個案分析-

利用 Excel IQY 檔案散播後門程式事件分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

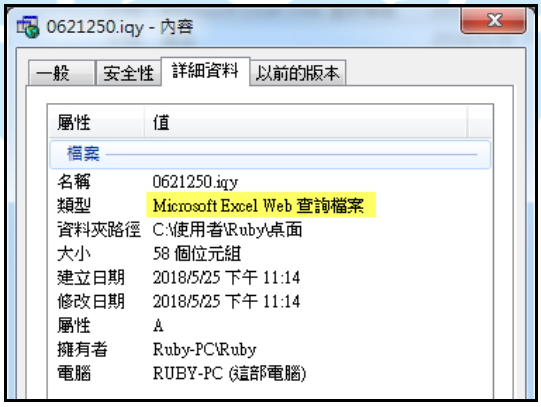
107 年 7 月

I. 事件簡介

1. 2018 年 5 月中旬在網路上出現以主旨為 Unpaid invoice[ID:隨機亂數]的信件被散播著，該類型的信件皆夾帶一個副檔名為 IQY 的附件，因為附檔本身不含惡意行為，故可輕鬆躲避防毒軟體的檢查。
2. IQY 為純文字格式，是 Microsoft Excel 所使用的 Web 查詢設定檔，以 Excel 開啟該類型檔案後會連向指定的網址取得資料，最後下載 Flawed Ammy RAT 後門程式。
3. 為了瞭解該類型資安事件的觸發原因與攻擊行為，本中心取得 IQY 樣本後進行檢測。

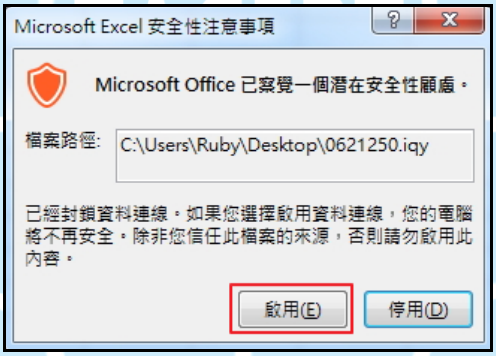
II. 事件檢測

1. 首先，檢視 IQY 樣本 0621250.iqy 的內容，可以得知該檔案類型是 Microsoft Excel Web 查詢檔案，而 VirusTotal 檢測檔案 0621250.iqy 的結果為 28/59，僅 28 家防毒軟體公司的防毒軟體可以檢測出來，有些防毒軟體公司稱它為 IQYDownloader。

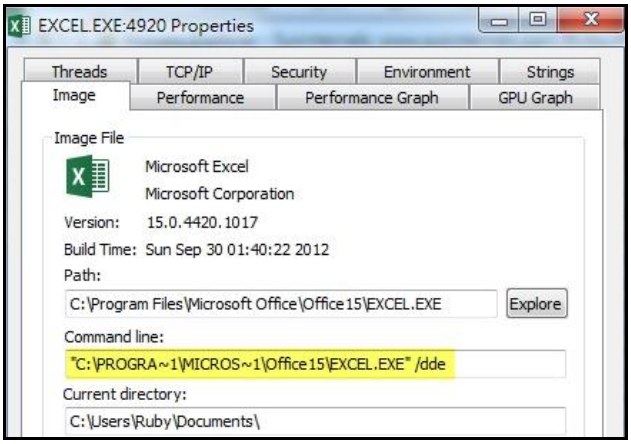


防毒	結果	更新
Ad-Aware	Generic.IQYDownloader.1.65001743	20180530
AegisLab	Troj.Downloader.Msexcell!c	20180530
AhnLab-V3	IQY/Downloader	20180529
ALYac	Trojan.Downloader.Agent	20180530
Arcabit	Generic.IQYDownloader.1.65001743	20180530
Avira (no cloud)	BAT/Dldr.Agent.76444	20180530
BitDefender	Generic.IQYDownloader.1.65001743	20180530
ClamAV	Txt.Malware.Agent-6558868-0	20180530
Cyren	JS/Downldr.MY	20180530
Emsisoft	Generic.IQYDownloader.1.65001743 (B)	20180530
ESET-NOD32	LNK/TrojanDownloader.Agent.LH	20180530
F-Prot	JS/Downldr.MY	20180530
F-Secure	Generic.IQYDownloader.1.65001743	20180530
GData	Generic.IQYDownloader.1.65001743	20180530

2. 開啟檔案 0621250.iqy 後，出現 Microsoft Excel 安全性注意事項的提醒視窗，點選「啟用」後即進入 Excel 工作表畫面。

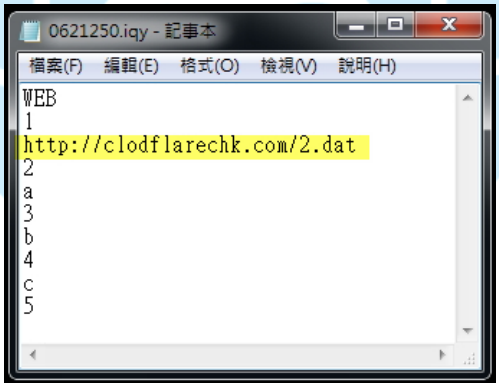


3. 檢視背景程式，發現 Excel 執行檔在執行時，啟動 dde 功能，因此當雙擊多個 excel 文檔時只會打開一個 excel 進程。



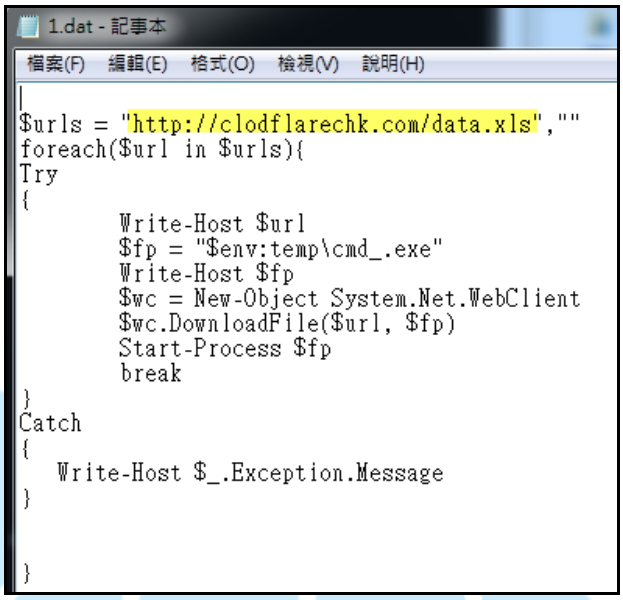
4. 檢視所開啟的 Excel 檔內儲存格內容，發現僅有一欄有值，該值為 621250，與檔案名稱相同，在「編輯查詢」內發現「編輯 Web 查詢」的地址為「http://clodflarechk.com/2.dat」，可見該檔案開啟後會連至該網址下載 2.dat 檔回來。

5. 以記事本開啟檔案 0621250.iqy，發現內容中有一個網址 http://clodflarechk.com/2.dat，與 Web 查詢的地址相同。

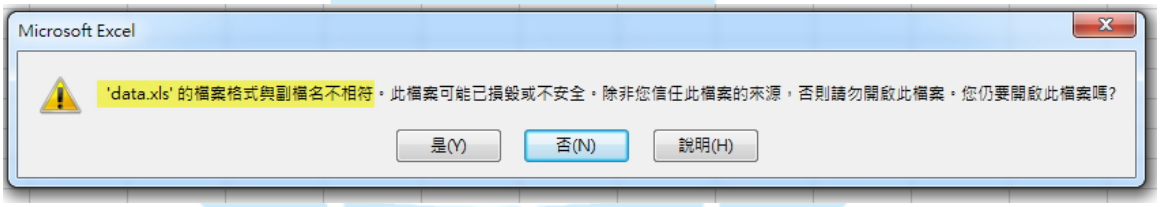


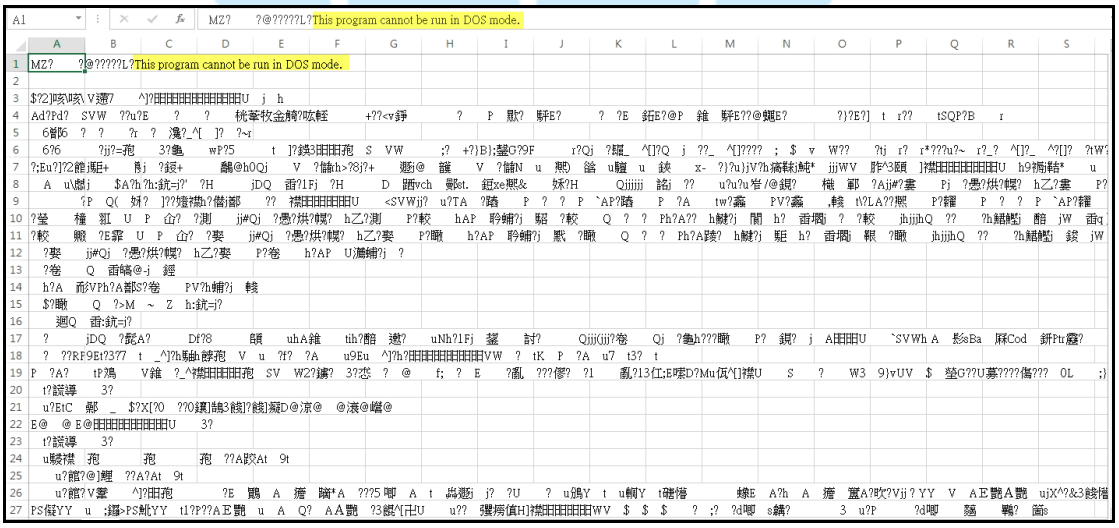
6. 檢視 2.dat 內容，發現該檔案會透過 Powershell.exe 執行某一段下載指令，將 1.dat 下載到受害主機內。

7. 查看 1.dat 內容，發現透過 PowerShell.exe 直接執行指令檔 1.dat 後，會下載檔案 data.xls，並且執行它。

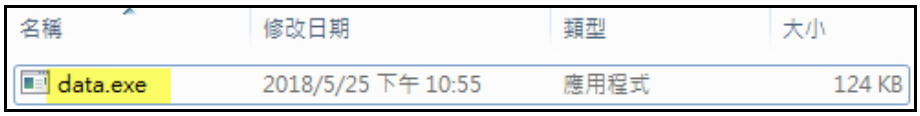


8. 查看 data.xls 內容，發現該檔案開啟時出現該檔案格式與副檔名不相符的訊息，而且開啟檔案後出現一堆亂碼，其中出現「This program cannot be run in DOS mode」的文字，推測該檔案的副檔名可能為.exe 的執行檔。

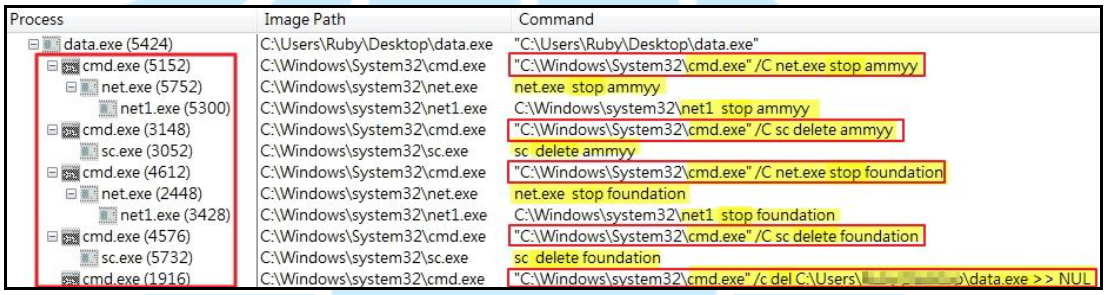




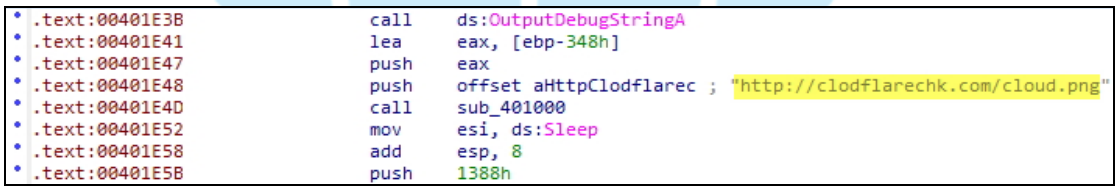
9. 將檔案 data.xls 之檔名改為 data.exe 後並執行它，發現它執行完成後即消失不見，推測該檔案在執行後會自我刪除自己本身。

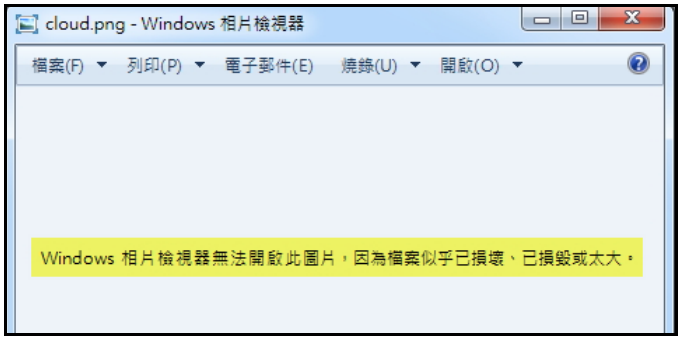


10. 將 data.exe 執行後，從 Process tree 可以看到它會呼叫多個 cmd.exe，透過 cmd.exe 去呼叫 net.exe 與 sc.exe，其中指令 cmd.exe /C net.exe stop ammyy、cmd.exe /C sc delete ammyy、cmd /C net.exe stop foundation 與 cmd.exe /C sc delete foundation 是用來偵測是否已安裝惡意程式，如果惡意程式已存在，則終止已經存在而且執行中的惡意程式，避免重複執行，最後它會自我刪除 data.exe。

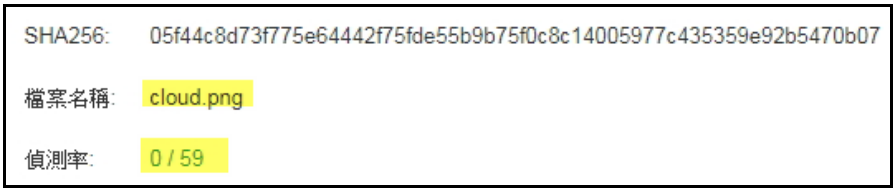


11. 檢視 data.exe 程式碼，得知 data.exe 執行後會連線網址 http://clodflarechk.com/cloud.png 並下載 cloud.png，嘗試開啟 644 KB 大小的 cloud.png，但無法開啟。





經 Virustotal 檢測，該檔案惡意比例為 0/59，而檔案資訊中 File type 為不知，可見該檔案為其他的檔案類型，因此 Virustotal 無法檢測出其是否為惡意。



SHA256:	05f44c8d73f775e64442f75fde55b9b75f0c8c14005977c435359e92b5470b07
檔案名稱:	cloud.png
偵測率:	0 / 59

MD5	7c0ffdb5a4dd0c120281aab273e2600e
SHA1	105626244b2be7c9a302cce50119a96253ba5357
SHA256	05f44c8d73f775e64442f75fde55b9b75f0c8c14005977c435359e92b5470b07
ssdeep	12288:VR2ouSmDlbd7/HV+BYd9lVYEaGv9NDHfJjFtaldK1MY69hr9L7o/2suYslA:3X9kZH8+nlZ/v9NzfySY69HLq2njlA
File size	644.0 KB (659456 bytes)
File type	unknown
Magic literal	data
TrID	Unknown!

12. 檔案 2.dat、1.dat 與 data.xls 經 VirusTotal 檢測的結果，分述如下:

(1) 2.dat 檢測出為惡意程式的比例為 28/59，多家防毒軟體公司稱它為 IQYDownloader 或者 Downloader。

SHA256:	05660c8d652fb9df8dab6a5705e3e2243b215ad5354000961feaebc07ed89ad9
檔案名稱:	2.dat
偵測率:	28 / 59
分析日期:	2018-05-31 07:51:10 UTC (0 分鐘 前)

防毒	結果	更新
Ad-Aware	Generic.IQYDownloader.1.28BF0E82	20180531
AegisLab	Troj.Downloader.Msexcell!c	20180531
ALYac	Trojan.Downloader.Agent	20180531
Antiy-AVL	Trojan[Downloader]/PowerShell.Agent	20180531
Arcabit	Generic.IQYDownloader.1.28BF0E82	20180531
Avira (no cloud)	VBS/Dldr.Agent.734342	20180531
BitDefender	Generic.IQYDownloader.1.28BF0E82	20180531
Cyren	PSH/Downloader.C	20180531
DrWeb	PowerShell.DownLoader.597	20180531
Emsisoft	Generic.IQYDownloader.1.28BF0E82 (B)	20180531
ESET-NOD32	PowerShell/TrojanDownloader.Agent.AOV	20180531
F-Prot	PSH/Downloader.C	20180531
F-Secure	Generic.IQYDownloader.1.28BF0E82	20180531
GData	Generic.IQYDownloader.1.28BF0E82	20180531
Ikarus	Trojan-Downloader.PowerShell.Agent	20180530
Kaspersky	HEUR:Trojan-Downloader.MSExcel.DdeExec.c	20180531
MAX	malware (ai score=96)	20180531
McAfee	PS/Downloader.ad	20180530
McAfee-GW-Edition	PS/Downloader.ad	20180531
eScan	Generic.IQYDownloader.1.28BF0E82	20180531

（2） 1.dat 檢測出為惡意程式的比例為 25/59，多家防毒軟體公司稱它為 IQYDownloader 或者 Downloader。

SHA256: ebce76b8efff3a0568aa2b07d5fba8f21fe3dd6f56bfad0a77194a494b634079

檔案名稱: 1.dat

偵測率: 25 / 59

分析日期: 2018-05-30 08:11:13 UTC (0 分鐘 前)

防毒	結果	更新
Ad-Aware	Generic.IQYDownloader.1.70D567FC	20180530
AegisLab	Troj.Downloader.Powershelllc	20180530
ALYac	Trojan.Downloader.Agent	20180530
Arcabit	Generic.IQYDownloader.1.70D567FC	20180530
Avira (no cloud)	VBS/Dldr.Agent.73434	20180530
BitDefender	Generic.IQYDownloader.1.70D567FC	20180530
DrWeb	PowerShell.DownLoader.596	20180530
Emsisoft	Generic.IQYDownloader.1.70D567FC (B)	20180530
ESET-NOD32	PowerShell/TrojanDownloader.Agent.PF	20180530
F-Prot	JS/Downldr.MZ	20180530
F-Secure	Generic.IQYDownloader.1.70D567FC	20180530
GData	Generic.IQYDownloader.1.70D567FC	20180530
Ikarus	Trojan-Downloader.PowerShell.Agent	20180529
Kaspersky	Trojan-Downloader.PowerShell.Agent.er	20180530
MAX	malware (ai score=85)	20180530
McAfee	PS/Downloader.ab	20180530
McAfee-GW-Edition	PS/Downloader.ab	20180530
eScan	Generic.IQYDownloader.1.70D567FC	20180530
Qihoo-360	Win32/Trojan.Downloader.40e	20180530

(3) Data.xls 檢測出為惡意程式的比例為 47/65，少數防毒軟體公司稱它為 Downloader。

SHA256: f4b6b0c8787ea344ce9f68f5d506a5d6cc7447114b3dcdbb6d0207372054dfe2

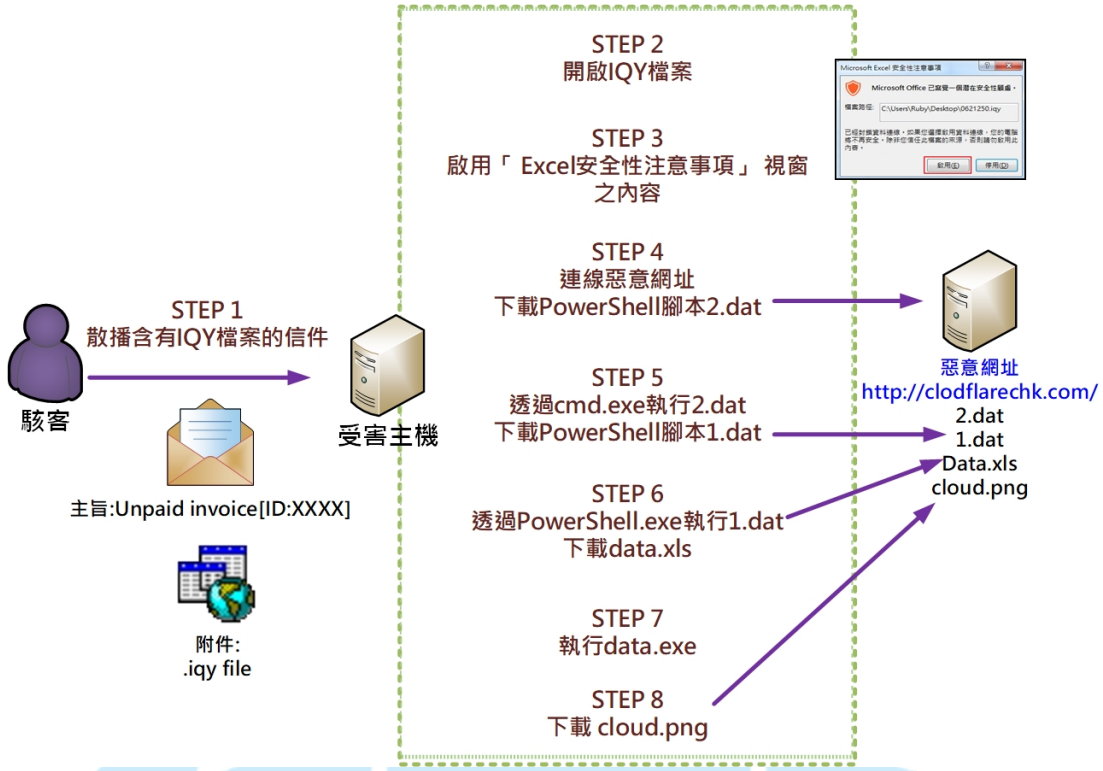
檔案名稱: data.xls

偵測率: 47 / 65

分析日期: 2018-05-30 08:15:35 UTC (1 分鐘 前)

防毒	結果	更新
ESET-NOD32	a variant of Win32/TrojanDownloader.Agent.DZY	20180530
Ikarus	Trojan-Downloader.Win32.Agent	20180529
Sophos ML	heuristic	20180503
K7AntiVirus	Trojan-Downloader (00532ae51)	20180530
K7GW	Trojan-Downloader (00532ae51)	20180530
Kaspersky	Backdoor.Win32.RA-based.gv	20180530
Malwarebytes	Trojan.Downloader	20180530

III. 網路架構圖



1. 駭客散播含有惡意 IQY 檔案的信件。
2. 受害者開啟含有 IQY 檔案的信件，並且開啟 IQY 檔案。
3. 受害者啟用「Excel 安全性注意事項」視窗之內容。
4. 受害主機連線惡意網址並下載 PowerShell 腳本 2.dat。
5. 透過 cmd.exe 執行 2.dat 來下載 PowerShell 腳本 1.dat。
6. 透過 PowerShell.exe 執行 1.dat 來下載 data.xls。
7. 執行偽裝為 Excel 檔案的 data.exe 執行檔。
8. 連線 http://clodflarechk.com/cloud.png，並下載 cloud.png。

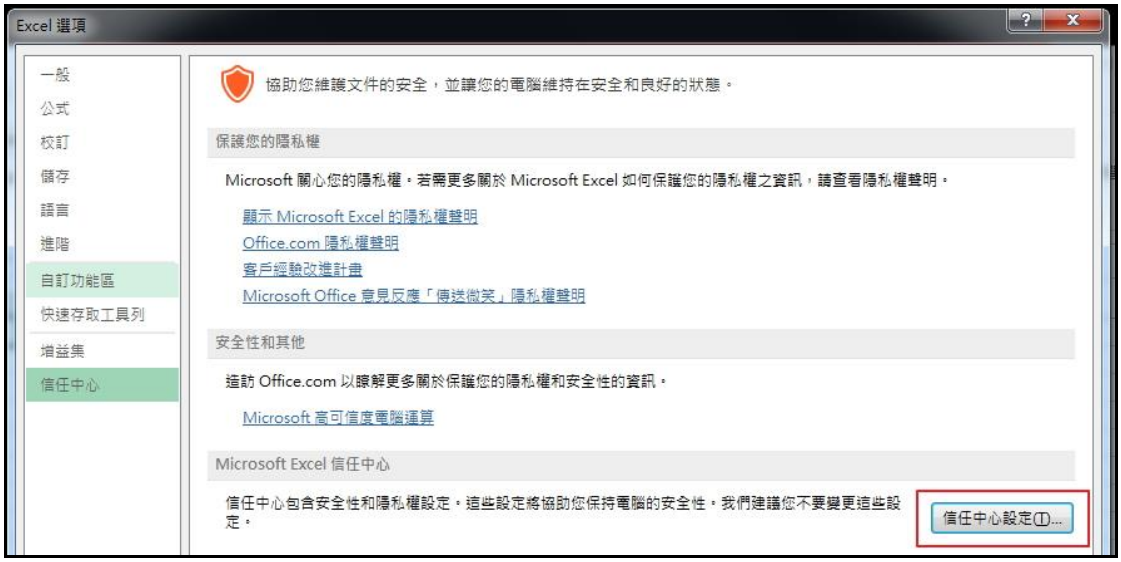
IV. 建議與總結

1. 本事件的發生是駭客散播含有 IQY 附件的信件，讓受害者開啟附件後，下載惡意程式於受害主機上執行，導致受害主機被植入後門程式 Flawed Ammy RAT。

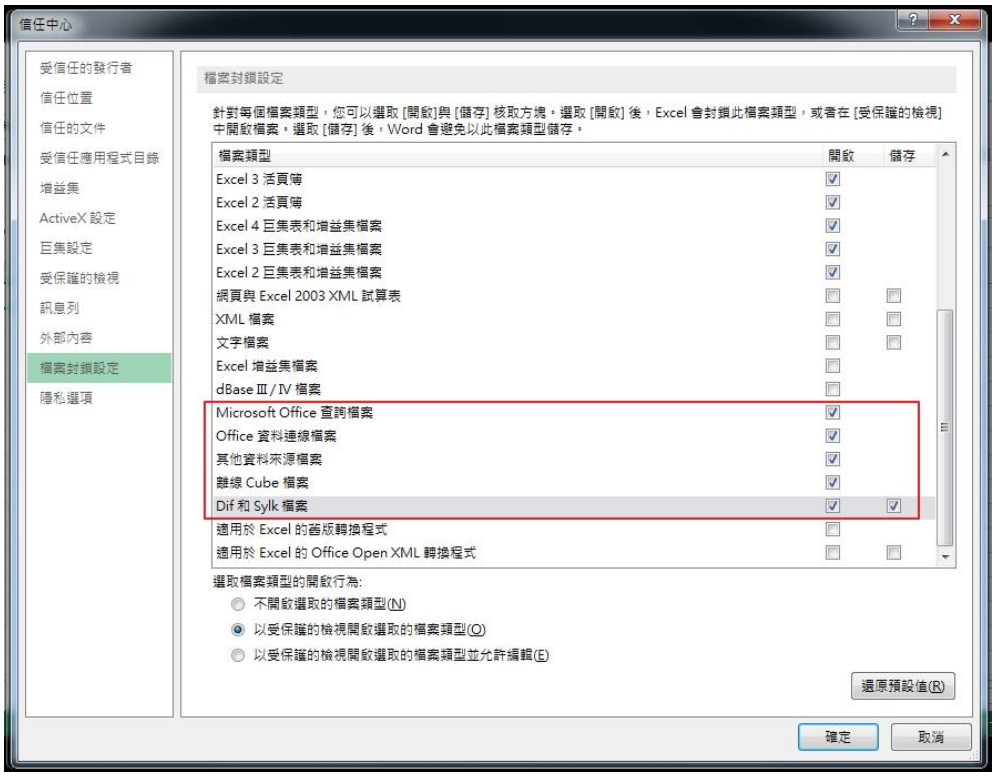
2. 因為 IQY 檔案為純文字格式，而且預設的檔案開啟程式是 Excel，駭客利用這個特性將惡意的網址寫入 IQY 檔，欺騙受害者開啟檔案後連外取得惡意程式回來執行，也因為 IQY 的純文字內容不含有惡意行為，因此也能有效規避防毒軟體的檢查。
3. 駭客在本事件所使用的 IQY 檔案，因為是 Excel Web 查詢的設定檔，可連到指定網址，因此駭客可以很輕易的變更惡意網址，產生新的 IQY 檔案。
4. 本事件所用到的 1.dat 與 2.dat 兩個檔案，可以用記事本編輯後存檔，因此駭客可以很容易隨時修改惡意程式的下載網址與修改執行內容。
5. 為了預防該類型的攻擊事件發生，建議下列幾點措施。

(1)關閉 Excel 檔案的 Web 查詢功能。

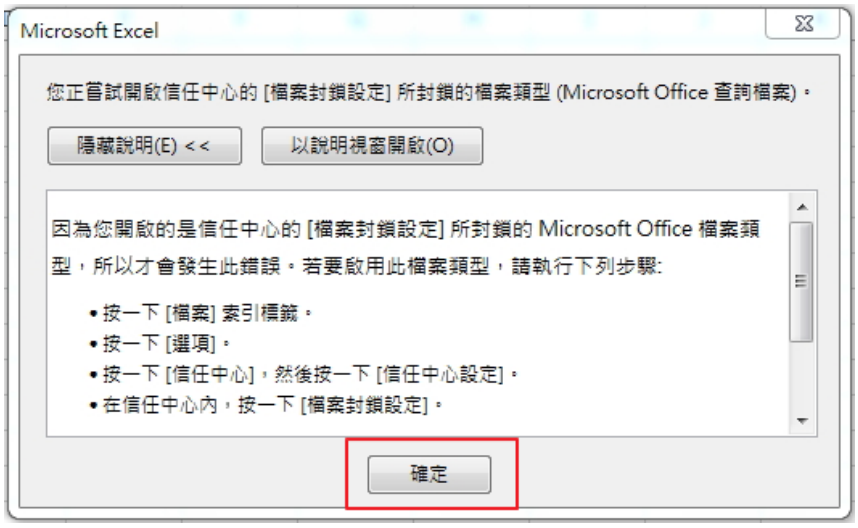
在 Excel 選項的「信任中心」頁面，點選「信任中心設定」。



在信任中心的「檔案封鎖設定」頁面，將從「Microsoft office 查詢檔案」的選項開始至「Dif 和 Sylk 檔案」的選項都打勾。



設定完成後，當開啟檔案封鎖設定所封鎖的檔案類型時則會啟動封鎖，並出現提醒視窗。



(2)不開啟不明來源之檔案。

(3)安裝防毒軟體，並定期進行系統掃毒作業。