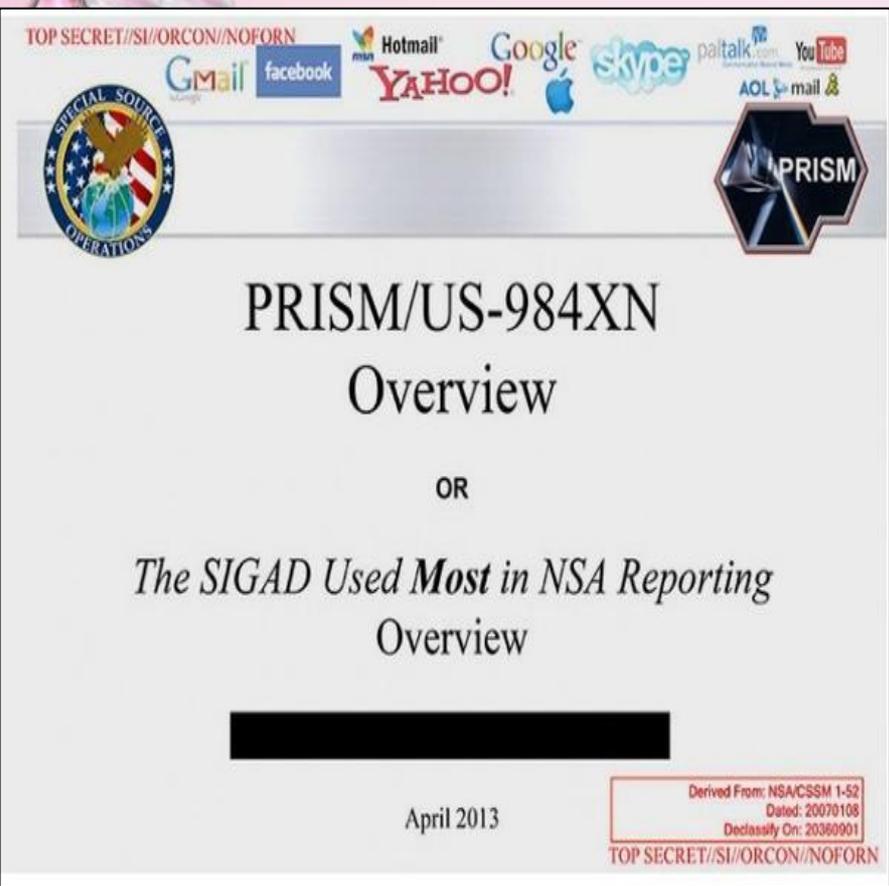




資安案例分享



世界級電子監聽計畫：美國稜鏡計畫



PRISM(稜鏡計畫) 是美國最高機密等級之電子監聽計畫，由美國國家安全局 (NSA) 以反恐名義實施，所追蹤的內容包括了照片、音訊、視訊、電郵、語音交談、檔案傳輸、帳號登入等等，對於人們隱私影響鉅大

參與PRISM的網路巨頭包括了Microsoft, Google, Yahoo!, Facebook, PalTalk, YouTube, Skype, AOL, Apple.

PRISM資料量蒐集前三名
伊朗：共收集140億則情報
巴基斯坦：共收集135億則情報
約旦：共收集127億則情報

PRISM(稜鏡計畫)外流之簡報首頁



大規模簡訊蒐集民意：太陽花學運

 太陽花反服貿！ 全民反核四！街頭意志愈加壯大 百萬「紅衫軍」會不會再現？扁政府賴權 馬政府低頭 如果執政部門不能滿足民眾訴求，下一次，你是否會走上街頭 ? 參與臉書投票，表達真實意願

<http://vote.tw.am/?id=3&d=63qMO,eX,44dc37>

 大嘴鄭重公告，上一輪投票中，54.1%的民眾選擇"徹底停止核四建設"！

  感謝表明態度的你！



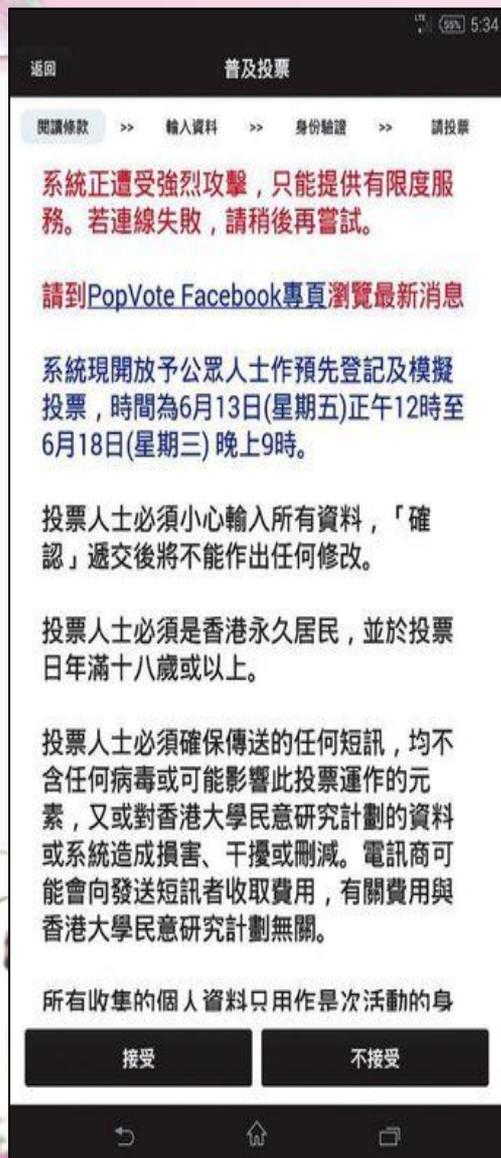
IP	時間	電話	回應
723	2014/4/30		所謂的開放 並不等於入侵 服貿是為了讓貿易更加順暢 減少許多貿易上的壁壘 對於進出口是有9b
724	2014/4/30		投票真有用馬英九早就回應林飛帆 玩笑了嗎? 9b
725	2014/4/30		過 63l
726	2014/4/30		經濟流通較活絡 9b
727	2014/4/30		小朋友不要再玩了 9b
728	2014/4/30		台灣加油! 9b
729	2014/4/30		開放是唯一的 路 63l
730	2014/4/30		服貿過了人民等於死了 9b
731	2014/4/30		沒道理不過 9b
732	2014/4/30		黑箱決議並不能呈現真正的民意，請選給人民真正的民主價值。 9b
733	2014/4/30		We aren't scare of competitions, bring it on 9b
734	2014/4/30		服貿若死，下一代草莓也將等死 9b
735	2014/4/30		死冥燻黨不要因自己選不上，就一直找執政黨麻煩一直大吵大鬧，什麼事就故意因反對而反對 61
736	2014/4/30		馬英九 幹你娘 9b
737	2014/4/30		不能過！自經區也該再重省查！ 9b
738	2014/4/30		台灣獨立 9b
739	2014/4/30		服貿本質就不是國與國之間的關係在協商 而且還不僅僅這樣 9b
740	2014/4/30		為何沒第三種選擇 9b
741	2014/4/30		官逼民反 9b
742	2014/4/30		開放才有錢途 9b
743	2014/4/30		統一完成中國富強人民幸福 63l
744	2014/4/30		林飛帆，最好沒有政治操作！ 9b
745	2014/4/30		臺灣別他媽再犯蠢了！已經連韓國一般都不如了！對岸都有原子彈，你反正也打不贏，還不如 9b
746	2014/4/30		既然當政就尊重執政者，吵什麼吵。阿扁當年還不是我行我素，有聽、有鳥、有回應紅衫軍於 9b
747	2014/4/30		相關應有的法規如果有設立、修改服貿相關條約，服貿就有機會可以讓全台人民心服口服的選 9b
748	2014/4/30		是誰用何方式強逼人民展開公投 噁心死了 9b
749	2014/4/30		我好帥 9b
750	2014/4/30		服貿不過無所謂。 凡是都有一體兩面 過與不過都有好有壞。重點是法的通過須符合程 9b
751	2014/4/30		退回服貿 9b
752	2014/4/30		服貿不過台灣只有向下沉淪 9b
753	2014/4/30		不要再口口聲聲說你代表台灣人民。每個人只能代表自己。 9b
754	2014/4/30		服貿 如果不通過 台灣怎跟人競爭? 9b
755	2014/4/30		反服貿之名，行台獨之實，當我們是白痴啊 9b
756	2014/4/30		台灣要向前走，要有競爭力，要再次創造經濟。 9b
757	2014/4/30		不簽代表我們不是國家，已經和大陸統一。簽了代表我們是個獨立國家，合作需經我們同意。 9b
758	2014/4/30		沒有服貿會失信於國際，還有誰會與台灣締結任何協定? 9b
759	2014/4/30		投票很有意義 9b
760	2014/4/30		少數人占立法院，其實不能代表我發聲 63l
761	2014/4/30		過了~經濟才過的了，太多短視近利，唯有跳出框架才能大部向前 9b
762	2014/4/30		請你把數據公佈 黨工 辛苦你了 61l
763	2014/4/30		亂糟糟這套民進黨專屬，國民黨學不會，因為民粹政治這招是向共產黨取經的，民進黨太像以 9b
764	2014/4/30		台獨必敗！炎黃子孫，中華民族大團結！ 9b
765	2014/4/30		只要走出去才會有希望，我們對自己要有要求也願意提升自己，絕對可以跟別人一起競爭。讓更 9b
766	2014/4/30		請服從多數選出來的總統和立委，不要再自以為代表民意了，也不要自以為在拯救台灣的未來 9b
767	2014/4/30		經濟 61l
768	2014/4/30		經濟 61l
769	2014/4/30		我愛我的國家更忠誠台灣，服貿問題不應泛政治化，理應回歸於經濟發展，就新加坡為例，政 9b

Source: Devco.re與北區ASOC整理





香港民間全民投票PopVote



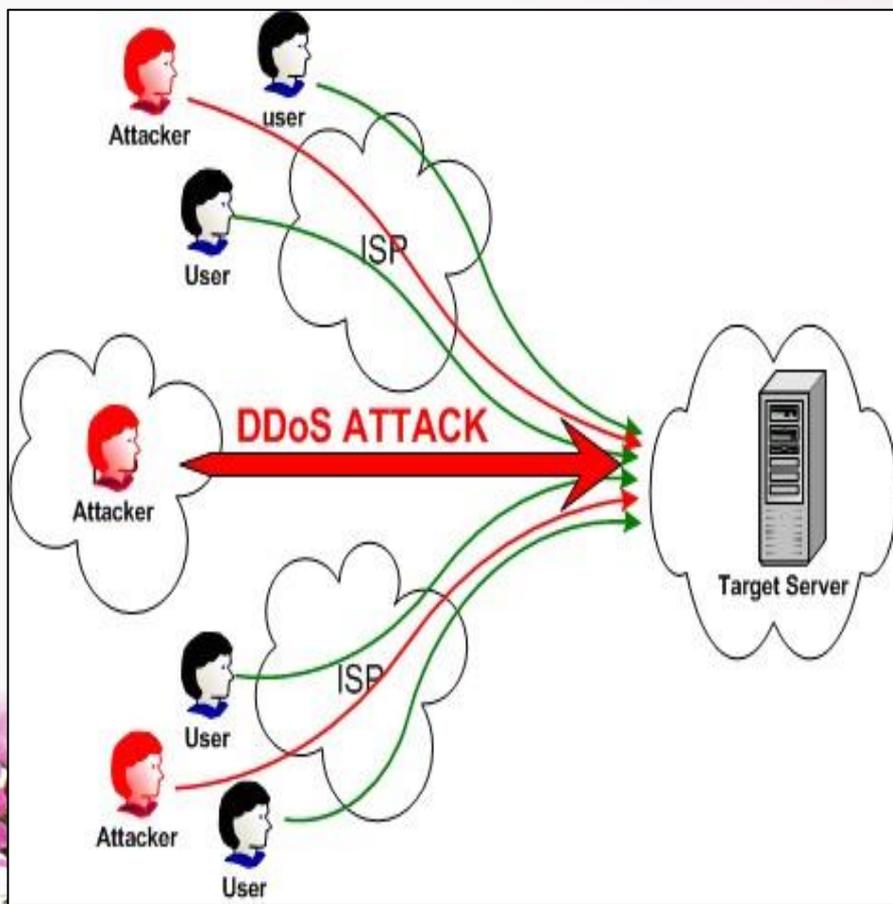
6/20-6/29香港大學與香港理工大學合作舉辦民間全民投票(PopVote)，表決2017特首選舉與政府方案不符國際標準讓選民有真正選擇，香港立法會應予否決，此全民投票資訊提供予香港政府參考。

PopVote線上投票網站陸續遭受到破記錄的大量DDoS攻擊，攻擊流量高達每秒300Gb(全世界最強的攻擊紀錄是每秒鐘400GB)。

攻擊流量之大連香港當地ISP網路服務供應商都無法承受；攻擊活動中採用多重攻擊手法，造成該網站一度無法正常運作。



針對特定言論攻擊：PTT遭受107部 殭屍電腦攻擊



批踢踢實業坊是台灣一個網路論壇，簡稱 PTT，採用電子佈告欄系統架設，目前在 Ptt / Ptt2 註冊總人數約一百五十萬人，尖峰時段兩站超過十五萬名使用者同時上線。

8/27 20:45分PTT網站遭受國外100多個 IP 以DDoS方式攻擊，最高流量接近 1Gbps，攻擊者幾乎來自中國。

今日網路技術可在幾秒內發動大量電腦攻擊，直接阻斷目標網站流量，使網站無法對外提供資訊，且攻擊多為跨境，單一國無法解決。

手持裝置案例：小米機蒐集使用者相關資訊

小米手机2

28纳米全球首发，发烧级四核手机

堪比XBOX 360游戏机的图形性能
2GB大内存，4.3英寸IPS超高PPI精度视网膜屏
新一代800万像素背照式相机
应有尽有！

¥1999

了解更多

9月18日工程机预订，10月正式上市



今年八月份，台灣知名網路雜誌 iThome 測試小米手機，發現手機的國際行動用戶辨識碼 (IMSI) 資訊，及手機序號 IMEI 號碼和電話號碼，都傳送到 api.account.xiaomi.com 伺服器(位於北京)。

現今中國對臺灣仍是保持政治敵意的態度，這些行銷手法、廣告包裝，讓資安意識不若資安專家的一般民眾，輕忽了可能的風險，也看不見可能的資安風險和威脅。

若中國政府掌握臺灣政治人物的通話紀錄等，如果其中隱含不法行為，中國政府就可以拿此資料，以要脅甚至控制臺灣政治人物，藉以左右臺灣政局。

Source: ithome.com.tw 與北區ASOC整理



手持裝置案例：觸寶輸入法 (Android)

觸寶輸入法為大陸觸寶公司所推出的輸入法，目前針對Android以及iOS兩大移動裝置平臺皆有推出相關輸入法。



北區ASOC此次是針對Android平臺中的觸寶輸入法於獨立的環境中進行封包側錄與分析，而在一開始安裝觸寶輸入法時，即可發現觸寶輸入法向系統要求許多特殊權限，而一旦安裝後，亦會透過明碼傳輸方式，將使用者所使用的移動裝置型號，作業系統版本，甚至IMEI等資訊回傳至外部伺服器。

由於Android作業系統平臺相較於Apple iOS，對於各app存取權限管理相對寬鬆，故建議Android平臺使用者若擔心移動裝置中的機敏資料有外洩之疑慮，可在安裝app時，仔細閱讀app所要求之權限，避免給與過大之權限進而導致機敏資料外洩。

手持裝置案例：觸寶輸入法(Android)

```
Stream Content
1 POST /forward/both/ws2/auth/activate HTTP/1.1
Content-Length: 670
Content-Type: text/plain; charset=UTF-8
Host: ime2.service.cootek.com
2 Connection: Keep-Alive
User-Agent: TouchPalv5 (C6802 14.4.A.0.108)
3 {"physical_size": "6.62", "locale": "zh-
4 t", "imei": "357656051325890", "android.version": "5643", "resolution": "1824*1080", "channel_cod
5 e": "000000", "sys_app": false, "device_info": "C6802", "app_name": "cootek.smartinput.interna
6 tional.android.public", "investigate_timestamp": "1407739937392", "point": "CNT
7 (v)", "send_time": "1407739937392", "consume_time": "0", "success_time": "0", "build_id": "0", "pid": "144
8 53", "uid": "35977ab-8c0e-4f80-8b92-6a392811a336", "rid": "14504", "last_timestamp": "0", "consume
9 _time_inter": "0", "os_version": "4.4.4", "os_name": "Android", "manufacture": "sony", "recomme
10 nd_channel": "000000", "dpi": "320", "identifier": "357656051325890##4c:21:d0:4e:f3:e0"}
HTTP/1.1 200 OK
Date: Mon, 11 Aug 2014 06:59:09 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 48
Connection: keep-alive
Server: TornadoServer/2.4.1
Set-Cookie: auth_token=56eb5904-f51f-4129-94ba-d63e46ebf4d6; Path=/
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: HEAD,OPTIONS,GET,POST,PUT,DELETE
Access-Control-Allow-Headers: Content-Type,Server,Date,Content-Length,Cache-
Control,Keep-Alive,Connection,X-Requested-With,X-File-Name,Origin,Accept
Access-Control-Max-Age: 1728000
Expires: Mon, 11 Aug 2014 06:59:08 GMT
Cache-Control: no-cache

{"recommend_channel": "000000", "error_code": 0}GET /forward/both/ws2/auth/info
Entire conversation (2818 bytes)
```



- 1.)利用http post明碼向外步傳送資訊。
- 2.)user-agent包含使用者手機型號及作業系統版本
- 3.)IMEI資訊
- 4.)手機螢幕解析度

- 5.)手機型號
- 6.)設備時間
- 7.)作業系統名稱、版本、廠牌
- 8.)網卡mac address

#觸寶輸入法於Android安裝時所要求之權限



H-worm 初步分析報告

簡介

操作介面

H-worm為北區A-SOC近期所偵測到的大量感

染事件，故深入分析此蠕蟲感染途徑，行為模式及防範措施。

H-worm為一透過VBS(*visual basic script*)所撰寫的

RAT(*Remote Access Trojans*)木馬，此類型木馬相較於其他

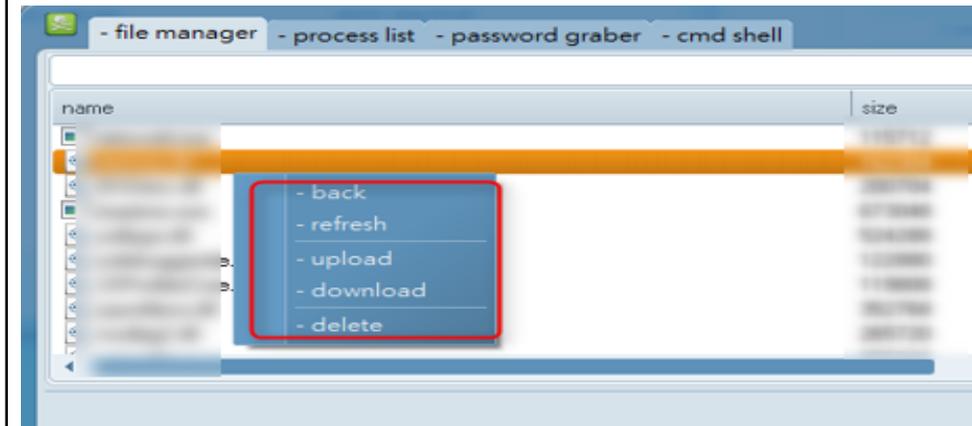
類行的木馬，不同之處在於特別著重在遠端操控受害

者電腦，一旦主機遭感染，攻擊者將可透過C&C

server與受害主機連線，瀏覽受害主機的檔案，讀取記

憶體中執行的process，側錄密碼資訊，甚至可以透過

cmd shell方式操作受害主機。



※攻擊者可遠端瀏覽受害主機相關檔案

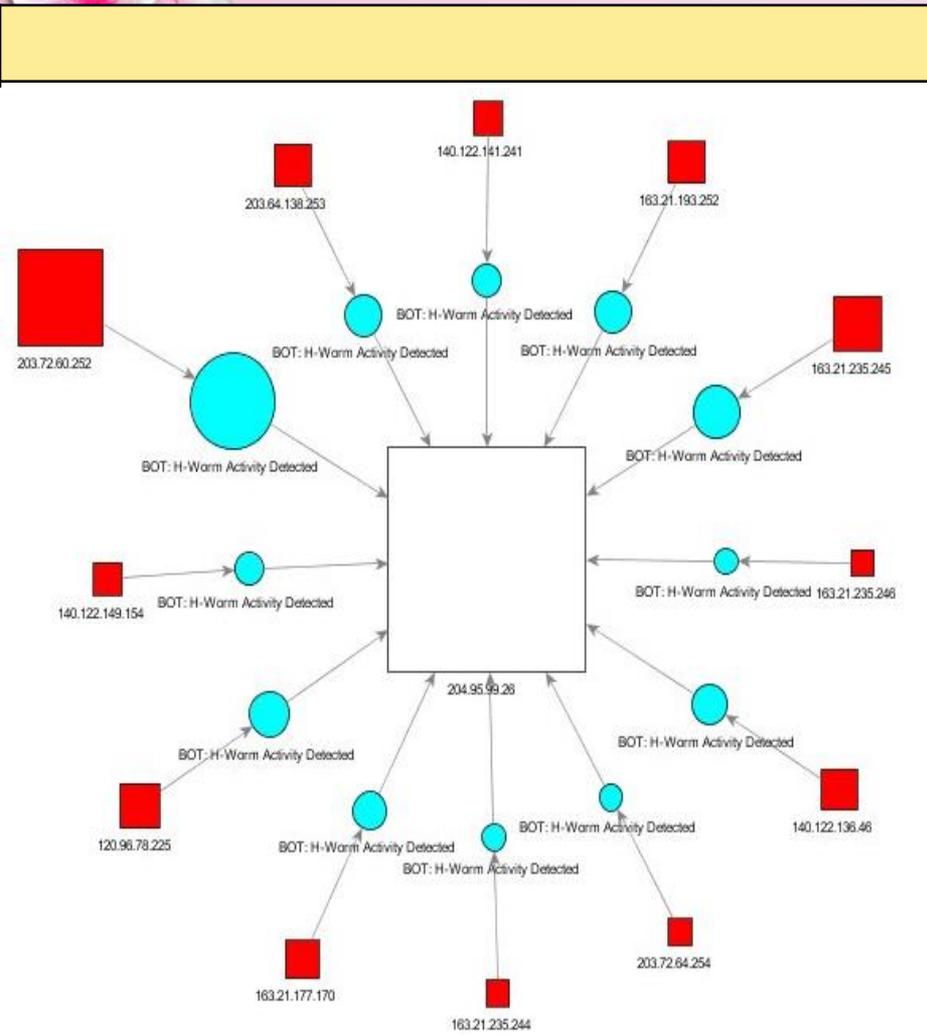


※攻擊者可遠端瀏覽受害主機相關檔案

Source : 北區ASOC整理



H-worm 初步分析報告



Follow TCP Stream

```

Stream Content
POST /is-ready HTTP/1.1
Accept: */*
Accept-Language: zh-tw
User-Agent: [D6DB5851<|>ALLE-PC<|>alle<|>Microsoft windows 7 ..... <|>
>underworld final<|>nan-av<|>true
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
Host: [1ovesyr.sytes.net:8844]
Content-Length: 0
Connection: Keep-Alive
Cache-Control: no-cache
  
```

C&C Server Address

Entire conversation (322 bytes)

Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw

Help Filter Out This Stream Close

※北區ASOC目前偵測H-worm感染概況

※受感染主機向C&C server通訊之封包
Source : 北區ASOC整理





電子郵件 社交工程攻擊(案一)

寄件者: 謝繼昌

寄件日期: 2014/8/13 (週三) 下午 11:40

收件者:

副本: litingying@will.m1.ntu.edu.tw; litolin@will.m1.ntu.edu.tw; wu_zheng_lu_ying@will.m1.ntu.edu.tw; mno2@wlan95.cc.ntu.edu.tw; jjlee@xtal.ch.ntu.edu.tw; boswell.bbs@zoo.ee.ntu.edu.tw; bs@zoo.ee.ntu.edu.tw; chabird.bbs@zoo.ee.ntu.edu.tw; daymoon.bbs@zoo.ee.ntu.edu.tw; dodo0919.bbs@zoo.ee.ntu.edu.tw; fanamo.bbs@zoo.ee.ntu.edu.tw; fujiran.bbs@zoo.ee.ntu.edu.tw; honorguard.bbs@zoo.ee.ntu.edu.tw; icecube.bbs@zoo.ee.ntu.edu.tw;

主旨: 技術支持團隊

親愛的台大 Mail 帳戶的用戶，

我們的技術服務部正在開展有計劃的軟件 upgrade.Please 點擊這裡重新確認您的帳戶。

<http://hldesk.esy.es/>

該指令已被送往台大所有郵件帳戶的用戶和必須遵照。

謝謝，

IT 服務台支持

©版權所有 2014 年，系統管理員的技術支持團隊，並保留所有權利



電子郵件 社交工程攻擊(案一)

IT-服务台 IT-Help Desk

更新您的帐户 Update Your Account

全名 Full Name:

电子邮件地址 Email Address:

帳號 Account :

密碼 Password :

确认密码 Confirm password:

Sign in

版權所有©計算機與信息Networking中心，所有的Righte保留。
Copyright©Computer and information Networking Center, ALL Righte Reserved.



電子郵件 社交工程攻擊(案二)

https://mail.ntu.edu.tw/owa/?ae=Item&a=Open&t=IPM.Note&id=RgAAAAC2s3aW8

回覆 全部回覆 轉寄



faculty and staff

"National Taiwan University"

ntumail.yolasite.com

至: 台大計中

點擊 [MyNTU](#) 查看您的帳

Copyright © 2006 臺灣

10617 臺北市羅斯福路

WELCOME TO NTU WEBMAIL

台大WEBMAIL帳戶狀態

電子郵件

Username | 用戶名:

PasswOrd | 密碼

[查看帳戶狀態](#) | View

FAQ : [Web Mail User Manual](#),

[Improve web mail login speed-HOWTO](#)





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

➤ 請參考:

http://cert.ntu.edu.tw/Module/Security/social_engineering.php



Thank You !

Q & A