行政院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	NCCST-ANA-2018-0109	發布時間	Fri Nov 09 16:52:58 CST 2018
事件類型	其他	發現時間	Fri Nov 09 00:00:00 CST 2018
警訊名稱	社交工程攻擊通告：請加強防範駭客假冒公務名義發送 107 年選舉公告相關主旨之惡意電子郵件		
內容說明	行政院國家資通安全會報技術服務中心近期自惡意電子郵件檢測服務中發現，駭客利用九合一大選時事，冒用公務名義發送選務相關標題電子郵件，誘使使用者開啟惡意附件後植入惡意程式，已知相關攻擊郵件特徵如下: 1.冒名寄件者: 「lgagl@cec[.]gov[.]tw」 2.惡意信件主旨: (1)「107 年台中選舉公告」 (2)「107 年臺南選舉公告」 (3)「107 年直轄市、縣市議員選舉區變更公告.doc?[__空白__].exe」 3.惡意附件名稱:「107 年直轄市、縣市議員選舉區變更公告.doc.exe」 4.惡意中繼站:「www[.]account_mentgooggl[.]serveuser[.]com」		
影響平台	所有 Microsoft 環境系統		
影響等級	高		
建議措施	1.確認電子郵件檔案類型後才開啟該檔案，若發現檔案名稱中存在異常字元(如 rcs, exe, moc 等可執行檔案附檔名的逆排序)，請提高警覺。 2.建議取消「隱藏已知檔案類型的附檔名」功能，Windows 平台設定方式如下:		

	(1)滑鼠點選【開始】>【控制台】>【資料夾選項】，出現資料夾選項視窗。 (2)於資料夾選項視窗點選「檢視」，將「隱藏已知檔案類型的附檔名」選項取消核選，再點選「套用」與「確定」即可完成設定。 3.請勿開啟未受確認之電子郵件附件。 4.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。 5.確實更新防火牆並阻擋惡意中繼站。 6.加強內部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	

此類通告發送對象為通報應變網站登記之資安人員。若貴 單位之資安人員有變更，可逕自登入通報應變網站（https://www.ncert.nat.gov.tw）進行修改。若您仍為貴單位之資安人員但非本事件之處理人員，請協助將此通告告知相關處理人員。

如果您對此通告的內容有疑問或有關於此事件的建議，請勿直接回覆此信件，請以下述聯絡資訊與我們連絡。

地 址： 台北市富陽街 116 號
聯絡電話： 02-27339922
傳真電話： 02-27331655
電子郵件信箱： service@nccst.nat.gov.tw