教育機構 ANA 通報平台

發佈編號	TACERT-ANA-2026013008012222	發佈時間	2026-01-30 08:58:23
事故類型	ANA-攻擊預警	發現時間	2026-01-30 08:58:23
影響等級	低		

[主旨說明:]【攻擊預警】社交工程攻擊通告：請加強防範偽冒行政院法規會名義並以修正就業安定基金收支保管及運用辦法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-400-202601-00000012

資安院近期接獲外部情資，攻擊者以「修正就業安定基金收支保管及運用辦法第 5 條條文」為由，寄送含惡意下載連結之社交工程釣魚郵件，誘導收件者點擊郵件內釣魚連結並下載惡意檔案。

建議貴單位加強防範與通知各單位提高警覺，避免點擊該郵件帳號寄送之信件、釣魚連結與附檔，以免受駭。

已知攻擊相關郵件特徵如下：

1.駭客利用之寄件帳號：「executive_yuan@boitedebijou.com.tw」、「executive-yuan@boitedebijou.com.tw」

2.主旨：「修正「就業安定基金收支保管及運用辦法」第 5 條條文」

3.相關惡意連結：hxxps://www[.]boitedebijou[.]com[.]tw/Mns/populace/EYG/e_detail[.]do?metaid=162736&accesskey_c=3447

4.惡意檔案名稱：「1140202422A.rar」、「1140202422A.chm」

5.相關惡意中繼站：79[.]108[.]224[.]222

6.惡意檔案 SHA1 雜湊值：73281aa5a69f2d39aa5f6e08868073a24020d677、599217201b4db537db681a21d6115d33289eb965

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/social_ioc_0128.csv