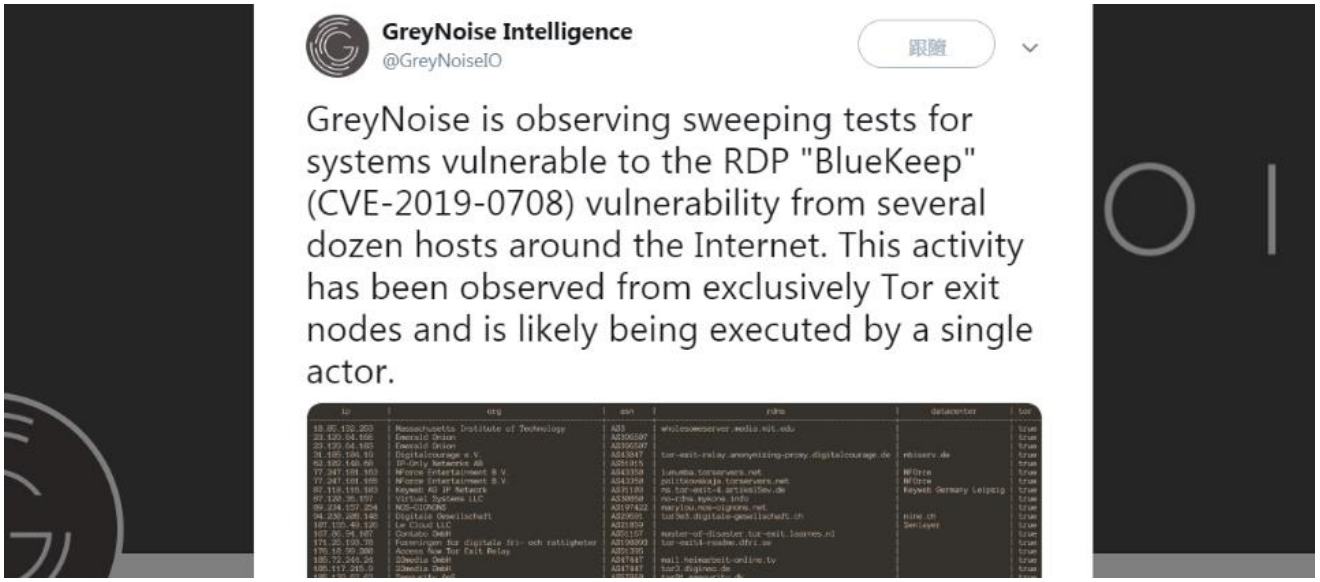
Windows RDP 漏洞 PoC 攻擊程式問世，疑似有駭客開始掃瞄

微軟在兩周前公布的 Windows RDP 協定重大漏洞，可能引發類似 WannaCry 的災情，除了影響 Windows 8 和 Windows 10 系統，Windows XP、Server 2003、Windows 7、Windows Server 2008 及 2008 R2 都受影響，微軟還例外對 XP 及 Server 2003 釋出修補

文/林妍溱 | 2019-05-28 發表



微軟在兩周前公佈 Windows RDP 協定重大漏洞後，安全專家發現（5 月 27 日）已經有駭客開始大規模掃瞄網路上有漏洞的

Windows 系統，顯示可能發動攻擊。而多家安全廠商也製作出概念驗證攻擊程式。

編號 CVE-2019-0708 的漏洞存在於舊版 Windows 遠端桌面服務（Remote Desktop Service，RDS）中，本漏洞可使未授權攻擊者得以利用 RDP 連上目標系統傳送惡意呼叫。成功開採者可於遠端執行任意程式碼、安裝惡意程式、讀取或刪改資料、或新開具完整權限的用戶帳號。

本漏洞的 CVSS Score v3 風險評分皆為重大等級的 9.8 分（滿分 10 分），微軟強烈建議用戶應儘速安裝修補程式。除了 Windows 8 和 Windows 10 系統外，從 Windows XP 及 Server 2003，到 Windows 7、Windows Server 2008 及 2008 R2 都受影響，微軟還例外對 XP 及 Server 2003 釋出修補程式。這項漏洞也被稱為 BlueKeep。

雖然微軟說尚未看到有攻擊情形，不過安全廠商 GreyNoise 本周發現網路上有數十臺主機，針對 BlueKeep 漏洞進行大規模掃瞄。安全公司觀察到掃瞄行動全是來自 Tor 網路的出口節點，判斷是由單一組織或人士所為。

GreyNoise 創辦人 Andrew Morris 對此指出，他相信攻擊者用的是滲透測試工具 Metasploit 模組來掃瞄 BlueKeep 漏洞主機。雖然掃瞄不代表一定是攻擊行動，但這極可能是駭客攻擊的前兆。

在此之前，已經有卡巴斯基、McAfee 及 CheckPoint 等安全廠商，宣稱已經開發出 BlueKeep 的概念驗證（PoC，Proof of Concept）攻擊工具。主持 MalwareTech 的資安研究人員（及前駭客）Marcus Hutchins 也表示，他只花了一小時搞清楚怎麼攻擊，4 天就寫出 PoC 攻擊程式。安全公司也呼籲用戶及早安裝修補程式。

資料來源：iThome