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-2017-0070	發布時間	Wed Jun 28 16:33:06 CST 2017
事件類型	其他	發現時間	Wed Jun 28 00:00:00 CST 2017
警訊名稱	近期勒索軟體 Petrwrap 活動頻繁，請立即更新作業系統、Office 應用程式與防毒軟體，並注意平時資料備份作業		
內容說明	全球多個國家於本(106)年 6 月 27 日晚間陸續傳出遭勒索軟體 Petrwrap 攻擊事件，受影響範圍以烏克蘭、俄羅斯及東歐等地區災情最為嚴重。 Petrwrap 為 2016 年勒索軟體 Petya 變種，攻擊者主要利用社交工程郵件誘使使用者開啟附件檔案，藉由攻擊 Office RTF 漏洞(CVE-2017-0199)執行惡意程式碼，以取得系統控制權，並配合微軟 MS17-010 漏洞、Windows 遠端管理指令 Psexec 或 WMIC(Windows Management Instrumentation Command-line)等方式進行內部擴散，受感染主機之作業系統開機磁區(MBR)與檔案配置表(MFT)將被加密，導致無法進入作業系統，只會在電腦螢幕上看到要求贖金的訊息。		
影響平台	Windows XP Windows Vista Windows 7 Windows 8.1 Windows RT 8.1 Windows 10 Windows Server 2003 Windows Server 2008 Windows Server 2008 R2		

	Windows Server 2012 Windows Server 2012 R2 Windows Server 2016
影響等級	高
建議措施	1.確實持續更新電腦的作業系統、Office 應用程式及防毒軟體等至最新版本。Petrwrap 勒索軟體所利用之作業系統弱點與 Office 應用程式弱點，已分別於 3 月與 4 月釋出修復程式，請至微軟官方網頁進行更新： (1)MS17-010：https://technet.microsoft.com/zh-tw/library/security/ms17-010.aspx 。另外已超過維護週期之作業系統，例如 XP/Server 2003 等，請參考連結(https://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598)下載後進行更新。 (2)CVE-2017-0199：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0199 2.更新電腦防毒軟體病毒碼。 3.作業系統登入密碼應符合複雜性原則，並定期變更密碼。 4.定期備份電腦上的檔案及演練資料還原程序。 5.避免開啟來路不明郵件，包含附件與連結。
參考資料	1.https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0199 2.https://technet.microsoft.com/zh-tw/library/security/ms17-010.aspx

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