個案分析-

Pylocky 勒索病毒攻擊事件分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

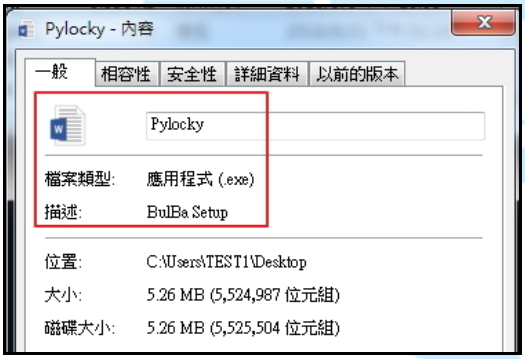
107 年 10 月

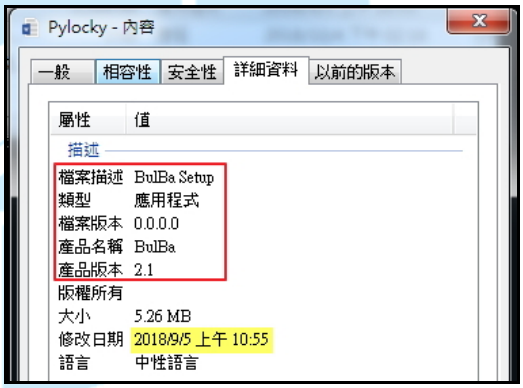
I. 事件簡介

1. 在 2018 年 7-8 月資安公司的安全研究人員發現名為 PyLocky 的勒索病毒，該病毒是用 Python 語言編寫，與 PyInstaller 一起打包，具有反機器學習能力，而且還利用開源腳本的 Inno Setup Installer。
2. 駭客透過大量垃圾郵件來散播 PyLocky 勒索軟體，儘管它在勒索信中號稱是 Locky，但事實上 PyLocky 與 Locky 勒索病毒是無關的。
3. 為了解 Pylocky 勒索病毒感染受害主機後之系統行為與網路行為，本中心取得該病毒樣本後進行實機檢測。

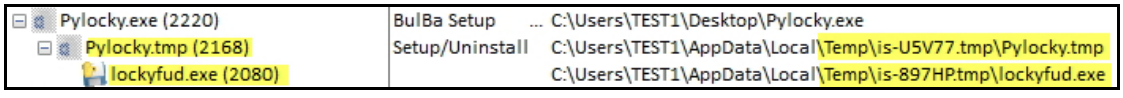
II. 事件檢測

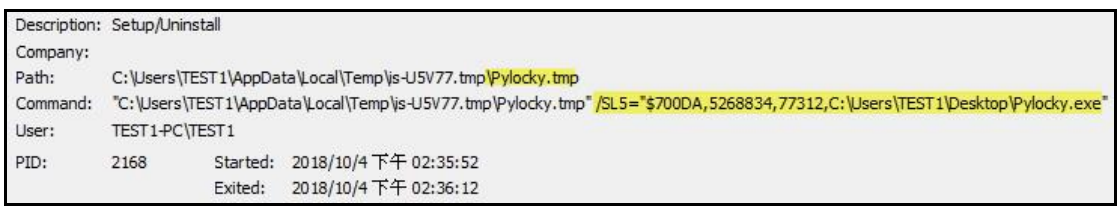
1. 首先，使用 1 台安裝 Windows 7 系統的 VM 虛擬主機進行隔離環境測試，該主機有設定連接一個網路磁碟機 Z，而惡意程式樣本為 Pylocky.exe，將它放於受測主機上執行。



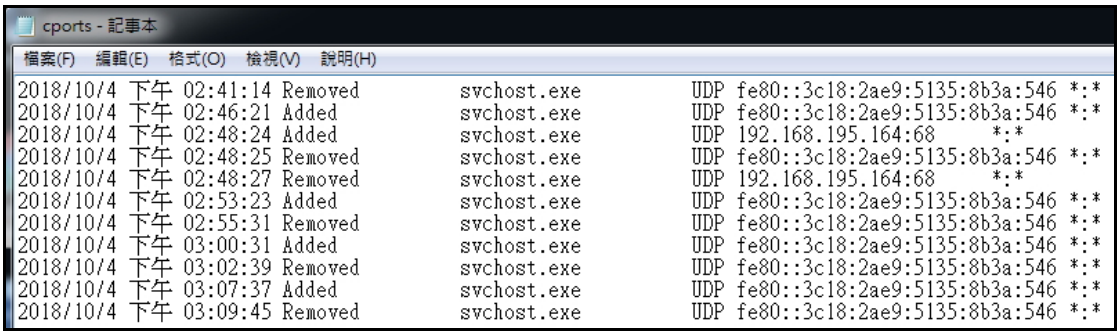


2. 檢視背景程式執行情形，發現當 Pylocky.exe 執行後，會呼叫 Pylocky.tmp，之後會執行 lockyfud.exe。



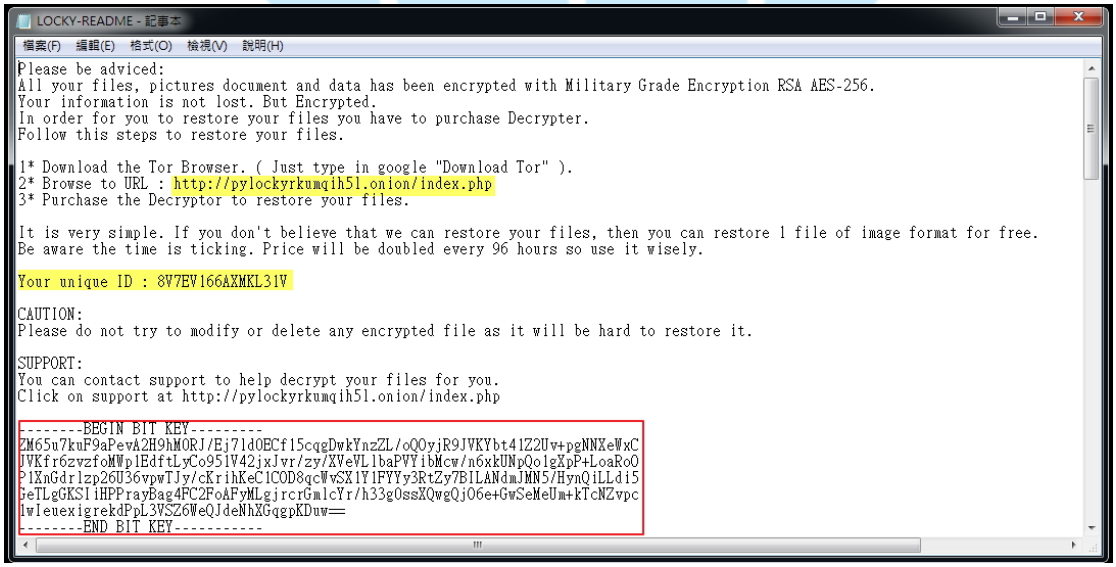


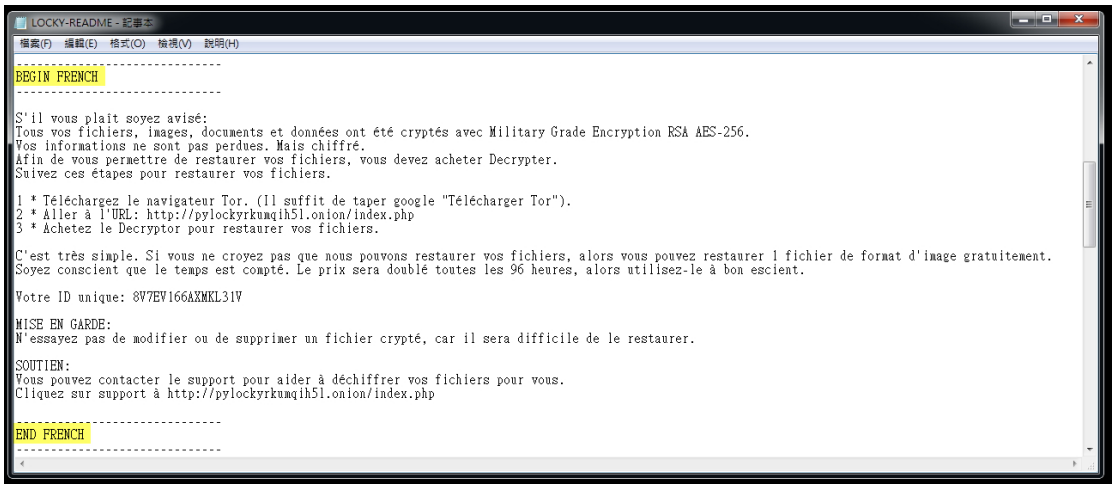
3. 檢視受害主機對外連線的情形，發現在 Pylocky.exe 執行後並未對外連線其他網外主機，可見此病毒主要針對受害主機進行勒索，無網路連線行為。

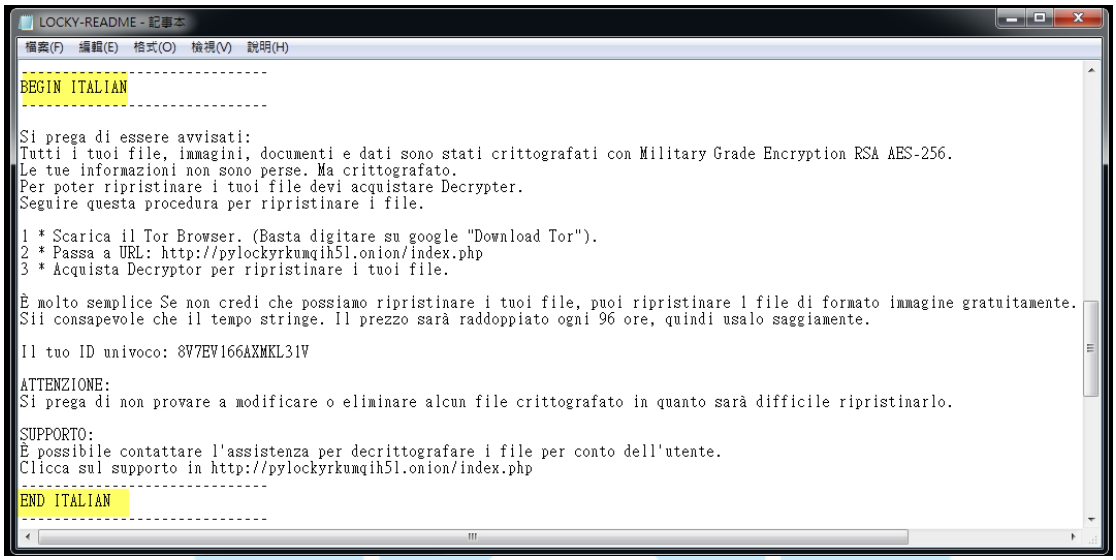


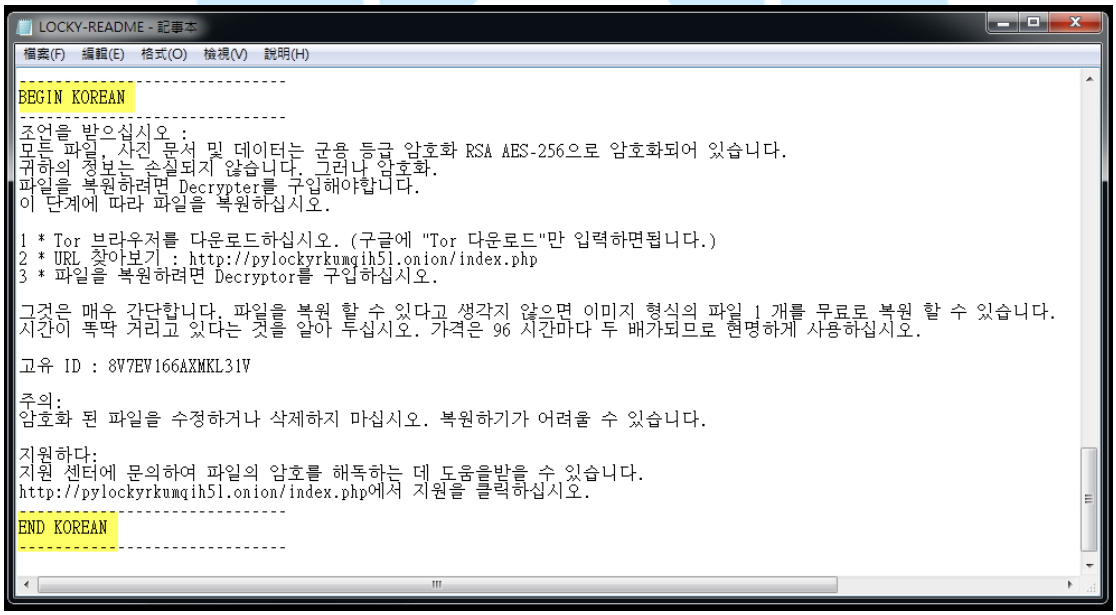
4. Pylocky.exe 執行完成後，會在桌面與使用者資料夾內新增一個 LOCKY-README.txt 的勒索通知信，該通知信內容以四種語言撰寫，分別為英文、法文、義大利文與韓文，這表示該病毒可能針對懂這四種語言之一的使用者發動攻擊。

在勒索通知信中，駭客告訴受害者使用 Tor Browser 至網址 http://pylockyrkumqih51.onion/index.php 去取得購買解密器來恢復被加密檔案的方式，也提供受害者個人 ID 與 BIT KEY 資訊。



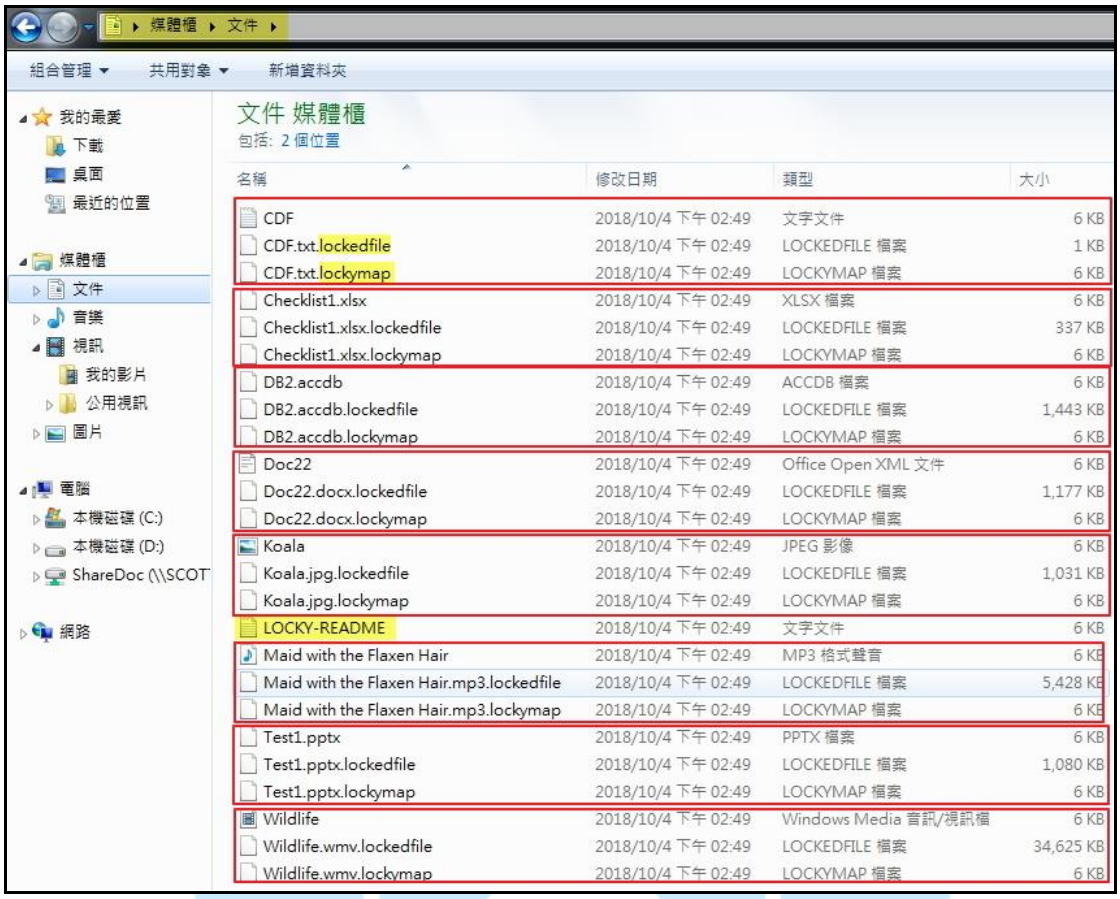


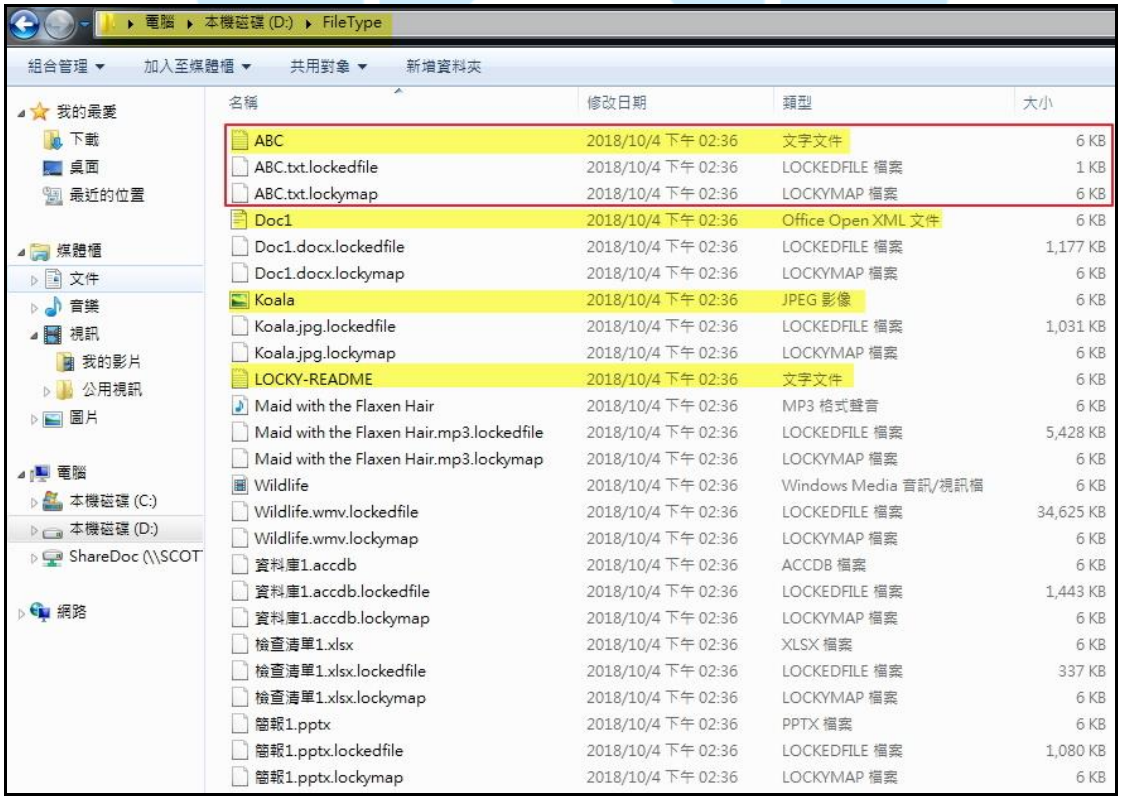


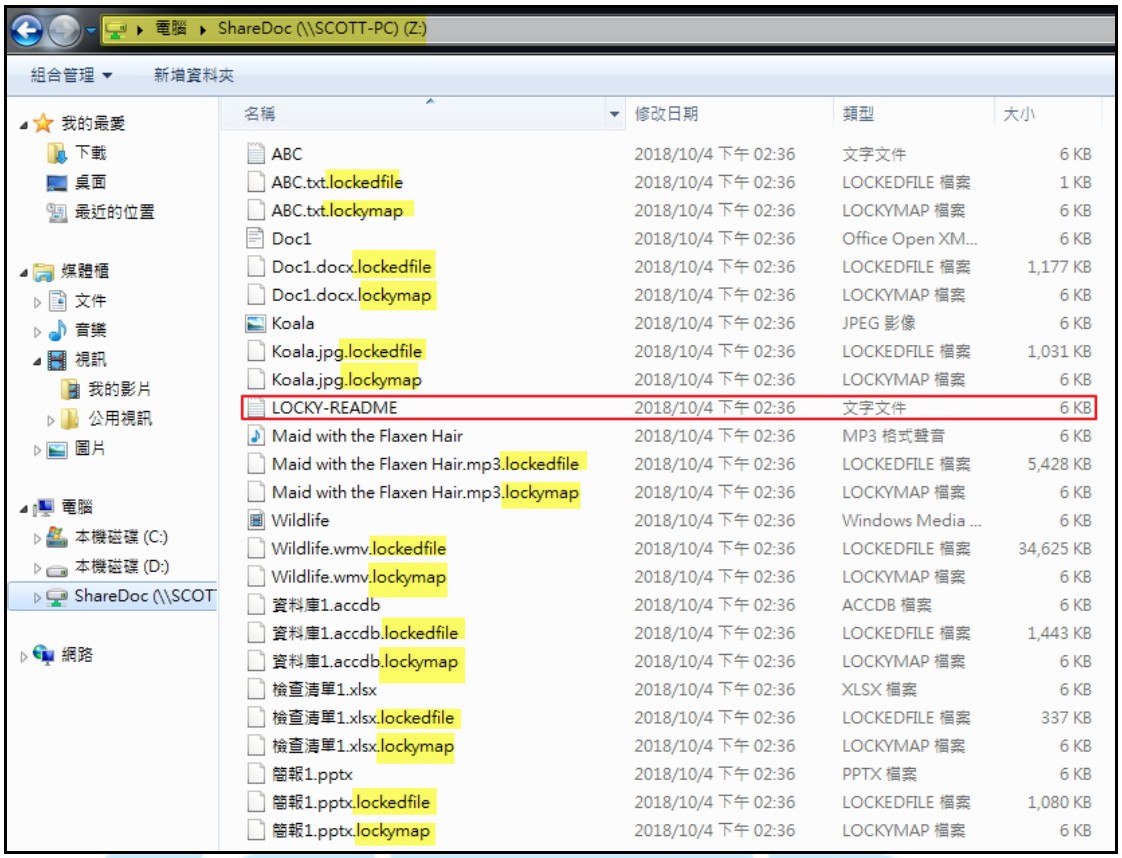


5. 檢視受害主機內檔案被加密的情形，發現使用者的文件資料夾、D 槽磁碟機的資料夾與網路磁碟機 Z 的資料夾內的檔案都被加密，但是在使用者的媒體

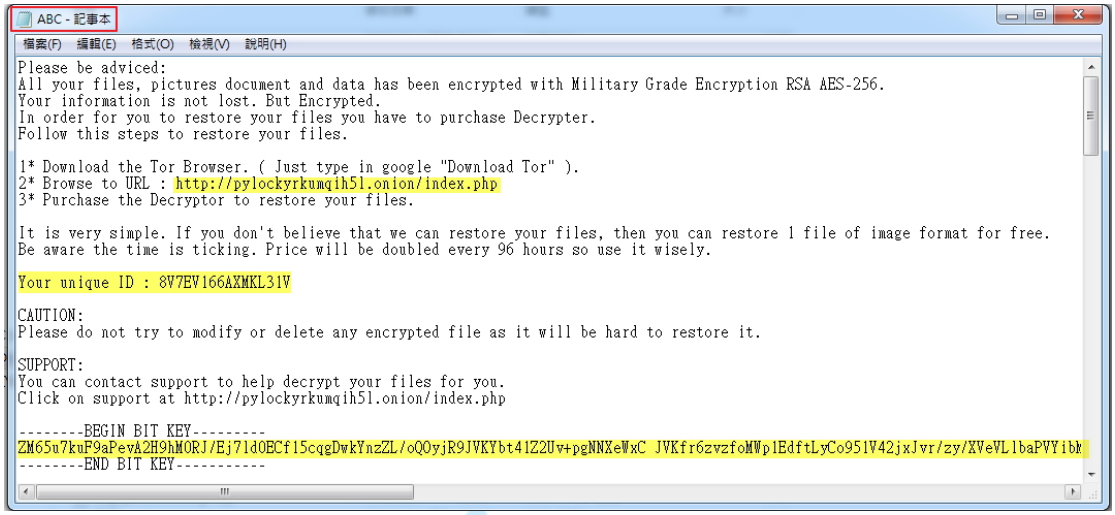
櫃之音樂、視訊與圖片等資料夾內檔案未被加密。該惡意程式在加密後會針對每個被加密的檔案產生兩個副檔名為「.lockedfile」與「.lockymap」檔案。

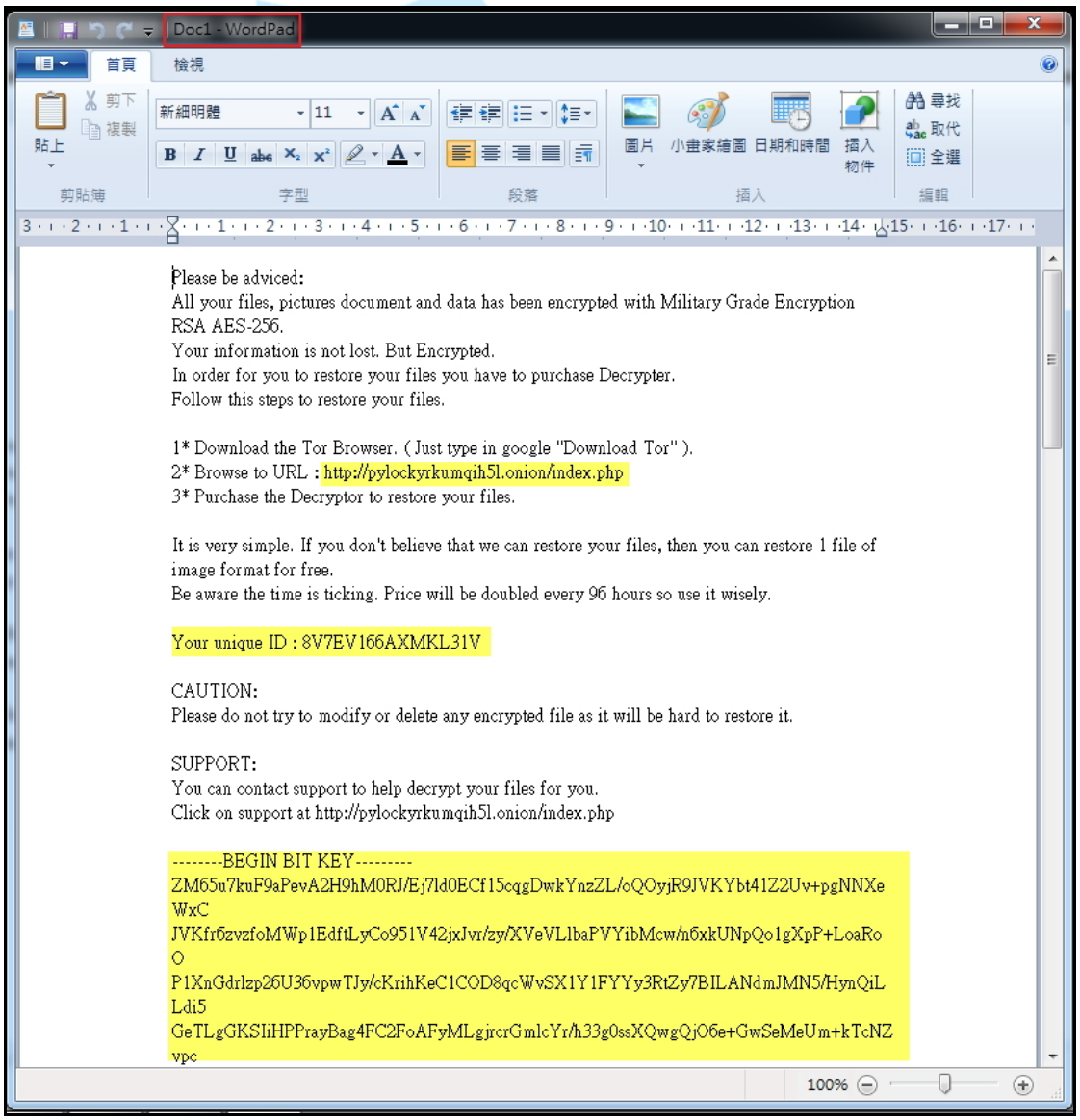


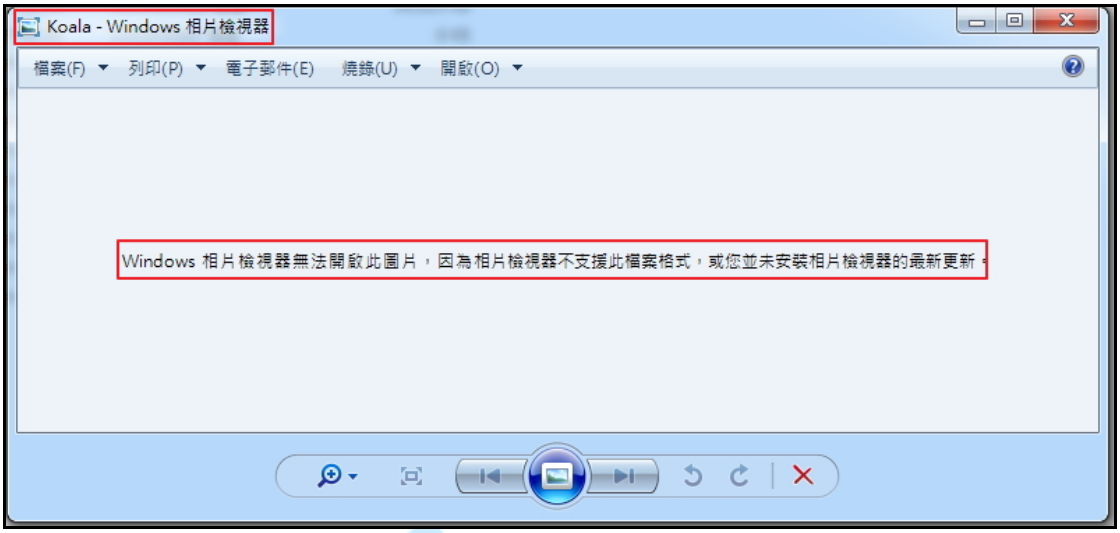




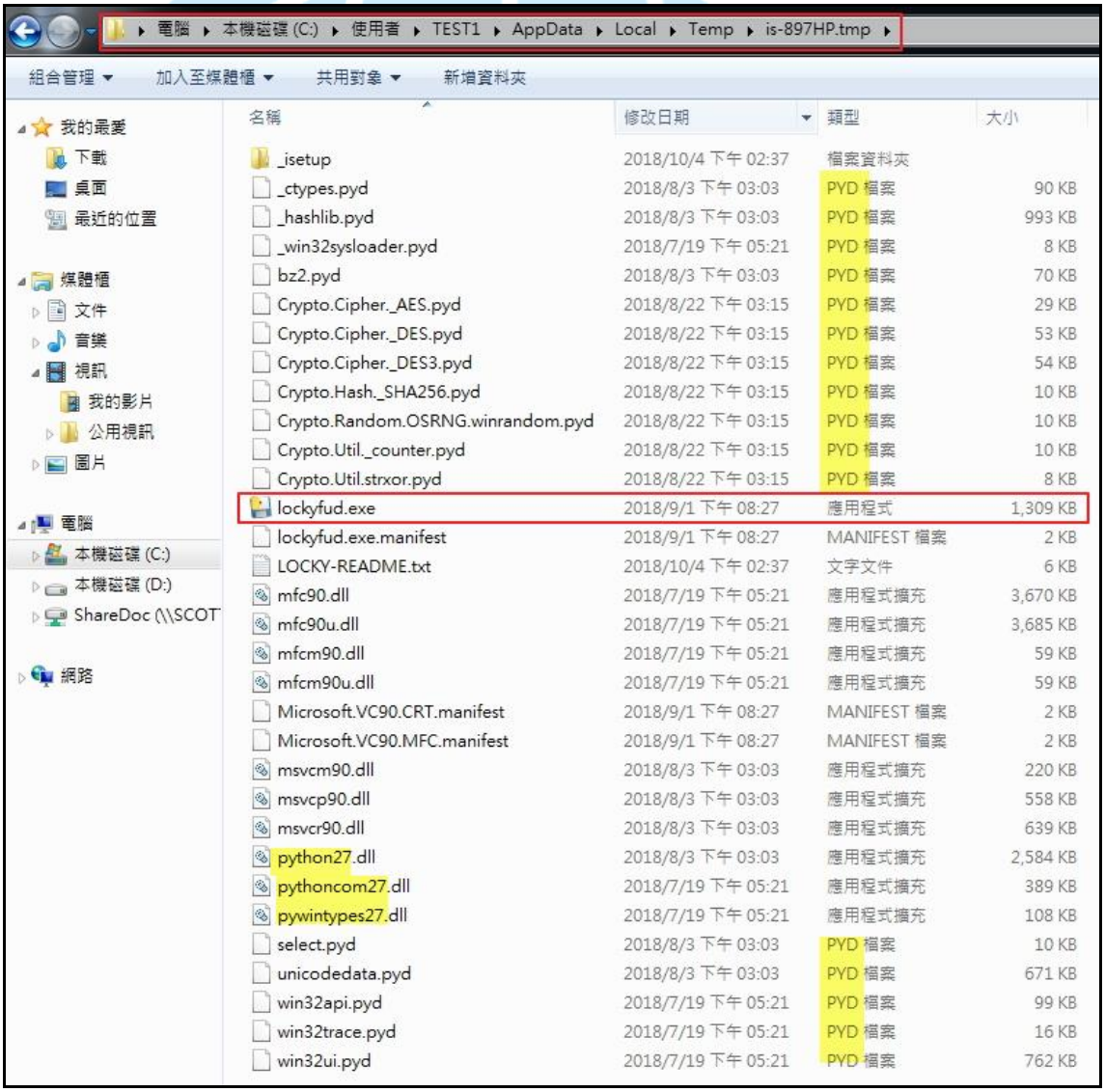
6. 測試已被加密的檔案是否可以開啟，結果發現檔案類型為文字檔者其內容變成勒索通知信的內容，而圖檔與其他檔案類型的檔案若被加密則無法開啟。


ABC - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)
Please be adviced:
All your files, pictures document and data has been encrypted with Military Grade Encryption RSA AES-256.
Your information is not lost. But Encrypted.
In order for you to restore your files you have to purchase Decrypter.
Follow this steps to restore your files.
1* Download the Tor Browser. (Just type in google "Download Tor").
2* Browse to URL : http://pylockyrkumqih5l.onion/index.php
3* Purchase the Decryptor to restore your files.
It is very simple. If you don't believe that we can restore your files, then you can restore 1 file of image format for free.
Be aware the time is ticking. Price will be doubled every 96 hours so use it wisely.
Your unique ID : 8V7EV166AXMKL31V
CAUTION:
Please do not try to modify or delete any encrypted file as it will be hard to restore it.
SUPPORT:
You can contact support to help decrypt your files for you.
Click on support at http://pylockyrkumqih5l.onion/index.php
--------BEGIN BIT KEY---------
ZM65u7kuF9aPevA2H9hM0RJ/Ej71d0ECf15cqgDwkYnzZL/oQOyjR9JVKYbt41Z2Uv+pgNNXeWxC JVKfr6zvzfoMWp1EdftLyCo951V42jxJvr/zy/XVeVL1baPVYibM
--------END BIT KEY-----------

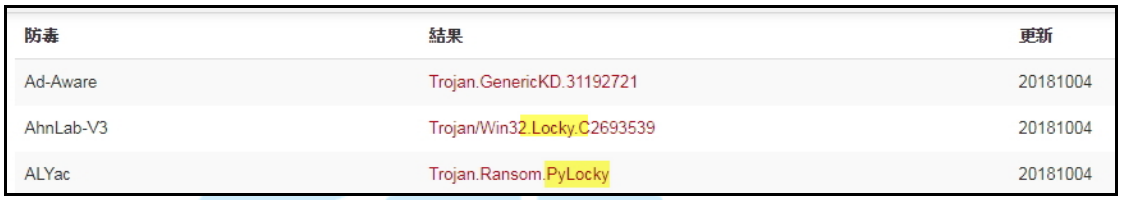

Doc1 - WordPad
首頁 檢視
貼上 剪下 複製
新細明體 11
圖片 小畫家繪圖 日期和時間 插入物件
尋找 取代 全選
剪貼簿 字型 段落 插入 編輯
Please be adviced:
All your files, pictures document and data has been encrypted with Military Grade Encryption RSA AES-256.
Your information is not lost. But Encrypted.
In order for you to restore your files you have to purchase Decrypter.
Follow this steps to restore your files.
1* Download the Tor Browser. (Just type in google "Download Tor").
2* Browse to URL : http://pylockyrkumqih5l.onion/index.php
3* Purchase the Decryptor to restore your files.
It is very simple. If you don't believe that we can restore your files, then you can restore 1 file of image format for free.
Be aware the time is ticking. Price will be doubled every 96 hours so use it wisely.
Your unique ID : 8V7EV166AXMKL31V
CAUTION:
Please do not try to modify or delete any encrypted file as it will be hard to restore it.
SUPPORT:
You can contact support to help decrypt your files for you.
Click on support at http://pylockyrkumqih5l.onion/index.php
--------BEGIN BIT KEY---------
ZM65u7kuF9aPevA2H9hM0RJ/Ej7ld0ECf15cqgDwkYnzZL/oQOyjR9JVKYbt41Z2Uv+pgNNXeWxC
JVKfr6zvzfoMWp1EdftLyCo951V42jxJvr/zy/XVeVL1baPVYibMcw/n6xkUNpQo1gXpP+LoaRoO
P1XnGdrlzp26U36vpwTJy/cKrihKeC1COD8qcWvSX1Y1FYYy3RtZy7BILANdmJMN5/HynQiLLdi5
GeTLgGKSliHPPrayBag4FC2FoAFyMLgjrcrGmlcYr/h33g0ssXQwgQjO6e+GwSeMeUm+kTcNZvpc
100%



7. 檢視 lockyfud.exe 所在之資料夾內容，發現 is-897HP.tmp 的資料夾為 Python 執行檔案的資料夾，推測 Lockyfud.exe 使用 Python 程式語言撰寫。



8. 程式 Pylocky.exe 經 VirusTotal 檢測，其惡意比例為 42/68，比例不高，仍有許多防毒軟體公司的防毒軟體無法檢測出它，該病毒被防毒軟體公司稱為 Pylocky 或 locky，但是該病毒卻與 locky 勒索病毒家族無關。



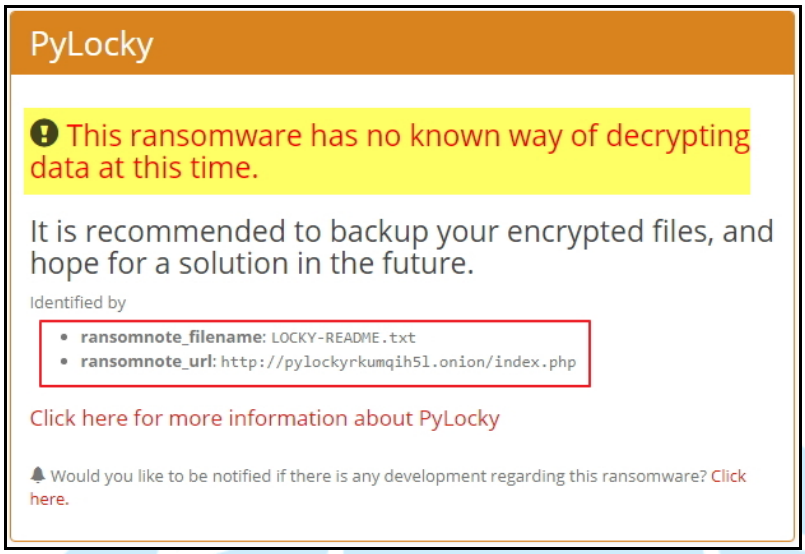
防毒	結果	更新
Ad-Aware	Trojan.GenericKD.31192721	20181004
AhnLab-V3	Trojan/Win32.Locky.C2693539	20181004
ALYac	Trojan.Ransom.PyLocky	20181004

TrendMicro	Ransom_PyLocky.B	20181004
TrendMicro-HouseCall	Ransom_PyLocky.B	20181004
VBA32	TrojanRansom.Encoder	20181003
ViRobot	Trojan.Win32.Z.Locky.5524987	20181004

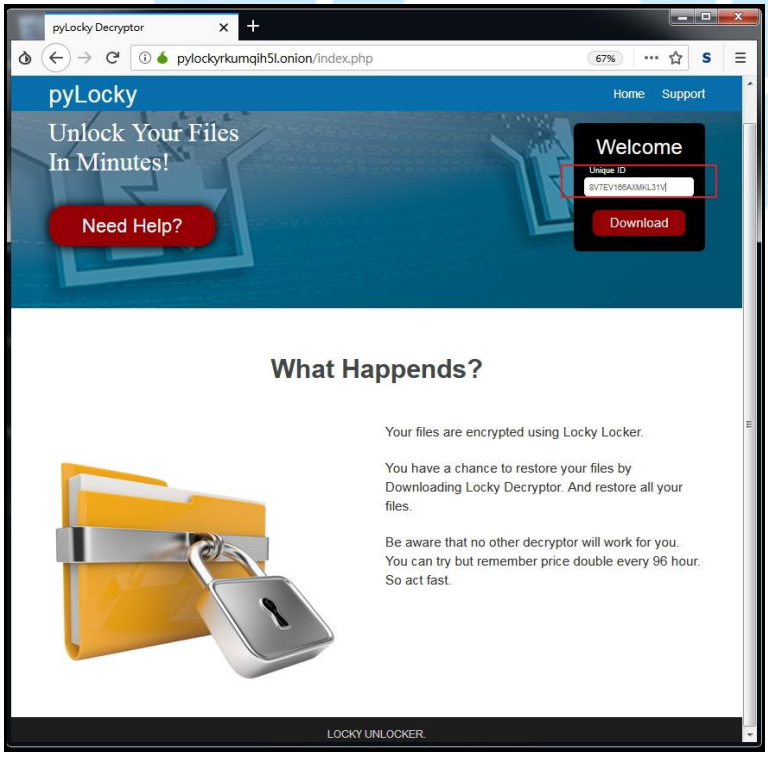
9. 程式 lockyfud.exe 經 VirusTotal 檢測，得知其惡意比例為 37/68，比例低，可見有許多防毒軟體公司的防毒軟體無法檢測出它。

防毒	結果	更新
Ad-Aware	Trojan.GenericKD.31192392	20181004
AhnLab-V3	Trojan/Win32.FileCoder.C2693626	20181004
ALYac	Trojan.GenericKD.31192392	20181004
Arcabit	Trojan.Generic.D1DBF548	20181004
Avast	Win32:Malware-gen	20181004
AVG	Win32:Malware-gen	20181004
Avira (no cloud)	TR/FileCoder.inpfo	20181004
AVware	Trojan.Win32.Generic!BT	20180925
BitDefender	Trojan.GenericKD.31192392	20181004
CAT-QuickHeal	Ransom.Locky.S3759392	20181001
CrowdStrike Falcon (ML)	malicious_confidence_100% (W)	20180723
Cylance	Unsafe	20181004
Cyren	W32/Trojan.ZYEX-5724	20181004
Emsisoft	Trojan.GenericKD.31192392 (B)	20181004
ESET-NOD32	Python/Filecoder.Locky.B	20181004
F-Secure	Trojan.GenericKD.31192392	20181004
Fortinet	Python/Filecoder_Locky.B!tr	20181004
GData	Trojan.GenericKD.31192392	20181004
Ikarus	Trojan-Ransom.Locky	20181003
Sophos ML	heuristic	20180717
K7AntiVirus	Trojan (0053a2de1)	20181003
K7GW	Trojan (0053a2de1)	20181003
Malwarebytes	Ransom.FileCryptor	20181004
McAfee	Artemis!D494FFDCE960	20181004
McAfee-GW-Edition	BehavesLike.Win32.Locky.tc	20181004
Microsoft	Trojan:Win32/Occamy.B	20181004
eScan	Trojan.GenericKD.31192392	20181004
Palo Alto Networks (Known Signatures)	generic.ml	20181004
Panda	Trj/Genetic.gen	20181003
Qihoo-360	Win32/Trojan.daf	20181004
Sophos AV	Mal/Generic-S	20181004
Symantec	Trojan.Gen.2	20181004
Tencent	Win32.Trojan.Generic.Wrge	20181004
TheHacker	Trojan/Spy.KeyLogger.au	20181001
TrendMicro	Ransom.Python.LOCKY.SM	20181004
TrendMicro-HouseCall	Ransom.Python.LOCKY.SM	20181004
VIPRE	Trojan.Win32.Generic!BT	20181004

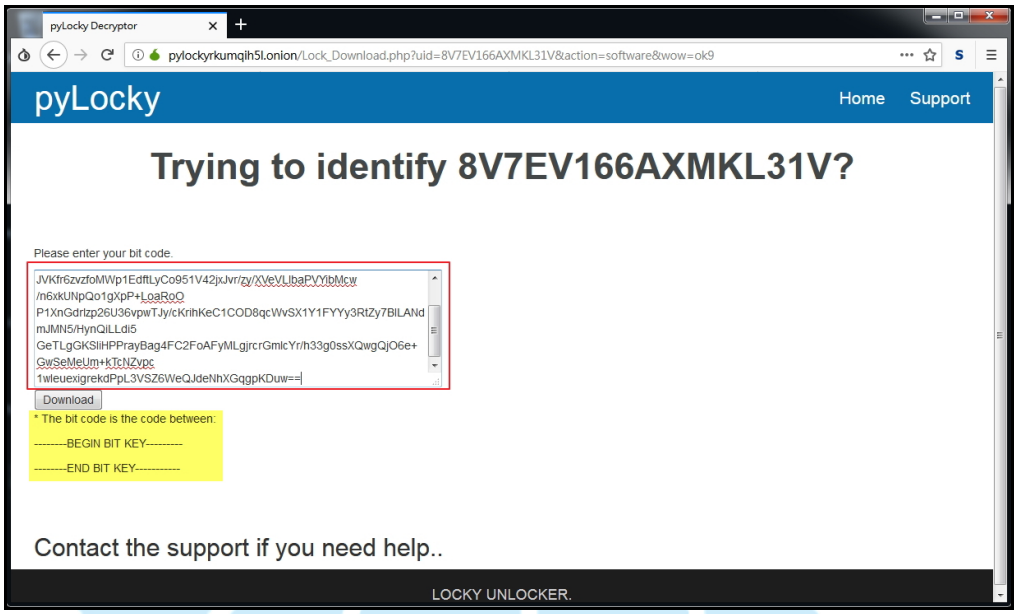
10. 將 LOCKY-README.txt 與受害主機內一個被加密圖檔上傳至 ID Ransomware 勒索病毒辨別網站 (https://id-ransomware.malwarehunterteam.com)，經檢測判定它為 Pylocky 勒索病毒，也得知該病毒目前沒有任何可解開被加密檔案的方式。



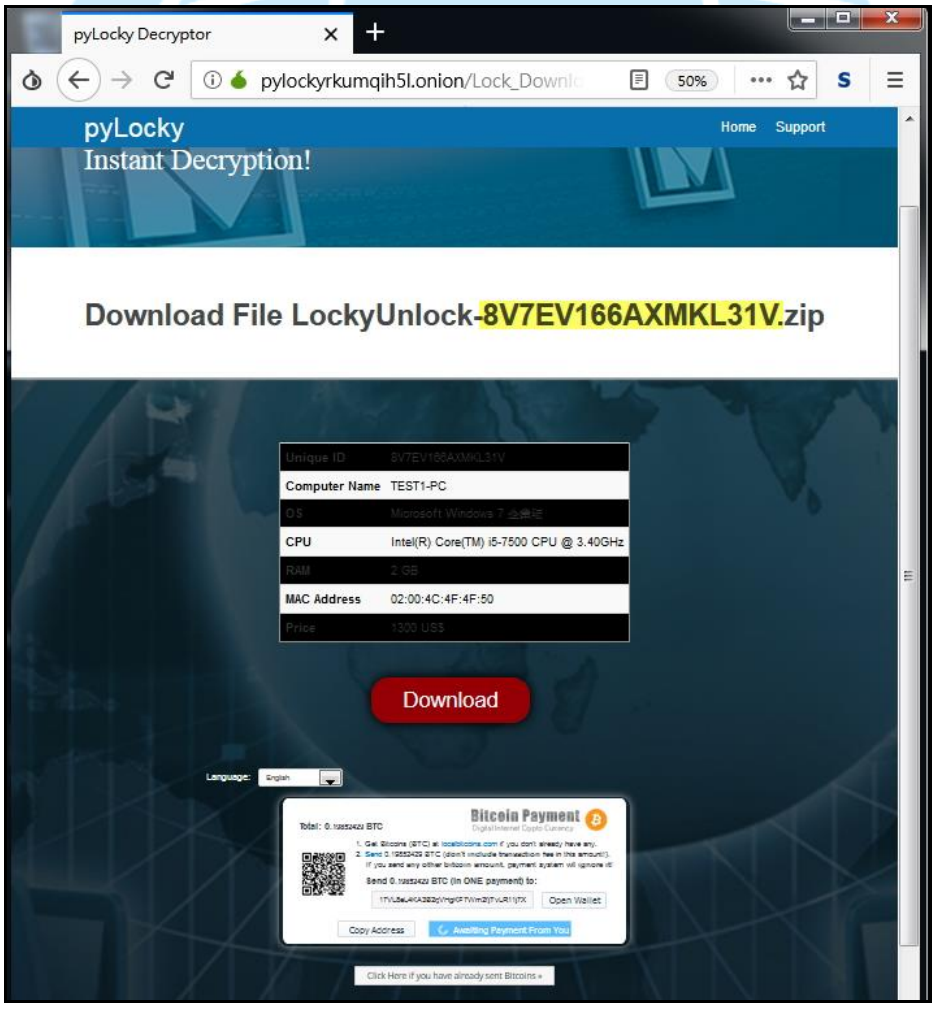
11. 安裝 Tor Browser 軟體後連至駭客所提供的網址，在網頁上明確告訴受害者該病毒名稱為 Pylocky，下載解密器需受害者輸入勒索通知信內所提供的個人 ID，也告訴受害者需要在 96 小時內支付贖金，否則贖金金額會加倍。



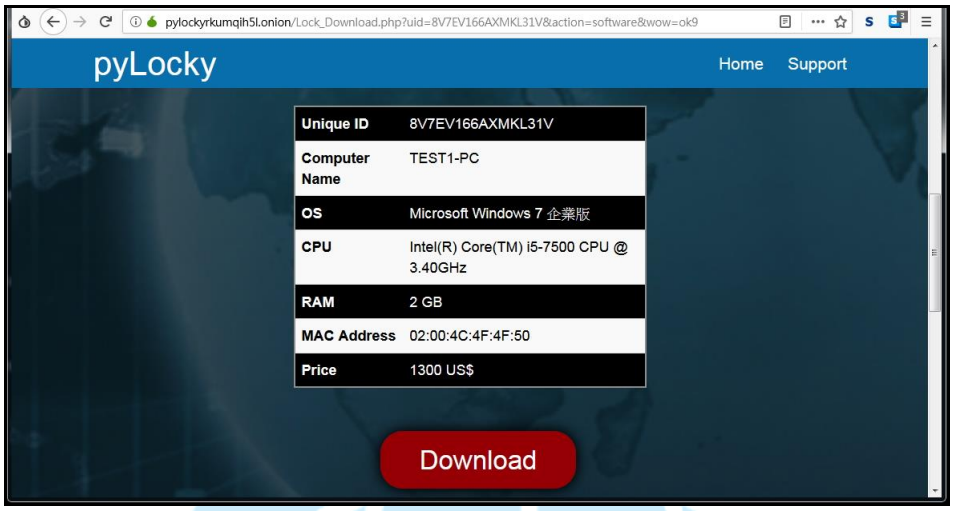
12. 在輸入受害者個人 ID 並點選 Download 後，出現識別受害者 ID 的認證頁面，要求受害者輸入 BIT KEY 的內容。



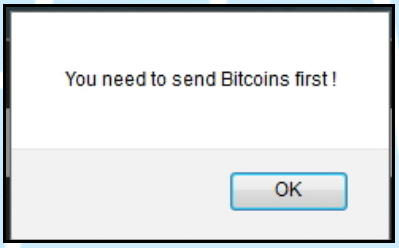
13. 將 BIT KEY 輸入並點選 Download 後，出現告知如何支付贖金的頁面。



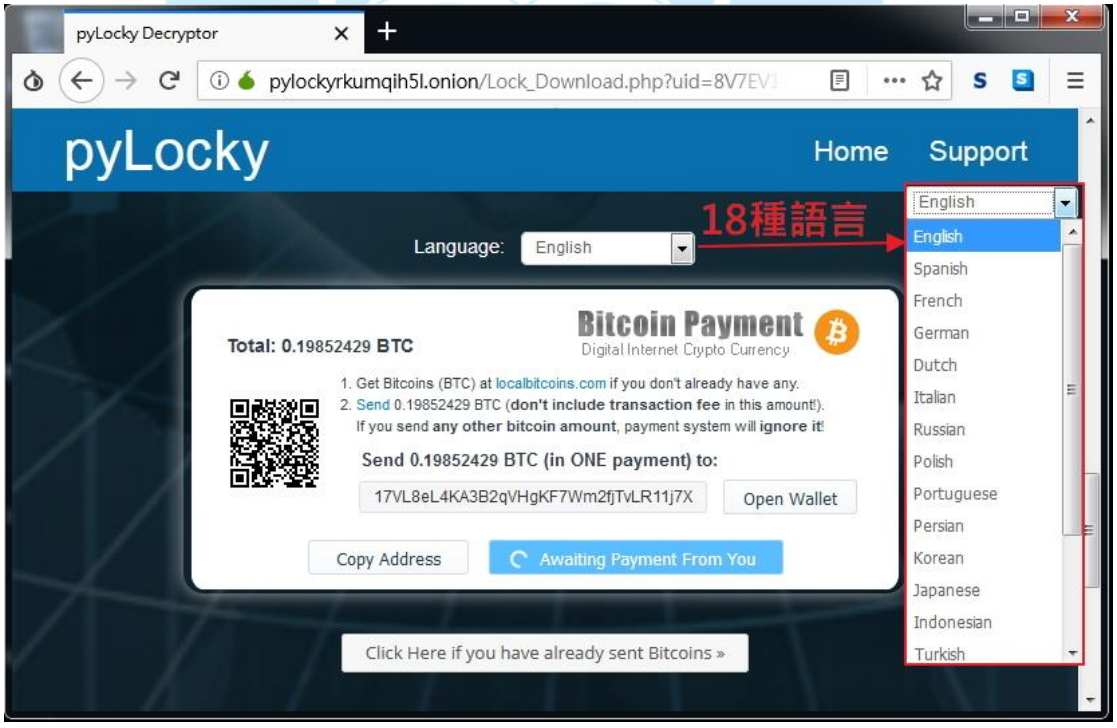
在支付贖金的頁面中，詳細記載受害主機的電腦名稱、作業系統、CPU、RAM 與 MAC 位置等資訊，也告訴受害者需要支付 1,300 元美金來購買解密器。



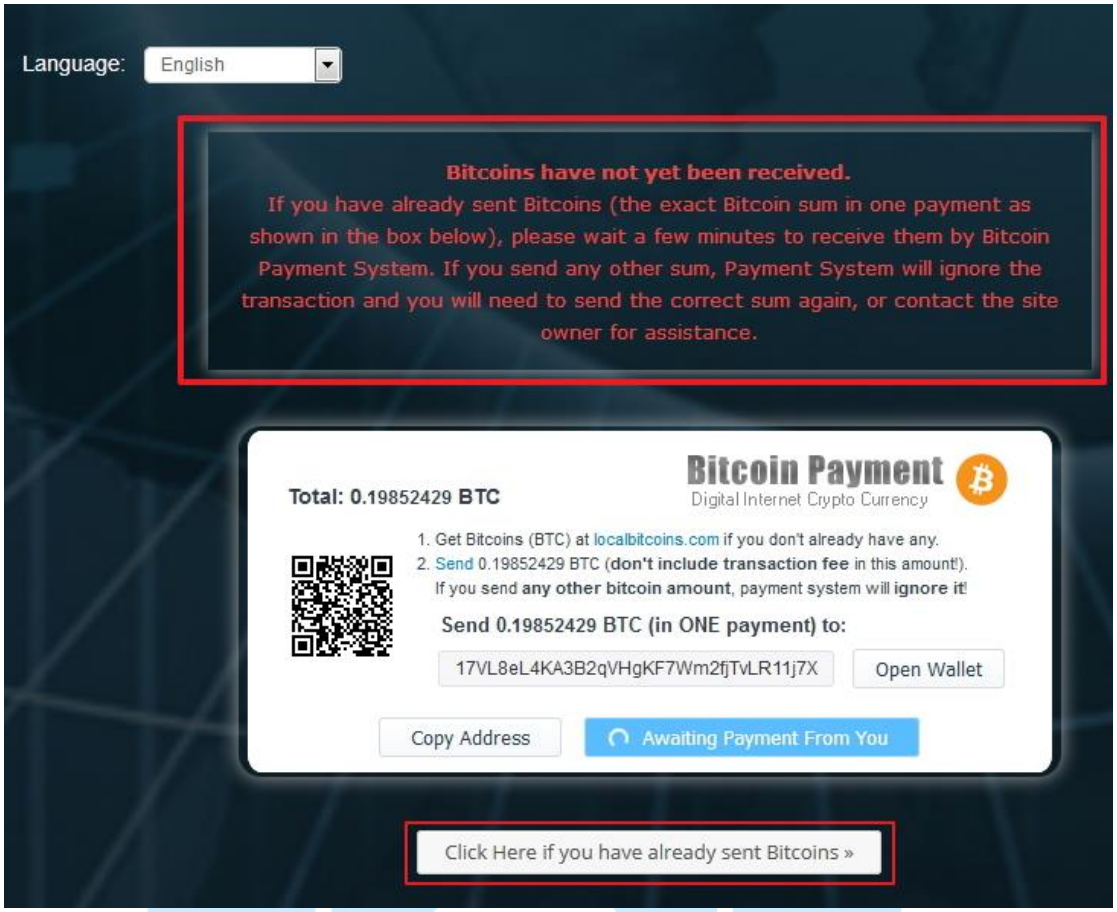
點選 Download 按鈕，出現提示受害者需先以比特幣支付贖金的視窗。



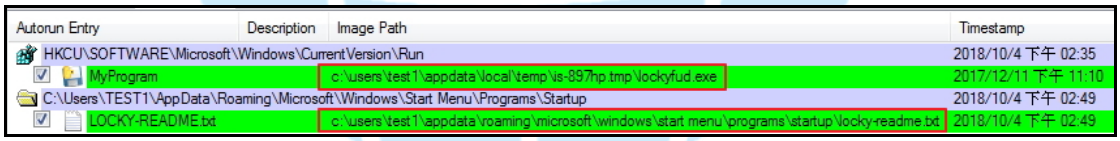
14. 查看支付贖金的內容，發現駭客準備 18 種語言版本告訴受害者如何以比特幣付款。



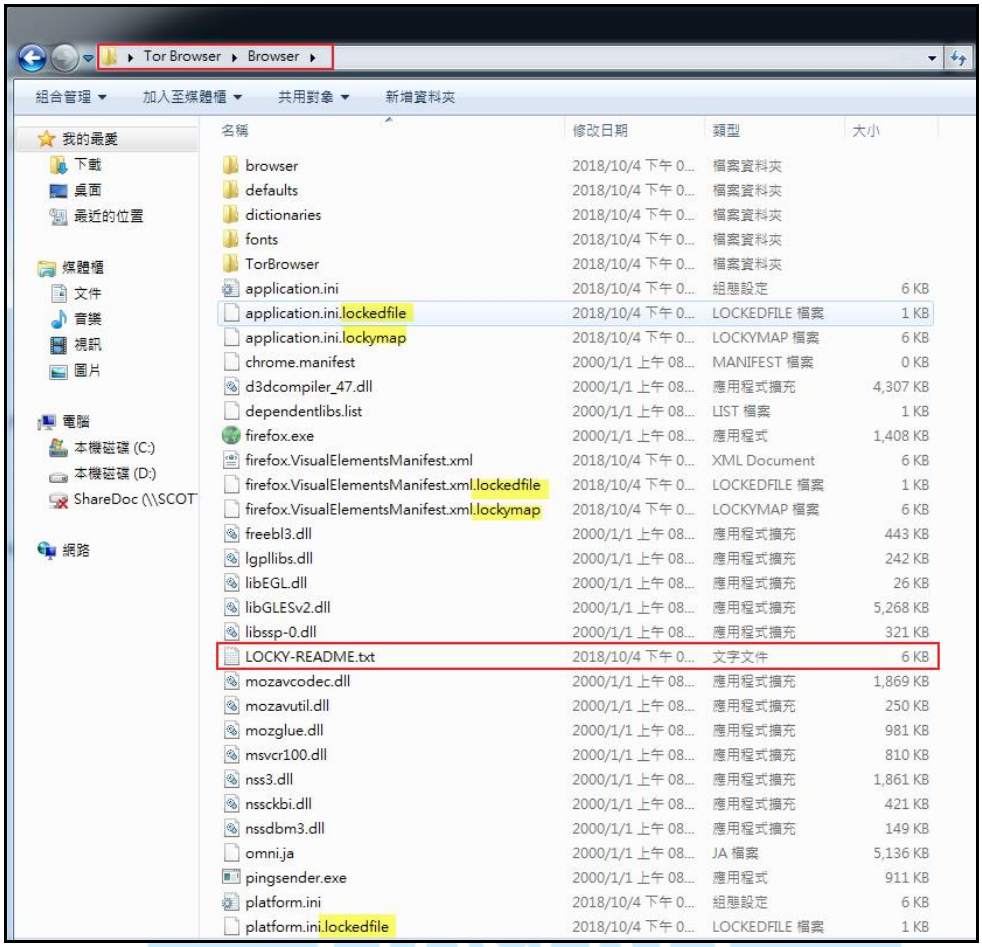
15. 在未付款的情況下，點選「Click Here if you have already sent Bitcoins」按鈕，則出現尚未收到受害者支付贖金的提示語。



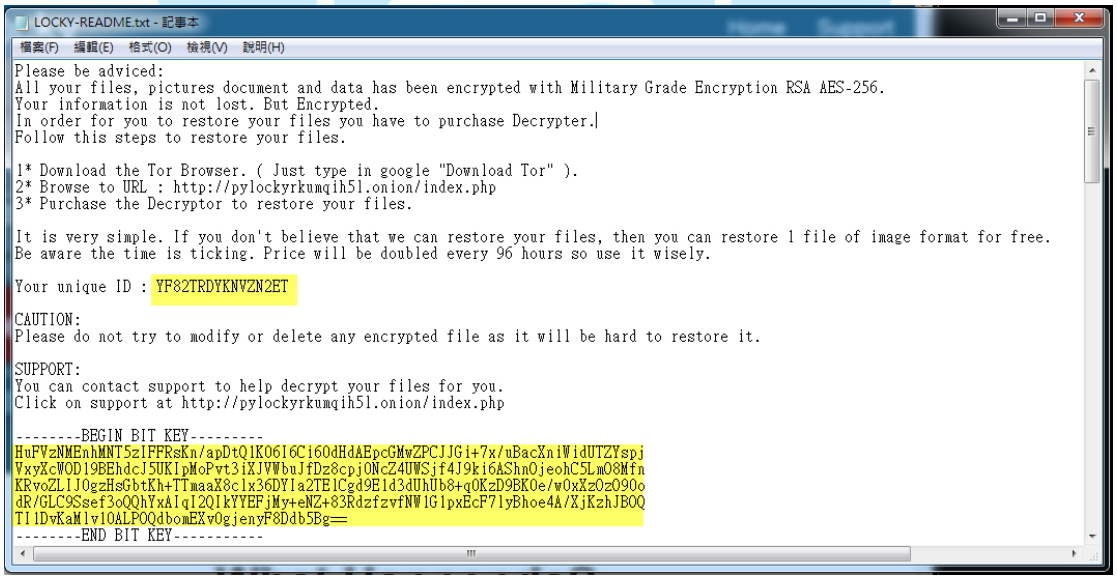
16. 檢視受害主機重新開機後程式執行情形，發現 lokcyfud.exe 與 locky-readme.txt 在每次重新開機後會自動執行。



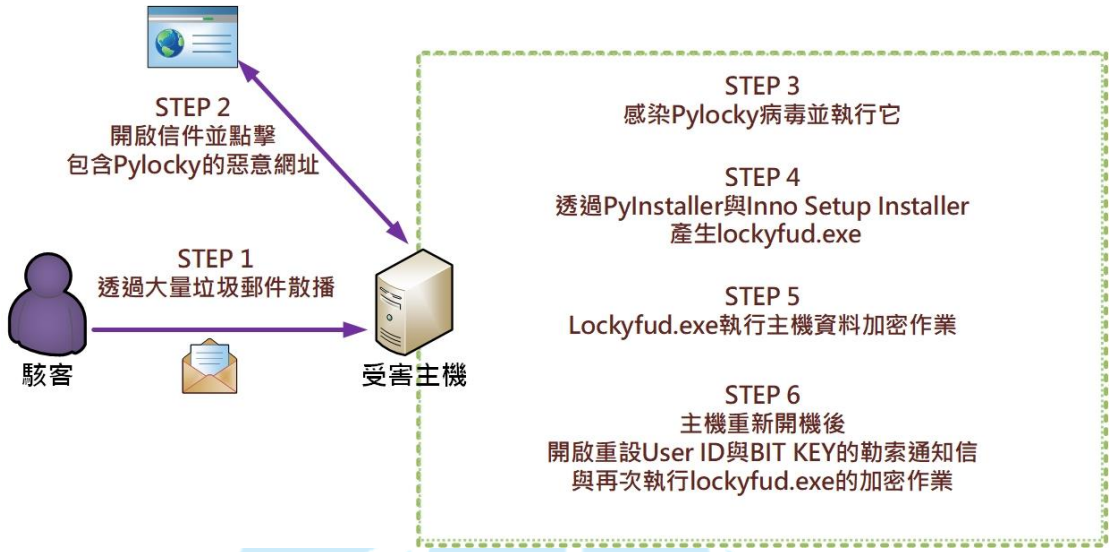
17. 將受害主機重新開機後，發現原本在加密完成後安裝的 Tor Browser 軟體無法開啟，原因為該軟體所用的部分檔案已被 lokcyfud.exe 加密了，在重新安裝該軟體後即解決此問題。



檢視重新開機後開啟的 LOCKY-README.txt 勒索通知信內容，發現受害者個人 ID 已被重設成一組新的 ID，而 BIT KEY 之內容也產生一組新的 KEY。



III. 網路架構圖



1.駭客利用大量垃圾郵件的方式來散播 Pylocky 病毒。

2.受害者開啟郵件，並且點擊郵件中包含 Pylocky 的惡意網址。

3.受害者瀏覽惡意網頁後，主機感染 Pylocky 病毒並執行它。

4.Pylocky 病毒執行後，透過 PyInstaller 與 Inno Setup Installer 產生 lockyfud.exe。

5.Lockyfud.exe 執行主機資料加密作業。

6.受害主機重新開機後，開啟重設 User ID 與 BIT KEY 的勒索通知信，並再次執行 lockyfud.exe 的加密作業。

IV. 建議與總結

1. 本個案之 Pylocky 病毒的攻擊行為與一般勒索病毒不同，在加密後會針對每個被加密的檔案產生兩個副檔名為「.lockedfile」與「.lockymap」檔案。
2. 該病毒使用 PyInstaller 與 Inno Setup Installer 來產生加密用的惡意程式 lockyfud.exe，而且受害主機每次重新開機後會重新執行加密作業。
3. 目前針對 Pylocky 勒索病毒沒有任何解密器，而且仍有許多防毒軟體公司無法檢測出它，建議使用者定期備份重要資料，並且不隨意開啟不明來源的信件或點選不明網址，以降低感染該病毒的風險。