個案分析-

Cridex C&C 分析報告

TACERT 臺灣學術網路危機處理中心團隊製

2013/04

事件說明

TWCERT 接到國外舉報，TANET 主機成為 Cridex C&C 主機。Cridex 是一個專取金融資料的特洛伊惡意程式，國外資安單位表示他們有許多 Cridex 的樣本，其上層都是連往某個 TANET 主機：163.xx.107.65。

163.xx.107.65 是 C 國小的官網主機，底層作業系統為 CentOS，主機除了網頁伺服器，也提供 FTP（使用 ProFTPD 套件）讓老師上傳分享資料，FTP 的帳號密碼只有一組，全校通用。國外提供的檢舉資料顯示（圖 1），Cridex 的許多 bots 樣本與 163.xx.107.65 的 8080 port 有往來連線。

追蹤 163.xx.107.65 主機的連線狀態也顯示其 8080 port 的確有多個來自不同國家的 IP 與之連線（圖 2），163.xx.107.65 主機上層則僅有 x.61.36.44。另外從圖 2 也可以看到，惡意的網路活動 PID 為 26812 程式名稱為 ld-linux.so.2。

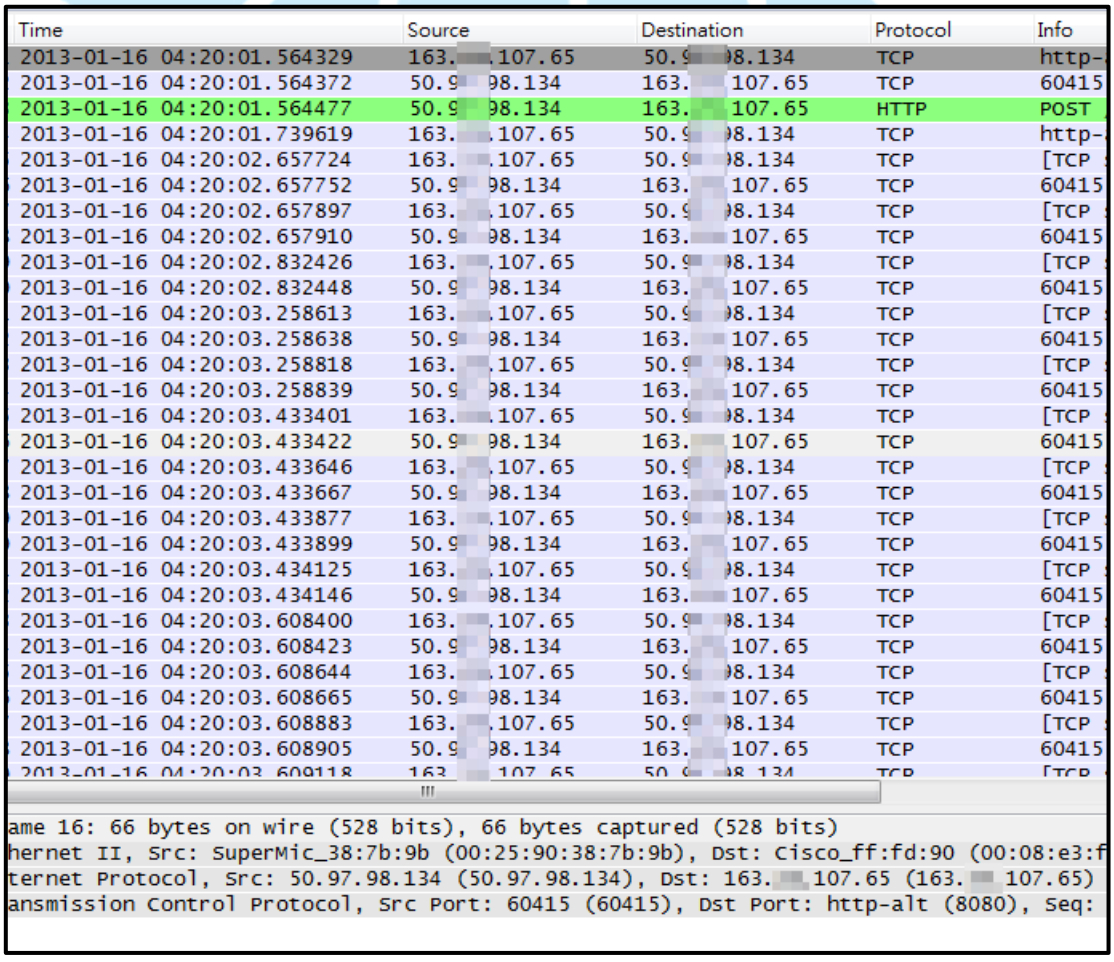


圖 1 國外單位檢附的佐證資料

```
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             State       PID/Program name
tcp        0      0 163.xx.107.65:8080          175.139.228.2:51268         SYN_RECV    -
tcp        0      0 163.xx.107.65:8080          68.186.64.31:55296          SYN_RECV    -
tcp        0      0 163.xx.107.65:8080          174.63.39.29:1063           ESTABLISHED 26812/ld-linux.so.2
tcp        0      0 163.xx.107.65:35847         163.xx.107.125:1969         TIME_WAIT   -
tcp        0      0 163.xx.107.65:8080          207.119.116.5:50213         ESTABLISHED 26812/ld-linux.so.2
tcp        0      0 163.xx.107.65:8080          113.28.165.209:56142        ESTABLISHED 26812/ld-linux.so.2
tcp        0      1 163.xx.107.65:40639         xx.61.36.44:8080            SYN_SENT    26812/ld-linux.so.2
tcp        0      1 163.xx.107.65:40638         xx.61.36.44:8080            SYN_SENT    26812/ld-linux.so.2
tcp        0      1 163.xx.107.65:40637         xx.61.36.44:8080            SYN_SENT    26812/ld-linux.so.2
tcp        0      1 163.xx.107.65:40636         xx.61.36.44:8080            SYN_SENT    26812/ld-linux.so.2
tcp        0      1 163.xx.107.65:40635         xx.61.36.44:8080            SYN_SENT    26812/ld-linux.so.2
tcp        0      1 163.xx.107.65:40634         xx.61.36.44:8080            SYN_SENT    26812/ld-linux.so.2
tcp        0      1 163.xx.107.65:40633         xx.61.36.44:8080            SYN_SENT    26812/ld-linux.so.2
tcp        0      1 163.xx.107.65:40632         xx.61.36.44:8080            SYN_SENT    26812/ld-linux.so.2
```

圖 2 163.xx.107.65 主機的網路狀態

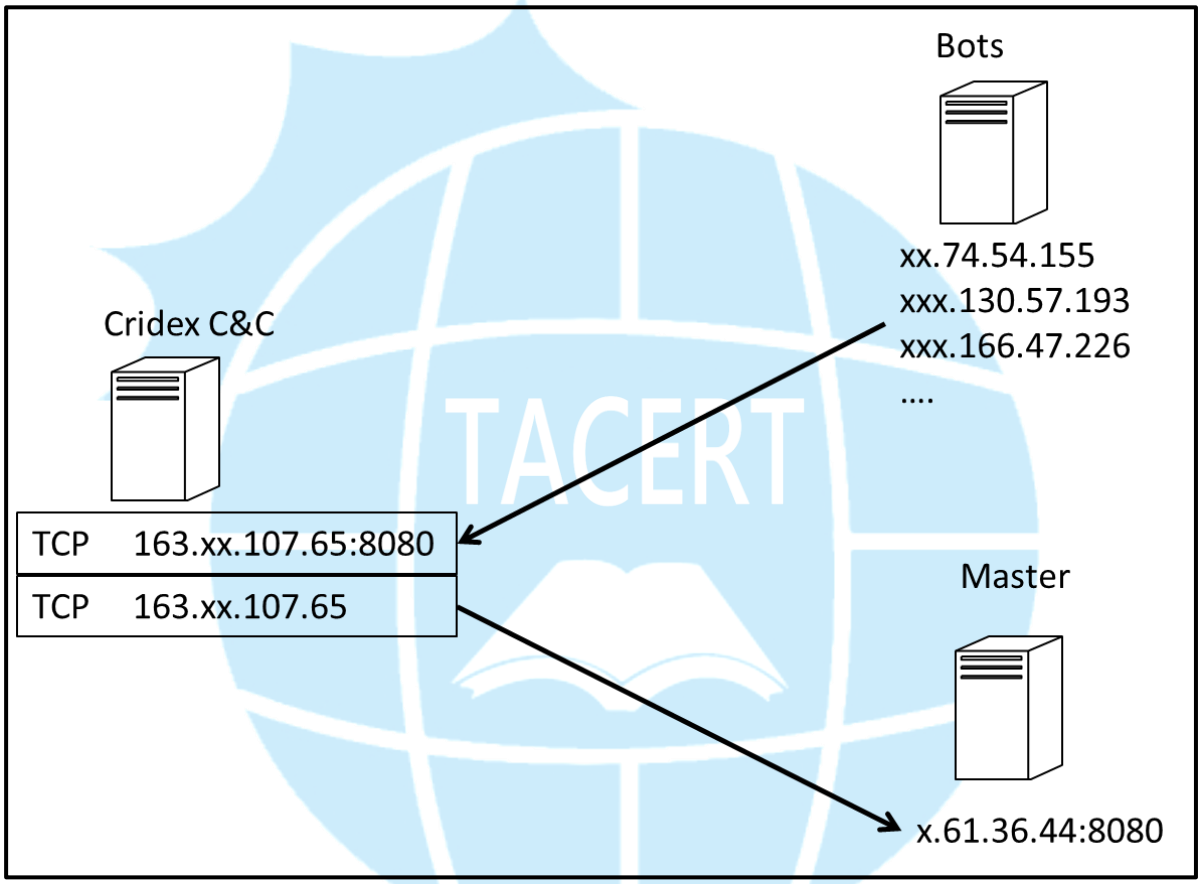


圖 3 網路活動概念圖

ld-linux.so.2 放置路徑為[/tmp/.estbuild/lib/ ld-linux.so.2]，由圖 4 可以看到放置 ld-linux.so.2 的是一個隱藏資料夾[/tmp/.estbuild/]，資料夾擁有者和群組為 cgesftp，這是該台主機的 FTP 帳號，如果設定恰當 cgesftp 應該僅能在 FTP 的上傳目錄活動且不能使用 SSH 登入。但是在主機的 Log 中可以看到如圖 5 的紀錄，89.149.223.104 使用 cgesftp 帳號成功登入了三次，其中第二次的登入時間為[Jan 31 21:38:25]，這個時間剛好與[/tmp/.estbuild/]資料夾建立的時間相符合，所以可以知道駭客先是得到 cgesftp 的密碼之後，利用 SSH 登入植入惡意程式。

由於在 SSH 登入檔裡面沒有任何關於 cgesftp 帳號被暴力攻擊的紀錄，所以推斷駭客得到 cgesftp 帳號密碼並不是透過嘗試 SSH 暴力攻擊，有可能是透過其他管道得到 FTP 的帳號密碼後，才拿來登入 SSH。

```
total 68    /tmp
drwxrwxrwt 12 root    root    4096 Feb  1 10:42 .
drwxr-xr-x 25 root    root    4096 Oct  7 11:02 ..
drwxr-xr-x  6 cgesftp teacher 4096 Jan 31 21:39 .estbuild
drwxrwxrwt  2 root    root    4096 Jan  5 03:50 .font-unix
drwxrwxrwt  2 root    root    4096 Jan  5 03:50 .ICE-unix
drwx------  2 root    root    4096 Aug 30 10:35 keyring-AIufuv
drwx------  2 root    root    4096 May 17  2012 keyring-q2QC6i
srwxrwxr-x  1     500 wam        0 Mar 16  2012 mapping-admin
srwxr-xr-x  1 root    root       0 Aug 30 10:35 mapping-root
drwx------  2 root    root    4096 Aug 30 12:04 orbit-root
srw-------  1 root    root       0 Aug 30 10:35 scim-helper-manager-socket-root
srw-------  1     500 wam        0 Mar 16  2012 scim-panel-socket:0-admin
srw-------  1 root    root       0 Aug 30 10:35 scim-panel-socket:0-root
srw-------  1 root    root       0 Aug 30 10:35 scim-socket-frontend-root
drwx------  2 root    root    4096 Aug 30 10:35 ssh-Lmodg28386
drwxr-xr-x  2 root    root    4096 Feb  1 10:43 tmp
drwxr-xr-x  2 root    root    4096 Oct  7 20:55 .webmin
-r--r--r--  1 root    root      11 Aug 30 10:35 .X0-lock
drwxrwxrwt  2 root    root    4096 Jan  5 03:50 .X11-unix
```

圖 4 放置 ld-linux.so.2 的資料夾所有者以及群組為 cgesftp

```
Jan 28 17:33:28 dns sshd[676]: Accepted password for cgesftp from 89.149.223.104 port 39099 ssh2
Jan 28 17:33:28 dns sshd[676]: pam_unix(sshd:session): session opened for user cgesftp by (uid=0)
Jan 28 17:33:56 dns sshd[676]: pam_unix(sshd:session): session closed for user cgesftp
Jan 31 21:38:25 dns sshd[26734]: Accepted password for cgesftp from 89.149.223.104 port 52649 ssh2
Jan 31 21:38:25 dns sshd[26734]: pam_unix(sshd:session): session opened for user cgesftp by (uid=0)
Jan 31 21:39:07 dns sshd[26734]: pam_unix(sshd:session): session closed for user cgesftp
Feb  1 12:29:33 dns su: pam_unix(su:session): session opened for user cgesftp by root(uid=0)
2:Jan 18 21:06:34 dns sshd[10793]: Accepted password for cgesftp from 89.149.223.104 port 57027 ssh2
2:Jan 18 21:06:34 dns sshd[10793]: pam_unix(sshd:session): session opened for user cgesftp by (uid=0)
2:Jan 18 21:06:59 dns sshd[10793]: pam_unix(sshd:session): session closed for user cgesftp
4:Jan  5 03:49:43 dns sshd[22727]: Accepted password for cgesftp from 46.47.82.70 port 56345 ssh2
4:Jan  5 03:49:43 dns sshd[22727]: pam_unix(sshd:session): session opened for user cgesftp by (uid=0)
4:Jan  5 03:50:36 dns su: pam_unix(su:auth): authentication failure; logname=cgesftp uid=601 euid=0 tt
pt
4:Jan  5 03:50:51 dns sudo:  cgesftp : user NOT in sudoers ; TTY=pts/0 ; PWD=/home/teacher/cgesftp ; U
ser/id
4:Jan  5 03:50:59 dns sshd[22727]: pam_unix(sshd:session): session closed for user cgesftp
```

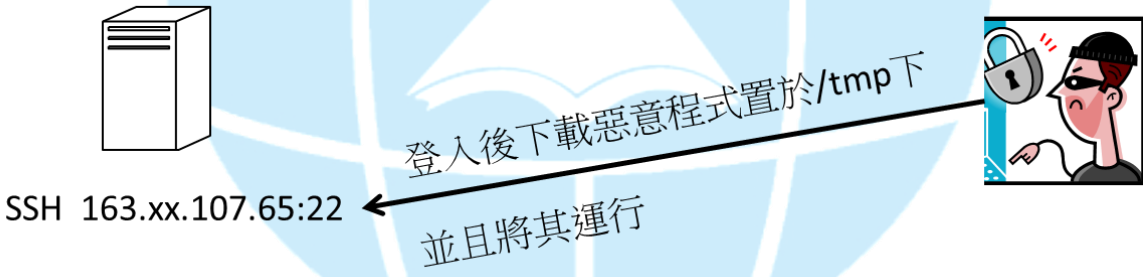
圖 5 主機所有 cgesftp 帳號的 SSH 登入紀錄

入侵手法推測

Step 1:駭客對FTP暴力攻擊取得cgesftp帳號的密碼

Step 2: 使用cgesftp帳號與密碼登入SSH服務

Step 3: 由於權限的關係，駭客將惡意程式放在/tmp底下



建議措施

- 對 SSH 登入的帳號做限制
- 由於/tmp 沒有設置權限的特性，建議使用獨立的分割區或硬碟掛載/tmp
- 對所有可以遠端存取的服務設定存取網路位址
- 資安事件處理完畢後，登入服務的密碼應進行更換避免駭客使用同組帳密再度登入

這個案例中使用的 FTP 服務（ProFTPD），在登入帳號的設定上採用實體用戶，意即直接使用本機端的一般使用者帳號當作 FTP 的登入帳號，這種設定雖然方便，但是若沒限制 SSH 登入，則容易因為 FTP 帳號密碼被破解而得到一組可以登入 SSH 的帳號。Linux 上的/tmp 是一個所有人都可以存取、寫入、刪除的資料夾，由於其特性，建議重要主機的/tmp 另外獨立掛載。本案例中的 C 國小採用一個 FTP 帳號全校使用的政策，雖然建立多個帳號會增加帳號密碼被破解的機率，但是多人使用同一組帳密會使得管理不便，一般使用者無法隨意更改密碼以確保自己的帳號安全，而由於多人共用，管理者若要進行定時更改密碼的動作，也會影響許多人員的使用，因此，多人共用的帳號鮮少更改密碼，甚至在系統重新重灌升級後，密碼仍會維持原先的設定以避免影響人員的使用。當主機被侵入是因為帳號密碼已經被駭客得知，而礙於使用者眾，變更密碼會影響許多人的情況下，有些主機在資安事件發生之後，雖然清除了惡意程式，但仍繼續沿用原本的帳密，導致駭客仍可以繼續登入進行惡意活動。

參考

http://labs.m86security.com/2012/03/the-cridex-trojan-targets-137-financial-organizations-in-one-go/