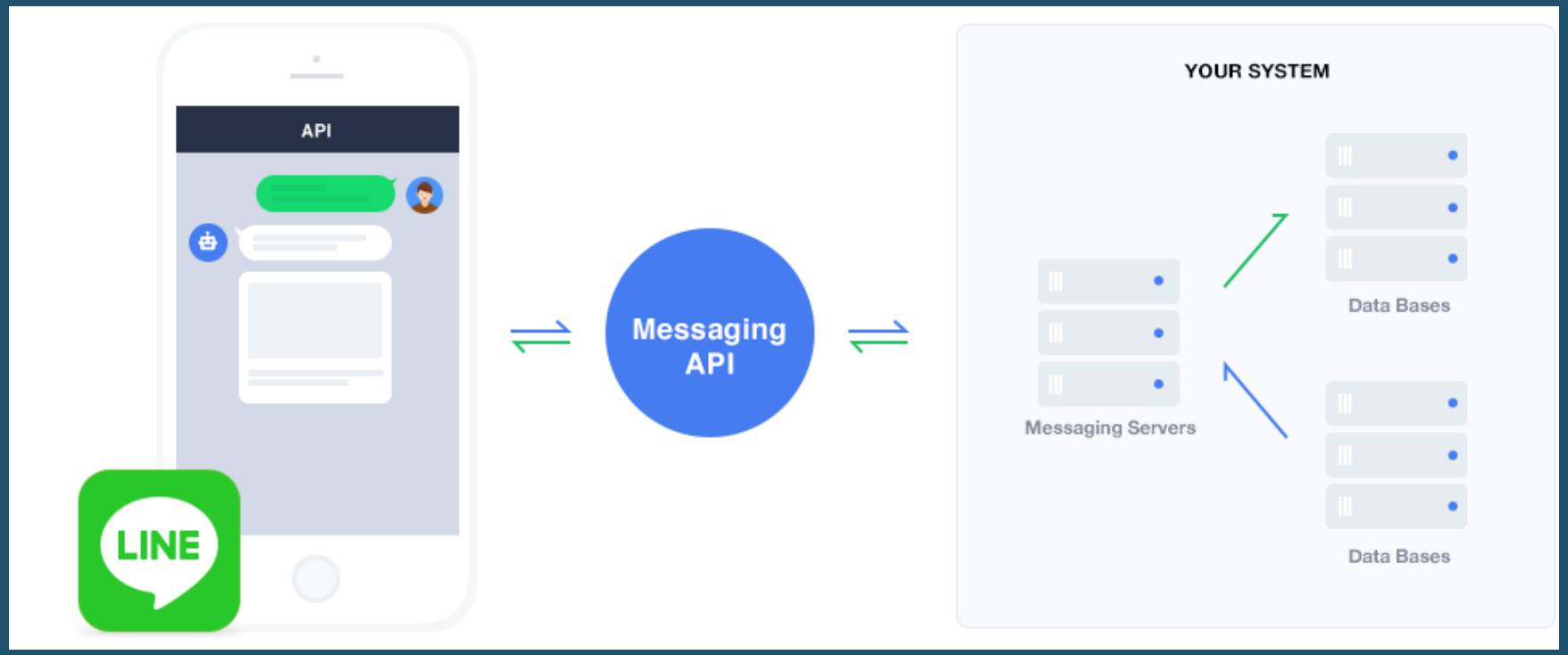
運用手機通訊軟體
自動即時通知網路資安事件

陳仕豪　2017/09/05

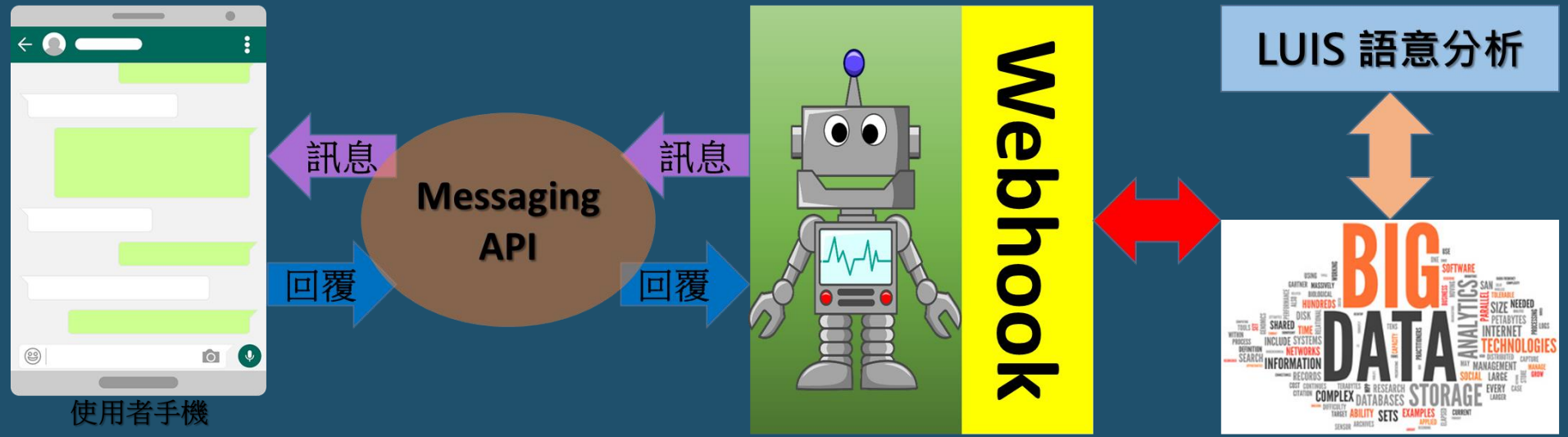
關於 LINE BOT

- 是一項能夠讓 LINE 用戶與您所提供的服務進行雙向溝通的功能。
- 新版叫做 Messaging API。
- Messaging API 將透過 LINE 伺服器，在您的伺服器與 LINE 應用程式間互相收發訊息。



關於 LINE BOT

- 所有從用戶傳送給 LINE BOT 的訊息，就會傳送到 **Webhook**，而你透過程式碼寫的這個Webhook，在接收到這個訊息之後，就可以依照用戶的訊息內容，來回應(回覆)不同的訊息給用戶。這就是一個 LINE 對談器人最基本的架構：

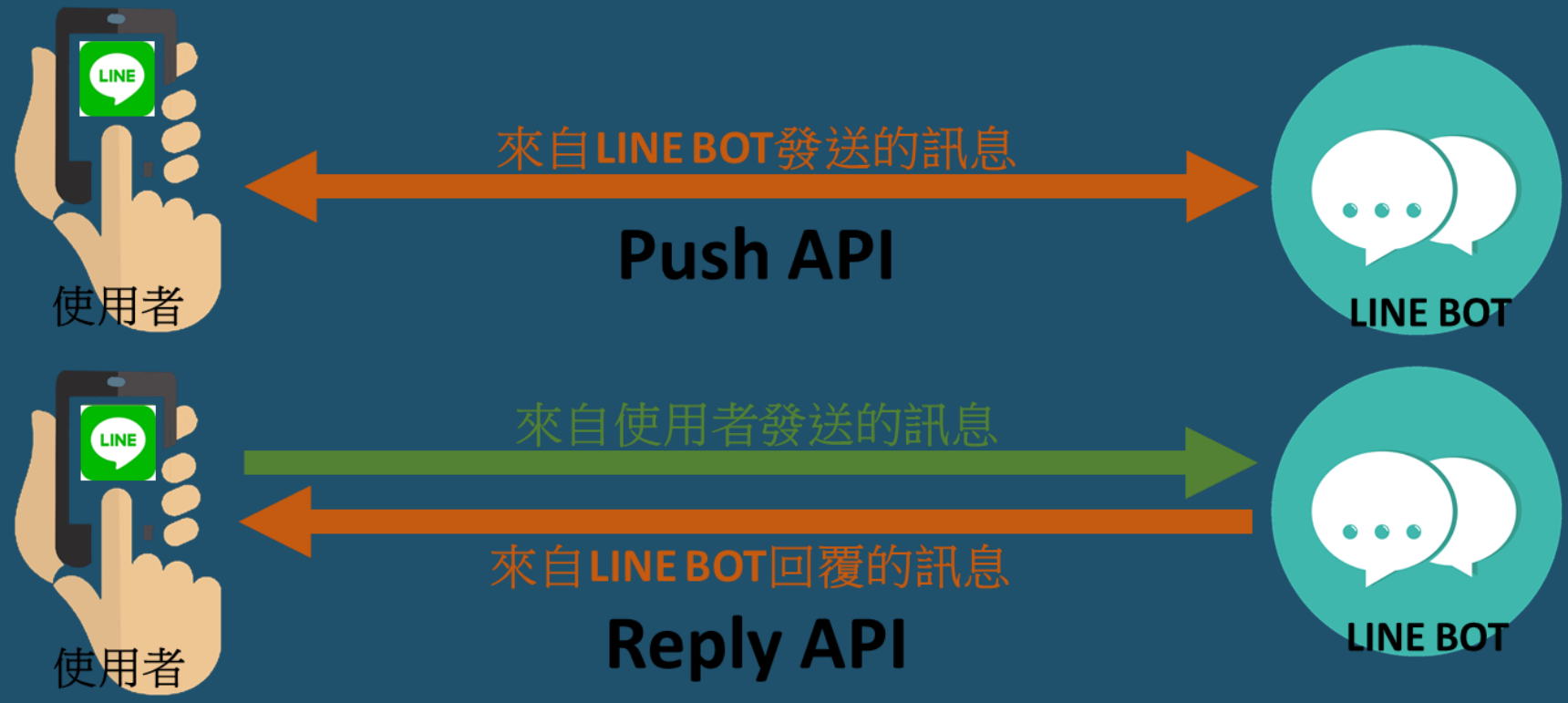


Webhook 是一種 Http 推送 API，為所建立的應用服務提供即時回覆訊息的一種方法。當 Webhook 被觸發後，會將回覆內容傳送到應用程式端去，這樣使用者可以立即獲得回覆訊息。

關於 LINE BOT

- Push API 與 Reply API
- Push API 指的是 BOT 能夠在任何時間點主動對用戶傳送訊息的 API。
- Reply API 指的是 BOT 可以針對用戶傳來的訊息進行回覆的 API。

我們用這個！



關於 LINE BOT

- 申請 LINE BOT (https://business.line.me/zh-hant/services/bot)

1. 開始使用 Messaging API
2. 開始使用 Developer Trial
3. 若要透過現有 LINE 帳號開始使用 Messaging API....

如果你選擇1,2，其實是先建立一個 LINE 帳號，然後頁面會引導你把該 LINE 帳號轉成支援 Messaging API。如果你選擇3，則是把以前舊的 LINE 帳號改為支援 Messaging API。但請注意，當你的 LINE 改為支援 Messaging API 之後，你就不能用你的 LINE App 直接回覆用戶的訊息了(而且這動作不可逆，也就是轉過去轉不回來)，用戶的訊息也只會被轉傳到你的 LINE Webhook URL，讓你透過 BOT 程式碼來回覆訊息。

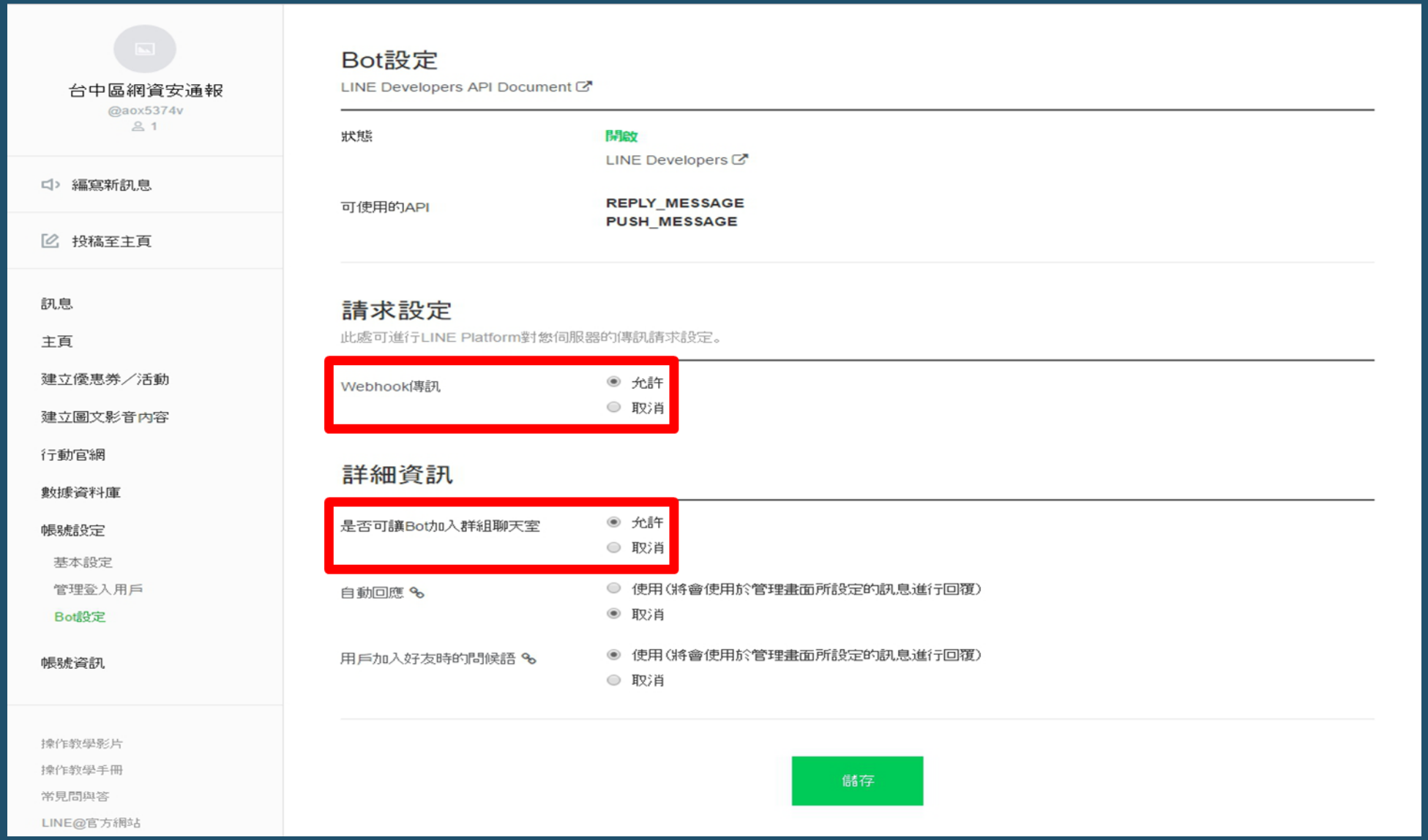
關於 LINE BOT

方案介紹

加入各種方案，即可使用方便的Messaging API功能。

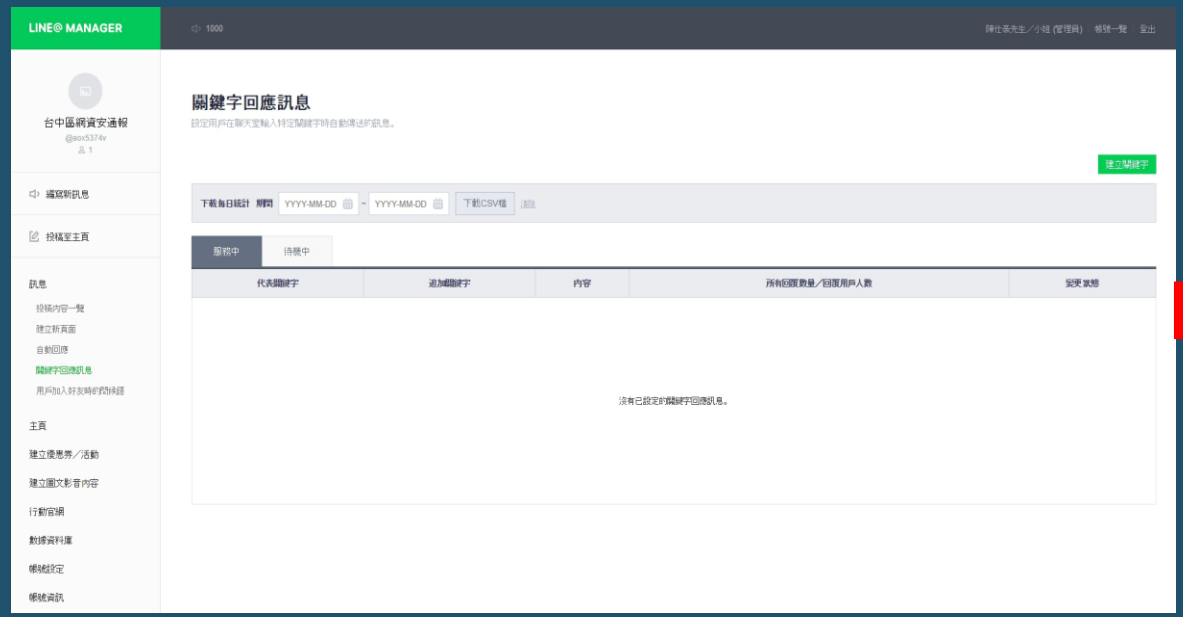
		Developer Trial 0元 月費	免費版 0元 月費	入門版 798元 月費	進階版(API) 3,888元 月費	專業版(API) 8,888元 月費
Messaging API	Reply API	○	○	○	○	○
	Push API	○	×	×	○	○
各項限制	好友人數	50人	-	-	-	-
其他功能	LINE@的功能		另外還提供其他各種功能。 詳細內容請見LINE@的服務介紹頁面。 進階版(API)或專業版(API)方案能使用的LINE@功能 與進階版或專業版方案相同。			
選購項目	專屬ID	×	798元(第一年) 398元(第二年起可享此優惠價)			

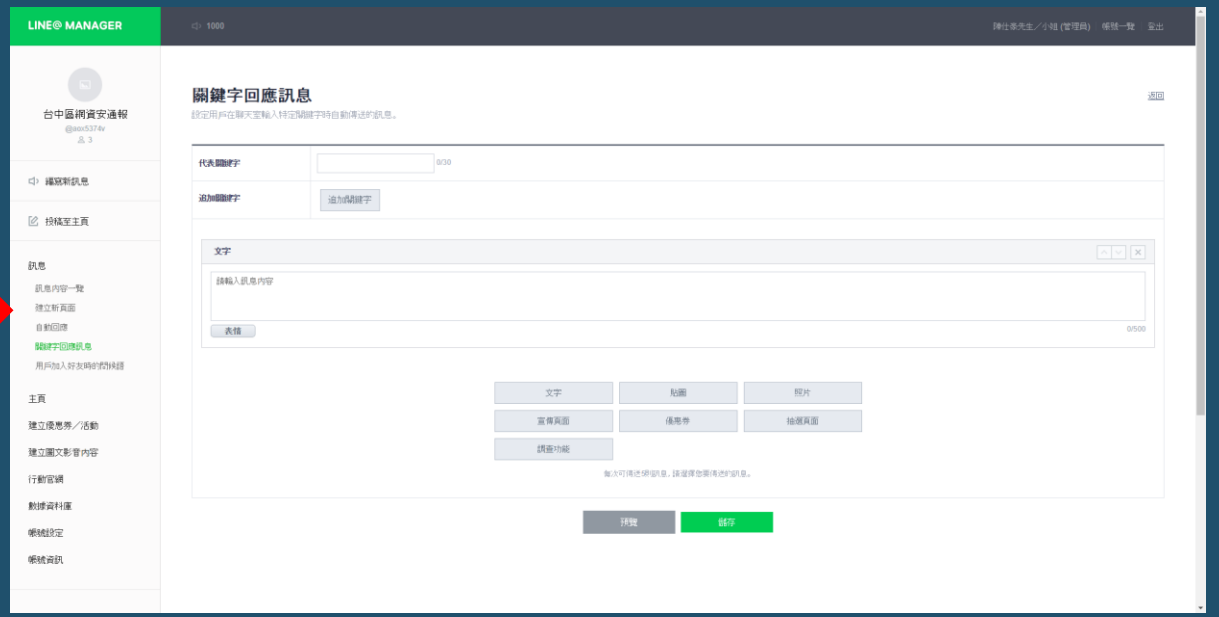
LINE BOT 設定


台中區網資安通報
@aox5374v
1
編寫新訊息
投稿至主頁
訊息
主頁
建立優惠券／活動
建立圖文影音內容
行動官網
數據資料庫
帳號設定
基本設定
管理登入用戶
Bot設定
帳號資訊
操作教學影片
操作教學手冊
常見問與答
LINE@官方網站
Bot設定
LINE Developers API Document
狀態
開啟
LINE Developers
可使用的API
REPLY_MESSAGE
PUSH_MESSAGE
請求設定
此處可進行LINE Platform對您伺服器的傳訊請求設定。
Webhook傳訊
允許
取消
詳細資訊
是否可讓Bot加入群組聊天室
允許
取消
自動回應
使用(將會使用於管理畫面所設定的訊息進行回覆)
取消
用戶加入好友時的問候語
使用(將會使用於管理畫面所設定的訊息進行回覆)
取消
儲存

LINE BOT 開發

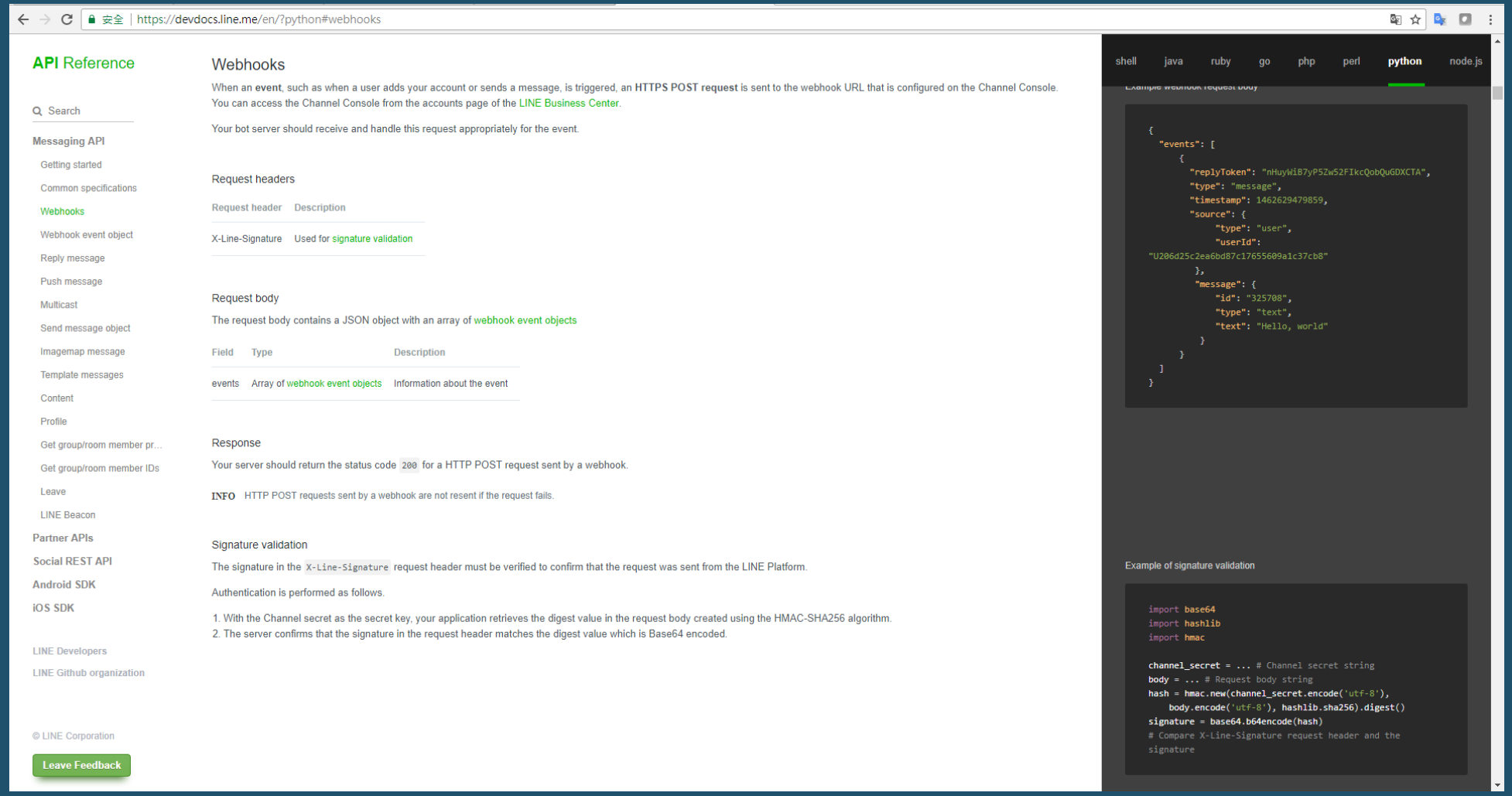
- 簡單製作回應訊息



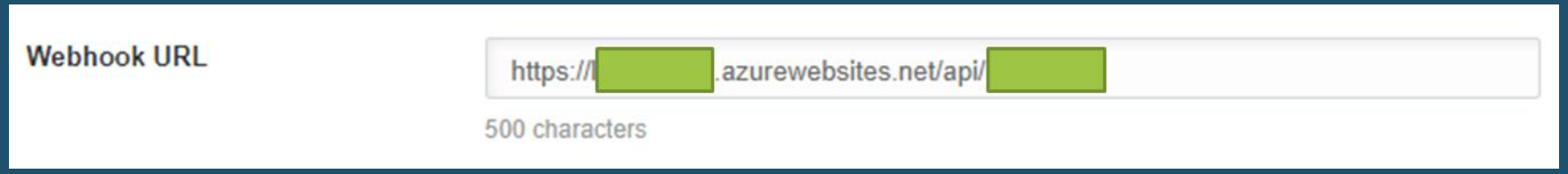


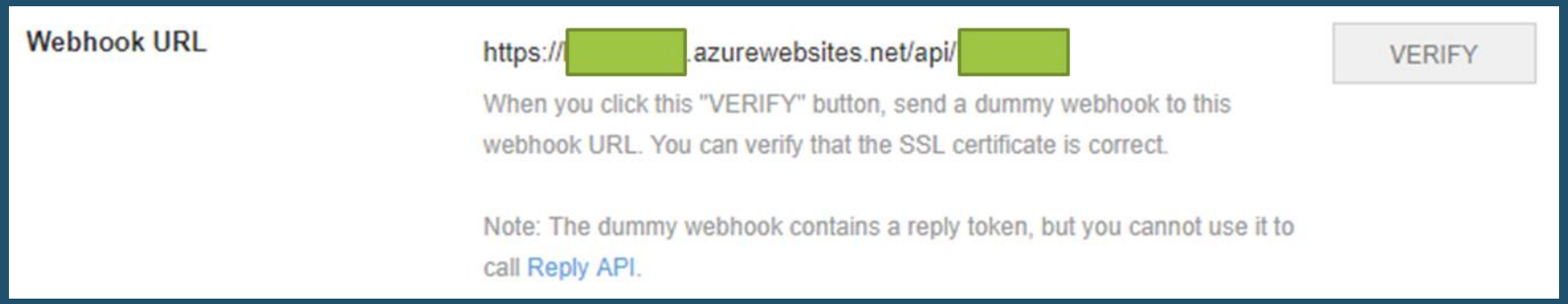
LINE BOT 開發

- LINE Messaging API Reference (https://devdocs.line.me/en/#messaging-api)



LINE BOT 開發

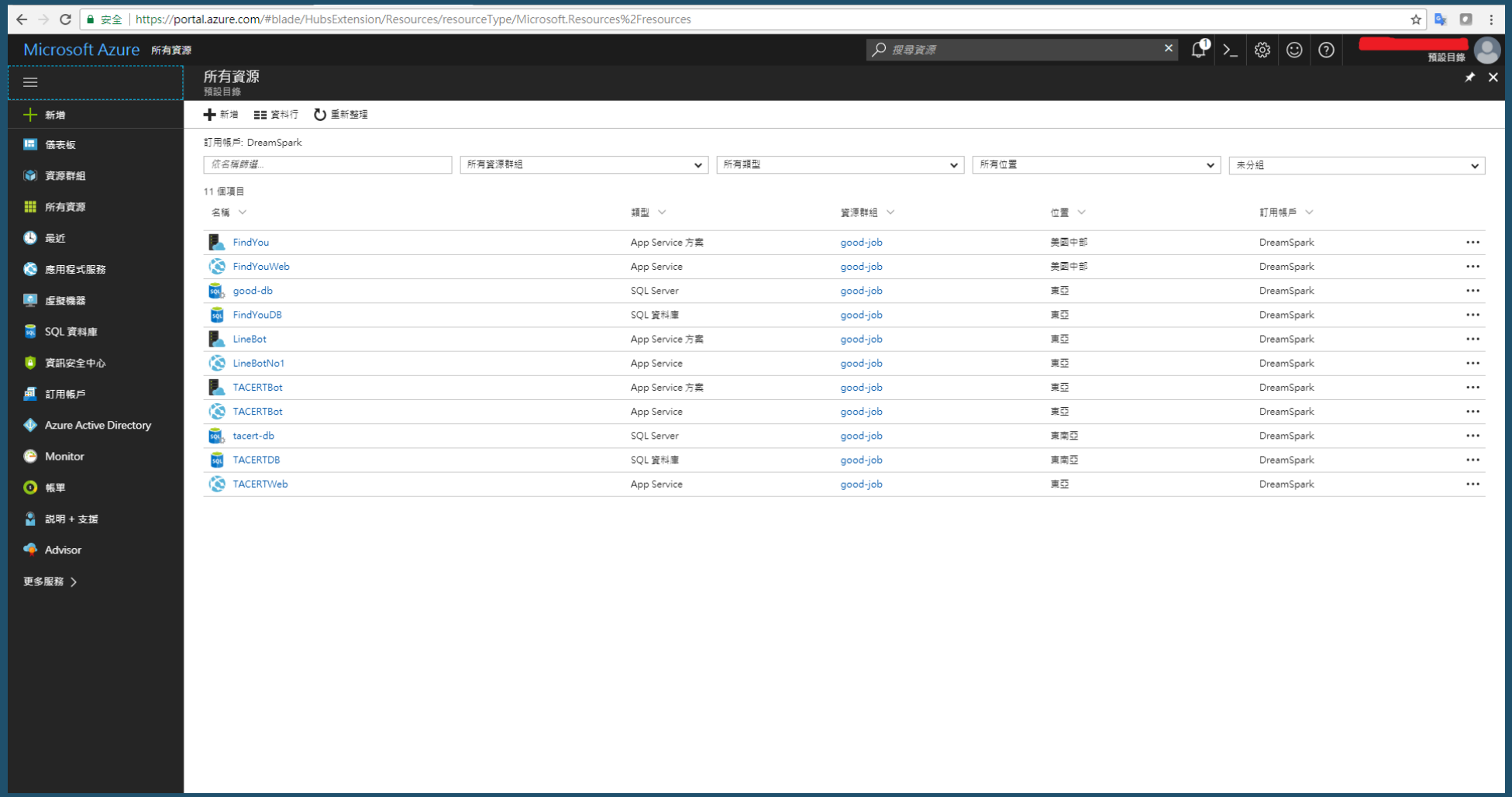




需要支援 SSL 的網站

LINE BOT 開發

- Microsoft Azure (https://azure.microsoft.com/zh-tw/)



LINE BOT 開發

- LINE BOT 傳送與接收的訊息封包

使用 LINE BOT 於資安通報

- 運作流程 1：取得 LINE 群組 GROUP ID

群組將 LINE BOT 加為好友

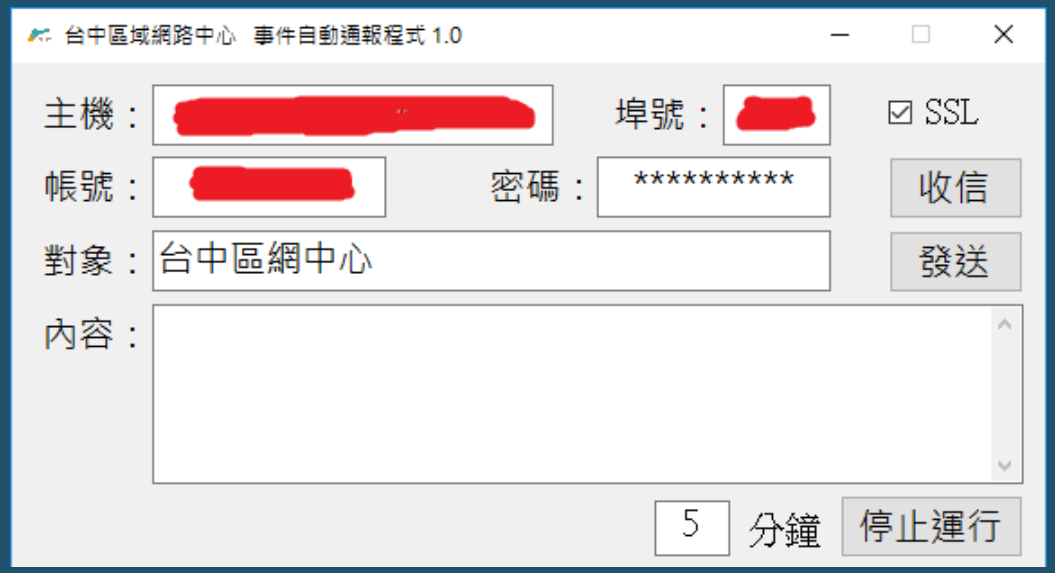
向 LINE BOT 發送對話訊息

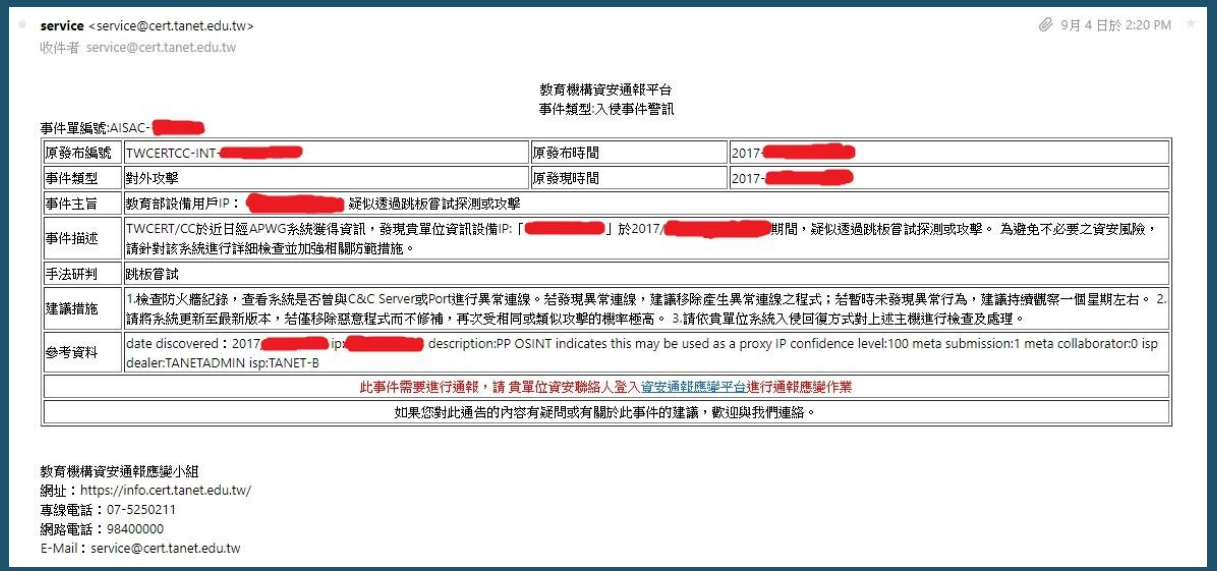
Webhook 程式解析對話 JSON 封包取得群組 GROUP ID

使用 LINE BOT 於資安通報

- 運作流程 2：接收資安通報信件，解析信件資料
  - ➢ 找出通報單位，與通報事件

確認是否有資安通報郵件 → 接收資安通報郵件 → 解析郵件資料 找出通報單位 與事件類型





service <service@cert.tanet.edu.tw>
收件者 service@cert.tanet.edu.tw
9月 4 日於 2:20 PM

教育機構資安通報平台
事件類型:入侵事件警訊

事件單編號:AISAC-[redacted]

原發布編號	TWCERTCC-INT-[redacted]	原發布時間	2017[redacted]
事件類型	對外攻擊	原發現時間	2017-[redacted]
事件主旨	教育部設備用戶IP：[redacted] 疑似透過跳板嘗試探測或攻擊		
事件描述	TWCERT/CC於近日經APWG系統獲得資訊，發現貴單位資訊設備IP:「[redacted]」於2017/[redacted]期間，疑似透過跳板嘗試探測或攻擊。 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	跳板嘗試		
建議措施	1.檢查防火牆紀錄，查看系統是否曾與C&C Server或Port進行異常連線。若發現異常連線，建議移除產生異常連線之程式；若暫時未發現異常行為，建議持續觀察一個星期左右。 2.請將系統更新至最新版本，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。 3.請依貴單位系統入侵回復方式對上述主機進行檢查及處理。		
參考資料	date discovered：2017[redacted] ip[redacted] description:PP OSINT indicates this may be used as a proxy IP confidence level:100 meta submission:1 meta collaborator:0 isp dealer:TANETADMIN isp:TANET-B		
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。			

教育機構資安通報應變小組
網址：https://info.cert.tanet.edu.tw/
專線電話：07-5250211
網路電話：98400000
E-Mail：service@cert.tanet.edu.tw

使用 LINE BOT 於資安通報

- 運作流程 2：接收資安通報信件，解析信件資料
  - ➢ 找出通報單位

完成通報內容重新組合 → 將訊息內容與群組 GROUP ID 包裝成 JASON 訊息封包 → 將包裝好的 JASON 封包透過 API 發送至 LINE 群組

```
{
 'events':
  [
   {
    'type':'message',
    'replyToken':'c049d461facc41268cf74dd0c79b5843',
    'source':
     {
      'groupId':'C8c86064b3991[redacted]',
      'userId':'Ufe21d353ced1b[redacted]',
      'type':'group'
     },
    'timestamp':1498809522091,
    'message':
     {
      'type':'text',
      'id':'6316095243215',
      'text':'?你好'
     }
   }
  ]
}
```

LINE BOT 開發參考

http://studyhost.blogspot.tw/2016/05/linebot-1-clinebot.html