我國能源領域關鍵基礎設施之惡意程式分析

行政院國家資通安全會報
National Information & Communication Security Taskforce
中華民國110年6月

目　次

1. 摘要 5
2. 惡意程式分析 6
　2.1 惡意程式列表 6
　2.2 惡意程式行為分析 8
3. 受駭偵測指標 17
4. Snort 與 YARA Rule 19

圖 目 次

圖 1　惡意程式運作方式 9
圖 2　惡意程式之第 1 個 Payload 10
圖 3　第 1 個 Payload 內遭混淆之 C2 節點 12
圖 4　前 8 位資料疊代運算之解密範例 12
圖 5　XOR 演算法之運作方式 13
圖 6　解密之 C2 節點 13
圖 7　第 2 個 Payload 產生 XOR 金鑰之程式片段 15
圖 8　第 2 個 Payload 產生之網路流量 16
圖 9　XOR 金鑰(0x37)解密與解壓縮之系統資訊 16

表 目 次

表 1　dot3xbfru.dll 檔案基本資訊 6
表 2　dot3jebiy.dll 檔案基本資訊 6
表 3　dot3jybmc.dll 檔案基本資訊 7
表 4　dot3wbnec.dll 檔案基本資訊 7
表 5　dot3wbnec.dll 檔案基本資訊 7
表 6　dot3fekxk.dll 檔案基本資訊 8
表 7　分析之惡意程式 dot3fekxk.dll 檔案資訊 9
表 8　第 1 個 Payload 之基本資訊 11
表 9　第 2 個 Payload 之基本資訊 13
表 10　惡意程式受駭偵測指標 17
表 11　網路之受駭偵測指標 17
表 12　惡意程式之連線樣態 17
表 13　偵測惡意行為之 Snort Rule 19
表 14　偵測惡意行為之 YARA Rule 19

1. 摘要

國內能源領域關鍵基礎設施於近期查獲 6 個惡意動態連結函式庫檔案(Dynamic-link library, DLLs)，此系列 DLL 檔案為 Gh0st RAT 木馬程式之變種，被命名為「SALTYGHOST」，6 個惡意 DLL 之功能函式包含相同 C2 資訊。經分析發現這些 DLL 夾帶有攻擊目標之內網代理伺服器資訊，由此可知其係針對攻擊目標所客製之惡意 DLL。

惡意 DLL 檔案使用 AES 加密演算法(Advanced Encryption Standard)加密隱藏 2 個 Payload，第 1 個 Payload 是目前未知且用於連線 C2 伺服器與接收任務之報到功能，經多個 YARA Rule 偵測到第 2 個 Payload 為客製化之 Gh0st RAT 木馬程式。

2 個 Payload 使得攻擊者得以通道(Tunnel)/跳板(Pivot)方式進入攻擊目標之內網，並提供攻擊者完整的遠端存取木馬程式功能，包含鍵盤側錄等。

透過公開來源情報(Open-source intelligence, OSINT)尋找業界是否已有此系列惡意程式之相關報告，然而尚未發現任何相關情資。

2. 惡意程式分析

2.1 惡意程式列表

國內能源領域關鍵基礎設施所查獲 6 個惡意檔案基本資訊，詳見表 1 至表 6。

表1　dot3xbfru.dll 檔案基本資訊

檔案名稱	dot3xbfru.dll
檔案類型	PE32 portable executable, dll
檔案大小	795.50 KB
MD5	CA3B100DB19964E618AE78EECD7E745D
SHA1	B871BD2C82EF5E10F279B2AD3F771299338807A8
SHA256	401ba8c8b99398ec3f4ecc2d8a7ebcfc82dadf0c84f088845485163a1cb455eb
編譯時間	Wed Aug 07 09:31:19 2019

表2　dot3jebiy.dll 檔案基本資訊

檔案名稱	dot3jebiy.dll
檔案類型	PE32 portable executable, dll
檔案大小	795.50KB
MD5	9FBF58DB93041FCA0638DC134A7477C9
SHA1	B3AEA95991D86300AF66E4E9636BD160E110C40A
SHA256	C0E28FA67635D3C3382B993500C9B28B65DCCD882AF0F1641AA551398A457B10
編譯時間	Wed Aug 07 09:31:19 2019

表3　dot3jybmc.dll 檔案基本資訊

檔案名稱	dot3jybmc.dll
檔案類型	PE32 portable executable, dll
檔案大小	795.50 KB
MD5	56CE3CAA73590BB97D2EBB0DCB64D6C6
SHA1	9F2D9DCCFC0FE15DC2D04DCF348742DB79B9BAE0
SHA256	F894704BF002094A217A90755899166198EA36AEA45E11D6B9F56C858FB2
編譯時間	Wed Aug 07 09:31:19 2019

表4　dot3wbnec.dll 檔案基本資訊

檔案名稱	dot3wbnec.dll
檔案類型	PE32 portable executable, dll
檔案大小	795.50 KB
MD5	824351A92175C99E7527D9CFB4BA3345
SHA1	14D1E1DD72DC1F2AD5EA3FEB3D3CC893942BA0C1
SHA256	1098AA7C7C635CEAFC3F5090288F6E991D258482BEFCF3EF5AEF726B03E067F5
編譯時間	Wed Aug 07 09:31:19 2019

表5　dot3wbnec.dll 檔案基本資訊

檔案名稱	dot3wbnec.dll
檔案類型	PE32 portable executable, dll
檔案大小	795.50 KB
MD5	58456F8D9BD522B3B15FE7C40689EA8A
SHA1	24749147E174658C3C8458B9C34C279C719AFA3B

SHA256	80EB02F63AF65D0921E290686287F032EFDD665EFF89F14BF60A35CFAD12CCB3
編譯時間	Wed Aug 07 09:31:19 2019

表6　dot3fekxk.dll 檔案基本資訊

檔案名稱	dot3fekxk.dll
檔案類型	PE32 portable executable, dll
檔案大小	795.50 KB
MD5	4B3382AEECB12BFD55B784D8B18B9861
SHA1	E181C2A31F9FC9C1F7143FDBF7330C8E5FB91ABA
SHA256	7FF99F31F8E42B5BCA702662CC2F6F2DEAE683D60668940DCF2633D999ECCF9F
編譯時間	Wed Aug 07 09:31:19 2019

2.2 惡意程式行為分析

國內能源領域關鍵基礎設施所查獲 6 個惡意檔案，其行為模式大致相同，以下說明惡意程式行為，以 dot3fekxk.dll 樣本之分析結果為主(MD5：9FBF58DB93041FCA0638DC134A7477C9)。

惡意程式之運作方式可分為 1 至 6 步驟，運作方式詳見圖 1。

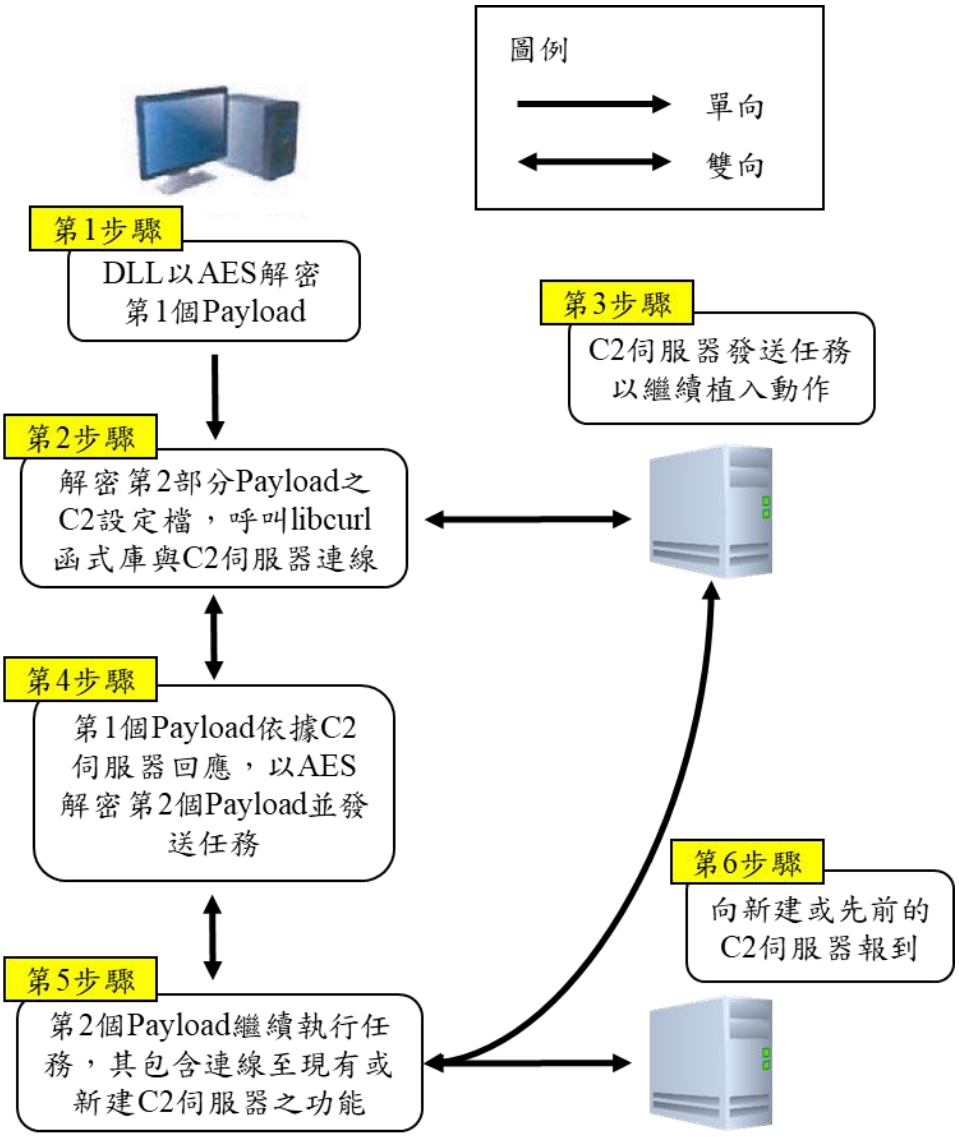


圖1　惡意程式運作方式

2.2.1 第 1 步驟行為分析

表7　分析之惡意程式 dot3fekxk.dll 檔案資訊

檔案名稱	dot3fekxk.dll
檔案類型	PE32 portable executable, dll
檔案大小	795.50 KB
MD5	4B3382AEECB12BFD55B784D8B18B9861
SHA1	E181C2A31F9FC9C1F7143FDBF7330C8E5FB91ABA

SHA256	7FF99F31F8E42B5BCA702662CC2F6F2DEAE683D60668940DCF2633D999ECCF9F
編譯時間	Wed Aug 07 09:31:19 2019
檔案敘述	無

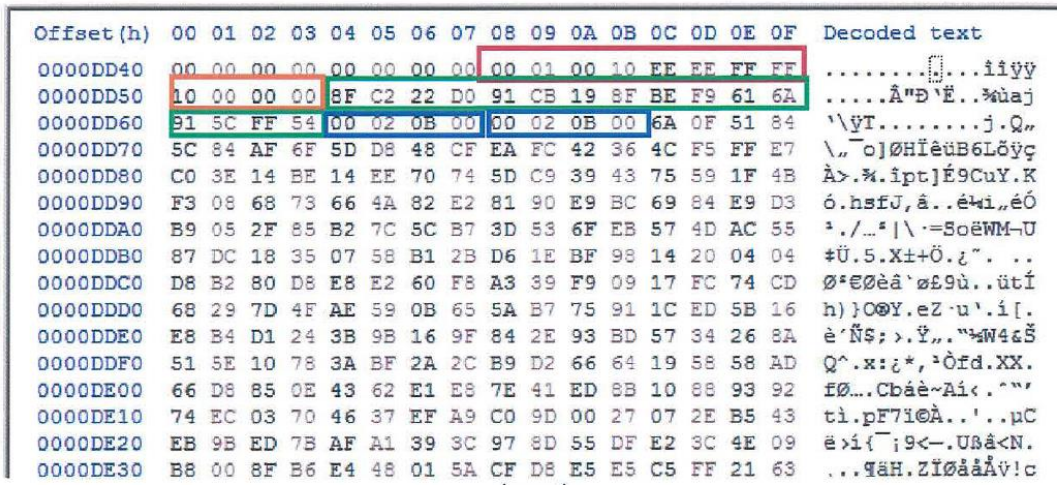
二進位檔案「dot3fekxk.dll」是一個包含「ServiceMain」匯出函式(export function)之 Windows DLL，此惡意程式透過未知方式安裝至受駭目標系統，但 DLL 並沒有自行持續潛伏之能力。

若惡意 DLL 執行時，會掛載於 Windows 的 BSS 服務(Bluetooth Support Service)下執行。

dot3fekxk.dll 可視為一個載入程式(Loader)，當執行於受駭目標設備時，能辨別 AES 加密之 Payload 位置，接著將其解密並執行第 1 個 Payload。

●Payload 解密演算法：

此 Loader 存在客製化 AES Header，做為搜尋與解密下一個 Payload 之用，Payload 內容詳見圖 2。



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
0000DD40  00 00 00 00 00 00 00 00 00 01 00 10 EE EE FF FF  ............îîÿÿ
0000DD50  10 00 00 00 8F C2 22 D0 91 CB 19 8F BE F9 61 6A  .....Â"Ð'Ë..¾ùaj
0000DD60  91 5C FF 54 00 02 0B 00 00 02 0B 00 6A 0F 51 84  '\ÿT........j.Q„
0000DD70  5C 84 AF 6F 5D D8 48 CF EA FC 42 36 4C F5 FF E7  \„¯o]ØHÏêüB6Lõÿç
0000DD80  C0 3E 14 BE 14 EE 70 74 5D C9 39 43 75 59 1F 4B  À>.¾.îpt]É9CuY.K
0000DD90  F3 08 68 73 66 4A 82 E2 81 90 E9 BC 69 84 E9 D3  ó.hsfJ‚â..é¼i„éÓ
0000DDA0  B9 05 2F 85 B2 7C 5C B7 3D 53 6F EB 57 4D AC 55  ¹./…²|\·=SoëWM¬U
0000DDB0  87 DC 18 35 07 58 B1 2B D6 1E BF 98 14 20 04 04  ‡Ü.5.X±+Ö.¿˜. ..
0000DDC0  D8 B2 80 D8 E8 E2 60 F8 A3 39 F9 09 17 FC 74 CD  Ø²€Øèâ`ø£9ù..ütÍ
0000DDD0  68 29 7D 4F AE 59 0B 65 5A B7 75 91 1C ED 5B 16  h)}O®Y.eZ·u'.í[.
0000DDE0  E8 B4 D1 24 3B 9B 16 9F 84 2E 93 BD 57 34 26 8A  è´Ñ$;›.Ÿ„.“½W4&Š
0000DDF0  51 5E 10 78 3A BF 2A 2C B9 D2 66 64 19 58 58 AD  Q^.x:¿*,¹Òfd.XX.
0000DE00  66 D8 85 0E 43 62 E1 E8 7E 41 ED 8B 10 88 93 92  fØ….Cbáè~Aí‹.ˆ“’
0000DE10  74 EC 03 70 46 37 EF A9 C0 9D 00 27 07 2E B5 43  tì.pF7ï©À..'..µC
0000DE20  EB 9B ED 7B AF A1 39 3C 97 8D 55 DF E2 3C 4E 09  ë›í{¯¡9<—.Ußâ<N.
0000DE30  B8 00 8F B6 E4 48 01 5A CF D8 E5 E5 C5 FF 21 63  ...¶äH.ZÏØååÅÿ!c
```

圖2　惡意程式之第 1 個 Payload

– 紅色框內 8 byte header 用以確保 Loader 搜尋時能找到 AES 加密片段

– 橘色框內表示 AES 金鑰長度(此案例為 16 byte)

– 綠色框內為 AES 金鑰(8F C2 22 D0 91 CB 19 8F BE F9 61 6A 91 5C FF 54)

– 藍色框內 2 個數值皆為加密 Payload 之長度

– 其餘為加密之 Payload

當 Loader 搜尋到 AES OFB 模式之加密 Payload，將會使用 AES 金鑰與 hardcoded 初始向量解密 Payload，並呼叫第 1 個 Payload 經解密後發現之「GetSession」匯出函式(export function)。

2.2.2 第 2 步驟行為分析

表8　第 1 個 Payload 之基本資訊

Payload 名稱	第 1 個 Payload
類型	PE32 portable executable, dll
大小	745,472 Bytes
MD5	80EC332AE9CA8C132EFE59EBE9E08D85
SHA1	C5C8124446CA90D5E029D90EE0298DDA1FC6722F
SHA256	F950874119691C4B936D10F0D41D86F535390F6A75DCEB0DFD0A47FCDA27EE8A
編譯時間	Wed Aug 07 09:31:23 2019
檔案敘述	無

以 Loader 解密之第 1 個 Payload，為另一個包含「GetSession」匯出函式之 Windows DLL，第 1 個 Payload 功能為連線至設定檔內 hardcoded 之 C2 節點，內容包含 3 個 URL、2 個 C2 節點及受害目標之 Proxy 伺服器，由此可說明此惡意程式專門為此受駭目標所客製化製作。第 1 個 Payload 內遭混淆之 C2 節點，詳見圖 3。

Obfuscated C2 Nodes in Hex
CAA2BFB9A0A7E3F0C9998076227640443 63D1607E1EFDCE9AE81204B25591EFA8BEBCF2D7000 EA97B29F11304F9FE365055BA4F7CA4D02F1FE670C56D7914E03CFC45B05C0
CAA2BFB9A0A7E3F0C98C9E66687951522D310614E6B2DFA2AAD96D487D031CAA8BEECB2D2407 B1CBB7C846624B9EB3340B55A1F7994F07A7AF35101AD593450E849A431D

圖3　第 1 個 Payload 內遭混淆之 C2 節點

第 1 個 Payload 會使用 exclusive OR (XOR)演算法，解密 C2 節點與受駭目標 Proxy 伺服器。

第 1 個 byte 資料「0xCA」做為 XOR 演算法之金鑰，並以此 byte 資料與第 2 個 byte 進行 XOR 運算。舉例來說，0xA2 必須被金鑰 0xCA 進行 XOR 運算，當此運算完成後，以 loop 迴圈增加 counter 之值與 XOR 金鑰「0xCA」每次進行疊代(iterations)。前 8 位資料疊代運算之解密範例，詳見圖 4。XOR 演算法之運作方式，詳見圖 5。解密之 C2 節點，詳見圖 6。

XOR Key	0xCA	0xCB	0xCD	0xD0	0xD4	0xD9	0xDF	0xE6
Obfuscated C2	0xA2	0xBF	0xB9	0xA0	0xA7	0xE3	0xF0	0xC9
Deobfuscated C2 in ASCII	h	t	t	p	s	:	/	/

圖4　前 8 位資料疊代運算之解密範例

```
20  if ( *(&v10 + v3) != 35 )
21    return 0;
22  *(&v10 + v3) = 0;
23  sub_6A325F30(v2);
24  starting_key_0xCA = *v2;
25  counter = 0;
26  if ( (strlen(a2) & 0xFFFFFFFE) > 2 )
27  {
28    obfuscated_C2 = v2;
29    while ( 1 )
30    {
31      key = counter + starting_key_0xCA;
32      *obfuscated_C2 = key ^ obfuscated_C2[1];
33      ++counter;
34      v10 = key;
35      if ( (unsigned int)&(++obfuscated_C2)[1 - (_DWORD)v2] >= strlen(a2) >> 1 )
36        break;
37      starting_key_0xCA = v10;
38    }
39    v2 = v9;
40  }
41  v2[counter] = 0;
42  return 1;
43}
```

圖5　XOR 演算法之運作方式

```
https://www[.]newtourism[.]pw/ba9ca11400dc8da6a376f79722acf0a3/cache.php
https://bigdataocean[.]net/ba9ca11400dc8da6a376f79722acf0a3/cache.php
```

圖6　解密之 C2 節點

第 1 個 Payload 包含已編譯之「CLIENT libcurl 7.59.0」函式庫，可用 libcurl 與 C2 伺服器連線，提供第 1 個 Payload 多種方式與 C2 伺服器連線。

2.2.3 第 3 步驟行為分析

當第 1 個 Payload 成功與 C2 伺服器連線後，C2 伺服器將發送一個特定指令，以進行第 2 個 Payload 解密之初始化工作。

2.2.4 第 4 步驟行為分析

表9　第 2 個 Payload 之基本資訊

Payload 名稱	第 2 個 Payload

類型	PE32 portable executable, dll
大小	139,192 Bytes
MD5	05945B801B9C9188E9E54989F14F631E
SHA1	F53816BF98A4CB6E70D4E8726B18D7EA5AF1C8E7
SHA256	C816571366E23479A8EC3730EF101AC766F53DF1B4915394EB78A82201F4BB89
編譯時間	Sat Oct 12 21:39:59 2019

第 1 個 Payload 使用與第 1 步驟所述之相同的 AES 演算法，包含相同之 Header、AES 金鑰及 hardcoded 初始向量，以解密第 2 個 Payload。

第 2 個 Payload 亦為 Windows DLL，內部包含「create_work3」之匯出函式，第 1 個 Payload 將呼叫「create_work3」匯出函式，並提供任務給第 2 個 Payload 完成。

第 2 個 Payload 為完整遠端存取木馬(Remote Access Trojan, RAT)，被判定為 gh0st RAT 木馬之變種。

2.2.5 第 5 與第 6 步驟行為分析

當第 2 個 Payload 被第 1 個 Payload 執行後，將依據指令選擇 C2 伺服器與連線方式(如經由 Proxy 連線或直接連線)，再連線至 C2 伺服器報到。

接著第 2 個 Payload 會快速蒐集系統資訊，如作業系統版本、Service Pack 修正檔資訊及網路配置資訊，所蒐集之系統資訊利用 zlib 函式庫進行壓縮。

第 2 個 Payload 並使用生成之 XOR 金鑰，將已壓縮的系統資訊進行加密混淆。

XOR 金鑰為利用呼叫 Windows API「GetTickCount」之結果，與 8 個 hardcoded 固定數值進行 8 次模運算(modulus operation)所生成。第 2 個

Payload 產生 XOR 金鑰之程式片段，詳見圖 7。

```
34  v5 = GetTickCount();
35  v20 = v5 % 0x1BD;
36  v21 = v5 % 0x14E;
37  v22 = v5 % 0x22C;
38  v23 = v5 % 0x29B;
39  v24 = v5 % 0x30A;
40  v25 = v5 % 0xFF;
41  v26 = v5 % 0x379;
42  v6 = v5 % 0x3E6;
```

圖7　第 2 個 Payload 產生 XOR 金鑰之程式片段

第 2 個 Payload 會針對「GetTickCount」模運算之結果，檢查其是否小於 0xFF，並取 1 個 byte 之值做為 XOR 金鑰。

第 2 個 Payload 取 1 個 byte 之值做為 XOR 金鑰，再以此將壓縮資料每個 Byte 做 XOR 運算並傳送至 C2 伺服器。

第 2 個 Payload 於測試環境所產生之網路流量，其流量內容詳見圖 8。

圖 8 之第 1 個藍色框之 8 位數為模運算結果，第 2 個 Payload 用其生成 1 個 byte 之 XOR 金鑰，生成之 XOR 金鑰為 0x37 且是小於 0xFF，即用於加密以 zlib 壓縮之系統資訊。綠色框內之 8 byte 數值為未知資料，而黑色框內 4 bytes 之數值(34 01 00 00)為一個常數，且固定存在於第 2 個 Payload 之網路流量，故能以此常數尋找網路流量中向 C2 伺服器發送之加密壓縮系統資訊。

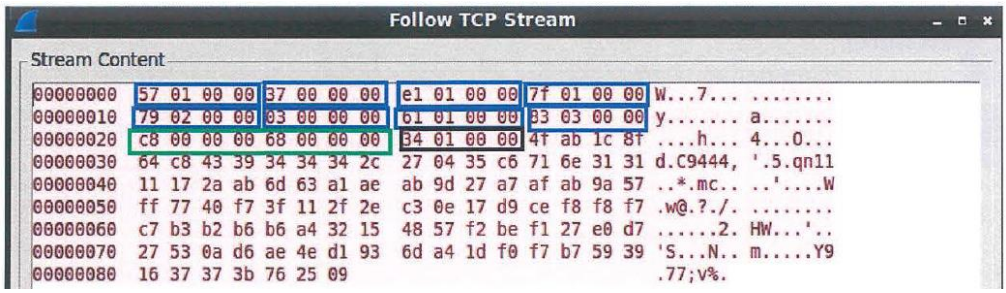


圖8　第 2 個 Payload 產生之網路流量

測試環境產生之加密壓縮系統資訊，經 XOR 金鑰(0x37)解密與解壓縮後之結果，詳見圖 9。

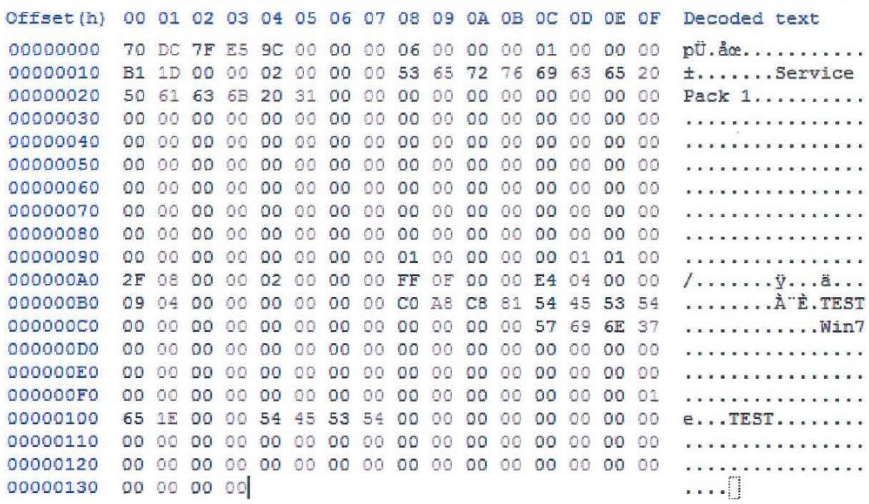


圖9　XOR 金鑰(0x37)解密與解壓縮之系統資訊

3. 受駭偵測指標

惡意程式已客製化為掛載於 Windows BSS 服務(Bluetooth Support Service)下運作，惡意程式受駭偵測指標(Indicators of compromise, IoC)，詳見表 10。

表10 惡意程式受駭偵測指標

惡意程式檔名	MD5
dot3xbfru.dll	CA3B100DB19964E618AE78EECD7E745D
dot3jebiy.dll	9FBF58DB93041FCA0638DC134A7477C9
dot3jybmc.dll	56CE3CAA73590BB97D2EBB0DCB64D6C6
dot3wbnec.dll	824351A92175C99E7527D9CFB4BA3345
dot3wbnec.dll	58456F8D9BD522B3B15FE7C40689EA8A
dot3fekxk.dll	4B3382AEECB12BFD55B784D8B18B9861

惡意程式網路受駭偵測指標，詳見表 11。惡意程式之連線樣態，詳見表 12。

表11 網路之受駭偵測指標

項次	域名
1	www[.]newtourism[.]pw
2	bigdataocean[.]net

表12 惡意程式之連線樣態

連線類型	連線樣態
HTTPS	GET /ba9cal1400dc8da6a376f79722acf0a3/cache.php HTTP/1.1 Host: bigdataocean.net Accept: */*

連線類型	連線樣態
	User-Agent: Mozilla/5.0 Firefox 59.0.2.6656 Connection: keep-alive GET /ba9cal1400dc8da6a376f79722acf0a3/cache.php HTTP/1.1 Host: www.newtourism.pw Accept: */* User-Agent: Mozilla/5.0 Firefox 59.0.2.6656 Connection: keep-alive
Proxy	CONNECT bigdataocean.net:443 HTTP/1.1 Host: bigdataocean.net:443 Proxy-Connection: Keep-Alive CONNECT www.newtourisrm.pw:443 HTTP/1.1 Host: www.newtourisrm.pw:443 Proxy-Connection: Keep-Alive

4. Snort 與 YARA Rule

可用於偵測上述惡意行為之 Snort 與 YARA Rule，詳見表 13 與表 14。

表13 偵測惡意行為之 Snort Rule

項次	Snort Rule
1	alert udp any any -> any 53 (content: "www.newtourism.pw"; msg: "Malware RAT";)
2	alert udp any any -> any 53 (content: "bigdataocean.net"; msg: "Malware RAT";)

表14 偵測惡意行為之 YARA Rule

項次	YARA Rule

1	rule RAT_loader
	{
	strings:
	$compile_date = { B7 E0 4A 5D }
	$AES string = "AVAES"
	$opcodes = { 81 3F 00 01 00 10 0F 85 C4 00 00 00 81 7F 04 EE EE FF FF 0F 85 B7 00 00 }
	$custom AES header = { 00 01 00 10 EE EE FF FF 10 00 00 00 8F C2 22 D0 }
	condition:
	($compile_date i.n (0 .. 300) and any of them) or
	$opcodes or $custom AES header
	}