DDoS 攻擊簡介與案例分享

行政院國家資通安全會報 技術服務中心

大綱

- DDoS 攻擊簡介
  - DoS 與 DDoS 攻擊
  - DDoS 攻擊趨勢發展
  - 常見 DDoS 攻擊手法
- DDoS 攻擊案例分享
  - Spamhaus & Cloudflare 被攻擊事件
  - Anonymous Asia 攻擊事件
- DDoS 攻擊應變與防護
- 結論

DDoS 攻擊簡介

DoS 與 DDoS 攻擊

- 阻斷服務攻擊
  - Denial of Service (DoS) Attack，是一種網路攻擊手法，其目的在於使目標電腦的網路或系統資源耗盡，使服務暫時中斷或停止，導致其對目標客戶不可用
- 分散式阻斷服務攻擊
  - 當攻擊者利用網路上兩個或以上的電腦作為向特定的目標發動阻斷服務攻擊時，就稱為分散式阻斷服務攻擊 Distributed Denial of Service (DDoS) Attack

DDoS 攻擊趨勢發展(1/3)

- 關於史上第一次 DDoS 的攻擊，有紀錄可考的為 1996 / 9 /12 ，美國紐約的 ISP 業者 PANIX.COM
  - 遭受到的偽造源 IP 地址的 TCP SYN Flood 攻擊，導致業務中斷，影響其大部分的客戶服務包括郵件、新聞群組、網頁服務等
  - 面對每秒傳送超過 150 個 SYN 封包，PANIX 難以負載

DDoS 攻擊趨勢發展(2/3)

- 2001 / 2 陸續發生一系列 DDoS 攻擊事故
  - 如 yahoo、eBay、Amazon、ZDNet 和 CNN 等諸多國際知名網站均先後受到攻擊或波及，導致這些網站長時間中斷服務，涉及的經濟損失高達幾百萬美元
  - 從此 DDoS 攻擊開始受到廣泛關注
- 2004年以後，越來越多攻擊者開始利用殭屍網絡(Botnet)進行 DDoS 攻擊
  - 2005 年摩洛哥駭客 Farid Essabar 因散播自行撰寫的 Zotob (Mytob) 惡意程式而被逮捕，這是第一個已知大量感染 Windows 作業系統的 Botnet 程式
  - Essabar 承認他預計出售 Botnet 控制權來謀利，至此 DDoS 攻擊不僅僅是危害攻擊目標，也開始嚴重威脅一般用戶安全

DDoS 攻擊趨勢發展(3/3)

- 自2010年起，DDoS 攻擊也逐漸從牟利為主轉變為政治訴求、意識形態表達及抗議的常用手段
  - 隨著殭屍網路急速成長，DDoS 攻擊的規模也與日俱增
  - 在 2010 年，DDoS 攻擊規模首次突破了 100 Gbps
  - 最著名的意識形態表達的案例為 2010 / 12 VISA、MasterCard 與 PayPal 被攻擊事故，駭客團體 Anonymous 為了報復上述三家金融機構封鎖Wikileaks 的帳戶並取消相關金融服務，對其發動 DDoS 攻擊，稱為 Operation Payback
- 迄今(2015年)，一般 DDoS 攻擊規模平均在 7 Gbps 左右，但最大曾達 400 Gbps

常見 DDoS 攻擊手法(1/5)

- DDoS 攻擊可以具體分成兩種形式：
- 頻寬消耗型
  - 以消耗頻寬為目的，使正常用戶因連線頻寬耗盡而無法連線至目標系統
- 資源消耗型
  - 以耗盡系統記憶體或處理器資源為目的，阻止目標系統處理合法請求
- 它們都是透過大量合法或偽造的請求占用大量網路以及設備資源，以達到癱瘓網路及系統之目的

常見的 DDoS 攻擊手法(2/5)

- User Datagram Protocol (UDP) Floods
  - 以大量 UDP Fragment 封包直接塞滿頻寬，或是：
  - 攻擊者產生任意埠號的 UDP 封包，目標主機接收 UDP 封包後，若無程式可處理該 UDP 封包，目標主機即會回傳給來源 IP 無法到達的 ICMP 封包，但因攻擊者會隱藏來源 IP，造成此 ICMP 封包充斥整個網路，影響網路頻寬
- ICMP Floods
  - Internet Control Message Protocol (ICMP) Floods是攻擊者透過向未良好設置的路由器發送廣播信息，以占用系統資源的做法

常見的 DDoS 攻擊手法(3/5)

- Ping of Death
  - 利用 Ping 的方式，產生超過 65536 Bytes 的封包攻擊目標主機，65536 Bytes 封包格式超出 IPv4 規定最大封包大小，大部分電腦無法處理會導致緩衝區溢位，可能會造成系統當機或是重開
- SYN Flood
  - 攻擊者以多個隨機位址向目標主機發送 SYN 封包，而在收到目標主機的 SYN ACK 封包後就不回應，這樣，目標主機就為這些連線請求建立了大量的連接佇列，但因沒有收到 ACK 封包而一直維護著這些佇列，造成了資源的大量消耗而無法處理正常請求

常見的 DDoS 攻擊手法(4/5)

- SSDP Amplification
  - Simple Service Discovery Protocol (SSDP) 是一種偵測 Plug & Play (UPnP) 裝置的協定。攻擊者藉由發送偽造目標主機 IP 之 SSDP 封包至網路上所有開啟該協定的主機使其回應至目標主機，具有放大約 **30** 倍的效果
- DNS Amplification
  - 藉由不斷發送偽造成目標主機 IP 的 DNS Query 封包來進行遞迴查詢，而將目標主機頻寬塞滿。因 DNS 伺服器所回應封包比原有封包大上約 **100** 倍，有放大的效果
- Application-Level Floods
  - 針對應用軟體層，透過向網路應用程式伺服器提出無限制的資源申請，阻斷其正常之網路服務

常見的 DDoS 攻擊手法(5/5)

- CHARGEN Amplification
  - Character Generator Protocol (CHARGEN)，中文為字元符號產生協定。預設通訊埠為 TCP 19 以及 UDP 19，若透過 TCP 19 來連結，則 Server 端會不斷回傳任意字串到 Client，直到連線結束。若改採 UDP 19 進行連線，則 Server 端會重新產生帶有一長串字串的封包檔給 Client 端
  - 此服務主要用途是利用這些網路流量，測試兩台主機間的網路連線或網路頻寬
  - 攻擊者通常利用 UDP 連線方式，向 Server 端發送偽造來源 IP 位址的封包，讓提供此服務的 Server 向受害主機不斷傳送含有亂數字元的封包
  - CHARGEN 具有放大約 **358.8** 倍的效果

DDoS 攻擊案例

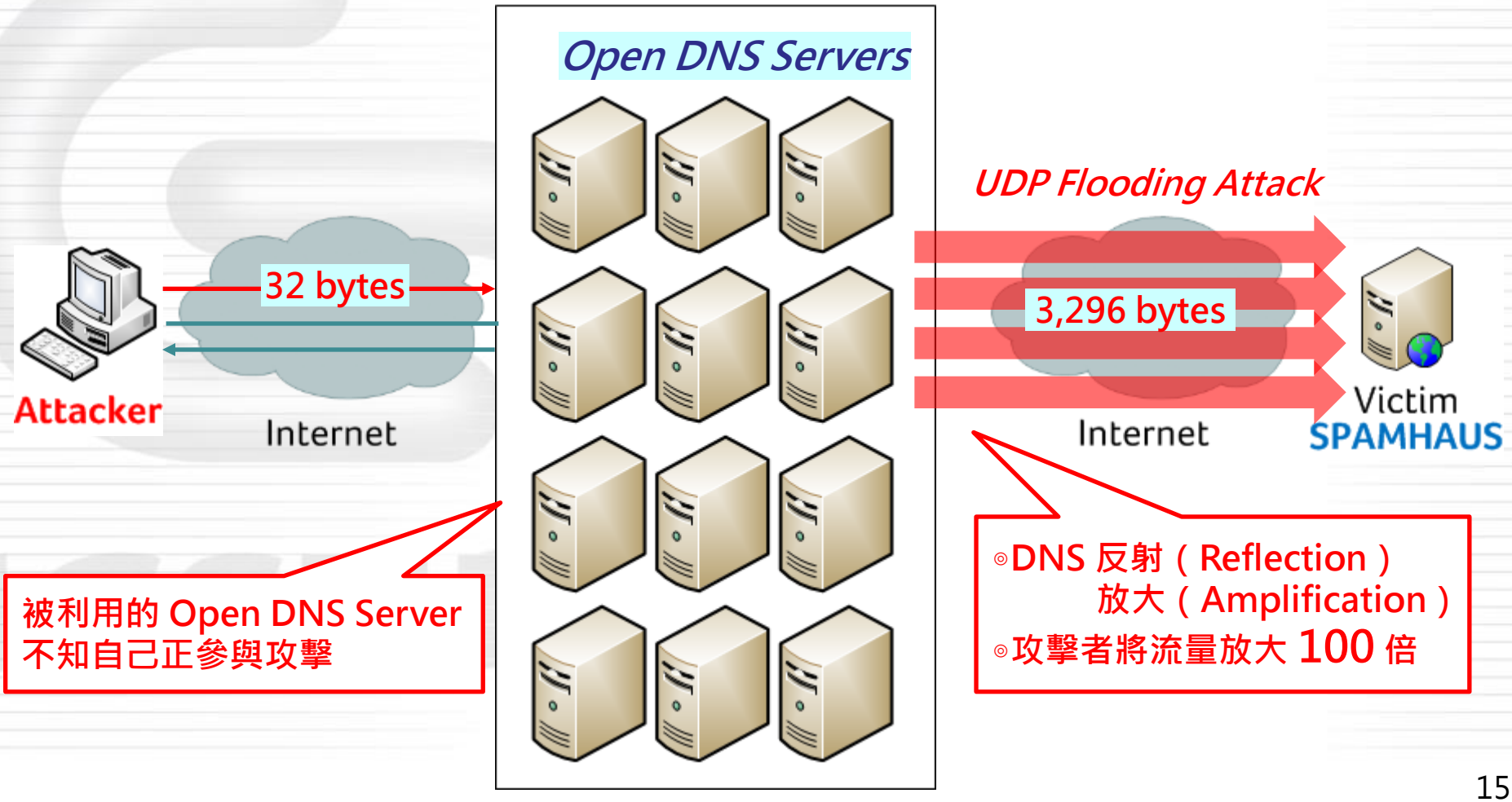
Spamhaus & Cloudflare
被攻擊事件

史上首次超過 300 Gbps 的攻擊

- Spamhaus 簡介
  - 是全球最大反垃圾郵件非營利組織，運用多樣化的精密方法找出垃圾郵件業者，並列出所有已知垃圾郵件業者，供大眾隨時查閱
- Spamhaus 在 2013/3/19 遭受流量 300Gbps 之 DDoS 攻擊，持續近一週
  - 合法用戶無法使用 Spamhaus 系統
  - Spamhaus 的網路服務供應商 CloudFlare 也遭攻擊，還有數個相關網路業者也受波及
- 被攻擊原因疑似是 Spamhaus 將 CyberBunker 列入最差 ISP 的首位引發駭客不滿而發動攻擊
  - CyberBunker 負責人認為 Spamhaus 濫用權力，但不承認是攻擊 Spamhaus 的幕後主使者

Spamhaus DDoS 攻擊手法說明

根據 CloudFlare 統計，這次被用來攻擊的 68,495 台 Open DNS Server 中，台灣 ISP 佔了 2,992 台，排名第二



被利用的 Open DNS Server 不知自己正參與攻擊

- DNS 反射（Reflection）放大（Amplification）
- 攻擊者將流量放大 100 倍

CloudFlare 再次被攻擊

- 史上最大的 300 Gbps 攻擊量保持不到一年...
- 2014/2/10 Cloudflare 宣稱遭到攻擊流量約 400Gbps以上的 DDoS 攻擊
  - 駭客使用網路校時協定(Network Time Protocol, NTP)類型的 DDoS 攻擊
  - 與 DNS 類型的攻擊相仿，NTP 也是一種只要以簡單的小小要求就能造成系統龐大回應的 UDP 類型協定
  - 遭受攻擊的同樣是 CloudFlare 的客戶，但 CloudFlare 並未公布客戶名稱，僅說該客戶連續兩小時受到 400Gbps流量的轟炸，進而拖慢了整個歐洲的網路流量

NTP 逐漸成為駭客最愛

- 利用 NTP 協定恐怖的放大效果
  - 舉例說明：ntpdc –c monlist xxx.xxx.xxx.xxx
    - monlist (或 mon_getlist)是向 NTP 伺服器請求回傳該伺服器所監控的位址列表，最多可回傳 600 筆
    - monlist 本身只有 234 bytes，但回傳的流量以 6 個位址切為一個封包 (446 bytes)，600 筆將回傳 100 個封包 (44,600 bytes)，等於放大了約 **190** 倍！
- 根據 US-CERT 之警訊(**TA14-017A**)，駭客可利用 NTP 協定放大自身攻擊封包最多至 **556.9** 倍之多！！
- 目前尚無有效方法防範此類型的攻擊
  - 資安專家呼籲所有組織企業提高警覺，做好自身 NTP 伺服器的安全設定，以減少駭客可利用的 NTP 伺服器

Anonymous Asia 攻擊事件

We Are Anonymous

- Anonymous(匿名者)主要是依**理念聚集而成的群體**，由網路行動分子與駭客組成的自發性鬆散組織
  - 理念或想法相似即可成為匿名者成員，由於參與任何形式駭客攻擊都是違法行為，亦表示**成員必須自行承擔相關法律責任**
  - 匿名者群體之間以**IRC(網路聊天程式)**或**社群網站**作為其溝通聯繫管道
  - 主要透過**分散式阻斷服務(DDoS)**、**置換網頁**、**駭入特定網站**或**直接癱瘓網站**等攻擊方式，進行不流血抗爭行動

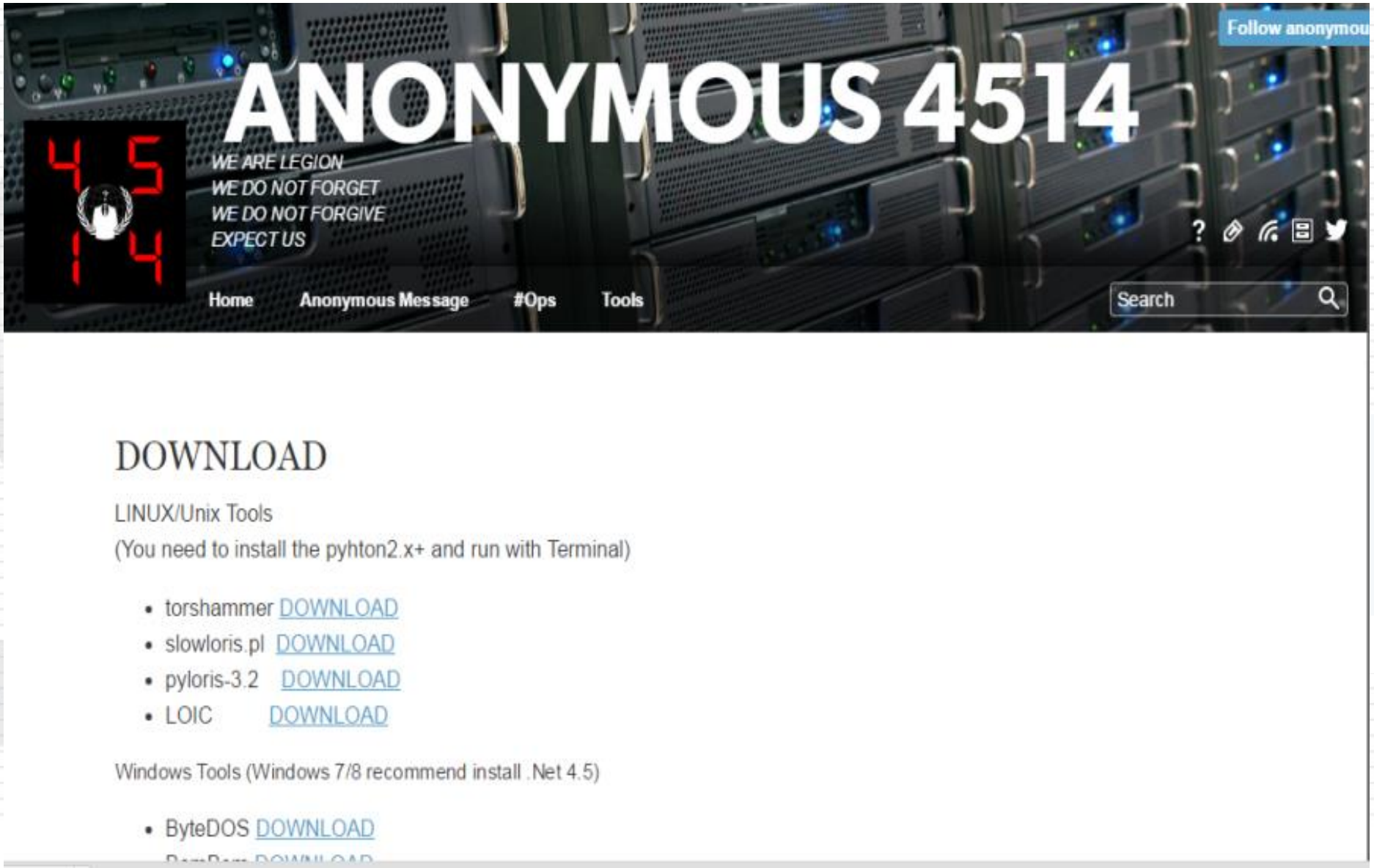
戰爭的開始...

- 因課綱微調爭議不斷，加上反課綱北區高校聯盟發言人於 7 / 30 燒炭自殺身亡，引發反課綱學生情緒高漲發動抗爭行動
- 駭客組織 Anonymous Asia 在 Facebook 專頁發表文章支持反課綱學生，於 7 / 31 起陸續攻擊政府機關與部分民間組織/機構所屬網站

#OpTaiwan 行動(1/4)

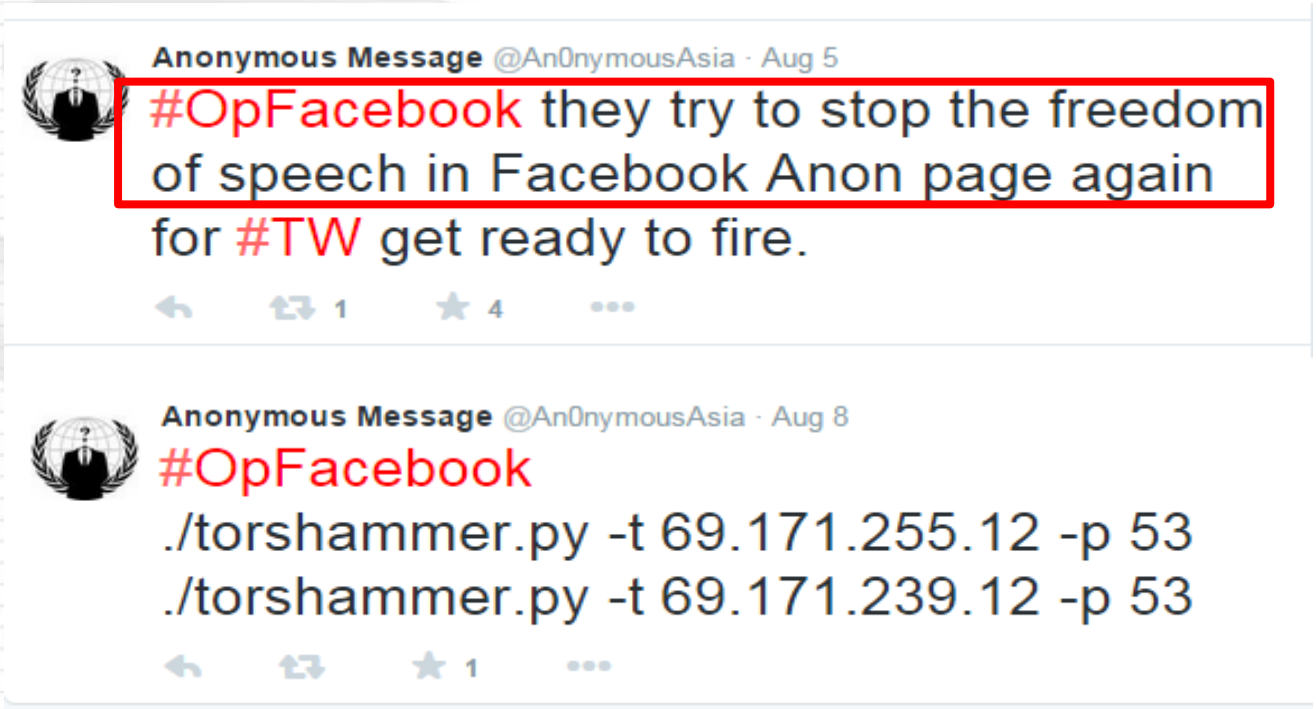
- 聚集的理念：反課綱微調
  - 以「反課綱微調」作為號召理念，召集相同理念的網路使用者與駭客
- 抗爭方式：分散式阻斷服務為主
  - 攻擊目標以政府機關為主，亦包含部分民間組織/機構
- 號召與溝通平台：Facebook (臉書)
  - 104/8/5 Anonymous Asia 的 Facebook 專頁無預警關閉，轉至 Twitter、google+ 及 tumblr 等作為溝通平台

#OpTaiwan 行動(2/4)



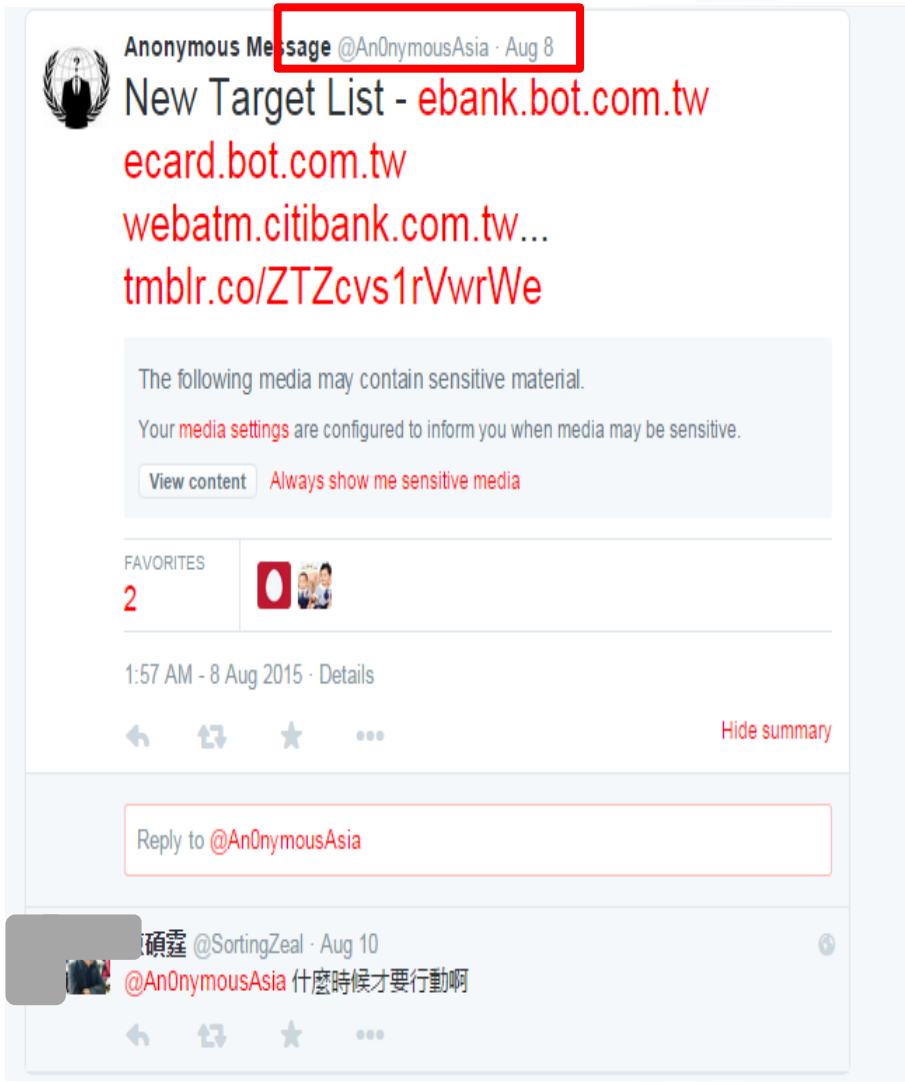
#OpTaiwan 行動(3/4)

- #OpTaiwan 行動於 Anonymous Asia 發起 #OpFacebook 後趨緩
  - Anonymous Asia 表示因 Facebook 限制 Anonymous Asia 言論自由，因此發起 #OpFacebook 行動



#OpTaiwan 行動(4/4)

- 時間：2015/ 7 /31 至 2015 / 8 /7 攻擊行動以**遊擊戰**方式攻擊目標，各機關透過**阻擋攻擊來源**、**新增阻擋設備**及**限制頻寬**等方式，緩解攻擊行動造成影響
  - **影響網站時間不長**，除教育部外，其他網站平均影響時間約 65 分，其中最短為 20 分鐘，最長為 171 分鐘



#OpTaiwan 行動_攻擊手法(1/4)

- DDoS 攻擊工具
  - Torshammer.py
    - Tor’ s Hammer 是一個能發起緩慢 post Dos 攻擊的測試工具
    - 可透過 Tor Networks 隱藏 IP

透過Port：9050連至Tor Networks

```
#!/usr/bin/python

# cks.py (http://phiral.net/socks.py)
# al.net/terminal.py) in the
# same directory and that you have tor running locally
# on port 9050. run with 128 to 256 threads to be effective.
# kills apache 1.X with ~128, apache 2.X / IIS with ~256
# not effective on nginx

useragents = [
"Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30)",
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)",
"Googlebot/2.1 (http://www.googlebot.com/bot.html)",
"Opera/9.20 (Windows NT 6.0; U; en)",
"Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.1.1) Gecko/20061205 Iceweasel/2.0.0.1 (Debian-2.0.0.1+dfsg-2)",
"Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; FDM; .NET CLR 2.0.50727; InfoPath.2; .NET CLR 1.1.4322)",
"Opera/10.00 (X11; Linux i686; U; en) Presto/2.2.0",
"Mozilla/5.0 (Windows; U; Windows NT 6.0; he-IL) AppleWebKit/528.16 (KHTML, like Gecko) Version/4.0 Safari/528.16",
"Mozilla/5.0 (compatible; Yahoo! Slurp/3.0; http://help.yahoo.com/help/us/ysearch/slurp)", # maybe not
"Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.2.13) Gecko/20101209 Firefox/3.6.13"
"Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 5.1; Trident/5.0)",
"Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 1.1.4322; .NET CLR 2.0.50727)",
"Mozilla/4.0 (compatible; MSIE 7.0b; Windows NT 6.0)",
"Mozilla/4.0 (compatible; MSIE 6.0b; Windows 98)",
"Mozilla/5.0 (Windows; U; Windows NT 6.1; ru; rv:1.9.2.3) Gecko/20100401 Firefox/4.0 (.NET CLR 3.5.30729)",
"Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.2.8) Gecko/20100804 Gentoo Firefox/3.6.8",
"Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.2.7) Gecko/20100809 Fedora/3.6.7-1.fc14 Firefox/3.6.7",
"Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)",
"Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)",
"YahooSeeker/1.2 (compatible; Mozilla 4.0; MSIE 5.5; yahooseeker at yahoo-inc dot com ; http://help.yahoo.com/help/us/shop/merchant/)"
```

總計使用20個 Useragent

#OpTaiwan 行動_攻擊手法(2/4)

攻擊指令

```
111  def usage():
112      print "./torshammer.py -t <target> [-r <threads> -p <port> -T -h]"
113      print " -t|--target <Hostname|IP>"
114      print " -r|--threads <Number of threads> Defaults to 256"
115      print " -p|--port <Web Server Port> Defaults to 80"
116      print " -T|--tor Enable anonymising through tor on 127.0.0.1:9050"
117      print " -h|--help Shows this help\n"
118      print "Eg. ./torshammer.py -t 192.168.1.100 -r 256\n"
```

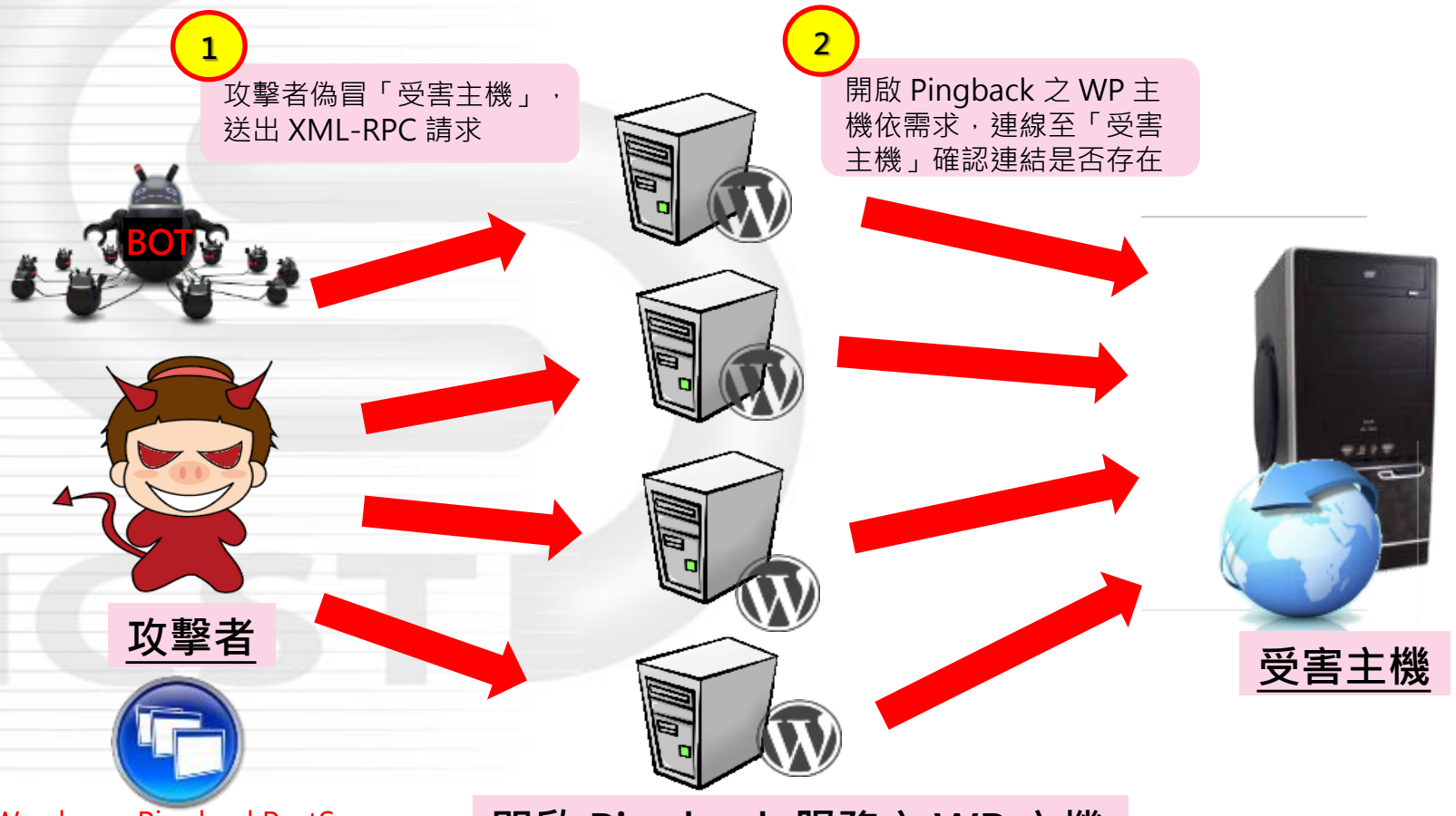
```
Posting: w
Posting: U

Posting: L
Posting: i
Posting: S
Posting: t
Posting: C
Posting: i
Posting: LPosting: APosting: PConnected to host...

Posting: p Posting: 6

Posting: t

Posting: d
Posting: P
Posting: T
Connected to host...Posting: 1

Posting: K
Posting: aPosting: u

Posting: 4
Posting: r
Posting: f
Posting: P
Posting: p
Posting: J
 Posting: 1Connected to host...Posting: bPosting: b
```

透過Port：9050連至 Tor Networks

#OpTaiwan 行動_攻擊手法(3/4)

– 系統功能 (Wordpress Pingback)

➢ Pingback 為參考或連線 Wordpress 網站文章時，進行回報的一個 XML-RPC 請求



#OpTaiwan 行動_攻擊手法(4/4)

```
<?xml version="1.0" encoding="iso-8859-1"?>
<methodCall>
  <methodName>pingback.ping</methodName>
  <params>
   <param><value><string>http://Target:Port</string></value></param>
   <param><value><string>http://validpostlink</string></value></param>
  </params>
</methodCall>
```

攻擊目標

引用URL

2015/7/31	17:29:55 [redacted] 1.31	WordPress/4.2.3;-http://www.scratchmommy.com;+verifying+pingback+from+112.119.194.23	302	15234
2015/7/31	17:39:16 [redacted] 248.104	WordPress/4.2.3;-http://www.dassport.net;+verifying+pingback+from+112.119.194.23	302	28361
2015/7/31	17:29:27 [redacted] 77.65	WordPress/3.9.1;-http://maureeneoconnell.com;+verifying+pingback+from+112.119.194.23	302	1326

套件名稱

遭利用部落格

攻擊IP

其他攻擊手法(1/2)

- 利用攻擊工具/網頁，以合法網路流量，進行攻擊行為

1

http://loveedu.ddns.net/edu

2

http://thlserver.ddns.net/edu/

其他攻擊手法(2/2)

原始碼: http://loveedu.ddns.net/edu/ - Mozilla Firefox

檔案(F) 編輯(E) 檢視(V) 說明(H)

```
70              「汝思華，吾思台！」 <br>
71          </h5>
72        </div>
73        <div class="row text-center">
74          <h2><font color="yellow">親愛的思華：撤回課綱，我們會更愛您
75        </div>
76      </div>
77      <div class="container">
78        <div class="row text-center"><img src="img/rex.png" alt="">
79          <p>部分原始碼參照自 PTTATK鍵盤開戰</p>
80        </div>
81      </div>
82      <div id="board"></div>
83      <script>
84          var index, length, board = document.getElementById('board');
85          board.innerHTML += get_iframe_syntax('http://www.edu.tw');
86          ifs = document.getElementsByTagName('iframe');
87          setInterval(refresh_website_page, 150);
88      </script>
89      <script>
90          (function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[
91          (i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.
```

*無線網路連線 [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

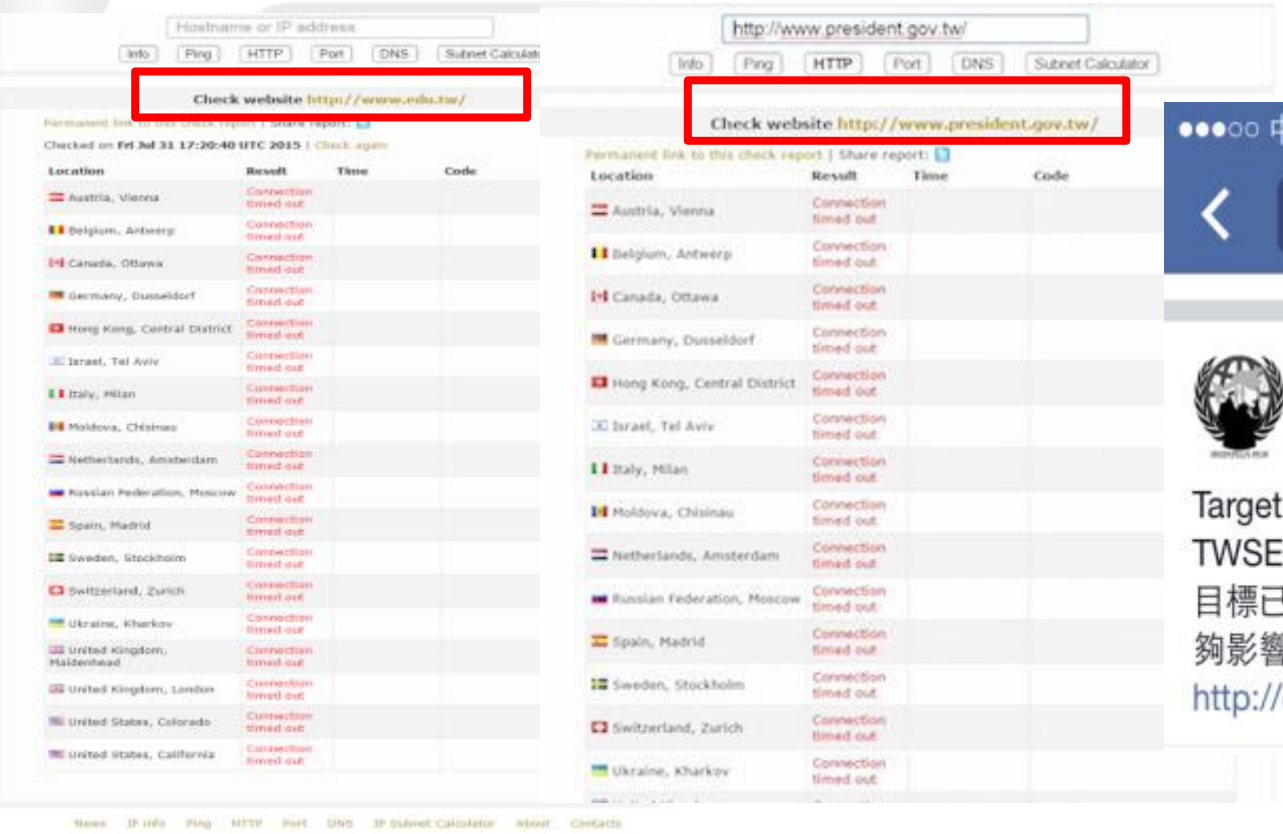
Filter: ip.addr == 140.111.1.140 Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
518	8.489911000	192.168.1.106	140.111.1.140	TCP	54	5417→80 [FIN, ACK] Seq=427 Ack=
559	8.609259000	192.168.1.106	140.111.1.140	TCP	66	5420→80 [SYN] Seq=0 Win=8192 Le
564	8.624250000	192.168.1.106	140.111.1.140	TCP	54	5420→80 [ACK] Seq=1 Ack=1 Win=6
565	8.624397000	192.168.1.106	140.111.1.140	HTTP	480	GET /?074582852315373541317dc9
568	8.641118000	192.168.1.106	140.111.1.140	TCP	54	5420→80 [ACK] Seq=427 Ack=163 W
569	8.654381000	192.168.1.106	140.111.1.140	TCP	54	5420→80 [FIN, ACK] Seq=427 Ack=
608	8.758369000	192.168.1.106	140.111.1.140	TCP	66	5422→80 [SYN] Seq=0 Win=8192 Le
612	8.772855000	192.168.1.106	140.111.1.140	TCP	54	5422→80 [ACK] Seq=1 Ack=1 Win=6
613	8.773058000	192.168.1.106	140.111.1.140	HTTP	481	GET /?047041698302794366=0c0aec
616	8.790510000	192.168.1.106	140.111.1.140	TCP	54	5422→80 [ACK] Seq=428 Ack=163 W
617	8.802243000	192.168.1.106	140.111.1.140	TCP	54	5422→80 [FIN, ACK] Seq=428 Ack=
657	8.911576000	192.168.1.106	140.111.1.140	TCP	66	5424→80 [SYN] Seq=0 Win=8192 Le
662	8.925836000	192.168.1.106	140.111.1.140	TCP	54	5424→80 [ACK] Seq=1 Ack=1 Win=6
663	8.926076000	192.168.1.106	140.111.1.140	HTTP	479	GET /?827748582550863 5=d3e754c3
666	8.942278000	192.168.1.106	140.111.1.140	TCP	54	5424→80 [ACK] Seq=426 Ack=163 W
667	8.964258000	192.168.1.106	140.111.1.140	TCP	54	5424→80 [FIN, ACK] Seq=426 Ack=
714	9.081612000	192.168.1.106	140.111.1.140	TCP	66	5426→80 [SYN] Seq=0 Win=8192 Le

```
⊞ Frame 564: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
⊞ Ethernet II, Src: IntelCor_56:90:5f (f8:16:54:56:90:5f), Dst: ZyxelCom_48:b6:b1 (10:7b:ef:48:
⊞ Internet Protocol Version 4, Src: 192.168.1.106 (192.168.1.106), Dst: 140.111.1.140 (140.111.
⊞ Transmission Control Protocol, Src Port: 5420 (5420), Dst Port: 80 (80), Seq: 1, Ack: 1, Len:
```

政府機關受害概況(1/2)

- Anonymous Asia 宣稱已成功攻擊多個政府機關與民間組織/機構，其中包含 14 個政府機關
  - –技服中心陸續接獲 10 個政府機關 DDoS 攻擊事件通報



政府機關受害概況(2/2)

- 技服中心分析機關日誌檔，多數攻擊IP來源分屬如下：
  - 大量Tor網路IP
    - XX部網站於8/3 1:40至2:05左右遭癱瘓
    - 分析該時段防火牆紀錄，發現Tor連線占該時段流量50%

時間	合計	時間	合計	時間	合計
00:50-01:00	2,718	01:00-02:00	20,134	02:00-03:00	4,387
client	volume	client	volume	client	volume
68.180.228.228	219	89.105.194.88	3,970	68.180.228.228	277
5.9.111.70	125	91.109.247.173	2,048	171.96.181.76	150
118.170.3.72	110	194.150.168.79	1,536	207.46.13.68	135
114.45.166.99	100	109.163.234.8	1,536	157.55.39.173	114
188.165.15.84	87	188.138.9.49	1,009	182.235.38.50	102
123.192.223.69	81	68.180.228.228	310	188.165.15.84	98

  - Amazon EC2 雲端主機
    - 有心人士租用雲端主機使用DDoS攻擊程式，對政府網站進行攻擊，頻率約30萬次/分
  - 國內零散IP
    - 國內民眾可能亦參與癱瘓教育部網站

序號	IP	連線次數	國家	所屬網域名稱	所有人
1	106.105.190.27	1969	Taiwan	NCICNET-NET	New Century InfoComm Tech. Co., Ltd.
2	60.250.226.61	1089	Taiwan	HINET-NET	Taipei Taiwan
3	1.172.110.191	991	Taiwan	HINET-NET	Taipei Taiwan
4	192.83.167.2	981	Taiwan	TANET-CNET4	imported inetnum object for MOEC
5	220.142.69.228	945	Taiwan	HINET-NET	Taipei Taiwan
6	220.132.233.59	457	Taiwan	HINET-NET	Taipei Taiwan
7	36.234.38.101	410	Taiwan	HINET-NET	Taipei Taiwan
8	118.169.53.138	164	Taiwan	HINET-NET	Taipei Taiwan

中央機關應變與防護(1/2)

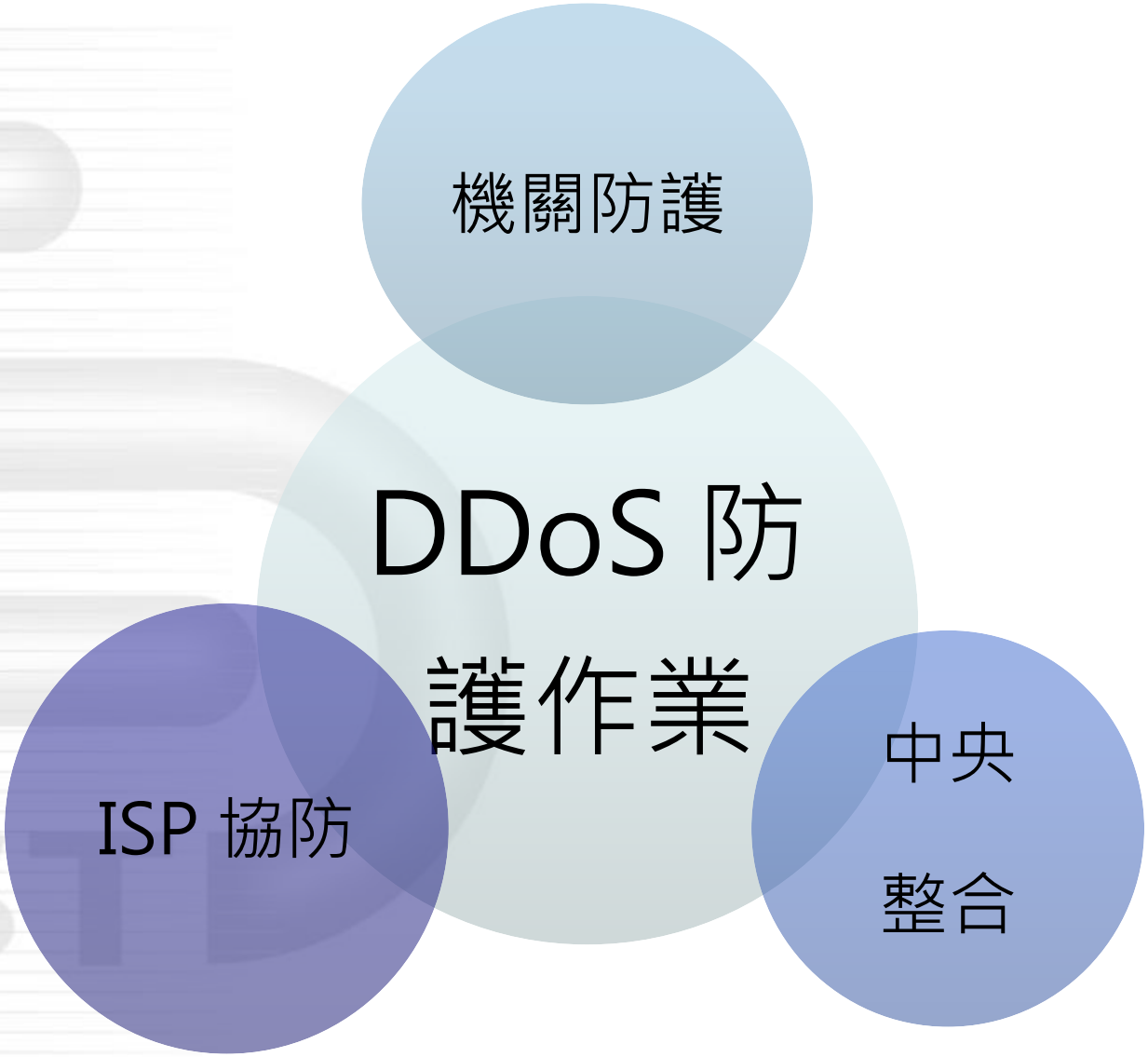
- 技服中心依攻擊紀錄，對外發布攻擊訊息與阻擋資訊
  - 8/2發布資安警訊，提醒各政府機關提高警覺，加強網路監控與相關防範措施
  - 分析攻擊紀錄與情資，請國發會協助阻擋攻擊來源(Tor Network)，並於8/5提供攻擊手法與阻擋資訊予政府機關與G-ISAC會員
  - 透過TWCERT/CC與TWNCERT，通報攻擊來源所屬之國際交流組織進行事件處理
- 警調單位進行攻擊來源與手法調查
  - 【調查局】分析攻擊來源與攻擊手法，調查攻擊者與攻擊資訊設備
  - 【刑事局】追查攻擊事件發動者，掌握攻擊動態與工具

中央機關應變與防護(2/2)

- 因應 Anonymous Asia 發布 48 小時通碟，召開臨時緊急應變會議
  - 刑事局持續關注 Anonymous Asia 動態，必要時向社群管理單位檢舉
  - 調查局針對國內攻擊來源進行調查，依法移送檢察機關偵辦
  - 通傳會轉技服中心彙整之攻擊來源予國內 ISP 業者，進行阻擋或相關處置
  - 關鍵(資訊)基礎設施之主管機關掌握重要資訊系統運作情況，並轉知攻擊資訊予維運單位，以加強防護作業

DDoS 攻擊應變與防護

DDoS 攻擊應變與防護



DDoS 攻擊應變與防護_政府機關

準備階段	偵測與分析階段	封鎖根除與復原	事後處置
●識別重要資訊系統/服務，**建置各式備援機制** ●維護網路維護人員/廠商聯繫資訊 ●**制定/維護 DDoS 應變程序**，並定期執行 DDoS 攻擊演練 ●**建立日誌保存機制** ●**基礎設備 DDoS 防護設置** ●設置入侵偵測與入侵防護系統 ●**設置流量監控機制** ●設置/維護阻擋清單	●**網路流量觀察與監控** ●定期檢視與分析各式日誌檔	●**分析攻擊來源 IP** ●識別攻擊類型，分析攻擊手法與特徵 ●保留相關攻擊紀錄 ●**啟用備援機制**或變更頻寬 ●**依攻擊特徵，設置阻擋規則** ●協請 ISP 業者或 DDoS 防禦廠商協助清洗攻擊流量 ●攻擊情況緩解後，復原資訊設備運作與設定	●紀錄事件處理過程 ●紀錄事件解決方案 ●檢討事件處理經過，提出改善方案

DDoS 攻擊應變與防護_ISP協防

DDoS 攻擊應變與防護_中央機關

- 面對大規模 DDoS 攻擊事件，透過國家資通安全會報**整合各部會資源**，邀集相關單位協助政府機關盡速回復正常運作
  - 攻擊來源與手法調查
    - 由**技服中心**偕同**調查局**與**刑事局**成立「技術調查小組」，蒐集相關攻擊紀錄，調查攻擊來源與手法
  - 攻擊來源阻擋
    - 技術調查小組分析資訊包含攻擊來源與手法，此階段應將**相關資訊通報國內/國際組織**，並**適度公告分析資訊**，以利政府機關進行阻擋
    - 國發會與通傳會應將相關資訊，轉請 **ISP 業者進行阻擋與相關防護措施**
  - 關鍵(資訊)基礎設施阻擋與防護
    - 避免遭惡意攻擊事件影響，應加強關鍵(資訊)基礎設施防護作業，除**依攻擊資訊進行阻擋**外，亦須確認**備援機制可正常啟用**

結論

結論

- DDoS 攻擊種類眾多，其防禦方式不可寄望於單一方案，必須先行研判攻擊種類才能選擇適合之防禦方式
- 其他相關防禦考量重點：
  - 建置多層次過濾防護
  - 提升伺服器安全 (DNS、NTP 等)
  - 落實 BCP 與 DRP
  - 設計多重網路出口
  - 建立與 ISP 業者之緊急聯繫管道
  - 定期執行弱點更新與系統效能調校
  - 進行流量監控與建立緊急應變程序

報告完畢
敬請指教