WannaCry

2017/05/15

From NTU CC

敬啟者，

近幾天出現一款新的變種勒索病毒為**WannaCry（WanaCrypt0r 2.0）**，不需要使用者開啟檔案或點擊網頁，連上網路就有可能遭受攻擊與感染，導致檔案被加密遭受勒索，主要是透過**Windows XP/Vista/7/8/8.1** 的漏洞進行攻擊，短時間內就能導致肆虐全球電腦與伺服器，而台灣也在這次名單中，也成為了感染排行第二的名單國家。

攻擊手法
駭客掃描校園網路主機並檢查port 445 是否開啟，如果有開啟立即檢查使用者主機是否存在網路芳鄰(SMB)漏洞，當遭受入侵的電腦植入勒索軟體後，會繼續自動掃描網芳其它主機的port 445主機，重複攻擊與感染。

自我檢測步驟:
1. 關閉網路連線(無線、有線均關閉)
2. 檢視工作管理員，若是看到此兩隻程式， tasksche.exe 或 mssecsvc.exe，立即關機(立即拔掉電源)，代表已經感染。
3. 以安全模式(F8按鍵)重新開機，備份剩餘未被加密檔案。或是，重新安裝電腦，或更新KB4012215漏洞。
4. Windows 10的版本，基本上不會影響，但如果瀏覽網頁突然跳出警示訊息，**切勿點取**下載修復，此為另一種誘導啟發式病毒。

如主機尚未被感染請採取以下緊急防護措施
緊急防護措施
1. 關閉主機網芳TCP port 445
2. 請盡快更新微軟官方釋出的主機Windows系統漏洞
3. 備份主機資料

計資中心 關心您!

Please spend 5 minutes to read about WannaCry exploit now.

Goal: derive a strategy for our department's network and hosts.

Take action now (R204 desktop + your laptop)

- Disconnect your Windows host (R204 desktop + your own laptop) from the Internet
  - (How?)
- Backup your data
  - (without the Internet)
- Patch your Windows host
- What else?

Have your impact

- Develop a strategy for the department
- Write down a step-by-step instruction for “not-so-technical users”. Make sure it is correct!
- Distribute it on your social media page

Resources

- Windows 10 is not affected
- KB4012598: (including “unsupported” windows XP, vista, 7, server 2003, 2008, etc.) http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598