

國家資通安全會報 技術服務中心
漏洞/資安訊息警訊

發布編號	ICST-ANA-2012-0005	發布時間	2012/04/20
事故類型	攻擊活動預警	發現時間	2012/04/20
通告名稱	社交工程攻擊通告：請加強防範駭客假冒公務名義發送之惡意電子郵件		
內容說明	<p>技術服務中心近期接獲情資且自惡意電子郵件服務檢測中發現，駭客冒用公務名義發送公務相關標題的電子郵件，誘使收件者開啟惡意附件後植入惡意程式。</p> <p>已知本波攻擊信件特徵如下：</p> <p>寄件者：An I</p> <p>主旨：行政院暨所屬各機關發言人及新聞聯絡組聯絡資料</p> <p>惡意附件：003 行政院暨個部會新聞連絡組.doc</p> <p>連線中繼站：203.179.82.187、119.82.117.69、202.176.89.79</p> <p>研判應為針對性攻擊，攻擊對象主要為各機關發言人與聯繫窗口，技術服務中心特別呼籲相關單位加強警戒。</p>		
影響平台	所有 Microsoft Office 環境系統		
影響等級	高		
建議措施	<ol style="list-style-type: none"> 1. 提醒電子郵件使用者提高警覺，注意郵件之來源及內容的正確性，避免開啟不明來源信件的附檔，以防遭植入後門程式。 2. 全面更新作業系統及辦公室常用軟體的修補程式。 3. 安裝防毒軟體並更新至最新病毒碼，並注意病毒碼須持續更新。 4. 阻擋以上惡意中繼站，並確實更新防火牆。 5. 加強宣導與防範駭客利用電子郵件進行社交工程攻擊。 		
參考資料	無		