個案分析-

常見的 Ramnit 殭屍網路病毒事件分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

2016/11

I. 事件簡介

1. 殭屍網路主機一直是駭客最有利的攻擊利器，因為駭客組織透過這些殭屍們，就能對特定網路造成大量的 DDoS 攻擊，造成許多網路服務被迫中斷。
2. Ramnit 蠕蟲病毒在今年初中華電信公布的台灣資安威脅排名中位居第一，讓許多主機淪陷成為肉雞而不自知。
3. 本單位取得其中一個 Ramnit 的病毒樣本進行測試，並透過其網路行為進行分析。

II. 事件檢測

1. 使用 VM 虛擬主機並且為 Windows 7 (X64)系統進行隔離環境測試，惡意程式樣本名稱為 「ramnit_unpacked」的執行檔。
2. 該惡意程式的圖案以 Windows Media Player 作為 Logo 顯示，企圖混淆使用者認知。

3. 測試前先透過 Virustotal 掃描，比例為 42/56 的木馬或 ramnit 的惡意程式。

SHA256: a5c15445c74be819d4c3bd67fbc91f8f2b825a484096cedc88cd8077a90539c1

File name: a5c15445c74be819d4c3bd67fbc91f8f2b825a484096cedc88cd8077a90539c1.bin

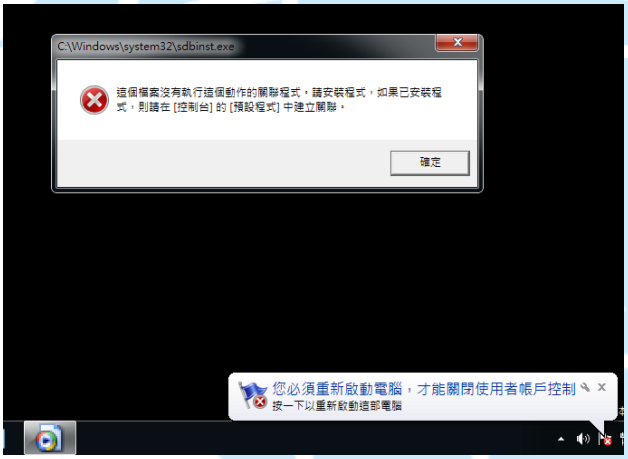
Detection ratio: 42 / 56

Analysis date: 2016-05-26 19:32:04 UTC (5 months, 1 week ago)

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

Antivirus	Result	Update
AVG	Generic_r.IIU	20160526
AVware	Trojan.Win32.Generic.pak!cobra	20160526
Ad-Aware	Gen:Trojan.Heur.oqY@yrzyixgii	20160526
AegisLab	Troj.W32.Lebag!c	20160526
AhnLab-V3	Malware/Win32.Generic	20160526
Antiy-AVL	Trojan/Win32.SGeneric	20160526

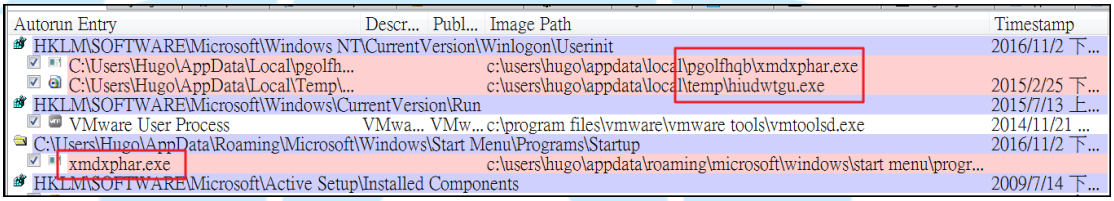
4. 在實際測試執行後，該惡意程式為了感染系統內部的檔案及取得一些控制權限，會強制將主機系統重新開機。



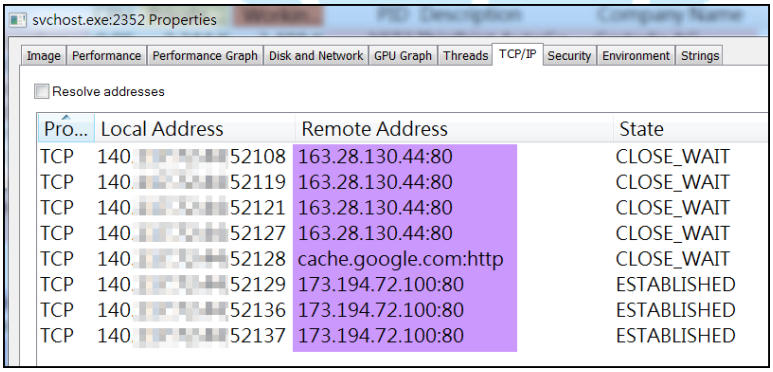
5. 檢查使用者帳戶控制設定的等級後發現，安全性等級已經被調整至最低等級。

6. 因為確保重開機後惡意程式還會繼續作用，故一定會有自動開機啟用的寫入，透過 autoruns 檢查的確有多出幾項未知的註冊機碼。

7. ramnit_unpacked.exe 會分別在系統暫存的隱藏資料夾中建立 xmdxphar.exe 和 hiudwtgu.exe，而該兩支檔案 virustotal 查看都是 ramnit_unpacked.exe 的複本。

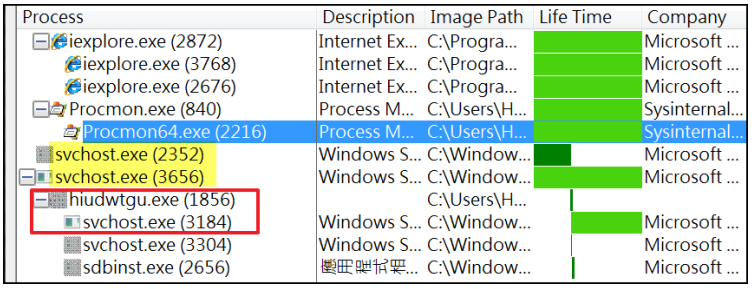


8. 接著在背景程式中會多出兩支異常的 svchost.exe 在執行，事實上原本的惡意程式將系統 \system32 底下的 svchost.exe 進行感染病操控，並且有大量對外的網路行為產生。

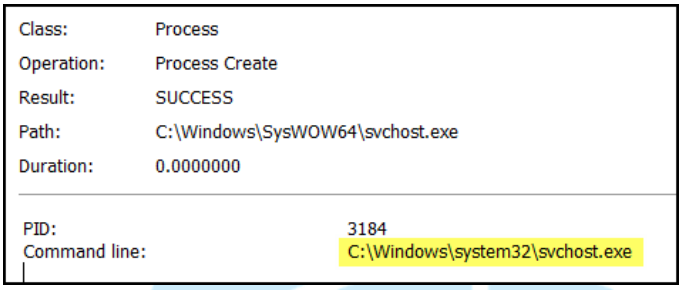


9. 經過測試將該 svchost.exe 程序 kill 之後，很快就又建立一個新的 svchost.exe 程序，因此觀察到 ~\temp\hiudwtgu.exe (1856)這支程式

專門去執行 svchost.exe 的惡意程序(3184)。



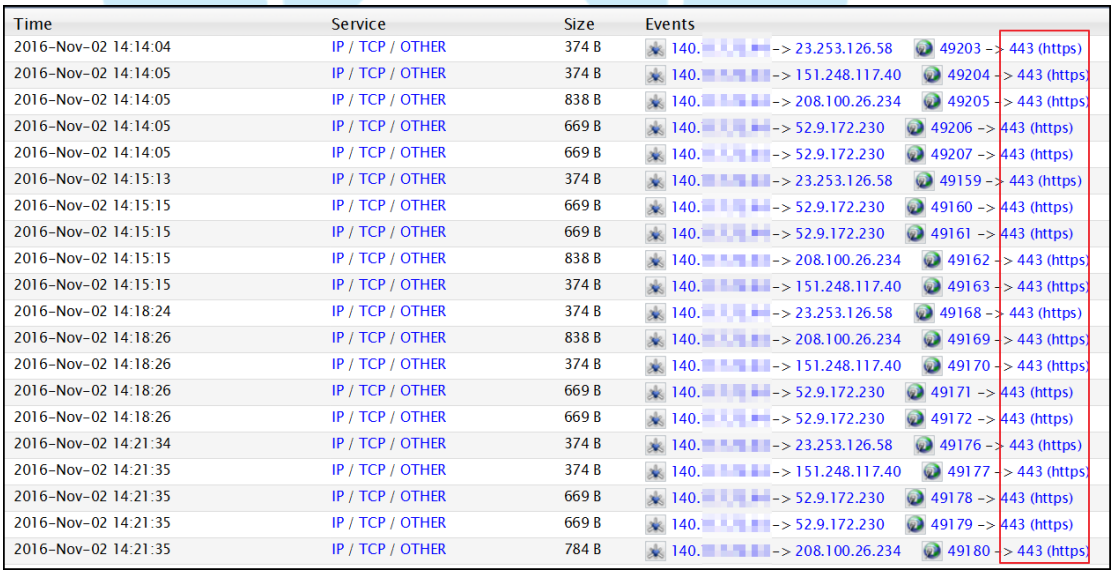
Process	Description	Image Path	Life Time	Company
iexplore.exe (2872)	Internet Ex...	C:\Progra...		Microsoft ...
iexplore.exe (3768)	Internet Ex...	C:\Progra...		Microsoft ...
iexplore.exe (2676)	Internet Ex...	C:\Progra...		Microsoft ...
Procmon.exe (840)	Process M...	C:\Users\H...		Sysinternal...
Procmon64.exe (2216)	Process M...	C:\Users\H...		Sysinternal...
svchost.exe (2352)	Windows S...	C:\Window...		Microsoft ...
svchost.exe (3656)	Windows S...	C:\Window...		Microsoft ...
hiudwtgu.exe (1856)		C:\Users\H...		
svchost.exe (3184)	Windows S...	C:\Window...		Microsoft ...
svchost.exe (3304)	Windows S...	C:\Window...		Microsoft ...
sdbinst.exe (2656)	[illegible]	C:\Window...		Microsoft ...



Class:	Process
Operation:	Process Create
Result:	SUCCESS
Path:	C:\Windows\SysWOW64\svchost.exe
Duration:	0.0000000
PID:	3184
Command line:	C:\Windows\system32\svchost.exe

10. 因此若要手動排除感染檔案，不能移除系統內建的 svchost.exe，而是要針對 xmdxphar.exe 和 hiudwtgu.exe 的惡意程式主體進行移除，才能防止再啟動惡意程序。

11. 檢查 svchost.exe 產生的網路行為都是連到外部主機的 port 80 和 443，其中 port 443 的主機經過測試大多已經沒回應。初步判定惡意程式的行為目的應該是產生大量的 HTTP(S)連線降低網站服務效能。



Time	Service	Size	Events
2016-Nov-02 14:14:04	IP / TCP / OTHER	374 B	140.[redacted] -> 23.253.126.58 49203 -> 443 (https)
2016-Nov-02 14:14:05	IP / TCP / OTHER	374 B	140.[redacted] -> 151.248.117.40 49204 -> 443 (https)
2016-Nov-02 14:14:05	IP / TCP / OTHER	838 B	140.[redacted] -> 208.100.26.234 49205 -> 443 (https)
2016-Nov-02 14:14:05	IP / TCP / OTHER	669 B	140.[redacted] -> 52.9.172.230 49206 -> 443 (https)
2016-Nov-02 14:14:05	IP / TCP / OTHER	669 B	140.[redacted] -> 52.9.172.230 49207 -> 443 (https)
2016-Nov-02 14:15:13	IP / TCP / OTHER	374 B	140.[redacted] -> 23.253.126.58 49159 -> 443 (https)
2016-Nov-02 14:15:15	IP / TCP / OTHER	669 B	140.[redacted] -> 52.9.172.230 49160 -> 443 (https)
2016-Nov-02 14:15:15	IP / TCP / OTHER	669 B	140.[redacted] -> 52.9.172.230 49161 -> 443 (https)
2016-Nov-02 14:15:15	IP / TCP / OTHER	838 B	140.[redacted] -> 208.100.26.234 49162 -> 443 (https)
2016-Nov-02 14:15:15	IP / TCP / OTHER	374 B	140.[redacted] -> 151.248.117.40 49163 -> 443 (https)
2016-Nov-02 14:18:24	IP / TCP / OTHER	374 B	140.[redacted] -> 23.253.126.58 49168 -> 443 (https)
2016-Nov-02 14:18:26	IP / TCP / OTHER	838 B	140.[redacted] -> 208.100.26.234 49169 -> 443 (https)
2016-Nov-02 14:18:26	IP / TCP / OTHER	374 B	140.[redacted] -> 151.248.117.40 49170 -> 443 (https)
2016-Nov-02 14:18:26	IP / TCP / OTHER	669 B	140.[redacted] -> 52.9.172.230 49171 -> 443 (https)
2016-Nov-02 14:18:26	IP / TCP / OTHER	669 B	140.[redacted] -> 52.9.172.230 49172 -> 443 (https)
2016-Nov-02 14:21:34	IP / TCP / OTHER	374 B	140.[redacted] -> 23.253.126.58 49176 -> 443 (https)
2016-Nov-02 14:21:35	IP / TCP / OTHER	374 B	140.[redacted] -> 151.248.117.40 49177 -> 443 (https)
2016-Nov-02 14:21:35	IP / TCP / OTHER	669 B	140.[redacted] -> 52.9.172.230 49178 -> 443 (https)
2016-Nov-02 14:21:35	IP / TCP / OTHER	669 B	140.[redacted] -> 52.9.172.230 49179 -> 443 (https)
2016-Nov-02 14:21:35	IP / TCP / OTHER	784 B	140.[redacted] -> 208.100.26.234 49180 -> 443 (https)

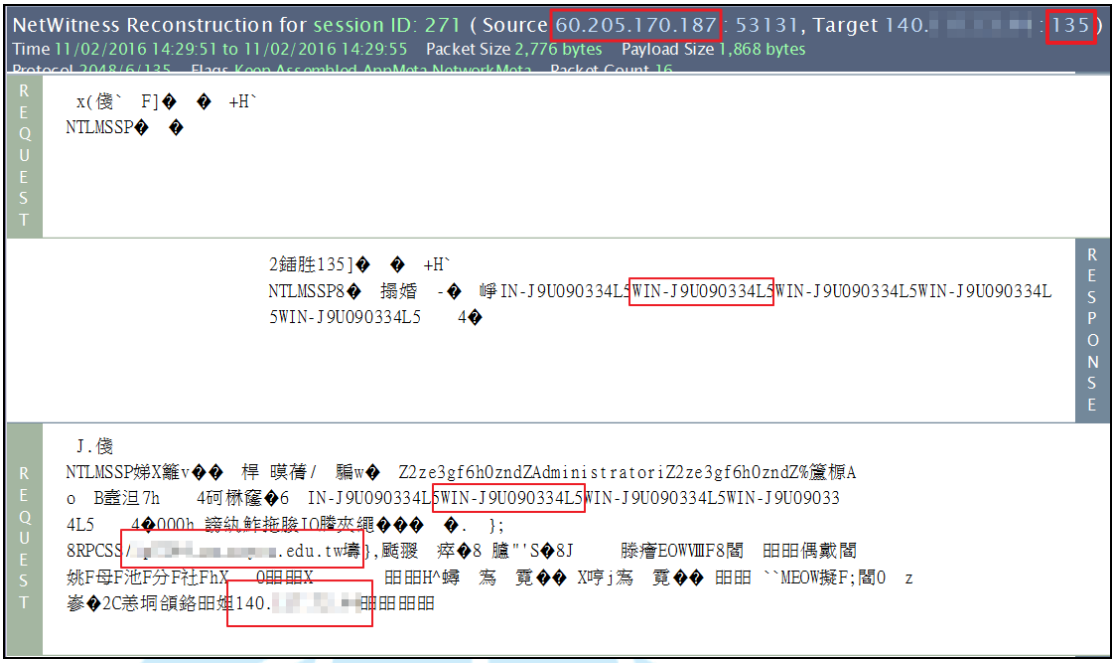
12. 另外連到 port 80 的主機大多是 google 的 cache 伺服器，包含了學術網路內的快取伺服器，並且都是發送 300 Bytes 左右的無內容封包。

Time	Service	Size	Events
2016-Nov-02 14:13:36	IP / TCP / OTHER	480 B	140 -> 163.28.130.42 49160 -> 80 (http)
2016-Nov-02 14:14:02	IP / TCP / OTHER	300 B	140 -> 216.58.199.14 49202 -> 80 (http)
2016-Nov-02 14:15:06	IP / TCP / HTTP	990 B	140 -> 163.28.5.10 49157 -> 80 (http)
2016-Nov-02 14:15:12	IP / TCP / OTHER	300 B	140 -> 163.28.130.38 49158 -> 80 (http)
2016-Nov-02 14:16:23	IP / TCP / OTHER	300 B	140 -> 163.28.130.38 49166 -> 80 (http)
2016-Nov-02 14:17:34	IP / TCP / OTHER	300 B	140 -> 163.28.130.38 49167 -> 80 (http)
2016-Nov-02 14:18:45	IP / TCP / OTHER	300 B	140 -> 163.28.130.38 49173 -> 80 (http)
2016-Nov-02 14:19:56	IP / TCP / OTHER	300 B	140 -> 163.28.130.38 49174 -> 80 (http)
2016-Nov-02 14:21:08	IP / TCP / OTHER	300 B	140 -> 163.28.130.59 49175 -> 80 (http)
2016-Nov-02 14:22:19	IP / TCP / OTHER	300 B	140 -> 163.28.130.59 49181 -> 80 (http)
2016-Nov-02 14:23:30	IP / TCP / OTHER	300 B	140 -> 163.28.130.59 49182 -> 80 (http)
2016-Nov-02 14:24:11	IP / TCP / OTHER	114 B	148 -> 140.117.72.44 7097 -> 80 (http)
2016-Nov-02 14:24:41	IP / TCP / OTHER	300 B	140 -> 163.28.130.59 49183 -> 80 (http)
2016-Nov-02 14:25:52	IP / TCP / OTHER	300 B	140 -> 163.28.130.59 49189 -> 80 (http)
2016-Nov-02 14:27:03	IP / TCP / OTHER	300 B	140 -> 163.28.130.44 49190 -> 80 (http)
2016-Nov-02 14:28:14	IP / TCP / OTHER	300 B	140 -> 163.28.130.44 49196 -> 80 (http)
2016-Nov-02 14:28:45	IP / TCP / OTHER	114 B	140 -> 141.138.130.12 14079 -> 80 (http)
2016-Nov-02 14:29:25	IP / TCP / OTHER	300 B	140 -> 163.28.130.44 49197 -> 80 (http)
2016-Nov-02 14:30:36	IP / TCP / OTHER	300 B	140 -> 163.28.130.44 49198 -> 80 (http)
2016-Nov-02 14:31:47	IP / TCP / OTHER	300 B	140 -> 163.28.130.44 49203 -> 80 (http)

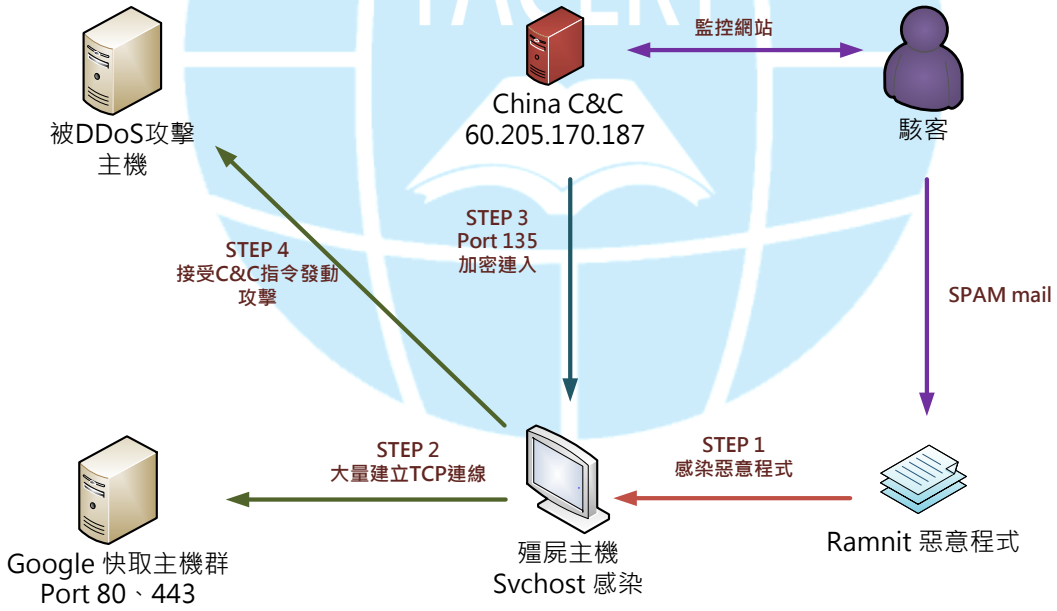
13. 一般主機成為殭屍電腦後應該都會留有一個 port 來接收 C&C 指令，然而在測試過程中尚未明顯的大量流量。不過在此正常的系統開啟的 port 中，有記錄到疑似 C&C 連入的封包。

Process	PID	Protocol	Local A...	Loca...	Remote...	Remote...	State
svchost.exe	676	TCP	0.0.0.0	135	0.0.0.0	0	LISTENING
svchost.exe	676	TCPV6	[0:0:0:0:...	135	[0:0:0:0:...	0	LISTENING

14. 從此封包紀錄得知，確實有外部 IP 中國 60.205.170.187 連入到感染主機的 port 135，而該 port 是由系統的 svchost.exe 控制，故若惡意程式能控制 svchost.exe 也是有可能被用接收指令。封包內容包含了一些加密字串以及主機名稱和 IP 資訊。



III. 網路架構圖



1. 使用者可能透過 SPAM 郵件開啟含有惡意程式 ramnit 的檔案。
2. 主機感染惡意程式後不斷地向 google 快取伺服器建立連線。
3. 疑似中國 C&C 透過系統 port 135 漏洞連入主機下達指令。
4. 必要時候駭客透過 C&C 下達攻擊指令對外部主機進行 DDoS 攻擊。

IV.建議與總結

1. 使用者可能透過被 SPAM 或 APT 攻擊執行到惡意程式而遭受感染成為 ramnit 殭屍主機。
2. 此惡意程式會感染系統的檔案 svchost.exe 並透過他進行網路連線。
3. 駭客能透過系統 svchost 預設開啟的 port 135 下達 C&C 指令，不容易被發現。
4. 雖然嘗試將有有問題的 svchost 程序關閉，依然會被惡意程式恢復執行，但是卻不能刪除系統檔案 svchost。
5. 惡意程式會寫入開機自動啟用，故透過啟用路徑刪除真正的檔案 xmdxphar.exe 和 hiudwtgu.exe 後，在關閉問題程序 svchost 就能排除問題。
6. 此類病毒會控制使用者權限並感染系統程式，不容易從程式管理工具中發現移除。
7. 此 Ramnit 相關連結如下:
   1. 中華電信揭露臺灣 20 大惡意程式：Ramnit 蠕蟲最兇單日攻擊 3 萬件 http://www.ithome.com.tw/news/104775
   2. Ramnit 殭屍網絡在香港的偵測及清理 https://www.hkcert.org/my_url/zh/blog/15062601

V. 國外報導

1. **Ramnit Rears Its Ugly Head Again, Targets Major UK Banks**
   a. IBM X-Force 的研究人員最近報告說，Ramnit 木馬已經重新啟動，針對英國的六大銀行。
   b. 大約八個月沉默期後，研究人員觀察到 Ramnit 的開發者成立了兩個新的活躍的攻擊服務器和一個新的命令與控制（C&C）服務器。
   c. 他們在英國開發新的木馬配置方式並且蔓延，透過網站置入去感染以獲得使用者銀行帳戶資料。
   d. https://securityintelligence.com/ramnit-rears-its-ugly-he

ad-again-targets-major-uk-banks/

2. **Ramnit Malware Back and Better at Avoiding Detection**
   a. The Ramnit malware family has been given a facelift with new anti-detection capabilities, a troubleshooting module, as well as enhanced encryption and malicious payloads.
   b. Ramnit was detected in 2010 and has been proficient in stealing credentials, focusing primarily on online bank accounts, FTP log-ins and even Facebook passwords.
   c. https://wp.me/p3AjUX-kc8