臺灣學術網路 電腦危機處理中心

學術網路安全趨勢分析
與
資安個案分享

TAIWAN ACADEMIC NETWORK COMPUTER EMERGENCY RESPONSE TEAM

臺灣學術網路
電腦危機處理中心
TACERT

Tel: 07-5250211 Fax: 07-5250212
VoIP代表號：98400000
service@cert.tanet.edu.tw
804高雄市鼓山區蓮海路70號

cert.tanet.edu.tw
TACERT

課程大綱

- TACERT中心簡介
- 學術網路資安事件統計
- 教育機構資安通報流程簡介
- 平台功能介紹
- 通報演練簡介
- 攻擊趨勢分析與個案分享
- Q & A

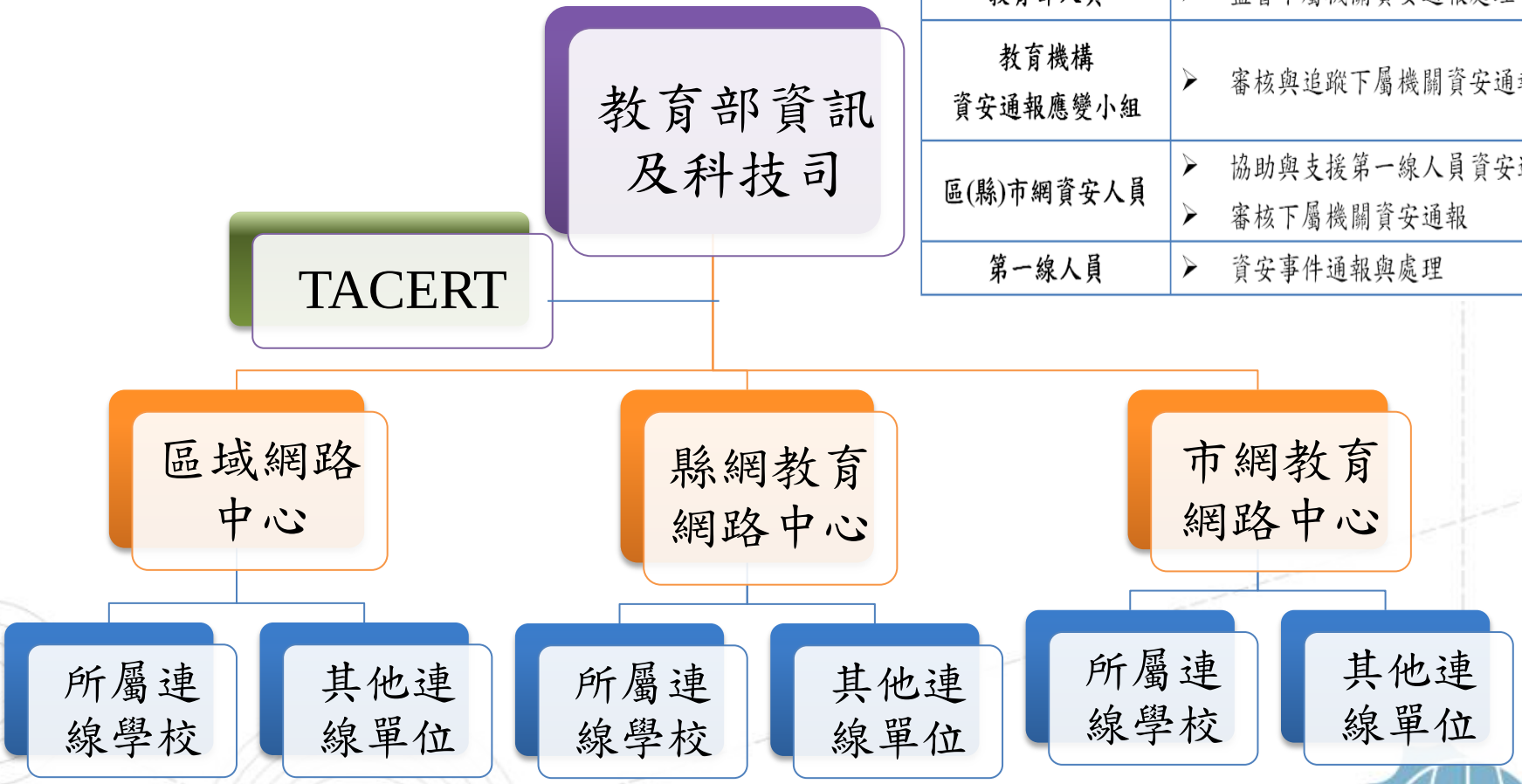
TACERT中心簡介

臺灣學術網路危機處理中心(TACERT)成立緣起

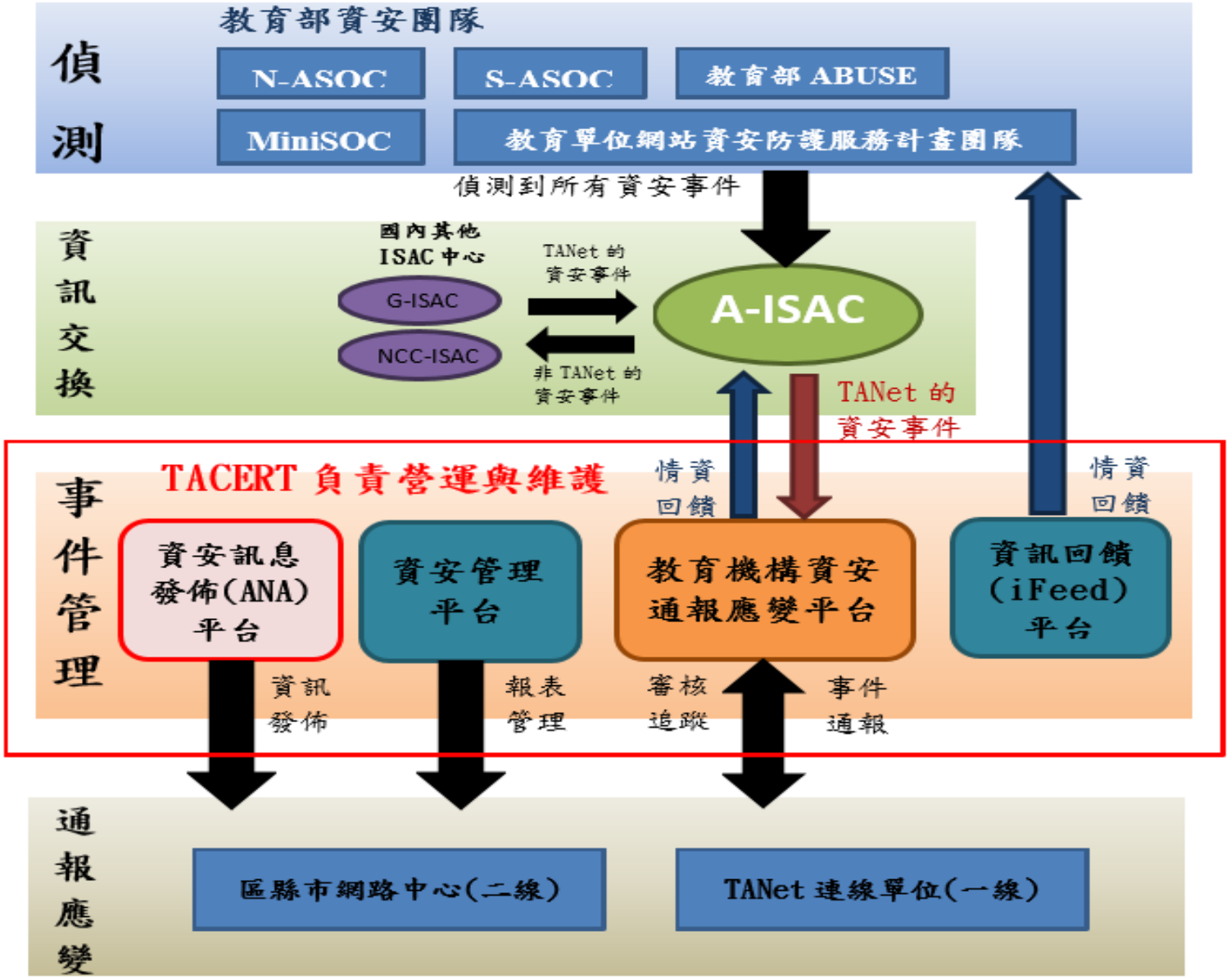
- 學術網路近年來成為臺灣網路攻擊的主要目標之一
- 面對層出不窮、日新月異的網路攻擊事件，需要有一個共同平台進行資安事件通報及應變
- 故教育部資訊及科技教育司(原教育部電算中心)成立***臺灣學術網路危機處理中心***(Taiwan Academic Network Computer Emergency Response Team)，簡稱**TACERT**，並委由國立中山大學營運。
- 臺灣學術網路危機處理中心將致力於強化學術網路資通安全的防護力，形成臺灣網路資安防護網重要的一環。

TACERT組織架構

使用角色	工作事項
教育部人員	➢ 監督下屬機關資安通報處理
教育機構 資安通報應變小組	➢ 審核與追蹤下屬機關資安通報
區(縣)市網資安人員	➢ 協助與支援第一線人員資安通報 ➢ 審核下屬機關資安通報
第一線人員	➢ 資安事件通報與處理



教育機構資安通報機制運作



TACERT中心營運目標

- 臺灣學術網路危機處理中心(TACERT)
- 專線：07-5250211　網站：cert.tanet.edu.tw
- 服務信箱：service@cert.tanet.edu.tw

資安事件階段處理目標

事前預防

- 資安預警情資
- 提供資安訊息、新知
- 辦理資安防護教育訓練

事發控制

- 自動化通報應變平台
- 完整資安通報流程機制
- 即時資安諮詢服務

事終檢討

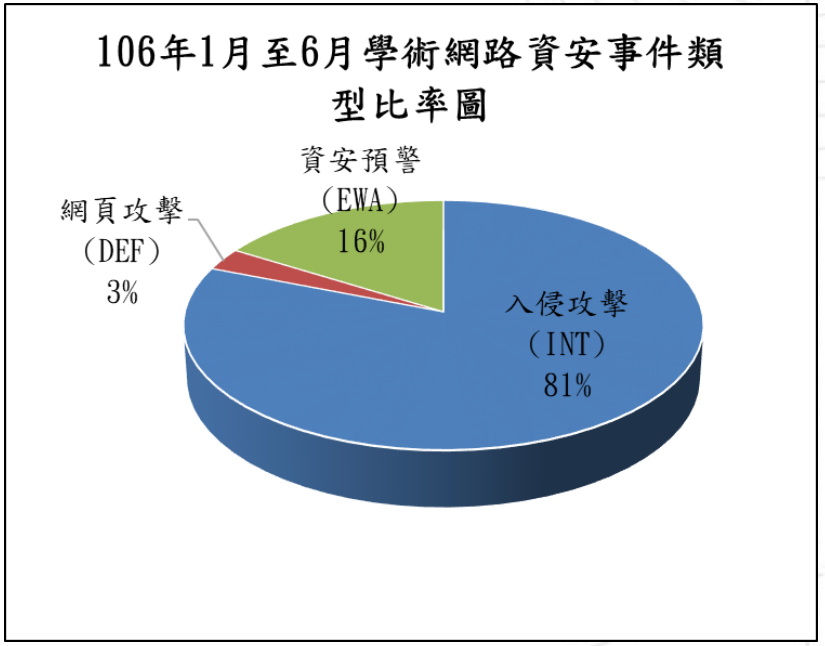
- 資安事件分析報告
- 資安事件處理教材
- 加強安全性與防護設定

106年學術網路資安事件統計

學術網路資安事件類型比例

■ 統計時間：106年1月至106年6月

事件類型	數量
入侵攻擊(INT)	11,564
網頁攻擊(DEF)	412
資安預警(EWA)	2,313
總計	14,289

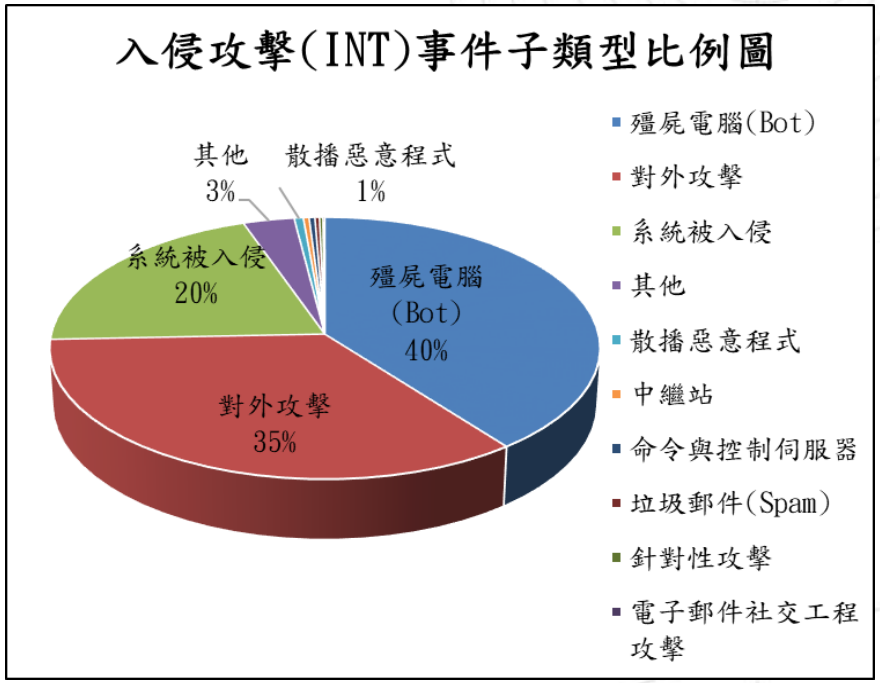


■ 資料來源：教育機構資安通報平台

學術網路資安事件INT子類型比例

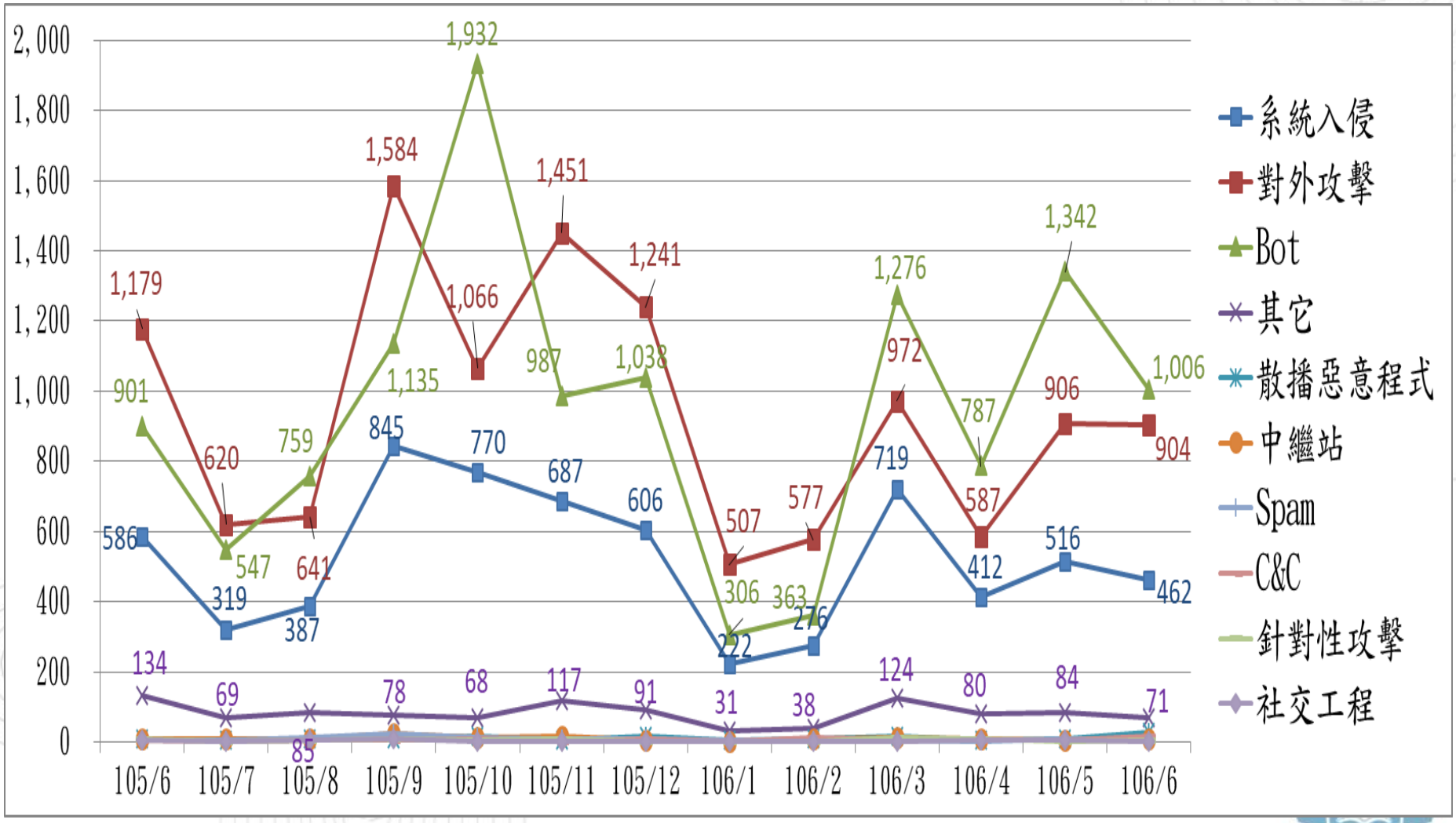
■ 統計時間：106年1月至106年6月

事件類型	子類別	數量
入侵攻擊(INT)	殭屍電腦(Bot)	5,080
	對外攻擊	4,453
	系統被入侵	2,607
	其他	426
	散播惡意程式	76
	中繼站	48
	命令與控制伺服器	48
	垃圾郵件(Spam)	38
	針對性攻擊	29
	電子郵件社交工程攻擊	16
總計		11,564



■ 資料來源：教育機構資安通報平台

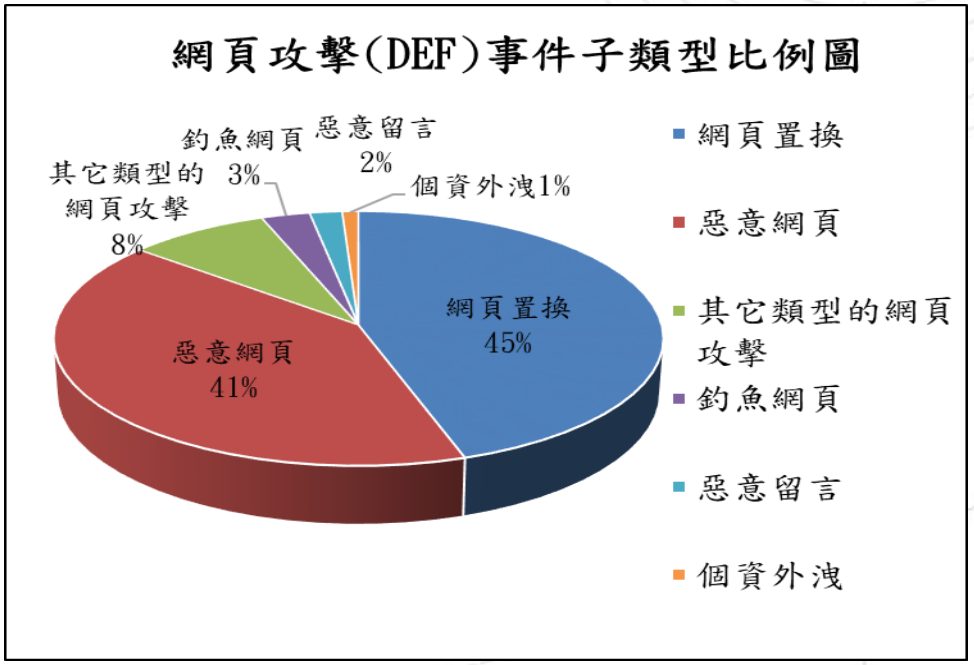
INT子類型曲線圖


2,000
1,800
1,600
1,400
1,200
1,000
800
600
400
200
0
105/6
105/7
105/8
105/9
105/10
105/11
105/12
106/1
106/2
106/3
106/4
106/5
106/6
系統入侵
對外攻擊
Bot
其它
散播惡意程式
中繼站
Spam
C&C
針對性攻擊
社交工程
1,179
620
641
1,584
1,066
1,451
1,241
507
577
972
587
906
904
901
547
759
1,135
1,932
987
1,038
306
363
1,276
787
1,342
1,006
586
319
387
845
770
687
606
222
276
719
412
516
462
134
69
85
78
68
117
91
31
38
124
80
84
71

學術網路資安事件DEF子類型比例

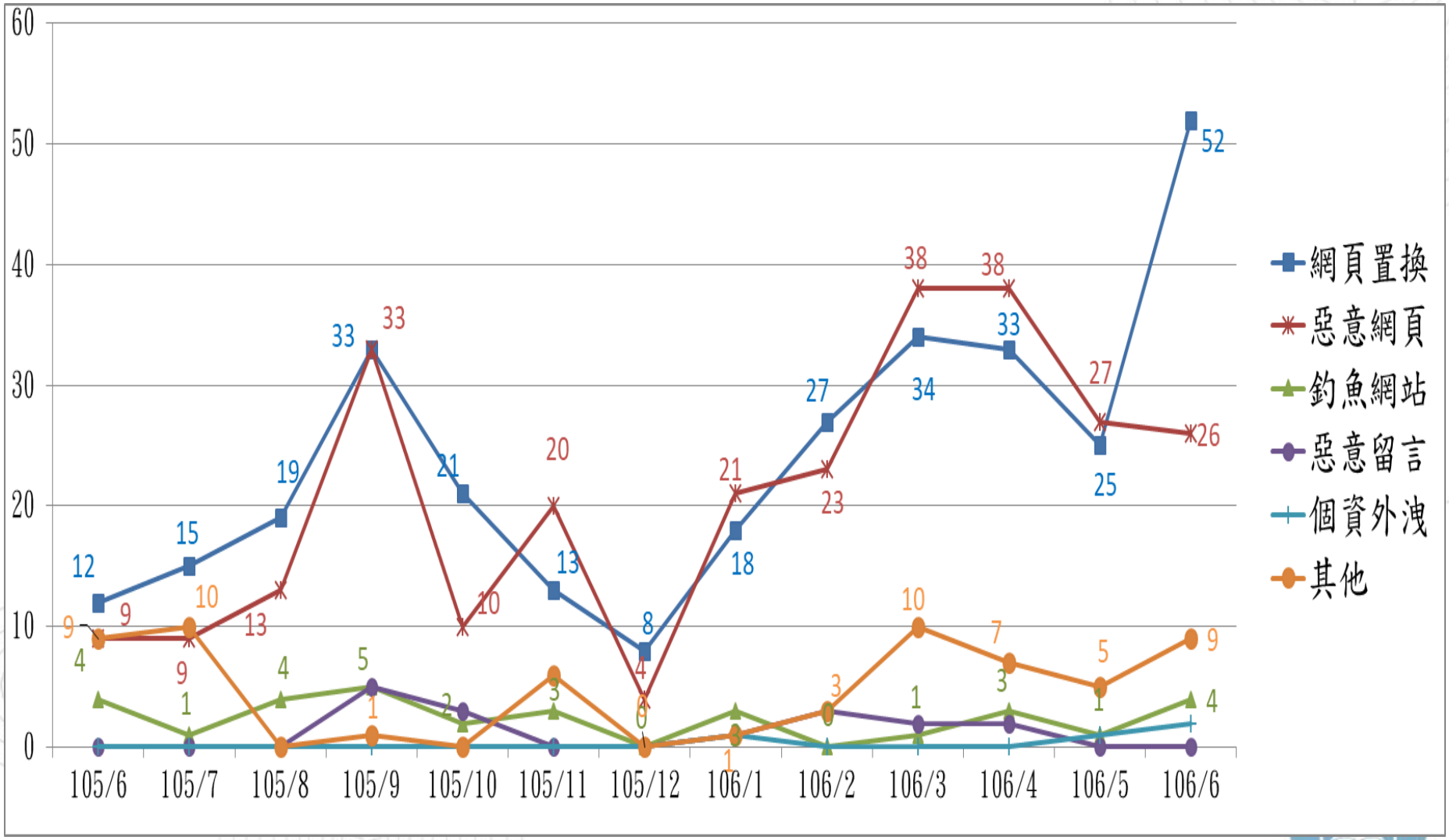
■ 統計時間：106年1月至106年6月

事件類型	子類別	數量
網頁攻擊(DEF)	網頁置換	189
	惡意網頁	173
	其它類型的網頁攻擊	35
	釣魚網頁	12
	惡意留言	8
	個資外洩	4
總計		412



■ 資料來源：教育機構資安通報平台

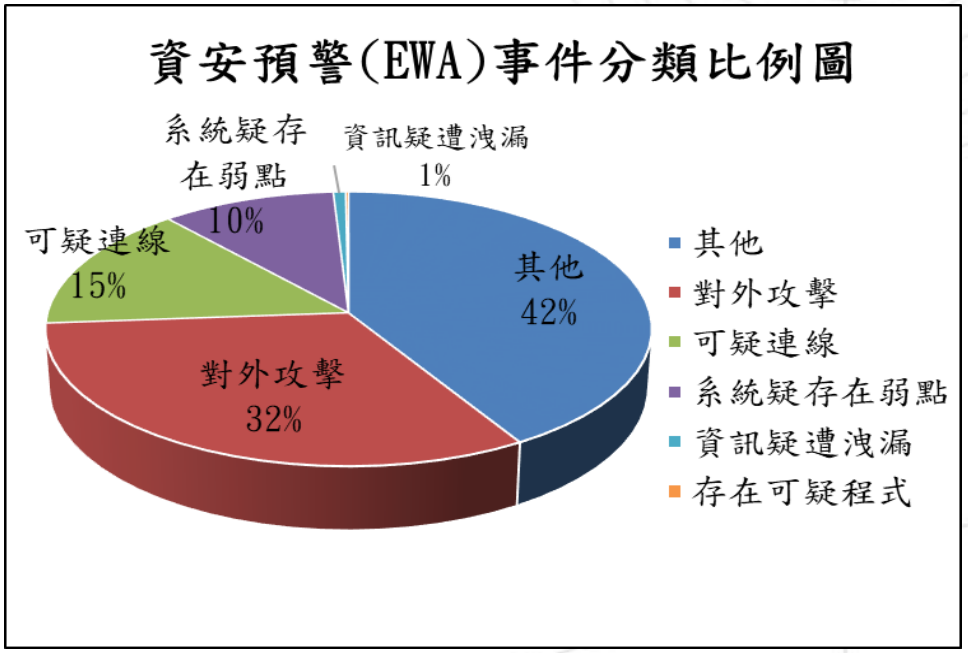
DEF子類型曲線圖


60
50
40
30
20
10
0
105/6
105/7
105/8
105/9
105/10
105/11
105/12
106/1
106/2
106/3
106/4
106/5
106/6
網頁置換
惡意網頁
釣魚網站
惡意留言
個資外洩
其他

資安預警(EWA)事件類型比例

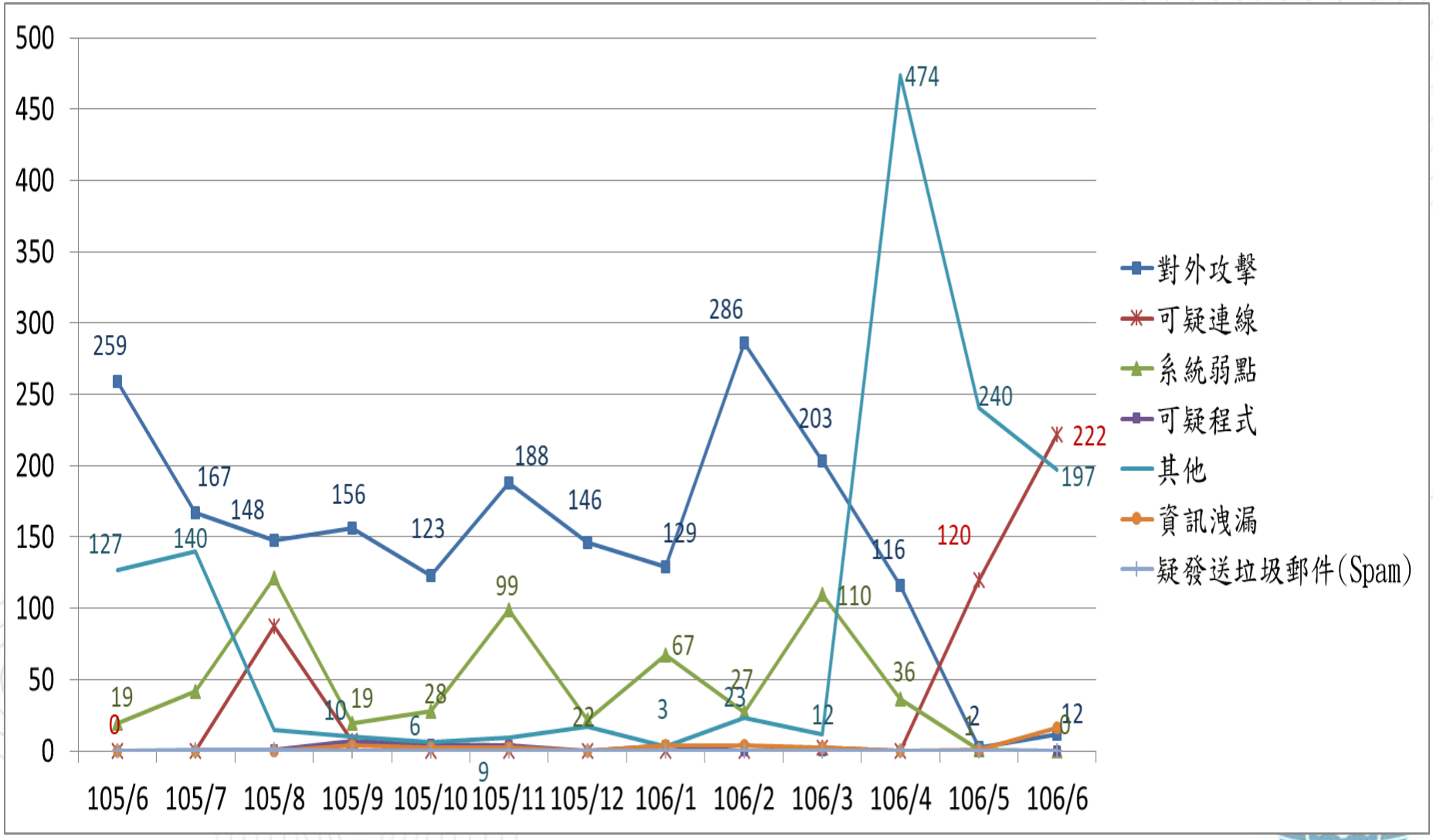
■ 統計時間：106年1月至106年6月

事件類型	子類別	數量
資安預警(EWA)	其他	959
	對外攻擊	748
	可疑連線	344
	系統疑存在弱點	241
	資訊疑遭洩漏	17
	存在可疑程式	4
總計		2,313



■ 資料來源：教育機構資安通報平台

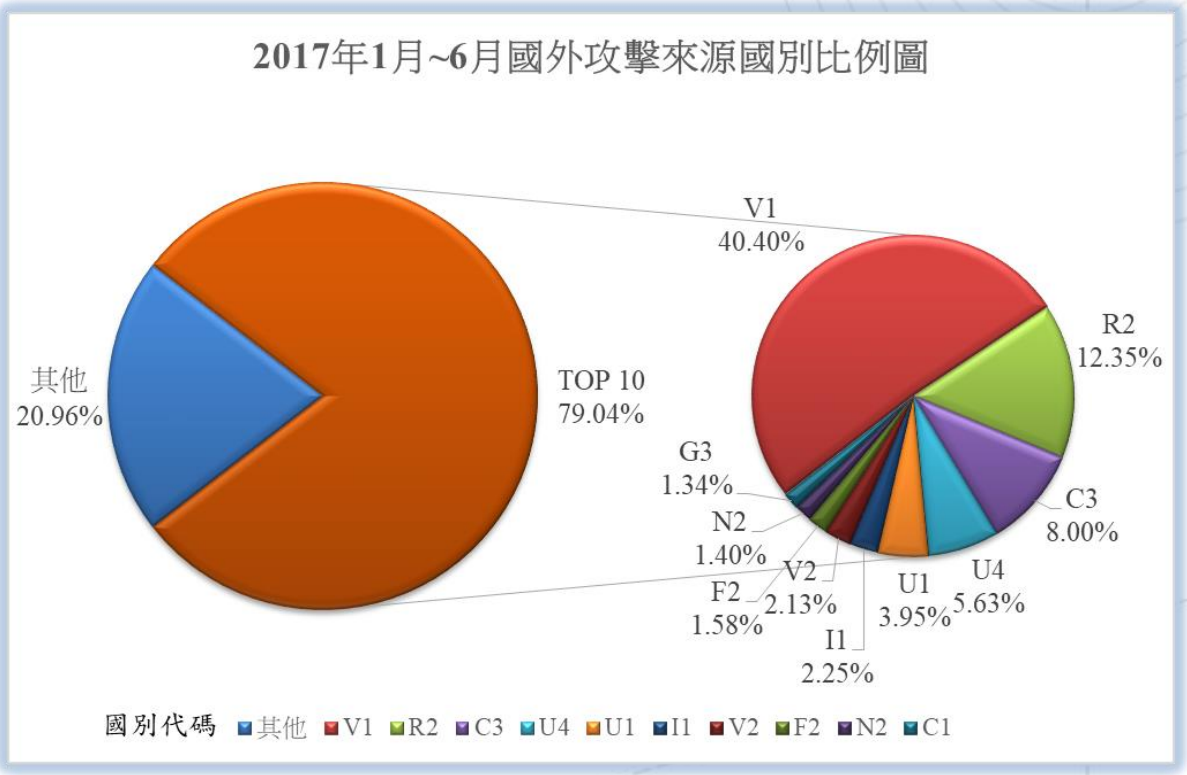
資安預警情資(EWA)


500
450
400
350
300
250
200
150
100
50
0
105/6
105/7
105/8
105/9
105/10
105/11
105/12
106/1
106/2
106/3
106/4
106/5
106/6
對外攻擊
可疑連線
系統弱點
可疑程式
其他
資訊洩漏
疑發送垃圾郵件(Spam)
259
167
148
156
123
188
146
129
286
203
116
2
12
127
140
474
240
197
19
0
10
19
6
28
99
9
22
67
3
27
23
110
12
36
120
222
12

國外惡意威脅來源國別比例

國家	攻擊IP數量
Venezuela(V1)	1328
Russian Federation(R2)	406
China(C3)	263
United States (U4)	185
Ukraine(U1)	130
India(I1)	74
Vietnam(V2)	70
France(F2)	52
Netherlands(N2)	46
Canada(C1)	44
其他	689
總計	**3,287 (95)**

■ 統計時間：2017年1月至6月



- 列舉於此列表需於1星期內攻擊學術網路超過一萬次之IP方列舉其上，其攻擊量需乘上10000，亦有32,870,000的攻擊量，而低於一萬次未列舉因此總量應為更多。
- 括號中之數字(95)代表國家數量，亦上表攻擊來自95個國家。

教育機構資安通報流程簡介

通報應變規劃重點

1.為使通報應變流程更有效掌握，通報應變平台之流程畫分為**通報流程**與**應變流程**。

2.第一線人員由於處理時間的限制，可先進行通報流程，待完成處理後再進行應變流程。

3.請各單位盡可能通報與應變同時進行。

4.所有通報應變流程之通報，都必須審核過後才是(教育部規範)正式結束通報流程。

如此規劃著眼於不同層級之資安人員可充分掌握所發生之資安事件，並能依輕重等級啟動不同對應之處理機制。

依資安等級區分

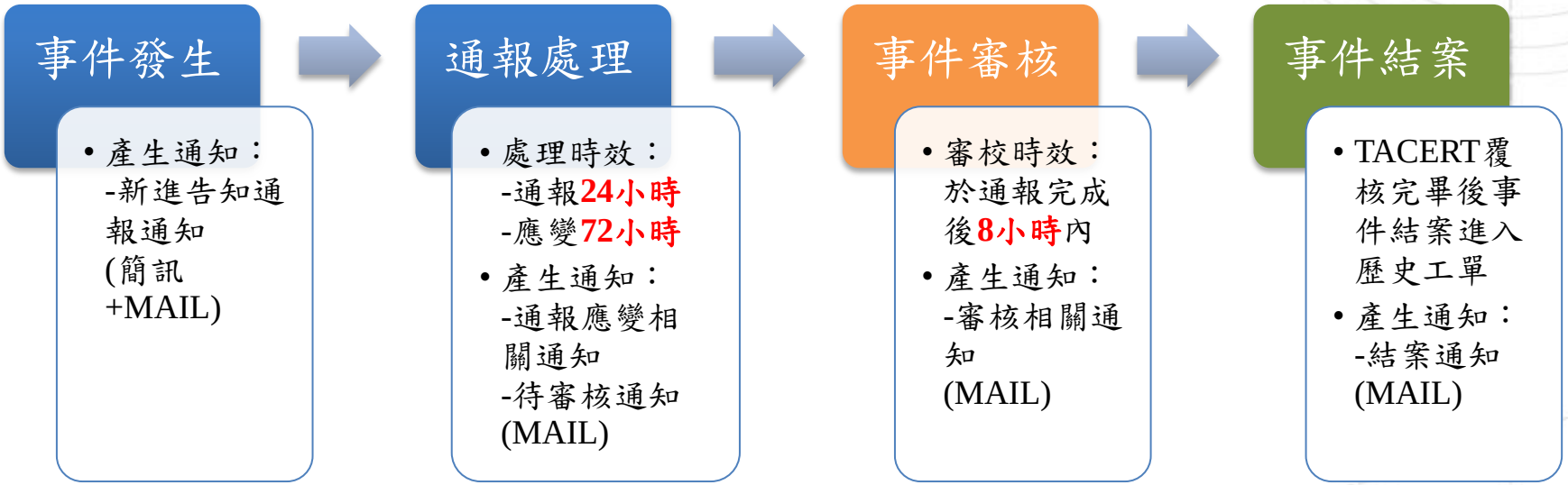
1、2級資安事件

- 事件處理時間通報於**24小時**內完成，應變於**72小時**內完成(通報+應變)
- 電子郵件通知寄發
  - 事件單成立後1個小時
  - 事件單成立後每隔12個小時
  - 事件單成立後72小時後每隔12個小時寄發逾時通知

3、4級資安事件

- 針對政府或國家等級之攻擊行為或其他重大資訊安全事件。
- 事件處理時間為**36小時**內完成
- 需和上級管理單位報備且建立連絡並指定相關人員待命追蹤處理狀況
- 電子郵件通知寄發
  - 事件單成立後1個小時
  - 事件單成立後每隔12個小時
  - 事件單成立後36小時後每隔12個小時寄發逾時通知

事件單處理流程


事件發生
• 產生通知：
-新進告知通報通知
(簡訊+MAIL)
通報處理
• 處理時效：
-通報24小時
-應變72小時
• 產生通知：
-通報應變相關通知
-待審核通知
(MAIL)
事件審核
• 審校時效：
於通報完成後8小時內
• 產生通知：
-審核相關通知
(MAIL)
事件結案
• TACERT覆核完畢後事件結案進入歷史工單
• 產生通知：
-結案通知
(MAIL)

事件單種類及通報簡介

告知通報事件單(INT&DEF)

教育機構資安通報平台

事件類型:入侵事件警訊

工單編號:AISAC-166

發單單位-事件類別-年度月份-流水編號

原發布編號	ICST-INT-201010-0023	原發布時間	2010-10-0801:51:30
事件類型	對外攻擊	原發現時間	2010-10-08
事件主旨	140.　.218.　資訊設備對外攻擊警訊通知		
事件描述	技術服務中心發現 貴單位註冊 IP 140.　.218.　於 2010/10/07 16:54 ~ 16:55 左右對外進行攻擊行為。 該電腦嘗試透過 TCP Port 135與445攻擊微軟MS08-067相關弱點。 為避免不必要之資安風險，請針對該系統進行詳細檢查並加強相關防範措施。		
手法研判	MS08-067		
建議措施	回復措施： 1.檢查該系統上是否有不明程式正大量對外建立網路連線(可能但不限於TCP Port 135與445)，若有則停止該程式並刪除系統上該不明程式檔案。 2.由於所得資訊有限，無法提供較明確之回復措施，請依該系統平台參考相關檢查暨回復措施。 3.對於此次攻擊行為，技術服務中心無法經由外部確認是否已完成相關回復措施。 相關建議： 1.檢查防火牆記錄，查看內部是否有對外大量不同目的 IP 之異常連線，特別注意但不限於 TCP Port 135與445。 2.檢查個別系統上是否有異常連線、異常執行中程序、異常服務及異常開機自動執行程式等。 3.注意個別系統之安全修補，若僅移除惡意程式而不修補，再次受相同或類似攻擊的機率極高。修補程式須持續更新，自動安裝更新程式機制可參考微軟保護電腦三步驟。 4.系統上所有帳號需設定強健的密碼，非必要使用的帳號請將其刪除。 5.安裝防毒軟體並更新至最新病毒碼。 6.檢驗防火牆規則，確認個別系統僅開放所需對外提供服務之通訊埠。 7.若無防火牆可考慮安裝防火牆或於 Windows 平台使用 Windows XP/2003 內建之 Internet Firewall/Windows Firewall或 Windows 2000 之 TCP/IP 篩選。Linux 平台可考慮使用 iptables 等內建防火牆。		
參考資料	微軟資訊安全錦囊 http://www.microsoft.com/taiwan/security/protect/ 微軟內建防火牆: http://www.microsoft.com/taiwan/security/protect/firewall.asp http://www.microsoft.com/windowsxp/using/security/internet/sp2_wfintro.mspx http://www.microsoft.com/windowsxp/using/networking/learnmore/icf.mspx 微軟相關弱點 http://www.microsoft.com/technet/security/current.aspx(英文-更新較快) http://www.microsoft.com/taiwan/security/bulletins/default.asp(中文-更新較慢) http://www.microsoft.com/taiwan/technet/security/bulletin/ms08-067.mspx http://www.microsoft.com/technet/security/bulletin/MS08-067.mspx		
此事件需要進行通報，請 貴單位資安聯絡人登入資安通報應變平台進行通報應變作業			
如果您對此通告的內容有疑問或有關於此事件的建議，歡迎與我們連絡。			

◎標示為必填欄位

通報流程：
填寫受害主機設備的基本資訊、事件分類、等級判斷與損害程度的資訊

應變流程：
填寫單位緊急應變措施、解決辦法與解決時間。

預警情報事件單(EWA)

*資安預警情報只派發MAIL通知，不派發簡訊通知

寄件者: service <service@cert.tanet.edu.tw>
收件者: service@cert.tanet.edu.tw
副本:
主旨: 資安預警情報(發布編號:ASOC-EWA-201206[redacted])
寄件日期: 2012/6/21 (週四) 上午 08:

資安聯絡人您好：
此為資安預警情報，請您協助確認資安預警事件(EWA)是
並登入資安通報平台後，於資安預警事件中完成通報作業
(如需相關佐證資料，登入通報平台後於事件附檔下載中

(1) 誤判：
經確認後設備相關記錄無符合項目，選擇「誤判」選項後
(2) 確實事件：
經確認後確實發生資安事件，請先於自行通報中完成事件
(3) 無法判斷：
經確認後，部份資料符合或設備相關記錄已不存在，選擇

如果您對此事件單內容有疑問或有關於此事件之建議，

原發布編號	ASOC-EWA-201206[redacted]
事件類型	對外攻擊
事件主旨	通報:[redacted].81 HTTP_Wind
事件描述	ASOC發現貴單位([redacted])所屬[redacted]
手法研判	惠請貴單位： 1.檢查防火牆紀錄：查看內部是否有可以執行此功能。 3.請檢查是否有不明之程序對
建議措施	本攻擊相關資訊可於下列網址http://www.iss.net/sec

如果此事件需要
如果您

寄件者: service <service@cert.tanet.edu.tw>
收件者: service@cert.tanet.edu.tw
副本:
主旨: 資安預警情報(發布編號:NTUSOC-EWA-201206[redacted])
寄件日期: 2012/6/18 (週一) 上午 0

主旨：資安預警情報(發佈編號：發單單位-EWA-年度月份-EWA編號

資安聯絡人您好：
此為資安預警情報，請您協助確認資安預警事件(EWA)是否確實發生。
並登入資安通報平台後，於資安預警事件中完成通報作業，作業說明如下：
(如需相關佐證資料，登入通報平台後於事件附檔下載中依發佈編號即可取得。)

(1) 誤判：
經確認後設備相關記錄無符合項目，選擇「誤判」選項後，於「原因」處填寫說明。
(2) 確實事件：
經確認後確實發生資安事件，請先於自行通報中完成事件通報應變後，取得事件單編號後。選擇「確實事件」選項後，於右側填入自行通報事件單編號。
(3) 無法判斷：
經確認後，部份資料符合或設備相關記錄已不存在，選擇「無法判斷」選項後，於「原因」處填寫說明。

如果您對此事件單內容有疑問或有關於此事件之建議，歡迎與本單位連絡。

原發布編號	NTUSOC-EWA-201206[redacted]	原發布時間	2012-06-18 07:33:09
事件類型	可疑連線	原發現時間	2012-06-18 07:19:00
事件主旨	教育部資安事件通告－[redacted].90]疑似大量BO2K後門連線目標主機警訊通知		
事件描述	目標IP可能遭受駭客入侵或遭植入木馬程式，並造成資訊外洩或成為殭屍網路一員而對外發動攻擊。 這個警示表示，有遠端使用者正嘗試使用 Back Orifice2K 特洛伊木馬程式，連線至您網路中的系統。特洛伊木馬程式可讓遠端使用者危害被安裝特洛伊木馬伺服器的系統。 此外，一些對等應用程式會在初始連線設定階段使用 Back Orifice2K 通訊協定，因此這個警示可能表示兩台電腦間的對等通訊。 入侵偵測防禦系統偵測到大量來源IP，啟用包含木馬後門特徵之封包，對目標IP（[redacted].90）目標 PORT （2015）進行連線。 感染 Back Orifice 特洛伊木馬，會讓遠端攻擊者取得對系統未經授權的存取。這類型的攻擊可能導致系統關機、記錄鍵盤輸入，以及允許無用的檢視/關閉程序。Back Orifice2K 特洛伊木馬可能也會允許遠端使用者，藉由重新設定系統及重新導向流量，來危害您的網路。 此外，請調查舉證報告中的封包記錄，以判斷目標主機是否正在執行對等應用程式。 ●影響的平台： 套裝軟體 Microsoft Windows 2000 Microsoft Windows NT Microsoft Windows 98 Microsoft Windows 95 Microsoft Windows Me		
手法研判	建議解決方案: - 若目標IP該連線行為已得到授權，則請忽略此訊息。 - 若目標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.請查看目標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。 部署防毒掃描程式來掃描您的系統是否具有此種病毒。請使用可移除受感染檔案的掃描程式。 視您的安全性政策而定，您可能想要求使用者從網路中的電腦上解除安裝對等應用程式。		

資安預警情報

- 資安預警情報(EWA)為教育部各資安計畫團隊或是其他情資來源單位，偵測到**疑似網路攻擊行為**時所發送的預警通知。
- **由一線單位進行檢查、處理及填報作業，區縣市網路中心進行追蹤作業**
- 連線單位收到資安預警通知時，請檢查該主機是否有異常網路活動跡象，並進行處理狀態回覆：
  - 確實事件：先於通報平台採**『自行通報』**取得事件單編號
  - **誤報：請詳填原因 (以利發單單位調校規則)**
  - 無法判斷：證據不足
- 處理時效：一星期內

資安預警情報回報方式

EWA事件單

事件編號	ASOC-EWA-201206
單位名稱	
填表時間	2012-06-21 08:02:46
發佈時間	2012-06-21 02:09:50
發生時間	2012-06-21 01:28:49
受害IP	.135
受害網址	
事件等級	low
事件分類	
主旨	通報] .135 Stacheldraht_Agent
說明	ASOC發現貴單位)所屬 .135 疑似對外進行 Stacheldraht_Agent 攻擊
手法研判	Stacheldraht 是基於 Tribe FloodNet (TFN) 工具的「分散式拒絕服務」(DDoS) 攻擊工具，係以 Tribe FloodNet (TFN) 工具為基礎。它結合了 Trin00 (AKA trinoo) 的功能與 TFN 的功能，並針對這些功能
應變措施	惠請貴單位： 1.確認內部主機是否有不明程式或網路路由問題造成此攻擊行為。 2.利用工具程式(如:TCPview、procexp)於來源主機觀
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/Stacheldraht_Agent.htm內查詢

EWA事件單狀態

○ 誤判		
◉ 確實事件	事件單編號	
○ 無法判斷		
原因		

送出

完整資安預警(EWA)事件單訊息

回報資安預警(EWA)事件單的處理狀況

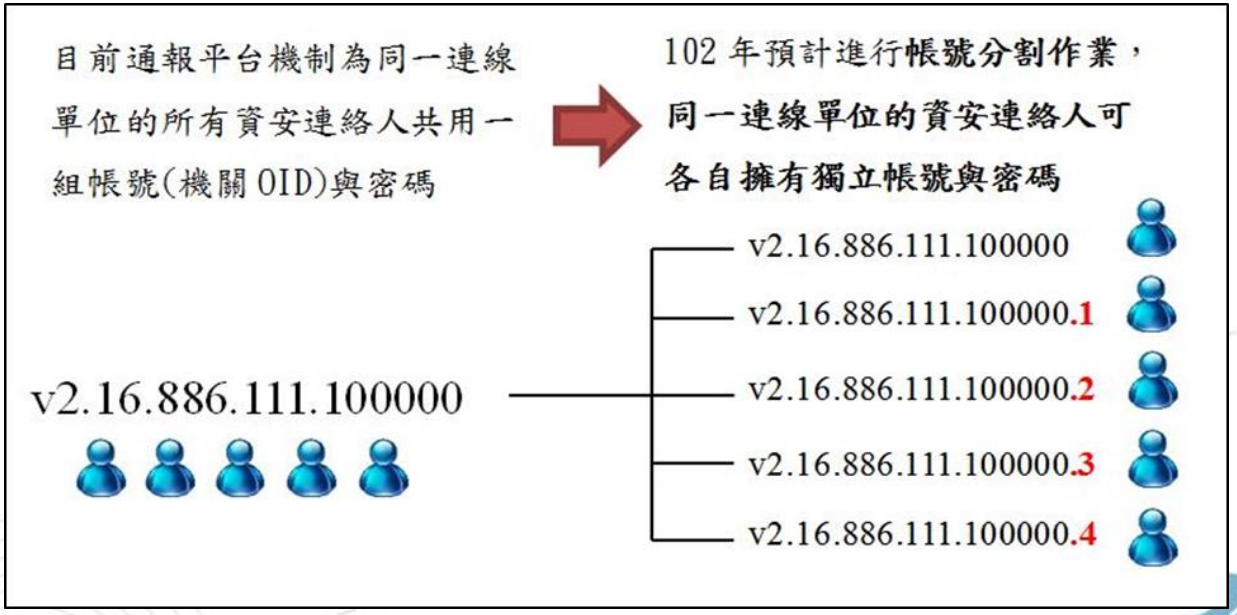
教育機構資安通報平台功能介紹

教育機構資安通報平台

- 教育機構資安通報平台網址：info.cert.tanet.edu.tw

會員登入

- 使用OID及密碼登入
- 一個單位最多有五位連絡人
- 每個連絡人OID及密碼可不同



機關OID查詢

- 可至國發會網站(網址為「http://oid.nat.gov.tw/」)，點選「組織與團體物件識別碼(OID)查詢」進行查詢
- 來電(信)至本中心查詢

密碼查詢

- 密碼查詢機制將核對「單位OID」、「連絡人姓名」、「連絡人郵件」、「連絡人手機」及「驗證碼」，且**以上資訊需和教育機構資安通報平台內連絡人資料符合**
- 以「**重設8碼亂數密碼**」，並以簡訊及電子郵件通知該連絡人

登入畫面

個人資料區

事件單處理區

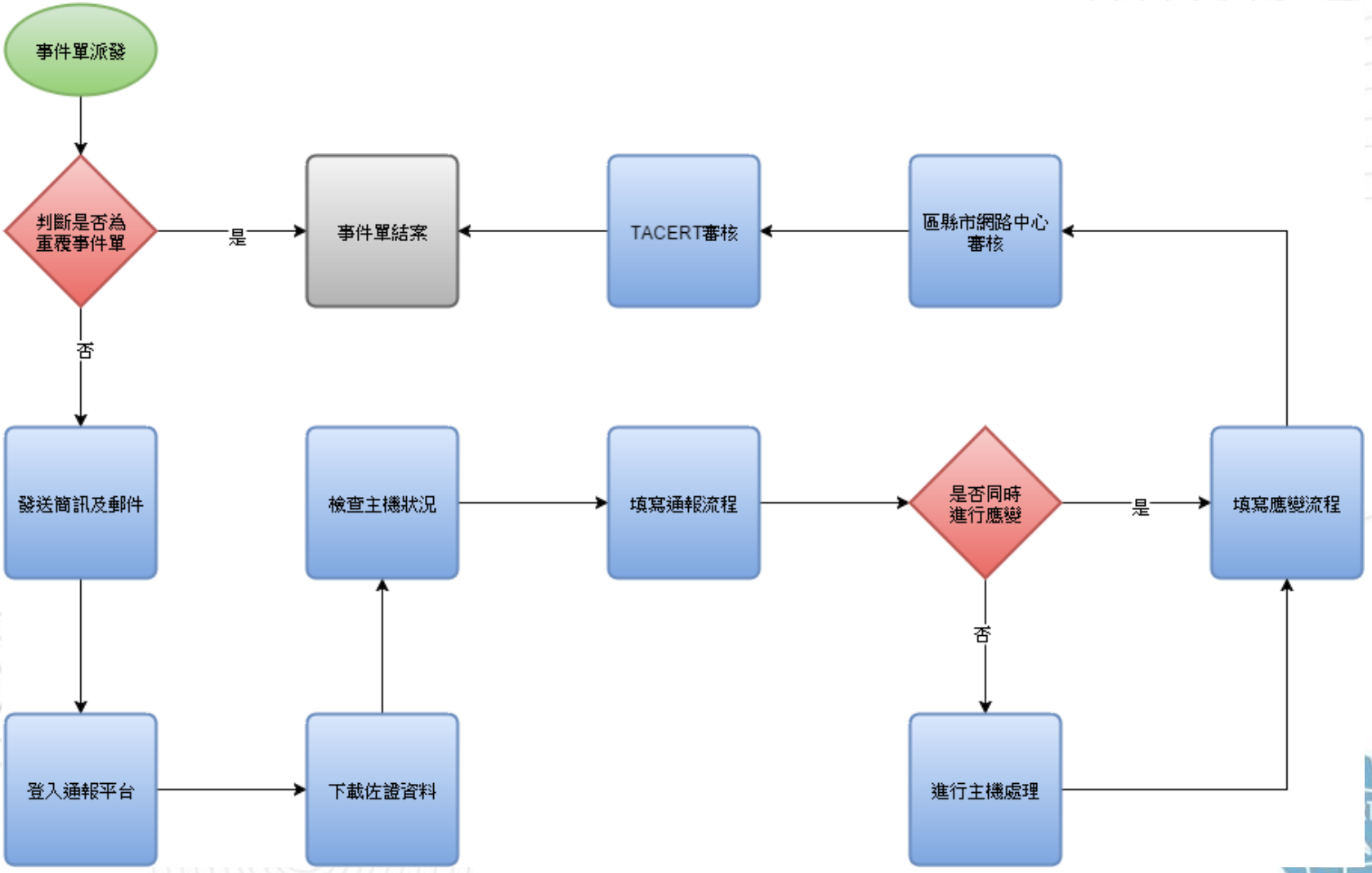
資安通報平台功能簡介

- 個人資料區各功能說明：
  - 首頁：顯示未處理完成事件
  - 修改個人資料：修改個人連絡資料
- 事件單處理區各功能說明：
  - 通報/應變：未完成通報應變事件單表列於此，以利處理
  - 自行通報：如發現資安事件或EWA事件單確認屬實，可利用此攻能完成通報應變。
  - 事件單處理狀態：未結案前之事件單狀態查詢
  - 歷史通報：已結案事件單表列於此
  - 帳號管理：管理第三~五連絡人帳號開啟關閉
  - **事件附檔下載：事件單佐證表列於此，依發佈編號查詢下載。**
  - 資安預警事件：預警事件單表列於此
- 網址：https://info.cert.tanet.edu.tw
  - 操作手冊：http://cert.tanet.edu.tw/pdf/doc6.doc

連線單位資安連絡人異動

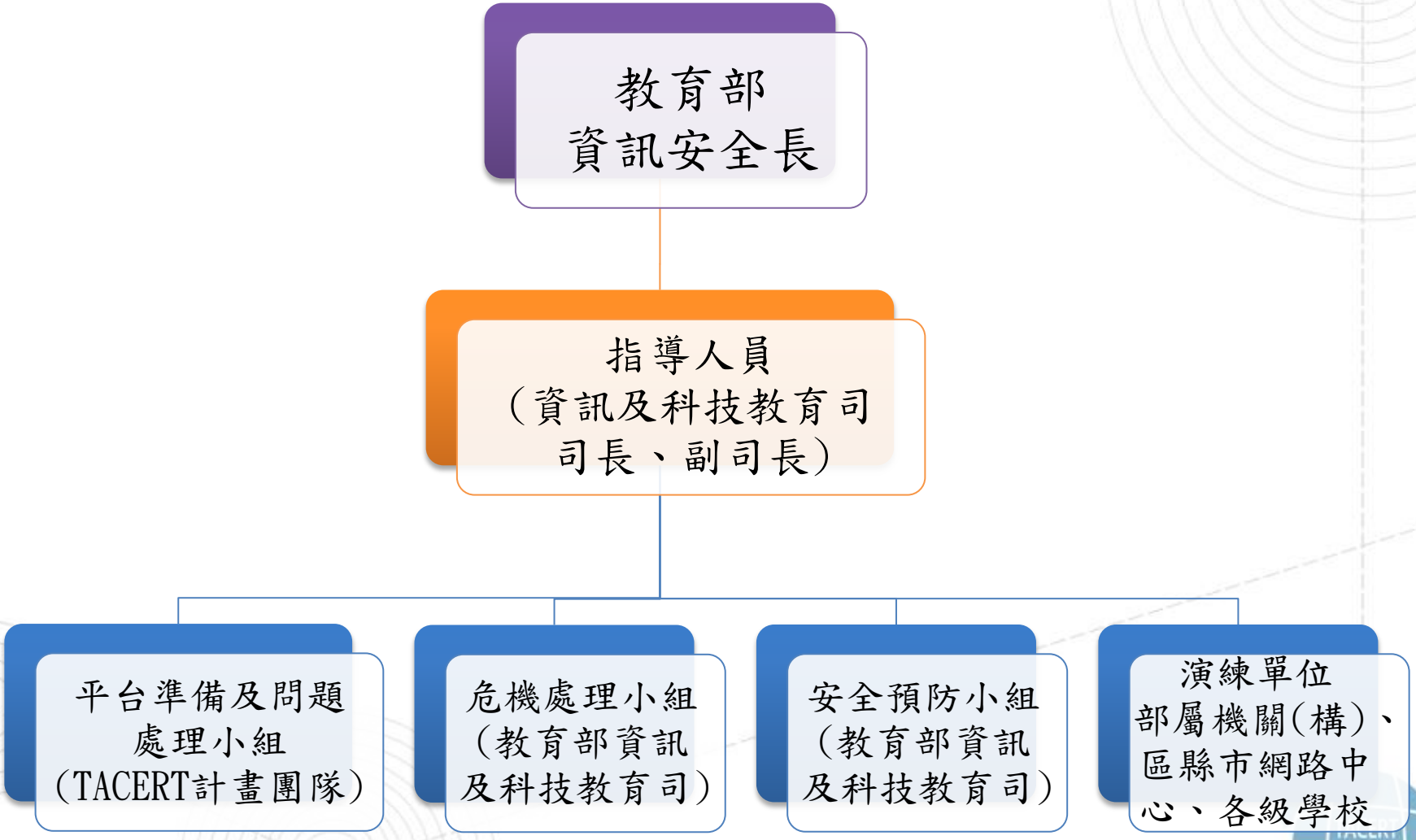
- 為確保資安事件能夠即時通知與處理，故煩請各連線單位於資安連絡人發生異動時，**務必確保資安事件的處理業務能妥善完成交接**
  1. 資安連絡人員至少需有二位，以建立代理人制度
  2. **建議將主要負責人員填寫於第一、二連絡人**
  3. 教育機構資安通報平台的帳號密碼進行交接
  4. 登入教育機構資安通報平台於「修改個人資料」進行連絡人資訊更新
  5. 新接任資安連絡人可至本中心網站的資安文件下載資安通報應變手冊，了解通報平台基本操作。
     - TACERT中心網站資安文件網址：
       http://cert.tanet.edu.tw/prog/Document-1.php

事件單處理流程


事件單派發
判斷是否為重覆事件單
是
事件單結案
TACERT審核
區縣市網路中心審核
否
發送簡訊及郵件
檢查主機狀況
填寫通報流程
是否同時進行應變
是
填寫應變流程
否
登入通報平台
下載佐證資料
進行主機處理

教育機構資安通報演練簡介

任務編組架構


教育部
資訊安全長
指導人員
（資訊及科技教育司
司長、副司長）
平台準備及問題
處理小組
（TACERT計畫團隊）
危機處理小組
（教育部資訊
及科技教育司）
安全預防小組
（教育部資訊
及科技教育司）
演練單位
部屬機關(構)、
區縣市網路中
心、各級學校

工作內容

- 平台準備及問題處理小組：
  - 負責教育機構資安通報演練平台維護、規劃演練各項事宜及問題處理
- 危機處理小組：
  - 負責規劃演練各種模擬狀況及處理突發狀況
- 安全預防小組：
  - 負責規劃參演單位及支援演練計畫執行處理作業
- 演練單位：
  - 針對演練模擬事件，研擬應變處理作為，並於教育機構通報演練平台回覆應變處理作為

通報演練時程簡介

演練計畫規劃

演練整備階段

演練執行階段

演練計畫規劃階段

- 提交演練計畫草稿
- 確認演練單位
- 演練平台整備

演練整備階段

- 帳號資料確認(關閉未使用帳號)
- 資安聯絡人資料確認(第一、二聯絡人)
- 變更聯絡人密碼(第一、二聯絡人)
- 本年度整備期：
  接獲演練公文至2017/9/15止

整備項目

- 教育機構資安通報平台帳號資料確認
  - 進行登入測試，登入時使用OID登入
  - 忘記OID可至行政院研考會OID管理網址查詢(http://oid.nat.gov.tw)
- 教育機構資安通報平台資安聯絡人資料確認
  - 依序填寫二位資安聯絡人
  - 各聯絡人填寫資料需正確、有效
  - 進行密碼更新作業

配合注意事項

- 各聯絡人以各自帳號直入進行資料確認及密碼更新作業
- 第一、二連絡人為主要連絡人，建議將業務負責人員填寫於前二位，並將未使用連絡人帳號關閉，以達風險控管目的
- 單位收到演練公文後可開始更新密碼，且第一、二連絡人需進行密碼變更
- 建議使用高強度密碼，以大小寫英文、數字、符號至少擇其二種組合成8碼以上之密碼

演練執行階段

- 分梯執行演練
  第一梯：
  北區、東區 2017/09/18 ~ 2017/09/22
  第二梯：
  中區、南區 2017/09/25 ~ 2017/09/29
  每梯次前三日為演練事件派發作業時間，
  後二日為預留作業時間
- 於教育機構資安通報演練平台進行通報
  https://drill.cert.tanet.edu.tw

演練方式

- 演練將以「**告知通報**」形式進行，以郵件及簡訊傳送「資安演練事件通知」，並加註「告知通報演練」字樣，事件單編號以「DRILL」開頭編碼

- 系統將以教育部模擬之10種情境樣本以亂數方式分發送至所有演練學術單位，執行演練單位需至「教育機構資安通報演練平台」完成事件通流程(網址：https://drill.cert.tanet.edu.tw)

演練模擬事件類型

模擬狀況編號	攻擊類型(事件類型)	攻擊子類型(事件子類型)	攻擊事件說明
1	DEF	網頁置換	單位網站首頁遭竄改
2	DEF	釣魚網站	單位內某網站被植入偽造認證網站(釣魚網站)
3	DEF	惡意網頁	單位內網站被植入惡意網頁
4	DEF	惡意留言	單位內網站討論區被灌入大量不當留言
5	DEF	個資外洩	單位內透過不同方式散播個人資料
6	INT	對外攻擊	單位內某電腦重複嘗試入侵他人系統
7	INT	散播惡意程式	單位內部電腦中毒並迅速感染其他電腦
8	INT	BOT	單位內電腦中毒成為BOTNET成員
9	INT	SPAM	單位內某電腦大量散佈電子郵件
10	INT	中繼站	單位內部電腦被植入惡意程式後形成BOT中繼站

- 演練子類型會依前一年較常發生之類型進行更新，以演練計畫核定內容為主

演練模擬事件通報方式

- 發送之演練簡訊格式與範例：
  - 格式：(告知通報演練)[受測單位],[事件類型]警訊,[事件編號],請盡速至平台完成事件處理。
  - 範例：(告知通報演練)[國立XX大學],[入侵攻擊]事件警訊,[15],請盡速至平台完成事件處理。
- 發送之演練事件通知電子郵件主旨格式與範例：
  - 格式：(事件單編號：DRILL-AISAC-XX)(告知通報演練)[事件類型]事件警報
  - 範例：(事件單編號：DRILL- AISAC-15)(告知通報演練)入侵攻擊事件警報)

演練事件通知單內容範例

範例　　教育機構資安通報【演練平台】

教育部暨學術機構分組資通安全演練事件通知單

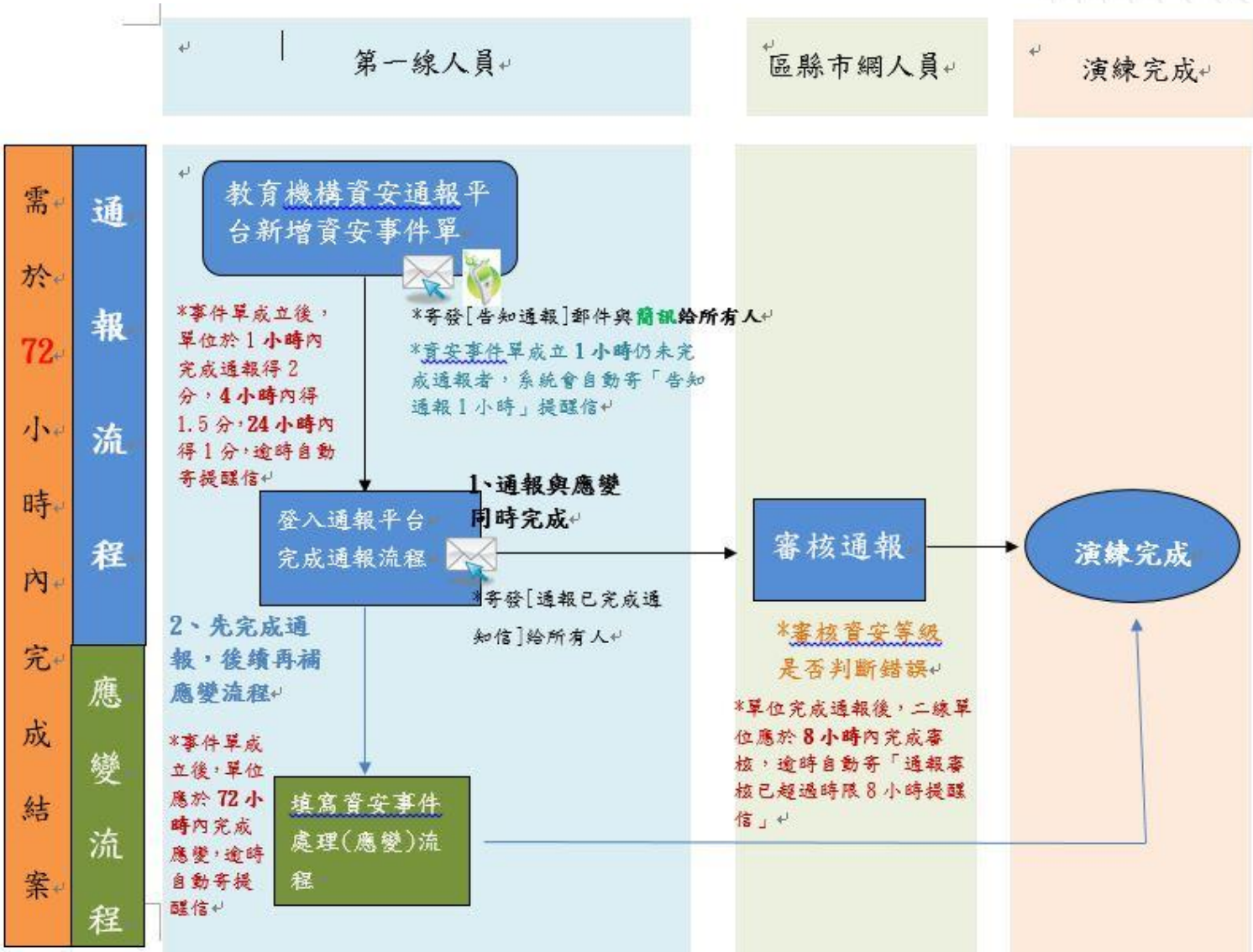
演練事件類型:入侵事件警訊

演練事件單編號:DRILL-AISAC-xx

原發布編號	DRILL-INT-201610-xxxx	原發布時間	2015-10-xx xx:xx:xx
演練事件類型	中繼站	原發現時間	2015-10-xx xx:xx:xx
演練事件主旨	貴單位[**受測單位**][IP:xxx.xxx.xxx.xxx]主機進行大量 BOT 嘗試連線警訊通知		
演練事件描述	1.若來源 IP 該連線行為已得到授權，則請忽略此訊息。2.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。3.請查看事證報告，確認該流量是否合法。		
手法研判	無		
建議措施	來源 IP 可能遭受駭客入侵或遭植入木馬程式，並造成資訊外洩或成為殭屍網路一員而對外發動攻擊。此警示表示有人企圖利用 Pushdo 殭屍病毒（Bot）進行拒絕服務（DoS）攻擊。 入侵偵測防禦系統偵測到來源 IP(xxx.xxx.xxx.xxx)，啟用包含 BotNet 特徵之封包，對目標 IP（多個目標 IP）進行連線。此事件來源 PORT （多個來源 PORT)，目標 PORT （多個目標 PORT)。 攻擊若是得逞，可能會造成目標伺服器發生 DoS 狀況。		
此演練事件需要進行通報，請 貴單位資安聯絡人登入資安通報演練平台進行通報應變作業			
如果您對此通告的內容有疑問或有關於此演練事件的建議，歡迎與我們連絡。			

教育機構資安通報應變小組
演練平台網址：https://drill.cert.tanet.edu.tw
電話 1：07-5250211
電話 2：07-5251535
VOIP 網路電話：98400000
E-Mail：service@cert.tanet.edu.tw

演練通報應變流程說明


第一線人員
區縣市網人員
演練完成
需於72小時內完成結案
通報流程
應變流程
教育機構資安通報平台新增資安事件單
*事件單成立後，單位於1小時內完成通報得2分，4小時內得1.5分，24小時內得1分，逾時自動寄提醒信
*寄發[告知通報]郵件與簡訊給所有人
*資安事件單成立1小時仍未完成通報者，系統會自動寄「告知通報1小時」提醒信
登入通報平台完成通報流程
1、通報與應變同時完成
*寄發[通報已完成通知信]給所有人
審核通報
演練完成
*審核資安等級是否判斷錯誤
*單位完成通報後，二線單位應於8小時內完成審核，逾時自動寄「通報審核已超過時限8小時提醒信」
2、先完成通報，後續再補應變流程
*事件單成立後，單位應於72小時內完成應變，逾時自動寄提醒信
填寫資安事件處理(應變)流程

外部單位調查注意事項

說明及注意事項

- 緣由：
  近來校園內陸續發生重大資安事件，外部單位有時需要學術單位配合調查

- 注意事項：
  - 建議外部單位以公文方式告知相關單位知悉
  - 調查過程中除受調查單位外，建議需有區縣市網路中心人員或資安團隊人員陪同

攻擊趨勢分析

DDoS

分散式阻斷服務攻擊

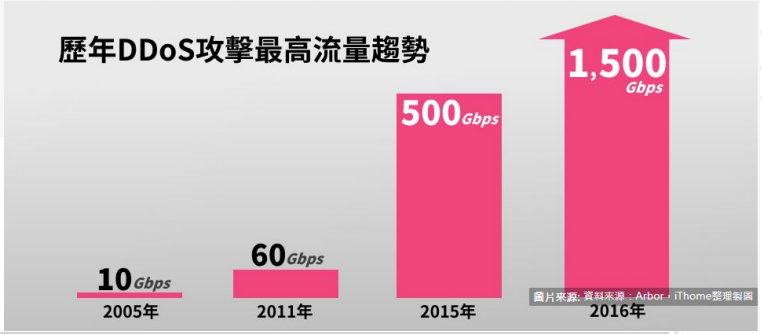
(Distributed Denial of Service)

DDoS新聞

新聞

【2017資安趨勢】百萬IoT殭屍大軍來勢洶洶，Tb級DDoS攻擊越演越烈

殭屍網路Mirai於2016年9月現身之後，造成全球網路世界開始發生好幾起大規模DDoS攻擊事件，最高攻擊流量甚至超過1Tbps，超越過去10年以來DDoS攻擊的最高流量紀錄



新聞

臺灣首次券商集體遭DDoS攻擊勒索名單出爐：累計13家！

2月7日一開盤就出現DDoS攻擊，當天累計有4家券商下單系統遭殃，其中有多家是沒有不在第一波攻擊名單的新受害者，累計從過年期間到2月7日攻擊預告日為止，共有13家券商遭DDoS攻擊勒索。

新聞

駭客16歲自建販售DDoS攻擊服務被判刑2年

Mudd在16歲時創立了DDoS攻擊服務Titanium Stresser，該服務吸引11.2萬名註冊用戶，共執行了170萬次的網路攻擊，攻擊對象包含Minecraft、微軟Xbox Live及學校等單位，賺進38.6萬歐元，遭英國法官判刑2年。

DDoS特性

初期

- 攻擊時間「集中」且「短」
- 控制主機數量「少」
- 攻擊封包「大」

現在

- 攻擊時間「分散」且「長」
- 控制主機數量「多」
- 攻擊封包「小」

DDoS常見類型

體積規模

- 透過大規模連線塞滿網路資源，以拒絕合法用戶的存取

以小博大

- 利用少量的惡意數據大幅降低網路速度

運算消耗

- 消耗CPU與記憶體資源

弱點攻擊

- 針對漏洞進行攻擊

DDoS攻擊現況

Digital Attack Map

- http://www.digitalattackmap.com/

Norse Dark Intelligence

- http://map.norsecorp.com/

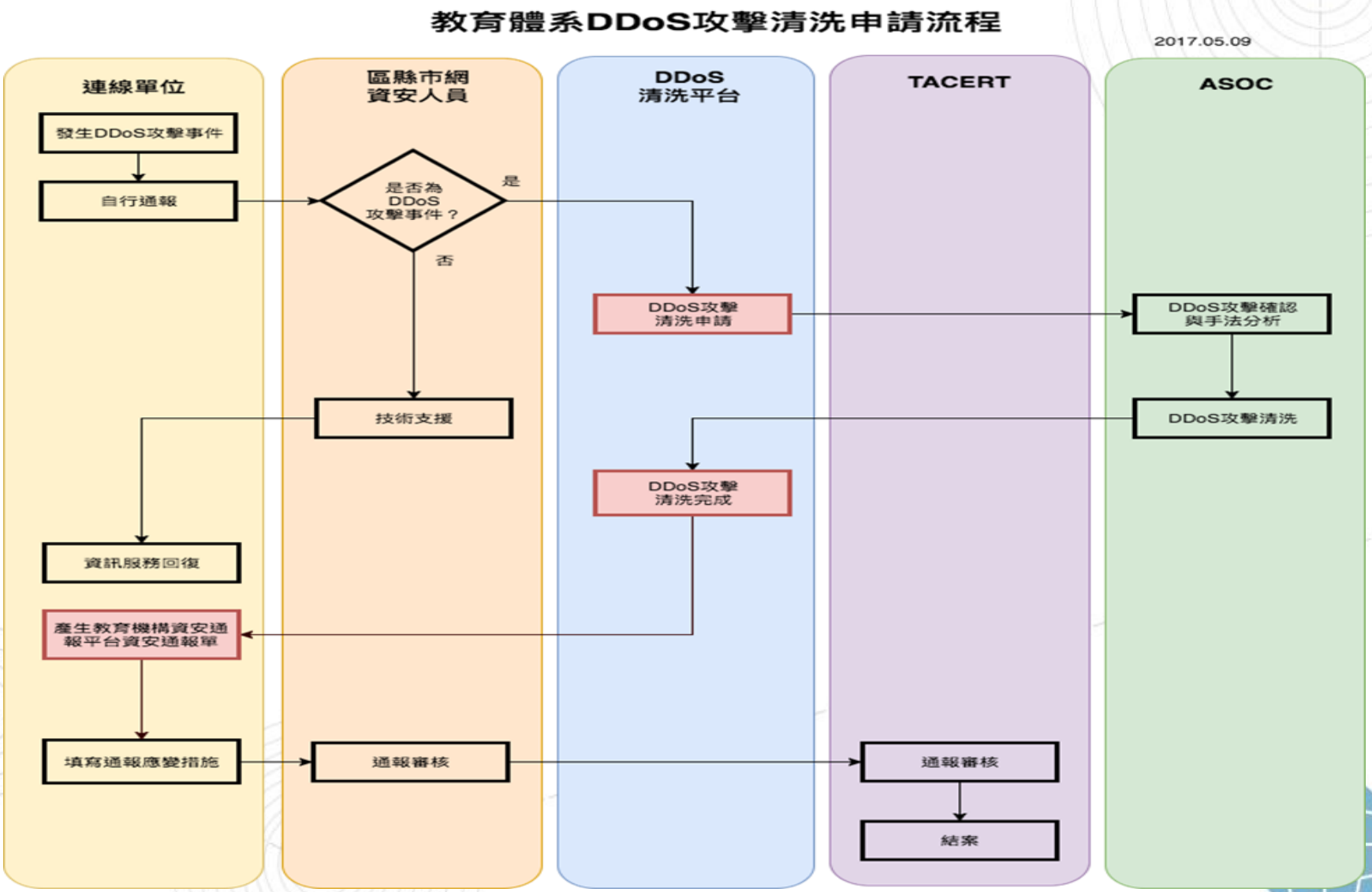
DDoS防禦建議

- 使用多層次過濾防護
- 執行弱點補強及系統更新
- 服務備援及災難復原機制
- 安全監控及緊急應變程序

學術網路DDoS清洗機制

- 現今的網路攻擊日益頻繁，規模更大，且複雜度更勝以往。尤其近年來國際間發生多起大規模DDoS(Distributed Denial of Service，分散式阻斷服務攻擊)攻擊事件，而且攻擊規模更頻頻創新高
- 有鑑於此，教育部已於S-ASOC及N-ASOC建置TANet流量清洗中心，當TANet內部單位遭受DDoS攻擊時，可透過TANet流量清洗中心過濾掉攻擊封包，讓系統可迅速回復正常
- TACERT團隊負責開發「DDoS清洗申請系統」以協助二線區縣市網路中心人員以及SOC團隊申請DDoS清洗服務以及管理清洗流程進度使用
- 「DDoS清洗申請系統」位於教育機構資安通報回饋平台(https://portal.cert.tanet.edu.tw)中之「資安通報報表系統」內，目前僅開放由區縣市網路中心申請

學術網路DDoS清洗申請流程



圖片來源：S-ASOC

零時差攻擊

(Zero-Day Attack)

<漏洞攻擊 Loopholes Attack>

零時差攻擊新聞

新聞

比特幣集體勒索又來了，這次鎖定全臺4千校！不只大學，桃園3小學也出現駭客勒索信

桃園市有3所中小學近日收到駭客恐嚇信，揚言若不支付比特幣，就會在3月1日癱瘓學校網路。此外，也有部分大學同樣收到駭客威脅信。駭客利用連線印表機的公開IP和預設密碼，侵入學校網路列印。

新聞

WannaCry 2.0勒索蠕蟲狠襲全球，上百個國家受駭，台灣也是重災區

週五開始出現全球性攻擊，到了週六，災情更從十幾個國家迅速擴大到104個國家，攻擊次數擴大到12.6萬次，儘管全球都是受災區，但WCry的主要攻擊目標為俄國、烏克蘭與台灣

新聞

勒索軟體Petya再襲全球，車諾比核設施、WPP廣告集團都受駭

資安業者指出Petya變種勒索軟體至少利用了Eternal Blue感染受害者的電腦，除了加密電腦內的檔案，勒索約300美元比特幣，還會竄改主開機紀錄，受害者包括海運公司、石油公司、廣告代理商、電廠等等。

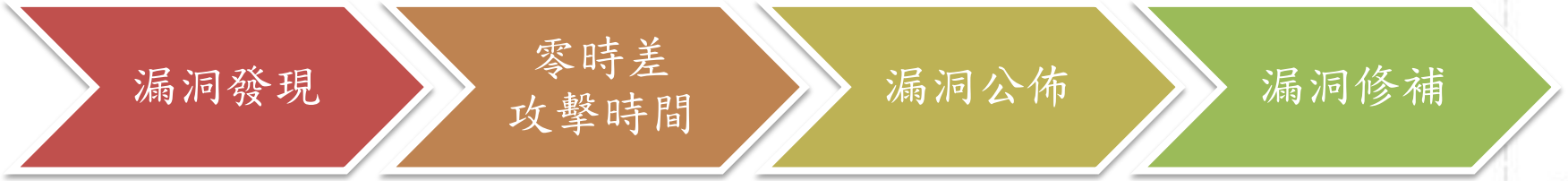
新聞

美國安局轄下的網路攻擊軍火庫疑遭駭，大批駭客工具外流

名為「影子掮客」的駭客集團在網路上拍賣來自神祕網路攻擊組織「方程式」的駭客工具，「方程式」被認為和美國國安局有關，擁有強大的木馬軍火庫、複雜的駭客技術，並多次與美國國安局的網路間諜活動有關。

零時差攻擊週期

定義：透過還沒有修補程式的安全漏洞進行攻擊之行為



零時差攻擊防禦建議

- 關閉未使用之服務
- 限制存取服務來源
- 內部服務勿用於公開環境
- 建置異常監控系統
- 修補漏洞

個案分享

校園主機感染WannaCry病毒事件

學術網路感染WannaCry與應變措施的時程表

106/4/28

- TACERT團隊**發布ANA-漏洞預警**，說明微軟SMB漏洞的影響範圍及建議相關弱點修補方式，建議單位儘速進行更新！

106/5/12

- H大學電腦教室上課上到一半時，突時有幾台電腦感染WannaCry病毒，檔案被加密且出現勒索訊息畫面，立即請學生關機並中斷網路。因電腦教室電腦皆裝有還原卡，重新開機即可復原。 並於5/13(六)進行更新windows 漏洞。

106/5/13

- TACERT**發佈ANA-【高風險】【攻擊預警】勒索軟體 WanaCrypt0r 2.0 攻擊 Windows 系統漏洞**，造成檔案加密無法使用，請儘速進行更新。

106/5/15

- TACERT派發調查表至區縣市網路中心，調查學術網路WannaCry受害狀況。

學術網路感染WannaCry與應變措施的時程表

106/5/17

- TACERT團隊發佈「預防 Wanacrypt0r 2.0 勒索病毒攻擊的方法」技術文件。

106/5/22

- 統計自106/5/12~106/6/7為止，受害單位共計14間，受害主機數量共計133臺。受害單位類型以「大專院校」佔86%為大宗，其次為「國民中小學」佔14%，主機大都為電腦教室或學生的個人電腦，尚無公務電腦受害。

106/6/5

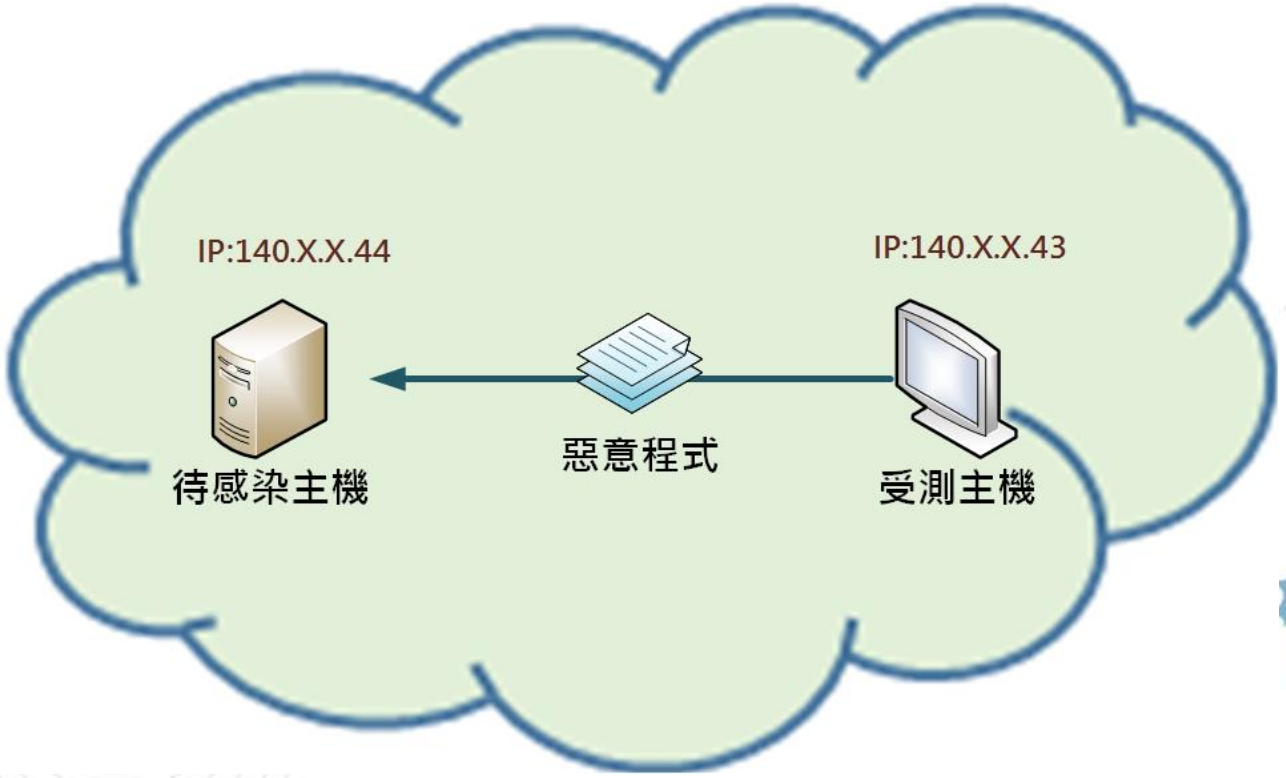
- S大學自行通報學校內部有約60台設備遭受WannaCry感染，目前均為橫向感染，大都為學生與助理的個人電腦，且沒有被加密，只有對外攻擊445port，同時取得樣本，進行鑑識分析。

事件簡介

- 在今年5月中旬爆發WannaCry病毒利用Windows系統的SMB漏洞，透過TCP445連接埠來傳播，進行大規模攻擊未更新Windows系統的電腦。
- 本事件為S大學之校內一台測試主機發生疑似惡意程式連線行為，對外進行大量445 連接埠的連線。
- 該主機為測試用的虛擬主機，所安裝的系統為Windows Server 2008 R2系統，而且自今年3月初過後關機至今年5月17日才再次開機。
- 本單位取得該虛擬主機的樣本後，以還原系統的方式進行研究分析。

事件檢測

- 首先我們將已感染中毒的虛擬主機在VM環境內還原，並執行檢測工具來觀察其程式行為與其對外網路行為。此外，也準備一台Windows 7系統的待感染主機，來觀察其病毒感染途徑與網路行為。



事件檢測

- 以Nmap工具檢視受測主機對外的連接埠資訊，發現135、445、3389、49154等連接埠為開啟狀態。

```
Discovered open port 3389/tcp on 140.[redacted].43
Discovered open port 135/tcp on 140.[redacted].43
Discovered open port 445/tcp on 140.[redacted].43
Discovered open port 49154/tcp on 140.[redacted].43
```

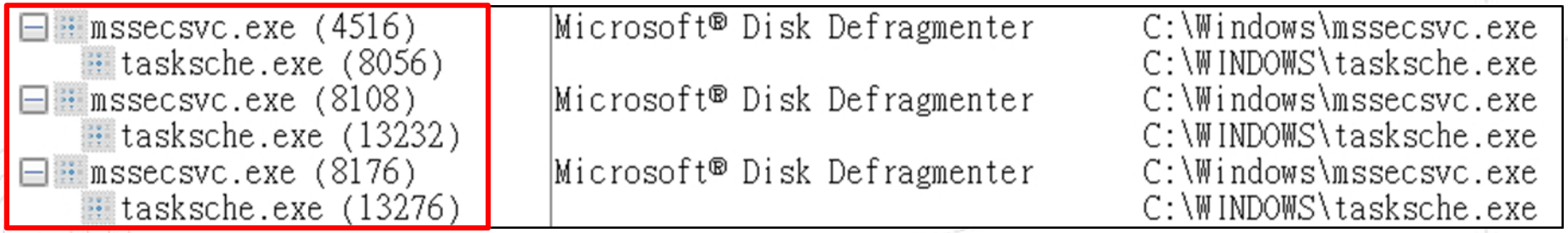
事件檢測

- 透過Currports工具發現有一個執行中的程式 mssecsvc.exe，正在產生大量對外連線445連接埠行為，嘗試對外進行連線攻擊。

Process Name	Process ID	Protocol	Local Port	Local Address	Remote Port	Remote Address	State	Process Path
svchost.exe	768	TCP	49153	::		::	Listening	C:\Windows\System32\svchost.exe
svchost.exe	812	TCP	49154	::		::	Listening	C:\Windows\System32\svchost.exe
System	4	TCP	47001	0.0.0.0		0.0.0.0	Listening	System
System	4	TCP	47001	::		::	Listening	System
wininit.exe	396	TCP	49152	0.0.0.0		0.0.0.0	Listening	C:\Windows\System32\wininit.exe
wininit.exe	396	TCP	49152	::		::	Listening	C:\Windows\System32\wininit.exe
svchost.exe	956	UDP	57851	0.0.0.0				C:\Windows\System32\svchost.exe
mssecsvc.exe	1104	TCP	51286	140.[redacted].43	445	92.149.107.15	Syn-Sent	C:\WINDOWS\mssecsvc.exe
mssecsvc.exe	1104	TCP	51287	140.[redacted].43	445	48.149.193.76	Syn-Sent	C:\WINDOWS\mssecsvc.exe
mssecsvc.exe	1104	TCP	51288	140.[redacted].43	445	61.76.48.20	Syn-Sent	C:\WINDOWS\mssecsvc.exe
mssecsvc.exe	1104	TCP	51290	140.[redacted].43	445	68.146.33.5	Syn-Sent	C:\WINDOWS\mssecsvc.exe
mssecsvc.exe	1104	TCP	51298	140.[redacted].43	445	214.254.212.56	Syn-Sent	C:\WINDOWS\mssecsvc.exe
mssecsvc.exe	1104	TCP	51302	140.[redacted].43	445	184.14.167.141	Syn-Sent	C:\WINDOWS\mssecsvc.exe
mssecsvc.exe	1104	TCP	51304	140.[redacted].43	445	94.89.108.205	Syn-Sent	C:\WINDOWS\mssecsvc.exe
mssecsvc.exe	1104	TCP	51305	140.[redacted].43	445	60.210.138.175	Syn-Sent	C:\WINDOWS\mssecsvc.exe
mssecsvc.exe	1104	TCP	51308	140.[redacted].43	445	104.133.190.36	Syn-Sent	C:\WINDOWS\mssecsvc.exe
mssecsvc.exe	1104	TCP	51313	140.[redacted].43	445	40.239.116.238	Syn-Sent	C:\WINDOWS\mssecsvc.exe
mssecsvc.exe	1104	TCP	51318	140.[redacted].43	445	100.254.120.227	Syn-Sent	C:\WINDOWS\mssecsvc.exe
mssecsvc.exe	1104	TCP	51325	140.[redacted].43	445	81.65.174.129	Syn-Sent	C:\WINDOWS\mssecsvc.exe
mssecsvc.exe	1104	TCP	51327	140.[redacted].43	445	1.199.242.100	Syn-Sent	C:\WINDOWS\mssecsvc.exe
mssecsvc.exe	1104	TCP	51330	140.[redacted].43	445	113.208.185.162	Syn-Sent	C:\WINDOWS\mssecsvc.exe

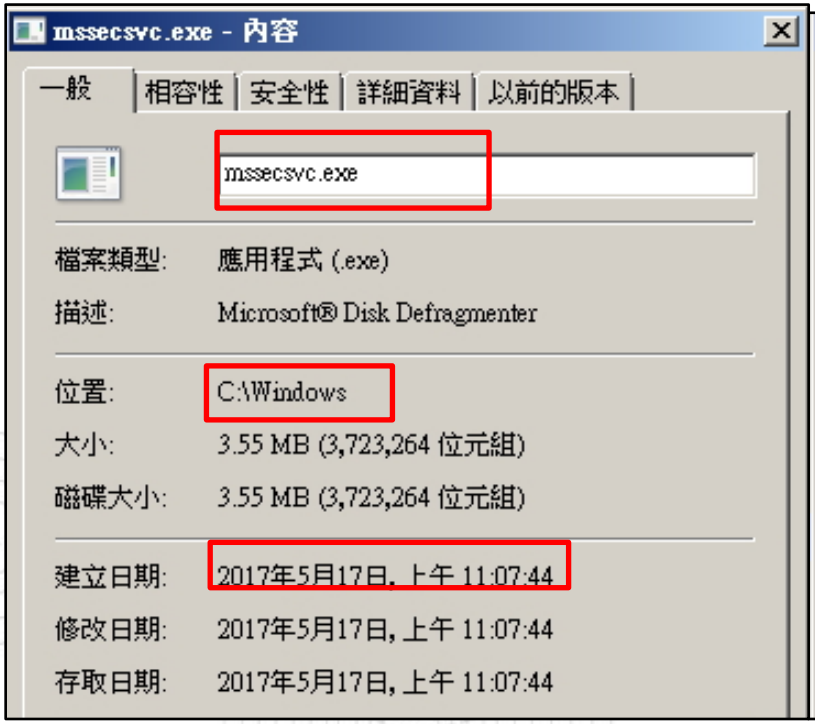
事件檢測

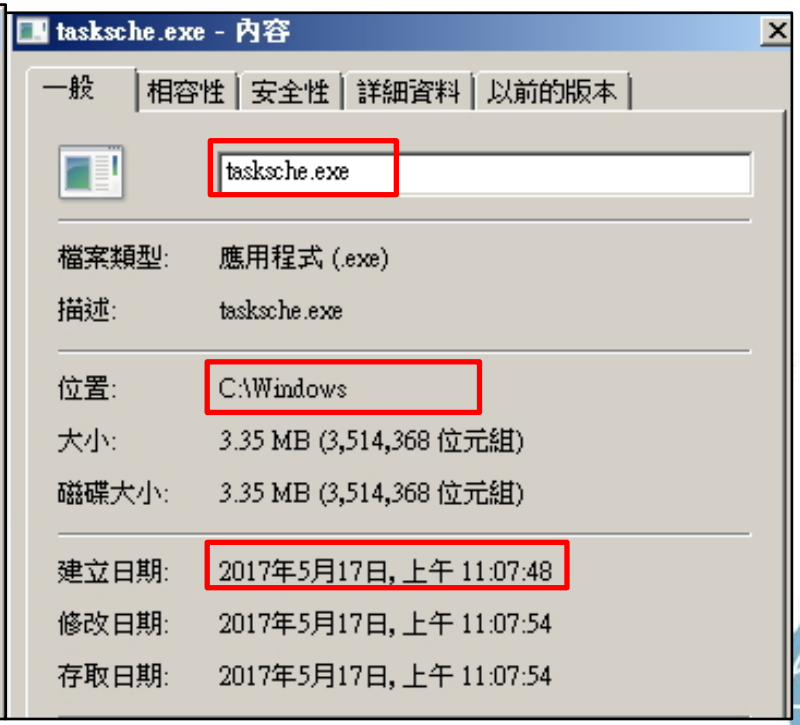
- 透過procexp與procmon工具檢視背景程式狀態，發現程式mssecsvc.exe執行時會啟動另一個程式tasksche.exe。



事件檢測

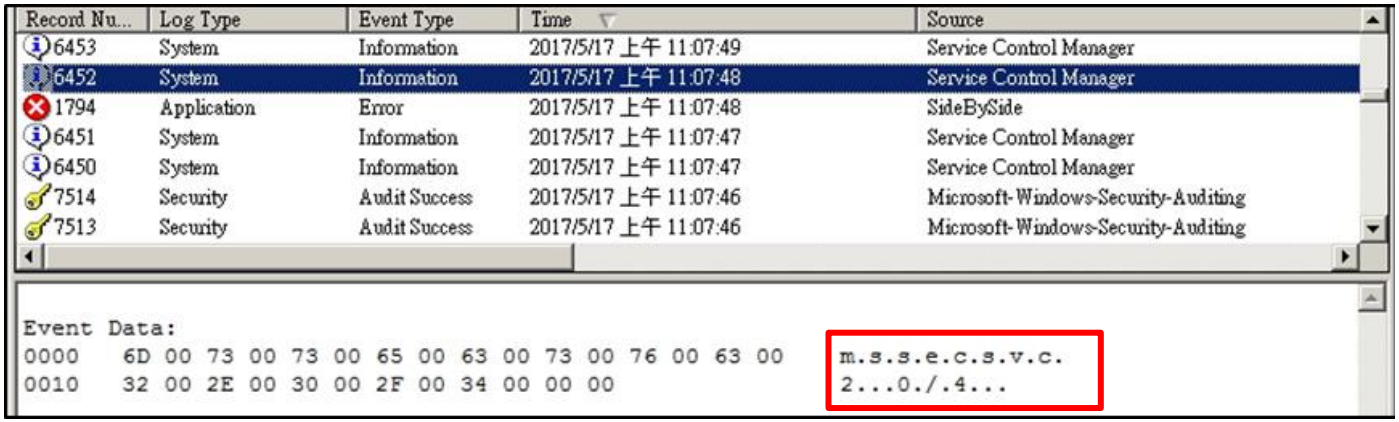
- 查看程式mssecsvc.exe與tasksche.exe 內容
- 建立日期皆為106年5月17日11:07
  - 推測可能為受測主機感染病毒的時間點。





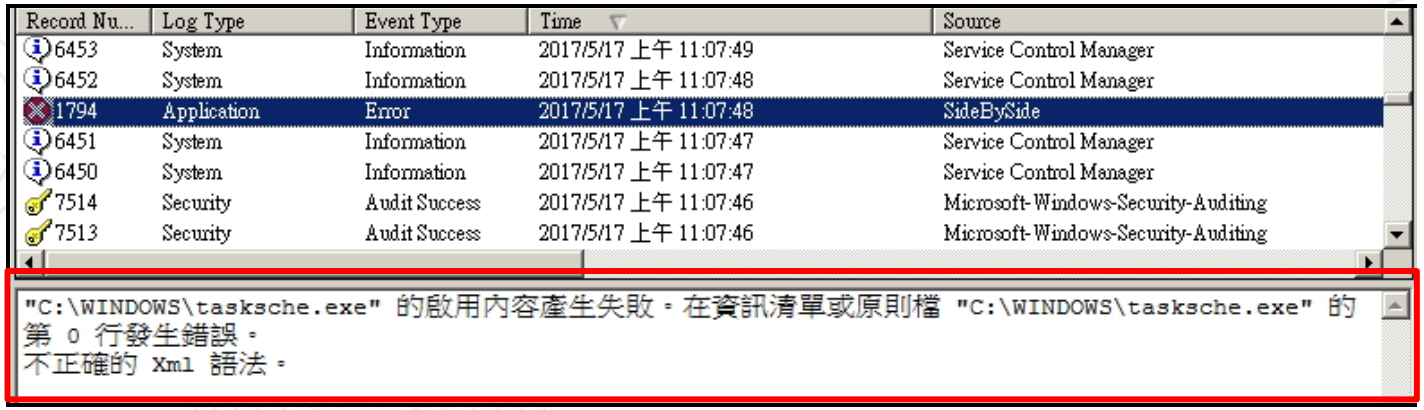
事件檢測

- 事件檢視紀錄發現
- 只有mmsecsvc.exe成功被執行
- tasksche.exe被啟用失敗，發生XML語法錯誤。



Record Nu...	Log Type	Event Type	Time	Source
6453	System	Information	2017/5/17 上午 11:07:49	Service Control Manager
6452	System	Information	2017/5/17 上午 11:07:48	Service Control Manager
1794	Application	Error	2017/5/17 上午 11:07:48	SideBySide
6451	System	Information	2017/5/17 上午 11:07:47	Service Control Manager
6450	System	Information	2017/5/17 上午 11:07:47	Service Control Manager
7514	Security	Audit Success	2017/5/17 上午 11:07:46	Microsoft-Windows-Security-Auditing
7513	Security	Audit Success	2017/5/17 上午 11:07:46	Microsoft-Windows-Security-Auditing

```
Event Data:
0000    6D 00 73 00 73 00 65 00 63 00 73 00 76 00 63 00    m.s.s.e.c.s.v.c.
0010    32 00 2E 00 30 00 2F 00 34 00 00 00                2...0./.4...
```



Record Nu...	Log Type	Event Type	Time	Source
6453	System	Information	2017/5/17 上午 11:07:49	Service Control Manager
6452	System	Information	2017/5/17 上午 11:07:48	Service Control Manager
1794	Application	Error	2017/5/17 上午 11:07:48	SideBySide
6451	System	Information	2017/5/17 上午 11:07:47	Service Control Manager
6450	System	Information	2017/5/17 上午 11:07:47	Service Control Manager
7514	Security	Audit Success	2017/5/17 上午 11:07:46	Microsoft-Windows-Security-Auditing
7513	Security	Audit Success	2017/5/17 上午 11:07:46	Microsoft-Windows-Security-Auditing

```
"C:\WINDOWS\tasksche.exe" 的啟用內容產生失敗。在資訊清單或原則檔 "C:\WINDOWS\tasksche.exe" 的
第 0 行發生錯誤。
不正確的 Xml 語法。
```

事件檢測

- Evidences:
  - 受測主機存在惡意程式 mssecsvc.exe與tasksche.exe
  - 大量以445連接埠對外連線攻擊的行為
- 推斷受測主機可能感染WannaCry病毒。
- 搜尋主機是否存在該病毒特徵:
  - tasksche.exe執行後會產生的三個檔案(@WanaDecryptor@.exe、Taskdk.exe與Taskdl.exe)
- 結果:無法搜尋到。
  - 可能與tasksche.exe無法被成功開啟有關。

事件檢測

- 檢視封包內容發現:
- mssecsvc.exe 對DNS發出網域名稱解析請求
  - 網域名稱 www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
  - Kill switch domain registered accidentally

	Time	Source	Destination	Protocol	Length	Info
40	34.304588	140.[redacted].43	140.[redacted].1	DNS	109	Standard query 0x8bee A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
41	34.304593	140.[redacted].43	140.[redacted].1	DNS	109	Standard query 0x8bee A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
42	34.316426	140.[redacted].1	140.[redacted].43	DNS	549	Standard query response 0x8bee A www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea

事件檢測

- 檢視封包內容與逆向工程mssecsvc.exe發現:
- mssecsvc.exe會檢查
  www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com網址是否可以連線
- 若無法連線，則繼續進行後續程式行為，判斷該網址為Kill-Switch

```
sub     esp, 50h
push    esi
push    edi
mov     ecx, 0Eh
mov     esi, offset aHttpWww_iuqerf ; "http://www.iuqerfsodp9ifjaposdfjhgosuri"...
lea     edi, [esp+58h+szUrl]
xor     eax, eax
rep movsd
```

```
aHttpWww_iuqerf db 'http://www.iuqerfsodp9ifjaposdfjhgo'
db 'surijfaewrwergwea.com',0
```

事件檢測

- 下圖為DNS回覆網域解析內容
  - 共對應到5台主機的IP位址
  - 第一台主機為104.17.37.137

```
> Frame 42: 549 bytes on wire (4392 bits), 549 bytes captured (4392 bits)
> Ethernet II, Src: [redacted] (80:[redacted]:81), Dst: [redacted] (00:[redacted]:1f)
> Internet Protocol Version 4, Src: 140.[redacted].1, Dst: 140.[redacted].43
> User Datagram Protocol, Src Port: 53, Dst Port: 51343
v Domain Name System (response)
    [Request In: 41]
    [Time: 0.011833000 seconds]
    Transaction ID: 0x8bee
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 5
    Authority RRs: 13
    Additional RRs: 7
  v Queries
    v www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com: type A, class IN
        Name: www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
        [Name Length: 49]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  v Answers
    > www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com: type A, class IN, addr 104.17.37.137
    > www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com: type A, class IN, addr 104.17.39.137
    > www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com: type A, class IN, addr 104.17.38.137
    > www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com: type A, class IN, addr 104.17.40.137
```

事件檢測

- 下圖為受測主機140.x.x.43連線到Kill-Switch網址的主機104.17.37.137之封包來往紀錄
  - 連線成功

	Time	Source	Destination	Protocol	Length	Info
43	35.553016	140.[illegible].43	104.17.37.137	TCP	66	49156 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
44	35.553021	140.[illegible].43	104.17.37.137	TCP	66	[TCP Out-Of-Order] 49156 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
45	35.579111	104.17.37.137	140.[illegible].43	TCP	66	80 → 49156 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PE
46	35.579454	140.[illegible].43	104.17.37.137	TCP	54	49156 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
47	35.579458	140.[illegible].43	104.17.37.137	TCP	54	[TCP Dup ACK 46#1] 49156 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
48	35.616897	140.[illegible].43	104.17.37.137	HTTP	154	GET / HTTP/1.1
49	35.616901	140.[illegible].43	104.17.37.137	TCP	154	[TCP Retransmission] 49156 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65536 L
50	35.643682	104.17.37.137	140.[illegible].43	TCP	60	80 → 49156 [ACK] Seq=1 Ack=101 Win=29696 Len=0
51	36.283536	104.17.37.137	140.[illegible].43	TCP	516	[TCP segment of a reassembled PDU]
52	36.283531	104.17.37.137	140.[illegible].43	HTTP	60	HTTP/1.1 200 OK (text/html)
53	36.283532	104.17.37.137	140.[illegible].43	TCP	60	80 → 49156 [FIN, ACK] Seq=468 Ack=101 Win=29696 Len=0
54	36.283978	140.[illegible].43	104.17.37.137	TCP	54	49156 → 80 [ACK] Seq=101 Ack=469 Win=65024 Len=0
55	36.283983	140.[illegible].43	104.17.37.137	TCP	54	[TCP Dup ACK 54#1] 49156 → 80 [ACK] Seq=101 Ack=469 Win=65024 Len=
56	36.339250	140.[illegible].43	104.17.37.137	TCP	54	49156 → 80 [FIN, ACK] Seq=101 Ack=469 Win=65024 Len=0
57	36.339254	140.[illegible].43	104.17.37.137	TCP	54	[TCP Out-Of-Order] 49156 → 80 [FIN, ACK] Seq=101 Ack=469 Win=65024
58	36.339393	140.[illegible].43	104.17.37.137	TCP	54	49156 → 80 [RST, ACK] Seq=102 Ack=469 Win=0 Len=0
59	36.339396	140.[illegible].43	104.17.37.137	TCP	54	49156 → 80 [RST, ACK] Seq=102 Ack=469 Win=0 Len=0
60	36.364724	104.17.37.137	140.[illegible].43	TCP	60	80 → 49156 [ACK] Seq=469 Ack=102 Win=29696 Len=0

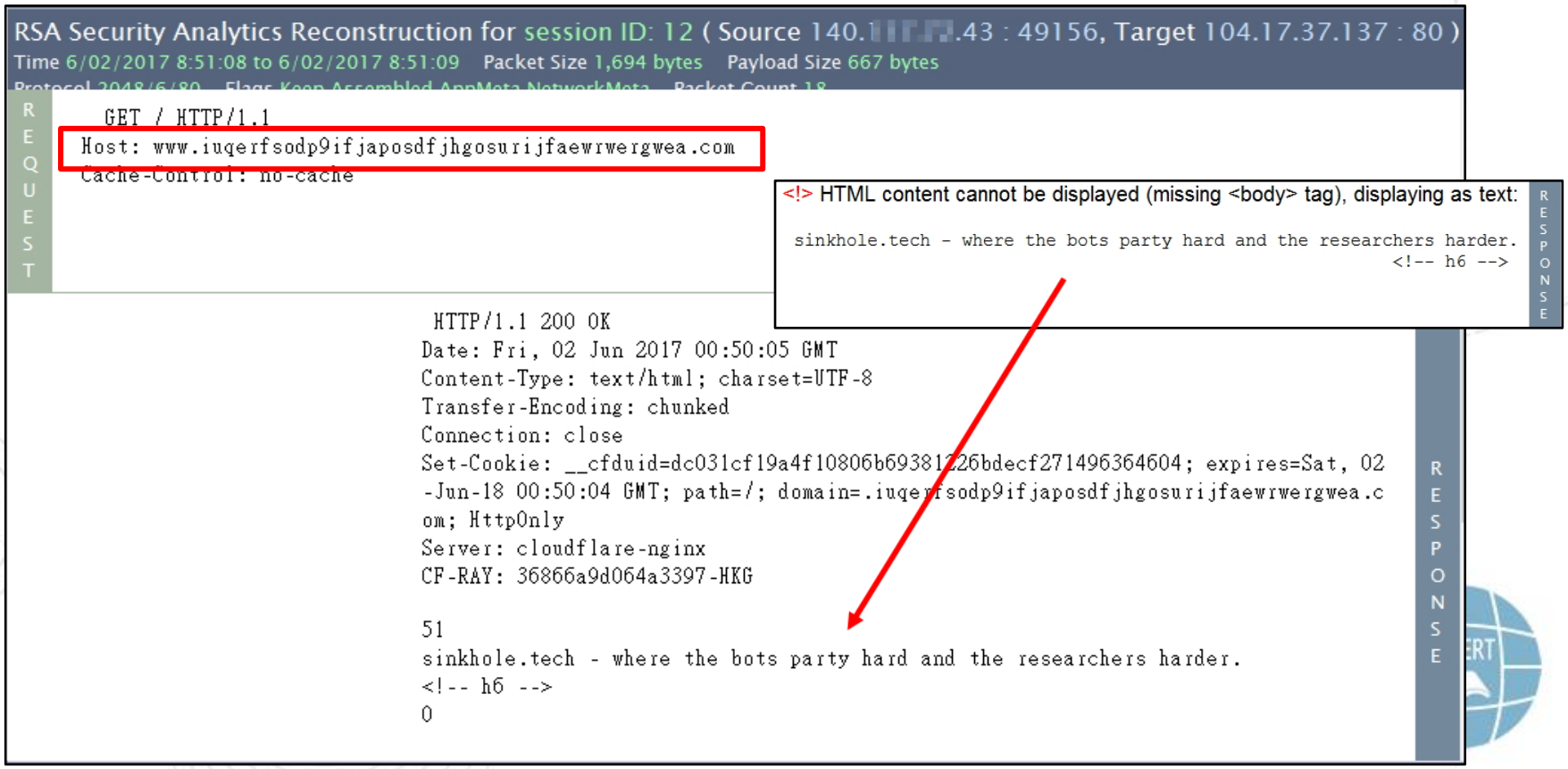
事件檢測

- 以Nmap工具檢視Kill-Switch網址所對應主機(104.17.37.137)之對外連線發現:
  - 443、80、8080、8443 開啟狀態
  - 該網址的80埠可連線

```
Discovered open port 443/tcp on 104.17.37.137
Discovered open port 80/tcp on 104.17.37.137
Discovered open port 8080/tcp on 104.17.37.137
Discovered open port 8443/tcp on 104.17.37.137
```

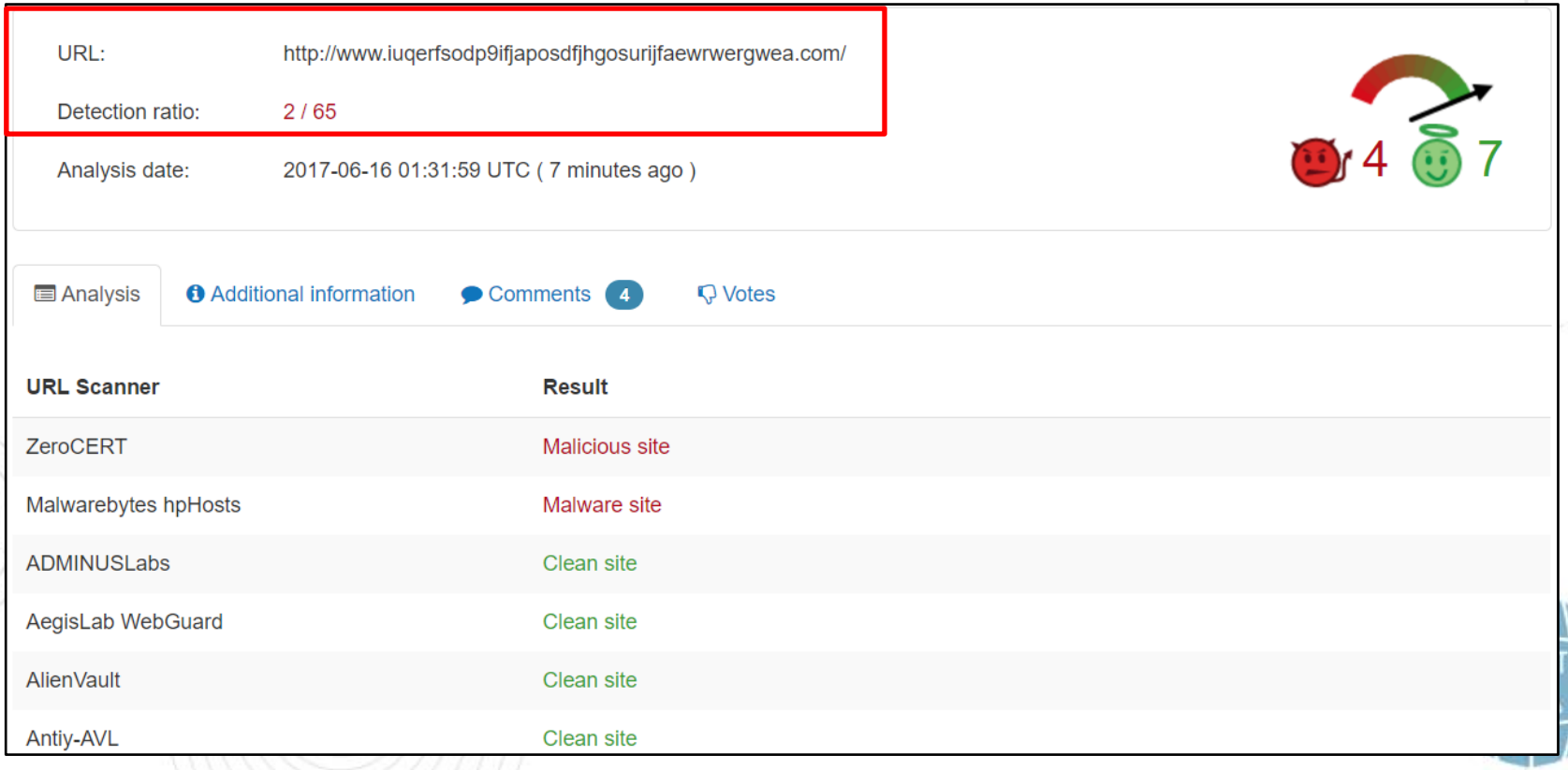
事件檢測

- 檢視受測主機連到Kill-Switch網址封包發現
  - 該網頁無法正常顯示
  - 該網址只是作為程式判斷是否可以連線的用途。



事件檢測

- 將該網址送到Virustotal檢測
  - 檢測比率為2/65



事件檢測

- 7小時測試期間，有70萬次 445埠攻擊
  – 232個國家

TCP Destination Port (3 items)

445 (cifs) (697,488) - 443 (https) (22) - 80 (http) (8)

Destination Country (232 items)

united states (299,870) - china (62,917) - japan (38,362) - united kingdom (24,711) - germany (22,644) - korea, republic of (21,310) - brazil (15,686) - france (15,496) - canada (13,659) - italy (10,293) - netherlands (9,683) - australia (9,462) - russian federation (8,471) - india (7,874) - taiwan (6,782) - spain (5,909) - south africa (5,479) - mexico (5,464) - sweden (4,997) - belgium (4,398) - poland (3,833) - egypt (3,810) - switzerland (3,762) - argentina (3,549) - indonesia (3,276) - colombia (3,225) - turkey (3,061) - norway (3,002) - vietnam (2,862) - finland (2,551) - denmark (2,357) - hong kong (2,341) - iran, islamic republic of (2,323) - ukraine (2,243) - austria (2,062) - ireland (1,979) - chile (1,850) - saudi arabia (1,842) - morocco (1,736) - thailand (1,680) - romania (1,652) - czech republic (1,604) - israel (1,526) - singapore (1,408) - new zealand (1,354) - venezuela (1,317) - malaysia (1,297) - portugal

事件檢測

- Virustotal檢測 mssecsvc.exe結果: 57/61

SHA256:	95ab184ecc89b9a593c024963650f54fe0a597c3f75d75ff3bf4f33f648c6d13
File name:	mssecsvc.exe
Detection ratio:	57 / 61
Analysis date:	2017-06-01 07:37:27 UTC (0 minutes ago)

- tasksche.exe檢測結果: 55/61

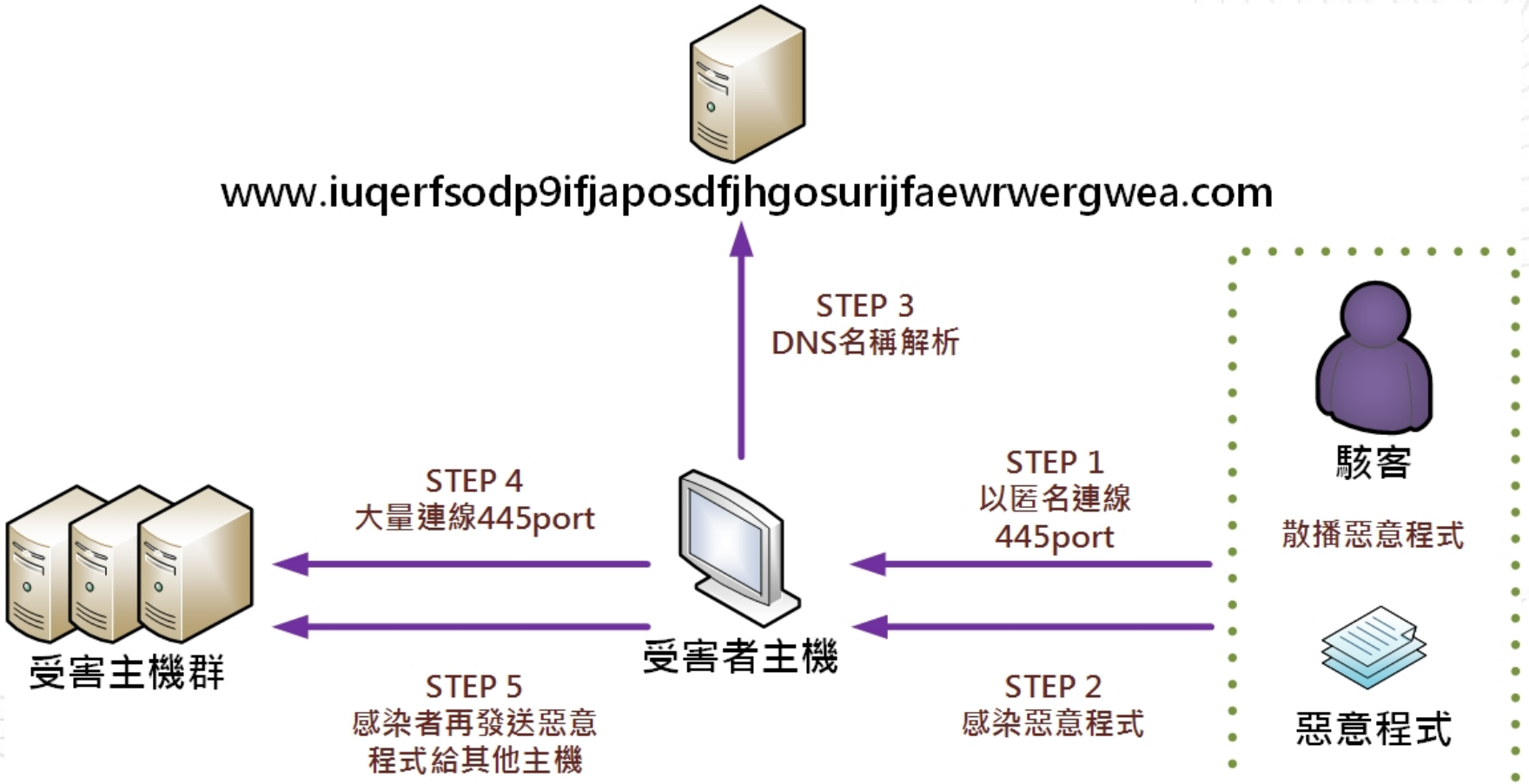
SHA256:	802d815d1cd9e4193cf586124622bde16ecb5d7127a1c0aa9a13d1e3e46f564a
File name:	tasksche.exe
Detection ratio:	55 / 61
Analysis date:	2017-06-01 07:52:38 UTC (0 minutes ago)

事件檢測

- 觀察待感染主機發現:
- 當受測主機進行445 port連線時，匿名連線方式與待感染主機建立連線
- 之後mssecsvc.exe與tasksche.exe安裝執行
- 受測主機與待感染主機兩者行為相同

	Time	Source	Destination	Protocol	Length	Info
1	0.000000	140.[redacted].43	140.[redacted].44	TCP	66	49287 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.000004	140.[redacted].43	140.[redacted].44	TCP	66	[TCP Out-Of-Order] 49287 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
3	0.000095	140.[redacted].44	140.[redacted].43	TCP	66	445 → 49287 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256
4	0.000097	140.[redacted].44	140.[redacted].43	TCP	66	[TCP Out-Of-Order] 445 → 49287 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len
5	0.000247	140.[redacted].43	140.[redacted].44	TCP	54	49287 → 445 [ACK] Seq=1 Ack=1 Win=65536 Len=0
6	0.000250	140.[redacted].43	140.[redacted].44	TCP	54	[TCP Dup ACK 5#1] 49287 → 445 [ACK] Seq=1 Ack=1 Win=65536 Len=0
7	0.000907	140.[redacted].43	140.[redacted].44	SMB	191	Negotiate Protocol Request
8	0.000911	140.[redacted].43	140.[redacted].44	TCP	191	[TCP Retransmission] 49287 → 445 [PSH, ACK] Seq=1 Ack=1 Win=65536
9	0.001203	140.[redacted].44	140.[redacted].43	SMB	171	Negotiate Protocol Response
10	0.001207	140.[redacted].44	140.[redacted].43	TCP	171	[TCP Retransmission] 445 → 49287 [PSH, ACK] Seq=1 Ack=138 Win=6553
11	0.026808	140.[redacted].43	140.[redacted].44	SMB	194	Session Setup AndX Request, User: anonymous
12	0.026811	140.[redacted].43	140.[redacted].44	TCP	194	[TCP Retransmission] 49287 → 445 [PSH, ACK] Seq=138 Ack=118 Win=65
13	0.027137	140.[redacted].44	140.[redacted].43	SMB	251	Session Setup AndX Response
14	0.027141	140.[redacted].44	140.[redacted].43	TCP	251	[TCP Retransmission] 445 → 49287 [PSH, ACK] Seq=118 Ack=278 Win=65
15	0.047142	140.[redacted].43	140.[redacted].44	SMB	146	Tree Connect AndX Request, Path: \\172.16.99.5\IPC$
16	0.047145	140.[redacted].43	140.[redacted].44	TCP	146	[TCP Retransmission] 49287 → 445 [PSH, ACK] Seq=278 Ack=315 Win=65
17	0.047253	140.[redacted].44	140.[redacted].43	SMB	114	Tree Connect AndX Response
18	0.047257	140.[redacted].44	140.[redacted].43	TCP	114	[TCP Retransmission] 445 → 49287 [PSH, ACK] Seq=315 Ack=370 Win=65
19	0.081932	140.[redacted].43	140.[redacted].44	SMB	1138	NT Trans Request, <unknown>
20	0.081935	140.[redacted].43	140.[redacted].44	TCP	1138	[TCP Retransmission] 49287 → 445 [PSH, ACK] Seq=370 Ack=375 Win=65
21	0.082067	140.[redacted].44	140.[redacted].43	SMB	93	NT Trans Response, <unknown (0)>
22	0.082070	140.[redacted].44	140.[redacted].43	TCP	93	[TCP Retransmission] 445 → 49287 [PSH, ACK] Seq=375 Ack=1454

網路架構圖


www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
STEP 3
DNS名稱解析
駭客
散播惡意程式
STEP 1
以匿名連線
445port
STEP 4
大量連線445port
受害者主機
受害主機群
STEP 5
感染者再發送惡意
程式給其他主機
STEP 2
感染惡意程式
惡意程式

網路架構圖

1. 駭客散播惡意程式，以匿名方式445port連線受害者主機。
2. 植入惡意程式mssecsvc.exe於受害主機，該程式會呼叫與執行另一個惡意程式tasksche.exe。
3. mssecsvc.exe進行DNS名稱解析。
4. 受害者主機對外進行大量445 port攻擊。
5. 受害者主機植入惡意程式到受感染主機。

建議與總結

此個案為電腦未執行系統更新來修補SMB漏洞，而被駭客透過開啟的445 port植入惡意程式。為有效預防感染WannaCry病毒，建議使用者進行下列的防禦措施:

1. 關閉 Windows系統的 445 通訊埠。
2. 立即使用隨身碟、外接硬碟或者雲端空間，備份重要資料。
3. 使用 Windows Update 自動更新或手動更新微軟KB4012215的漏洞修補程式(漏洞編號 MS17-010)。
4. 確認防毒軟體已更新至最新版本病毒碼與偵測程式碼，並定期執行電腦掃毒作業。


Q
&
A
dreamstime.com