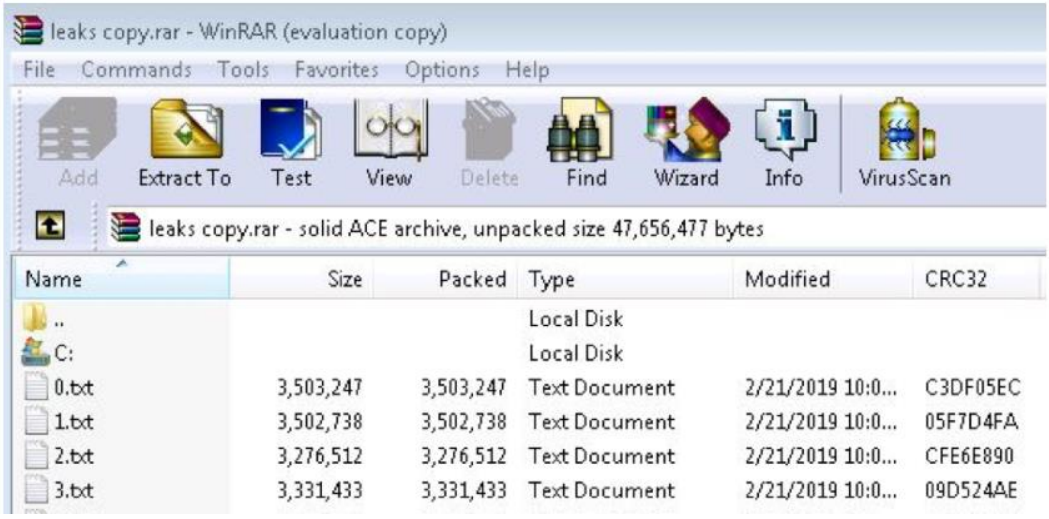
WinRAR 用戶小心了，攻擊文件五花八門

擁有 5 億用戶的 WinRAR，由於缺乏自動更新機制，加上漏洞本身容易開採，導致大量攻擊手法不斷出現

文/陳曉莉 | 2019-03-28 發表



今年 2 月曝光的 WinRAR 安全漏洞 CVE-2018-20250 可藉由壓縮檔案將惡意程式植入使用者的開機程序，受到廣大駭客的青睞，除了 McAfee 透露在 CVE-2018-20250 漏洞被公布的第一周就偵測到逾 100 種不同的攻擊行動之外，其它資安業者也相繼披露鎖定該漏洞的攻擊樣本。

例如 360 威脅情報發現，在韓國出道的台灣女星葉舒華的壓縮檔案「10802201010 葉舒華.rar」其實暗藏了遠端控制後門程式 OfficeUpdateService.exe，可用來掌控電腦的啟動或關閉，竊取系統上的檔案，或是盜錄螢幕畫面等。

另有一個 RAR 檔案是鎖定阿拉伯地區的使用者，駭客所散布的「JobDetail.rar」檔案看似含有一個描述工作機會的 PDF 檔，但解壓縮之後，它卻在系統上植入了一個 PowerShell 後門程式，可再自遠端伺服器下載其它惡意程式。

至於 FireEye 最近發現的攻擊樣本「Scan_Letter_of_Approval.rar」則假冒為美國社會工作教育協會（CSWE）申請許可，但實則暗藏一個可與遠端伺服器交流的 VBS 後門程式。

還有一個「SysAid-Documentation.rar」檔案鎖定的攻擊對象是以色列的軍事產業，它偽裝成來自 IT 服務管理軟體業者 SysAid，解壓縮之後卻在啟動程序中植入了惡意程式 SappyCache。

針對烏克蘭的「zakon.rar」則是以烏克蘭前任總統所發出的產官合作訊息為誘餌，只要以 WinRAR 解壓縮它就會在啟動程式中植入 Empire 後門程式。

FireEye 還發現一個有趣的攻擊樣本，此一「leaks copy.rar」看似含有眾多遭竊的電子郵件帳號及密碼，但其實可能含有各種不同的惡意程式，從鍵盤側錄、密碼竊取到遠端存取木馬等，該樣本主要吸引的族群就是駭客。

研究人員警告，之所以能在短期內就能看到如此五花八門的 WinRAR 漏洞攻擊樣本，除了因為 WinRAR 擁有 5 億的龐大用戶之外，也因 WinRAR 缺乏自動更新機制，再加上 CVE-2018-20250 非常容易開採，相信未來會有更多的駭客繼續利用該漏洞。

WinRAR 已於 2 月 28 日釋出修補此一漏洞的 WinRAR 5.70，WinRAR 用戶應儘速展開升級。

資料來源：iThome