

個案分析-

會說話的加密勒索病毒  
Cerber Ransomware 事件分  
析報告

TACERT 臺灣學術網路危機處理中心團隊製

2016/8

## I. 事件簡介

1. 近年來加密勒索病毒盛行，市面上出現的 ransomware 版本琳瑯滿目，台灣的受害單位更不計其數，企業、政府或醫院都深受其害。
2. 除了一般企業會遭受加密勒索病毒攻擊，政府單位或學術單位也成為被攻擊的對象，很多都是透過瀏覽器漏洞或 APT 郵件感染。
3. 此類加密勒索共同點都是以比特幣為贖金的支付方式，因為比特幣的匿名性可以輕易規避金流追查，更成為犯罪組織喜愛的使用方式。
4. 本單位取得近期標榜會說話的加密勒索病毒樣本進行研究分析，此版本病毒已被破解能夠還原解密檔案。

## II. 事件檢測

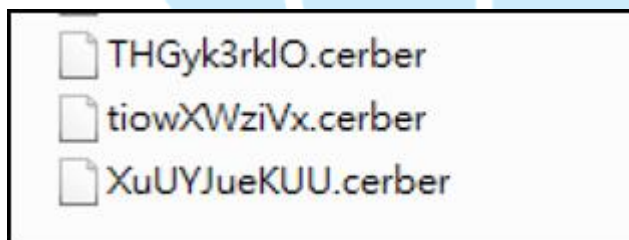
1. 使用 VM 虛擬主機並且為 Windows 7 系統進行隔離環境測試，惡意程式樣本名稱為 cerber.exe 的執行檔。
2. 原本的惡意程式會開始針對內部文件、影音、圖像檔案進行加密，然後惡意程式主體就會自我刪除。
3. 當主機內部的文件檔案被加密完成之後，桌面背景會被置換成灰底白字的警告文字，說明你的文件和其他檔案都已經被加密。



4. 系統會撥放一段語音，其內容為 “Attention! Attention! Attention! Your documents, photos, databases and other important files have been encrypted!”。

而這段語音的意思是，「注意！注意！注意！你的文件、照片、資料庫和其他重要檔案都已經被加密！」

5. 此時檢查所有資料夾內文件，其檔案名稱都被更換為副檔名是 cerber 的加密文字。



6. 在所有被加密檔案的資料夾中皆會新增四個檔案，分別有 html、txt、lnk 和 vbs 檔案，都是告知使用者加密勒索的說明文件。



7. 執行並檢查 vbs 內的程式碼得知，該檔案會使用迴圈播放十次關於檔案已經被加密的警告語音。

```
1 Set SAPI = CreateObject("SAPI."+"SpVoice")
2 SAPI.Speak "Attention! Attention! Attention!"
3 For i = 1 to 10
4 SAPI.Speak "Your documents, photos, data and other important files have been encrypted!"
5 Next
```

8. 從 txt 或 html 文件檔中得知，該病毒名稱為 cerber ransomware，不像其他加密勒索病毒，它並未顯示是使用何種加密演算法加密。但卻顯示該惡意程式 cerber ransomware 已經從主機中移除，並且警告任何嘗試用第三方的解密工具都可能毀壞已被加密的檔案。必須透過購買他們的解密工具 decryptor 才能夠解救檔案。

## CERBER RANSOMWARE

Cannot you find the files you need?

Is the content of the files that you looked for not readable?

It is normal because the files' names, as well as the data in your files have been encrypted.

Great!!!

You have turned to be a part of a big community #Cerber\_Ransomware.

If you are reading this message it means the software "Cerber Ransomware" has been removed from your computer.

It is necessary to realize that we are the ones who closed the lock on your files and we are the only ones who have this secret key to open them.

Any attempts to get back your files with the third-party tools can be fatal for your encrypted files.

For your information the software to decrypt your files (as well as the private key provided together) are paid products.

After purchase of the software package you will be able to:

1. decrypt all your files;
2. work with your documents;
3. view your photos and other media;
4. continue your usual and comfortable work at the computer.

If you understand all importance of the situation then we propose to you to go directly to your personal page where you will receive the complete instructions and guarantees to restore your files.

9. 該說明文件提供很多的付款網域名稱，但大多名稱都無法正常解析出地址，因此還是得用提供的匿名網路去解析，而該網域名稱會以“<http://XXXX.onion.to/識別碼>”的形式出現，並透過 tor 洋蔥瀏覽器才能登入。

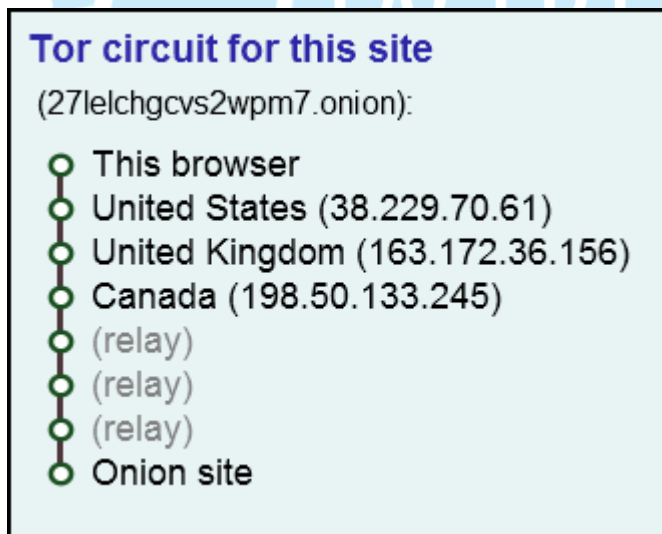
There is a list of temporary addresses to go on your personal page below:

1. <http://271elchgcv2wpm7.h079j8.top/40B8-7CB3-C853-006D-FCF9>
2. <http://271elchgcv2wpm7.fm0cga.top/40B8-7CB3-C853-006D-FCF9>
3. <http://271elchgcv2wpm7.5pyr5p.top/40B8-7CB3-C853-006D-FCF9>
4. <http://271elchgcv2wpm7.b7mciu.top/40B8-7CB3-C853-006D-FCF9>
5. <http://271elchgcv2wpm7.onion.to/40B8-7CB3-C853-006D-FCF9>

10. 透過 tor 登入付款頁面還會提供多國語言讓受害者選擇，表示駭客的目標是世界各國主機。



11. 從 Tor 瀏覽器可以得知目前透過那些 proxy 節點進行連線到贖金支付伺服器 <http://271elchgcvs2wpm7.onion/40B8-7CB3-C853-006D-FCF9>，此例中能夠看到至少透過三個 IP 節點當作中繼跳板才能連到 onion site。



12. 在勒贖頁面中使用者必須支付 320 美元的贖金來購買 cerber decryptor，並且以比特幣作為唯一支付方式，防止被追查到金錢流向。一旦超過 5 天付款期限，贖金將會提高至 2 倍金額 640 美元。

您的文档、照片、数据库和其他重要文件将被加密！

若要解密您的文件，您需要购买特殊的软件 – «Cerber Decryptor»。

所有的交易仅通过  bitcoin 网络完成。

在 5 天内您可以按照特惠价格 **฿0.4917 (≈ \$320)** 购买该产品。

5 天后该产品价格将提高到 **฿0.9834 (≈ \$641)**。

特惠价有效

04 . 23:59:36

13. 駭客為了提高受害者完成支付贖金比率，還特地教學如何使用以及購買比特幣，來完成購買駭客提供的解密軟體 Cerber Decryptor。

### 如何购买«Cerber Decryptor»?

1. 创建比特币钱包 (我们推荐 [Blockchain.info](https://blockchain.info))

2. 购买所需金额的比特币

别忘记比特币网络会收取交易手续费 (≈ **฿0.0005**)。

这是我们的建议：

[btcdirect.eu](https://btcdirect.eu) – 为欧洲很好的服务

[bittylicious.com](https://bittylicious.com) – 通过 Visa / MC 或者 SEPA (EC) 银行转账汇划取得 BTC

[localbitcoins.com](https://localbitcoins.com) – 该服务让您寻找希望直接把 Bitcoins 卖出去的人 (WU, 现金, SEPA, Paypal 等等)

[cex.io](https://cex.io) – 通过 Visa/Mastercard 或者 Wire Transfer 把 Bitcoins 购买。

[coincafe.com](https://coincafe.com) – 为快速简单的服务推荐。付款方式: Western Union, 美国银行, 用现金通过 FedEx, Moneygram, 汇款

14. 受害者若要支付贖金，還必須學會使用發送比特幣款項 0.4917 BTC 至駭客提供的錢包地址，並會顯示該錢包的支付狀態在網頁底下。

3. 向以下比特币地址发送 **0.4917** :

12DC7TEbHGJcsF9YWuq544RDhh5Cneb9gG



4. 在下方«付款历史记录»面板中控制交易金额

15. 除此之外為了取信受害者網站提供的 Cerber Decryptor 確實能夠還原檔案，因此還免費解開一個檔案做驗證，也確實能夠還原檔案。



16. 幸運地是此 cerber ransomware 在各大防毒軟體廠商努力下，已經成功製作出免費的 Cerber Decryptor，有一定機率能夠成功解密還原檔案，使用者可以到趨勢科技參考教學下載。


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

17. 值得注意的是，因為一旦感染會產生短暫的對外 udp 攻擊，封包此類型的加密勒索軟體 cerber ransomware，其特徵能有效的被學術網路的團隊偵測到並且開立資安事件單。

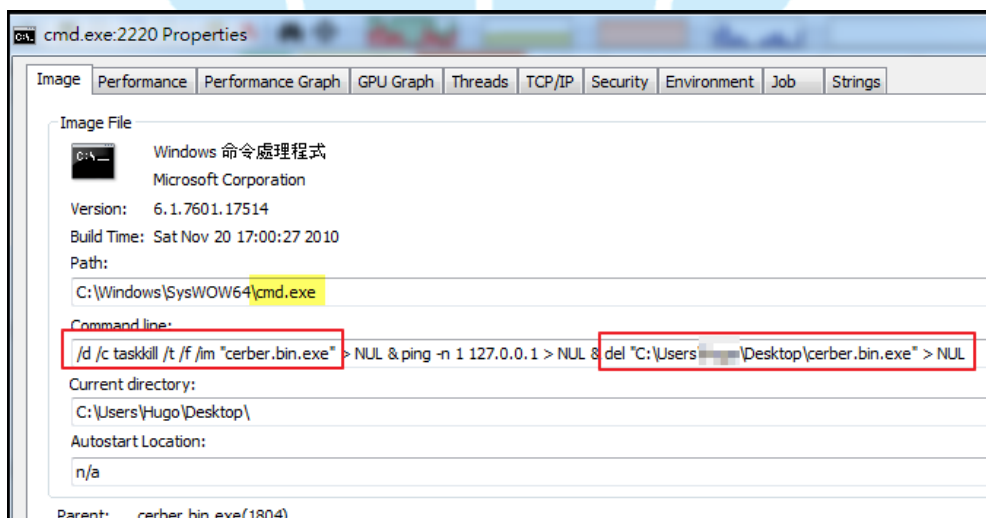


教育機構資安通報平台			
事件類型: 入侵事件警訊			
事件單編號: AISAC-0000			
原發布編號	ASOC-INT-0000000	原發布時間	2016-07-25 15:10:19
事件類型	對外攻擊	原發現時間	2016-07-25 14:57:06
事件主旨	通報: (國立中山大學) 140 疑似對外進行 utm: udp 攻擊		
事件描述	ASOC 發現貴單位(國立中山大學)所屬 140 疑似對外進行 utm: udp 攻擊		
手法研判	貴單位疑似對外進行非法攻擊行為, Cerber Botnet 是一個透過強行加密用戶檔案進而獲利的語音勒索軟體。Cerber Botnet 使用 json 格式的設定檔, 這種檔案格式通常用來傳送和儲存定義在屬性值對內的資料。攻擊者並以恢復正常功能作為交換條件進而勒索金錢, 要求使用者支付 1.24 比特幣, 七天後增加至 2.48 比特幣。		

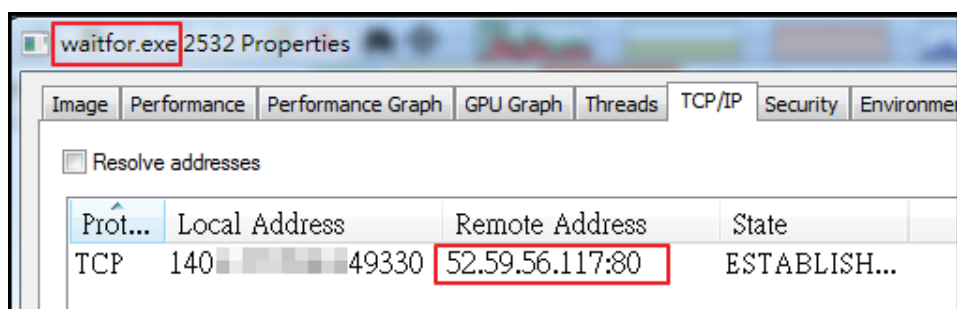
18. 透過 Virustotal 線上掃毒, 該病毒的檢測比例為 44/53, 其中有少數幾間的防毒軟體判定為 cerber ransomware。

SHA256:	9122248bbc055931b5acf1c2f1611dc5799721ae76af886589931fe77e9660bd	
檔案名稱:	9122248bbc055931b5acf1c2f1611dc5799721ae76af886589931fe77e9660bd.bin	
偵測率:	44 / 53	
分析日期:	2016-07-22 19:32:06 UTC (2 週, 2 天前)	
防毒	結果	更新
ALYac	Trojan.GenericKD.3395575	20160722
AVG	Generic_r_LCR	20160722
AVware	Trojan.Win32.Generic!BT	20160722
Ad-Aware	Trojan.GenericKD.3395575	20160722
AegisLab	Troj.W32.Selfdelc	20160722
AhnLab-V3	Trojan/Win32-Cerber.N2044559344	20160722

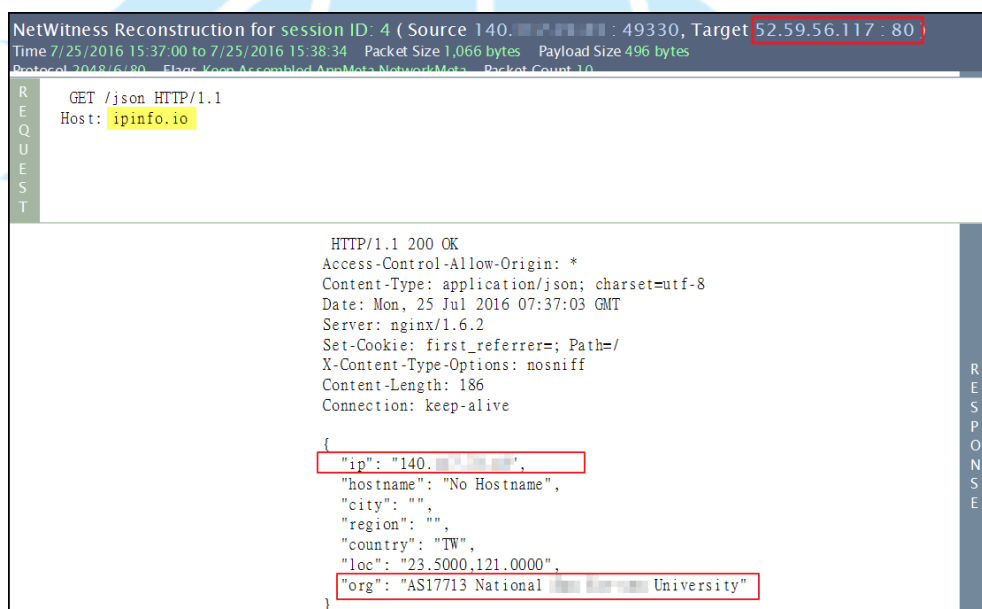
19. 測試惡意程式過程中, 待所有檔案都被加密之後會執行 cmd 一段指令 taskkill 和 del, 將背景的 cerber 程序和原始執行檔進行自刪除, 確保使用者找不到原始的程式樣本。



20. 透過 cports 去紀錄惡意程式執行後的網路行為，可以看到程序 waitfor.exe 先對外部的 52.59.56.117 的 port 80 進行 TCP 連線。



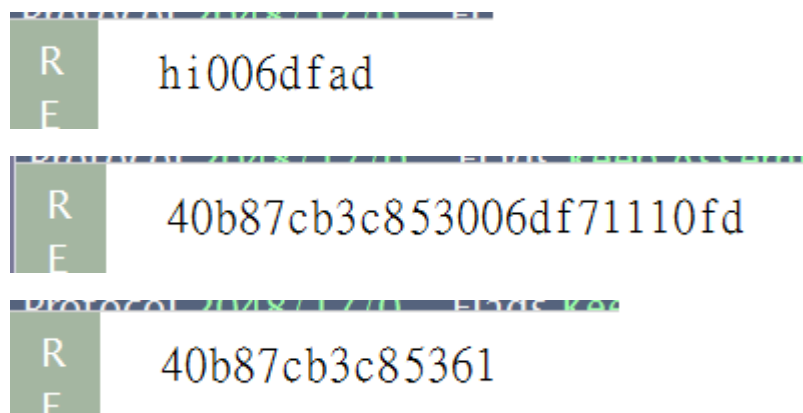
21. 從封包紀錄中查看得知該 IP 52.59.56.117 的網域名稱是 ipinfo.io，一個能夠查詢自己主機外部 IP 的一個網站，是惡意程式先將受感染主機 IP 資訊找出後回報給 C&C 主機所用。



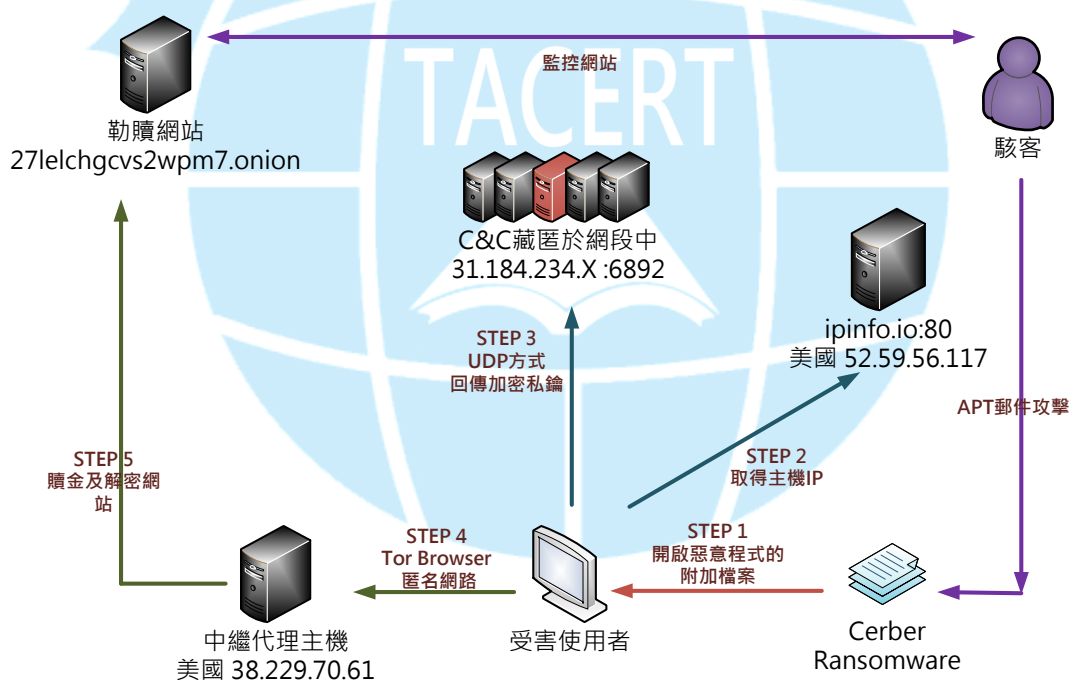
22. 接著惡意程式會開始對 31.184.234.0 和 31.184.235.0 的網段 port 6892 開始發送 UDP 封包，該網段 IP 位於烏克蘭，而此發送的 UDP 封包就是被偵測開立資安事件單的主要原因。

No.	Time	Source	Destination	Protocol	Length	Info
25	1.186758	140....	31.184.234.11	UDP	51	62151 → 6892 Len=9
26	1.186813	140....	31.184.234.12	UDP	51	62151 → 6892 Len=9
27	1.186867	140....	31.184.234.13	UDP	51	62151 → 6892 Len=9
28	1.186921	140....	31.184.234.14	UDP	51	62151 → 6892 Len=9
29	1.186976	140....	31.184.234.15	UDP	51	62151 → 6892 Len=9
30	1.187031	140....	31.184.234.16	UDP	51	62151 → 6892 Len=9
31	1.187085	140....	31.184.234.17	UDP	51	62151 → 6892 Len=9
32	1.187140	140....	31.184.234.18	UDP	51	62151 → 6892 Len=9
33	1.187194	140....	31.184.234.19	UDP	51	62151 → 6892 Len=9

23. 檢查這些 UDP 封包內容主要都是三個加密字串，可能是 cerber 加密後產出的私鑰，回傳給藏匿於該網段中的 C&C 伺服器。



### III. 網路架構圖



1. 使用者可能透過 APT 郵件攻擊開啟含有 cerber 惡意程式的檔案。
2. 主機感染惡意程式後向網站「ipinf.io」取得 IP 位址。
3. 惡意程式開始向 31.184.234.0 網段發送含有密鑰的 UDP 封包給 C&C。
4. 受害者必須透過 Tor 瀏覽器連到勒贖網站 271elchgcvs2wpm7.onion。

5. 駭客要求受害者以比特幣方式支付贖金取得解密金鑰。
6. 現今已有破解的解密工具能夠免費在防毒軟體網站取得。

#### IV. 建議與總結

1. 使用者可能透過被 APT 攻擊或網路下載執行到惡意程式而遭受感染，目前有多數人回報是透過瀏覽器就莫名遭受感染，並未下載執行到可疑檔案。
2. 惡意程式感染主機後會開始加密所有磁碟中的文件檔、圖片檔和影音檔案。
3. 惡意程式一旦加密完文件檔案後會自我刪除，不讓使用者取得惡意程式。
4. 惡意程式隨後會更改系統桌面以及跳出灰底白字勒索畫面，引導受害者如何去支付贖金來取得解密私鑰。
5. Cerber 惡意程式與其他 ransomware 最大不同處在於感染後會有人工語音的提示。
6. 防毒軟體廠商雖已經破解製作出解密工具，但病毒也可能會持續進化變形，建議使用者還是要定期備份重要資料避免無法挽回。
7. 建議使用者將系統重新安裝，避免病毒遺留的影響往後可能再次發生。
8. 建議使用者將作業系統更新，並且更新常用套件如 Adobe Flash Player、Adobe Reader、Java 等，這些漏洞都有可能導致感染類似的勒索程式。