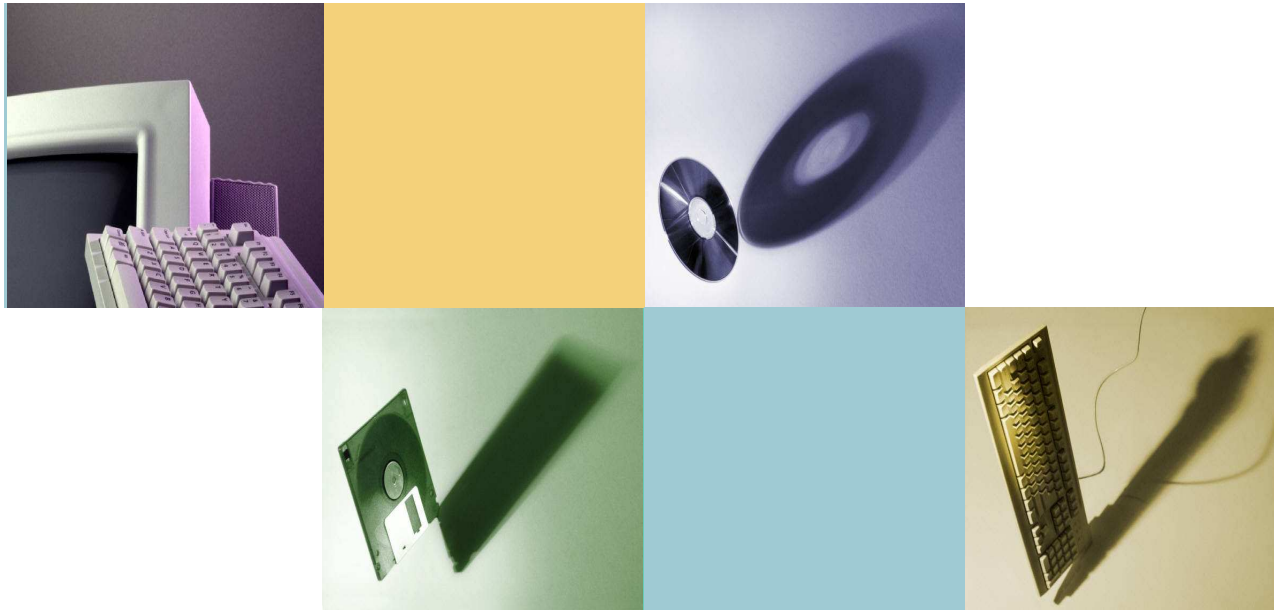


資安事件通報程序

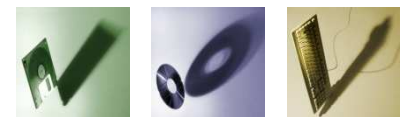


Wednesday, Jun 20 2012

曾國旭

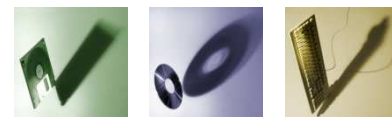
資安事件分級

- 依影響程度分成4個等級，說明如下：
- 符合下列任一情形者，屬4級事件
 - 國家機密資料遭洩漏
 - 國家重要資訊基礎建設系統或資料遭竄改
 - 國家重要資訊基礎建設運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作
- 符合下列任一情形者，屬3級事件
 - 密級或敏感公務資料遭洩漏
 - 核心業務系統或資料遭嚴重竄改
 - 核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作



資安事件分級(續)

- 符合下列任一情形者，屬2級事件
 - 非屬密級或敏感之核心業務資料遭洩漏
 - 核心業務系統或資料遭輕微竄改
 - 核心業務運作遭影響或系統效率降低，於可容忍中斷時間內回復正常運作
- 符合下列任一情形者，屬1級事件
 - 非核心業務資料遭洩漏
 - 非核心業務系統或資料遭竄改
 - 非核心業務運作遭影響或短暫停頓
- 資安事件於發生後1小時內須通報，1、2級事件需於72小時內處理完成並結案(包括通報與應變)，3、4級事件需於36小時內完成。



教育機構資安通報平台

⇒ <https://info.cert.tanet.edu.tw/>

The screenshot shows the website interface for the Education Institution Security Incident Reporting Platform. The browser window title is "教育機構資安通報平台 - Windows Internet Explorer". The address bar shows the URL "https://info.cert.tanet.edu.tw/prog/index.php". The website header features the TAnet CERT logo and the title "教育機構資安通報平台" with the subtitle "Ministry of education information & communication security contingency platform".

On the left side, there is a "會員登入" (Member Login) section with the following fields and options:

- 機關OID: 2 16 886 111 100317
- 登入密碼: [masked]
- 验证码: vfffx
- 登入: [button]
- [TACERT本學電子報](#)

The main content area has a navigation menu with "公告", "帳密更新Q&A", "常見問題Q&A", and "資安事件單錯誤回報Q&A". The "公告" (Announcement) section contains the following text:

教育部為求有效掌握教育部所屬之各級教育機構之資通訊及網路系統現況，避免各機關及系統遭受破壞與不當使用，預期能迅速通報及緊急應變處理，並在最短時間內回復，以確保各級教育機構之正常運作，因此本平台提供各級教育機構資安人員進行資安事件通報功能及應變處理。

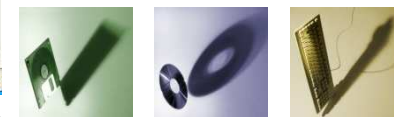
本平台之營運單位由臺灣學術網路危機處理中心(TACERT)進行服務

臺灣學術網路危機處理中心自2012年度起將於每季發佈「TACERT資安電子季報」於TACERT網站，將匯整當季學術網路資安事件類型趨勢、安全性公告、資安事件個案分析、重要資安新聞回顧等資訊，期能提供學術網路使用者學習資安知識與能力，共同加強學術網路的防護。

2012年第一季TACERT資安電子報：
<http://cert.tanet.edu.tw/pdf/TACERT2012Q1.pdf>

TACERT(臺灣學術網路危機處理中心)
服務電話：(07)525-0211
網路電話：98400000
E-mail：service@cert.tanet.edu.tw
網址：<http://cert.tanet.edu.tw/>

At the bottom of the page, it says "台灣學術網路危機處理中心(TACERT)".



教育機構資安通報平台(續)

教育機構資安通報平台 - Windows Internet Explorer

https://info.cert.tanet.edu.tw/prog/login.php

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

khtzeng@niu.edu.tw - 1232.8... 國立宜蘭大學 - 區縣(市)網... 教育機構資安通報平台

教育機構資安通報平台
Ministry of education information & communication security contingency platform

聯絡資訊

機關名稱: 國立宜蘭大學 使用者: 曾國旭	主管機關: 宜蘭區域網路中心 聯絡電話: 03-931-7126# E-Mail: khtzeng@niu.edu.tw	教育機構資安通報應變小組 聯絡電話: 07-525-0211 E-Mail: service@cert.tanet.edu.tw
--------------------------	--	--

回首頁
修改個人資料
登出

通報

- 通報/應變
- 自行通報
- 事件單處理狀態
- 歷史通報
- 事件附檔下載
- 資安預警事件

事件單編號	發佈時間	距通報時間(小時)	流程
Page 1/1			

當有通報資安事件時，
按一下事件單編號即可
進行通報程序

台灣學術網路危機處理中心(TACERT)

教育機構資安通報平台(續)

教育機構資安通報平台
Ministry of education information & communication security contingency platform

聯絡資訊

機關名稱: 國立宜蘭大學
使用者: 曾國旭

主管機關: 宜蘭區域網路中心
聯絡電話: 03-931-7126#
E-Mail: khtzeng@niu.edu.tw

教育機構資安通報應變小組
聯絡電話: 07-525-0211
E-Mail: service@cert.tanet.edu.tw

回首頁
修改個人資料
登出

通報

通報/應變
自行通報
事件單處理狀態
歷史通報
事件附檔下載
資安預警事件

事件單編號	發佈時間	距通報時間(小時)	流程
-------	------	-----------	----

Page 1/1

更改資安聯絡人資訊及
變更通行碼

台灣學術網路危機處理中心(TACERT)

教育機構資安通報平台(續)

教育機構資安通報平台 - Windows Internet Explorer

https://info.cert.tanet.edu.tw/prog/login.php

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

khtzeng@niu.edu.tw - 1232.8... 國立宜蘭大學 - 區縣(市)網... 教育機構資安通報平台

教育機構資安通報平台
Ministry of education information & communication security contingency platform

聯絡資訊

機關名稱: 國立宜蘭大學 使用者: 曾國旭	主管機關: 宜蘭區域網路中心 聯絡電話: 03-931-7126# E-Mail: khtzeng@niu.edu.tw	教育機構資安通報應變小組 聯絡電話: 07-525-0211 E-Mail: service@cert.tanet.edu.tw
--------------------------	--	--

回首頁
修改個人資料
登出

通報

- 通報/應變
- 自行通報**
- 事件單處理狀態
- 歷史通報
- 事件附檔下載
- 資安預警事件

事件單編號	發佈時間	距通報時間(小時)	流程
Page 1/1			

自行通報資安事件，例如資安預警事件經確認為正式資安事件，須由此進行通報

台灣學術網路危機處理中心(TACERT)

教育機構資安通報平台(續)

教育機構資安通報平台 - Windows Internet Explorer

https://info.cert.tanet.edu.tw/prog/login.php

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

khtzeng@niu.edu.tw - 1232.8... 國立宜蘭大學 - 區縣(市)網... 教育機構資安通報平台

教育機構資安通報平台
Ministry of education information & communication security contingency platform

聯絡資訊

機關名稱: 國立宜蘭大學 使用者: 曾國旭	主管機關: 宜蘭區域網路中心 聯絡電話: 03-931-7126# E-Mail: khtzeng@niu.edu.tw	教育機構資安通報應變小組 聯絡電話: 07-525-0211 E-Mail: service@cert.tanet.edu.tw
--------------------------	--	--

回首頁
修改個人資料
登出

通報

- 通報/應變
- 自行通報
- 事件單處理狀態
- 歷史通報
- 事件附檔下載
- 資安預警事件

事件單編號	發佈時間	距通報時間(小時)	流程
Page 1/1			

資安事件相關紀錄檔

台灣學術網路危機處理中心(TACERT)

網際網路 100%

教育機構資安通報平台(續)

教育機構資安通報平台
Ministry of education information & communication security contingency platform

聯絡資訊

機關名稱: 國立宜蘭大學
使用者: 曾國旭

主管機關: 宜蘭區域網路中心
聯絡電話: 03-931-7126#
E-Mail: khtzeng@niu.edu.tw

教育機構資安通報應變小組
聯絡電話: 07-525-0211
E-Mail: service@cert.tanet.edu.tw

回首頁
修改個人資料
登出

通報

通報/應變
自行通報
事件單處理狀態
歷史通報
事件附檔下載
資安預警事件

工單狀態

第一頁 | 上一頁 | 下一頁 | 最終頁

時間	發佈編號	IP	單位	來源	LOG附檔
Thu 14, Jun 2012	ASOC-EWA-201206-0378	120.101.36.57	國立宜蘭大學	S-ASOC	下載
Fri 01, Jun 2012	ASOC-EWA-201206-0014	120.101.41.49	國立宜蘭大學	S-ASOC	下載
Thu 10, May 2012	ASOC-EWA-201205-0245	120.101.12.59	國立宜蘭大學	S-ASOC	下載
Mon 07, May 2012	ASOC-EWA-201205-0182	120.101.37.168	國立宜蘭大學	S-ASOC	下載
Tue 01, May 2012	ASOC-EWA-201205-0010	120.101.9.133	國立宜蘭大學	S-ASOC	下載
Wed 25, Apr 2012	ASOC-EWA-201204-0561	120.101.10.199	國立宜蘭大學	S-ASOC	下載
Sun 22, Apr	ASOC-EWA-201204-	120.101.22.211	國立宜蘭	S-	下載

台灣學術網路危機處理中心(TACERT)



教育機構資安通報平台(續)

教育機構資安通報平台 - Windows Internet Explorer

https://info.cert.tanet.edu.tw/prog/login.php

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

khtzeng@niu.edu.tw - 1232.8... 國立宜蘭大學 - 區縣(市)網... 教育機構資安通報平台

教育機構資安通報平台
Ministry of education information & communication security contingency platform

聯絡資訊

機關名稱: 國立宜蘭大學 使用者: 曾國旭	主管機關: 宜蘭區域網路中心 聯絡電話: 03-931-7126# E-Mail: khtzeng@niu.edu.tw	教育機構資安通報應變小組 聯絡電話: 07-525-0211 E-Mail: service@cert.tanet.edu.tw
--------------------------	--	--

回首頁
修改個人資料
登出

通報

- 通報/應變
- 自行通報
- 事件單處理狀態
- 歷史通報
- 事件附檔下載
- 資安預警事件

事件單編號	發佈時間	距通報時間(小時)	流程
Page 1/1			

資安預警事件處理

台灣學術網路危機處理中心(TACERT)

教育機構資安通報平台(續)

教育機構資安通報平台 - Windows Internet Explorer

https://info.cert.tanet.edu.tw/prog/ewaindex.php

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

khtzeng@niu.edu.tw - 1232.8... 國立宜蘭大學 - 區縣(市)網... 教育機構資安通報平台

教育機構資安通報平台

Ministry of education information & communication security contingency platform

聯絡資訊

機關名稱: 國立宜蘭大學
使用者: 曾國旭

主管機關: 宜蘭區域網路中心
聯絡電話: 03-931-7126#
E-Mail: khtzeng@niu.edu.tw

教育機構資安通報應變小組
聯絡電話: 07-525-0211
E-Mail: service@cert.tanet.edu.tw

回首頁
修改個人資料
登出

通報

通報/應變
自行通報
事件單處理狀態
歷史通報
事件附檔下載
資安預警事件

EWA編號	單位名稱	事件等級	事件分類	狀態
ASOC-EWA-201206-0378	國立宜蘭大學	low	對外攻擊	誤報
ASOC-EWA-201206-0014	國立宜蘭大學	low	對外攻擊	誤報
ASOC-EWA-201205-0245	國立宜蘭大學	low	對外攻擊	誤報
ASOC-EWA-201205-0182	國立宜蘭大學	low	對外攻擊	誤報
ASOC-EWA-201205-0010	國立宜蘭大學	low	對外攻擊	誤報
ASOC-EWA-201204-0561	國立宜蘭大學	low	對外攻擊	誤報
ASOC-EWA-201204-0491	國立宜蘭大學	low	對外攻擊	誤報
ASOC-EWA-201204-0166	國立宜蘭大學	low	對外攻擊	誤報
ASOC-EWA-201203-0150	國立宜蘭大學	low	對外攻擊	無法判斷
ASOC-EWA-201203-0026	國立宜蘭大學	low	對外攻擊	無法判斷

Page 1/2

台灣學術網路危機處理中心(TACERT)

確認是否有「未處理」之工單

按工單編號進行預警事件處理

教育機構資安通報平台(續)

close or Esc Key

措施 2.利用工具程式於來源主機觀察，找出實際執行連線的程式，確認該程式是否為惡意程式。

參考資訊 本攻擊相關資訊可於下列網址
http://www.iss.net/security_center/reference/vuln/WINS_UDP_Pointer_Code_Exec.htm內查詢

EWA事件單狀態

誤判


確實事件

無法判斷

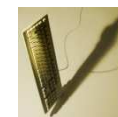
原因

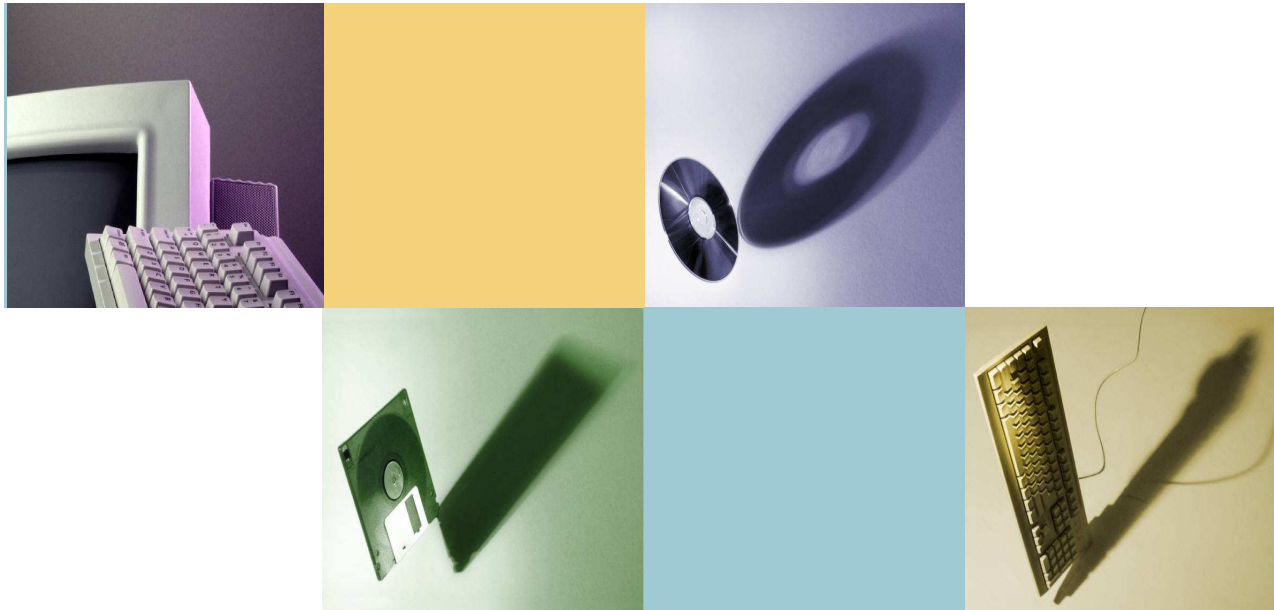
經比對防火牆紀錄，乃是使用teamviewer軟體，並非攻擊事件

送出



Q and A





THANKS !