

個案分析-

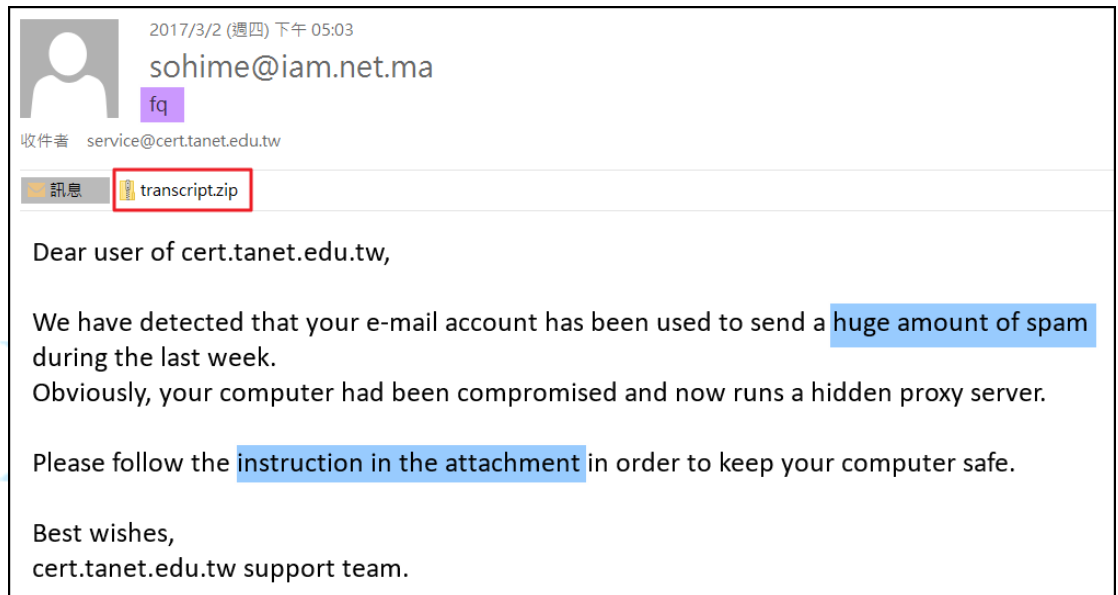
帶有惡意程式的垃圾郵件
SPAM 攻擊事件分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

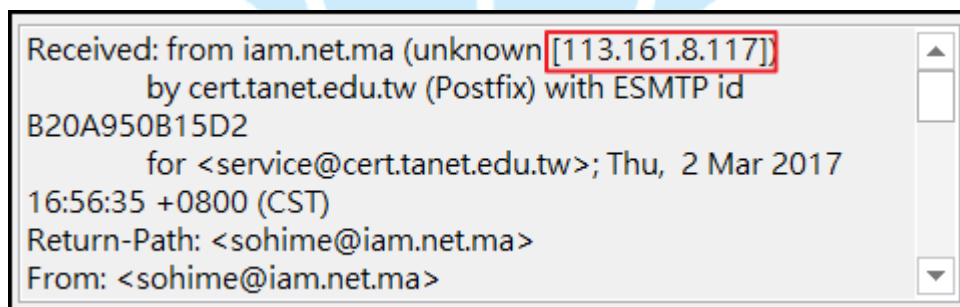
106 年 5 月

1. 事件簡介

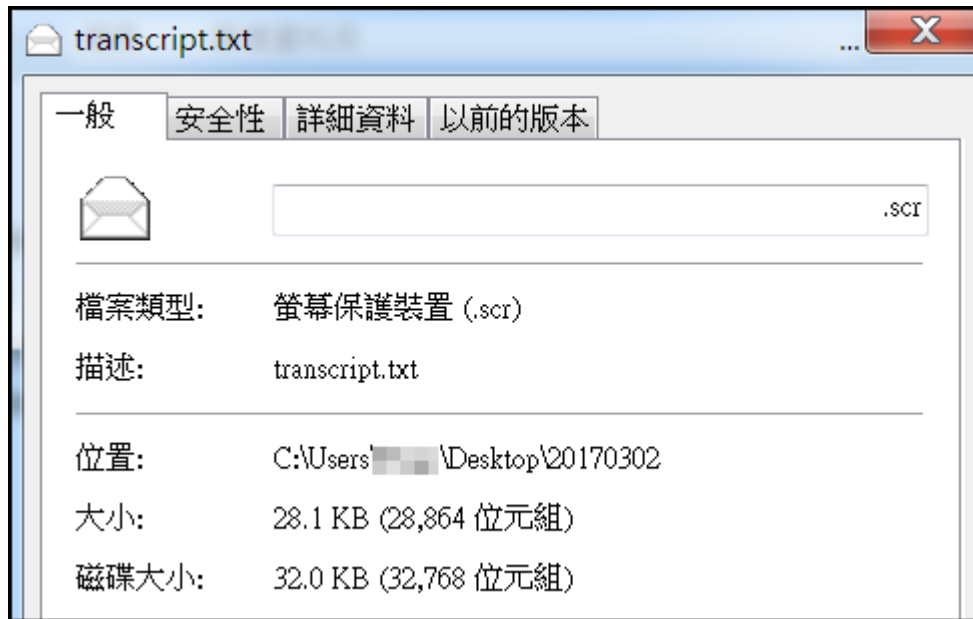
1. 近期發現有針對本單位進行垃圾郵件 SPAM 攻擊，其郵件以“fq”作為主旨，且內容為述說我們大量發送 SPAM 郵件，並要求依照信件內容開啟附加檔案進行修補感染，實質上為惡意程式的壓縮檔案“transcript.zip”。



2. 這次事件收件者位址為單位的公開服務地址，故有心人士會容易取得並且嘗試進行滲透。從郵件 Header 檢查發信者的 IP，為來自越南的 113.161.8.117，而非位於寄件者的網域(.ma)國家摩洛哥，表示寄件者名稱是偽造的。



3. 郵件附加檔案解壓縮後，為一支偽裝成文件檔 TXT 的 SCR 執行檔“transcript.txt...scr”，透過在檔案名稱尾端插入大量空白字元來遮蔽其附檔名 SCR，誘使使用者不注意執行。

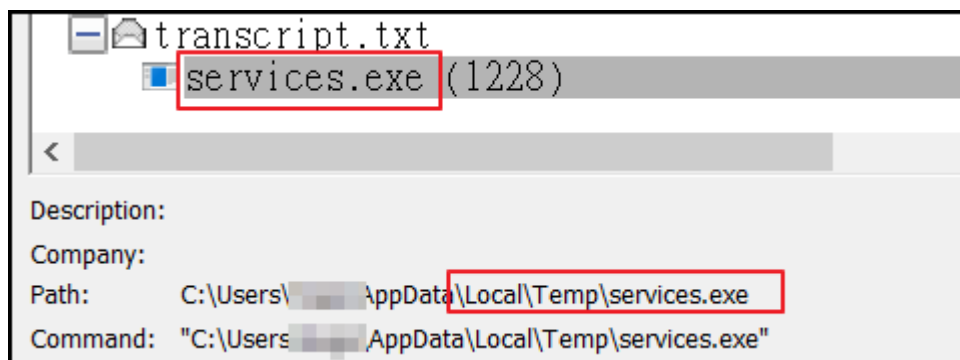


II. 事件檢測

1. 在測試惡意程式時候，預先使用 Win7(x86)來開啟執行該惡意程式
“transcript.txt.scr”，因為預設檔名插入大量空白過於冗長，導致
32 位元系統無法正常辨識執行。因此該惡意程式只對於 64 位元系統有
效。

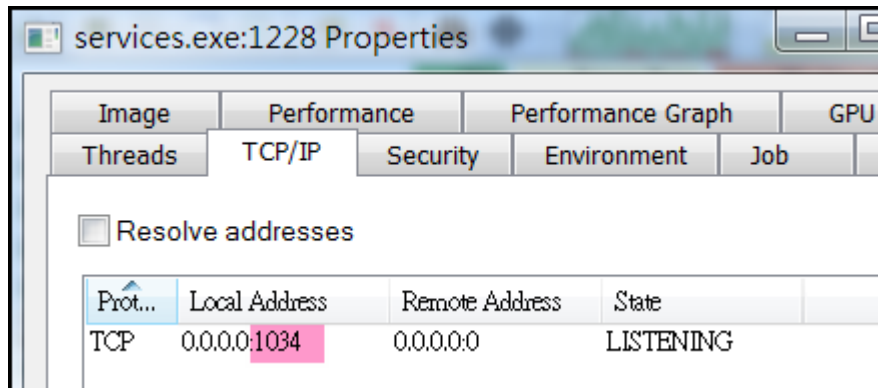
```
2004/03/02 上午 09:03 28,864 transcript.txt  
...  
.scr
```

2. 實際執行惡意程式 scr 檔案後，在視窗上並無出現任何訊息，但透過
procexp 檢視背景程式狀態，可以看到 scr 惡意程式產生出新的子程式
services.exe。

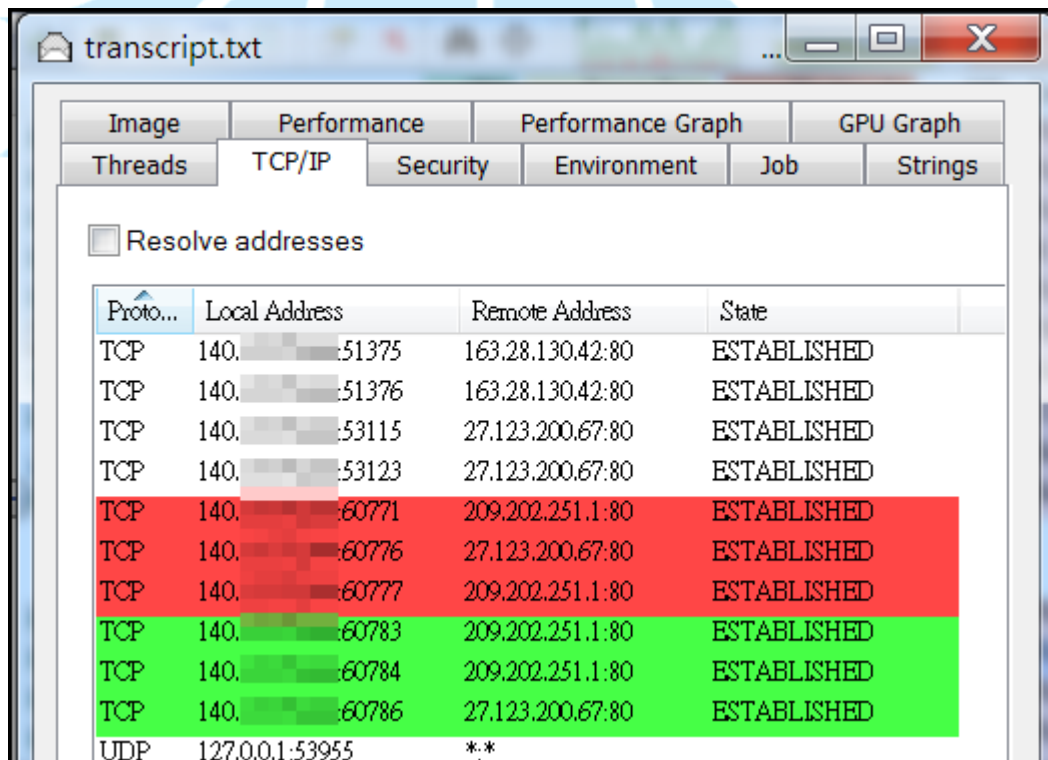


3. 該 services.exe 是由 transcript.txt.scr 所產生，並且位於暫存資料夾

內，檢查 services.exe 的連線狀態能看出有開啟 Port Listening，表示能夠讓駭客或 C&C 連入做控制。



4. 在檢查父程式 transcript.txt.scr 的連線狀態，可以看到有大量的對外連線和流量，檢查以下連線 IP 幾乎都是搜尋引擎網站。



5. 除此之外還觀察到惡意程式 transcript.txt.scr 除了會連到搜尋引擎網站，還會產生大量對外 port 25 的連線，可能是正在對外發送 SPAM 郵件。

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port
[System Process]	0	TCP	140.	62479	173.194.67.27	25
[System Process]	0	TCP	140.	62487	74.125.201.26	25
[System Process]	0	TCP	140.	62485	142.103.226.211	25
[System Process]	0	TCP	140.	62482	164.15.128.114	25
[System Process]	0	TCP	140.	62488	173.194.175.26	25
[System Process]	0	TCP	140.	62489	64.233.189.26	25
[System Process]	0	TCP	140.	62484	173.38.212.150	25
[System Process]	0	TCP	140.	62490	173.194.219.26	25
[System Process]	0	TCP	140.	62492	173.37.147.230	25
[System Process]	0	TCP	140.	62491	134.184.129.114	25
[System Process]	0	TCP	140.	62494	72.163.7.166	25
[System Process]	0	TCP	140.	62503	134.58.240.2	25

6. 從封包內容來檢視，transcript.txt 連到的 port 80 幾乎都是各大家的搜尋引擎，並且大量搜尋可用的電子郵件網域，並且開始準備發送 SPAM。

```

RSA Security Analytics Reconstruction for session ID: 23 ( Source 140. : 49176, Target 27.123.200.67 : 80
Time 3/31/2017 14:55:32 to 3/31/2017 16:26:36 Calculated Packet Size 272,184 bytes Calculated Payload Size 253,026 bytes
Protocol 3048/6/80 Flags Keep Assembled AppMeta NetworkMeta Packet Count 352

REQUEST
GET /search?p=reply+126.com&ei=UTF-8&fr=fp-tab-web-t&cop=mss&tab=&n=100 HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/4.0
; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center
PC 6.0)
Host: search.yahoo.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Fri, 31 Mar 2017 06:55:34 GMT

```

```

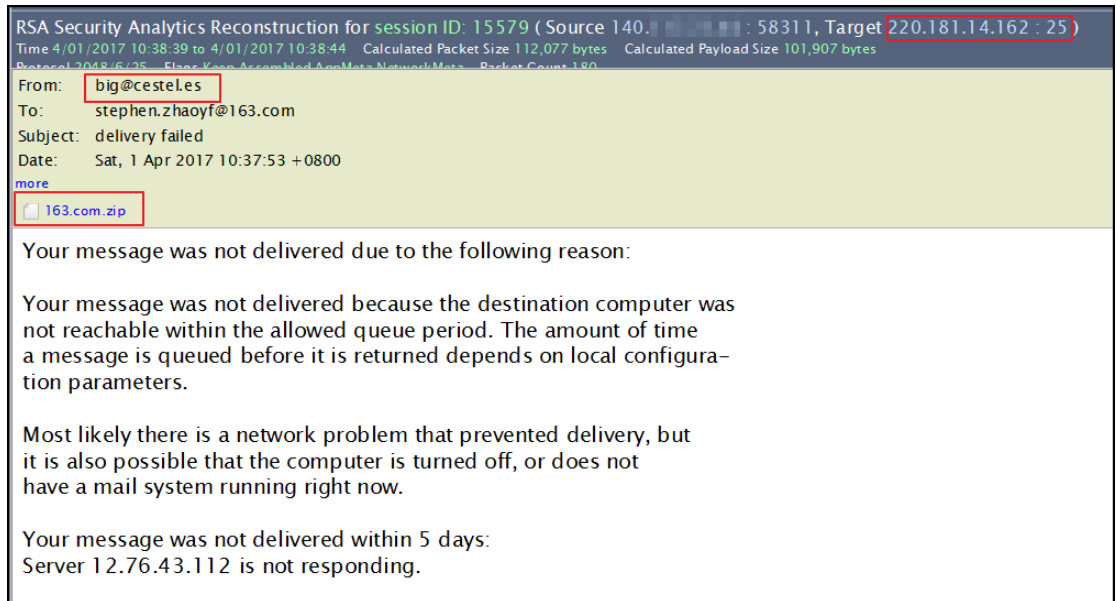
1. 126.COM 163.COM LEAKED DATABASE // Slexy 2.0

slexy.org/raw/s206EFYd0t
Cached

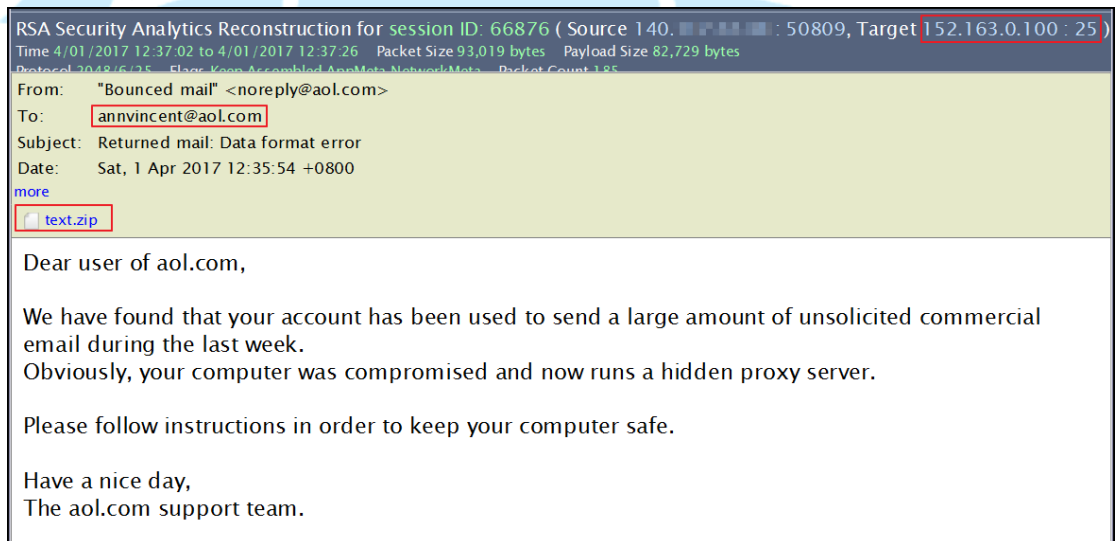
23 hours ago ... View raw paste · Reply. 126.COM 163.COM
LEAKED DATABASE: 24 MILLION ACCOUNTS. Here is the link
to this hacked databases: ... bedard.comeres.sarl@
126.com:bedard.come. bedanmwatha@126.com:milcah.

```

7. 檢查其中一比較完整的 SPAM 封包紀錄，得知惡意程式會偽造發信人地址，並且發送給搜尋到的 domain 為 163.com 收件者，通常會夾帶惡意檔案。



8. 檢查惡意程式發送較多的網域是 aol.com 的郵件來看，其內容格式來看與本事件收到的郵件內容相符，表示其不算是 APT 攻擊，只是亂槍打鳥方式的 SPAM 惡意郵件。



9. 惡意程式 Transcript.txt.scr 在大量向搜尋引擎查詢 domain 資料後，Google 的網站會開始進行存取封鎖，因為有異常大量連線的偵測機制。

RSA Security Analytics Reconstruction for session ID: 26123 (Source 140.140.140.55701, Target 163.28.130.49:80)
Time 4/01/2017 10:44:35 to 4/01/2017 11:20:36 Packet Size 8,389,589 bytes Payload Size 7,309,331 bytes
Protocol 302/6/80 - Flags: Keep-Assembled-AppMeta-NetworkMeta- Packet Count 10,482

REQUEST
GET /search?hl=en&ie=UTF-8&oe=UTF-8&q=hsu-hh.de+email&num=50 HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET CLR 1.1.4324; PC 6.0)
Host: www.google.com
Connection: Keep-Alive

HTTP/1.1 302 Found
Location: http://ipv4.google.com/sorry/index?continue=http://www.google.com/search%3Fhl%3Den%26ie%3DUtf-8%26oe%3DUtf-8%26q%3Dhsu-hh.de%26email%26num%3D50&hl=en&q=EgSMdUgsGJOo_MYFIhka8aeDS-I-jOxIFmSdcXKHDCOyzTj4k7PqMgNyY24
Date: Sat, 01 Apr 2017 02:44:35 GMT

我們的系統偵測到您的電腦網路送出的流量有異常情況。請稍後重新傳送要求。為什麼會發生這種情況?
IP 位址: 140.140.140.55701
時間: 2017-04-13T06:45:06Z
網址: http://www.google.com/search?hl=en&ie=UTF-8&oe=UTF-8&q=hsu-hh.de+email&num=50

10. 從本次測試一周期間統計出，至少有對外部相異 2000 個 email 位址發送 SPAM 攻擊，以國別來說也有 59 個國家受害。發送 SPAM 期間也會消耗大量網路頻寬而造成網路壅塞。

E-mail Address (2017 items)
noreply@aol.com (36) - mailer-daemon@aol.com (33) - postmaster@163.com (18) - noreply@damiannou.eu (16) - noreply@pennwell.com (14) - noreply@263.net (12) - bdoctm@wlink.com.np (12) - postmaster@earthlink.net (11) - amir.rehman@tdap.gov.pk (11) - postmaster@aol.com (10) - noreply@mindspring.com (10) - noreply@kvack.org (10) - email@kvack.org (10) - chixson@joinagm.com (10) - wkt@cs.adfa.oz.au (9) - widad.charqi@villasofmorocco.com (9) - steve@vrma.co.za (9) - scott@hammock.net (9) - postmaster@ibl.bm (9) - postmaster@atlasnet.net.ma (9) - postmaster@alcatel-lucent.com (9) - postmaster@263.net (9) - ordemow@alcatel-lucent.com (9) - noreply@tdap.gov.pk (9) - mailer-daemon@hammock.net (9) - mailer-daemon@airmail.net (9) - jcantieri@juno.com (9) - info123@ektro.cz (9) - hover1@airmail.net (9) - skopje@damiannou.eu (8) - semlali@afriquia.ma (8) - postmaster@st.com (8) - postmaster@pennwell.com (8)

Destination Country (59 items)
united states (1,549) - morocco (230) - china (143) - germany (104) - france (93) - united kingdom (72) - netherlands (67) - canada (66) - argentina (35) - singapore (32) - hong kong (32) - spain (27) - south africa (25) - japan (25) - italy (24) - australia (22) - austria (18) - taiwan (17) - korea, republic of (17) - syrian arab republic (16) - europe (16) - russian federation (15) - ireland (15) - indonesia (15) - switzerland (13) - bermuda (13) - malaysia (12) - portugal (10) - jordan (8) - pakistan (7) - united arab emirates (6) - turkey (6) - poland (6) - luxembourg (6) - israel (6) - philippines (5) - czech republic (5) - belgium (5) - romania (4) - finland (4) - uruguay (3) - india (3) - estonia (3) - chile (3) - brazil (3) - thailand (2) - sweden (2) - peru (2) - moldova, republic of (2) - latvia (2) - egypt (2) - denmark (2) - bulgaria (2) - vietnam (1) - saudi arabia (1) - norway (1) - new zealand (1) - lebanon (1) - costa rica (1)

11. 最後將惡意程式樣本 transcript.txt.scr 送到 Virustotal 檢測，檢測為惡意的比例為 58/60 相當明顯，但也是有知名防毒廠商尚未檢測出。

SHA256: 1b4d12a35fe0619faec3e435d332da49b107102579544cca087dd8558013499
File name: transcript.txt.scr
Detection ratio: 58 / 60

Analysis Additional information Comments Votes

Antivirus	Result	Update
Palo Alto Networks (Known Signatures)	✓	20170413
TrendMicro	✓	20170413
McAfee-GW-Edition	BehavesLike.Win32.Mydoom.mc	20170413
Ikarus	Email-Worm.Win32.Mydoom	20170412

12. 另一支程式 services.exe 透過 Virustotal 檢測，檢出比例為 58/61 相當高，不過依然還是有知名防毒廠商尚未檢測出。

SHA256: bf316f51d0c345d61eaae3940791b64e81f676e3bca42bad61073227bee6653c

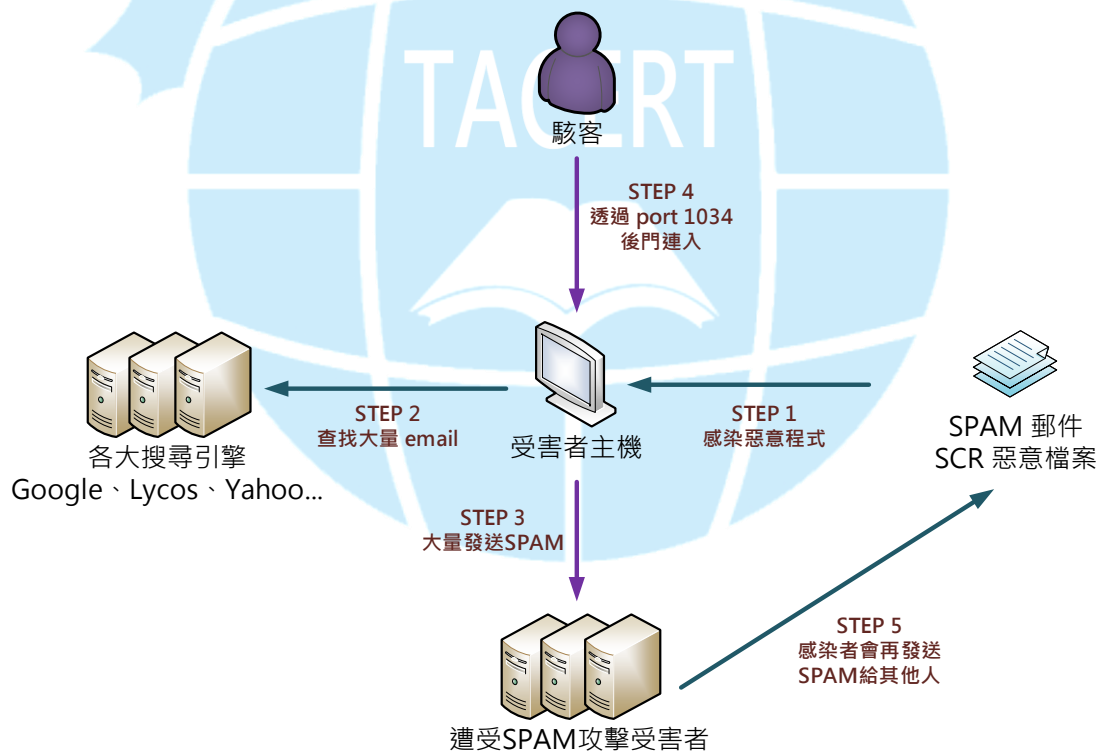
File name: b0fe74719b1b647e2056641931907f4a **services.exe**

Detection ratio: **58 / 61**

Analysis date: 2017-04-12 10:21:13 UTC (21 hours, 20 minutes ago)

Antivirus	Result	Update
Alibaba	☞	20170412
Kingsoft	✓	20170412
Symantec Mobile Insight	☞	20170412
TrendMicro	✓	20170412
TrendMicro-HouseCall	✓	20170412

III. 網路架構圖



1. 受害者開啟 SPAM 郵件中的附加檔案，為偽造成 TXT 的 SCR 惡意程式。
2. 受害主機會開始向外部的各大搜尋網站查找可用的郵件網域名稱。
3. 受害主機開始向搜尋到的 mail 位址發送大量的惡意 SPAM。

4. 駭客 C&C 可能透過 port 1034 連入感染主機，並下達其他攻擊指令。
5. 當新的受害者也感染惡意檔案後，也會開始對外發送 SPAM 郵件並成為新的 Botnet。

IV. 建議與總結

1. 此案例為惡意 SPAM 郵件攻擊，並附加偽造成 TXT 文件檔的 SCR 執行檔惡意程式。
2. 該惡意程式在副檔名 SCR 前塞入 TXT 和冗長的空白字元進行偽裝，一旦執行後會開啟 port 1034 為 Listen 狀態。
3. 惡意程式 SPAM 攻擊之前會大量向搜尋網站查找可攻擊的電子郵件網域，並且再對外進行 port 25 的 SPAM 郵件攻擊。
4. SPAM 郵件有可能會偽造寄件者的郵件地址為相同網域的地址，增加後受害者上當的機率。
5. 該事件受害者同時也會成為攻擊其他人的加害者，並且成為殭屍網路的主機讓駭客使用。
6. 所幸該惡意程式並不會寫入開機自動啟動區，當使用者重開主機後網路攻擊行為就不會再出現。
7. 此類型的社交工程郵件近年來一直很多，有的惡意程式多為加密勒索軟體，更應提高警覺避免誤觸。