機重新開機後自動啟動。

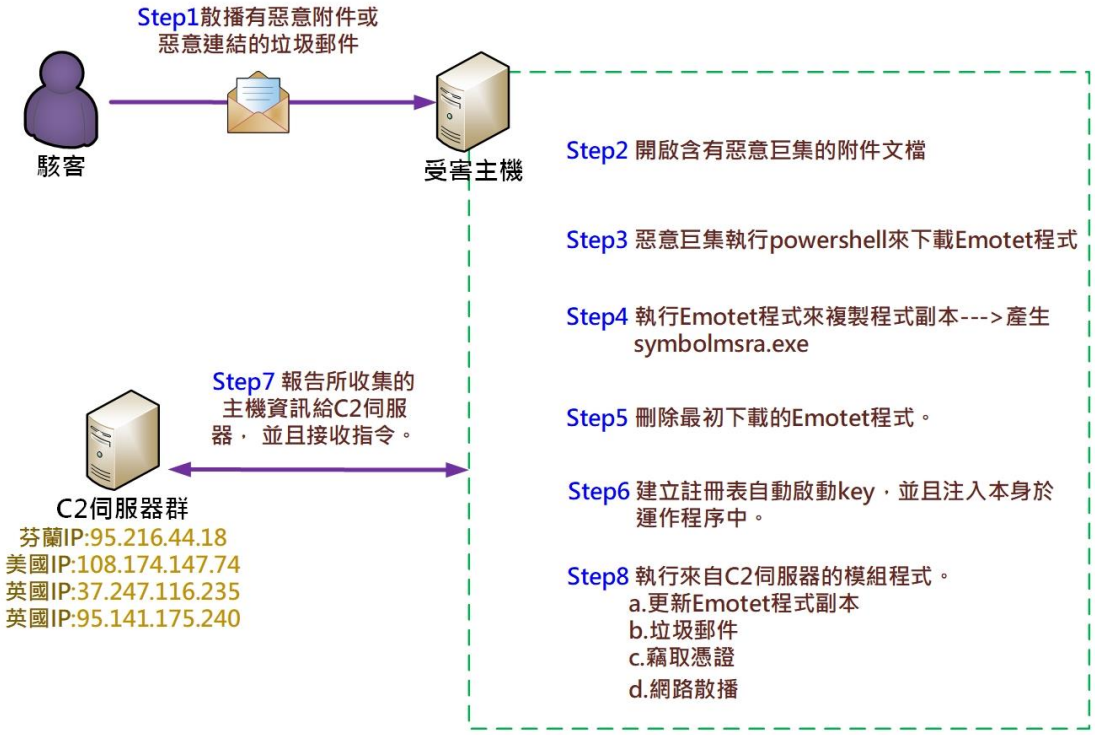


8. 查看 Final notice.doc 的內容，發現內藏巨集，而且透過該巨集會呼叫 cmd.exe 與 Powershell.exe 來執行惡意程式下載行為。從巨集的程式碼內容得知，Function Ahjos 會在 Word 檔被打開時自動執行。





三、 事件攻擊行為示意圖



1.駭客散播有惡意附件或惡意連結的垃圾郵件。

2.使用者開啟含有惡意巨集的附件文檔。

3.惡意巨集呼叫 cmd.exe 與 powershell.exe 來下載 Emotet 惡意程式(ex.462.exe)。

4.執行 Emotet 程式來複製程式副本至主機內，因而產生 symbolmsra.exe。

5.刪除最初下載的 Emotet 程式 (ex.462.exe)。

6.執行 symbolmsra.exe 建立註冊表自動啟動 key，並且注入本身於運作程序中。

7.報告所收集的主機資訊給 C2 伺服器，並且接收指令。

8.執行來自 C2 伺服器的模組程式(ex.91.exe)。(a.更新 Emotet 程式副本　b.垃圾郵件　c.竊取憑證　d.網路散播)

四、　建議與總結

1. Emotet 通常透過垃圾郵件（malspam）來進行散播。早期版本使用惡意 JavaScript 文件來感染主機，後來的版本演變為它可通過惡意腳本、啟用 macro 的文檔或惡意連結來感染受害主機。
2. 當使用者開啟或下載含有 Emotet 的惡意 PDF 或 Word 檔案，Emotet 就能常駐於受害者的電腦上，進而下載其它的惡意模組，或是伺機感染網路上的其它裝置。
3. Emotet 可使用 C&C 伺服器來接收更新，這允許攻擊者安裝軟體的更新版本、安裝其他惡意軟體（如其他銀行特洛伊木馬），或作為財務憑證，用戶名和密碼以及電子郵件地址等被盜信息的傾倒場。
4. Emotet 也可使用「Eternal Blue」 SMB 漏洞來直接感染未修補的 Windows 系統 ，而且都不需要任何使用者點擊或登錄。
5. 針對 Emotet 的資安防護與處理作業，提供幾點建議如下。
   (1) 定期更新作業系統的修補程序與更新病毒碼，使主機保持最新狀態。
   (2) 因 Emotet 可利用 Windows Eternal Blue 漏洞來執行其工作，建議關閉與此漏洞有關的 445 port。
   (3) 請勿下載與開啟可疑附件或點擊可疑的連結。
   (4) 加強使用者帳戶的密碼強度。