(ANA事件單通知:TACERT-ANA-2025121101120000)(【攻擊預警】社交工程攻擊通告：請加強防範以行政訴訟為由之社交工程郵件攻擊)

1 封郵件

service <service@cert.tanet.edu.tw> 2025年12月12日上午9:18
收件者: service@cert.tanet.edu.tw

教育機構ANA通報平台

發佈編號	TACERT-ANA-2025121101120000	發佈時間	2025-12-11 13:24:01
事故類型	ANA-攻擊預警	發現時間	2025-12-11 13:24:01
影響等級	低		

[主旨說明:]【攻擊預警】社交工程攻擊通告：請加強防範以行政訴訟為由之社交工程郵件攻擊

[內容說明:]

轉發　國家資安資訊分享與分析中心 資安訊息警訊 NISAC-400-202512-00000018

本院近期接獲外部情資，攻擊者以行政訴訟為由發動社交工程郵件攻擊，誘導收件者開啟並下載與執行惡意附檔。建議貴單位加強防範與通知各單位提高警覺，避免點擊郵件附檔與連結，以免受駭。 已知攻擊郵件特徵如下，相關受駭偵測指標請參考附件。

1.駭客寄送之主旨： [機關名稱]

2.相關惡意中繼站: giugh9ygiuhljbgh-1328314126[.]cos[.]ap-tokyo[.]myqcloud[.]com、202[.]79[.]168[.]155

3.惡意附檔SHA1雜湊值： 770e64e02d2cf2cac30d6074c201d44279996cbc、e69b347f9608abaf31cab02f0a34b3dfa1d7c872
註：相關網域名稱為避免誤點觸發連線，故以「[.]」區隔。

情資分享等級: WHITE(情資內容為可公開揭露之資訊)
此訊息僅發送到「區縣市網路中心」，煩請貴單位協助轉發與通知轄下各單位知悉

[影響平台:]

N/A

[建議措施:]

1.網路管理人員請參考受駭偵測指標，確實更新防火牆，阻擋惡意中繼站。

2.建議留意可疑電子郵件，注意郵件來源正確性，勿開啟不明來源之郵件與相關附檔。

3.安裝防毒軟體並更新至最新病毒碼，開啟檔案前使用防毒軟體掃描郵件附檔，並確認附檔檔案類型，若發現檔案名稱中存在異常字元(如lnk, rcs, exe, moc等可執行檔案附檔名的逆排序)，請提高警覺。

4.加強內部宣導，提升人員資安意識，以防範駭客利用電子郵件進行社交工程攻擊。

[參考資料:]
附件-社交工程攻擊_IOC：https://cert.tanet.edu.tw/pdf/report_IoC_1210.csv

(此通報僅在於告知相關資訊，並非為資安事件)，如果您對此通報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