個案分析-

假勒索真破壞的惡意程式

Cryptolocker 事件分析報告

TACERT 臺灣學術網路危機處理中心團隊製

2015/10

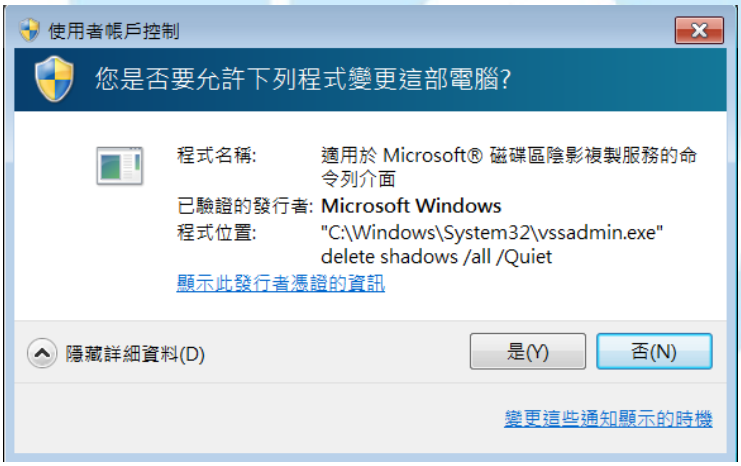
I. 事件簡介

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 Cryptolocker 的惡意勒索軟體測試。

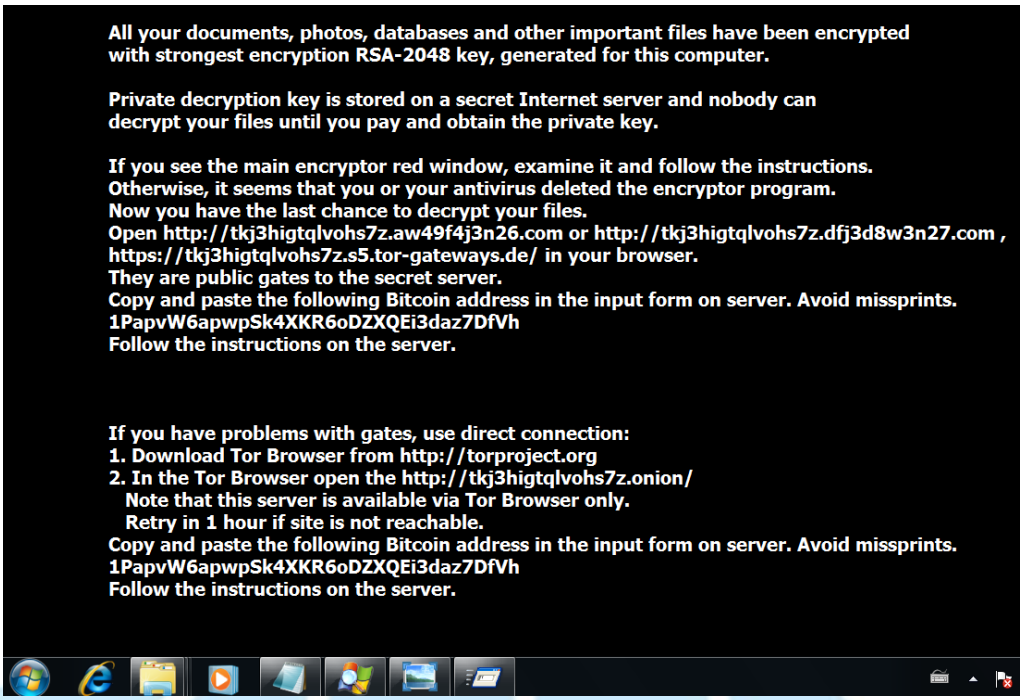
II. 事件檢測

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 128[…]d90.exe，實際執行後會先跳出權限存取的選項，此指令會刪除磁碟的快照備份，讓使用者無法還原系統。

   “vssadmin.exe delete shadows /all /Quiet”

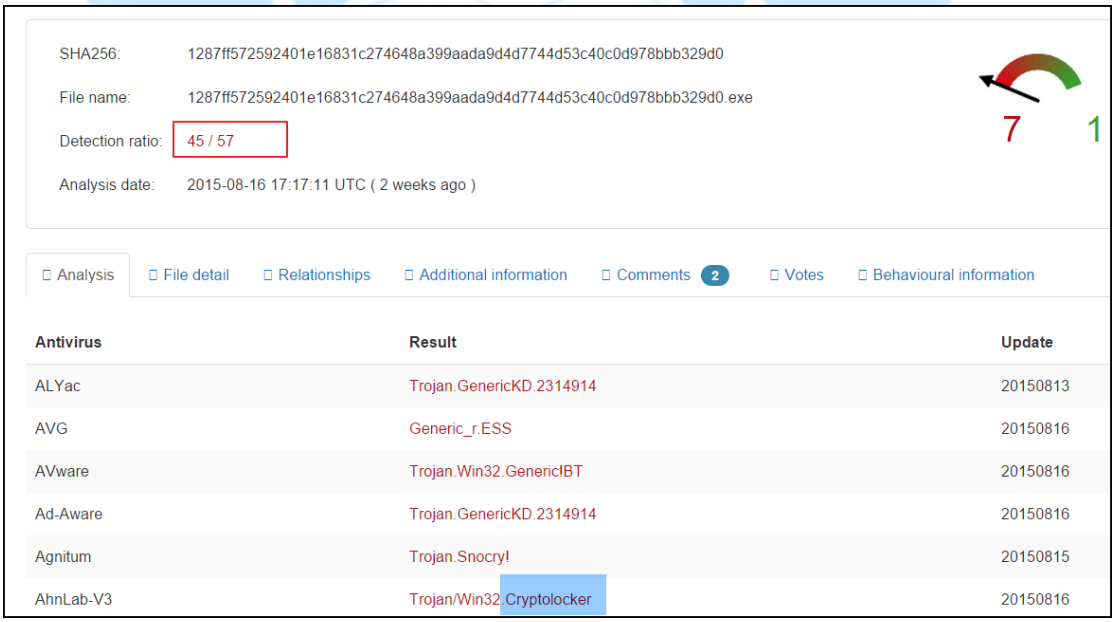


3. 原本的惡意程式會開始針對內部文件、影音、圖像檔案進行加密，然後惡意程式主體就會自我刪除。
4. 此時會顯示惡意程式執行的紅色視窗，告知使用者你的檔案已經被加密，而桌面的背景也會備置換成勒索軟體的相關訊息。



5. 惡意程式會威脅使用者必須在 96 小時內將贖金透過以下方式付款到駭客的比特幣的電子錢包中，並告知此加密是透過 RSA-2048 方式，必須用贖金來取回加密的私鑰。

6. 透過 Virustotal 線上掃毒，該病毒的檢測比例 45/57 相當高，為 Cryptolocker 系列的勒索軟體。



SHA256: 1287ff572592401e16831c274648a399aada9d4d7744d53c40c0d978bbb329d0

File name: 1287ff572592401e16831c274648a399aada9d4d7744d53c40c0d978bbb329d0.exe

Detection ratio: 45 / 57

Analysis date: 2015-08-16 17:17:11 UTC (2 weeks ago)

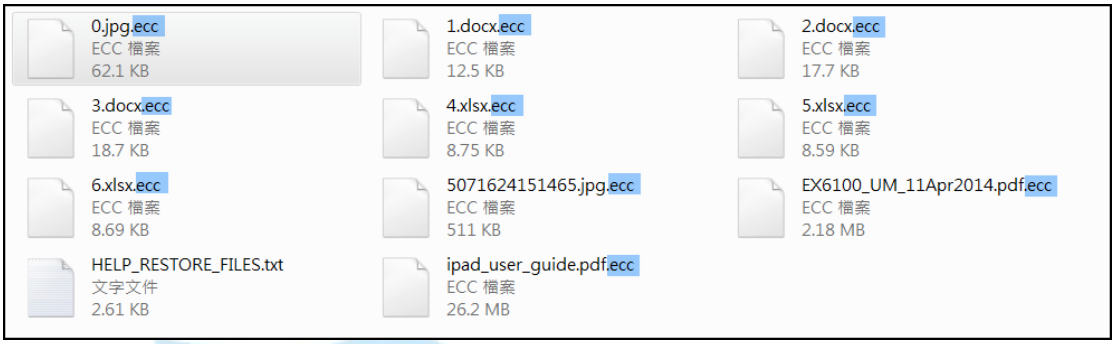
7 1

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

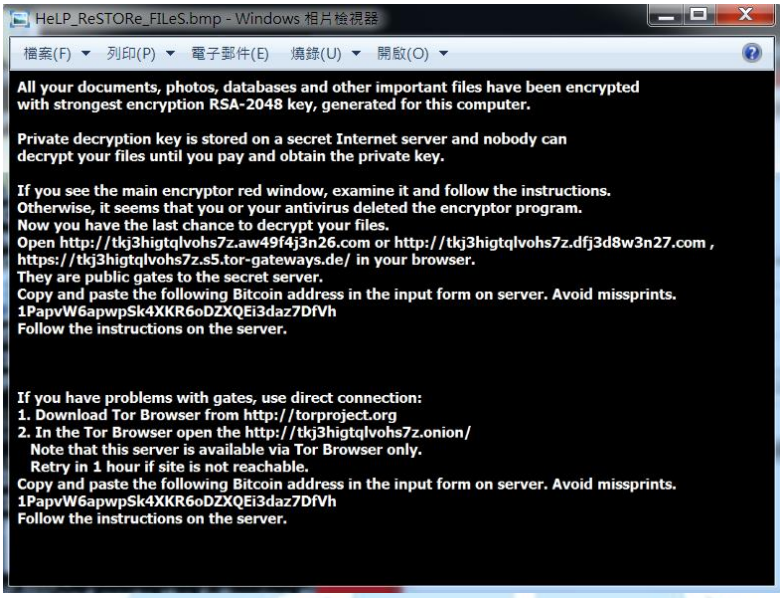
Antivirus	Result	Update
ALYac	Trojan.GenericKD.2314914	20150813
AVG	Generic_r.ESS	20150816
AVware	Trojan.Win32.GenericIBT	20150816
Ad-Aware	Trojan.GenericKD.2314914	20150816
Agnitum	Trojan.Snocry!	20150815
AhnLab-V3	Trojan/Win32.Cryptolocker	20150816

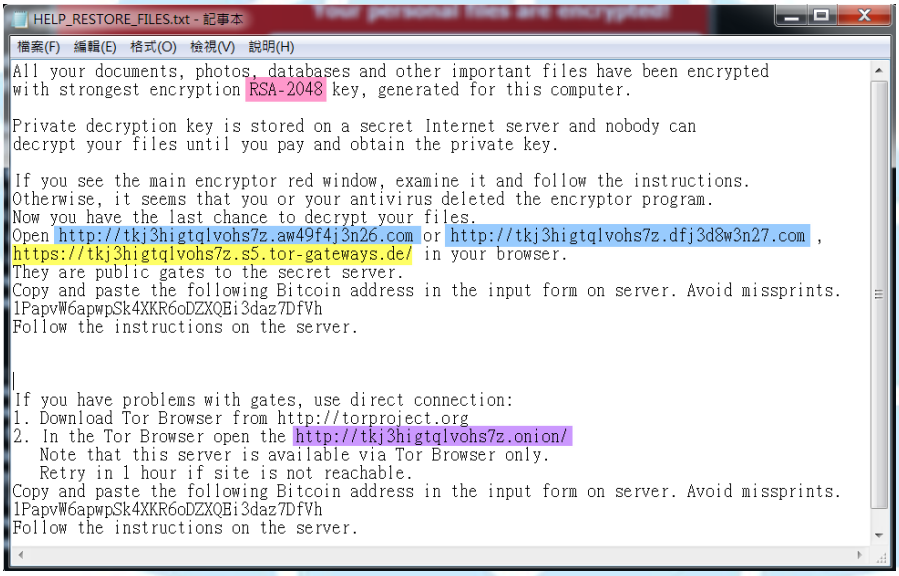
7. 測試時候將其中一個資料夾內放入一些文件檔，包含了 docx、xlsx、jpg、

pdf 四種格式檔案做測試，而惡意程式感染後所有文件檔案的附檔名都會變成 ecc 格式，導致磁碟中所有文件檔案都無法開啟。

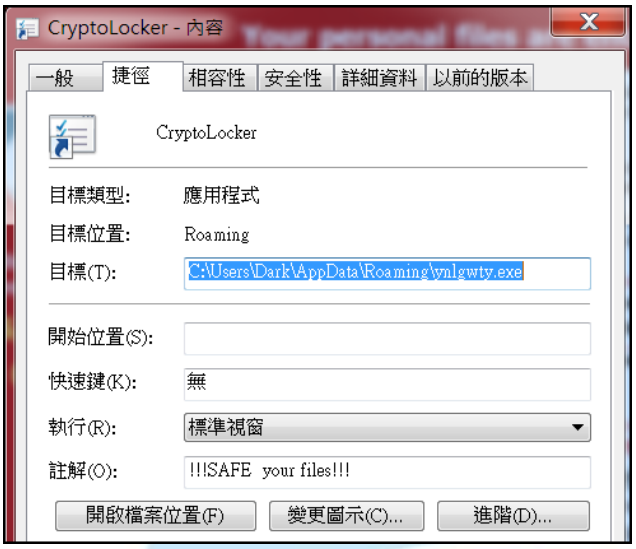


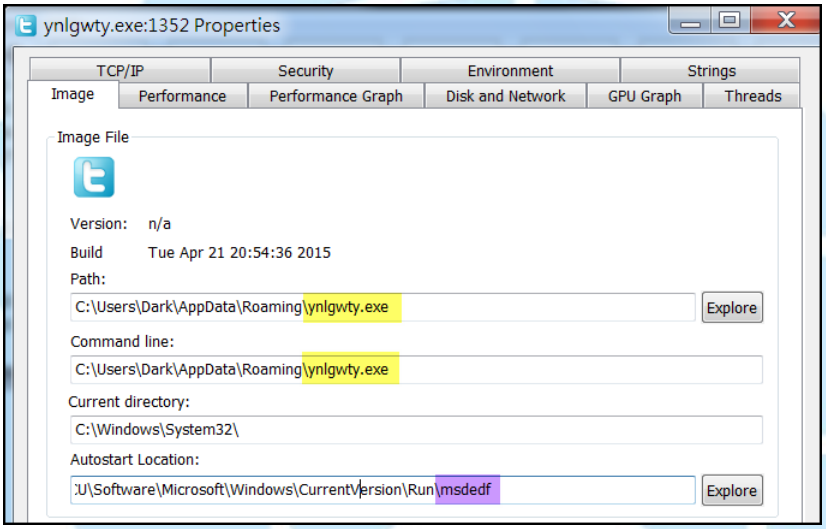
8. 當所有磁碟內部的關聯檔案都被加密後，在桌面中產生三個說明檔案，分別為「CryptoLocker.lnk、HeLP_ReSTORe_FILeS.bmp 和 HELP_RESTORE_FILES.txt」，其內容都是引導受害者如何進行繳付勒索贖金。



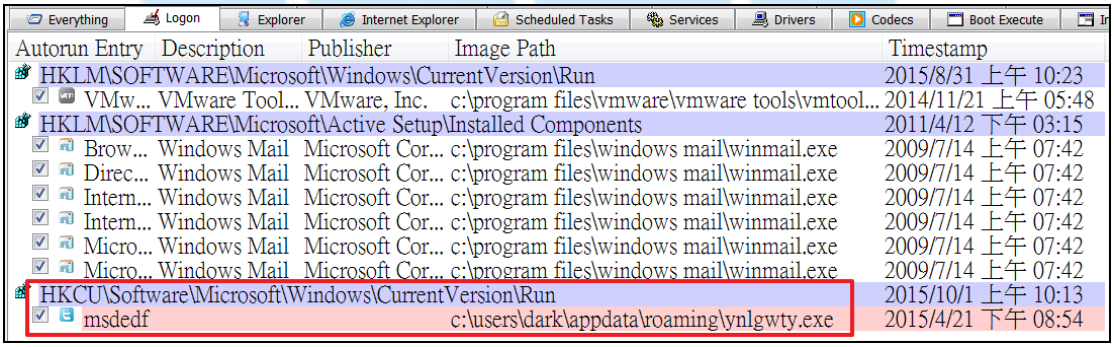


9. 惡意程式執行後會自動開啟 CryptoLocker 捷徑檔案，該惡意程式檔名為 ynlgwty.exe，此程式存於 C 槽的隱藏資料夾中「\AppData\Roaming\」，就是自動跳出的紅底黑字視窗程式。





10. 該程式同時會寫入開機自動啟用註冊檔中，程序名稱為 msdedf，檔案路徑為「\roaming\ynlgwty.exe」。



11. 開啟惡意程式 ynlgwty.exe 提供的三個贖金網站網址

「http://tkj3higtqlvohs7z.aw49f4j3n26.com、

http://tkj3higtqlvohs7z.dfj3d8w3n27.com 、

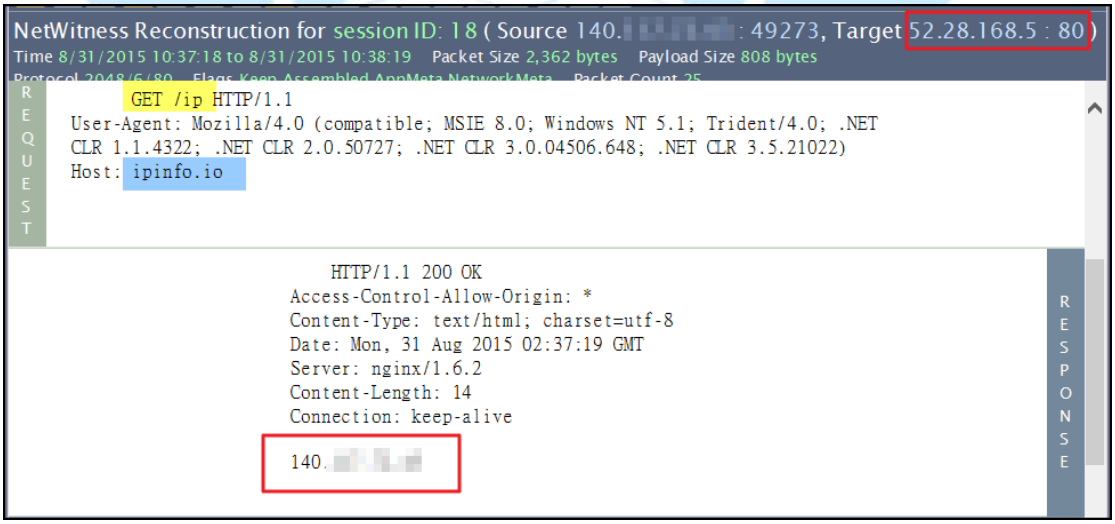
https://tkj3higtqlvohs7z.s5.tor-gateways.de/」，一般瀏覽器都無法正常開啟。

12. Tor Browser 為匿名網路瀏覽器，也就是透過該瀏覽器作為中繼代理，進而能夠連線到一般 DNS 無法解析的網站，為一種中繼網路。此例表示我們會使用 185.73.44.58 作為中繼代理，去連到匿名的贖金網站。

13. 因為前三個贖金網址都無法開啟，改用匿名網路瀏覽器 Tor Browser 開啟第四個匿名網址「http://tkj3higtqlvohs7z.onion/」，然而也無法正常顯示，判斷可能該惡意贖金網站已經被移除。

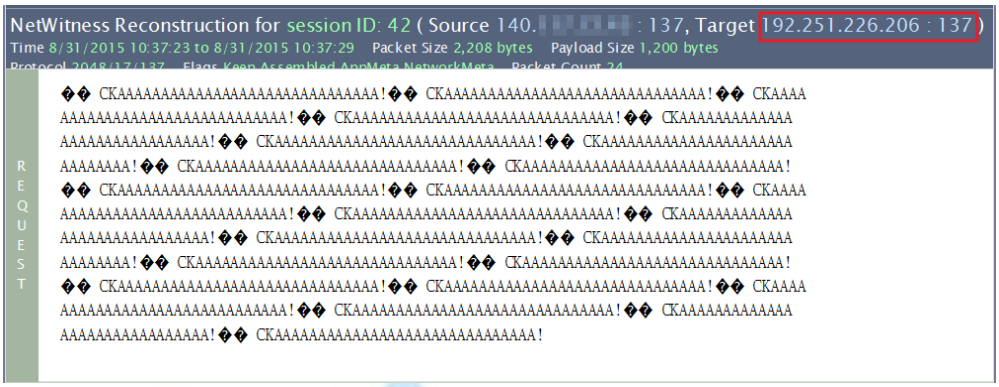
14. Tor Browser 連線的位址 185.73.44.58 為匿名中繼網路的其中一個主機，從本地端無法明確追查到惡意網址，故 Tor onion network 常用來作為犯罪匿名網路使用。

15. 從網路封包中可以看到，主機感染後惡意程式 ynlgwty.exe 一開始會連到網站「http://ipinfo.io」，IP 為美國的 52.28.168.5，該網站會回覆連線主機的 IP 資訊，可能是作為之後的報到用途。

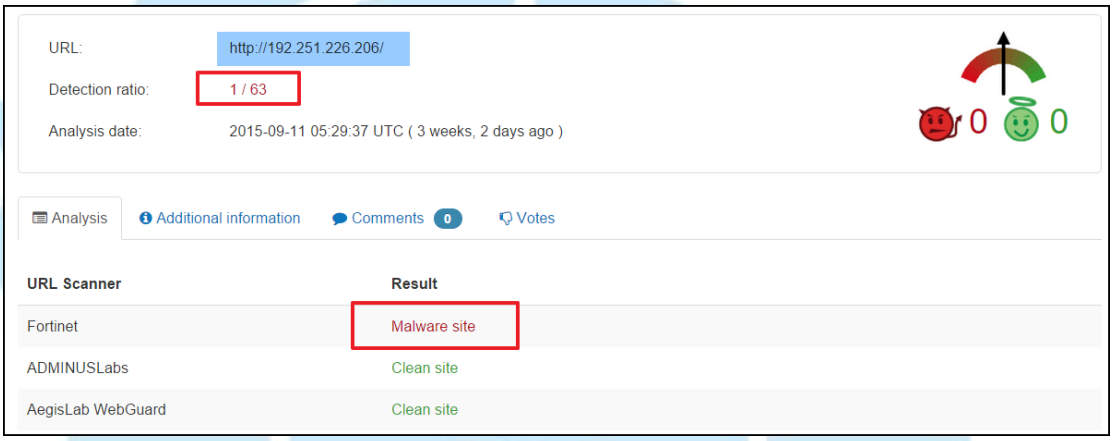


16. 當主機取得 IP 資訊後惡意程式會轉向德國的 192.251.226.206:137 發送 Netbois 協定的 UDP 封包，一般做為同網段網路芳鄰探測使用，此處研

判可能為向上層中繼站報到。



17. 透過 Virustotal 檢測此網站 192.251.226.206，發現到有一家防毒引擎偵測為惡意網址，因此懷疑可能為駭客所用。



18. 隨後惡意程式 ynlgwty.exe 會再向網址 secure2.alphassl.com 的 port 80 連線，位址為美國的 104.16.28.16，GET 取得一個名為 gsalphag2.crt 憑證公鑰，為產生惡意程式加密檔案私鑰。

NetWitness Reconstruction for session ID: 60 (Source 140.[redacted] : 49278, Target 104.16.28.16 : 80)
Time 8/31/2015 10:37:32 to 8/31/2015 10:38:20 Packet Size 10,212 bytes Payload Size 7,308 bytes

```
REQUEST
GET /cacert/gsalphag2.crt HTTP/1.1
Connection: Keep-Alive
Accept: */*
User-Agent: Microsoft-CryptoAPI/6.1
Host: secure2.alphassl.com

HTTP/1.1 200 OK
Date: Mon, 31 Aug 2015 02:37:32 GMT
Content-Type: application/x-x509-ca-cert
Content-Length: 1075
Connection: keep-alive
Set-Cookie: __cfduid=d5e52104f8defedef02b6626482a3ba9f1440988652; expires=Tue, 30
-Aug-16 02:37:32 GMT; path=/; domain=.alphassl.com; HttpOnly
Last-Modified: Sun, 22 May 2011 15:00:00 GMT
ETag: "154344e-433-4a3de9bdf1c00"
Cache-Control: public, max-age=2678400
Expires: Thu, 01 Oct 2015 02:37:32 GMT
Vary: Accept-Encoding,User-Agent
Via: 1.1 AN-0003011042473034
CF-Cache-Status: HIT
```

19. 惡意程式會向 ocsp.globalsign.com，IP 為 108.162.232.204 進行 HTTP GET 連線存取，封包中會回傳一串加密參數，應為惡意程式加密用的私鑰。

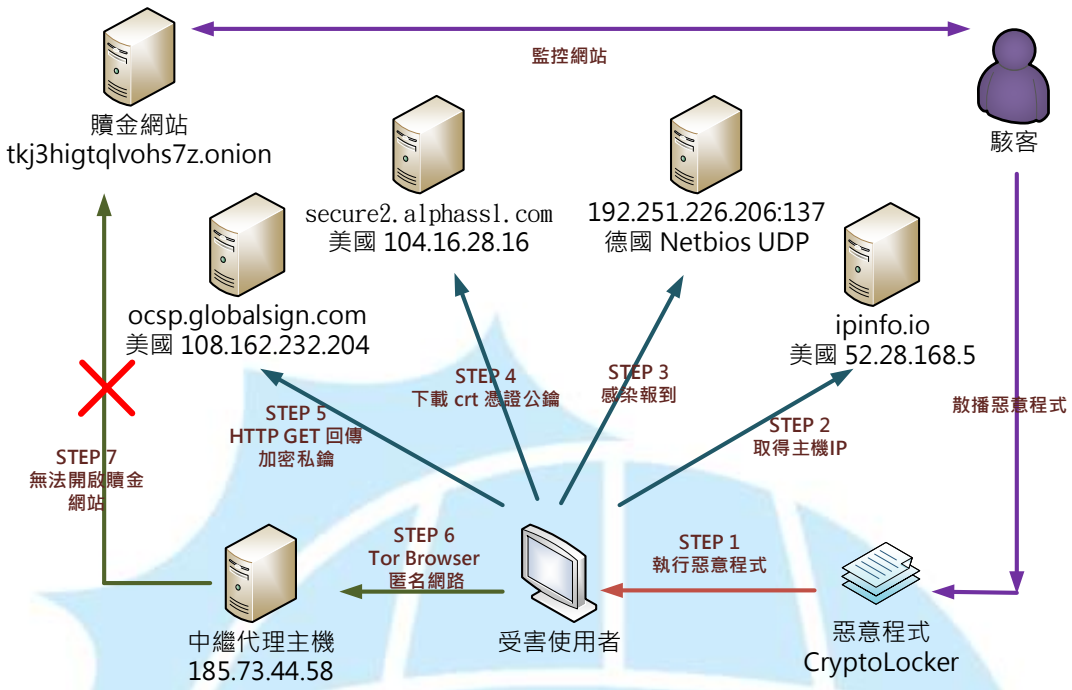
NetWitness Reconstruction for session ID: 69 (Source 140.[redacted] : 49279, Target 108.162.232.204 : 80)
Time 8/31/2015 10:37:37 to 8/31/2015 10:38:26 Packet Size 12,664 bytes Payload Size 9,288 bytes

```
REQUEST
GET /rootr1/MEwwSjBIMEYwRDAJBgUrDgMCGgUABBS3V7W2nAf4FiMTjpDJKg6%2BMgGqMQQUYHtmGkU
N18qJUC99BM00qP%2F8%2FUsCCwQAAAAAAS9O4TcC HTTP/1.1
Connection: Keep-Alive
Accept: */*
User-Agent: Microsoft-CryptoAPI/6.1
Host: ocsp.globalsign.com

HTTP/1.1 200 OK
Date: Mon, 31 Aug 2015 02:37:38 GMT
Content-Type: application/ocsp-response
Content-Length: 1518
Connection: keep-alive
Set-Cookie: __cfduid=dd434c48ff08a1fc0ef25a03b6529ccec1440988658; expires=Tue, 30
-Aug-16 02:37:38 GMT; path=/; domain=.globalsign.com; HttpOnly
Last-Modified: Sun, 30 Aug 2015 22:26:59 GMT
Expires: Thu, 03 Sep 2015 22:26:59 GMT
ETag: "28c3351c69528023771e94f60cbf0381426d9363"
Cache-Control: max-age=10800,public,no-transform,must-revalidate
CF-Cache-Status: HIT
Server: cloudflare-nginx
CF-RAY: 21e55ac8fb0c0ba5-HKG
```

20. 主機感染後無法透過 Tor 匿名網路開啟贖金網站，可能贖金網站已經被相關單位撤除，換言之一旦感染此惡意程式無法還原資料。

III. 網路架構圖



1. 使用者可能透過瀏覽器或系統漏洞誤執行到惡意程式 Cryptolocker。
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 192.251.226.206 發送 netbios 協定封包進行報到。
4. 惡意程式向 secure2.aplpassl.com 下載 crt 憑證公鑰。。
5. 惡意程式向 ocsp.globalsign.com HTTP GET 回傳加密私鑰。
6. 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。
7. 無法開啟贖金網站，可能該網站已經被相關單位撤除。
8. 駭客能持續監控贖金網站以及散播惡意程式。

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. 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. 惡意程式隨後會更改系統桌面以及跳出程式紅底畫面，引導受害者如何去支付贖金來取得解密私鑰。
5. CrytoLokcer 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. 理論上感染惡意程式後可以透過 Tor Browser 開啟匿名贖金網站，然而此例測試發現無法開啟，應該是贖金網站已經被撤除，故若使用者感染此惡意程式則無法取得私鑰還原。
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 Cryptolocker 勒索程式。