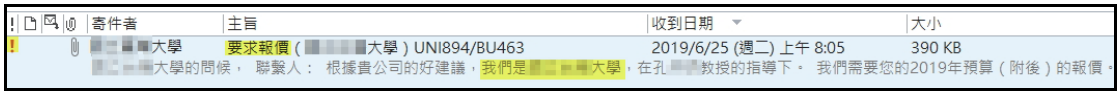
網路釣魚攻擊事件分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

2019 年 7 月

一、事件簡介

1. 2019/6/25 本中心收到一封來自某知名大學的信件，主旨為「要求報價(XX 大學)UNI894/BU463」，為了解該信件之攻擊行為與對收件者之危害程度，本中心進行信件檢測。



二、事件檢測

1. 首先，查看信件內容，信件內容提到這是來自某大學的問候，在某教授的指導下，請收件者在 2019 年 6 月 27 日當天或之前提供 2019 年預算的報價。在信件中有一個名為「要求報價 25-06-2019-pdf」的 zip 壓縮檔，該信件是以國內某知名大學的名義發出，若收件者為其常聯絡的廠商或其他業界公司，則收信者會點開此信件並開啟附件的可能性將大大增加。

2. 使用微軟的 Message Header Analyzer 分析信件的網際網路標題，從 Received headers 發現該信件由 cvps10523477067.hostwindsdns.com(美國 IP:104.168.171.157)所寄出，非來自寄件者所在地台灣(.tw)，表示寄件者名稱

是偽造的。

Summary

Subject	要求報價（[redacted]大學）UNI894/BU463
Message Id	<7f8b935baa66618911d956af5439fe95@[redacted].edu.tw>
Creation time	2019/6/25 上午8:20:45 (Delivered after -15 minutes 44 seconds)
From	[redacted]大學 <admin@[redacted].edu.tw>
To	undisclosed-recipients:;

Received headers

Hop↓	Submitting host	Receiving host	Time	Delay	Type ⇒
1	[::1] (port=55774 helo=cvps10523477067)	cvps10523477067.hostwindsdns.com	2019/6/25 上午 8:20:45		esmtpa (Exim 4.92) (envelope-from <admin@[redacted].edu.tw>)
2	cvps10523477067.hostwindsdns.com (cvps10523477067.hostwindsdns.com [104.168.171.157])	cert.tanet.edu.tw (Postfix)	2019/6/25 上午 8:05:01	-15 minutes 44 seconds	ESMTP

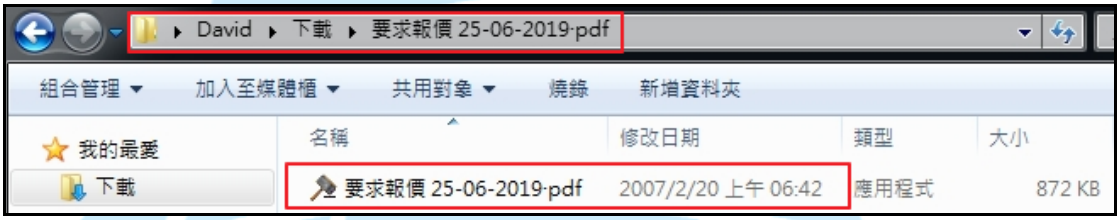
在其他 Header 資訊方面，發現若收信者回信則會回覆至 41e7e96794e44c007edebc97801881aa@batono.ge 的信箱，而該信箱為 References 的五個參考信箱之一，而從 References 發現這些信箱都是來自俄羅斯(ru)與喬治亞(ge)。本信件的 Message-ID 為 7f8b935baa66618911d956af5439fe95@某知名大學英文縮寫.edu.tw，偽裝為某知名大學所發出的信件，而且該信件的重要性設定為最優先，吸引收信者開啟信件。

Other headers

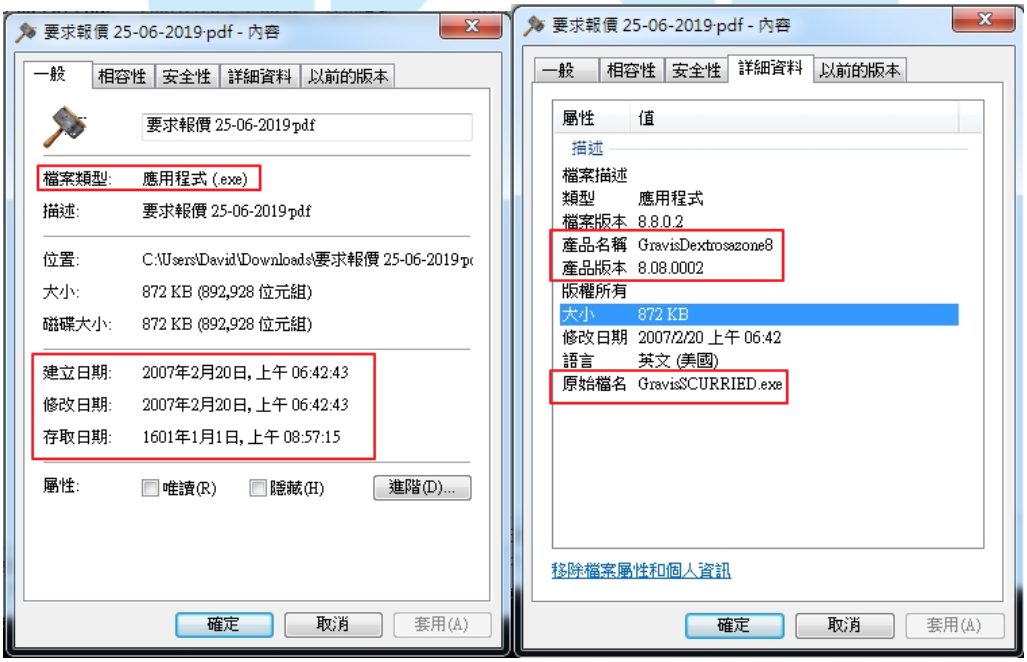
#↓	Header	Value
1	Return-Path	<admin@[redacted]edu.tw>
2	X-Original-To	s[redacted]e@cert.tanet.edu.tw
3	Delivered-To	s[redacted]e@cert.tanet.edu.tw
4	MIME-Version	1.0
5	Content-Type	multipart/mixed; boundary="=_a0a58c8905f5d0845a9a8b3258c5bacf"
6	Date	Mon, 24 Jun 2019 20:20:45 -0400
7	From	[redacted]大學 <admin@[redacted].edu.tw>
8	To	undisclosed-recipients:;
9	Subject	要求報價（[redacted]大學）UNI894/BU463
10	In-Reply-To	<41e7a96794e44c007edebc97801881aa@batono.ge>
11	References	<0dd2ac54edc611e2d42e3c510c9d076c@s176113.smrtp.ru> <94280fc94c72fb70b8fd165a5e35aa3b@batono.ge> <12841884c01f6ef1c7e4187eb2079266@s185648.smrtp.ru> <a10f8c4b4b74c08e9551315f716ba442@batono.ge> <41e7a96794e44c007edebc97801881aa@batono.ge>
12	X-Priority	1 (Highest)
13	Message-ID	<7f8b935baa66618911d956af5439fe95@[redacted].edu.tw>

14	X-Sender	admin@ .edu.tw
15	User-Agent	Roundcube Webmail/1.3.8
16	X-AntiAbuse	This header was added to track abuse, please include it with any abuse report
17	X-AntiAbuse	Primary Hostname - cvps10523477067.hostwindsdns.com
18	X-AntiAbuse	Original Domain - cert.tanet.edu.tw
19	X-AntiAbuse	Originator/Caller UID/GID - [47 12] / [47 12]
20	X-AntiAbuse	Sender Address Domain - .edu.tw

3. 將信件的附件「要求報價 25-06-2019.pdf.zip」解壓縮，發現解壓縮後原以為是 pdf 檔的檔案變成執行檔，若檢視時未設定視窗秀出副檔名，則使用者會以為是 pdf 檔而開啟它，這是一個常見的引誘使用者上當的小技巧。



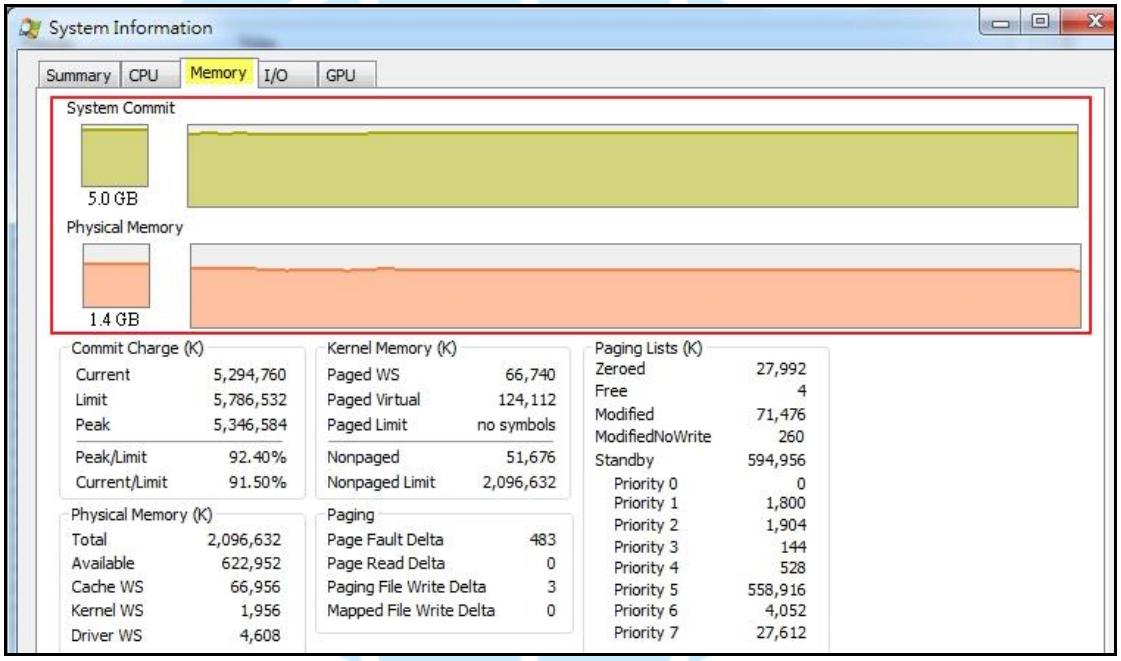
檢視該執行檔的檔案內容，發現該檔案是在 2007/2/20 6:42 建立的，但是存取日期卻是 1601/1/1 8:57，推測這些時間可能不是準確的，而在詳細資料內則寫明產品名稱為 GravisDextrosazone8，原始檔名為 GravisSCURRIED.exe。



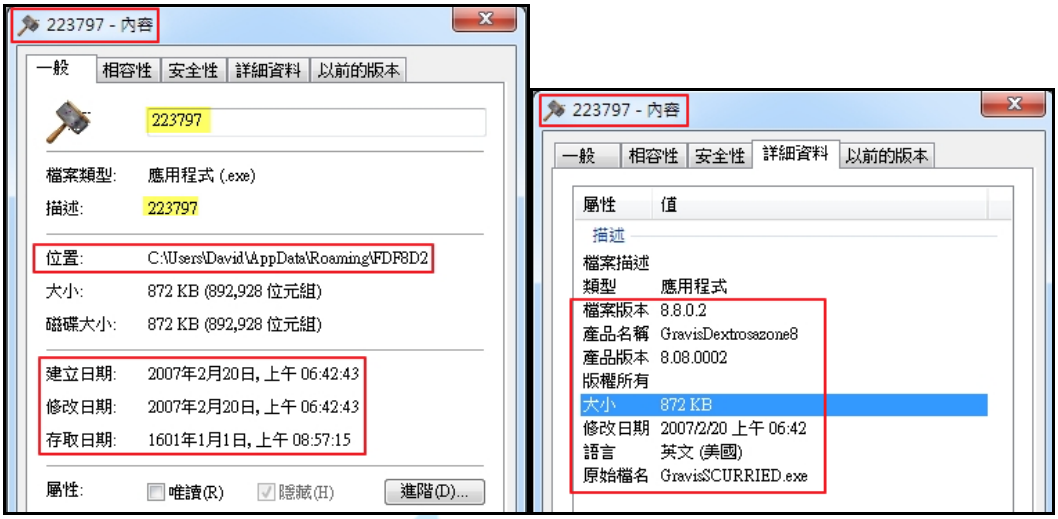
4. 在執行「要求報價 25-06-2019.pdf.exe」後，發現該檔案在原所屬位置的資料夾內消失。檢視背景程式運作情形，發現該程式在執行後產生一個與自己相

同名稱的程式來持續執行著，而且兩者的程式路徑相同，存在原所屬位置的資料夾內，但是查看資料夾卻無任何檔案存在。

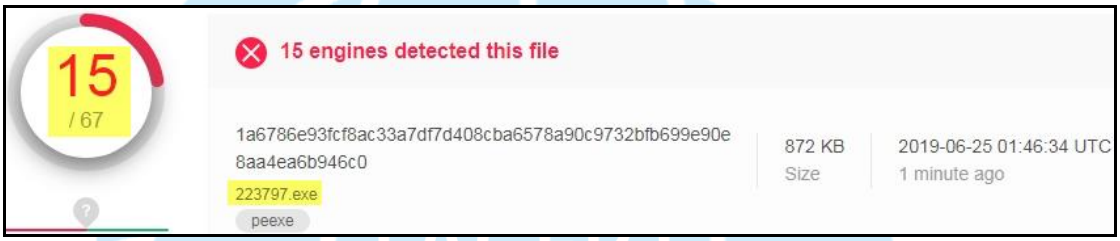
5. 當「要求報價 25-06-2019.pdf.exe」執行時，整個受害主機的記憶體使用率逐漸升高，佔用大多數的記憶體用量，最後系統會出現記憶體即將用盡的警訊。



6. 在 C:\使用者\David\AppData\Roaming\FDF8D2 資料夾內，發現程式 223797.exe，其檔案大小、修改日期、建立日期、存取日期與詳細資料等資訊與程式「要求報價 25-06-2019.pdf.exe」相同，推測兩者可能為相同程式。



223797.exe 經 Virustotal 檢測，其惡意比例為 15/67，僅有 15 家防毒公司的防毒軟體可以檢測出它的存在。

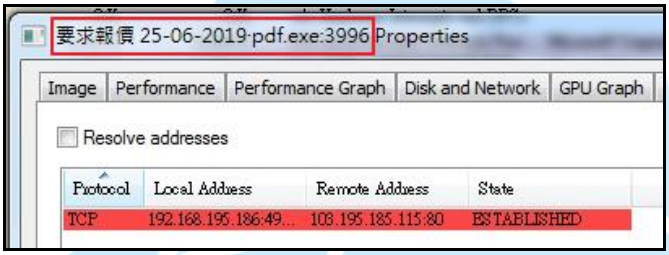


觀察程式「要求報價 25-06-2019.pdf.exe」執行後的行為，發現 223797.exe 是它所產生而且更名過的副本程式(PID:3996)。

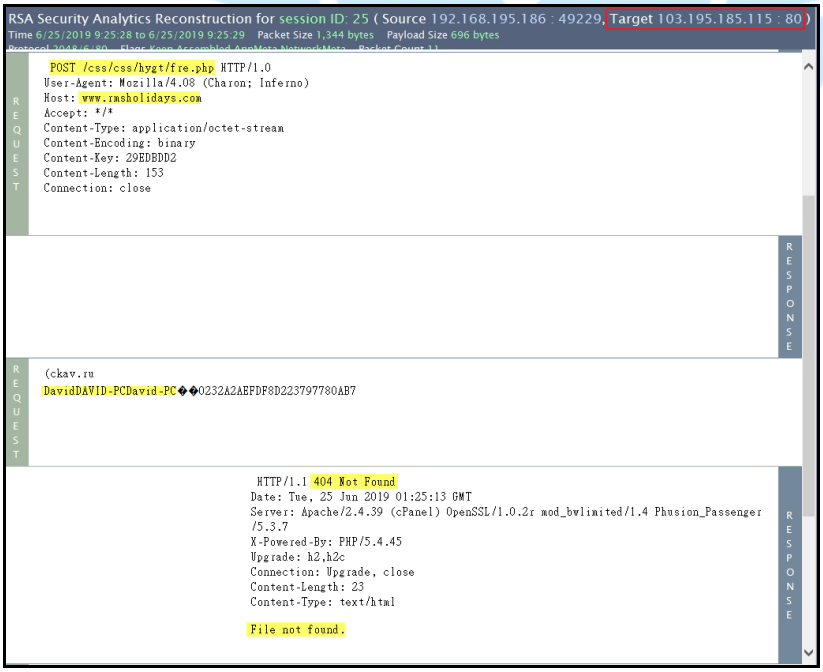
3996	CreateFile	C:\Users\David\AppData\Roaming\FDF8D2	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attribut...
3996	QueryBasicInformationFile	C:\Users\David\AppData\Roaming\FDF8D2	SUCCESS	CreationTime: 2019/6/25 上午 09:20:17, LastAccessTime: 2019/6/25 上午 09:20:17, Last...
3996	CloseFile	C:\Users\David\AppData\Roaming\FDF8D2	SUCCESS	
3996	CreateFile	C:\Users\David\Downloads\要求報價 25-06-2019.pdf\要求報價 25-06-2019.pdf.exe	SUCCESS	Desired Access: Read Attributes, Delete, Synchronize, Disposition: Open, Options: Synchr...
3996	QueryAttributeTagFile	C:\Users\David\Downloads\要求報價 25-06-2019.pdf\要求報價 25-06-2019.pdf.exe	SUCCESS	Attributes: A, ReparseTag: 0x0
3996	QueryBasicInformationFile	C:\Users\David\Downloads\要求報價 25-06-2019.pdf\要求報價 25-06-2019.pdf.exe	SUCCESS	CreationTime: 2007/2/20 上午 06:42:43, LastAccessTime: 1601/1/1 上午 08:57:15, LastW...
3996	CreateFile	C:\Users\David\AppData\Roaming\FDF8D2	SUCCESS	Desired Access: Write Data/Add File, Synchronize, Disposition: Open, Options: , Attribute...
3996	SetRenameInformationFile	C:\Users\David\Downloads\要求報價 25-06-2019.pdf\要求報價 25-06-2019.pdf.exe	SUCCESS	ReplaceIfExists: True, FileName: C:\Users\David\AppData\Roaming\FDF8D2\223797.exe
3996	CloseFile	C:\Users\David\AppData\Roaming\FDF8D2	SUCCESS	
3996	CloseFile	C:\Users\David\AppData\Roaming\FDF8D2\223797.exe	SUCCESS	

7. 查看受測主機對外連線狀況，發現「要求報價 25-06-2019.pdf.exe」執行時會連線印度 IP:103.195.185.115:80，而且是每隔幾分鐘持續連線。

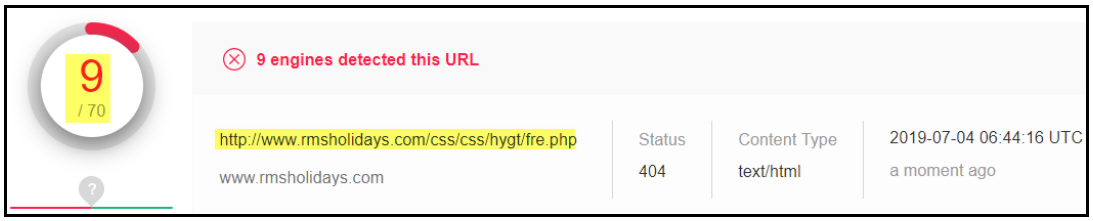
```
2019/6/25 上午 09:20:16 Added    要求報價 25-06-2019.pdf.exe TCP 192.168.195.186:49198  103.195.185.115:80
2019/6/25 上午 09:20:19 Added    Unknown                     TCP 192.168.195.186:49198  103.195.185.115:80
2019/6/25 上午 09:20:19 Added    Unknown                     TCP 192.168.195.186:49199  103.195.185.115:80
2019/6/25 上午 09:20:19 Added    Unknown                     TCP 192.168.195.186:49200  103.195.185.115:80
2019/6/25 上午 09:20:19 Removed  要求報價 25-06-2019.pdf.exe TCP 192.168.195.186:49198  103.195.185.115:80
2019/6/25 上午 09:20:20 Added    svchost.exe                 UDP fe80::2561:26b2:8cb6:acc7:546 *:*
2019/6/25 上午 09:21:19 Added    要求報價 25-06-2019.pdf.exe TCP 192.168.195.186:49201  103.195.185.115:80
2019/6/25 上午 09:21:19 Removed  Unknown                     TCP 192.168.195.186:49194  172.217.160.100:443
2019/6/25 上午 09:21:21 Added    Unknown                     TCP 192.168.195.186:49201  103.195.185.115:80
2019/6/25 上午 09:21:21 Removed  Unknown                     TCP 192.168.195.186:49190  172.217.24.13:443
2019/6/25 上午 09:21:21 Removed  要求報價 25-06-2019.pdf.exe TCP 192.168.195.186:49201  103.195.185.115:80
2019/6/25 上午 09:21:21 Removed  Unknown                     TCP 192.168.195.186:49191  172.217.27.142:443
2019/6/25 上午 09:21:37 Added    svchost.exe                 UDP 0.0.0.0:51207          *:*
2019/6/25 上午 09:21:43 Removed  svchost.exe                 UDP 0.0.0.0:51207          *:*
2019/6/25 上午 09:22:18 Removed  Unknown                     TCP 192.168.195.186:49198  103.195.185.115:80
2019/6/25 上午 09:22:18 Removed  Unknown                     TCP 192.168.195.186:49199  103.195.185.115:80
2019/6/25 上午 09:22:20 Added    要求報價 25-06-2019.pdf.exe TCP 192.168.195.186:49203  103.195.185.115:80
2019/6/25 上午 09:22:20 Removed  Unknown                     TCP 192.168.195.186:49200  103.195.185.115:80
2019/6/25 上午 09:22:22 Added    Unknown                     TCP 192.168.195.186:49203  103.195.185.115:80
2019/6/25 上午 09:22:22 Removed  要求報價 25-06-2019.pdf.exe TCP 192.168.195.186:49203  103.195.185.115:80
```

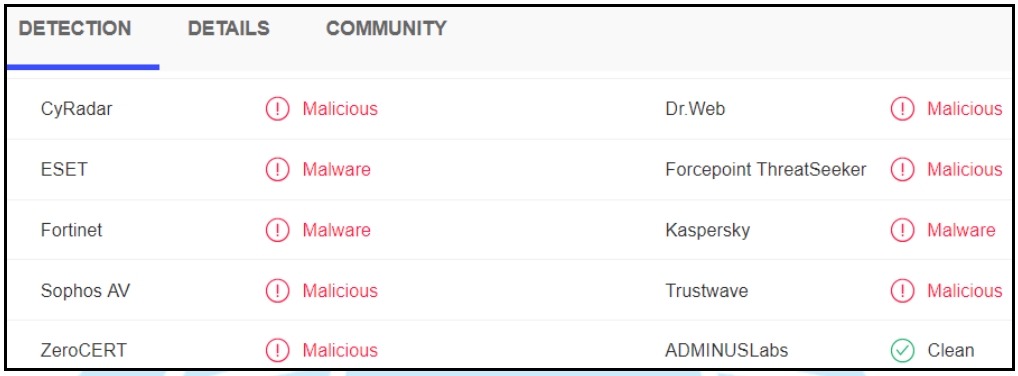


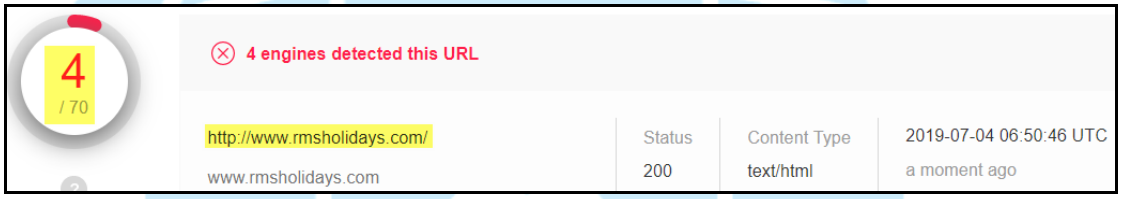
8. 檢視主機連線印度 IP:103.195.185.115 的封包內容，發現受測主機會 POST http://www.rmsholidays.com/css/css/hygt/fre.php，來傳送受測主機名稱的資訊給該 IP，但該印度主機回傳 File not found，推測 fre.php 網頁可能已不在該印度主機上。



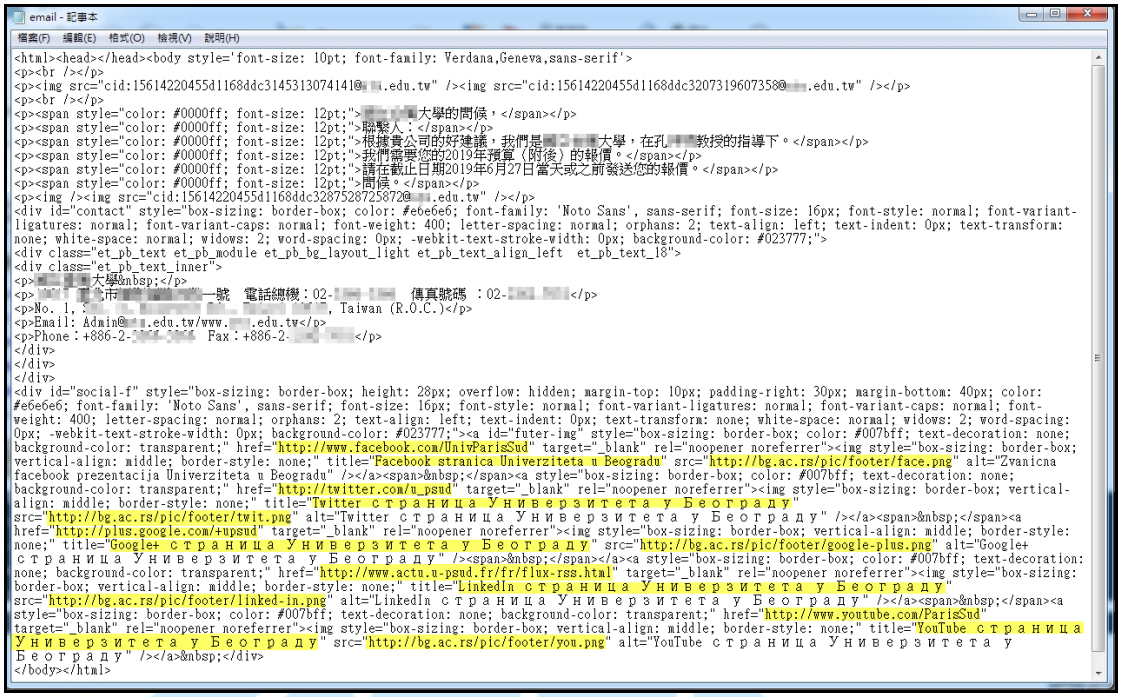
網址 http://www.rmsholidays.com/css/css/hygt/fre.php 經 virustotal 檢測，其惡意比例為 9/70，有 9 家防毒軟體公司的防毒軟體認為 fre.php 為惡意網頁，而有 4 家防毒軟體判定網址 http://www.rmsholidays.com 為惡意網址。

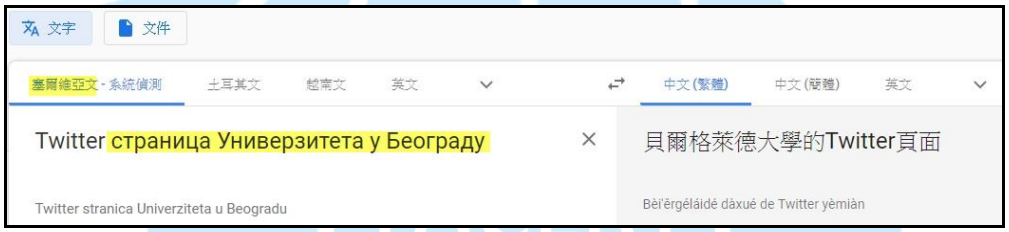




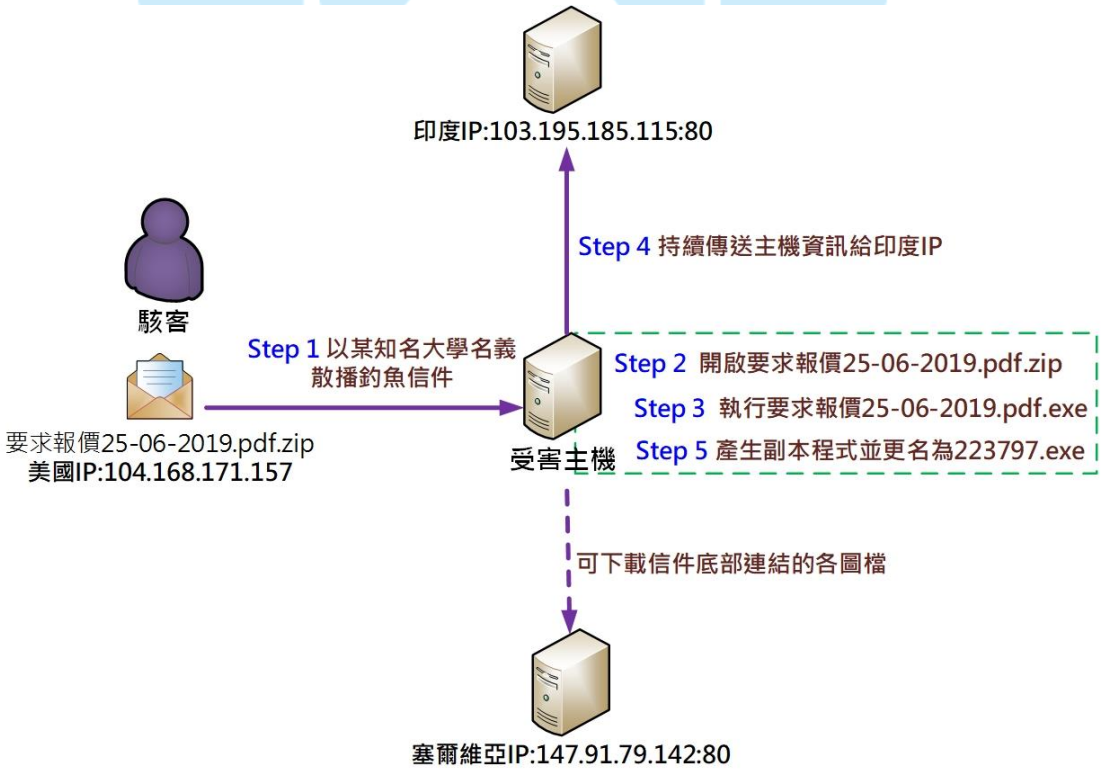


9. 查看信件原始碼內容，發現該信件的最後面有 5 個圖示的連結，這 5 個圖示會連線塞爾維亞 IP:147.91.79.142 來秀出 5 個圖檔(face.png、twit.png、google-plus.png、linked-in.png 與 you.png)，推測該信件可能是駭客由某個信件範本修改完成的。


email - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)


文字
文件
塞爾維亞文 - 系統偵測
土耳其文
越南文
英文
中文(繁體)
中文(簡體)
英文
Twitter страница Универзитета у Београду
貝爾格萊德大學的Twitter頁面
Twitter stranica Univerziteta u Beogradu
Bèi'ěrgélàidé dàxué de Twitter yèmiàn

三、事件攻擊行為示意圖


印度IP:103.195.185.115:80
Step 4 持續傳送主機資訊給印度IP
駭客
Step 1 以某知名大學名義
散播釣魚信件
Step 2 開啟要求報價25-06-2019.pdf.zip
Step 3 執行要求報價25-06-2019.pdf.exe
Step 5 產生副本程式並更名為223797.exe
要求報價25-06-2019.pdf.zip
美國IP:104.168.171.157
受害主機
可下載信件底部連結的各圖檔
塞爾維亞IP:147.91.79.142:80

1.駭客以國內某知名大學名義散播釣魚信件。

2.收件者收信後解壓縮附件「要求報價 25-06-2019.pdf.zip」，並開啟它。

3.收件者的主機開始執行「要求報價 25-06-2019.pdf.exe」。

4.「要求報價 25-06-2019.pdf.exe」執行後，主機會持續傳送主機資訊給印度 IP:103.195.185.115:80。

5.「要求報價 25-06-2019.pdf.exe」產生一個副本程式並更名為 223797.exe，來代替自己執行。

四、建議與總結

1. 本個案的攻擊手法為駭客以知名大學名義寄發網路釣魚的信件，企圖騙取收信者的信任，而附件的壓縮檔「要求報價 25-06-2019.pdf.zip」解開後使用者看到的是含.PDF 的中文檔名，更容易降低收件者的警戒心。
2. 「要求報價 25-06-2019.pdf.exe」執行後產生副本並更名為 223797.exe，但使用 Process 偵測工具查看「要求報價 25-06-2019.pdf.exe」的存放路徑，無法看到它對應到 223797.exe。因 223797.exe 本身為隱藏檔，又存放位置為 C:\系統使用者的隱藏資料夾，因此，使用者發現它的機率便大大降低。
3. 從信件的內容發現該信件有塞爾維亞的連結在信件底部，卻以中文撰寫信件內容與以中文命名附件檔案，推測駭客可能以某信件範本來進行修改，而本身對於中文與台灣的大學環境有一定程度的了解。
4. 對於本個案的攻擊手法有下列幾點建議措施，提供參考。
   (1) 不要隨意開啟不明來源的信件或信件附檔。
   (2) 定期更新防毒軟體的病毒碼，以利即時阻擋惡意程式的攻擊。
   (3) 可疑的信件如需開啟，建議於虛擬機或其它備用主機上開啟較佳。
   (4) 定期備份主機資料。