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-2021-0000202	發布時間	Fri Jun 04 10:55:06 CST 2021
事件類型	攻擊活動預警	發現時間	Tue May 25 00:00:00 CST 2021
警訊名稱	【更新附件】發現駭客組織 TEMP.Overboard 攻擊活動，目標為國內政府機關與 IT 服務供應商，請加強防護		
內容說明	近期接獲外部情資，發現駭客組織 TEMP.Overboard 於 2021 年 3 月起利用 EYEWELL 後門惡意軟體針對我國政府單位及相關 IT 服務供應商進行攻擊，請各機關加強防護，並留意 IT 服務供應商帳號登入情形。 本次攻擊活動已知 IoC 資訊提供如附，包含惡意程式資訊雜湊值(Hash)與中繼站資訊等。 註：警訊之內容(含附件 IoC 資訊)僅提供給機關資安防護作業相關人員使用，不可將公告內容與中繼站清單公開或分享給其他非服務機關人員。		
影響平台	所有平台		
影響等級	高		
建議措施	1. 請儘速將所提供惡意檔案名稱及相關之 HASH 值，加入防護機制設定偵測阻擋規則。 2. 請加強遠端存取控制機制，依「原則禁止、例外允許」方式辦理。 註：請參考行政院資安處 110 年 3 月 2 日「院臺護字第 1100165761 號」公文。		
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