個案分析-

駭客常用的 DDoS 攻擊程式分析報告

TACERT 臺灣學術網路危機處理中心團隊製

2015/11

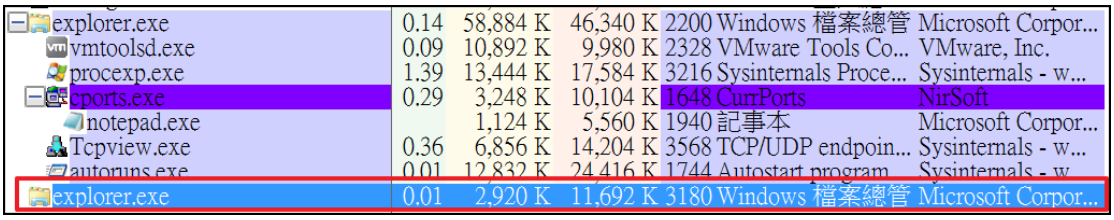
I. 事件簡介

1. 網路攻擊中最常發生的也最難防範的就是 DDoS 攻擊，因為駭客攻擊的伺服器主機都是透過合法的通訊埠進行流量攻擊，導致正常服務被癱瘓阻斷。
2. 駭客可能在某些地下網站散布此類的攻擊套件供民眾使用，除了讓使用者成為攻擊者，也可能讓使用者主機成為殭屍電腦為駭客所用。
3. 本單位透過一些方式取得到駭客常用的流量攻擊套件，並實地測試該套件的功能以及可能潛藏的危害。
4. 該惡意程式的檔案名稱為 DDoS Attack.exe，為 Windows 環境所用。

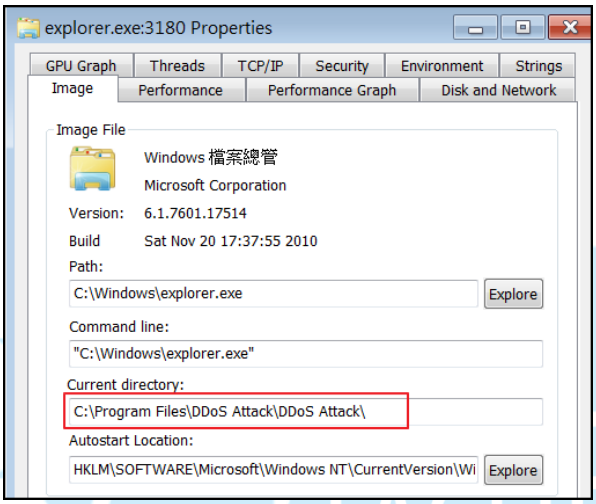
II. 事件檢測

1. 使用 VM 虛擬主機並且為 Windows 7 系統進行隔離環境測試。
2. 惡意程式樣本名稱為 DDoS Attack.exe，安裝過程中出現的都是簡體中文，因為編碼關係系統無法正常顯示。

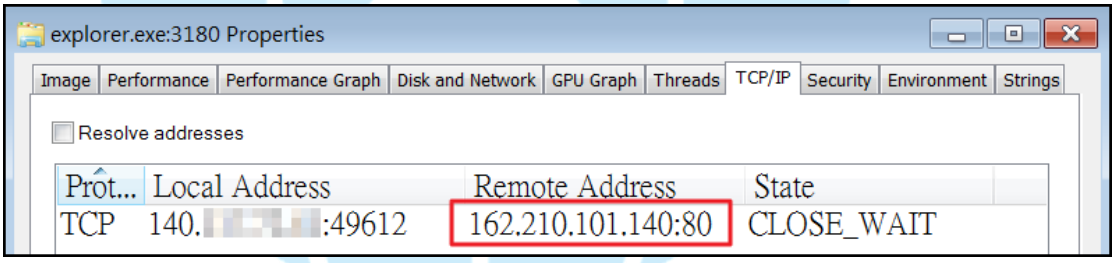
3. 待該惡意工具安裝完後先檢視其系統程式運作狀態，發現內部藏有木馬程式在背景執行。正常來說 explore 檔案總管只會有一個，該惡意程式會呼叫第二個 explore 在最下方進行監控主機資料。



4. 檢視惡意的 explore.exe 內容，是由剛剛所安裝的 DDoS Attack 軟體所執行，然而此時該軟體尚未啟用。

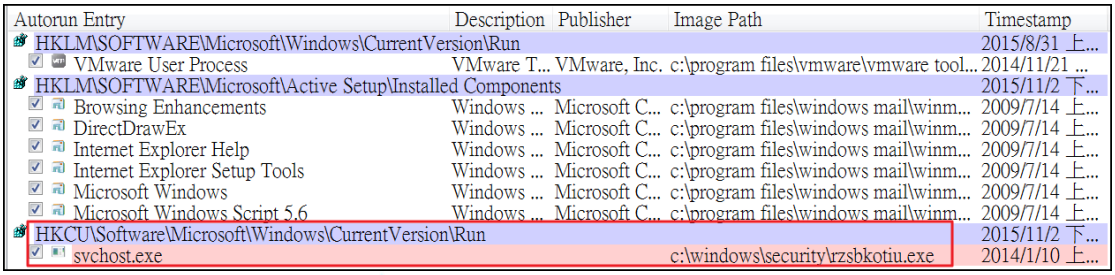


5. 檢查該 explore 的網路連線狀態，確實出現可疑的對外連線，疑似將資料傳送到美國的 IP 為 162.210.101.140 的 port 80。

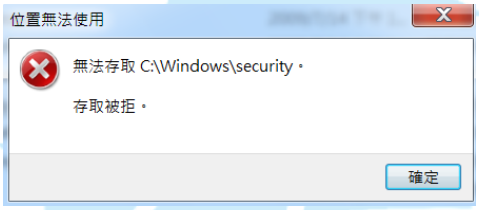


6. 實際測試該 IP 的網站狀態，確實 port 80 的 WEB 服務有啟用，然而並無權限進行存取，研判是程式進行回報監控動作。

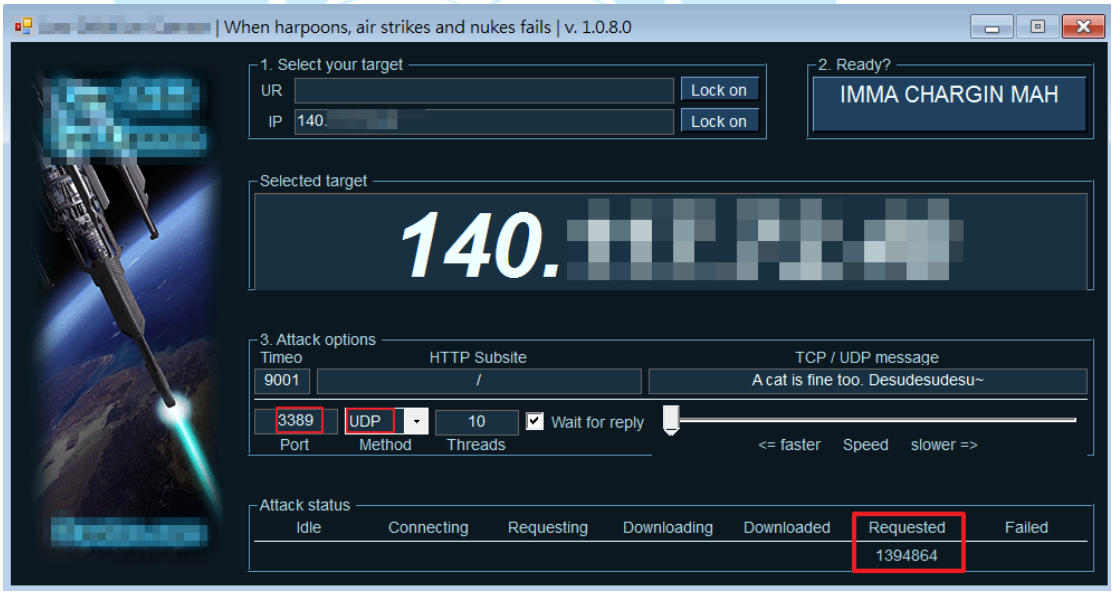
7. 檢查系統的開機啟用狀態，發現有一支惡意程式寫入開機自動啟用。然而進一步檢查 Windows\security\rzsblotiu.exe 卻無法開啟該以藏資料夾，疑似無權限存取。



Autorun Entry	Description	Publisher	Image Path	Timestamp
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2015/8/31 上...
VMware User Process	VMware T...	VMware, Inc.	c:\program files\vmware\vmware tool...	2014/11/21 ...
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				2015/11/2 下...
Browsing Enhancements	Windows ...	Microsoft C...	c:\program files\windows mail\winm...	2009/7/14 上...
DirectDrawEx	Windows ...	Microsoft C...	c:\program files\windows mail\winm...	2009/7/14 上...
Internet Explorer Help	Windows ...	Microsoft C...	c:\program files\windows mail\winm...	2009/7/14 上...
Internet Explorer Setup Tools	Windows ...	Microsoft C...	c:\program files\windows mail\winm...	2009/7/14 上...
Microsoft Windows	Windows ...	Microsoft C...	c:\program files\windows mail\winm...	2009/7/14 上...
Microsoft Windows Script 5.6	Windows ...	Microsoft C...	c:\program files\windows mail\winm...	2009/7/14 上...
HKCU\Software\Microsoft\Windows\CurrentVersion\Run				2015/11/2 下...
svchost.exe			c:\windows\security\rzsbkotiu.exe	2014/1/10 上...

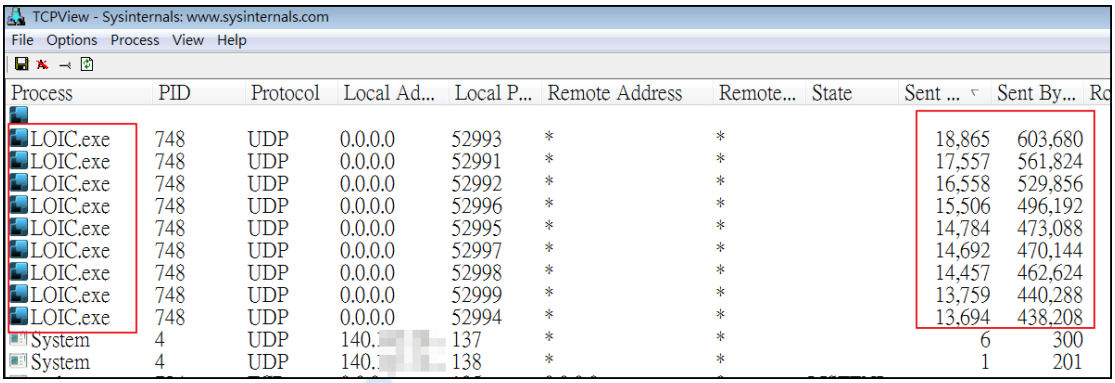


8. 實地開啟 DDoS Attack 軟體，出現的介面中可以輸入被攻擊者的 IP 或 URL，測試一台自己的內部主機 IP，下方可以選擇要攻擊的 port 號以及使用的協定共三種，分別為 TCP、UDP 以及 HTTP 方式。右邊可以選擇發送封包的速度，下方則會顯示目前已經發送的封包數量。



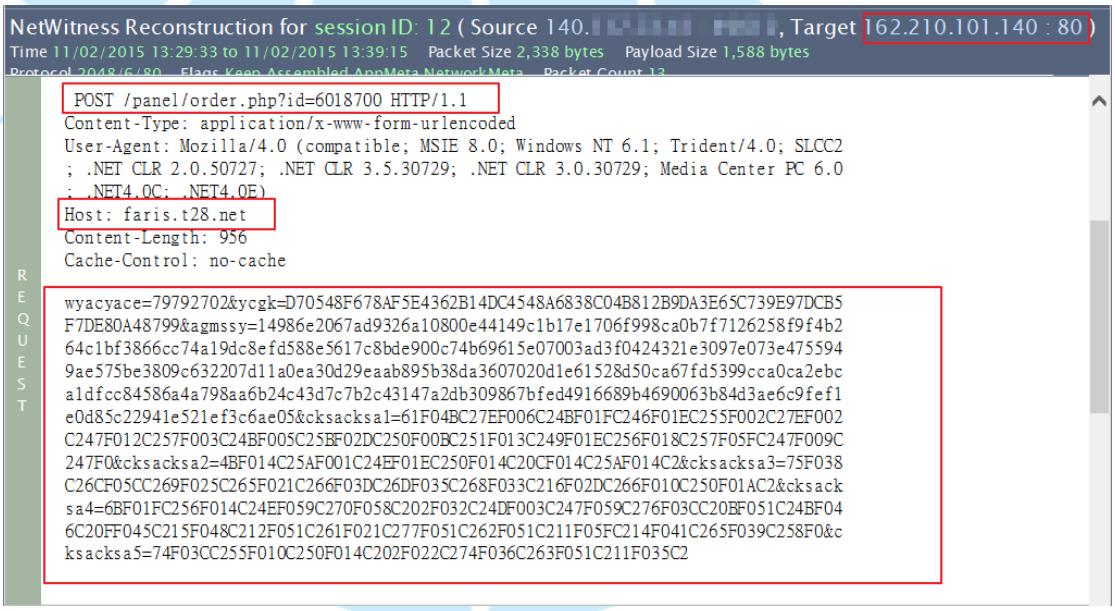
9. 以下為測試發送 UDP 封包至對方的 port 80，透過 TCPview 檢視可以看到本機端的 port 為亂數發送 UDP，卻無法看到目的 IP 地址以及 port 號，

都是以*符號顯示，但可以看到右側的封包流量在急速上升中，表示此攻擊確實在進行中。

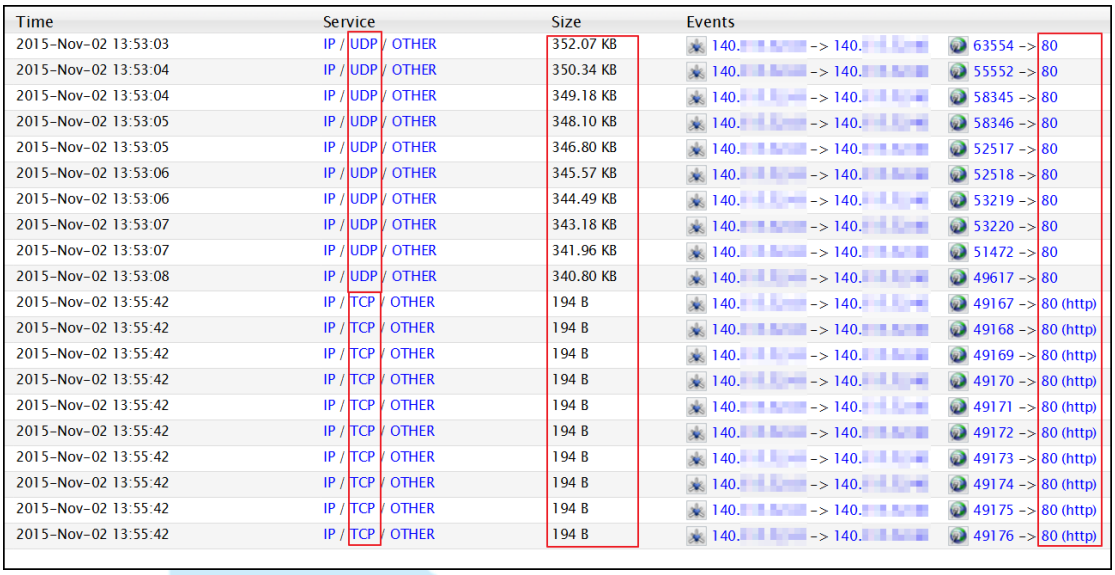


Process	PID	Protocol	Local Ad...	Local P...	Remote Address	Remote...	State	Sent ...	Sent By...	Rc
LOIC.exe	748	UDP	0.0.0.0	52993	*	*		18,865	603,680	
LOIC.exe	748	UDP	0.0.0.0	52991	*	*		17,557	561,824	
LOIC.exe	748	UDP	0.0.0.0	52992	*	*		16,558	529,856	
LOIC.exe	748	UDP	0.0.0.0	52996	*	*		15,506	496,192	
LOIC.exe	748	UDP	0.0.0.0	52995	*	*		14,784	473,088	
LOIC.exe	748	UDP	0.0.0.0	52997	*	*		14,692	470,144	
LOIC.exe	748	UDP	0.0.0.0	52998	*	*		14,457	462,624	
LOIC.exe	748	UDP	0.0.0.0	52999	*	*		13,759	440,288	
LOIC.exe	748	UDP	0.0.0.0	52994	*	*		13,694	438,208	
System	4	UDP	140.	137	*	*		6	300	
System	4	UDP	140.	138	*	*		1	201	

10. 檢查封包資訊，一開始攻擊程式安裝完後，explore.exe 會先向 162.210.101.140 的 port 80 進行資料傳送，透過 HTTP POST 方式傳送編碼過的資料，可能為敏感性的個資帳號或密碼。

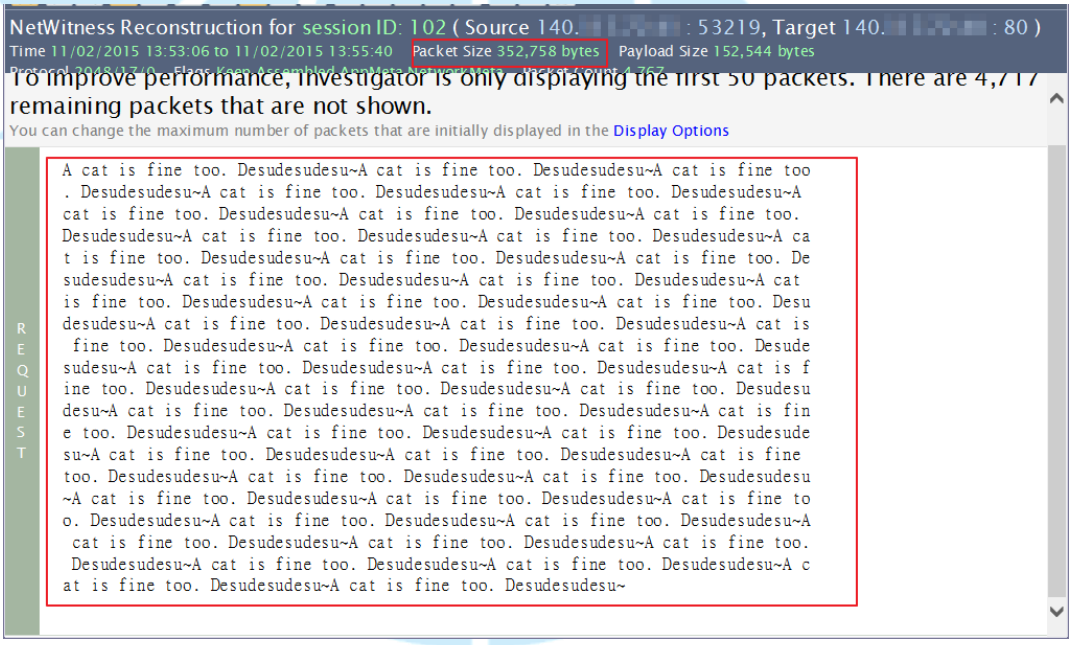


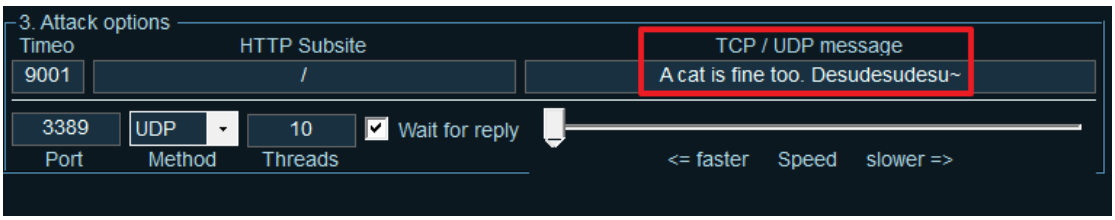
11. 檢查攻擊封包傳送狀態，測試方式有 UDP 和 TCP 的 port 80 攻擊，因為目的主機沒有開啟 TCP port 80 服務，故主要以 UDP 的 port 80 進行 Flood 攻擊。



Time	Service	Size	Events
2015-Nov-02 13:53:03	IP / UDP / OTHER	352.07 KB	140. -> 140. 63554 -> 80
2015-Nov-02 13:53:04	IP / UDP / OTHER	350.34 KB	140. -> 140. 55552 -> 80
2015-Nov-02 13:53:04	IP / UDP / OTHER	349.18 KB	140. -> 140. 58345 -> 80
2015-Nov-02 13:53:05	IP / UDP / OTHER	348.10 KB	140. -> 140. 58346 -> 80
2015-Nov-02 13:53:05	IP / UDP / OTHER	346.80 KB	140. -> 140. 52517 -> 80
2015-Nov-02 13:53:06	IP / UDP / OTHER	345.57 KB	140. -> 140. 52518 -> 80
2015-Nov-02 13:53:06	IP / UDP / OTHER	344.49 KB	140. -> 140. 53219 -> 80
2015-Nov-02 13:53:07	IP / UDP / OTHER	343.18 KB	140. -> 140. 53220 -> 80
2015-Nov-02 13:53:07	IP / UDP / OTHER	341.96 KB	140. -> 140. 51472 -> 80
2015-Nov-02 13:53:08	IP / UDP / OTHER	340.80 KB	140. -> 140. 49617 -> 80
2015-Nov-02 13:55:42	IP / TCP / OTHER	194 B	140. -> 140. 49167 -> 80 (http)
2015-Nov-02 13:55:42	IP / TCP / OTHER	194 B	140. -> 140. 49168 -> 80 (http)
2015-Nov-02 13:55:42	IP / TCP / OTHER	194 B	140. -> 140. 49169 -> 80 (http)
2015-Nov-02 13:55:42	IP / TCP / OTHER	194 B	140. -> 140. 49170 -> 80 (http)
2015-Nov-02 13:55:42	IP / TCP / OTHER	194 B	140. -> 140. 49171 -> 80 (http)
2015-Nov-02 13:55:42	IP / TCP / OTHER	194 B	140. -> 140. 49172 -> 80 (http)
2015-Nov-02 13:55:42	IP / TCP / OTHER	194 B	140. -> 140. 49173 -> 80 (http)
2015-Nov-02 13:55:42	IP / TCP / OTHER	194 B	140. -> 140. 49174 -> 80 (http)
2015-Nov-02 13:55:42	IP / TCP / OTHER	194 B	140. -> 140. 49175 -> 80 (http)
2015-Nov-02 13:55:42	IP / TCP / OTHER	194 B	140. -> 140. 49176 -> 80 (http)

12. 檢查 UDP 的封包內容，確實是以攻擊程式中的 TCP/UDP message 去填塞內容。





13. 透過 Virustotal 線上掃毒， DDoS Attack 的被偵測率有 39/57，雖然該程式主要是為 Hack tool，但同時也是一支木馬程式，一旦使用可能成為駭客的殭屍主機。

SHA256: 8af4e83cec21057d5ac720ada842508237339e30624029dccf768a335051b182

File name: DDoS Attack.exe

Detection ratio: 39 / 57

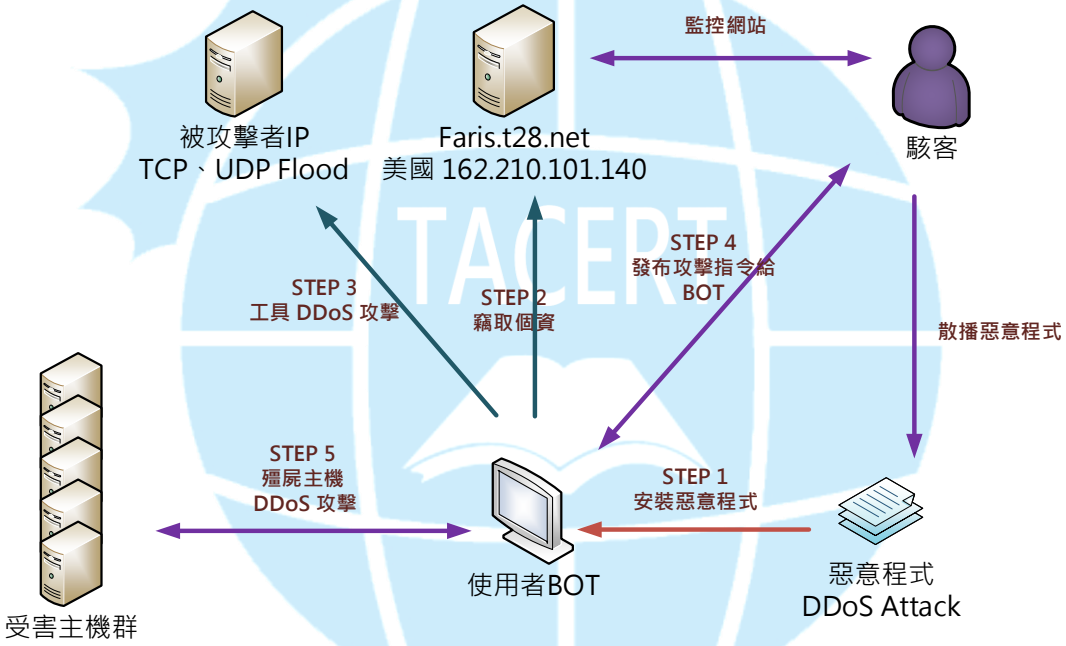
Analysis date: 2015-10-04 05:20:01 UTC (4 weeks, 1 day ago)

3 0

Analysis | File detail | Additional information | Comments 1 | Votes | Behavioural information

Antivirus	Result	Update
AVG	Luhe.MalMSIL.A	20151004
AVware	Trojan.Win32.Generic!BT	20151004
Ad-Aware	Gen:Variant.Application.HackTool.1	20151004

III. 網路架構圖



1. 使用者可能透過地下網站或論壇下載攻擊程式 DDoS Attack。
2. 主機安裝攻擊程式後向「162.210.101.140:80」報到並竊取個資成為殭屍主機。
3. 使用者使用攻擊工具向特定主機進行 UDP 或 TCP 的 Flood 攻擊。
4. 駭客可能透過該木馬程式下達攻擊指令。
5. 殭屍主機收到攻擊指令就會向其他主機進行 DDoS 攻擊。

IV.建議與總結

1. 建議使用者不要下載安裝此類的攻擊軟體，通常都內含木馬程式。
2. 使用者對外部主機進行 DDoS 的 Flood 攻擊是違法行為，因為任何攻擊行為都會留下 IP 紀錄。
3. 成為殭屍電腦後駭客也是可能利用來對外進行攻擊，成為駭客的攻擊跳板。
4. DDoS 攻擊往往透過合法的網路通訊埠進行大流量封包阻斷其他正常服務，其維持時間通常不會很久，並且此種攻擊很難防範，但是一旦發生時候服務中斷可能造成相當大的損失。