個案分析-

K 單位對外發送 SYN Flood 攻擊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

2015/4

I. 事件簡介

1. 該學術單位資安人員發現有一台主機占用大量頻寬，疑似遭受病毒感染，請本單位進行協助鑑識排除。
2. 該主機為一台 VM 虛擬主機，使用作業系統為 Linux 的 Centos 版本。
3. 該主機主要有網頁服務供學生能夠登入使用，且有啟用 SSH Server 的服務供管理者可以登入管理。
4. 該單位資安人員提供此主機的 VM 映像檔給本單位進行調查鑑識。

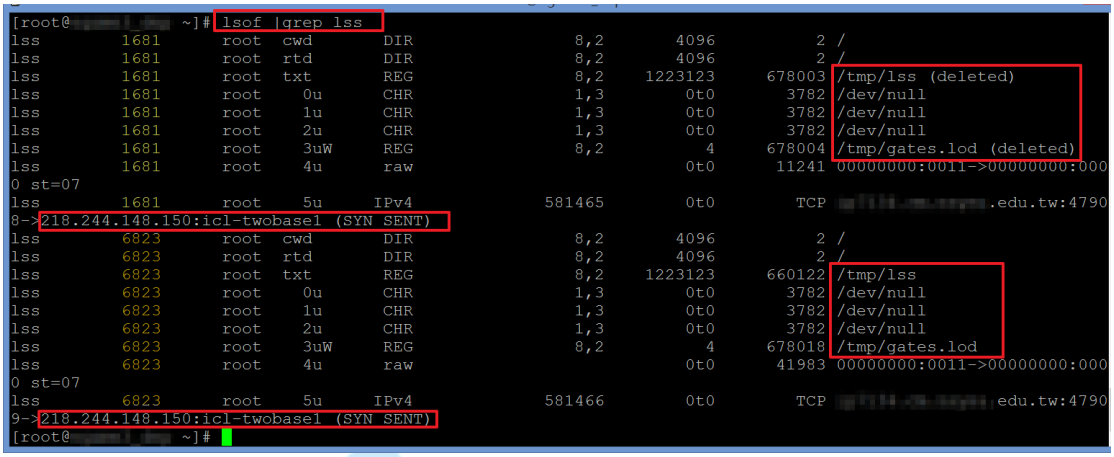
II. 事件檢測

1. 首先透過 SSH 連入該主機，並使用指令 netstat 觀察網路通訊埠的連線狀態，得知除了預設的 port 80、22 之外，尚有其他可疑連線正在活動。
2. 檢查 Web service 的 access log，並無發現異常的連入狀態，排除掉可能的 phpmyadmin 和 shellshock 網站漏洞。
3. 從圖中紅框標示知道，有一支名為 lss 的程式正在與 218.244.148.150 的 port 25000 進行 SYN_SENT 的資料傳送，而該主機是位於中國北京，可能是作為報到中繼站用途。

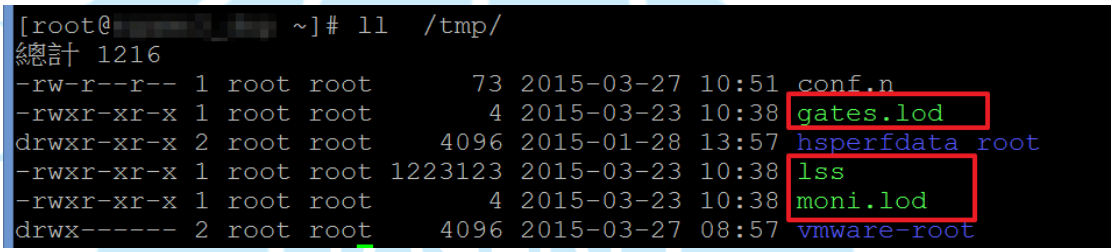
```
[root@ ~]# netstat -anpt
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             State       PID/Program name
tcp        0      0 0.0.0.0:111                 0.0.0.0:*                   LISTEN      1274/rpcbind
tcp        0      0 0.0.0.0:22                  0.0.0.0:*                   LISTEN      1476/sshd
tcp        0      0 127.0.0.1:631               0.0.0.0:*                   LISTEN      1357/cupsd
tcp        0      0 0.0.0.0:49271               0.0.0.0:*                   LISTEN      1292/rpc.statd
tcp        0      0 127.0.0.1:25                0.0.0.0:*                   LISTEN      1560/master
tcp        0     52 140.          :22           140.          :10575        ESTABLISHED 18642/sshd
tcp        0      1 140.          :47846        218.244.148.150:25000       SYN_SENT    1681/lss
tcp        0      1 140.          :47847        218.244.148.150:25000       SYN_SENT    6823/lss
tcp        0      0 :::111                      :::*                        LISTEN      1274/rpcbind
tcp        0      0 :::8080                     :::*                        LISTEN      1642/httpd
tcp        0      0 :::80                       :::*                        LISTEN      1589/java
tcp        0      0 :::53201                    :::*                        LISTEN      1292/rpc.statd
tcp        0      0 :::22                       :::*                        LISTEN      1476/sshd
tcp        0      0 ::1:631                     :::*                        LISTEN      1357/cupsd
tcp        0      0 ::1:25                      :::*                        LISTEN      1560/master
tcp        0      0 ::ffff:127.0.0.1:8005       :::*                        LISTEN      1589/java
tcp        0      0 :::8009                     :::*                        LISTEN      1589/java
tcp        0      0 :::873                      :::*                        LISTEN      1484/xinetd
```

4. 接著透過指令 lsof 觀察該程式 lss 的運行狀況，可以得知 lss 位於路徑 /tmp/ 中，並啟用兩個 PID 為 1681 和 6823 的程序，皆是向中繼站 218.244.148.150 進行 SYN SENT 動作。此時也發現到另一支惡意程式

/tmp/gates.lod 也參與其中。

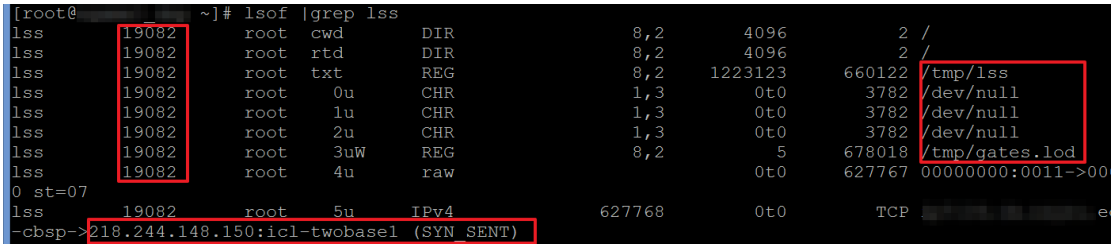


5. 透過線索檢查 /tmp/ 中發現到其他可疑檔案 gates.lod 和 moni.lod，該兩個檔案也是執行檔，系統中會以綠色顯示。

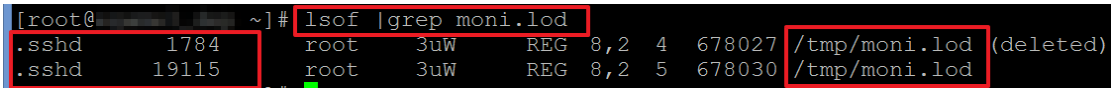


6. 嘗試手動將背景程式 lss 進行 kill，發現就算移除後一段時間還是會再次產生新的 lss 程序。故再次進行程序 kill，並且手動將檔案 lss 進行刪除，經過短暫時間該程式 lss 又再次復活執行。最後嘗試將三個檔案都進行刪除，經過短暫時間該三個檔案又再次還原並執行，此時便能確定應還有其他程式在監控主導還原，故此 /tmp/ 下的惡意程式並非源頭。

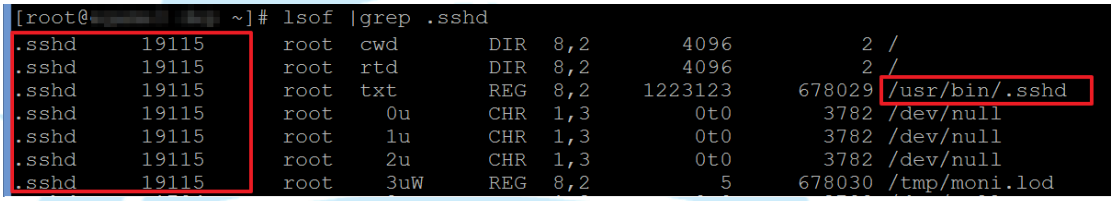
7. 此圖可以看到 lss 還原後會再次執行，且 PID 從原本的 6823 變為 19082。



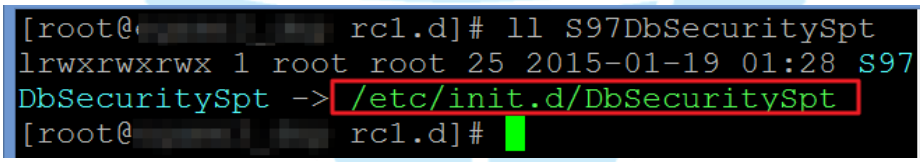
8. 為了找出源頭的惡意程式，透過指令 lsof 觀察惡意程式 moni.lod 的行為，發現到該程式的父程式名為 .sshd 的隱藏檔，其 PID 為 19115。

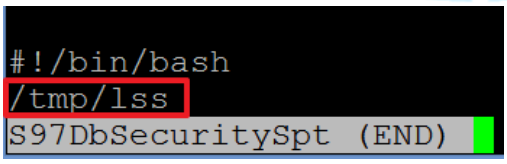


9. 再次透過指令 lsof 查詢程式 .sshd 的行為，能看到它的存在路徑為 /usr/bin/.sshd ，因為它是隱藏檔故不易從 ls 指令看出。



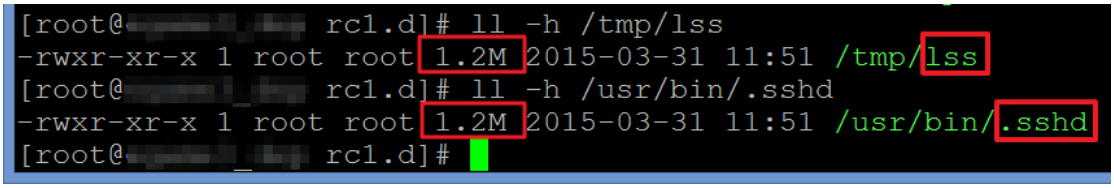
10. 因為該惡意程式會在開機時候自動啟動，表示說該惡意程式一定有執行可開機啟用的腳本中。分別追查 .sshd 及 lss 這兩支執行檔的啟用情形後，發現只有 /tmp/lss 被寫入 etc/rc[1-5].d/S97DbSecuritySpt，對應到的實體路徑為 /etc/init.d/DbSecuritySpt。



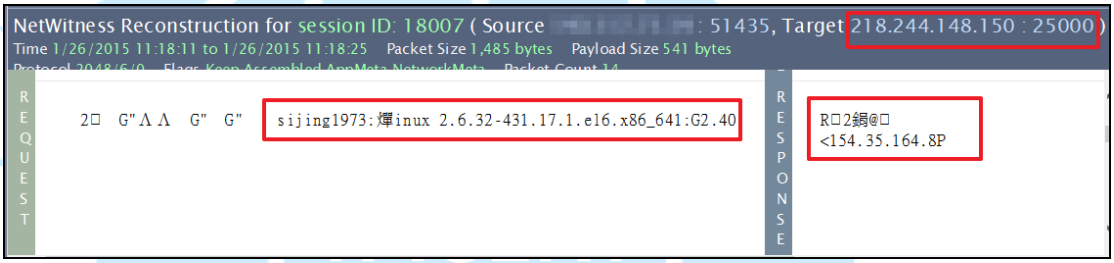


11. 由啟動的腳本得知，lss 應該才是惡意程式的主體，而 .sshd 則是 lss 執行後產生出的 watchdog 監控程式，用來還原 lss 、moni.lod 和 gates.lod 惡意程式。故以上 lss 和.sshd 惡意程式必須都刪除掉才能阻止再次還原。

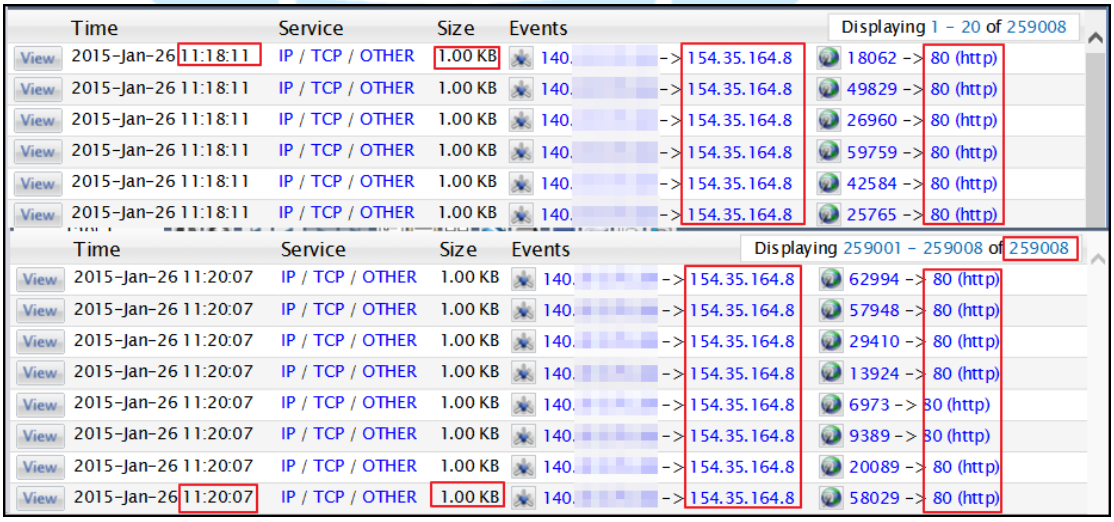
12. 仔細比較 lss 和.sshd 的差異，這兩支檔案都是執行檔，且檔案大小都是 1.2M 的大小，且.sshd 可以在無網路環境下還原被刪除的 lss 檔案，故 lss 和.sshd 實質上為同一支程式。



13. 觀察惡意程式產生的網路流量封包得知，該惡意程式 lss 一開始會向中國北京上層主機 218.244.148.150 的 port 25000 進行 SYN_SENT 的資料傳送。可以看到封包中帶有感染主機的 linux 版本資訊，且上層中繼站會回傳 IP 資訊 154.35.164.8，此 IP 為被感染主機攻擊的目標。



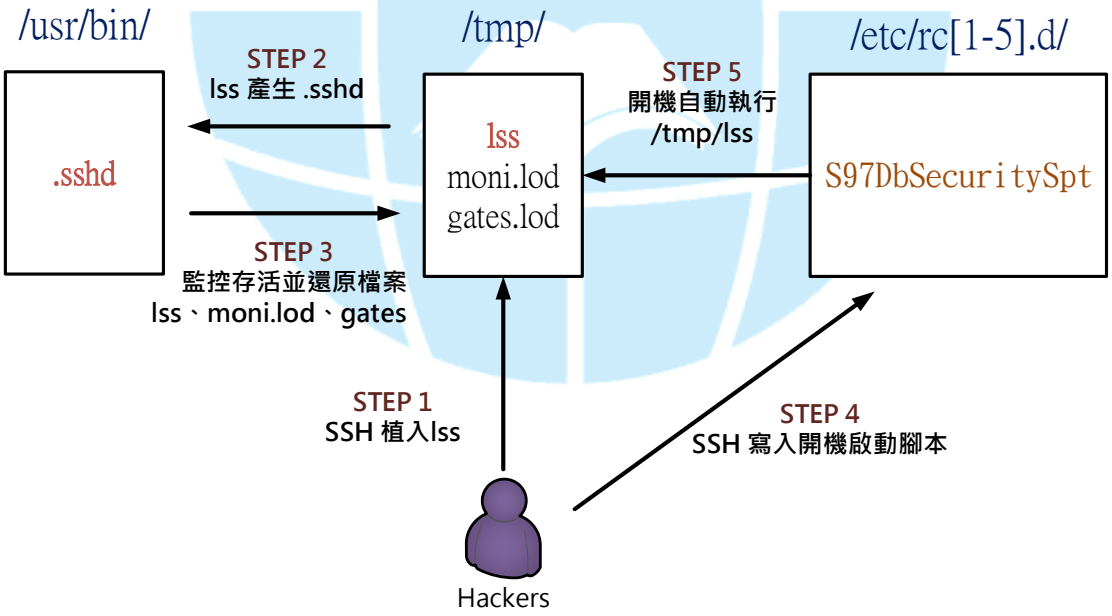
14. 從封包紀錄來看感染主機在短短 2 分鐘內就向 154.35.164.8 的 port 80 發送了 259,008 個 1KB 的 TCP SYN 封包，大約是 17.27Mbps，也就是 SYN Flood 攻擊阻斷 Web 服務。



15. 瀏覽被攻擊的主機 IP，是一個位在美國的“博訊新聞”網站，引述維基百科說明，『博訊新聞網，是一個中文資訊網，基於公民記者模式運

作。主要報道國際時事新聞，以及來自中國大陸的消息。但不時有分析人士認為博訊與中共高層有非常複雜的關係。』

III. 惡意程式運作流程圖

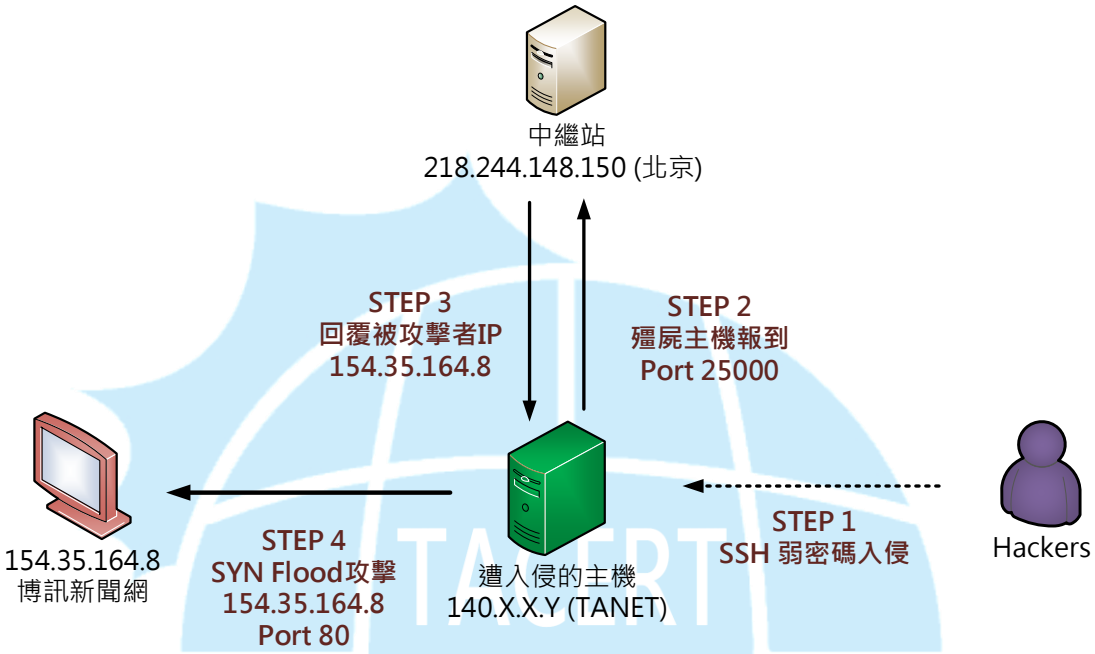


1. 駭客透過 SSH 植入惡意程式至 /tmp/lss 。
2. 執行 lss 後產生出看門狗程式 .sshd 和 moni.lod 及 gates.lod。
3. 看門狗程式 .sshd 持續監控/tmp/中的三支程式是否存活並能夠還原。

4. 駭客寫入開機自動執行惡意程式/tmp/lss 的腳本 S97DbSecuritySpt。

5. 就算主機重開機也能夠自動執行惡意程式 lss。

IV.網路架構圖



1. 駭客透過 SSH 方式弱密碼入侵受害主機並植入惡意程式。
2. 惡意程式開機執行後持續向上層中繼站 218.244.148.150 進行報到動作。
3. 中繼站收到報到的主機資訊後會回覆將被攻擊者的主機 IP。
4. 遭入侵的主機收到將被攻擊者主機 IP 後，開始向 154.35.164.8 的 port 80 進行 SYN Flood 攻擊，以阻斷該主機 Web 服務。

V. 建議與總結

1. 此次受害主機遭受駭客透過 SSH 弱密碼方式入侵並植入惡意程式 .sshd。
2. 在背景進行網路通訊的惡意程式偽裝成 lss 的檔案名稱。
3. 植入的惡意程式具有 watchdog 的功能，也就是 .sshd 會持續監控

lss、moni.lod 和 gates.lod 的存活，一旦這三個惡意程式被移除都能夠透過 .sshd 還原。

4. 駭客在 /etc/rc[1-5].d/ 寫入開機啟動的腳本 S97DbSecuritySpt，會自動執行 /tmp/lss 惡意程式。
5. 雖然 .sshd 能夠還原其他惡意程式，反之 lss 也能還原被刪除的 .sshd 惡意程式。故要同時刪除 .sshd 和 lss 才能徹底移除病毒。
6. 感染的主機持續會接收上層中繼站命令去 SYN Flood 攻擊特定 IP 主機。
7. 建議將主機的 root 密碼強度增強，並限制 SSH 來源端網段連線限制，確保不會遭受駭客破解入侵。
8. 時常檢查是否有大量異常網路流量，或檢查服務的網路連線狀態是否異常，確保無遭受惡意程式感染。