檔案加密勒索軟體(病毒)

近期本校發生多起電腦感染檔案加密勒索病毒之狀況，請全校教職員工生多加注意。

案例說明：

11/7日中心接獲通知校內某單位實驗室電腦發生異常，經了解該設備為一公用電腦，建有多組使用者帳號，前一天晚上病毒開始進行 加密感染，隔天早上才被發現異常。本次事件為其中一組帳號中了檔案加密勒索病毒，導致該帳號具有寫入權限的檔案都被加密，亦將連線的檔案伺服器 (網路芳鄰)共享資料夾內的檔案加密。遭加密檔案約20幾萬筆，受影響資料量超過10TB，依目錄下所留勒索資訊顯示是遭受病毒Crypt0L0cker加密。

Crypt0L0cker 檔案加密勒索軟體(病毒)說明

1. Crypt0L0cker 為2015年4月出現的 CryptoLocker 病毒變種。
2. 此病毒感染加密後之檔案，以目前的解密技術及設備效能無法在能接受 的時間內解密成功(等同於無法救回)。
3. Windows 作業系統感染途徑確認為下載檔案感染，會在瀏覽被竄改的惡意網站、開啟郵件附件、甚至點選彈跳視窗時強制安裝病毒。
4. 已知會影響檔案類型：*.odt, *.ods, *.odp, *.odm, *.odc, *.odb, *.doc, *.docx, *.docm, *.wps, *.xls, *.xlsx, *.xlsm, *.xlsb, *.xlk, *.ppt, *.pptx, *.pptm, *.mdb, *.accdb, *.pst, *.dwg, *.dxf, *.dxg, *.wpd, *.rtf, *.wb2, *.mdf, *.dbf, *.psd, *.pdd, *.pdf, *.eps, *.ai, *.indd, *.cdr, *.jpg, *.jpe, img_*.jpg, *.dng, *.3fr, *.arw, *.srf, *.sr2, *.bay, *.crw, *.cr2, *.dcr, *.kdc, *.erf, *.mef, *.mrw, *.nef, *.nrw, *.orf, *.raf, *.raw, *.rwl, *.rw2, *.r3d, *.ptx, *.pef, *.srw, *.x3f, *.der, *.cer, *.crt, *.pem, *.pfx, *.p12, *.p7b, *.p7c
5. Linux 作業系統也出現透過 Magento 內容管理系統軟體漏洞嘗試入侵的勒索病毒(Linux.Encoder.1)。

預防方法

1. 作業系統升級 windows 7 以上，開啟 Windows Update 並設定為自動更新。
2. 為增加系統安全性，建議安裝防毒軟體並設定自動更新。
3. 更新應用程式至最新版本：Java、Adobe Reader、Adobe Flash Player。
4. 定期備份重要資料，以降低傷害程度；備份資料宜以光碟、隨身硬碟方式備份，備份完畢後務必將儲存媒體另外收納，勿與電腦連接。
5. 不要開啟不熟悉的網頁或是不明電子郵件附件或連結，瀏覽網頁時顯現的彈出式視窗不要點選安裝，也不要安裝網路流傳之破解軟體，避免感染病毒。
6. 若多人共用一台電腦，請建立個人帳號及設定合適的權限，切勿共用一組帳號。如有提供遠端連入相關服務（例如：遠端桌面、SSH...等），務必限制管理員帳號：administrator、root、遠端登入。
7. 請避免開啟共用資料夾，若要開啟務必設定密碼及帳號檔案權限控管。
8. 察覺電腦有非常明顯速度變慢時，請第一時間拔除或關閉自己電腦的網路，避免病毒透過網路擴散。

檢查是否有感染

該病毒有潛伏期，中毒後不會馬上進行檔案加密，可以透過搜尋檔案功能，檢查是否有以下檔案：(中毒電腦可能會含有的檔案)

- HELP_TO_SAVE_FILES.txt

- HELP_RESTORE_FILES.txt
- DECRYPT_INSTRUCTIONS
- RECOVERY_FILE.txt
- .encrypted (在原本檔案後加入 .encrypted 的副檔名)
- .ezz
- .ecc

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
https://net.nthu.edu.tw/netsys/security:attack:ransomware

Last update: **2017/03/07 15:14**