# 教育機構資安回饋平台-DDOS 清洗系統操作手册 V2 版

TACERT 臺灣學術網路危機處理中心團隊 製 2019/12

- `	前言	. 2
ニヽ	系統說明	. 3
三、	操作說明(二線區縣市網路中心人員)	. 4
(1)	系統網址及登入說明	. 4
(2)	新增 DDoS 清洗服務申請	. 4
(3)	檢視 DDoS 工單資訊	. 5
(4)	自動產生告知通報事件單	. 6
四、	操作說明(SOC 人員)	. 7
(1)	系統網址及登入說明	. 7
(2)	新增 DDoS 清洗服務申請	. 7
(3)	管理 DDoS 工單	. 8



# 目錄

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 清洗系統」目前僅提供二線區縣市網路中心以及 SOC 團隊使用,若 學術單位遭受 DDoS 攻擊時,請透過其所屬之區縣市網路中心申請流量清洗 服務。教育體系 DDoS 攻擊清洗申請流程表依圖 1 所示,當 DDoS 攻擊清洗 完成後,平台會自動產生一張告知通報事件單,連線單位需登入資安通報 平台進行填寫通報應變措施,才算完成整個 DDoS 攻擊清洗申請流程。



圖1 教育體系 DDoS 攻擊清洗申請流程

#### 二、 系統說明

為方便二線區縣市網路中心人員以及 SOC 團隊人員使用, TACERT 團隊將「DDoS 清洗系統」整合進「教育機構資安通報回饋平台」, 使用者只需登入回饋平台即可使用此服務。



表1 DDoS 清洗作業系統功能說明

#### 三、 操作說明(二線區縣市網路中心人員)

下列將針對系統及子功能進行操作說明,並佐以畫面以利操作。

(1) 系統網址及登入說明

①系統網址:<u>https://portal.cert.tanet.edu.tw</u>

選擇	「資安通報報表系統」	,如圖3	0
----	------------	------	---

) () R(F) #1	🤗 https://j 輯(E) 檢視	portal	.cert.tanet.ec 我的最愛(A)	iu の + 工具(T)	▲ C (@); 説明(H)	portal.cert.tanet.edu.tw	×				- □ 分公	段 7
	Comput	ER EN	TANet Mergency Response Team				台灣學術 TAIWAN >>	網路危機處理 教育機構	<sup>p心</sup> 首女通	報回饋	P台	
						僅限二三線人員使用 催限發單單位使用	寶安逓報報表: 教育機構寶安3	<b>头送</b> 睡椒回讀平台				
	0	)+A	JX 64	+ <b>T</b>	圖	3 資安通	報報表	系統界面 <sup>終進</sup> ・1~1				
		211:	五 w	重叫		<del>限新·温</del> 森 登録	象界	面	<u></u>			
					使用者 密碼:	名稱:						
				<		971961 1				~		

#### (2) 新增 DDoS 清洗服務申請

①登入資安通報報表系統平台後先點選上方工作列「DDOS 清洗系統」, 再點選「新增申請單」。

OID查询 威脅名單 事件單列表 EWAP	別表 事件類型統計	等下單位密碼更動情況	DDOS#####				
		the second second second second	DO GOM DENK	9 新揃	由结留		
				新增申請單 4. 카기 7日	下明千~		
编號 申請時	調	清洗IP		通訊協定	東語峰	<b>秋</b> 苑	

圖 5 資安通報報表系統登錄後的界面

②產生如圖 6 所示的表單,平台會自動篩選出其轄下的連線單位列表供 使用者選擇,使用者將相關資訊(\*為必填欄位)填入「送出」即可。

清洗IP*		
單位名稱*	教育部	
通訊協定*	TCP 🔻	
服務說明*		例如:WEB FTP
通訊埠*		例如:80
申請理由		
	    洋山 ( 木 名 5 編 借 ) 南日	
	<u>这世</u> (小小尔部川重)通广	

- 圖 6 DDOS 清洗申請單表單內容
- (3) 檢視 DDoS 工單資訊

①點選「DDOS 清洗系統」功能將顯示所有 DDOS 工單資訊,其中「狀

態」說明如下
狀態:待處理(二線人員新增DDOS工單)
處理中(SOC人員正在處理)
處理完成並在保護中(已處理完成)
處理完成並已移出保護中(已處理完成)
失敗(SOC處理該工單失敗,無法清洗)

<mark>報表</mark> Develop	<mark>运)系统</mark> ed By TACER	Ŧ					_				
OID查詢	威脅名單	事件單列表	EWA列表	事件類型統計	轄下單位密碼更動情況	DDOS清洗系統	DDOS清洗功能				
							新增申請單				
編號 2000 111	10/2017-02-15	11:19:11	申謝問		140.117.101.5	達洗IP	tcp	通訊協定	道話追 80	<b>狀態</b> 待處理	檢視
										1.待處理	
										2.處理中 3.處理完成	
										1-總位八郎	

圖 7 檢視 DDoS 工單資訊

② 點選「檢視」即可查詢該工單,如圖 8 所示,其中「回覆意見」為 SOC 對於該 DDOS 工單的回覆(例如:無法清洗的原因)。

		close or Esc Key
編號	12	
申請時間	2017-03-07 09:52:35	
清洗IP	140.117.101.5	
通訊協定	tcp	
服務說明	WEB	
通訊埠	80	
狀態	待處理	
申請理由	遭受攻擊 	
回覆意見		
	圖 8	

#### (4) 自動產生告知通報事件單

當 SOC 中心完成清洗後,會登入 DDoS 清洗系統將工單狀態改為「處理完成」,此時平台會自動產生一張告知通報事件單至「教育機構資安通報應變 平台」,連線單位需依照「教育機構資安通報應變流程」完成填寫通報應變 ->二線區縣市網路中心通報審核->TACERT 團隊通報審核,此 DDoS 攻擊事 件單才算完整結案。

- 四、 操作說明(SOC 人員)
  - (1) 系統網址及登入說明

①系統網址:<u>https://portal.cert.tanet.edu.tw</u> 選擇「教育機構資安通報回饋平台」,如圖9。

(+) () https://portal.cert.tanet.edu.tw/index.html	\$ ★ ∰ 58€+Q
COMPUTER EMERGENCY RESPONSE TEAM	台灣學術網路危機處理中心 TAIWAN >>>>教育機構貧安通報回饋平台
	催眠二三線人員使用 <b>資気通報報表系統</b> 僅限發單單位使用 <b>教育機構資気通報回顧平台</b>
圖 9 教 ② 於登錄畫面鍵入	育機構資安通報回饋平台界面 帳號、密碼及驗證碼,如圖10。
	登錄界面
使用	1#4#: 6: 69108m
X	
(2) 新增 DDoS 清洗服務	圖 10 登録芥面 申請
①登入「資安通報回 統」,再點選「新建 DDC	7饋系統平台」後先點選上方工作列「DDOS 清洗系 S 工單」。
COMPUTER EMERGENCY Response Team	台灣學術網路危機處理中心 TAIWAN <sup>333</sup> 教育機構貪安通報回饋平台
基本資料 報表系統 登入LOG管理	1. DDOS 清洗系統 DDOS清洗系統 登出
	新達DDOS工單 管理DDOS工單
[語號[申読時間][清洗中]]通訊協定[通訊埠[[款册]]] Page 1/1	

圖 11 教育機構資安通報回饋平台登錄後的界面 ②產生如圖 12 所示的表單,單位名稱可輸入關鍵字,平台會進行模糊比 對,再點選出正確的單位名稱,使用者將相關資訊(\*為必填欄位)填入,, 送出即可。

清洗IP*	
單位名稱*	國立中山大學-2.16.886.111.1(
通訊協定*	TCP •
服務說明 <mark>*</mark>	例如:WEB FTP
通訊埠*	例如:80
申請理由	
	送出

圖 12 DDOS 清洗申請單表單內容

## (3) 管理 DDoS 工單

① 點選「管理 DDOS 工單」可查詢到所有 DDoS 工單的狀態。

COM	TANet PUTER EMERGENCY Response Team			CERT	台灣 TAIWA	學術網 N >>> 才
	基本資料 報表系統	登入LOG管理	e DDOS)	青洗系統	登出	
_						
编 <b>號</b> 20	申請時間 2017-03-13 14:32:45	清洗IP	通訊協定 tcp	通訊埠 80	状態	儲改
<b>編號</b> 20 19	<b>申請時間</b> 2017-03-13 14:32:45 2017-03-13 14:29:07	<b>涛洗P</b> 11111 140.117.72.33	通訊協定 tcp TCP/UDP	<b>通訊埠</b> 80 53	<b>默態</b> 待處理 待處理	修改修改
<b>編號</b> 20 19 18	<b>申請時間</b> 2017-03-13 14:32:45 2017-03-13 14:29:07 2017-03-10 08:42:42	<b>)清洗IP</b> 11111 140.117.72.33 140.117.101.6	通訊協定 tcp TCP/UDP tcp	[通訊埠] 80 53 80	<b>狀態</b> 待處理 待處理 處理完成	修改 修改 修改

### 圖 13 管理 DDOS 工單的界面

②SOC 人員於清洗完成後,可點選「修改」,更改「狀態」以及填寫「回覆 理由」。

基	本資料 報表系統 登入LOG管理	DDOS清洗系統	登出	
扁號	20			
申請時間	2017-03-13 14:32:45			
青洗IP	11111			
通訊協定	tcp			
服務說明	1356			
通訊埠	80			
申請理由		li		
犬態	待處理 ▼			
回覆理由		<i>h</i>		
	送出			
			10	

9