Raytheon

Customer Success Is Our Mission

C2 Decoding for the Lazy Reverser

September 22, 2009

Matt Richard

Unclassified

Who Am I?

- First and Foremost – A lazy reverser
- RayCERT Special Technologies and Analysis Team
- Formerly Director of Rapid Response at iDefense
- Co-author “Cyberfraud Tactics, Techniques and Procedures”
- CISSP, GCIA, GCIH, GCFA, GREM

Credits

- Michael Hale Ligh – MNIN Security, iDefense
- Greg Sinclair – iDefense
- Defcon 16 – "**Malware RCE: Debuggers and Decryptor Development**"

Goals

- Reverse engineer and instrument C2 decoders
- Use scripted debugging for automation
- Do it fast

Limitations

- Execution “leaks”
- Performance
- Must parse packets
- Time related to analyst
- Sharing

Decoder Writing

1. Collect traffic
2. Gather hints / malware
3. Find decoder function
4. Write decoder script
5. Automate collection and processing

Tools

- Sandnet/box
  - Semi-controlled execution
- IDA Pro / Disassembler
- Immunity Debugger / Ollydbg
  - Immunity has Python scripting interface
  - Simple usage of OS / CPU operations
    - Virtual alloc
    - Read/write strings from memory
    - Change EIP / regs

Immunity Python Primer

```
import immlib, base64
imm = immlib.Debugger()
t = imm.createTable('Name', ['Val 1', 'Val 2'])

def main(args):
    address = imm.remoteVirtualAlloc(0x100)
    imm.writeMemory(address,string)
    imm.setReg('EIP', 0xdeadbeef)
    regs = imm.getRegs()
    if regs['EIP'] > 0xabc123:
        imm.writeLong(regs['ESP']+ 0x4, string)
    imm.runTillRet()
    imm.stepOver()
    output = imm.readString(address)
    t.add('', [value1, value2])
```

Case Study #1 – Decoding comments <!-- V2VsY29tZSE= -->

Case Study – Comment Group

- Prolific user of comment strings for C2

- Several versions with different encoding
  - Base64
  - B64 w/ modified alphabet
  - Custom “encryption”

```
<!-- 2upczxAXha0t -->
<html>

<head>
<meta http-equiv="Content-Type"
content="text/html; charset=iso-8859-1">
<title> Web Posting Information </title>
</head>
```

```
<!-- czox -->
<html><!-- #BeginTemplate "/Templates/M&A_gray.dwt" -->
<head>
<!-- #BeginEditable "doctitle" -->
<!-- {685DEC108DA73FFC} -->
<title>Martin &amp; Associates Accounting Software and Business Solutions</title>
```

Comment Group - Hints

Raytheon
Customer Success Is Our Mission

```
InternetCloseHandle
InternetOpenA
InternetReadFile
HttpQueryInfoA
InternetOpenUrlA
WININET.dll
_stricmp
Kernel32.dll
.exe
Mozilla/4.0                                  1; MSIE 7.0)
Accept: */*
}    >
<!-- {
sleep
Mozilla/4.0 (compatible; Windo                 7.0) DLDLL.%s.LETUSROCKYOU)
thequickbrownfxjmpsvalzydg
`1234567890-=~!@#$^&*()_+qwertyuiop[]QWERTYUIOP|asdfghjkl;'ASDFGHJKL:zxcvbnm,./
  ZXCVBNM<>?
Dcryption Error! Invalid Character '%c'.
```

Comment delimiters for command

Password?

Error message?

Comment Group – Parsing Comments

Strings window

Address	Length	T...	String
.rdata:1000...	00000006	C	fopen
.rdata:1000...	00000005	C	atoi
.rdata:1000...	00000007	C	malloc
.rdata:1000...	00000007	C	strstr
.rdata:1000...	0000000B	C	MSVCRT.dll
.rdata:1000...	00000005	C	free
.rdata:1000...	0000000A	C	_initterm
.rdata:1000...	0000000D	C	_adjust_fdiv
.rdata:1000...	00000014	C	InternetCloseHandle
.rdata:1000...	0000000E	C	InternetOpenA
.rdata:1000...	00000011	C	InternetReadFile
.rdata:1000...	0000000F	C	HttpQueryInfoA
.rdata:1000...	00000011	C	InternetOpenUrlA
.rdata:1000...	0000000C	C	WININET.dll
.rdata:1000...	00000009	C	_stricmp
.data:1000...	0000000D	C	Kernel32.dll
.data:1000...	00000005	C	.exe
.data:1000...	00000033	C	Mozilla/4.0 (compatible; Windows NT 5.1; MSIE 7.0)
.data:1000...	00000006	C	} -->
.data:1000...	00000007	C	<!-- {
.data:1000...	00000006	C	sleep
.data:1000...	0000004A	C	Mozilla/4.0 (compatible; Windows NT 5.1; MSIE 7.0) DLDLL.%s.LETUSRO.
.data:1000...	0000001B	C	thequickbrownfxjmpsvalzydg
.data:1000...	0000005A	C	`1234567890-=~!@#$^&*()_+qwertyuiop[]QWERTYUIOPlasdfghjkl;'ASDFG.
.data:1000...	00000029	C	Dcryption Error! Invalid Character '%c'.

Media decode

Comment Group – Parsing Comments

Raytheon
Customer Success Is Our Mission

```
push    13Ch            ; Size
call    ds:malloc
mov     ebp, eax
mov     ecx, 4Fh
xor     eax, eax
mov     edi, ebp
rep stosd
mov     edi, offset asc_10003078 ; "<!-- {"
or      ecx, 0FFFFFFFFh
add     esp, 4
lea     edx, [ebp+0Ah]
repne scasb
not     ecx
sub     edi, ecx
mov     eax, ecx
mov     esi, edi
mov     edi, ebp
shr     ecx, 2
rep movsd
mov     ecx, eax
xor     eax, eax
and     ecx, 3
rep movsb
mov     edi, offset asc_10003070 ; "} -->"
or      ecx, 0FFFFFFFFh
repne scasb
not     ecx
```

Comment Group – Decoder?

Raytheon
Customer Success Is Our Mission

```
loc_100017A8:
mov     ecx, ebp
lea     esi, [esp+eax+2B64h+var_2800]
mov     eax, ecx
lea     edi, [esp+2B64h+var_2A08]
shr     ecx, 2
rep movsd
mov     ecx, eax
lea     edx, [esp+2B64h+var_2A08]
and     ecx, 3
rep movsb
lea     ecx, [esp+2B64h+Str]
push    ecx
push    edx
call    sub_10001930
add     esp, 8
test    eax, eax
jnz     short loc_100017EA
```

Comment Group – Decoder?

Raytheon
Customer Success Is Our Mission

```
loc_10001A70:
mov     edx, [esp+198h+arg_0]
lea     ecx, [esp+198h+Dest]
movsx   eax, byte ptr [ebx+edx]
push    eax
push    offset aDcryptionError ; "Dcryption Error! Invalid Character '%c'"...
push    ecx             ; Dest
call    ds:sprintf
mov     edx, [esp+1A4h+arg_4]
add     esp, 0Ch
xor     eax, eax
pop     edi
pop     esi
pop     ebp
mov     byte ptr [edx], 0
pop     ebx
add     esp, 188h
retn
sub_10001930 endp
```

Comment Group -

Raytheon
Customer Success Is Our Mission

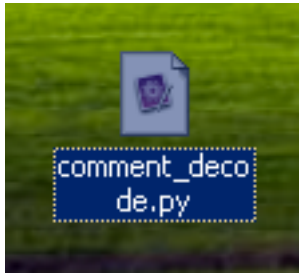
```
sub_10001930 proc near

var_188= dword ptr -188h
var_184= dword ptr -184h
var_180= dword ptr -180h
var_17C= dword ptr -17Ch
var_178= byte ptr -178h
Str= byte ptr -15Ch
Dest= byte ptr -100h
var_FF= byte ptr -0FFh
arg_0= dword ptr  4
arg_4= dword ptr  8

sub     esp, 188h
push    ebx
push    ebp
push    esi
push    edi
mov     ecx, 18h
mov     esi, offset a1234567890@_Qw ; "`1234567890-=~!@#$^&*()_+qwertyuiop[]QW"...
lea     edi, [esp+198h+Str]
mov     al, byte_10003180
rep movsd
movsw
mov     ecx, 8
mov     esi, offset aThequickbrownf ; "thequickbrownfxjmpsvalzydg"
lea     edi, [esp+198h+var_178]
mov     [esp+198h+Dest], al
rep movsd
movsw
```

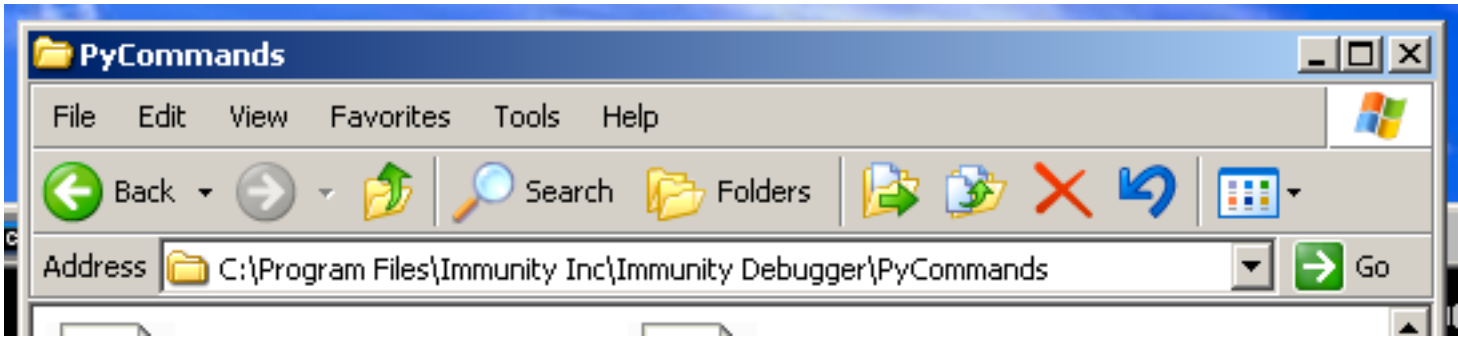
Comment Group - Scripted

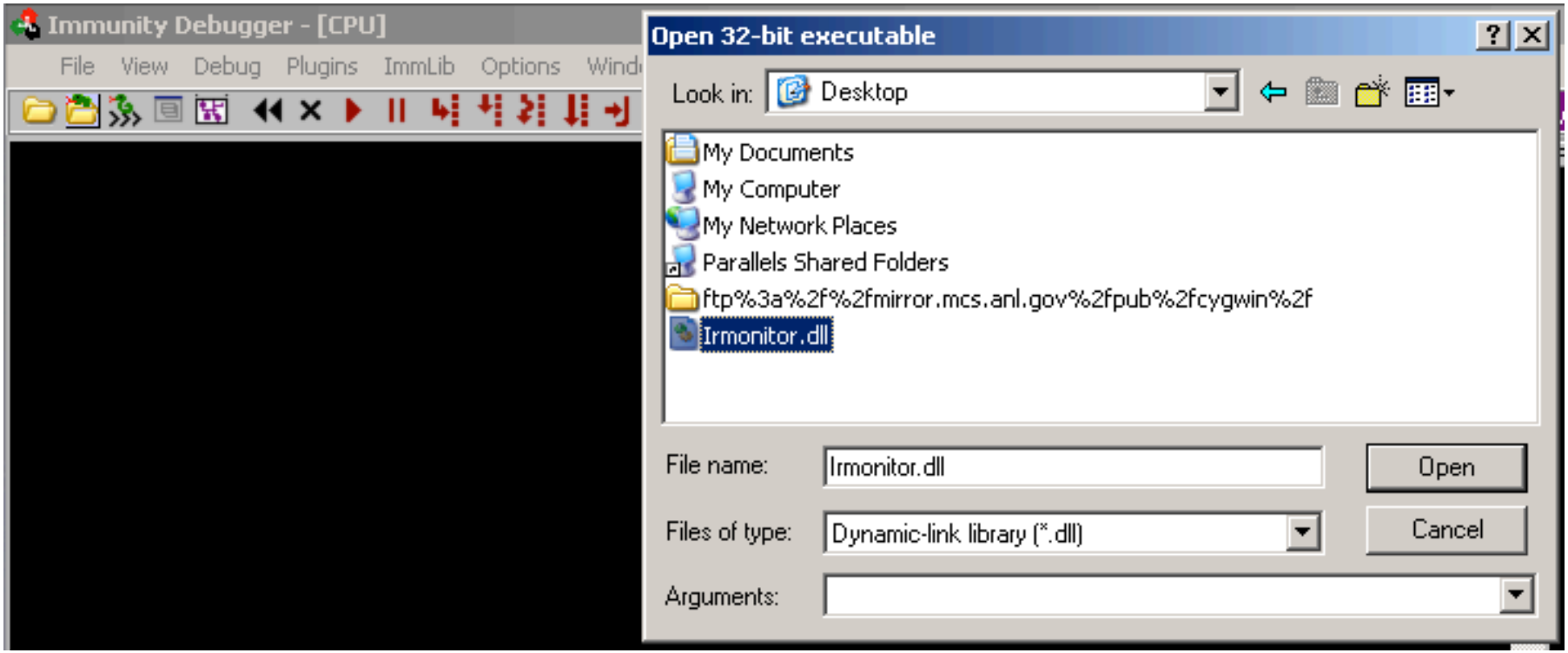
```
def main(args):
    strings = ["/*jgJ-.J", "ujQ~iY,UnQ[!,hvoZWg", "/*jgJ-,F",
    "/*jgJ-v;B", "/*jgJ-vl/", "uG]~oYZUntQ!Vjs'ZQ", "ujQ~iY,UnQ[!,hmoZWg",
     "/*jgJ-bAB", "/*jgJ-mS", "/*jgJ-vJ", "/*jgJ-,",

    for string in strings:
        decodefunc = 0x10001930
        imm.setReg('EIP', decodefunc)

        str_len = len(string)
        s1 = imm.remoteVirtualAlloc(str_len)
        s2 = imm.remoteVirtualAlloc(str_len)

        imm.writeMemory(s1,string)
        regs = imm.getRegs()
        imm.writeLong(regs['ESP']+ 0x4, s1)
        imm.writeLong(regs['ESP'] + 0x8, s2)
        imm.runTillRet()
        imm.stepOver()
        output = imm.readString(s2)
        table.add('', ['%s' % string,'%d' % len(string), '%s' % output])
```

Comment Group – Taking Action

Raytheon
Customer Success Is Our Mission







Comment Group – Taking Action

Raytheon
Customer Success Is Our Mission

1. For DLL Start to load

Immunity Debugger - Irm... ad, module LOADDLL]

File View Debug Options Window Help Jobs

```
00410070  LOADDLL.<ModuleEntryPoint>()
00410070  $ 8BEC          MOV EBP,ESP
00410072  . 6A 00         PUSH 0
00410074  . E8 310A0000   CALL <JMP.&KERNEL32.GetModuleHandleA>
00410079  . A3 B0004200   MOV DWORD PTR DS:[4200B0],EAX
0041007E  . A3 24004200   MOV DWORD PTR DS:[420024],EAX
00410083  . E8 160A0000   CALL <JMP.&KERNEL32.GetCommandLineA>
00410088  . 8BF0          MOV ESI,EAX
0041008A  . 46            INC ESI
0041008B  > 8A06          ... DS:[ESI]
0041008D  . 46
0041008E  . 0AC0
00410090  . 75 0F         ... .004100A1
00410092  . C705 2        ... [420020],LOADDLL.0042
0041009C  . E9 EB0        ... 28C
004100A1  > 3C 22
004100A3  .^75 E6         ... .0041008B
004100A5  > 8A06          ... S:[ESI]
004100A7  . 3C 20
004100A9  . 75 03         JNZ SHORT LOADDLL.004100AE
004100AB  . 46            INC ESI
004100AC  .^EB F7         JMP SHORT LOADDLL.004100A5
```

```
Registers (FPU)
EAX 00000000
ECX 0006FFB0
EDX 7C90EB94 ntdll.KiFastSystemCall
EBX 7FFDC000
ESP 0006FFC4
EBP 0006FFF0
ESI FFFFFFFF
EDI 7C910738 ntdll.7C910738
EIP ... uleEntryPo
C ... FF)
P ... FF)
A ... FF)
Z ... FF)
S ... (FFF)
O ... (0000000
EFL 00000246 (NO,... E,NS,PE,GE,L
ST0 empty -UNORM BBC... 050104 0079
```

2. Execution should be paused

3. Enter script name with no suffix

!comment_decode

Analysing LOADDLL: 1 heuristical procedure, 20 calls to known functions

Paused

“Live” Demo

Immunity Debugger - Irmonitor.dll

File View Debug Plugins ImmLib Options Window Help Jobs

l e m t w h c P k b z

CPU - main thread, module Irmonito

```
10001A6F  .  C3              RETN
10001A70  >  8B9424 9C0100   MOV EDX,DWORD PTR SS:[
10001A77  .  8D8C24 980000   LEA ECX,DWORD PTR SS:[
10001A7E  .  0FBE0413        MOVSX EAX,BYTE PTR DS:
10001A82  .  50              PUSH EAX
10001A83  .  68 54310010     PUSH Irmonito.10003154
10001A88  .  51              PUSH ECX
10001A89  .  FF15 30200010   CALL DWORD PTR DS:[<&M
10001A8F  .  8B9424 AC0100   MOV EDX,DWORD PTR SS:[
10001A96  .  83C4 0C         ADD ESP,0C
10001A99  .  33C0            XOR EAX,EAX
10001A9B  .  5F              POP EDI
```

```
Registers (
EAX 0000000
ECX 0000000
EDX FFFFFFE
EBX 10001B8
ESP 0006F8A
EBP 0006F8C
ESI 0006F8E
EDI 0000000
EIP 10001A6
C 0  ES 002
```

Address | Hex dump | ASCII

```
0006F8AC  003
0006F8B0  00E
0006F8B4  00E
```

Return Value must be a string

Comment Group - Unmasked

Raytheon
Customer Success Is Our Mission

Comment Decoder

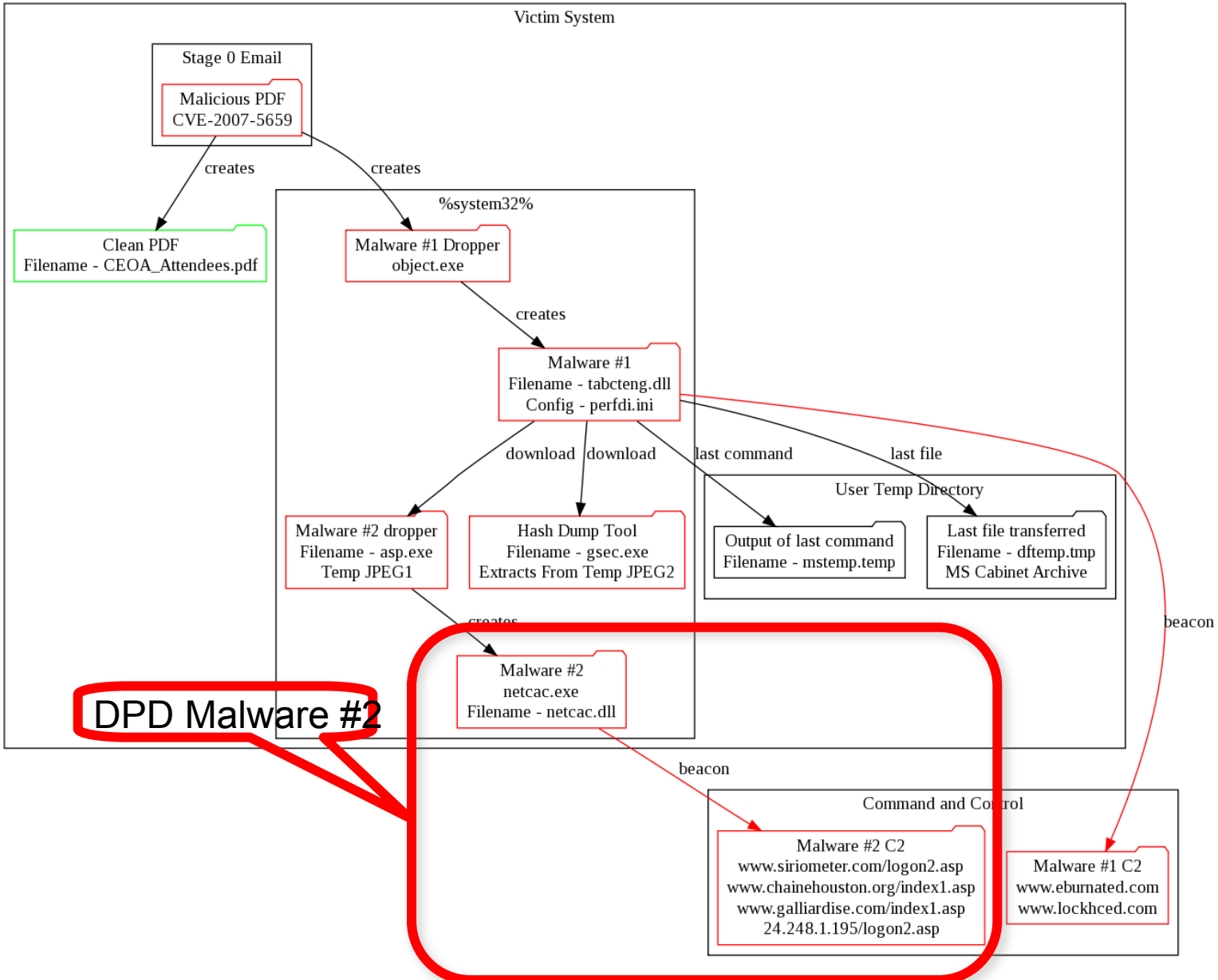
s1	len	s2
/*jgJ-.J	8	sleep:60
wjQ~iY,UnQ[!,hvoZWg	19	210.105.192.222:443
/*jgJ-,F	8	sleep:57
/*jgJ-,G	8	sleep:58
/*jgJ-.'	8	sleep:63
/*jgJ-.J	8	sleep:60
/*jgJ-.S	8	sleep:65
/*jgJ-bAB	9	sleep:240
/*jgJ-mD	8	sleep:46
/*jgJ-mGB	9	sleep:480
/*jgJ-mJ	8	sleep:40
/*jgJ-mS	8	sleep:45
/*jgJ-n'	8	sleep:33
/*jgJ-nDB	9	sleep:360
/*jgJ-nJ	8	sleep:30
/*jgJ-v'/	9	sleep:135
/*jgJ-v;B	9	sleep:120
/*jgJ-vl/	9	sleep:115
wGJ~oYZUntQ!Vjs'ZQ	18	209.208.114.83:443
wjQ~iY,UnQ[!,hmoZWg	19	210.105.192.225:443
/*jgJ-bAB	9	sleep:240
/*jgJ-mS	8	sleep:45
/*jgJ-vJ	8	sleep:10
/*jgJ-,	7	sleep:5

- Total project time – 20 minutes

Case Study #2 – DPD Enigma Machine

Case Study – DPD #2 Overview

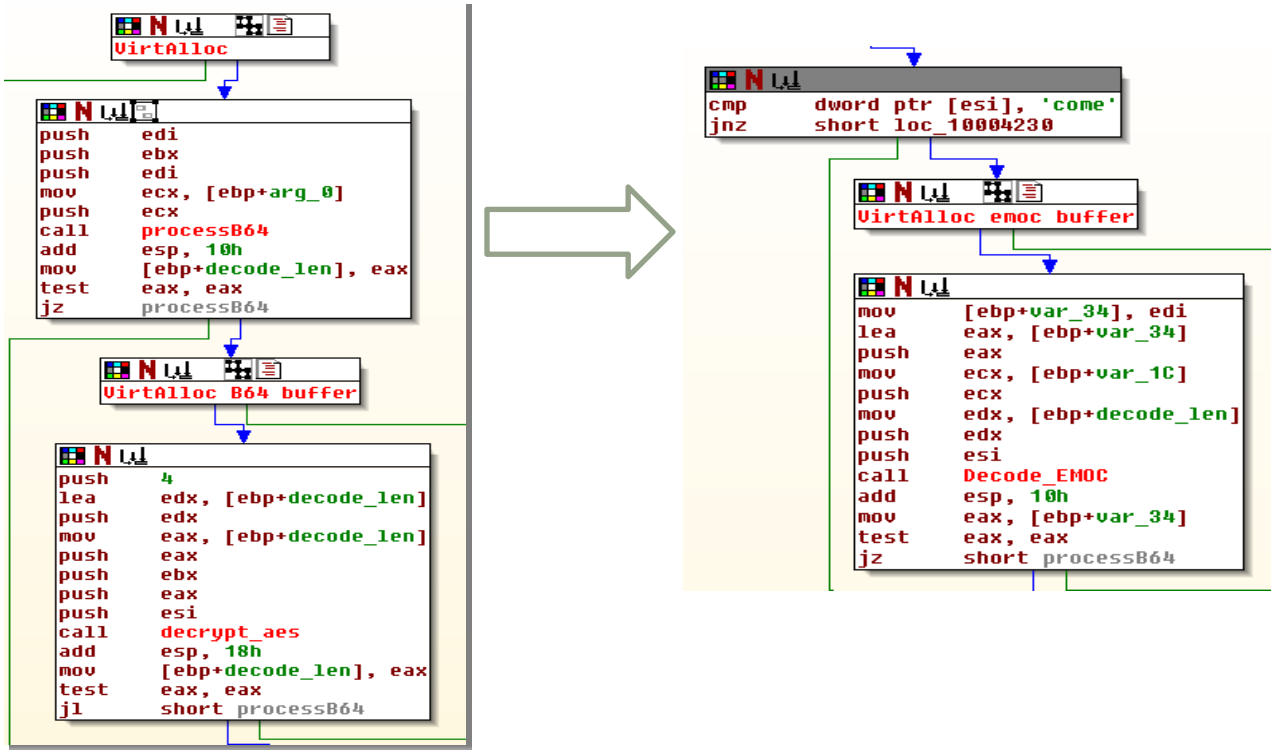
Raytheon
Customer Success Is Our Mission



DPD #2 – Finding the decryptor

Raytheon
Customer Success Is Our Mission

- Malcode uses 3 levels of data modification
  - Base64 encoding with modified alphabet
  - 128-bit AES encryption using Cipher Block Chaining (CBC)
  - Custom compression algorithm (response)



DPD – Complex Decoder

Raytheon
Customer Success Is Our Mission

```
import immlib, binascii, struct

imm = immlib.Debugger()
table = imm.createTable('Netcac Decoder', ['len', 's2'])

fout = open("c:\\output.txt", "w")
fout.write("[*] Starting decryption of encrypted commands\n")
fout.write('*' * 40)
fout.write('\n')
```

DPD – Complex Decoder

```
def main(args):

    init_b64()
    fin = open("c:\\strings.txt", "r")
    data = fin.readlines()

    for line in data:
        line = line.strip()
        (decode,dlen) = b64_decode(line.strip())
        (decode,dlen) = decode_aes(decode,dlen)
        if imm.readString(decode)[:4] == 'emoc':
            decomp(decode,dlen)

    fout.close()
```

```
def init_b64():
    init = 0x10003d20
    imm.setReg('EIP', init)
    imm.runTillRet()
    imm.stepOver()
```

DPD – Complex Decoder

```
def decomp(s, slen):
    imm.setReg('EIP', 0x100087a0)
    temp = imm.readMemory(s+4, 4)
    dlen = struct.unpack('<L', temp)[0] + 0x40
    decode_buffer = imm.remoteVirtualAlloc(dlen)
    ptr_len = imm.remoteVirtualAlloc(4)
    imm.writeLong(ptr_len,dlen)
    regs = imm.getRegs()
    imm.writeLong(regs['ESP']+0x4, s)
    imm.writeLong(regs['ESP']+0x8, slen)
    imm.writeLong(regs['ESP']+0xc, decode_buffer)
    imm.writeLong(regs['ESP']+0x10, ptr_len)
    imm.runTillRet()
    imm.stepOver()
    regs = imm.getRegs()
    decode_len = regs['EAX']
    decode = imm.readMemory(decode_buffer, decode_len)
    table.add('', ['%d' % decode_len, '%s' % decode])
    fout.write(decode)
```

DPD – What we wanted

****

[**] Decrypting command record of length 132

exec cmd.exe /c c:\windows\system32\rar.exe a
c:\windows\system32\crt "\\SERV1\c$\windows\system32\crt"
-inul -m5 -plonglongago

****

Data Collection - Decryption

s1	len	s2
73SVURM@Q2*qFt@HIkF75oPPfAW0DD6fC71IAxGBzajlWDEmu7Kb	80	ef749551133e436fea16df8722417be683cf7c05b40c3e9
∩tòQ‼>Co∩▂▀ç"A(µ▒▀!♣┤♀>ƒ∂ⁿ H♥◀ü=¿σX1&π▥¢╓G╪ZEö)-ü≡▫à┌=	59	exec net use \\EMS_CFG_MGMT\ipc$ nEwJ0bn07 /use
KhhNigpYYjfpWCfClR2sDOHu1ghEx*TCZIXg8YsiS6AcLyUJY30bl	64	2a184d8a0a586237e95827c2951dac0ce1eed60844c7f4c
emoc'	39	The command completed successfully.♪◘♪◘
gDSBMf@xf3rAIb4jalcJAT5N7gKnVux8o8xBt#ePiCWkpy8u*uKP!	64	80348131ffb17f7ac021be236a5709013e4dee02a756ec7
Ç4ü1 ▒▫z└!╡#jW▫0>M€☻♀V∞¦ü╠A╗%Ae%ñ♀/.▪┌Ar]bJ#A╓EL╡┤·ëi	37	exec net use \\EMS_CFG_MGMT\ipc$ /del
6cFy@CiutW1Igod0yTXc5JrweYbZDvyzoosmlxHR0NULSpl8OjMM=	80	e9c172f828aeb56d48828774c935dce49af07986d90efcb
emoc1	49	\\EMS_CFG_MGMT\ipc$ was deleted successfully.♪◘
85WayqI9Jb0Rp*5u4@GoAHj4XxwacqlKnrY2ojfNB7MoTiRdZwjO=	64	f3959acaa97d25bd11a7fe6ee3e1a80078f85f1c1a72a94
≤ôü╧r}%ⁿ◀♀▪n╥ß¿	46	exec cmd /c del c:\windows\system32\com\lb.txt
Ja4CDITUlQuF47r1Zm1onaWRzaC0KmRfEsQAcJeWJgTc4ZLqEKIG=	48	25ae020c84d4950b85e3baf5666d689da591cda0b42a645
emoc♂	14	I am so happy!
0hJ2pFB8Z8s0lbSe7fG0gnj4XxwacqlKnrY2ojfNB7MoTiRdZwjO=	64	d21276a4507c67cb3495b49eedf1b48278f85f1c1a72a94
╥♦vñP¦g╓4ô┤Æ♦±┤ex°_└+rrJ№‖6ô7═·|(N$]g◘┤┤╓└▫A| ═E◘◘0♫	46	exec cmd /c dir c:\windows\system32\com\lb.txt
RXYgeNk9QYbE5WJtiz4UUGNOfPeYn48FliEZsA4YT9@DBL*rcrgh=	208	45762078d93d4186c4e5626d8b3e1450634e7cf7989f8f0
emoc♥0	259	Volume in drive C has no label.♪◘ Volume Seria
U8zUJ789V11fWeAwz4XsEylukqiHmvaBFGLOKd4WlUA.	32	53ccd427bf3d575d5f59e030cf85ec13296e2aa8879af68
S╠ᵇ'┐=W]_Y∝0═à«‼)n*¿çü÷ü¶b╢)▌▂ò@	10	listdrives
hnzZOKGmOnkNZbQLriY1iqlvcG37BMVbv@uyLfe5ZabNjVASb*NCl	80	867cd938a1a63a790d65b40bae26358aa96f706dfb04c55
emocX	88	C:\ DRIVE_FIXED♪D:\ DRIVE_CDROM♪H:\ DRIVE_RE
85WayqI9Jb0Rp*5u4@GoAHj4XxwacqlKnrY2ojfNB7MoTiRdZwjO=	64	f3959acaa97d25bd11a7fe6ee3e1a80078f85f1c1a72a94
≤ôü╧r}%ⁿ◀♀▪n╥ß¿	46	exec cmd /c del c:\windows\system32\com\lb.txt
Ja4CDITUlQuF47r1Zm1onaWRzaC0KmRfEsQAcJeWJgTc4ZLqEKIG=	48	25ae020c84d4950b85e3baf5666d689da591cda0b42a645
emoc♂	14	I am so happy!
0hJ2pFB8Z8s0lbSe7fG0gnj4XxwacqlKnrY2ojfNB7MoTiRdZwjO=	64	d21276a4507c67cb3495b49eedf1b48278f85f1c1a72a94
╥♦vñP¦g╓4ô┤Æ♦±┤ex°_└+rrJ№‖6ô7═·|(N$]g◘┤┤╓└▫A| ═E◘◘0♫	46	exec cmd /c dir c:\windows\system32\com\lb.txt

Additional Ideas

- Streaming Decoder
- Function Fuzzing
- Tracing
- PyDbg / Custom
- PE Strapping

Questions?

matthew.richard@raytheon.com