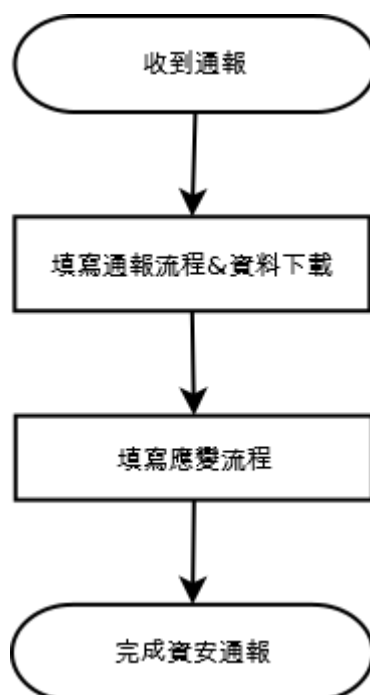



資安通報

收到教育部的資安通報時請登入 <https://info.cert.tanet.edu.tw> 教育機構資安通報平台進行結案流程如下圖



資安通報一共分成**通報**和**應變**兩部份，於收到資安通報後請於 **4 個小時**內完成通報程序，**36 小時**內完成應變(*1)，建議一次完成通報和應變，並針對問題主機進行停機或斷網處理。

以下為資安通報實例圖說：有標才  是必填

圖一、

詳細資料	
發佈編號	NTUSOC-INT-201410-0050
發佈時間	2014-10-02 08:24:00
事件類型	殭屍電腦(Bot)
事件主旨	教育部資安事件通告—國立暨南國際大學[163.22.2.2]主機進行惡意程式連線警訊通知
事件描述	來源IP可能主機弱點遭受駭客攻擊，且在背景連線並下載了惡意程式；或是主機已被入侵或植入木馬程式，並造成資訊外洩或成為殭屍網路一員而對外發動攻擊。入侵偵測防禦系統(B.22.2.2)，啟用包含木馬特徵之封包，對目標IP (多個目標IP) 進行封鎖 (多個來源PORT)，目標 PORT (多個目標PORT)。
處理建議	請檢視來源IP該連線行為是否已得到授權。若來源IP該連線為異常行為，可先利用掃毒軟體進行全系統掃描，並利用ACL暫時阻擋該可疑IP。同時建議管理者進行以下檢查：a. 請查看來源IP有無異常動作(如：新增帳號、開啟不明Port、執行不明程式)。b. 確認防毒軟體的病毒碼已更新為最新版本、系統已安裝相關修正檔，或關閉不使用的應用軟體與相關通訊埠。
參考資料	無

圖一

各機關因受外在因素所產生資通安全事件時通報事項：

以下表單各欄位若為紅色◎標示，則為必填欄位
欄位中不得輸入特殊符號，例如：「;」、「"」、「'」、「\$」、「&」、「%」、「!」、「^」、「*」、「<」、「>」、「_」、「|」、「-」

1. 通報型態：**告知通報**

2. ◎事件發生時間： 2014-10-02 08:24:00

填入上圖被檢舉的 IP 位址

◎IP位置 (IP address) :
範例: 120.114.22.33

◎網際網路位置 (web-url) :
範例: https://www.xxx.com/

◎設備廠牌、機型：
範例1: 華碩TS100 E6
範例2: Acer AT110 F1

直接填寫問題電腦的作業系統

◎作業系統 (名稱/版本) :
範例1: Centos Linux 5.4,
範例2: Windows XP SP2

◎受駭應用軟體 (名稱/版本) :
範例: sendmail server, 此為不確定版本的範例

◎已裝置之安全防護軟體:

防毒軟體 (名稱/版本): 無
範例: Avira 10.0.0.561

防火牆 (名稱/版本): 無
範例: iptables, 此為不確定版本的範例

IPS/IDS (名稱/版本): 無
範例: snort 2.8.3

其它 (名稱/版本): 無

4. 資通安全事件：基本資料

◎事件分類：

- INT (入侵攻擊) :
- 系統被入侵(資訊設備遭惡意使用者入侵)
 - 對外攻擊(對外部主機進行攻擊行為)
 - 針對性攻擊
 - 駭客攻擊
 - 中斷服務
 - 電腦病毒
 - 工程攻擊
 - 垃圾郵件(Spam)(資訊設備從事Spam Mail散播行為)
 - 命令與控制伺服器(C&C)(主機疑似為駭客之Botnet C&C Server)
 - 殭屍電腦(Bot)(資訊設備疑似成為駭客所控制之Botnet成員)
 - 其它類型的入侵攻擊

請選擇圖一所寫的事件類型

資安事件等級判斷（事件通常為 1、少數為 2 級，此部分非必要請勿隨意變更其級數）

5. 資通安全事件：影響等級及說明	
1. 事件等級：取底下三個欄位中最高等級當成最後之事件等級 2. 第3、4級事件係屬於重大資安事件，教育部各長官需親自督導進度 3. 若有3、4級事件，請立刻電話告知您所屬的主管機關 4. 如果您無法確定如何填寫時，請電話連絡您所屬的主管機關請求協助 5. 等級0之資安事件教育部另有規範，請至少填入等級1	
<input checked="" type="radio"/> 資安事件判斷：	
(1) 機密性衝擊 -	<input checked="" type="radio"/> 1級-非核心業務資料遭洩漏 <input type="radio"/> 2級-非屬密級或敏感之核心業務資料遭洩漏 <input type="radio"/> 3級-密級或敏感公務遭洩漏 <input type="radio"/> 4級-國家機密資料遭洩漏
(2) 完整性衝擊 -	<input checked="" type="radio"/> 1級-非核心業務系統或資料遭竄改 <input type="radio"/> 2級-核心業務系統或資料遭輕微竄改 <input type="radio"/> 3級-核心業務系統或資料遭嚴重竄改 <input type="radio"/> 4級-國家重要資訊基礎建設系統或資料遭竄改
(3) 可用性衝擊	<input checked="" type="radio"/> 1級-非核心業務運作遭影響或短暫停頓 <input type="radio"/> 2級-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 <input type="radio"/> 3級-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 <input type="radio"/> 4級-國家重要資訊基礎建設運作影響或系統停頓，無法於可容忍中斷時間內回復正常運作
資安事件綜合評估等級：	<input type="text" value="1級"/>
<input checked="" type="radio"/> 可能影響範圍及損失評估	(文字勿超過200字，)
<input type="text"/>	

此部份比較重要的是第 7 點，整個資安通報須要完成 1~5 的通報和 6~7 的應變才算完成資安通報的結案，**如果選否則須要另外再登入系統結案**

6. <input checked="" type="radio"/> 是否需要支援?	
<input type="radio"/> 是 你的上層機關負責人為： 陳彥良 聯絡電話： 049-600-3100#4041 E-mail： yenlchen@ncnu.edu.tw 期望支援方式： <input type="radio"/> 電話告知 <input type="radio"/> Email告知	<input checked="" type="radio"/> 否:通報單位自行解決
7. <input checked="" type="radio"/> 是否同時進行通報流程與應變流程?	
<input checked="" type="radio"/> 是 (請繼續完成 II.應變流程之作業)	<input type="radio"/> 否 (會先完成 I.通報流程 並結束，後續時間請儘快完成 II.應變流程)

收到通報後如何找到詳細資訊找出問題主機？

可以在系統內『事件附檔下載』下載事件檔，如下圖：

回首頁	工單狀態					
修改個人資料	事件單、EWA發佈編號或事件單編號 <input type="text"/> <input type="button" value="搜尋"/>					
登出	第一頁 上一頁 下一頁 最終頁					
通報	時間	發佈編號	IP	單位	來源	LOG附檔
事件審核	hu 09, Oct 2014	NTUSOC-INT-201410-0285	163.22.18.57	國立暨南國際大學	N-ASOC	下載
新進告知通報	ed 08, Oct 2014	NTUSOC-INT-201410-0225	163.22.18.50	國立暨南國際大學	N-ASOC	下載
事件單處理狀態	ue 07, Oct 2014	NTUSOC-INT-201410-0199	163.22.18.21	國立暨南國際大學	N-ASOC	下載
逾時事件單	ue 07, Oct 2014	NTUSOC-INT-201410-0204	163.22.175.1	私立五育高級中學	N-ASOC	下載
歷史通報	ue 07, Oct 2014	NTUSOC-INT-201410-0216	163.22.18.71	國立暨南國際大學	N-ASOC	下載
事件附檔下載	on 06, Oct 2014	NTUSOC-INT-201410-0137	163.22.18.56	國立暨南國際大學	N-ASOC	下載
資安預警事件						

下載下來的檔案通常有 html 及 png 兩個檔案，我們要的資訊通常在 html 檔裡面，png 檔則是他攻擊的手法圖示。

名稱	修改日期	類型	大小
0000427908	2014/10/2 上午 0...	Firefox HTML Do...	14 KB
0000427908	2014/10/2 上午 0...	PNG 影像	12 KB

點選 html 檔，請看他的『名稱』這個欄位，區網有整理常見的攻擊行為，可以至 <http://netcenter.ncnu.edu.tw/~yenlchen/>查詢，對事件內容仍有疑慮或須要協助請來電 049-2910960#4048 彥良。

發生次數: 2									
#s	開始時間	名稱	來源 IP	來源 Port	來源地區名	目的 IP	目的 Port	目的地區名	集合事件數
1	2014/10/01 17:36:38	MALWARE-CNC Torpig bot sinkhole server DNS lookup	163.22.2.2	28503	Taiwan	168.95.1.1	53	Taiwan	1
2	2014/10/01 17:36:39	MALWARE-CNC Torpig bot sinkhole server DNS lookup	163.22.2.2	26308	Taiwan	168.95.192.1	53	Taiwan	1

如果有問題的電腦並非伺機器可以考慮以關機拔網路線後再掃毒，如果有特殊狀況須要協助請來電 049-2910960#4048 彥良