

臺北市政府各機關
勒索病毒防範方法

105年06月07日

臺北市政府各機關勒索病毒防範方法					
文件編號	105-01-IF-001	機密等級	內部使用	版次	1.0

【目 錄】

壹、勒索病毒簡介	4
貳、對勒索病毒的防護方案	5
一、事件檢視器各紀錄檔收集（適用用戶端及伺服器端）	5
二、建議使用 Chrome 瀏覽器（適用用戶端）	6
三、使用 Windows Defender（適用用戶端）	9
四、下列軟體務必勤於更新.....	13
五、謹守「321 備份原則」	13
參、勒索病毒緊急處理	14
一、一般使用者	14
二、資訊人員	14
肆、勒索病毒相關解密工具	15
一、Trend Micro 解密工具	15
二、Kaspersky 解密工具.....	16

臺北市政府各機關勒索病毒防範方法					
文件編號	105-01-IF-001	機密等級	內部使用	版次	1.0

【圖目錄】

圖 1	Eventlog5	5
圖 2	Adblock 安裝畫面－1	6
圖 3	Adblock 安裝畫面－2	6
圖 4	Adblock 安裝後運行狀況	7
圖 5	Adblock 過濾清單訂閱	7
圖 6	Adblock 自訂過濾規則	8
圖 7	Abblock－firefox 版	8
圖 8	啟動 Defender	9
圖 9	Defender 控制面板	10
圖 10	設定 Defender 掃描選項及相關設定	10
圖 11	Defender 掃描畫面	11
圖 12	Windows 10 的 Defender 偵測紀錄	12
圖 13	解密工具（Trend Micro）	15
圖 14	解密工具（Kaspersky）	16
圖 15	CryptXXX 2.0 解密工具	16

臺北市政府各機關勒索病毒防範方法					
文件編號	105-01-IF-001	機密等級	內部使用	版次	1.0

壹、勒索病毒簡介

勒索軟體 Ransomware 是一種特殊的惡意軟體，讓受害者失去對系統或資料的控制，如果不付贖金給犯罪組織，將無法把遭加密的資料救回。而犯罪組織利用這種模式，這也是其被稱為「勒索軟體」的原因。

勒索軟體散播超過十年，第一個版本早在 2005 年在俄羅斯現身，從那時候起，勒索軟體傳遍了全球，發展出許多不同的版本。

近年來，甚至發展出各種攻擊手段、支援多國語言，及跨平台感染。最常見的攻擊手段，還是以釣魚郵件為大宗、次之為掛馬網站及惡意廣告。

不管如何，勒索軟體的變種速度極快，感染渠道也不斷在變化。雖各大防毒軟體商，對此類惡意軟體皆有可應對的偵測機制，但「道高一尺，魔高一丈」，唯有保持良好的使用習慣，勤於備份重要資料及修補安全漏洞，方為預防的根本之道。

臺北市府各機關勒索病毒防範方法					
文件編號	105-01-IF-001	機密等級	內部使用	版次	1.0

貳、對勒索病毒的防護方案

以下方案會註明適用於「用戶端」或「伺服器端」(例：File server)

一、事件檢視器各紀錄檔收集 (適用用戶端及伺服器端)

◇ 務必保持以下資料之正常收集



圖1 Eventlog

上述項目務必保持正常運行，否則如感染勒索病毒後，將難以追查感染狀況。此項目務必重點確認，不分伺服器端及用戶端。

臺北市府各機關勒索病毒防範方法					
文件編號	105-01-IF-001	機密等級	內部使用	版次	1.0

二、建議使用 Chrome 瀏覽器（適用用戶端）

請在 Chrome 內的線上應用程式商店中，搜尋 Adblock Plus 或 Adblock，並安裝於 Chrome 瀏覽器內。



圖2 Adblock 安裝畫面-1



圖3 Adblock 安裝畫面-2

臺北市政府各機關勒索病毒防範方法					
文件編號	105-01-IF-001	機密等級	內部使用	版次	1.0



圖4 Adblock 安裝後運行狀況

由上圖可確認安裝後，瀏覽網頁時，阻擋的廣告總數量，或可得知目前正瀏覽的網頁被阻擋了多少內嵌廣告。



圖5 Adblock 過濾清單訂閱

可設定並勾選需要的清單種類，該清單會自動更新。

臺北市府各機關勒索病毒防範方法					
文件編號	105-01-IF-001	機密等級	內部使用	版次	1.0



圖6 Adblock 自訂過濾規則

Adblock 亦有自定義過濾規則的方案，可讓使用者自己來設定要過濾的網頁廣告。

若使用的為 Firefox，該套件亦有支援，請於下方網址登入後進行安裝。

安裝網址：<https://addons.mozilla.org/zh-TW/firefox/>



圖7 Adblock—firefox 版

臺北市政府各機關勒索病毒防範方法					
文件編號	105-01-IF-001	機密等級	內部使用	版次	1.0

三、使用 Windows Defender (適用用戶端)

(一)、 Windows Defender 間諜程式掃描工具，工具特點如下：

- 該工具為 Windows 內建，本身免費。
- 該工具的病毒碼皆由微軟自己定期更新及維護，而核心元件部分會藉由 Windows update 發佈
- 與目前 Officescan 11.0 的掃描機制並不衝突（不建議如此操作，因 Windows Defender 仍屬於防毒軟體範疇，雖掃描機制不衝突，不代表其他功能皆可正常運作。且發現 Windows 10 的平台上如有安裝其他防毒，Defender 會自行關閉）

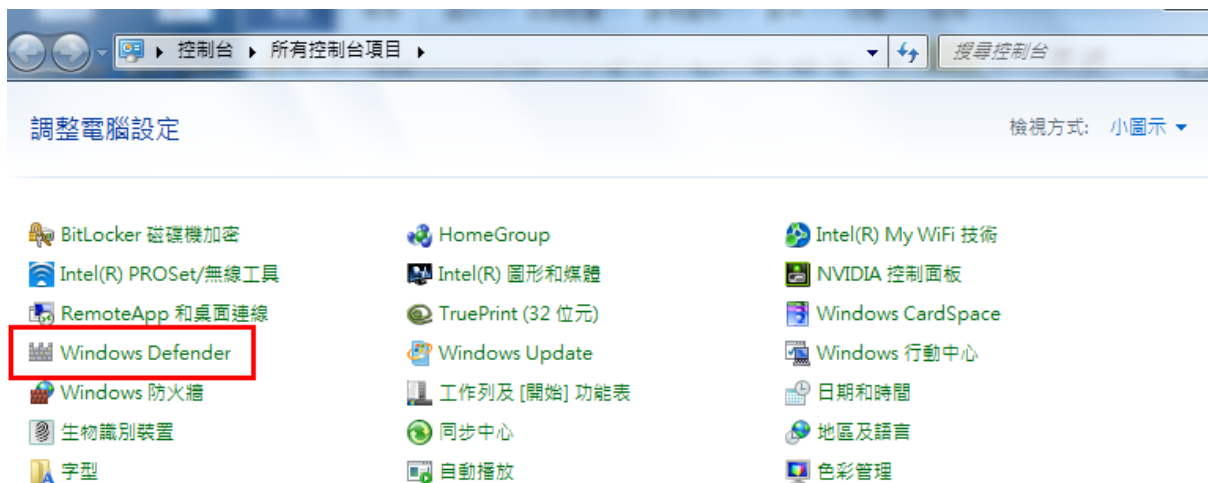


圖8 啟動 Defender

臺北市府各機關勒索病毒防範方法

文件編號	105-01-IF-001	機密等級	內部使用	版次	1.0
------	---------------	------	------	----	-----



圖9 Defender 控制面板

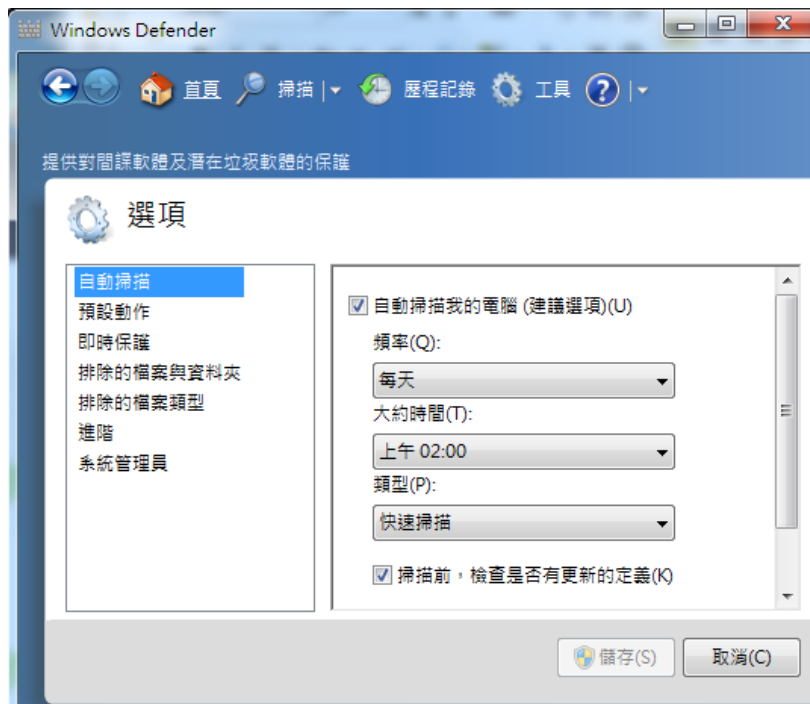


圖10 設定 Defender 掃描選項及相關設定

臺北市府各機關勒索病毒防範方法

文件編號	105-01-IF-001	機密等級	內部使用	版次	1.0
------	---------------	------	------	----	-----

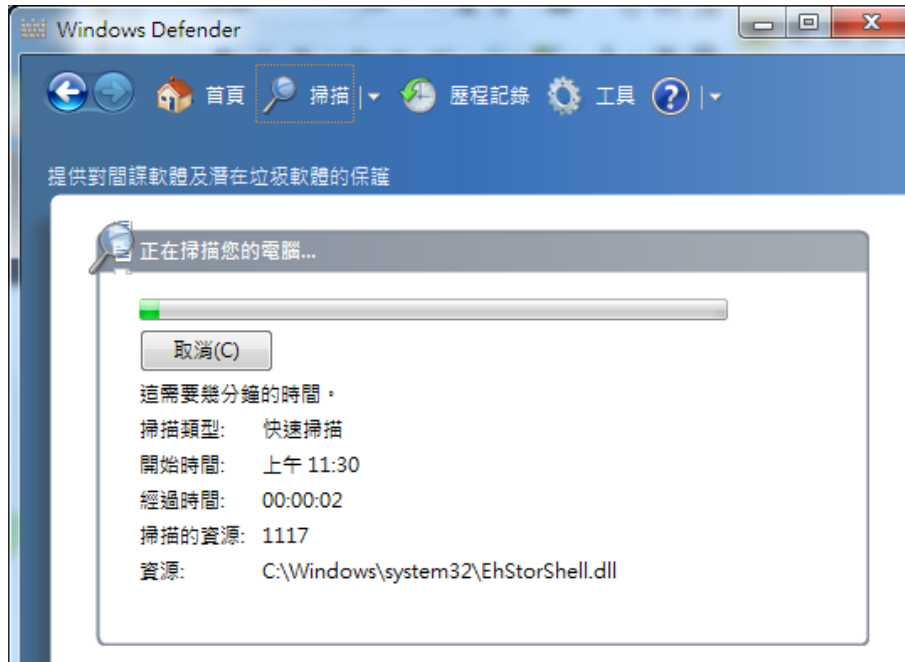


圖11 Defender 掃描畫面

Windows Defender 並不能取代防毒軟體，僅只是一個簡易的防護工具，而微軟近期亦開始重視勒索病毒的發展，相關的弱點也修補得很快，最新的 CryptXXX 3.0 在 Windows 10 上的 Defender 亦可偵測。

臺北市府各機關勒索病毒防範方法					
文件編號	105-01-IF-001	機密等級	內部使用	版次	1.0



圖12 Windows 10 的 Defender 偵測紀錄

如圖 12，可偵測到勒索病毒並有主動防護動作。

(二)、 如對 Windows Defender 的操作有問題，請參考以下說明：

1. **Windows 7 :**

<http://windows.microsoft.com/zh-tw/windows/using-defender#1TC=windows-7>

2. **Windows 8.1 :**

<http://windows.microsoft.com/zh-tw/windows/using-defender#1TC=windows-8>

3. **Windows 10 :**

<http://windows.microsoft.com/zh-tw/windows-10/how-to-protect-your-windows-10-pc#v1h=tab01>

臺北市政府各機關勒索病毒防範方法					
文件編號	105-01-IF-001	機密等級	內部使用	版次	1.0

四、下列軟體務必勤於更新

以下軟體請務必加強更新，避免遭惡意程式利用。

- Java
- Adobe Reader
- Adobe Flash Player
- Silverlight
- Chrome 瀏覽器、Internet Explorer 8、9、10、11、Edge
- Windows OS、Linux OS、Mac OS

五、謹守「321 備份原則」

- 至少備份三份
- 使用兩種不同的備份方式（例：磁帶備份、採備份至其他主機或外接式硬碟的方案等）
- 其中一份備份要存放異地。

臺北市政府各機關勒索病毒防範方法					
文件編號	105-01-IF-001	機密等級	內部使用	版次	1.0

參、勒索病毒緊急處理

一、一般使用者

- 斷網：斷開網路連線
- 斷電：馬上關機，避免加密程序繼續擴大受害範圍（5分鐘內或許可救回部分資料，但針對部分勒索病毒無效）
- 現場保留電腦並通知機關內資訊人員
- 切勿付錢

二、資訊人員

- 關閉帳號，暫時停止該帳號的網路存取登入權限
- 檢查該帳號權限可以寫入的公用資料夾是否感染
- 將硬碟取出，透過另一台電腦備份尚未被加密的檔案
- 回收事件檢視器內紀錄（請參考圖 1）
- 收集勒索訊息及勒索畫面（可加快判定病毒類型）
- 找出勒索病毒入侵管道

臺北市政府各機關勒索病毒防範方法					
文件編號	105-01-IF-001	機密等級	內部使用	版次	1.0

肆、勒索病毒相關解密工具

CryptXXX 2.0 目前已有解密工具，以下資訊供機關資訊人員參考：

一、 Trend Micro 解密工具

<http://esupport.trendmicro.com/solution/zh-TW/1114221.aspx>

此工具支援解密的勒索病毒家族，下表所列的勒索病毒種類及檔案類型是此工具最新版本可以解開的。

勒索軟體種類	被加密後的檔案名稱及副檔名格式
CryptXXX 1.0	{原始檔案名稱}.crypt
CryptXXX 2.0	{原始檔案名稱}.crypt
TeslaCrypt V1	{原始檔案名稱}.ECC
TeslaCrypt V2	{原始檔案名稱}.ECC
TeslaCrypt V3	{原始檔案名稱}.XXX 或 TTT 或 MP3 或 MICRO
TeslaCrypt V4	檔名及副檔名均未被變更
SNSLocker	{原始檔案名稱}.RSNSlocked

圖13 解密工具 (Trend Micro)

勒索訊息檔名格式如下：

- (1). CryptXXX 3.0 勒索訊息檔名格式：「!Recovery_XXXXXXXXXXXX.txt」
- (2). CryptXXX 2.0 勒索訊息檔名格式：「de_crypt_readme.txt」

臺北市政府各機關勒索病毒防範方法					
文件編號	105-01-IF-001	機密等級	內部使用	版次	1.0

二、 Kaspersky 解密工具：

<http://media.kaspersky.com/utilities/VirusUtilities/EN/rannohdecryptor.zip>

該工具適用以下病毒類型：(CryptXXX 僅適用 2.0 含之前版本)

This utility is designed to decrypt files encrypted by trojan programs
Trojan-Ransom.Win32.Rannoh, Trojan-Ransom.Win32.CryptXXX,
Trojan-Ransom.Win32.Cryakl (early variants).

圖14 解密工具 (Kaspersky)

使用解密工具時，仍需注意對應的病毒版本，否則會出現下列訊息。



圖15 CryptXXX 2.0 解密工具