張貼日期：2017/05/15

資安漏洞預警

主旨：

【高風險】【攻擊預警】勒索軟體 WanaCrypt0r 2.0 攻擊 Windows 系統漏洞，造成檔案加密無法使用，請儘速進行更新

說明：

1. 網路保安公司發現全球多個國家的機構及個人電腦遭受名為 WanaCrypt0r 2.0 的勒索軟體攻擊感染，有別於以往的攻擊方式，據了解該勒索軟體是直接透過系統漏洞進行攻擊，除 Windows 10 及 Server 2016 外，近乎所有 Windows 系統及其伺服器版本均受威脅，安全專家呼籲用戶盡快安裝官方釋出的安全性更新，避免機構及個人電腦受感染。
2. 此勒索軟體的運作模式一如既往，電腦遭受感染後，所有檔案均被加密成副檔名為 .WNCRY 的格式，無法正常開啟讀取資料。檔案加密後亦會彈出相應介面指示受害者需在 3 天內交付價值 300 美元的 Bitcoin 贖金，逾期加倍，若未能在 7 天內交付則再無法恢復檔案。
3. WanaCrypt0r 2.0 是透過 Windows 系統內名為 EternalBlue 的 Windows SMB 遠端執行程式碼弱點進行攻擊，成功利用弱點的攻擊者有機會獲得在目標伺服器上執行程式碼的能力。

影響平台:
Windows XP
Windows Vista
Windows7
Windows8
Windows8.1
Windows Server 2008
Windows Server 2008 R2
Windows Server 2012
Windows Server 2012 R2
Windows RT

建議措施:

1. 使用 Windows Update 更新 或 手動更新微軟 KB4012215 (漏洞編號 MS17-010) KB40122215 https://support.microsoft.com/zh-tw/help/4012215 MS17-101https://technet.microsoft.com/zh-tw/library/security/ms17-010.aspx?f=255&MSPPError=-2147217396#ID0EHB
2. Window XP 及 Windows Server 2003 等停止支援之作業系統，可到下列網址下載微軟提供之更新檔案進行更新作業：https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
3. 此次攻擊目前觀察到使用 Port 445 進行攻擊，可於前端防護設備上限制 Port 445 連線，或於個人電腦防火牆上限制 Port 445 連線
4. 目前 Windows Defender 已經可以針對發作中的惡意程式 WanaCrypt0r 有效的偵測並清除。可以從下列位置下載 Windows Defender https://support.microsoft.com/help/14210/security-essentials-download
5. 平常遵循 3-2-1 規則來養成良好的備份檔案習慣：建立三份副本，使用兩種不同媒體，一份副本要存放在不同的地方，此外至少有一個系統備份是處於實體隔離的網路環境。

參考資料:

1. https://www.facebook.com/twcertcc/posts/1947829248780144
2. https://www.facebook.com/twcertcc/posts/1947904648772604
3. https://www.facebook.com/MicrosoftTaiwan/posts/1024724287627679:0
4. http://technews.tw/2017/05/13/ransomeware-wanacrypt0r-2/

其它參考資料

1. http://www.ess.nthu.edu.tw/files/14-1163-118887,r1602-1.php?Lang=zh-tw (內含圖文步驟說明)
   感謝本校系所單位網管提供

計算機與通訊中心
網路系統組 敬啟