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-2022-0000451	發布時間	Thu Oct 06 14:16:21 CST 2022
事件類型	公告資訊	發現時間	Thu Oct 06 00:00:00 CST 2022
警訊名稱	近期駭侵事件相關資安防護資訊，請各級機關加強防護		
內容說明	技服中心近期發現政府機關遭駭客入侵且意圖跨機關橫向攻擊情事，技服中心掌握已知中繼站資訊提供如下，建議應提高警覺，落實加強監控防護與異常連線阻擋。 請機關清查系統是否存在連線情形，並確認是否有受駭跡象，若發現系統已遭入侵之情事，請儘速採取因應措施，並進行事件通報作業。 惡意 IP/DN 列表如下： 1. mxryboy-xlovemusic[.]com 2. subnotes[.]ignorelist[.]com 3. 20[.]62[.]112[.]133 4. 20[.]98[.]106[.]237		
影響平台	全		
影響等級	高		
建議措施	1. 請依據惡意 IP/DN 資訊，清查防火牆與網站日誌等相關紀錄，確認是否存在異常連線之狀況。 2. 檢視連線設備確認是否已遭入侵，並進行鑑識作業以釐清連線原因。 3. 建議將作業系統安裝至最新修補程式，並更換系統使用者之相關密碼，並選用強建之密碼原則。		

	4. 注意個別系統之安全修補與病毒碼更新，包含作業系統、辦公室常用文書處理軟體及防毒軟體等，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。 5. 確認系統是否存在外部連線存取之必要性，非必要之外部連線可設置白名單限定存取來源。 6. 依據所列之 IP/DN 資訊，設置阻擋並加強監控防護。
參考資料	無

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。

如果您對此通告內容有疑問或有關於此事件之建議，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