**WannaCry事件描述：**

2017年5月12日，一種利用微軟作業系統基於SMB漏洞MS17-010，以比特幣勒索贖金的惡意程式的勒索病毒WannaCry開始廣泛傳播，影響了大量的微軟用戶。微軟已於今年3月份發佈了該漏洞的修補更新程式。對於開放445埠SMB服務的微軟作業系統，必須確認是否安裝了MS17-010修補更新程式，如果沒有安裝則受威脅影響的機率將大增。據了解，此次影響的Windows作業系統包含XP/7/8/8.1、Server 2003/2012等，使用盜版或是沒有進行更新及安裝防毒軟體的上述作業系統使用者必須特別留意，應即刻進行檢查。

遭勒WannaCry勒索的電腦將出現下列訊息視窗，



勒索訊息截圖（中文）



勒索訊息截圖（英文）

當您的電腦出現上述視窗訊息，請即刻拔除網路線並通知圖書資訊中心，以避免勒索軟體透過校園網路攻擊校內其他使用者。

**漏洞預防及處理方式**

Windows系統一但遭到攻擊中毒，馬上就會開始進行全系統的檔案加密。所有資料檔案將會遭受到高度加密，除了付贖金，拿到解密金鑰之外，目前沒有其他方法可以救回遭加密檔案。提供以下步驟來降低電腦受到勒索病毒感染的風險：

1. 透過作業系統本身防火牆軟體關閉Port 445所有連線。
2. 『控制台』🡪『系統及安全性』🡪『Windows防火牆』🡪 『進階設定』。
3. 執行『輸入規則』🡪『新增規則』。
4. 選擇『連接埠』🡪『下一步』。
5. 規則選擇套用到TCP（UDP也要依此步驟再設一次），特定本機連接埠設定『445』🡪『下一步』。
6. 執行『封鎖連線』🡪『下一步』。
7. 所有選項全勾（網域、私人、公開）。
8. 指定一組名稱給此規則。
9. 接著依照上述步驟，把UDP也設定一次，連接埠一樣是445。
10. 下載Windows更新檔，並養成定期更新的習慣。
微軟已於今年3月份發佈了該漏洞的修補更新程式。對於開放445埠SMB服務的微軟作業系統，必須確認是否安裝了MS17-010修補更新程式，如果沒有安裝則受威脅影響的機率將大增。請開啟Windows Update功能，確認是否安裝下列更新（任一更新皆可）：
3月安全性更新號碼：**Windows 7 : KB4012215**、**Windows 8.1:KB4012216**
4月安全性更新號碼：**Windows 7 : KB4015549**、**Windows 8.1:KB4015550**
5月安全性更新號碼：**Windows 7 : KB4019264**、**Windows 8.1:KB4019215**
Windows 10作業系統也請記得進行Windows Update，以降低遭入侵的風險。
11. 安裝防毒軟體，並養成定期更新病毒碼習慣。
請下載安裝圖書資訊中心提供的趨勢科技OfficeScan授權防毒軟體，可有效防堵勒索病毒WannaCry的入侵。
12. 升級作業系統。
如果您仍使用Windows XP作業系統，由於微軟針對Windows XP已不提供任何更新服務，建議您升級至最新的Windows 10作業系統。如果您仍使用Windows XP，請透過下列連結下載最新修補程式：
Windows XP SP2 X64：<http://www.catalog.update.microsoft.com/ScopedViewInline.aspx?updateid=a679cafc-d8da-4c2a-9709-17a6e6a93f4f>
Windows XP SP3 X86：<http://www.catalog.update.microsoft.com/ScopedViewInline.aspx?updateid=9e189800-f354-4dc8-8170-7bd0ad7ca09a>
13. 備份資料。
為降低資料遺失的風險，請務必定期更新您的資料，提供【三二一備份原則】供大家參考。
三二一備份原則：**至少備三份**、**使用二種形式備份**、**一份離線或異地備份**。
離線備份尤其重要，因為勒索病毒感染時，會將您所有接取在電腦上的儲存空間進行資料加密，因此包含雲端儲存空間的資料都有可能被加密，因此建議至少要保留一份備份資料於離線儲存媒體（光碟片、行動硬碟、磁帶..等），以確保資料的安全。

圖資中心於校園網路已透過相關資安防堵手段，阻擋了WannaCry的感染途徑，但為避免內部的傳播感染，請大家務必確實做到上述預防措施，降低遭感染並造成資料遺失的風險。