臺北市政府各機關

勒索病毒防範方法

105年06月07日

	臺北市政府名	各機關勒索病	高毒防範方法		
文件编號	105-01-IF-001	機密等級	內部使用	版次	1.0
	【目	錄】			
壹、 勒穷	索病毒簡介				4
贰、 對著	劫索病毒的防護方	案			5
	事件檢視器各紀錄檔收算	〔適用用戶	端及伺服器端)	5
二、莫	建議使用 Chrome 瀏覽器	(適用用戶	端)		6
三、偵	吏用 Windows Defender	(適用用戶端	g)		9
四、一	下列軟體務必勤於更新.				13
五、言	堇守「321 備份原則」				13
冬、 勒穷	索病毒緊急處理				14
- 、 -	一般使用者				14
二、真	資訊人員				14
聿、 勒穷	索病毒相關解密工	具			15
- \ T	Frend Micro 解密工具				15
二、 K	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】

1	Eventlog55
2	Adblock 安裝畫面-16
3	Adblock 安裝畫面-2
4	Adblock 安裝後運行狀況7
5	Adblock 過濾清單訂閱7
6	Adblock 自訂過濾規則8
7	Abblock-firefox 版
8	啟動 Defender9
9	Defender 控制面板10
10	設定 Defender 掃描選項及相關設定10
11	Defender 掃描畫面11
12	Windows 10 的 Defender 偵測紀錄12
13	解密工具(Trend Micro)15
14	解密工具 (Kaspersky)16
15	CryptXXX 2.0 解密工具16
	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

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		

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

書件檢視器				1 4-2-4	
檔案(F) 執行(A) 檢視(V) 說明	(H)				
🗢 🔿 🔁 📰 🚺					
🛃 事件檢視器 (本機)	Windows 記錄				動作
▷ 😽 自訂檢視	名稱	類型	事件數目	大小	Windows 記錄
▲ 應用程式	應用程式	系統管理	16,936	13.07 MB	🦻 開啟已儲存的記錄
፼ 安全性	安全性	糸統管理	17,652	12.07 MB	🍸 建立自訂檢視
□ 安裝	安裝	操作	2,354	1.00 MB	匯入自訂檢視
■ 韓送的事件	条統	条統管理 44-66	49,057	18.07 MB 0.位二组	檢視
▶ 💾 應用程式及服務記錄檔	₩2△N)-要1+	1#TF	0		Q 重新整理
11111111111111111111111111111111111111					? 說明
					應用程式
					開啟
					□ 內容
					説明

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、 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

Ad 来源源 ****	Block 跳:g <u>etadblock.com</u> ★★ (188678) 雪用工具	10,000,000+ 位徳用書		린加램 CHROME 🔫
總覽	吉平論命	支援	相關項目	G+1 {
<image/>		<section-header></section-header>		日では、 日では、 日本のには、 日本のは、 日本のは、
and many r	more ads!			版本: 2.59 更新日期: 2016年6月1日 土小: 877K/B

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。

● AdBlock 一般 邊境清單 自訂 支援機協助
訂閱過濾清單 翻譯貢載: Tai-Lin Chu, II <i>請不要訂閱過多演單,每新博一個演單都會邀瀏覽開的速度降低 (更多詳細資訊和遵邀演單可在這個</i> 找到, AdBlock會自動取得更新。您也可以現在馬上更新
廣告過濾清單 ✓ Acceptable Ads (recommended) 3 小時前更新 ✓ AdBlock 自訂過濾清單(推薦) 3 天前更新 ✓ EasyList(推薦) 3 天前更新 ✓ 中文 3 天前更新 ✓ 依羅斯和烏克蘭 3 天前更新 替其他語言新增過濾清單 →攝擇語言- ▼
其他的過濾清單 Adblock Waming Removal list (removes wamings about using ad blockers) EasyPrivacy (隱私保護) Fanboy's Annoyances (blocks in-page pop-ups, social media and related widgets, and other annoyances) 反社群網站過濾器(社群網站的按鈕會被自動過濾掉) Z 惡意軟體防護 2 天前更新 又 在 AdBlock 檢測到惡意軟體時發出通知 <i>Beta</i>

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。



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/

ABP	Adblock Plus 2.7.3 不会意志的故意。 作者: Wladimir Palant
	討厭擾人的廣告嗎?害怕被追蹤嗎?痛恨一大片的橫幅廣告嗎?快安裝 Adblock Plus 讓 您重拾網路控制權,自己決定想看的內容。
	Adblock Plus 的一分鐘影片介紹〈英文〉: <u>http://www.youtube.com/watch?</u> <u>v=oNvb2SjVjjl</u>
	只在 Firefox 上才有,快來安裝! <u>過私擔保護政策</u>
	還是下載
	◎ 可於 Firefox 38.0 - 49.0 使用 檢視其他版本

圖7 Abblock—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 的掃瞄機制並不衝突(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)

●●● 控制台 → 所有控制	台項目 ▶	▼ 4 援尋控制台
調整電腦設定		檢視方式: 小圖示 ▼
🏘 BitLocker 磁碟機加密	🤣 HomeGroup	🎒 Intel(R) My WiFi 技術
🛜 Intel(R) PROSet/無線工具	🛃 Intel(R) 圖形和媒體	🛃 NVIDIA 控制面板
🔜 RemoteApp 和桌面連線	壑 TruePrint (32 位元)	📑 Windows CardSpace
🕍 Windows Defender	🖉 Windows Update	孋 Windows 行動中心
🔗 Windows 防火牆	🛄 工作列及 [開始] 功能表	□● 日期和時間
⑧ 生物識別裝置	📵 同步中心	🔊 地區及語言
💦 字型	📑 自動播放	💶 色彩管理
	圖8 啟動 Defend	ler

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9 Defender 控制面板

👑 Windows Defender	
会 ● 命 直 ▶ 掃描 提供對間諜軟體及潛在垃圾軟體的保 ● 選項	• 🦀 歴程記錄 🏠 工具 🕐 • R誰
<mark>自動掃描</mark> 預設動作 即時保護 排除的檔案與資料夾 排除的檔案類型 進階 系統管理員	 ✓ 自動掃描我的電腦 (建議選項)(U) 頻率(Q): 每天 ▼ 大約時間(T): 上午 02:00 ▼ 頻型(P): 快速掃描 ▼ ✓ 掃描前,檢查是否有更新的定義(K)
	儲存(S) 取消(C)

圖10 設定Defender 掃描選項及相關設定

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。

件编號	105-01-IF-001	機密等	級 內部	使用	版次	1.0
						0 10 75
首頁 更新	歷程記錄				い設定	? 説明 ▼
檢視被偵測為潤	晋在有害的項目,以及您對其所採	取的動作:				
○隔離的頂目	目(O)					
この時に対応	行但未從電腦移除的項目。					
 ○ Raining [已防止執行 ○ 允許的項目 	行但未從電腦移除的項目。 目(W)					
 一 Nation 4 一 己防止執行 一 公許的項目 您已經允 	行但未從電腦移除的項目。 目(W) 許在電腦上執行的項目。					
 「隔離的項目 已防止執1 〇 允許的項目 您已經允問 ④ 所有偵測 	行但未從電腦移除的項目。 目(W) 許在電腦上執行的項目。 到的項目(D)					
 高離的項目 己防止執行 允許的項目 您已經允問 ● 所有偵測3 在您電腦」 	行但未從電腦移除的項目。 目(W) 許在電腦上執行的項目。 到的項目(D) 上偵測到的項目。					
 高融的渠道 己防止執行 分許的項目 您已經允請 所有偵測器 在您電腦」 	行但未從電腦移除的項目。 目(W) 許在電腦上執行的項目。 到的項目(D) 上偵測到的項目。	警示等級	日期		己執行的動作	
 ○ 福祉的項目 ○ 允許的項目 ○ 所有偵測引 在您電腦」 値測到的項目 □ ② Trojan: 	行但未從電腦移除的項目。 目(W) 許在電腦上執行的項目。 到的項目(D) 上偵測到的項目。	警示等級 嚴重	日期 2016/4/15 下午	: 05:42	已執行的動作 隔離	
 ○ 福祉的項目 ○ 允許的項目 ⑥ 所有偵測3 在您電腦 ④ 「有有(面) ④ 「有有(面) ④ 「「」 ○ 「「」 ○ 「「」 ○ 「「」 ○ 「」 ○ 「」	行但未從電腦移除的項目。 目(W) 許在電腦上軌行的項目。 到的項目(D) 上偵測到的項目。 :Win32/Carberp.K m:HTML/Tescrypt.C	警示等級 嚴重 嚴重	日期 2016/4/15 下午 2016/4/15 下午	: 05:42 : 05:42	已執行的動作 隔離 隔離	
 高離的項目 己防止執行 分許的項目 所有偵測 在您電腦」 傾測到的項目 図 Trojan: ③ Ransor ③ Ransor 	行但未從電腦移除的項目。 目(W) 許在電腦上軌行的項目。 到的項目(D) 上偵測到的項目。 :Win32/Carberp.K m:HTML/Tescrypt.C m:HTML/Tescrypt.E	警示等級 嚴重 嚴重 嚴重	日期 2016/4/15 下午 2016/4/15 下午 2016/4/15 下午	: 05:42 : 05:42 : 05:42	已執行的動作 隔離 隔離	
 高離的渠道 己防止執行 分許的項目 您已經分詞 在您電腦」 有償測到 在您電腦」 (1) (2) (2) (3) (4) (5) (5) (6) (7) (7) (7) (8) (7) (8) (7) (9) (9)	行但未從電腦移除的項目。 目(W) 許在電腦上執行的項目。 到的項目(D) 上偵測到的項目。 :Win32/Carberp.K m:HTML/Tescrypt.C m:HTML/Tescrypt.E	警示等級 嚴重 嚴重 嚴重	日期 2016/4/15 下午 2016/4/15 下午 2016/4/15 下午	: 05:42 : 05:42 : 05:42	已執行的動作 隔離 隔離	
 ○ 福祉的項目 ○ 允許的項目 您已經允訂 ● 所有偵測到 在您電腦」 (圓測到的項目 ○ Trojan: ○ Ransor ○ Ransor ⑦ 和別: 特洛伊? 	行但未從電腦移除的項目。 目(W) 許在電腦上執行的項目。 到的項目(D) 上偵測到的項目。 :Win32/Carberp.K m:HTML/Tescrypt.C m:HTML/Tescrypt.E	警示等級 嚴重 嚴重 嚴重	日期 2016/4/15 下午 2016/4/15 下午 2016/4/15 下午	05:42 05:42 05:42	已執行的動作 隔離 隔離	

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-yo ur-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:

ー、 Trend Micro 解密工具

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

勒贖軟體種類	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_xxxxxxxxxxx.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						
文件编號	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