個案分析-

垃圾郵件的APT攻擊事件分析報告

TACERT 臺灣學術網路危機處理中心團隊製

2012/7

目錄

一、事件說明

垃圾郵件一直是駭客喜歡使用的社交工程手法，而最近熱門的 APT（Advanced Persistent Threat）更是以垃圾郵件為攻擊手法之一，攻擊者不斷地使用引誘人打開的關鍵字發送垃圾郵件。

四月開始，某些組織成員陸續收到夾帶有惡意文件檔的垃圾郵件。這些惡意文件檔打開之後會利用主機的漏洞入侵主機，使夾帶在惡意文件檔裡面的惡意程式順利在主機上面執行，進行惡意活動。

■ CVE 2012-0158

這些惡意文件使用 CVE20120158[1]漏洞入侵電腦，CVE20120158 漏洞在四月中由微軟發布的 MS12-027 更新進行修補[2]，其影響的 OFFICE 版本幾乎涵蓋所有市面上的版本，由時間上來看，微軟發布更新修補漏洞之前，該漏洞就已經大量被使用在垃圾郵件的夾帶檔。

Microsoft Office 2003 Service Pack 3
Microsoft Office 2003 Web Components Service Pack 3
Microsoft Office 2007 Service Pack 2
Microsoft Office 2007 Service Pack 3
Microsoft Office 2010 (32-bit editions)
Microsoft Office 2010 Service Pack 1 (32-bit editions)

惡意的 DOC 檔偽裝成正常的文件，利用社交工程引誘收件者打開。這些惡意 DOC 檔只是個載體，當使用者點擊 DOC 之後，與 DOC 綁在一起的惡意執行檔會釋出並自動執行。四、五月份已知的夾帶檔名如下所列：

英文.doc
kong.doc
薄熙來唱紅打黑，為什麼會身敗名裂？.doc
南海爭端不斷，中共領導人態度如何？.doc
Thupten.doc
Mission Command Outline.doc
子女教育補助費 101 新版.doc
a.doc
oracle readme.doc
民進黨二零一二年整體規劃.doc
1010415 違規停車單.doc

立法院 101 年 4 月國防部備詢(有關後備司-紅字)及詳細條文.doc

二、事件分析

■ 1010415 違規停車單.doc

其中這一份惡意檔打開後的網路行為如下：

Connect to 163.xxx.255.88:443

Connect to www.twnic.ddns.us:443

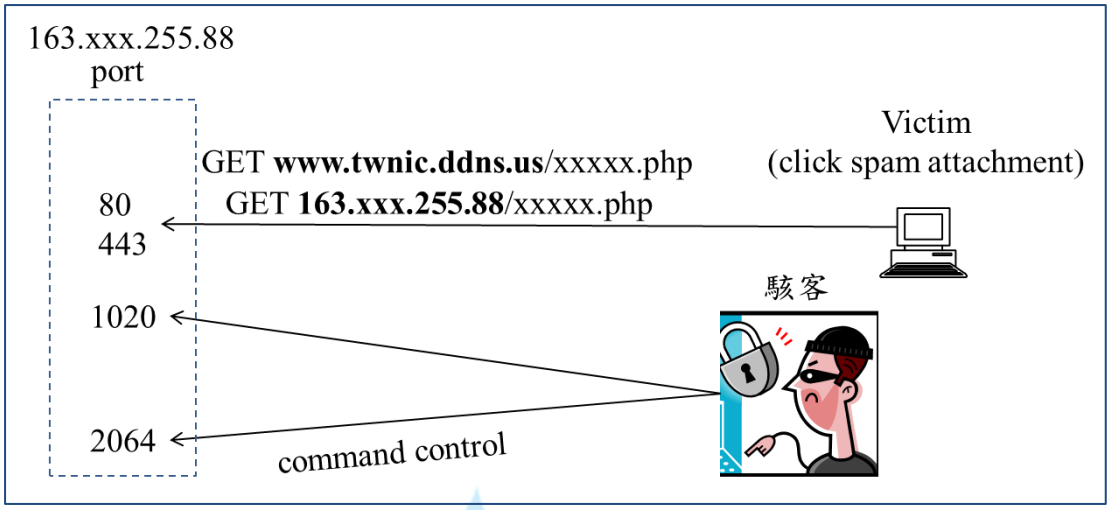
163.xxx.255.88 主機資訊：

- 位於台南市的 M 中學
- Windows 2008
- Web Server
- 提供 VOD 隨選線上影片教學系統

■ 163. xxx.255.88 主機的異常活動

我們已知異常連線到 163. xxx.255.88 主機的 443port，443port 由 udpxxxx.exe 這個程式擁有。細查了每個網路連線之後，發現 2046port 的網路活動也屬於異常活動。以下為說明圖表：

163.xxx.255.88 上的惡意程式	port	說明
C:\windows\syswow64\udpxxxx.exe	443	與 victim 聯繫
C:\windows\syswow64\udpxxxx.exe	1020	駭客傳輸資料
C:\windows\syswow64\svchost.exe –k netsvcs (C:\windows\syswow64\ntxxxx.dll)	2064	Command Control



當有使用者被攻擊成功，就會連到 163. xxx.255.88:443 進行報到的動作，而駭客則利用 port2064 進行 command control，port1020 則是提供駭客傳輸資料。

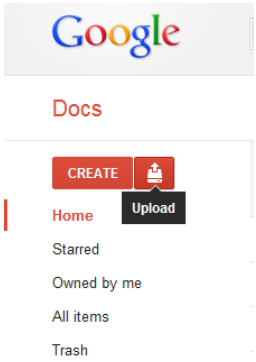
三、建議措施

如今許多提供電子郵件的公司，都有幫使用者進行郵件過濾的動作（如 Gmail），唯一般私人架設的 Mail Server 在抵擋惡意郵件的能力上可能有所疏漏，尤以學校政府單位自行架設的 Mail Server 為最，建議使用電子郵件軟體收信的使用者（如 Outlook 等）：

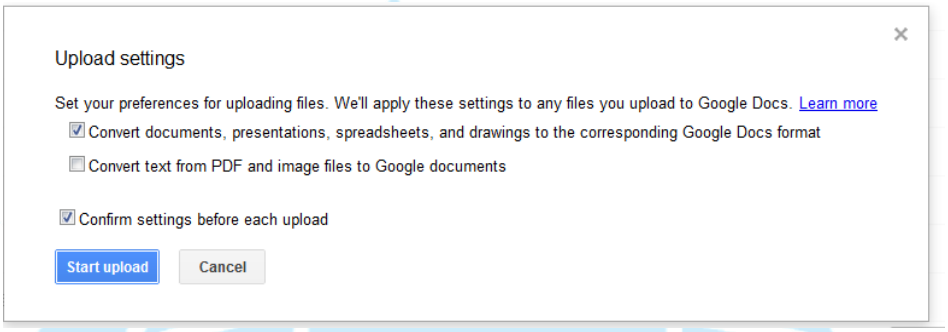
- 以純文字開啟郵件
- 取消郵件預覽功能
- 對於主旨與工作無關的郵件連開啟都不要馬上刪除
- 附加檔案不應該直接打開，應該另存新檔，以安全的方式打開
- 利用郵件簽章確保寄件者不被偽造

在附加檔案方面，若不能夠確定是否為惡意郵件，或基於公務上的需要必須打開，建議可以利用線上的文件軟體，如果檔案有惡意程式夾帶，利用線上文件軟體打開便不會傷害到本機；若文件並非惡意檔案，利用線上文件軟體打開，仍可以呈現檔案內容，並進行編輯。以下示範 Google 提供的線上文件[3]：

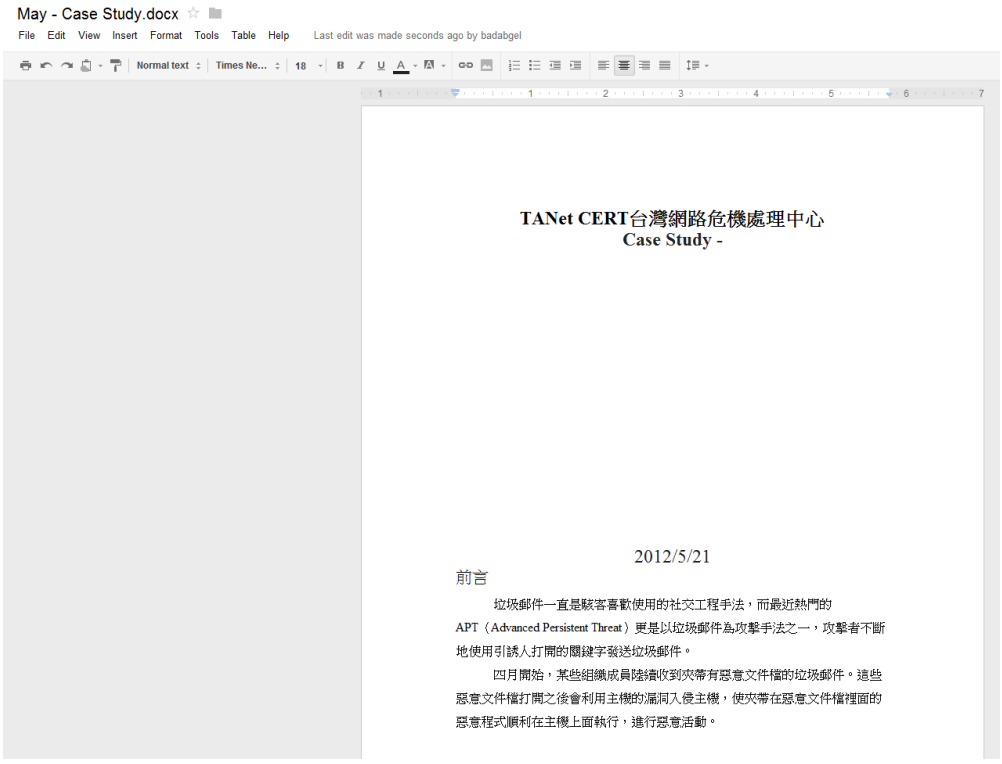
- 步驟一、您必須有帳號能登入 Google
- 步驟二、登入之後進入文件，將想打開的 DOC 檔案上傳



➢ 步驟三、將文件轉成 Google 的格式



➢ 步驟四、上傳完成之後打開可以在列表找到，打開後發現和原本的文件內容相同



在主機管理者端，建議：

- 伺服器前端應設置防火牆
- 防火牆僅開啟必須的埠號，其他關閉
- 備份主機初始設定值
  - 埠號、行程、dll 檔的 md5 等
  - 一段時間比對一次，看是否有不明埠號或行程活動

四、參考資料

[1] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0158
[2] http://technet.microsoft.com/en-us/security/bulletin/ms12-027
[3] https://docs.google.com/