



BBS-Era Exploitation *for* Fun & Anachronism

Derek Soeder & Paul Mehta

Cylance

June 17, 2016

All materials contained herein are the property of Cylance Inc. ("Cylance") and are protected by United States and international copyright laws. However, certain images have an associated source URL to provide credit to the original source. You may not reproduce, modify, distribute or republish materials contained herein (either directly or by hotlinking) without the prior written permission of Cylance. Inquiries should be directed to legal@cylance.com. You may not alter or remove any trademark, copyright or other notice from copies of content. You may, however, download material from the site for your personal, noncommercial use only. Cylance reserve all rights in and title to all material so downloaded.

All trademarks, service marks, trade names, trade dress, product names and logos appearing in the materials are the property of their respective owners, including in some instances Cylance. Any rights not expressly granted herein are reserved.



THE MODEM ERA

WILDCAT

Wildcat! tm



GOLD ^(C)

THE OPTICAL BBS
COPYRIGHT 1991 the Digital Publishing Company

IS WILD

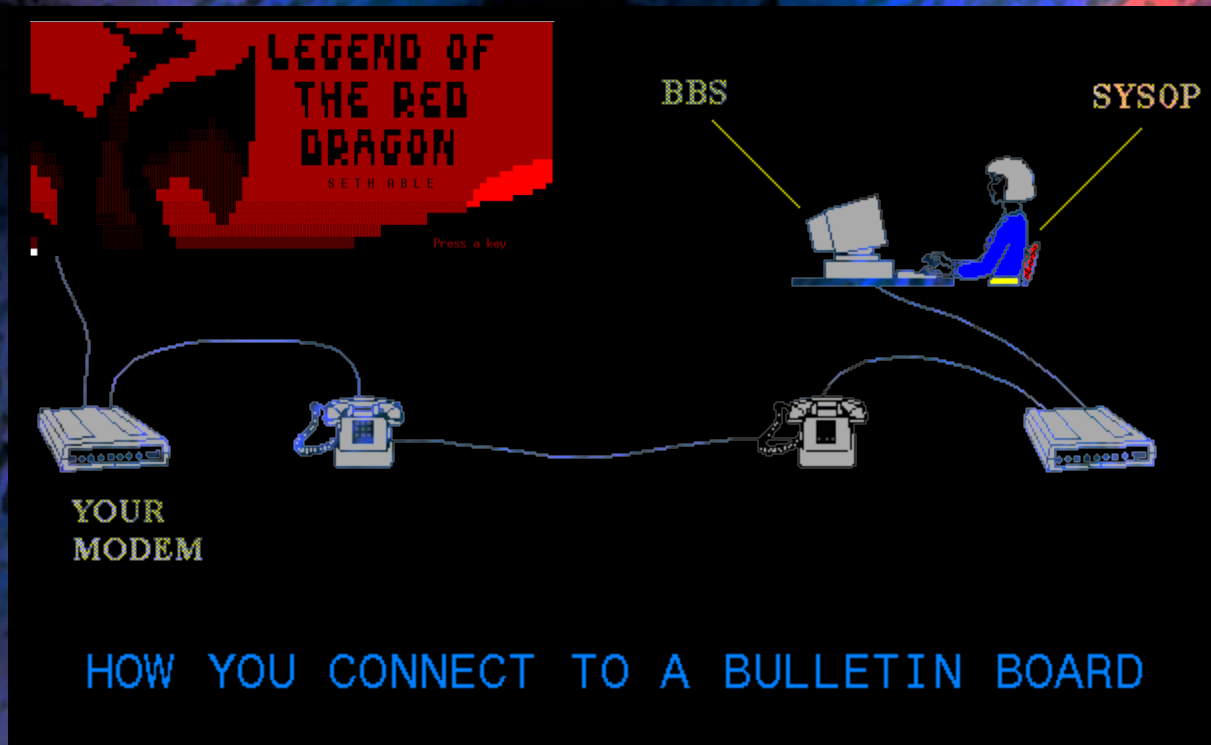
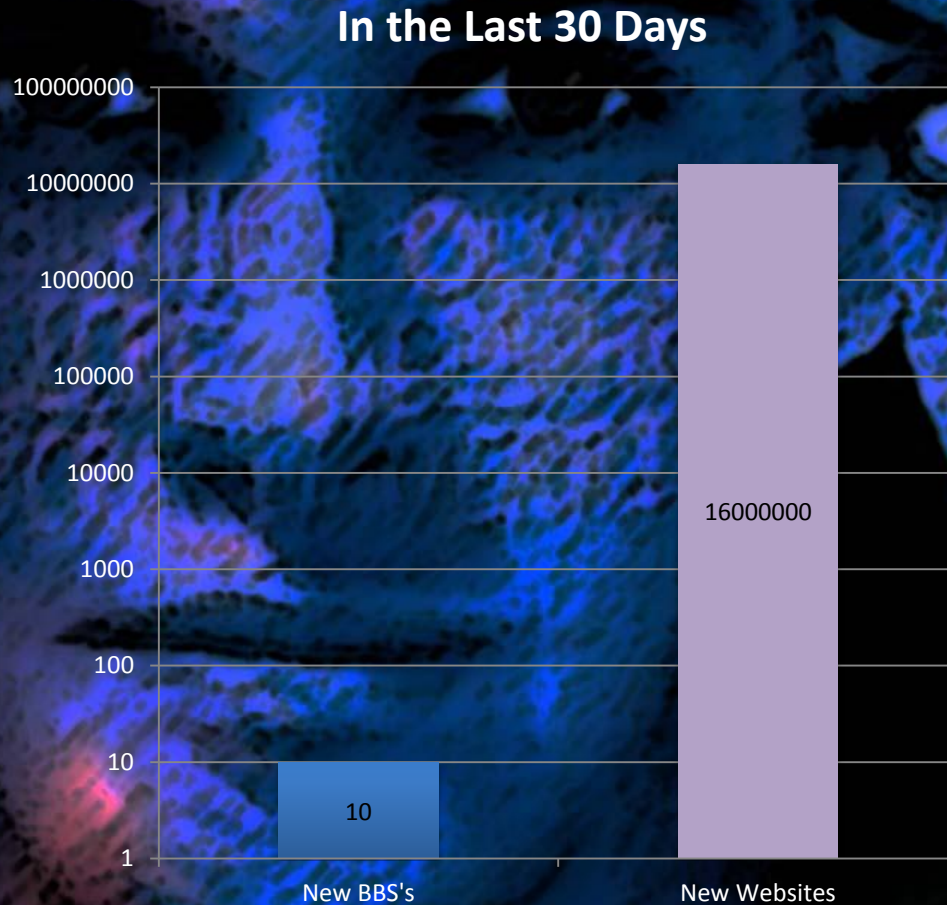


Image sources:

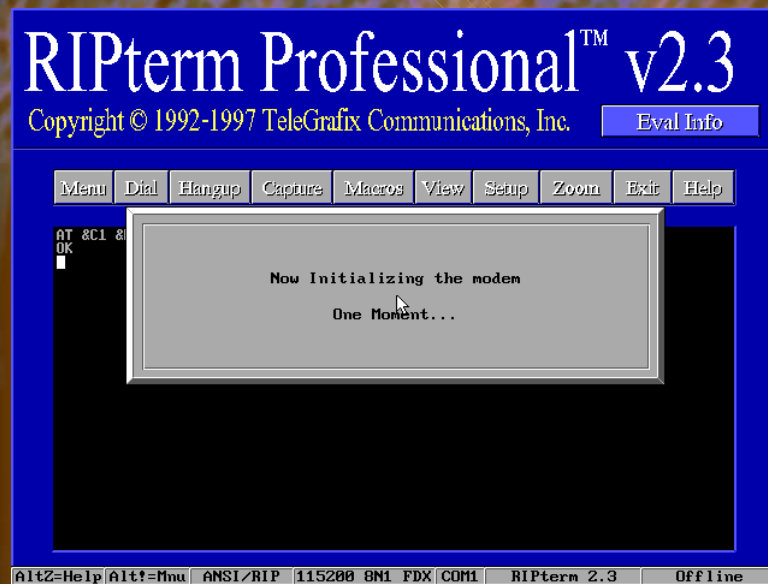
http://barnhard.nl/2014/08/03/before_internet_the_bulletin_board/

<http://www.tigerdroppings.com/rant/gaming/screenshots-from-some-of-your-earliest-gaming-experiences/42888787/page-3/>

Everyone Loves an Underdog...



The logarithmic scale is very misleading here!




Back then...

Booting to DOS from A:
DOS DEBUG.EXE
DOS DEBUG.EXE...
...?
Wardialing, guessing passwords
Stoned boot virus

Today...

VMware, NTVDM, DOSBox
windbg, DOSBox debugger
IDA + decompiler
Procmon
Million-dollar 0-days
AES-256 RSA-4096 ransomware



Meanwhile, in...

THE POSTMODEM ERA

A great leap forward often requires two steps back.

RIPterm: Attack Surface

- Protocols

- Modem ATDT 5551212 NO CARRIER

- TELNET

- ANSI ←[0;31m

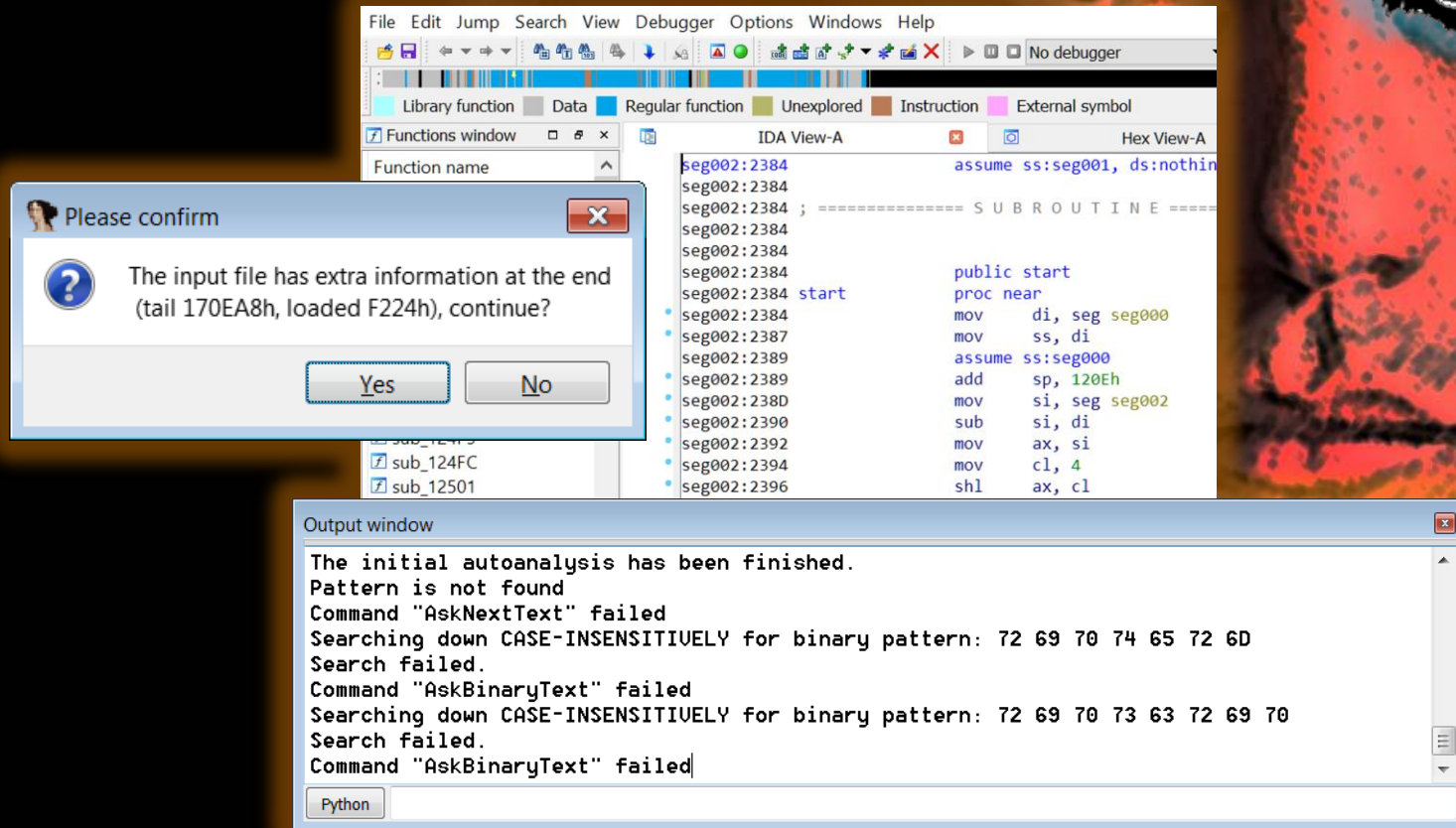
- File transfer

- RIPscrip !|c4|L00004030

- Not a programming script

RIPterm: Reversing

- IDA doesn't understand RIPTERM.EXE



- Reconstitute PE from LE, open in IDA
RIPTERM.EXE: DOS EXE → DOS/4GW → LE
- Dump memory during execution
 - Oldie but goodie



- Dump memory during execution
 - Oldie but goodie

```
03bf01aeaf5c b1 push ecx
03bf01aeaf5d 50 push eax
03bf01aeaf5e 0a mov cl, byte ptr [edx]
03bf01aeaf60 88 mov byte ptr [eax], cl ds:03c7:424241c2=7?
03bf01aeaf62 90 cap cl, 0
03bf01aeaf65 7413 je 01aeaf7a
03bf01aeaf67 8a4a01 mov cl, byte ptr [edx+1]
```

```
sub_1AEAF5C:
push ecx
push eax
mov cl, byte ptr [edx]
mov byte ptr [eax], cl
cmp cl, 0
jz short loc_1AEAF7A
mov [edx+1], cl
add eax, 2
mov [eax+1], cl
add eax, 2
cmp cl, 0
jnz short loc_1AEAF5E
loc_1AEAF7A:
pop eax
pop ecx
retn
sub_1AEAF5C:
endp
```

It's a strcpy!

RIPterm: Attacking

```
DOS/4GW Professional error (2001): exception 06h (invalid opcode) at 200:4141414
1
TSF32: prev_tsf32 80D8
SS      208 DS      208 ES      208 FS      0 GS      270
EAX     32D434 EBX   33333333 ECX   31313131 EDX   309E3C
ESI     53535353 EDI   44444444 EBP   42424242 ESP   309ED4
CS:IP   200:41414141 ID 06 COD   32D434 FLG      246
CS=  200, USE32, page granular, limit FFFFFFFF, base      0, acc CF9A
SS=  208, USE32, page granular, limit FFFFFFFF, base      0, acc CF92
DS=  208, USE32, page granular, limit FFFFFFFF, base      0, acc CF92
ES=  208, USE32, page granular, limit FFFFFFFF, base      0, acc CF92
FS=    0, USE16, byte granular, limit      0, base     16, acc 0
GS=  270, USE16, byte granular, limit    203F, base    99E0, acc 92
CRO: PG:0 ET:1 TS:0 EM:0 MP:0 PE:1  CR2: 0 CR3: 0
```

C:\RIPTERM>

AltZ=Help Alt!=Mnu ANSI/RIP 115200 8N1 FDX COM1 RIPterm 2.3 Online 00:02

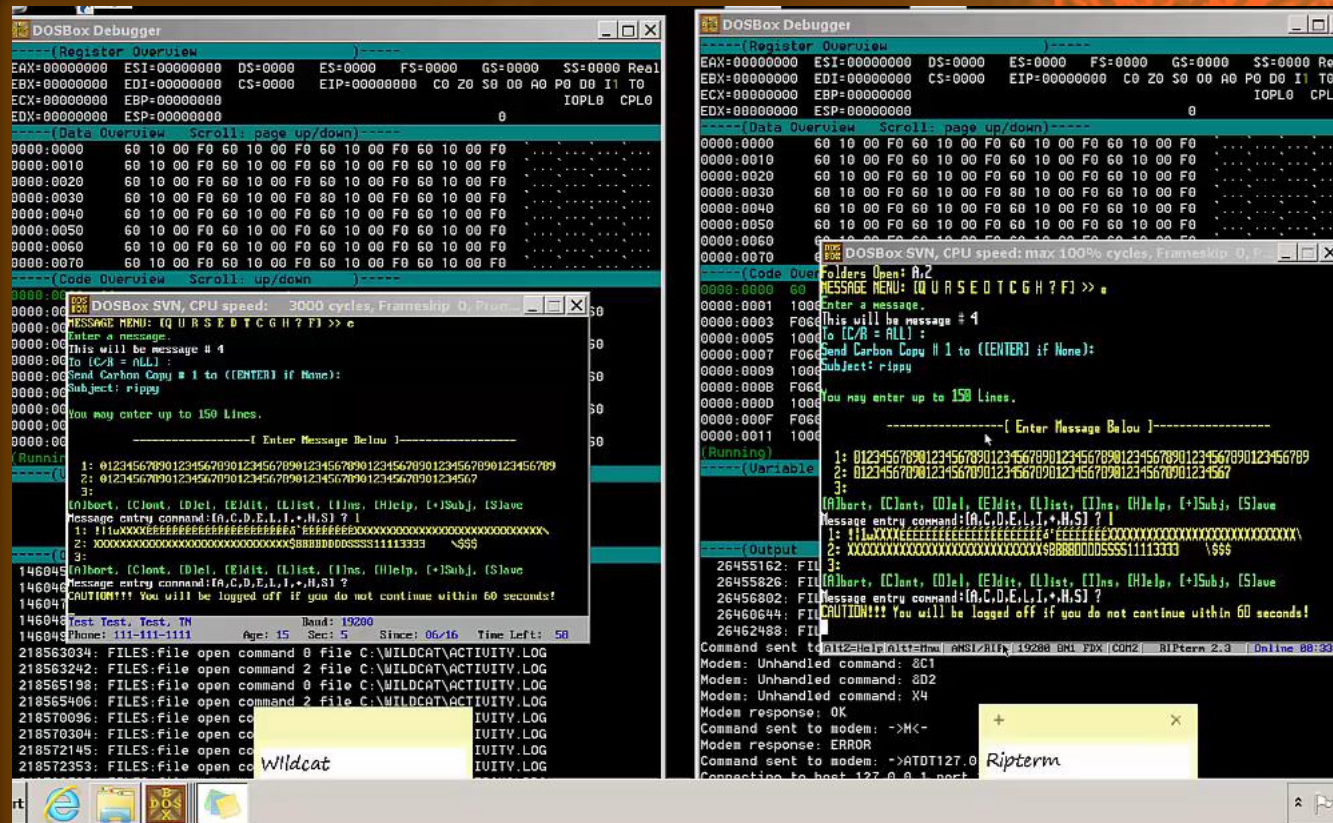
It looks like you're
trying to hack.

Would you like help?

☐ Don't show me
this tip again



RIPpy Demo!



RIPterm: Exploiting

- No DEP (everything is RWX)
- No ASLR
- No SafeSEH
- No GS
- No CFG
- No CET
- No Problem!



RIPterm: Debugging

```
Pid 2296 - WinDbg:6.11.0001.404 X86
File Edit View Debug Window Help
[Icons]
Command
Microsoft (R) Windows Debugger Version 6.11.0001.404 X86
Copyright (c) Microsoft Corporation. All rights reserved.

*** wait with pending attach
Symbol search path is: C:\WebSymbols
Executable search path is:
ModLoad: 0f000000 0f0ad000 C:\WINDOWS\system32\ntvdm.exe
ModLoad: 7c800000 7c8c0000 C:\WINDOWS\system32\ntdll.dll
ModLoad: 77e40000 77f42000 C:\WINDOWS\system32\kernel32.dll
ModLoad: 77f50000 77feb000 C:\WINDOWS\system32\ADVAPI32.dll
ModLoad: 77c50000 77cef000 C:\WINDOWS\system32\RPCRT4.dll
ModLoad: 76f50000 76f63000 C:\WINDOWS\system32\Secur32.dll
ModLoad: 77c00000 77c48000 C:\WINDOWS\system32\GDI32.dll
ModLoad: 77380000 77411000 C:\WINDOWS\system32\USER32.dll
ModLoad: 75e60000 75e87000 C:\WINDOWS\system32\apphelp.dll
ModLoad: 76aa0000 76acd000 C:\WINDOWS\system32\WINMM.dll
ModLoad: 5f090000 5f097000 C:\WINDOWS\system32\NTVDM.DLL
(8f8.d88): Break instruction exception - code 80000003 (first chance)
eax=7ffdf000 ebx=00000001 ecx=00000002 edx=00000003 esi=00000004 edi=00000005
eip=7c81a3e1 esp=01c7ffcc ebp=01c7fff4 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=0038  gs=0000             efl=00000246
ntdll!DbgBreakPoint:             int     3
0:004> sxe av
0:004> g
(8f8.8fc): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=01b46240 ebx=33333333 ecx=31313131 edx=01b19e3c esi=53535353 edi=44444444
eip=41414141 esp=01b19ed4 ebp=42424242 iopl=0         nv up ei pl zr na pe nc
cs=03bf  ss=03c7  ds=03c7  es=03c7  fs=0000  gs=042f             efl=00010246
03bf:41414141 ??                ???

0:000>
Ln 0, Col 0 | Sys 0: <Local> | Proc 000:8f8 | Thrd 000:8fc | ASM | OVR | CAPS | NUM
```

```
DOSBox Debugger
-----
(Register Overview)
EAX=00000000  ESI=00305871  DS=0208  ES=0208  FS=0000  GS=0270  SS=0208  Pr32
EBX=0030E0B9  EDI=00211A34  CS=0200  EIP=00211BBA  C0 Z1 S0 O0 A0 P1 D0 I1 T0
ECX=00000001  EBP=00309FA0
EDX=0031FE68  ESP=00309F9C                                     62130099
-----
(Data Overview) Scroll: page up/down
0200:0000  60 10 00 F0 08 00 70 00 08 00 70 00 08 00 70 00  \....p...p...p...
0200:0010  08 00 70 00 54 FF 00 F0 60 10 00 F0 60 10 00 F0  ..p.I.....
0200:0020  A5 FE 00 F0 87 E9 00 F0 55 FF 00 F0 60 10 00 F0  .....U.....
0200:0030  9E 03 5C 09 60 10 00 F0 80 10 00 F0 60 10 00 F0  \..
0200:0040  20 13 00 F0 20 11 00 F0 40 11 00 F0 60 11 00 F0  .....e.....
0200:0050  C0 11 00 F0 CC 12 DB 05 00 12 00 F0 40 12 00 F0  .....e.....
0200:0060  E0 12 00 F0 E0 12 00 F0 60 12 00 F0 68 11 DB 05  .....h.....
0200:0070  80 12 00 F0 A4 F0 00 F0 60 10 00 F0 8F 05 00 C0  .....h.....
-----
(Code Overview) Scroll: up/down
0200:2AE23E  89DA      mov     edx,ebx
0200:2AE240  4B        dec     ebx
0200:2AE241  85D2      test    edx,edx
0200:2AE243  7E11      jle     002AE256 <$+11>          <down>
0200:2AE245  8B54240C  mov     edx,[esp+000C]
0200:2AE249  40        inc     eax
0200:2AE24A  658A12    mov     dl,gs:[edx]              [illegal]
0200:2AE24D  FF44240C  inc     dword [esp+000C]
0200:2AE251  8B50FF    mov     [eax-0001],dl            [illegal]
0200:2AE254  EBE8      jmp     short 002AE23E <$-18>    <up>
I->
-----
(Variable Overview)
-----
(Output) Scroll: home/end
IU [seg]:[off] [name] - Create var name for memory address.
SV [filename] - Save var list in file.
LV [filename] - Load var list from file.
ADDLOG [message] - Add message to the log file.
MEMDUMP [seg]:[off] [len] - Write memory to file memdump.txt.
MEMDUMPBIN [sl]:[ol] [len] - Write memory to file memdump.bin.
SELINFO [segName] - Show selector info.
INTVEC [filename] - Writes interrupt vector table to file.
INTHAND [intNum] - Set code view to interrupt handler.
CPU - Display CPU status information.
GDT - Lists descriptors of the GDT.
LDT - Lists descriptors of the LDT.
IDT - Lists descriptors of the IDT.
PAGING [page] - Display content of page table.
EXTEND - Toggle additional info.
TIMERIRQ - Run the system timer.
HELP - Help
```


Wildcat: Attack Surface

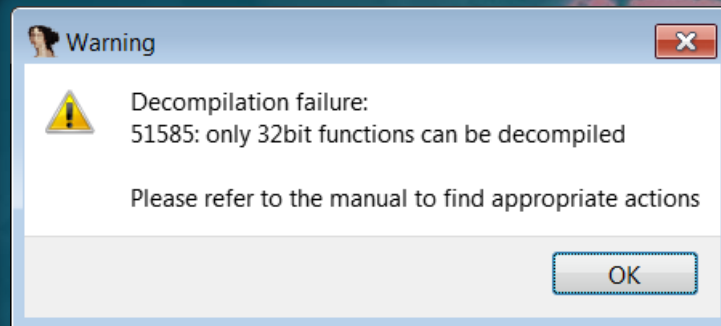


Wildcat: Reversing

- FLIRT works great:

```
our016:1619 loc_57579:                                ; CODE XREF: sub_574D3+78↑j  
our016:1619                                ; sub_574D3+7C↑j ...  
our016:1619      mov     ax, 310  
our016:161C      push    ax  
our016:161D      call   @GetMem$q4Word ; GetMem(var p: Pointer{DX:AX}; size: Word)  
our016:1622      mov     word ptr [bp+var_1F8], ax  
our016:1626      mov     word ptr [bp+var_1F8+2], dx  
our016:162A      mov     ax, 12231 ; = 151 * 81  
our016:162D      push    ax  
our016:162E      call   @GetMem$q4Word ; GetMem(var p: Pointer{DX:AX}; size: Word)  
our016:1633      mov     word ptr dword_29A68, ax  
our016:1636      mov     word ptr dword_29A68+2, dx  
our016:163A      mov     [bp+var_A8], 1  
our016:1640      jmp     short loc_575A6  
our016:1642 ; loc_575A2  
our016:1685 ...  
our016:1685      mov     [bp+var_A8], 1  
our016:168B      mov     [bp+var_1FE], 0  
our016:1690      lea     di, [bp+var_31E]  
our016:1694      push    ss  
our016:1695      push    di  
our016:1696      call   sub_1D24A  
our016:169B      mov     di, offset aEnterAMessage_ ; "Enter a message."  
our016:169E      push    cs  
our016:169F      push    di  
our016:16A0      call   @Concat$qm6Stringt1 ; Concat(dst, src: String): String
```

- Decompiler does not:



Wildcat: Attacking



Wildcat: Attacking



Wildcat: Attacking

E nter Message	U pdate Folder	? Command Help
T ext Search	D elete Message	G oodbye
S can Messages	F ile Area	[Icon] Not Used.

You have been on for 4 minutes, with 56 remaining for this call.
Folders Open: A,B,C,D,E,F,G,H,I,J,K,L,M,N,O,P,Q,R,S,T,Y,Z
MESSAGE MENU: [Q U R S E D T C G H ? F] >> e
Enter a message.
This will be message # 6
To [C/R = ALL] :
Send Carbon Copy # 1 to ([ENTER] if None):
Subject: pwn3d fr0m t3h fu7ur3

You may enter up to 150 lines.

-----[Enter Message Below]-----

1:
[A]bort, [C]ont, [D]el, [E]dit, [L]ist, [I]ns, [H]elp, [+]
Message entry command:[A,C,D,E,L,I,+,H,?] i
Begin inserting at which Line Number 12345
12345: _

The background of the slide features two close-up portraits of human faces. The face on the left is predominantly blue with red highlights, while the face on the right is predominantly red with blue highlights. The text is overlaid on the central area between the two faces.

Questions?

first initial last name @ cylance.com