CATCH ME IF YOU CAN

HUNTER
HUNTED
and HAUNTED

CYPHORT™

YOUR HUNTER TODAY

Marion Marschalek

CYPHORT.

ANALYST

aims to detect

MALWARE

MALWARE

aims to detect

ANALYST

CYPHORT

LEVELS of SOPHISTICATION

Mass Malware

Sophisticated Malware

Toolified Malware

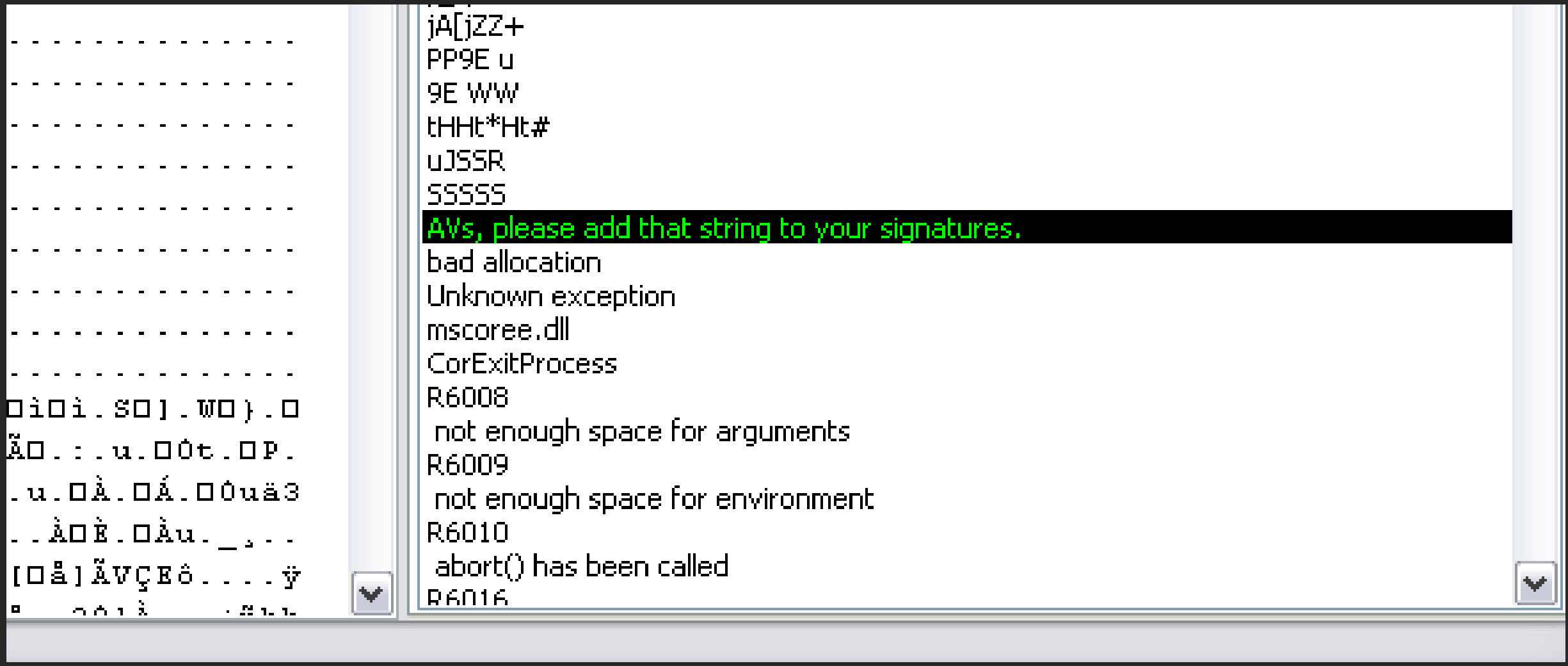
APT Malware

aAPT Malware

EPT Malware

?

CYPHORT



while some are not all that sophisticated ....

CYPHORT

SIMULATION

VIRTUALIZATION

STATIC ANALYSIS

DISASSEMBLING

DEBUGGING

ARTIFICIAL INTELLIGENCE

CYPHORT

SIMULATION

VIRTUALIZATION

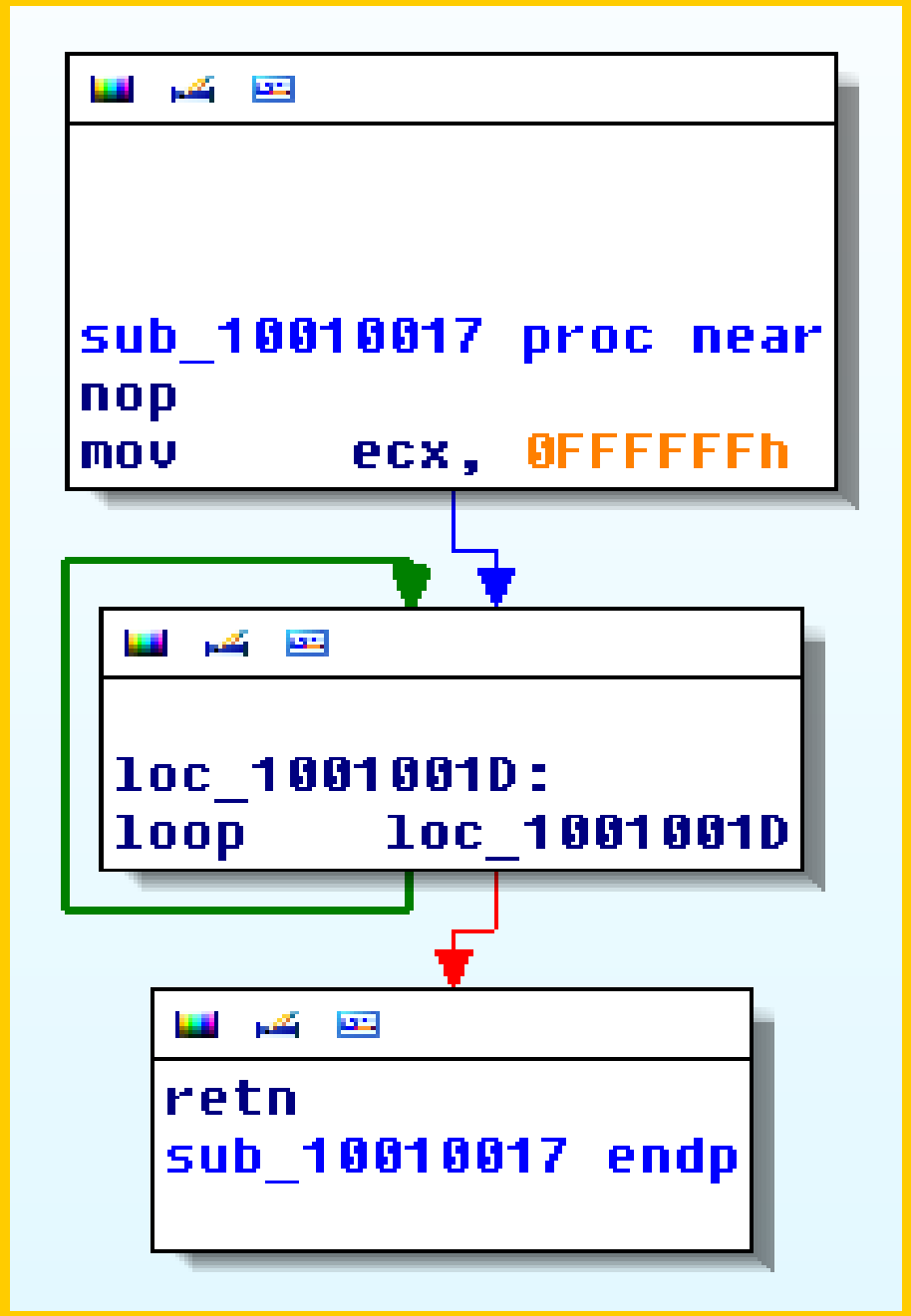
STATIC ANALYSIS

DISASSEMBLING

DEBUGGING

ARTIFICIAL

INTELLIGENCE



CYPHORT

SIMULATION

VIRTUALIZATION

STATIC ANALYSIS

DISASSEMBLING

DEBUGGING

ARTIFICIAL

INTELLIGENCE

```
2:003F2610 mov     [ebp+var_44], 'V'
2:003F2614 mov     [ebp+var_43], 'B'
2:003F2618 mov     [ebp+var_42], 'o'
2:003F261C mov     [ebp+var_41], 'x'
2:003F2620 mov     [ebp+var_40], 'S'
2:003F2624 mov     [ebp+var_3F], 'e'
2:003F2628 mov     [ebp+var_3E], 'r'
2:003F262C mov     [ebp+var_3D], 'v'
2:003F2630 mov     [ebp+var_3C], 'i'
2:003F2634 mov     [ebp+var_3B], 'c'
2:003F2638 mov     [ebp+var_3A], 'e'
2:003F263C mov     [ebp+var_39], '.'
2:003F2640 mov     [ebp+var_38], 'e'
2:003F2644 mov     [ebp+var_37], 'x'
2:003F2648 mov     [ebp+var_36], 'e'
2:003F264C mov     [ebp+var_35], bl
2:003F264F mov     byte ptr [ebp+var_2C], 'v'
2:003F2653 mov     byte ptr [ebp+var_2C+1], 'm'
2:003F2657 mov     byte ptr [ebp+var_2C+2], 't'
2:003F265B mov     byte ptr [ebp+var_2C+3], 'o'
2:003F265F mov     byte ptr [ebp+var_28], 'o'
2:003F2663 mov     byte ptr [ebp+var_28+1], 'l'
2:003F2667 mov     byte ptr [ebp+var_26], 's'
2:003F266B mov     byte ptr [ebp+var_26+1], 'd'
2:003F266F mov     byte ptr [ebp+var_24], '.'
2:003F2673 mov     byte ptr [ebp+var_24+1], 'e'
2:003F2677 mov     byte ptr [ebp+var_22], 'x'
2:003F267B mov     byte ptr [ebp+var_22+1], 'e'
2:003F267F mov     byte ptr [ebp+var_20], bl
```

CYPHORT

SIMULATION

VIRTUALIZATION

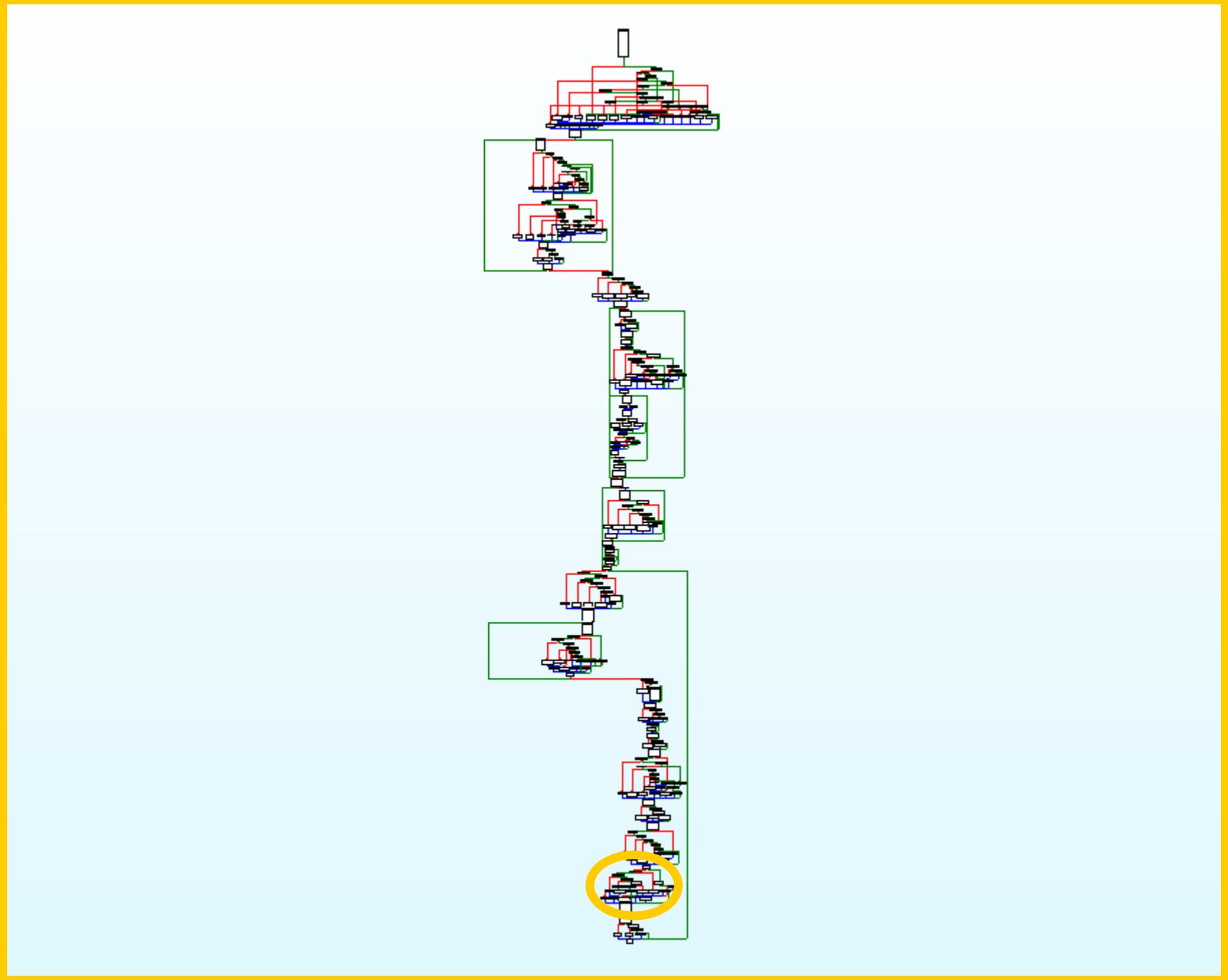
STATIC ANALYSIS

DISASSEMBLING

DEBUGGING

ARTIFICIAL

INTELLIGENCE



CYPHORT

SIMULATION

VIRTUALIZATION

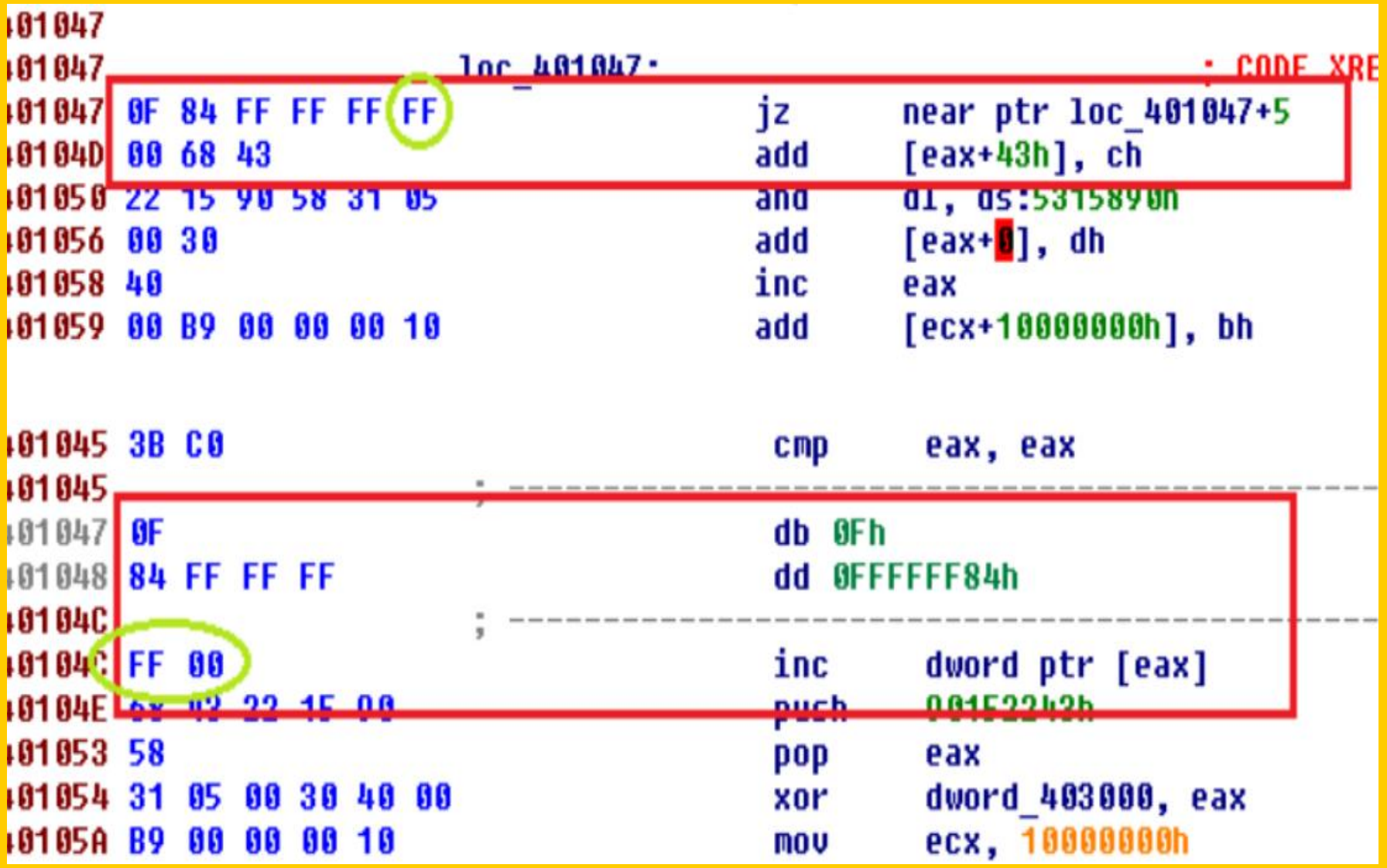
STATIC ANALYSIS

DISASSEMBLING

DEBUGGING

ARTIFICIAL

INTELLIGENCE



CYPHORT

SIMULATION

VIRTUALIZATION

STATIC ANALYSIS

DISASSEMBLING

DEBUGGING

ARTIFICIAL

INTELLIGENCE

```
00401C80 push    ebp
00401C81 mov     ebp, esp
00401C83 push    0FFFFFFFFh
00401C85 push    offset _WinMain@16_SEH
00401C8A mov     eax, large fs:0
00401C90 push    eax
00401C91 mov     large fs:0, esp
00401C98 sub     esp, 24h
```

...

```
00401D98
00401D98 loc_401D98:
00401D98 mov     ecx, 69805h
00401D9D call    ecx
00401D9F mov     eax, 69805h
00401DA4 mov     ecx, [ebp+__$EHRec$.pNext]
00401DA7 mov     large fs:0, ecx
00401DAE pop     edi
00401DAF pop     esi
00401DB0 pop     ebx
00401DB1 mov     esp, ebp
00401DB3 pop     ebp
00401DB4 retn    10h
```

CYPHORT

SIMULATION

VIRTUALIZATION

STATIC ANALYSIS

DISASSEMBLING

DEBUGGING

ARTIFICIAL

INTELLIGENCE

CYPHORT

THE ANCIENT ART OF BYPASSING ANTI-ANALYSIS

CYPHORT

PEBBeingDebugged Flag: IsDebuggerPresent()

PEBNtGlobalFlag, Heap Flags

DebugPort: CheckRemoteDebuggerPresent() / NtQueryInformationProcess()

Debugger Interrupts

Timing Checks

SeDebugPrivilege

Parent Process

DebugObject: NtQueryObject()

Debugger Window

Debugger Process

Device Drivers

OllyDbg: Guard Pages

Software Breakpoint Detection

Hardware Breakpoint Detection

Patching Detection via Code Checksum Calculation

Encryption and Compression

Garbage Code and Code Permutation

Anti-Disassembly

Misdirection and Stopping Execution via Exceptions

Blocking Input

ThreadHideFromDebugger

Disabling Breakpoints

Unhandled Exception Filter

OllyDbg: OutputDebugString() Format String Bug

Process Injection

Debugger Blocker

TLS Callbacks

Stolen Bytes

API Redirection

Multi-Threaded Packers

Virtual Machines

THE AWESOMENESS COMPILATION

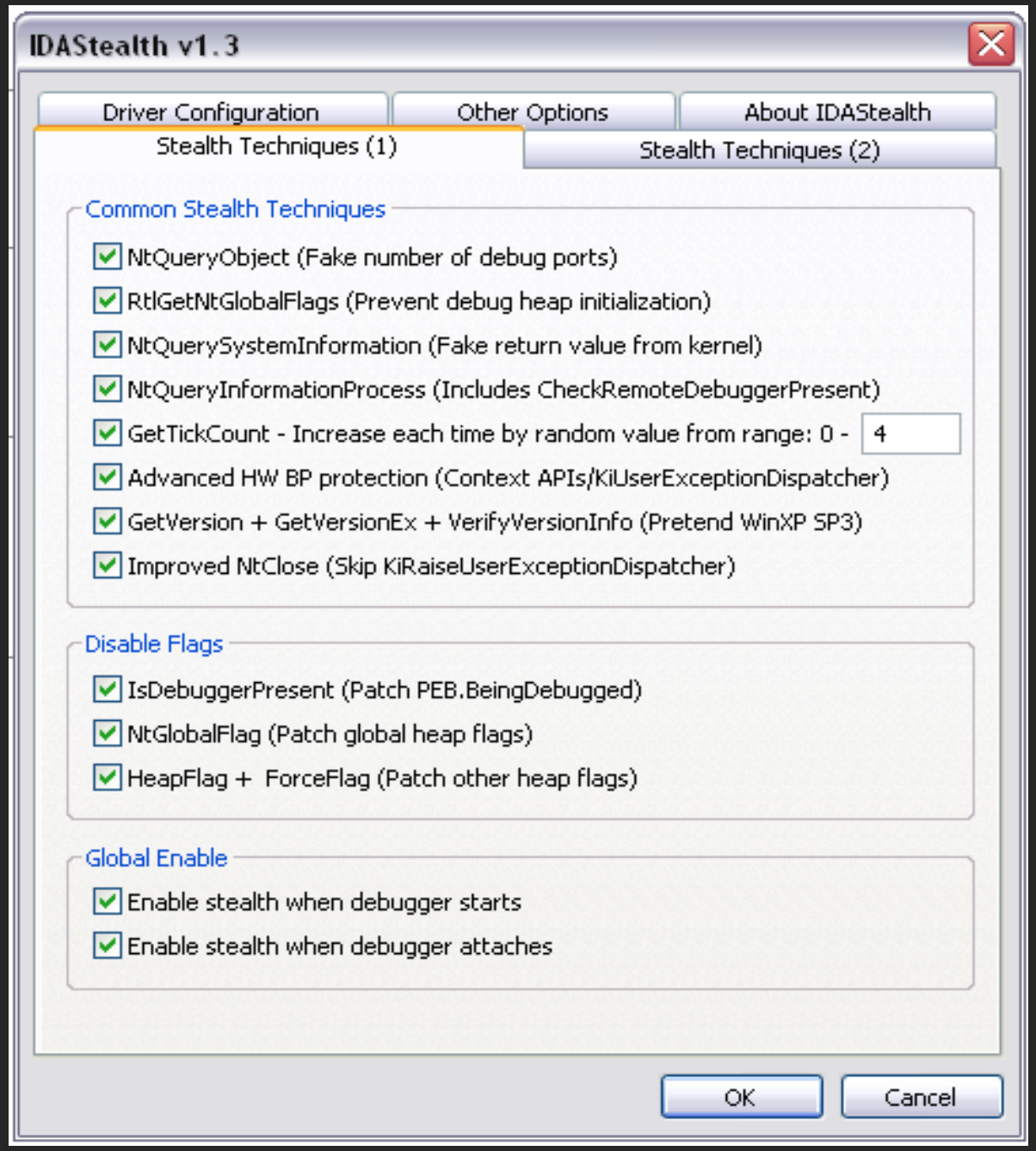
THE „ULTIMATE“ ANTI-DEBUGGING REFERENCE [Ferrie]
http://pferrie.host22.com/papers/antidebug.pdf

THE ART OF UNPACKING [Yason]
https://www.blackhat.com/presentations/bh-usa-07/Yason/Whitepaper/bh-usa-07-yason-WP.pdf

SCIENTIFIC BUT NOT ACADEMICAL OVERVIEW OF MALWARE ANTI-DEBUGGING, ANTI-DEBUGGING AND ANTI-VM TECHNIQUES [Branco, Barbosa, Neto]
http://research.dissect.pe/docs/blackhat2012-paper.pdf

VIRTUAL MACHINE DETECTION ENHANCED [Rin, EP_X0FF]
http://www.heise.de/security/downloads/07/1/1/8/3/5/5/9/vmde.pdf

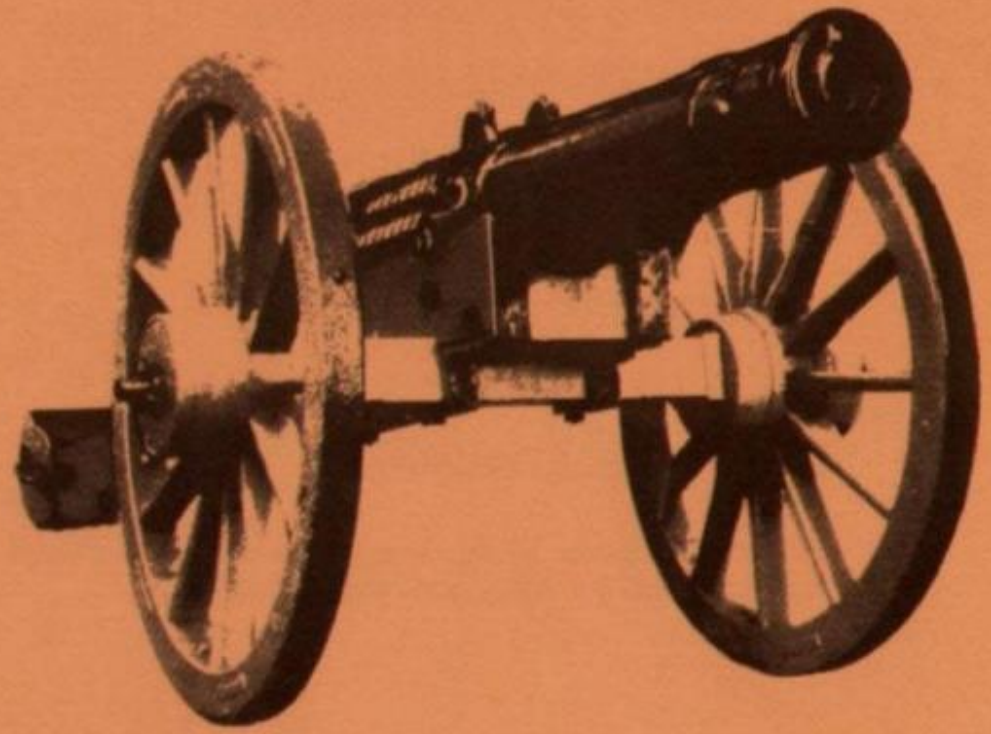
AWESOMENESS IMPLEMENTED



CYPHORT

080	NRWConfig.exe	1364	RegOpenKey	HKCU\Software\Policies\Microsoft\Control Panel\Desktop	NAME NOT FOUND	Desired Access: Read
21	NRWConfig.exe	1364	RegOpenKey	HKCU\Control Panel\Desktop	SUCCESS	Desired Access: Read
570	NRWConfig.exe	1364	RegQueryValue	HKCU\Control Panel\Desktop\MultiUILanguageId	NAME NOT FOUND	Length: 256
843	NRWConfig.exe	1364	RegCloseKey	HKCU\Control Panel\Desktop	SUCCESS	
960	NRWConfig.exe	1364	RegCloseKey	HKCU	SUCCESS	
220	NRWConfig.exe	1364	CreateFile	C:\WINDOWS\system32\comctl32.dll	SUCCESS	Desired Access: Gene
536	NRWConfig.exe	1364	CreateFileMapp...	C:\WINDOWS\system32\comctl32.dll	SUCCESS	SyncType: SyncTypeE
550	NRWConfig.exe	1364	QueryStandardI...	C:\WINDOWS\system32\comctl32.dll	SUCCESS	AllocationSize: 618.4S
871	NRWConfig.exe	1364	CreateFileMapp...	C:\WINDOWS\system32\comctl32.dll	SUCCESS	SyncType: SyncTypeE
790	NRWConfig.exe	1364	CreateFile	C:\WINDOWS\system32\comctl32.dll.124.Manifest	NAME NOT FOUND	Desired Access: Gene
573	NRWConfig.exe	1364	CreateFile	C:\WINDOWS\system32\comctl32.dll.124.Config	NAME NOT FOUND	Desired Access: Gene
808	NRWConfig.exe	1364	CloseFile	C:\WINDOWS\system32\comctl32.dll	SUCCESS	
415	NRWConfig.exe	1364	RegOpenKey	HKCU	SUCCESS	Desired Access: Read
733	NRWConfig.exe	1364	RegOpenKey	HKCU\Control Panel\Desktop	SUCCESS	Desired Access: Read
015	NRWConfig.exe	1364	RegQueryValue	HKCU\Control Panel\Desktop\SmoothScroll	NAME NOT FOUND	Length: 144
228	NRWConfig.exe	1364	RegCloseKey	HKCU\Control Panel\Desktop	SUCCESS	
510	NRWConfig.exe	1364	RegCloseKey	HKCU	SUCCESS	
806	NRWConfig.exe	1364	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\WS2HELP.dll	NAME NOT FOUND	Desired Access: Read
999	NRWConfig.exe	1364	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\WS2_32.dll	NAME NOT FOUND	Desired Access: Read
809	NRWConfig.exe	1364	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\HideDebugger.dll	NAME NOT FOUND	Desired Access: Read
572	NRWConfig.exe	1364	ReadFile	C:\Program Files\IDA\plugins\HideDebugger.dll	SUCCESS	Offset: 99.328, Length
265	NRWConfig.exe	1364	ReadFile	C:\Program Files\IDA\plugins\HideDebugger.dll	SUCCESS	Offset: 132.096, Leng
512	NRWConfig.exe	1364	ReadFile	C:\Program Files\IDA\plugins\HideDebugger.dll	SUCCESS	Offset: 66.560, Length
847	NRWConfig.exe	1364	ReadFile	C:\Program Files\IDA\plugins\HideDebugger.dll	SUCCESS	Offset: 168.960, Leng
580	NRWConfig.exe	1364	ReadFile	C:\Program Files\IDA\plugins\HideDebugger.dll	SUCCESS	Offset: 201.728, Leng
936	NRWConfig.exe	1364	ReadFile	C:\Program Files\IDA\plugins\HideDebugger.dll	SUCCESS	Offset: 33.792, Length
818	NRWConfig.exe	1364	RegOpenKey	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters	SUCCESS	Desired Access: Maxi
416	NRWConfig.exe	1364	RegQueryValue	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\WinSock_Registry_Version	SUCCESS	Type: REG_SZ, Leng
712	NRWConfig.exe	1364	RegQueryValue	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\WinSock_Registry_Version	SUCCESS	Type: REG_SZ, Leng
956	NRWConfig.exe	1364	RegOpenKey	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9	SUCCESS	Desired Access: Maxi
204	NRWConfig.exe	1364	RegQueryValue	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Serial_Access_Num	SUCCESS	Type: REG_DWORD,
508	NRWConfig.exe	1364	RegQueryValue	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Serial_Access_Num	SUCCESS	Type: REG_DWORD,
804	NRWConfig.exe	1364	RegOpenKey	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\00000005	NAME NOT FOUND	Desired Access: Maxi
005	NRWConfig.exe	1364	RegQueryValue	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Next_Catalog_Ent...	SUCCESS	Type: REG_DWORD,
094	NRWConfig.exe	1364	RegQueryValue	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Num_Catalog_Ent...	SUCCESS	Type: REG_DWORD,
087	NRWConfig.exe	1364	RegOpenKey	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries	SUCCESS	Desired Access: Maxi
226	NRWConfig.exe	1364	RegOpenKey	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\0	SUCCESS	Desired Access: Read

AC/DC



FOR THOSE ABOUT TO ROCK

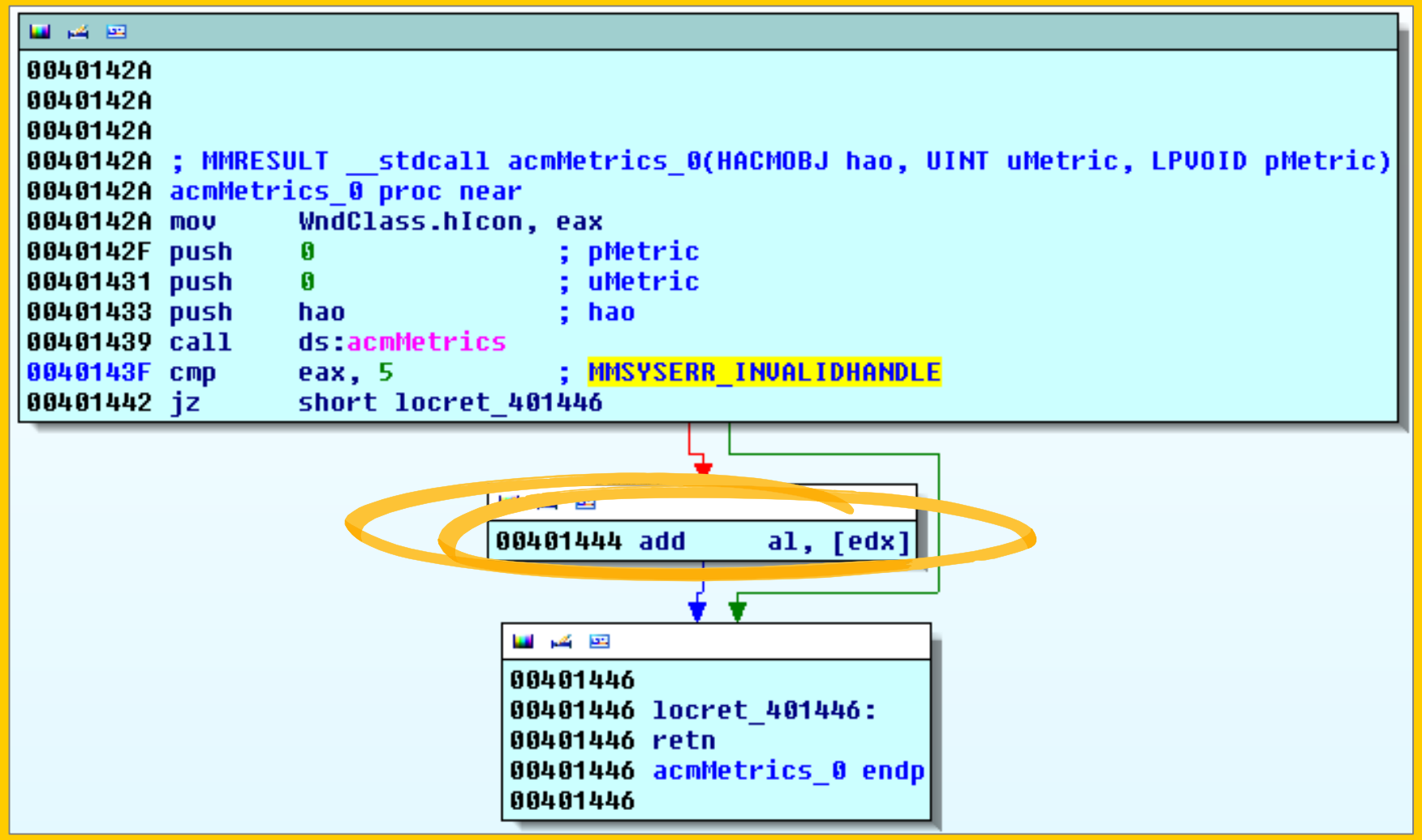
CYPHORT™

UPATRE

SMALL | NASTY | THORNY | standardmalwareofftheshelf

CYPHORT

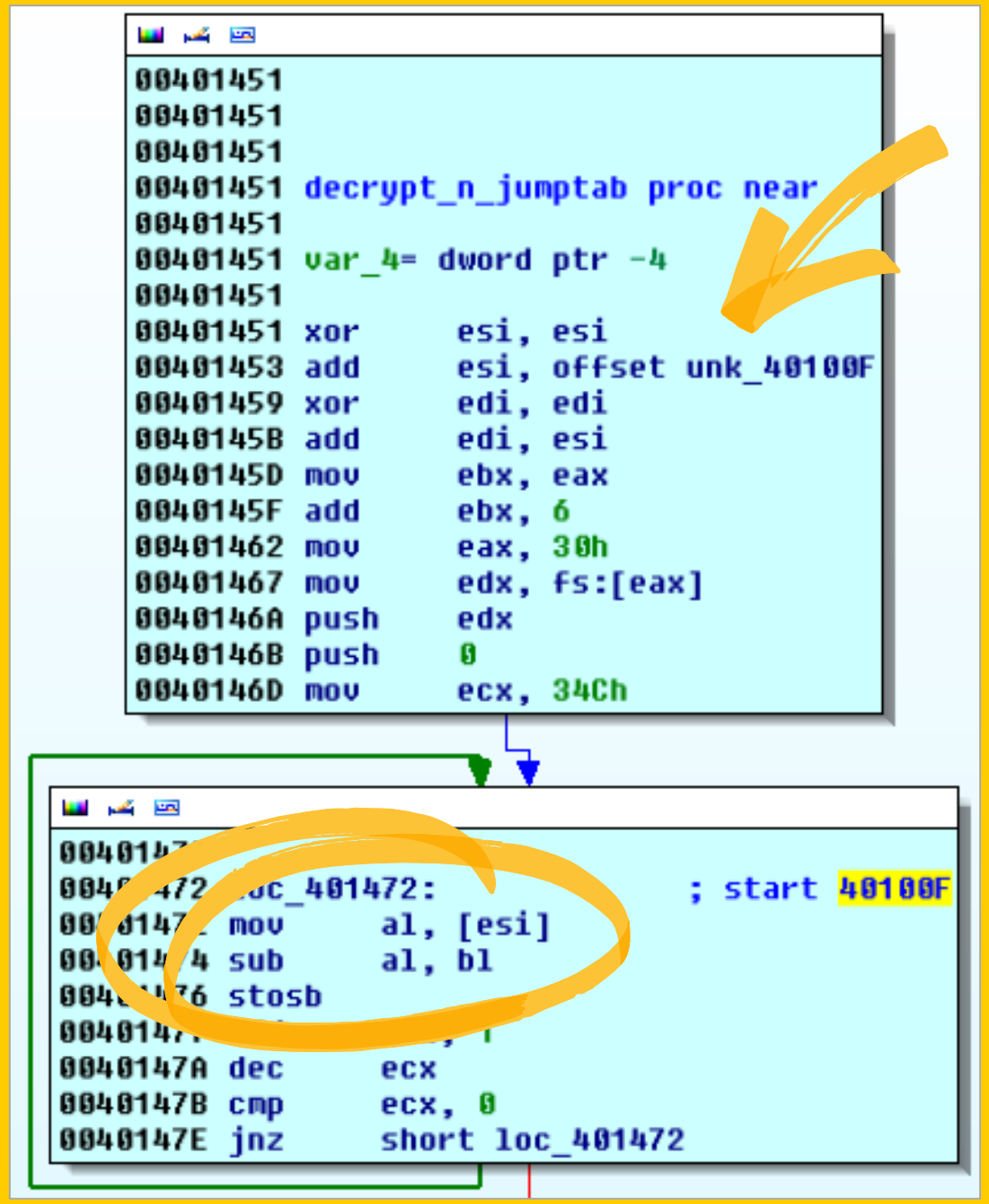
ANTI-SIMULATION



CYPHORT

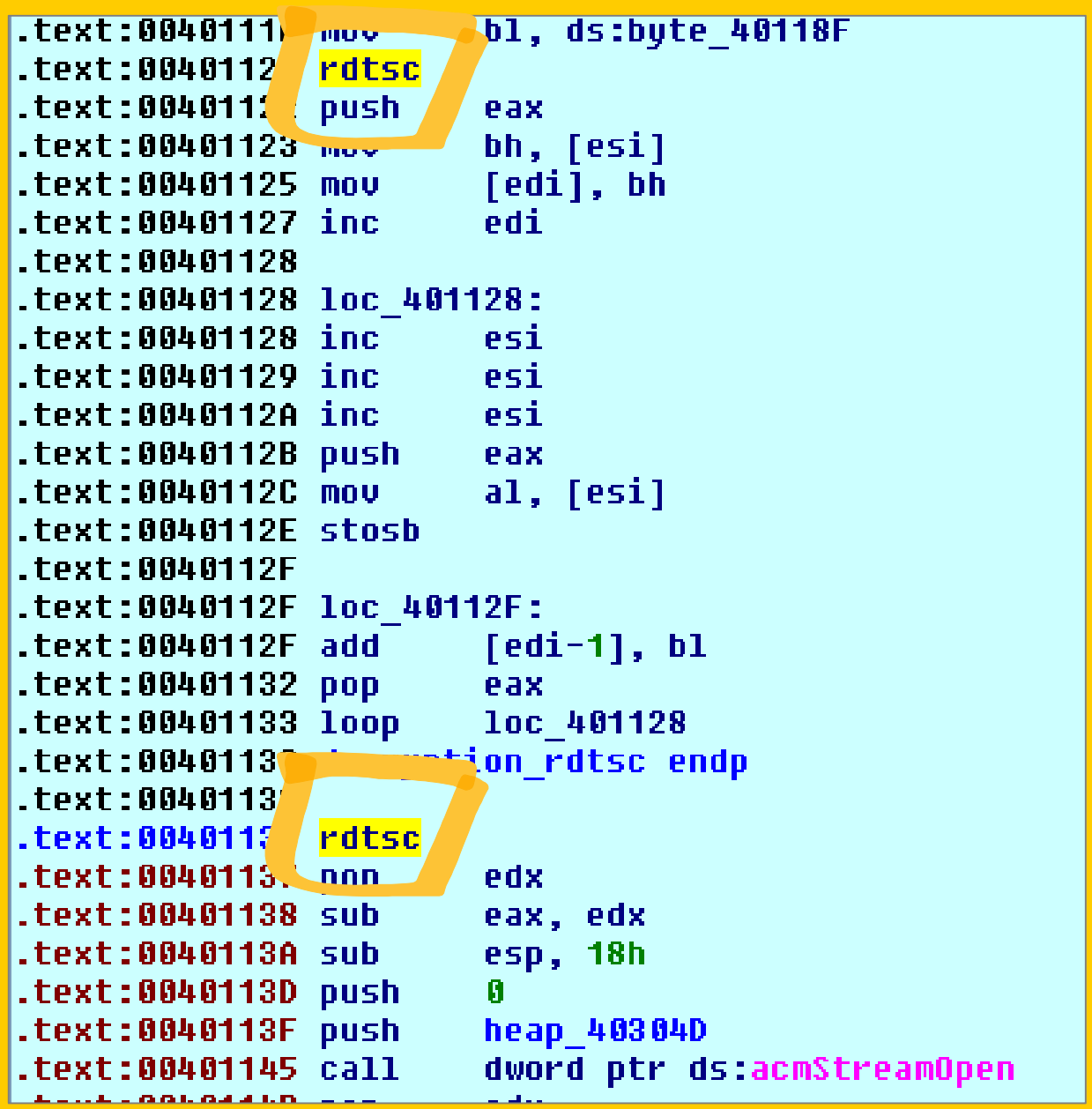
WINDOW CONFUSION

and implicit breakpoint detection



CYPHORT

WANNABE TIMING DEFENCE



CYPHORT

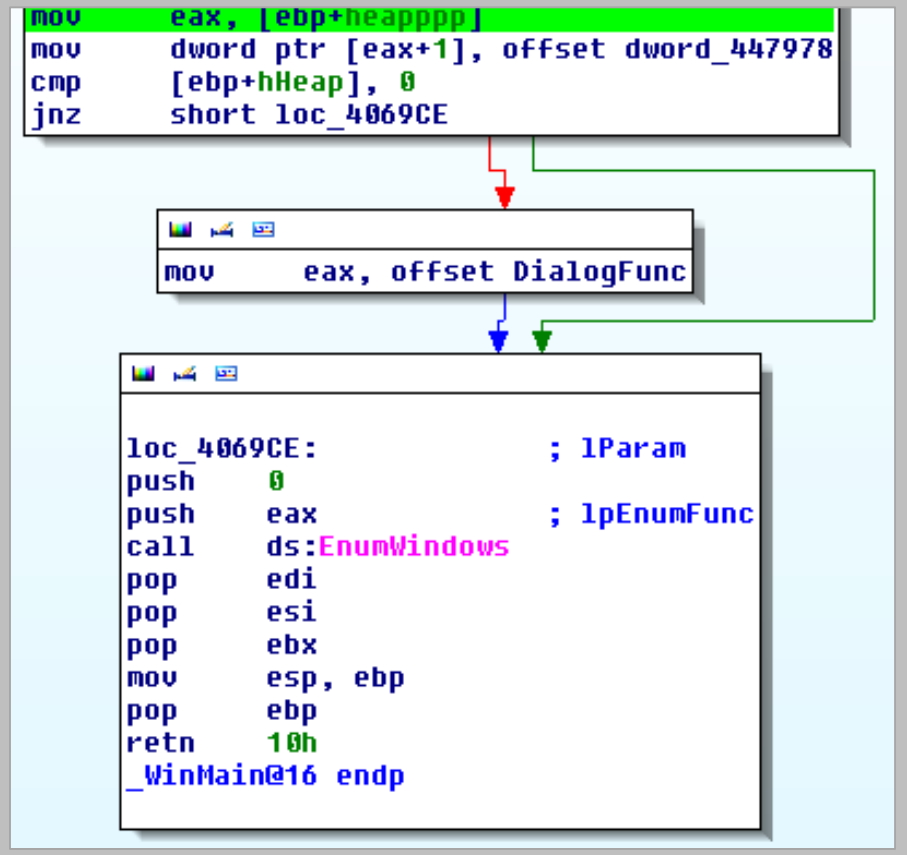
CITADEL

IDA Stealth Bruteforcing

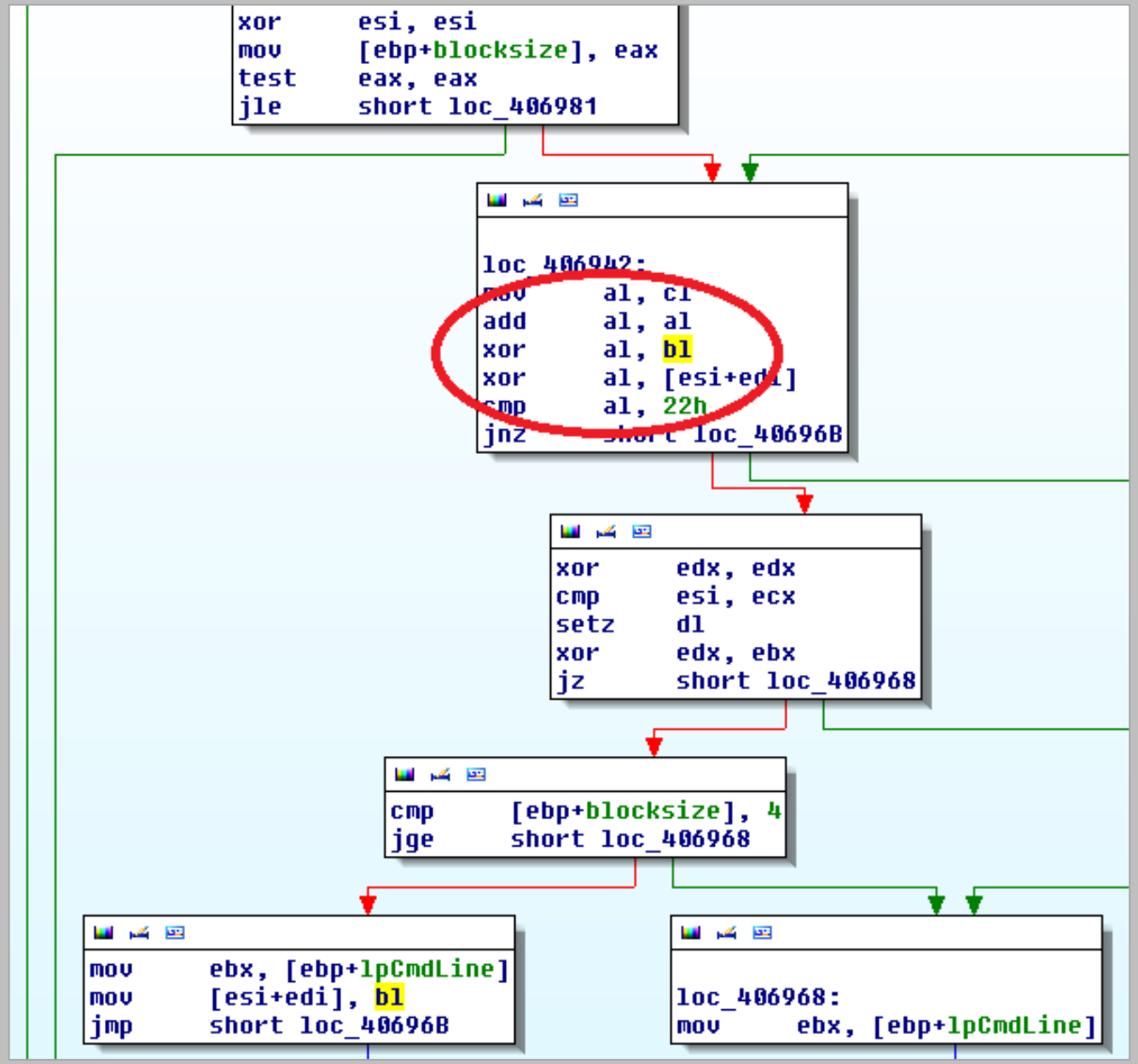
PEB!NtGlobalFlags Anti-debug r.e.d.a.c.t.e.d.

Let‘s start at the end .....

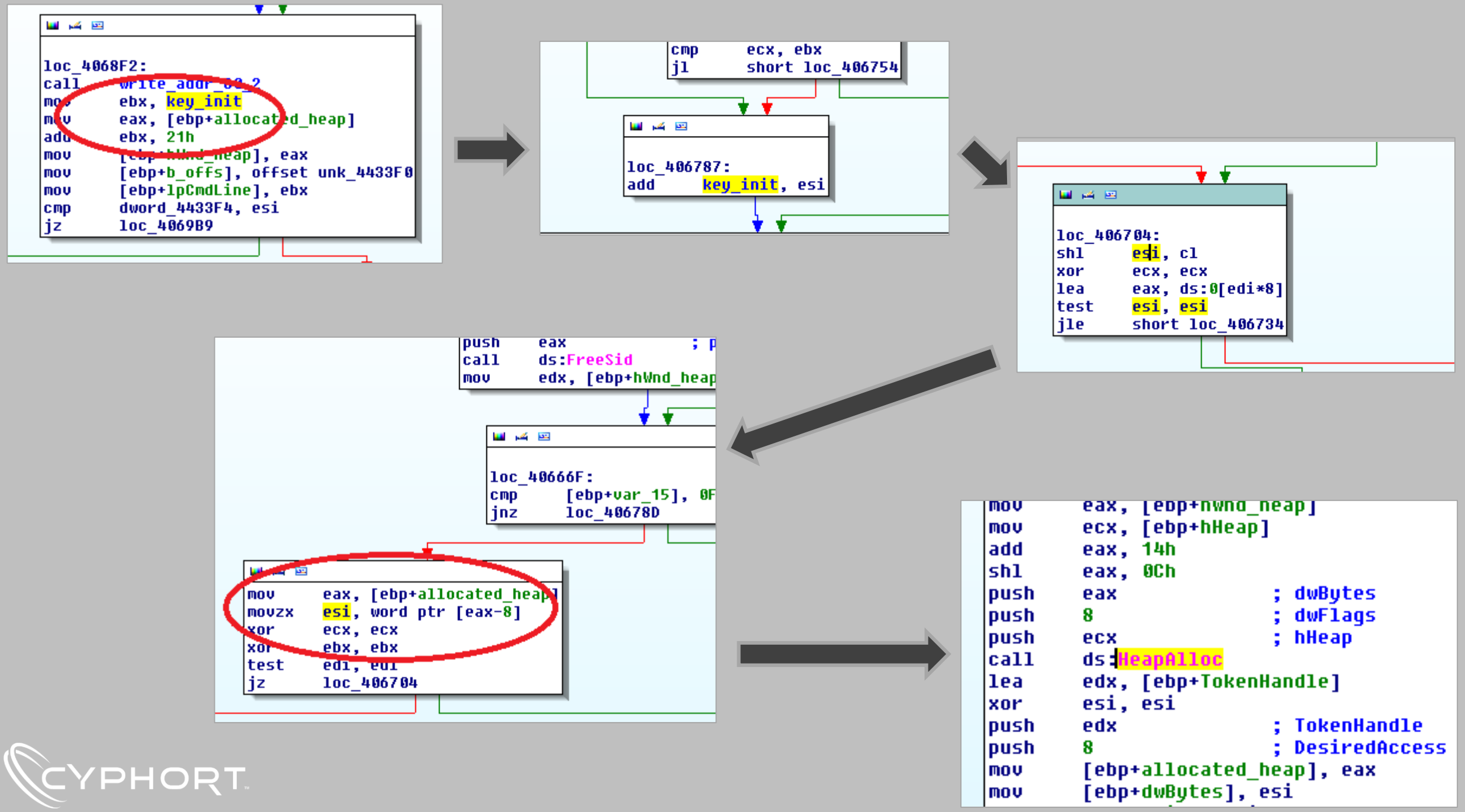
CYPHORT


mov eax, [ebp+heapppp]
mov dword ptr [eax+1], offset dword_447978
cmp [ebp+hHeap], 0
jnz short loc_4069CE
mov eax, offset DialogFunc
loc_4069CE: ; lParam
push 0
push eax ; lpEnumFunc
call ds:EnumWindows
pop edi
pop esi
pop ebx
mov esp, ebp
pop ebp
retn 10h
_WinMain@16 endp

. . .

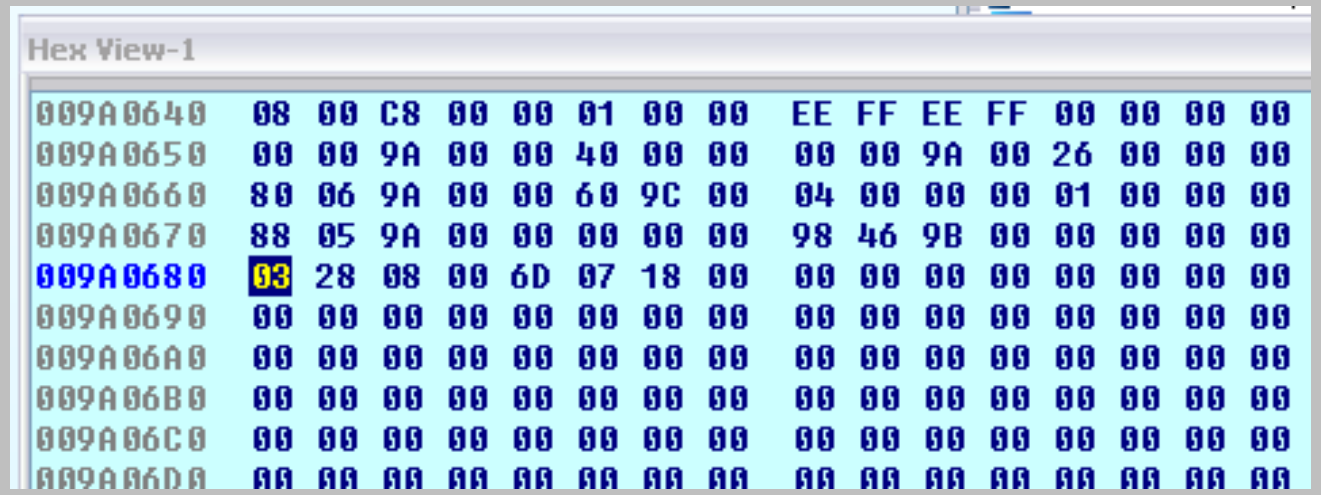

xor esi, esi
mov [ebp+blocksize], eax
test eax, eax
jle short loc_406981
loc_406942:
mov al, cl
add al, al
xor al, bl
xor al, [esi+edi]
cmp al, 22h
jnz short loc_40696B
xor edx, edx
cmp esi, ecx
setz dl
xor edx, ebx
jz short loc_406968
cmp [ebp+blocksize], 4
jge short loc_406968
mov ebx, [ebp+lpCmdLine]
mov [esi+edi], bl
jmp short loc_40696B
loc_406968:
mov ebx, [ebp+lpCmdLine]

CYPHORT

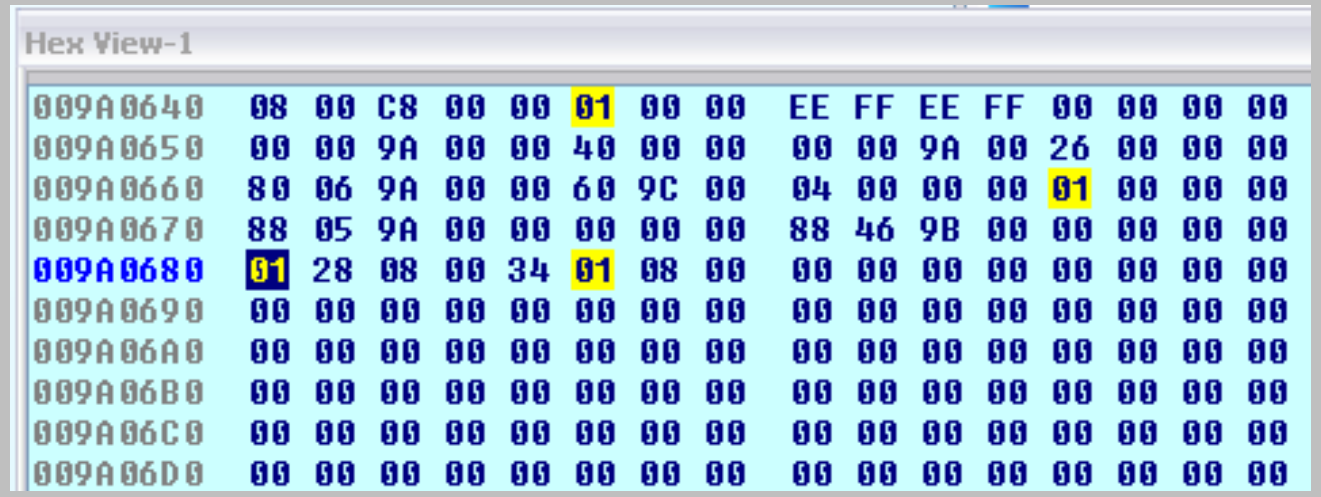

loc_4068F2:
call write_addr_00_2
mov ebx, key_init
mov eax, [ebp+allocated_heap]
add ebx, 21h
mov [ebp+hWnd_heap], eax
mov [ebp+b_offs], offset unk_4433F0
mov [ebp+lpCmdLine], ebx
cmp dword_4433F4, esi
jz loc_4069B9
cmp ecx, ebx
jl short loc_406754
loc_406787:
add key_init, esi
loc_406704:
shl esi, cl
xor ecx, ecx
lea eax, ds:0[edi*8]
test esi, esi
jle short loc_406734
push eax ; p
call ds:FreeSid
mov edx, [ebp+hWnd_heap
loc_40666F:
cmp [ebp+var_15], 0F
jnz loc_40678D
mov eax, [ebp+allocated_heap]
movzx esi, word ptr [eax-8]
xor ecx, ecx
xor ebx, ebx
test edi, edi
jz loc_406704
mov eax, [ebp+hWnd_heap]
mov ecx, [ebp+hHeap]
add eax, 14h
shl eax, 0Ch
push eax ; dwBytes
push 8 ; dwFlags
push ecx ; hHeap
call ds:HeapAlloc
lea edx, [ebp+TokenHandle]
xor esi, esi
push edx ; TokenHandle
push 8 ; DesiredAccess
mov [ebp+allocated_heap], eax
mov [ebp+dwBytes], esi

CYPHORT

WITH DEBUGGER



WITHOUT DEBUGGER




```
typedef struct _HEAP_ENTRY
 {

    USHORT Size ;                //: Uint2B
    USHORT PreviousSize;         //: Uint2B
    UCHAR CK ;    //: UChar
    UCHAR FL              ;  //: UChar
    UCHAR UN       ; //: UChar
    UCHAR SI       ;//: UChar

} HEAP_ENTRY, *PHEAP_ENTRY;
```

CYPHORT

CVE-2014-1776

.html

vshow.swf

Heap Preparation

Timer Registration

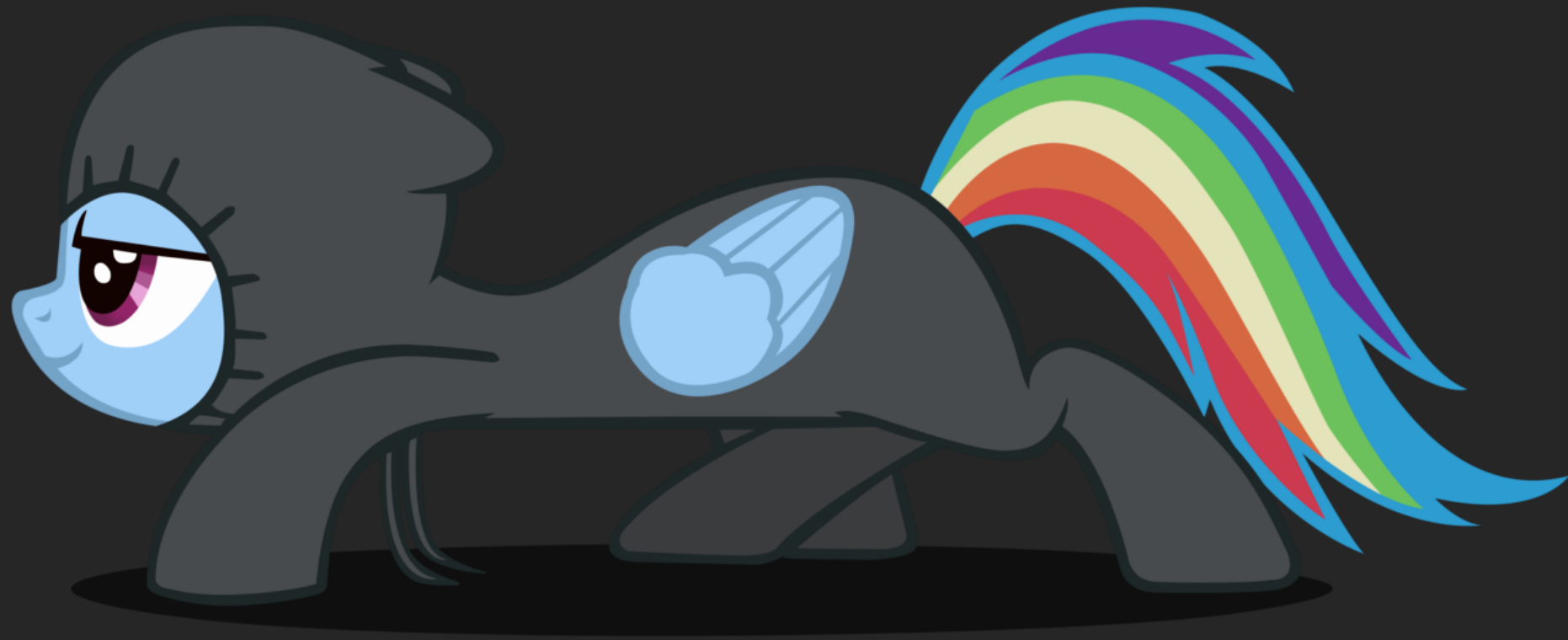
- Prepare ROP Chain
- Corrupt Memory
- Fill SoundObject with Shellcode
- Invoke SoundObject.toString()

cmmon.js

Eval (something)

CYPHORT

SNEAKY EXPLOIT BEING SNEAKY



CYPHORT

DECODING OF THE ACTUAL EXPLOIT

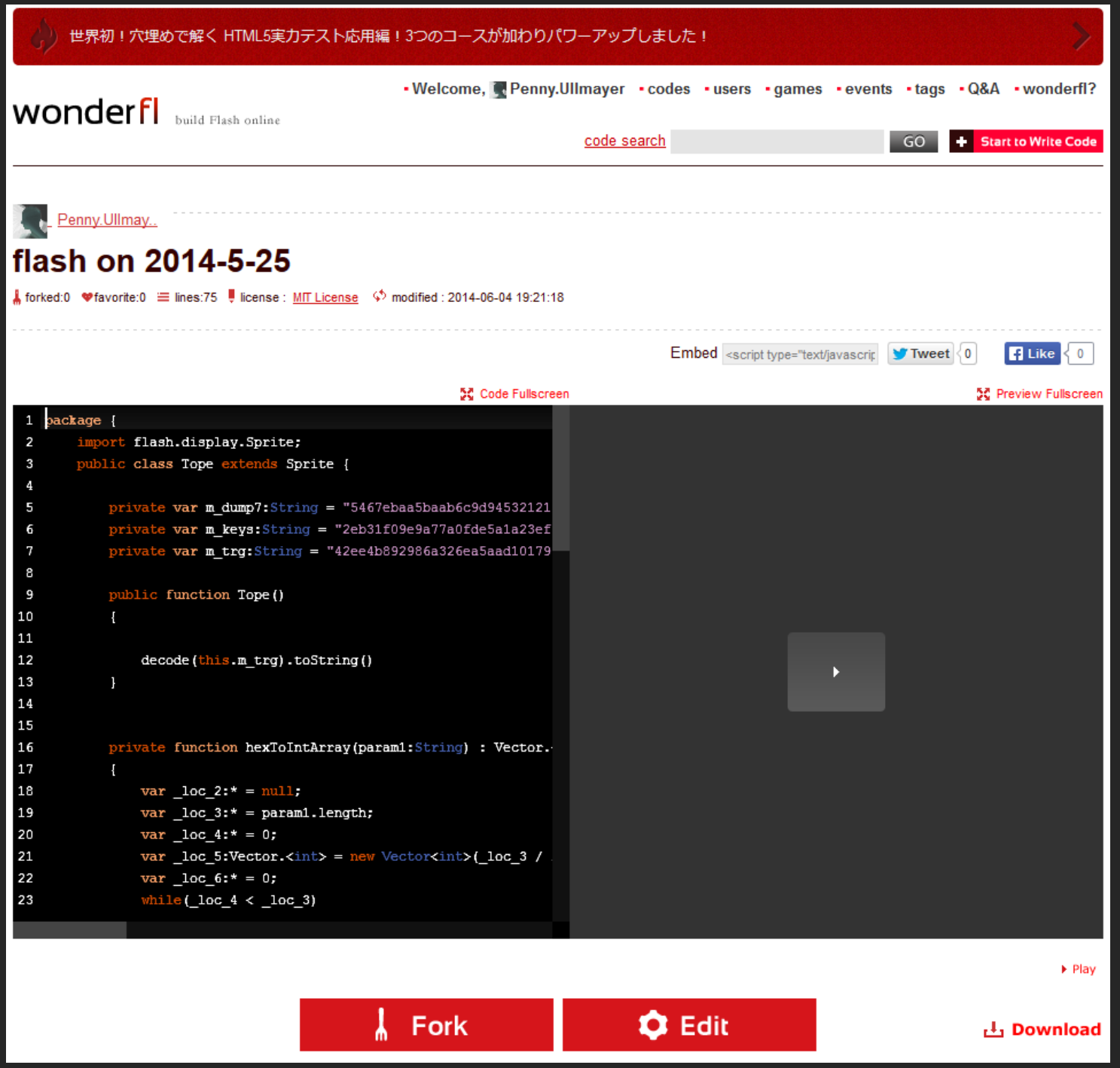
```
private function decode(param1:String) : ByteArray
{
    var _loc_6:int = 0;
    var _loc_8:int = 0;
    var _loc_9:* = undefined;
    var _loc_13:int = 0;
    var _loc_2:Vector.<int> = new Vector<int>(256);
    var _loc_3:Vector.<int> = new Vector<int>(256);
```

...

```
var _loc_10:ByteArray = new ByteArray();
_loc_10.endian = Endian.LITTLE_ENDIAN;
var _loc_11:Vector.<int> = hexToIntArray(param1);
_loc_6 = 0;
var _loc_12:int = 0;
_loc_9 = 0;
while(_loc_9 < _loc_11.length)
{
    _loc_6 = (_loc_6 + 1) & 255;
    _loc_12 = (_loc_12 + _loc_2[_loc_6]) & 255;
    _loc_8 = _loc_2[_loc_6];
    _loc_2[_loc_6] = _loc_2[_loc_12];
    _loc_2[_loc_12] = _loc_8;
    _loc_13 = (_loc_2[_loc_6] + _loc_2[_loc_12]) & 255;
    _loc_8 = _loc_2[_loc_13];
    _loc_10.writeByte(_loc_11[_loc_9] ^ _loc_8);
    _loc_9 = _loc_9 + 1;
}
return _loc_10;
```

CYPHORT

ALMOST WONDERFUL wonderfl



CYPHORT

```
private var delay:uint = 1000;
private var snd:Sound;
private var m_dump7:String = "5467ebaa5baab6c9d945321215d4f075251af2717b30cde85bdcede9d17bfb6eff2aa25e9b34ad7a1670ab5abc27b1
private var m_keys:String = "2eb31f09e9a77a0fde5a1a23eff067a24a98840ceabf048497b3";
private var m_trg:String = "42ee4b892986a326ea5aad1017918a235b0c5e940c449a9d40a585ce8f7b9a0ae8b6f4f0af281700b2064a6015fc0f16
private var work:Timer;
public var s:Vector.<Object>;
public var tf:TextField;
private var found:Boolean = false;
private var m_mark:Boolean = false;
```

```
}
if(ExternalInterface.available)
{
    ExternalInterface.call("eim", decode(this.m_trg).toString());
}
this.work.start();
this.work.addEventListener(TimerEvent.TIMER, this.proc);
```

```
var r,t,e,i;
var o=document.getElementById("l");
r=document.createElement('i');
t=r;
r=document.getElementById("k").childNodes[0].appendChild(r);
r=t.appendChild(o);
e=r.offsetParent;e.onpropertychange=fun;
i=o.firstChild.nextSibling;
try{i.disabled= o;}catch(e){}
```

CYPHORT

MIUREF

and it‘s packer

Once upon a time ...

CYPHORT

Form1

Visual Basic 6.0

Microsoft, 1998

Object-based / event-driven

Rapid Application Developme

Replaced by VB

End of support in 20


VB6 IS
NOT
DEAD
CYPHORT

```
lea     ecx, [ebp-24h]
mov     [ebp-24h], esi
mov     [ebp-54h], eax
mov     [ebp-44h], eax
mov     [ebp-34h], eax
mov     dword ptr [ebp-5Ch], offset aHelloWorld ; "Hello, World!"
mov     dword ptr [ebp-64h], 8
call    ds:__vbaVarDup
lea     eax, [ebp-54h]
lea     ecx, [ebp-44h]
push    eax
lea     edx, [ebp-34h]
push    ecx
push    edx
lea     eax, [ebp-24h]
push    esi
push    eax
call    ds:rtcMsgBox
lea     ecx, [ebp-54h]
```

NATIVE CODE

PSEUDO CODE

```
                dd 4505AFA7h, 74CD8DB4h, 0F9961AA2h, 4D765813h, 3F4F90BDh
                dd 65[illegible]h, 33AD4F3Ah, 11CF6699h, 0AA000CB7h, 93D36000h
                dd 6D[illegible]F46h, 0
dword_40133C    dd 0FCFB3D2Eh, 1068A0FAh, 838A7h, 0B571332Bh, 505C3A43h
                dd 72676F72h, 46206D61h, 73656C69h, 63694D5Ch, 6F736F72h
                dd 5[illegible]207466h, 61757369h, 7453206Ch, 6F696475h, 3942565Ch
                dd 4[illegible]565C38h, 4C4F2E36h, 42h, 4256h, 40133Ch, 0
                dd 6, 9, 40134Ch, 401384h, 4022C8h, 2 dup(0)
dword_4013AC    dd 1A98C0h, 33AD4EF2h, 11CF6699h, 0AA000CB7h, 93D36000h
                                        ; DATA XREF: .text:004018A4↓o
                dd 6D6D6F43h, 31646E61h, 0
                dd 44000Ch, 2 dup(0)
                dd 1Ah, 650048h, 6C006Ch, 2C006Fh, 570020h, 72006Fh, 64006Ch
                dd 21h, 36414256h, 4C4C442Eh, 0
dword_401404    dd 1, 401248h, 0        ; DATA XREF: .text:004014EC↓o
                                        ; .text:00401580↓o ...
                dd offset dword_40182C
                dd 0FFFFFFFFh, 0
                dd offset dword_401298+4
                dd offset unk_402000
```

P-CODE TRANSLATION

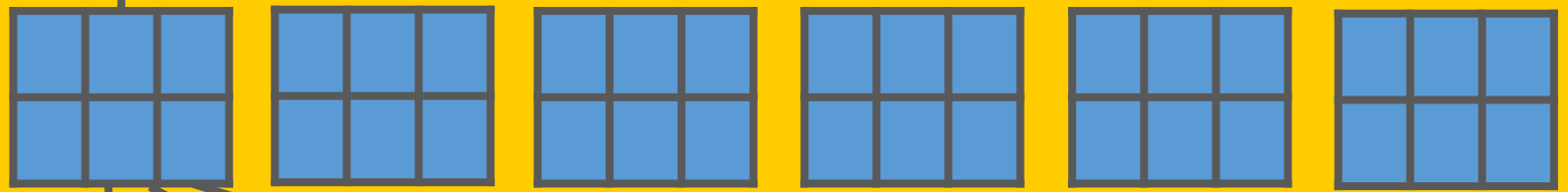
P-code mnemonics

interpreted

by msvbvm60.dll

```
h, 1068A0FAh, 838A7h, 0B571332Bh, 505C3A43h
, 46206D61h, 73656C69h, 63694D5Ch, 6F736F72h
, 61757369h, 7453206Ch, 6F696475h, 3942565Ch
, 4C4F2E36h, 42h, 4256h, 40133Ch, 0
34Ch, 401384h, 4022C8h, 2 dup(0)
33AD4EF2h, 11CF6699h, 0AA000CB7h, 93D36000h
```

... FC C8 **13** 76 ...



handler13:
ExitProcHresult
...

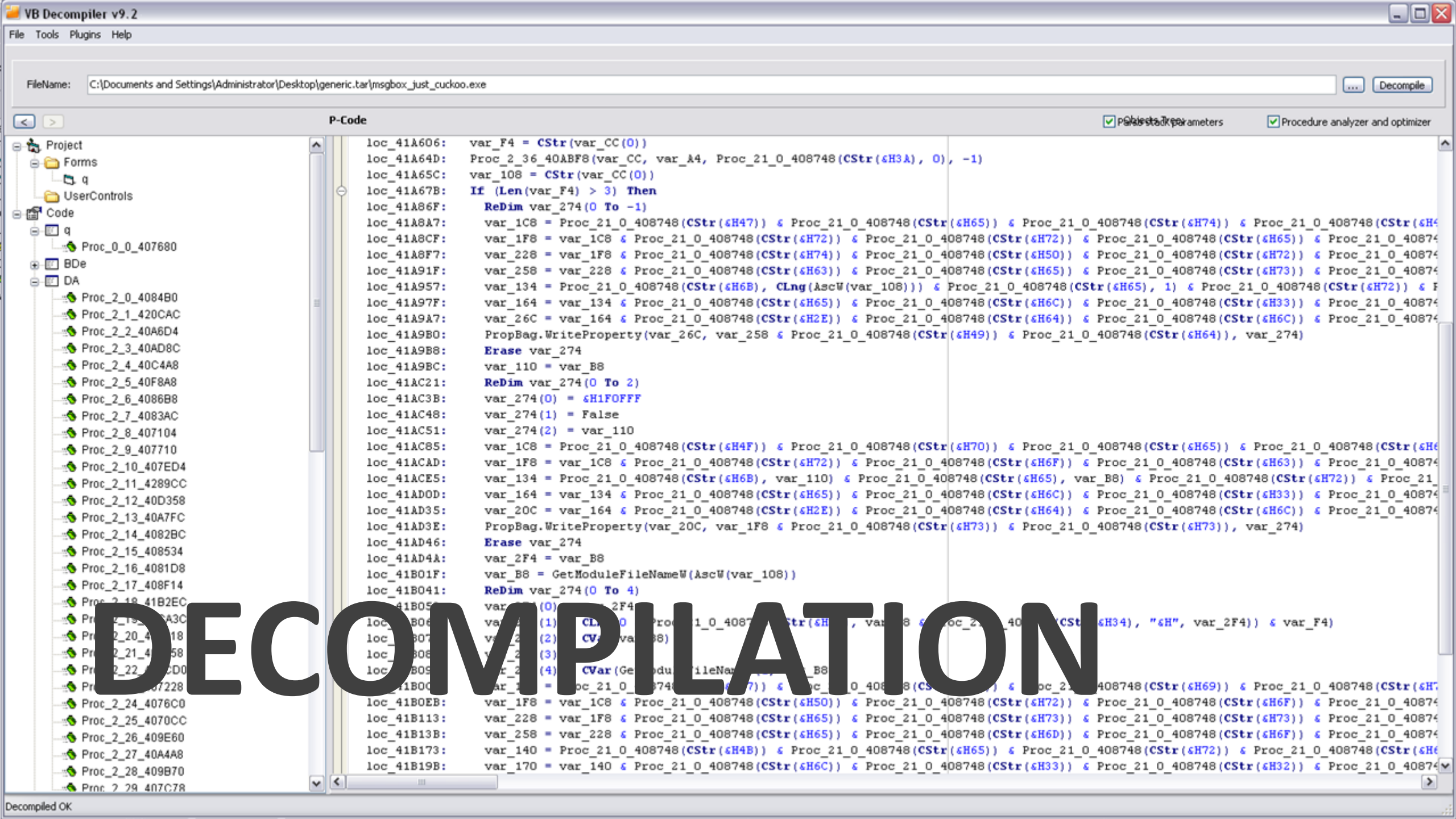
handler14:
ExitProc
...

handler15:
ExitProcI2
...

CYPHORT

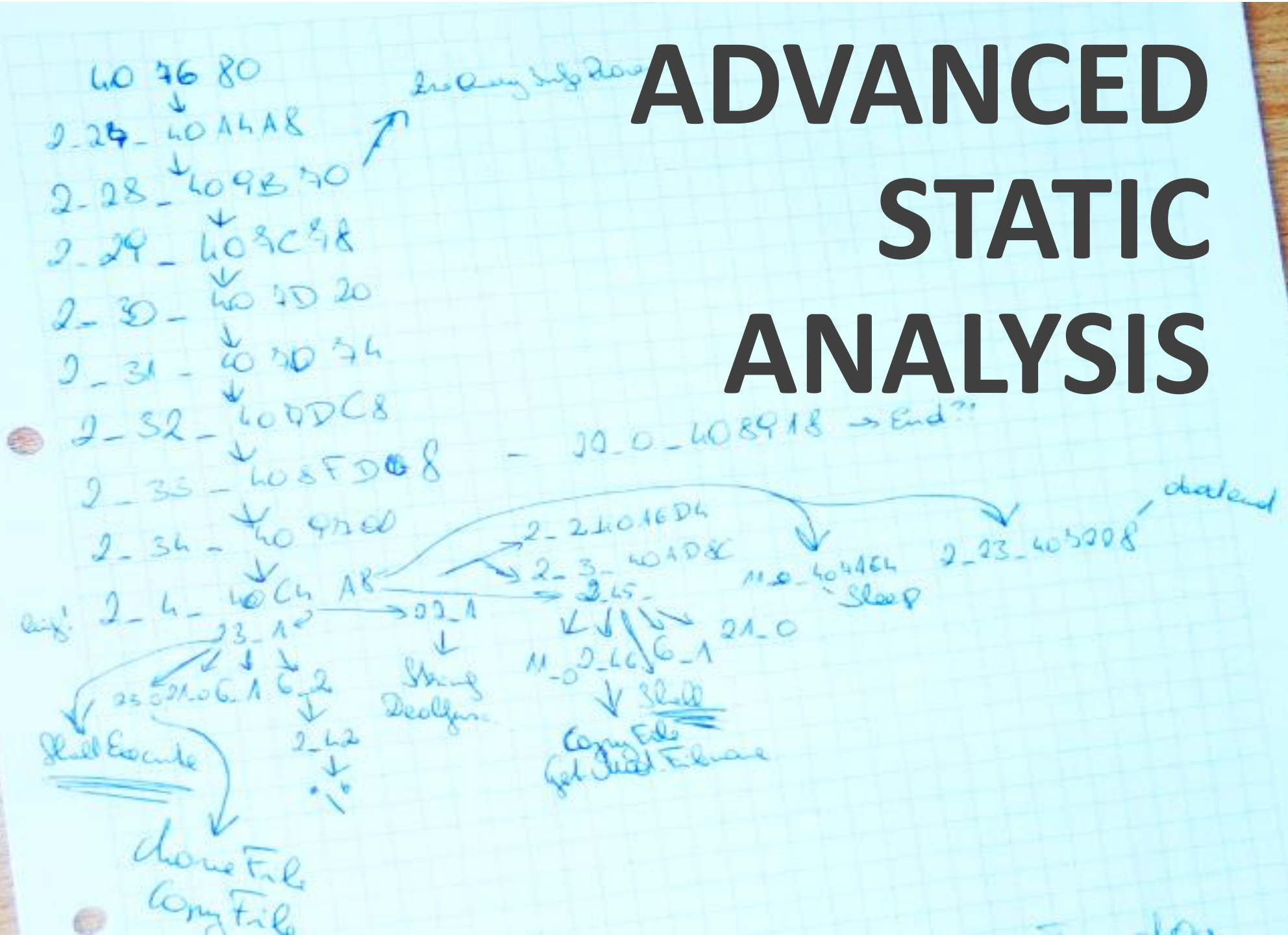
DYNAMIC ANALYSIS

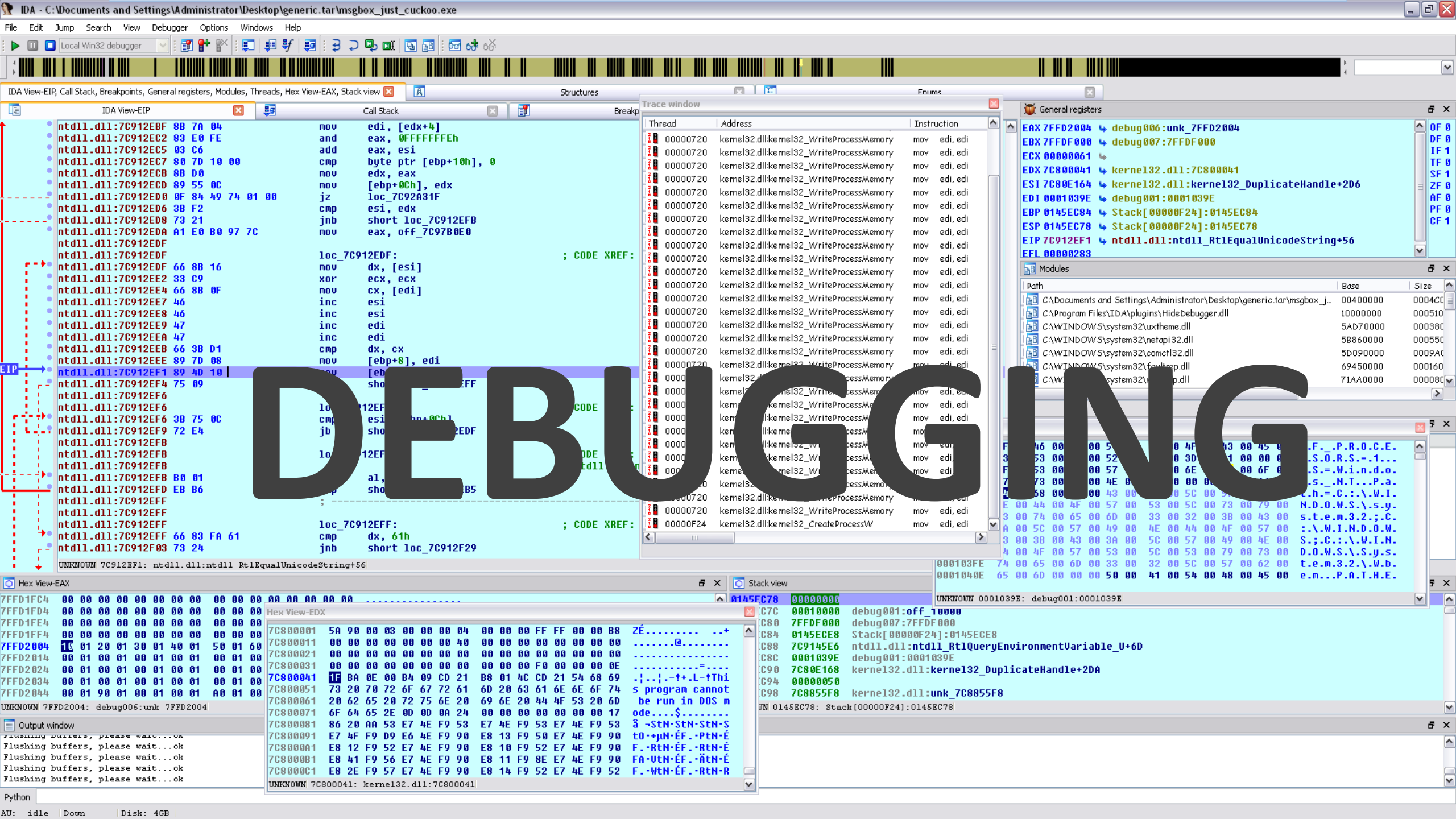
23:14:14,4220474	msgbox_just_c...	356	Thread Exit	SUCCESS	Thread ID: 2536, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:14,4246438	msgbox_just_c...	356	Thread Create	SUCCESS	Thread ID: 2344
23:14:14,4540749	msgbox_just_c...	356	Thread Exit	SUCCESS	Thread ID: 2344, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:14,4654225	msgbox_just_c...	356	Thread Create	SUCCESS	Thread ID: 2420
23:14:14,4688433	msgbox_just_c...	356	Thread Exit	SUCCESS	Thread ID: 2420, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:14,4716808	msgbox_just_c...	356	Thread Create	SUCCESS	Thread ID: 3912
23:14:14,4999919	msgbox_just_c...	356	Thread Exit	SUCCESS	Thread ID: 3912, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:14,5031882	msgbox_just_c...	356	Thread Create	SUCCESS	Thread ID: 3784
23:14:14,5308285	msgbox_just_c...	356	Thread Exit	SUCCESS	Thread ID: 3784, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:14,5338636	msgbox_just_c...	356	Thread Create	SUCCESS	Thread ID: 2916
23:14:14,5621018	msgbox_just_c...	356	Thread Exit	SUCCESS	Thread ID: 2916, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:14,5652441	msgbox_just_c...	356	Thread Create	SUCCESS	Thread ID: 1800
23:14:14,5938656	msgbox_just_c...	356	Thread Exit	SUCCESS	Thread ID: 1800, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:14,5990288	msgbox_just_c...	356	Thread Create	SUCCESS	Thread ID: 584
23:14:14,6096176	msgbox_just_c...	356	Thread Exit	SUCCESS	Thread ID: 584, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:14,6127552	msgbox_just_c...	356	Thread Create	SUCCESS	Thread ID: 3740
23:14:14,6402246	msgbox_just_c...	356	Thread Exit	SUCCESS	Thread ID: 3740, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:14,6433384	msgbox_just_c...	356	Thread Create	SUCCESS	Thread ID: 2784
23:14:14,6715177	msgbox_just_c...	356	Thread Exit	SUCCESS	Thread ID: 2784, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:14,6746130	msgbox_just_c...	356	Thread Create	SUCCESS	Thread ID: 2516
23:14:14,7027163	msgbox_just_c...	356	Thread Exit	SUCCESS	Thread ID: 2516, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:14,7057066	msgbox_just_c...	356	Thread Create	SUCCESS	Thread ID: 3796
23:14:14,7339756	msgbox_just_c...	356	Thread Exit	SUCCESS	Thread ID: 3796, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:14,7369989	msgbox_just_c...	356	Thread Create	SUCCESS	Thread ID: 3208
23:14:14,7496653	msgbox_just_c...	356	Thread Exit	SUCCESS	Thread ID: 3208, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:14,7522760	msgbox_just_c...	356	Thread Create	SUCCESS	Thread ID: 3780
23:14:14,7811637	msgbox_just_c...	356	Thread Exit	SUCCESS	Thread ID: 3780, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:14,7840959	msgbox_just_c...	356	Thread Create	SUCCESS	Thread ID: 1892
23:14:14,8120361	msgbox_just_c...	356	Thread Exit	SUCCESS	Thread ID: 1892, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:14,8150728	msgbox_just_c...	356	Thread Create	SUCCESS	Thread ID: 2608
23:14:14,8457767	msgbox_just_c...	356	Thread Exit	SUCCESS	Thread ID: 2608, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:14,8489293	msgbox_just_c...	356	Thread Create	SUCCESS	Thread ID: 2560
23:14:14,8744842	msgbox_just_c...	356	Thread Exit	SUCCESS	Thread ID: 2560, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:14,8774748	msgbox_just_c...	356	Thread Create	SUCCESS	Thread ID: 3284
23:14:14,9058229	msgbox_just_c...	356	Thread Exit	SUCCESS	Thread ID: 3284, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:14,9091638	msgbox_just_c...	356	Thread Create	SUCCESS	Thread ID: 3016
23:14:14,9369000	msgbox_just_c...	356	Thread Exit	SUCCESS	Thread ID: 3016, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:14,9479070	msgbox_just_c...	356	Thread Create	SUCCESS	Thread ID: 2016
23:14:14,9532359	msgbox_just_c...	356	Thread Exit	SUCCESS	Thread ID: 2016, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:14,9583558	msgbox_just_c...	356	Thread Create	SUCCESS	Thread ID: 212
23:14:14,9835663	msgbox_just_c...	356	Thread Exit	SUCCESS	Thread ID: 212, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:14,9864320	msgbox_just_c...	356	Thread Create	SUCCESS	Thread ID: 600
23:14:15,0147691	msgbox_just_c...	356	Thread Exit	SUCCESS	Thread ID: 600, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:15,0198035	msgbox_just_c...	356	Thread Create	SUCCESS	Thread ID: 856
23:14:15,0462237	msgbox_just_c...	356	Thread Exit	SUCCESS	Thread ID: 856, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:15,0488528	msgbox_just_c...	356	Thread Create	SUCCESS	Thread ID: 2896
23:14:15,0938244	msgbox_just_c...	356	Thread Exit	SUCCESS	Thread ID: 2896, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:15,0964739	msgbox_just_c...	356	Thread Create	SUCCESS	Thread ID: 3236
23:14:15,1252326	msgbox_just_c...	356	Thread Exit	SUCCESS	Thread ID: 3236, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:15,1278078	msgbox_just_c...	356	Thread Create	SUCCESS	Thread ID: 2648
23:14:15,1567950	msgbox_just_c...	356	Thread Exit	SUCCESS	Thread ID: 2648, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:15,1595716	msgbox_just_c...	356	Thread Create	SUCCESS	Thread ID: 3876
23:14:15,1880112	msgbox_just_c...	356	Thread Exit	SUCCESS	Thread ID: 3876, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:15,1907691	msgbox_just_c...	356	Thread Create	SUCCESS	Thread ID: 3864
23:14:15,2187741	msgbox_just_c...	356	Thread Exit	SUCCESS	Thread ID: 3864, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:15,2228550	msgbox_just_c...	356	Thread Create	SUCCESS	Thread ID: 3536
23:14:15,2502068	msgbox_just_c...	356	Thread Exit	SUCCESS	Thread ID: 3536, User Time: 0.0000000, Kernel Time: 0.0000000
23:14:15,2530460	msgbox_just_c...	356	Thread Create	SUCCESS	Thread ID: 2096

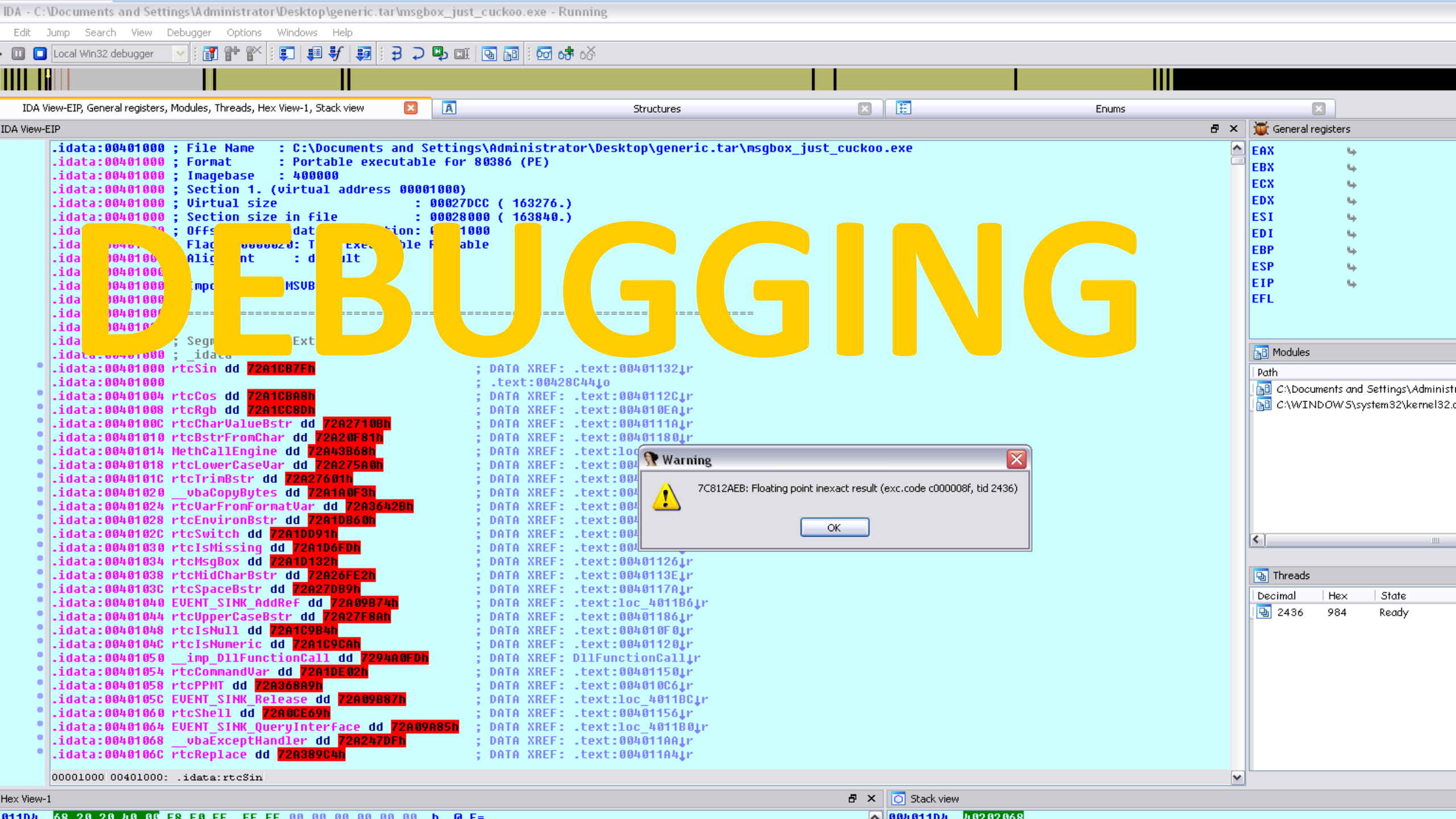


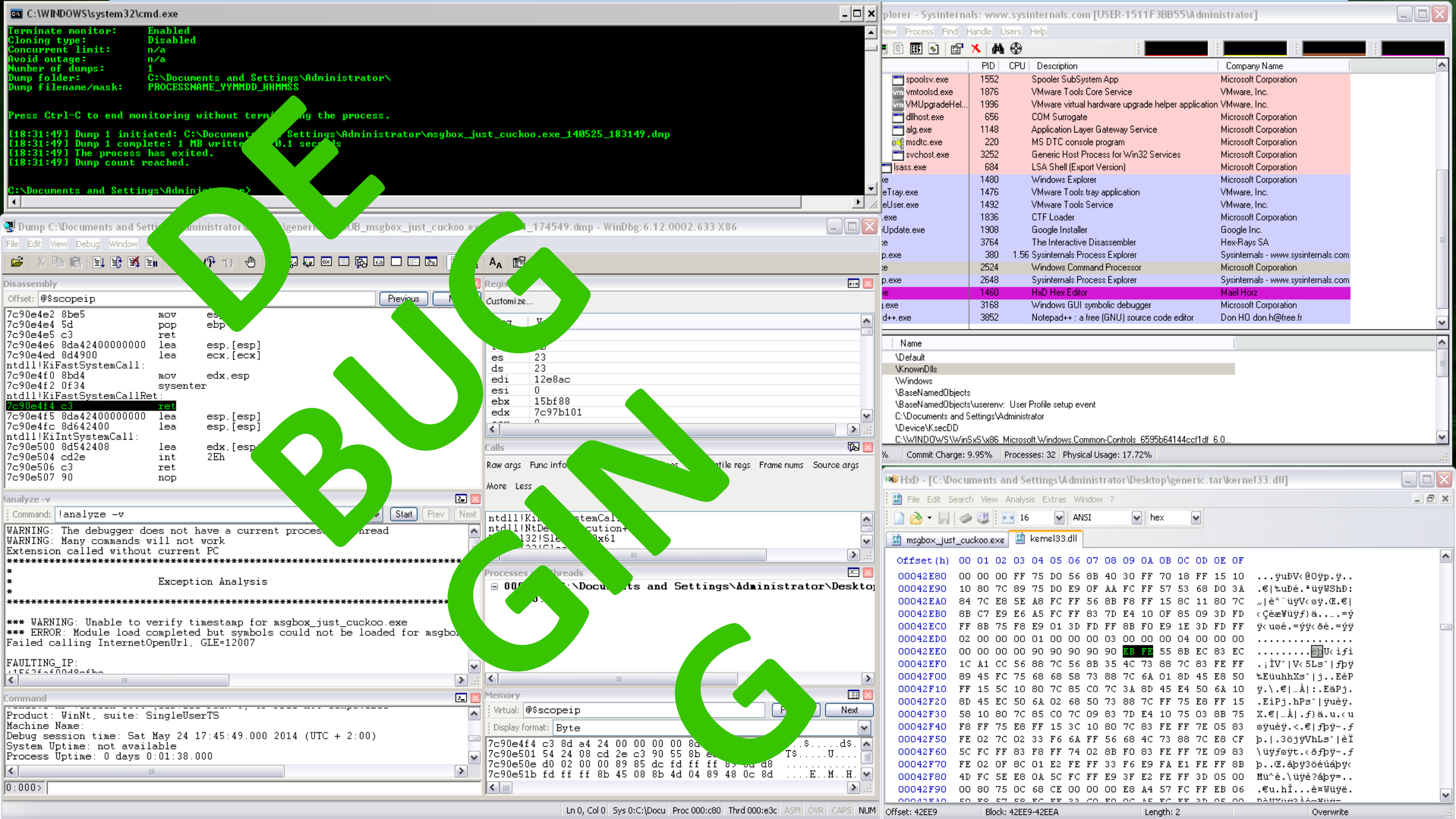
DECOMPILATION

ADVANCED STATIC ANALYSIS

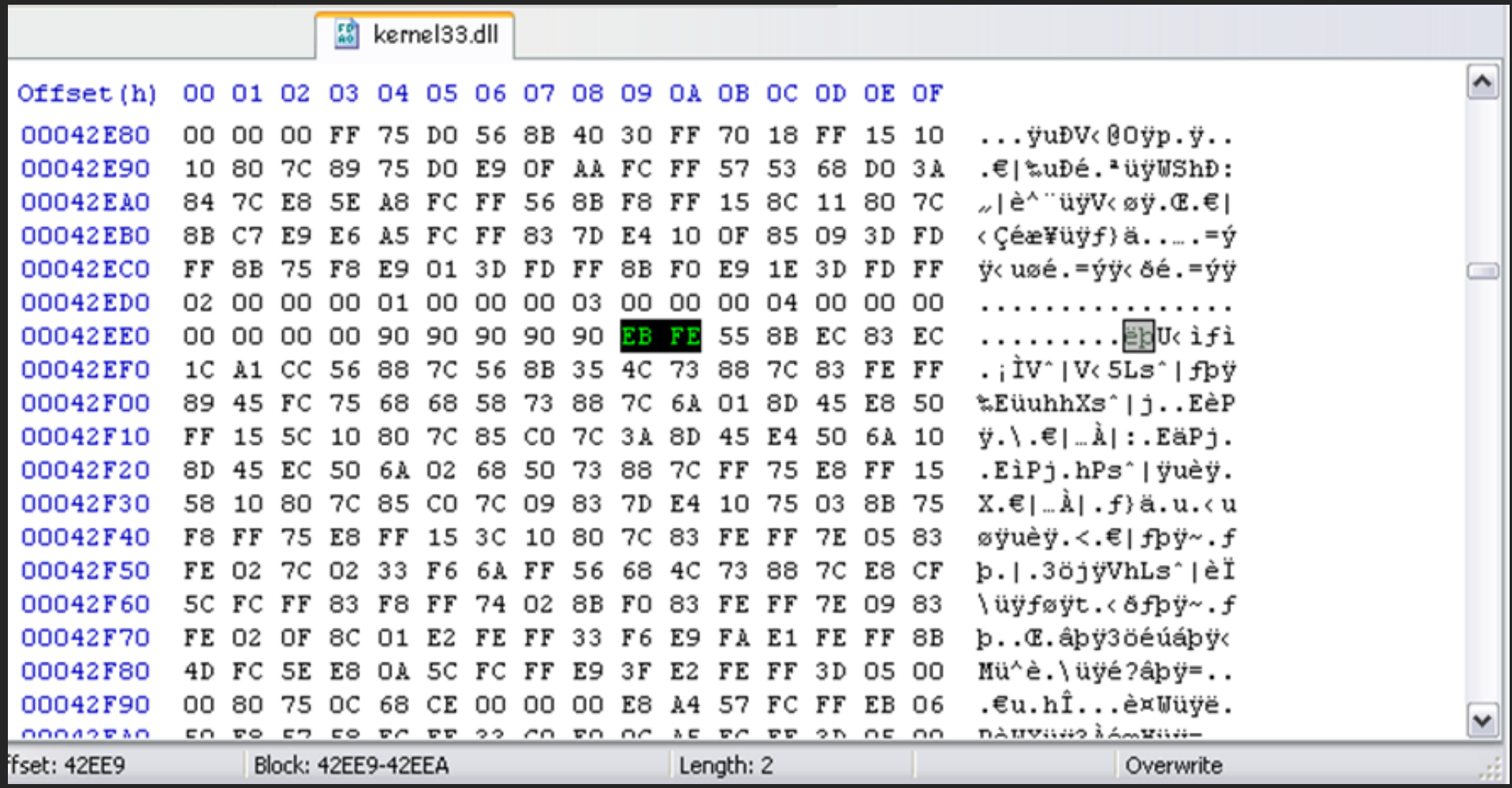



IDA - C:\Documents and Settings\Administrator\Desktop\generic.tar\msgbox_just_cuckoo.exe
File Edit Jump Search View Debugger Options Windows Help
IDA View-EIP, Call Stack, Breakpoints, General registers, Modules, Threads, Hex View-EAX, Stack view
Structures
Enums
IDA View-EIP
Call Stack
Trace window
Thread Address Instruction
General registers
EAX 7FFD2004 debug006:unk_7FFD2004
EBX 7FFDF000 debug007:7FFDF000
ECX 00000061
EDX 7C800041 kernel32.dll:7C800041
ESI 7C80E164 kernel32.dll:kernel32_DuplicateHandle+2D6
EDI 0001039E debug001:0001039E
EBP 0145EC84 Stack[00000F24]:0145EC84
ESP 0145EC78 Stack[00000F24]:0145EC78
EIP 7C912EF1 ntdll.dll:ntdll_RtlEqualUnicodeString+56
EFL 00000283
Modules
Path Base Size
C:\Documents and Settings\Administrator\Desktop\generic.tar\msgbox_j... 00400000
C:\Program Files\IDA\plugins\HideDebugger.dll 10000000
C:\WINDOWS\system32\uxtheme.dll 5AD70000
C:\WINDOWS\system32\netapi32.dll 5B860000
C:\WINDOWS\system32\comctl32.dll 5D090000
ntdll.dll:7C912EBF 8B 7A 04 mov edi, [edx+4]
ntdll.dll:7C912EC2 83 E0 FE and eax, 0FFFFFFFEh
ntdll.dll:7C912EC5 03 C6 add eax, esi
ntdll.dll:7C912EC7 80 7D 10 00 cmp byte ptr [ebp+10h], 0
ntdll.dll:7C912ECB 8B D0 mov edx, eax
ntdll.dll:7C912ECD 89 55 0C mov [ebp+0Ch], edx
ntdll.dll:7C912ED0 0F 84 49 74 01 00 jz loc_7C92A31F
ntdll.dll:7C912ED6 3B F2 cmp esi, edx
ntdll.dll:7C912ED8 73 21 jnb short loc_7C912EFB
ntdll.dll:7C912EDA A1 E0 B0 97 7C mov eax, off_7C97B0E0
ntdll.dll:7C912EDF
ntdll.dll:7C912EDF loc_7C912EDF: ; CODE XREF:
ntdll.dll:7C912EDF 66 8B 16 mov dx, [esi]
ntdll.dll:7C912EE2 33 C9 xor ecx, ecx
ntdll.dll:7C912EE4 66 8B 0F mov cx, [edi]
ntdll.dll:7C912EE7 46 inc esi
ntdll.dll:7C912EE8 46 inc esi
ntdll.dll:7C912EE9 47 inc edi
ntdll.dll:7C912EEA 47 inc edi
ntdll.dll:7C912EEB 66 3B D1 cmp dx, cx
ntdll.dll:7C912EEE 89 7D 08 mov [ebp+8], edi
EIP
ntdll.dll:7C912EF1 89 4D 10
ntdll.dll:7C912EF4 75 09
ntdll.dll:7C912EF6
ntdll.dll:7C912EF6
ntdll.dll:7C912EF6 3B 75 0C cmp esi
ntdll.dll:7C912EF9 72 E4 jb
ntdll.dll:7C912EFB
ntdll.dll:7C912EFB
ntdll.dll:7C912EFB
ntdll.dll:7C912EFB B0 01
ntdll.dll:7C912EFD EB B6
ntdll.dll:7C912EFF
ntdll.dll:7C912EFF
ntdll.dll:7C912EFF loc_7C912EFF: ; CODE XREF:
ntdll.dll:7C912EFF 66 83 FA 61 cmp dx, 61h
ntdll.dll:7C912F03 73 24 jnb short loc_7C912F29
UNKNOWN 7C912EF1: ntdll.dll:ntdll_RtlEqualUnicodeString+56
DEBUGGING
Hex View-EAX
7FFD1FC4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
7FFD1FD4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
7FFD1FE4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
7FFD1FF4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
7FFD2004 10 01 20 01 30 01 40 01 50 01 60
7FFD2014 00 01 00 01 00 01 00 01 00 01 00
7FFD2024 00 01 00 01 00 01 00 01 00 01 00
7FFD2034 00 01 00 01 00 01 00 01 00 01 00
7FFD2044 00 01 90 01 00 01 00 01 A0 01 00
UNKNOWN 7FFD2004: debug006:unk_7FFD2004
Hex View-EDX
7C800001 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 ZÉ.....
7C800011 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 .....@.....
7C800021 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
7C800031 00 00 00 00 00 00 00 00 00 00 00 F0 00 00 00 0E .....=....
7C800041 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 69 .¦..¦.-↑+.L-↑Thi
7C800051 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F 74 s program cannot
7C800061 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 6D be run in DOS m
7C800071 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 17 ode....$.....
7C800081 86 20 AA 53 E7 4E F9 53 E7 4E F9 53 E7 4E F9 53 å ¬StN·StN·StN·S
7C800091 E7 4F F9 D9 E6 4E F9 90 E8 13 F9 50 E7 4E F9 90 tO·+µN·ÉF.·PtN·É
7C8000A1 E8 12 F9 52 E7 4E F9 90 E8 10 F9 52 E7 4E F9 90 F.·RtN·ÉF.·RtN·É
7C8000B1 E8 41 F9 56 E7 4E F9 90 E8 11 F9 8E E7 4E F9 90 FA·VtN·ÉF.·ÄtN·É
7C8000C1 E8 2E F9 57 E7 4E F9 90 E8 14 F9 52 E7 4E F9 52 F.·WtN·ÉF.·RtN·R
UNKNOWN 7C800041: kernel32.dll:7C800041
Stack view
0145EC78 00000000
0145EC7C 00010000 debug001:off_10000
0145EC80 7FFDF000 debug007:7FFDF000
0145EC84 0145ECE8 Stack[00000F24]:0145ECE8
0145EC88 7C9145E6 ntdll.dll:ntdll_RtlQueryEnvironmentVariable_U+6D
0145EC8C 0001039E debug001:0001039E
0145EC90 7C80E168 kernel32.dll:kernel32_DuplicateHandle+2DA
0145EC94 00000050
0145EC98 7C8855F8 kernel32.dll:unk_7C8855F8
UNKNOWN 0145EC78: Stack[00000F24]:0145EC78
UNKNOWN 0001039E: debug001:0001039E
Output window
Flushing buffers, please wait...ok
Flushing buffers, please wait...ok
Flushing buffers, please wait...ok
Flushing buffers, please wait...ok
Flushing buffers, please wait...ok
Python
AU: idle Down Disk: 4GB


IDA - C:\Documents and Settings\Administrator\Desktop\generic.tar\msgbox_just_cuckoo.exe - Running
Edit Jump Search View Debugger Options Windows Help
Local Win32 debugger
IDA View-EIP, General registers, Modules, Threads, Hex View-1, Stack view
Structures
Enums
IDA View-EIP
.idata:00401000 ; File Name : C:\Documents and Settings\Administrator\Desktop\generic.tar\msgbox_just_cuckoo.exe
.idata:00401000 ; Format : Portable executable for 80386 (PE)
.idata:00401000 ; Imagebase : 400000
.idata:00401000 ; Section 1. (virtual address 00001000)
.idata:00401000 ; Virtual size : 00027DCC (163276.)
.idata:00401000 ; Section size in file : 00028000 (163840.)
DEBUGGING
.idata:00401000 rtcSin dd 72A1CB7Fh ; DATA XREF: .text:00401132↓r
.idata:00401000 ; .text:00428C44↓o
.idata:00401004 rtcCos dd 72A1CBA8h ; DATA XREF: .text:0040112C↓r
.idata:00401008 rtcRgb dd 72A1CC8Dh ; DATA XREF: .text:004010EA↓r
.idata:0040100C rtcCharValueBstr dd 72A2710Bh ; DATA XREF: .text:0040111A↓r
.idata:00401010 rtcBstrFromChar dd 72A20F81h ; DATA XREF: .text:00401180↓r
.idata:00401014 MethCallEngine dd 72A43B68h ; DATA XREF: .text:loc
.idata:00401018 rtcLowerCaseVar dd 72A275A0h ; DATA XREF: .text:004
.idata:0040101C rtcTrimBstr dd 72A27601h ; DATA XREF: .text:004
.idata:00401020 __vbaCopyBytes dd 72A1A0F3h ; DATA XREF: .text:004
.idata:00401024 rtcVarFromFormatVar dd 72A3642Bh ; DATA XREF: .text:004
.idata:00401028 rtcEnvironBstr dd 72A1DB60h ; DATA XREF: .text:004
.idata:0040102C rtcSwitch dd 72A1DD91h ; DATA XREF: .text:004
.idata:00401030 rtcIsMissing dd 72A1D6FDh ; DATA XREF: .text:004
.idata:00401034 rtcMsgBox dd 72A1D132h ; DATA XREF: .text:00401126↓r
.idata:00401038 rtcMidCharBstr dd 72A26FE2h ; DATA XREF: .text:0040113E↓r
.idata:0040103C rtcSpaceBstr dd 72A27DB9h ; DATA XREF: .text:0040117A↓r
.idata:00401040 EVENT_SINK_AddRef dd 72A09B74h ; DATA XREF: .text:loc_4011B6↓r
.idata:00401044 rtcUpperCaseBstr dd 72A27F8Ah ; DATA XREF: .text:00401186↓r
.idata:00401048 rtcIsNull dd 72A1C9B4h ; DATA XREF: .text:004010F0↓r
.idata:0040104C rtcIsNumeric dd 72A1C9CAh ; DATA XREF: .text:00401120↓r
.idata:00401050 __imp_DllFunctionCall dd 7294A0FDh ; DATA XREF: DllFunctionCall↓r
.idata:00401054 rtcCommandVar dd 72A1DE02h ; DATA XREF: .text:00401150↓r
.idata:00401058 rtcPPMT dd 72A368A9h ; DATA XREF: .text:004010C6↓r
.idata:0040105C EVENT_SINK_Release dd 72A09B87h ; DATA XREF: .text:loc_4011BC↓r
.idata:00401060 rtcShell dd 72A0CE69h ; DATA XREF: .text:00401156↓r
.idata:00401064 EVENT_SINK_QueryInterface dd 72A09A85h ; DATA XREF: .text:loc_4011B0↓r
.idata:00401068 __vbaExceptHandler dd 72A247DFh ; DATA XREF: .text:004011AA↓r
.idata:0040106C rtcReplace dd 72A389C4h ; DATA XREF: .text:004011A4↓r
Warning
7C812AEB: Floating point inexact result (exc.code c000008f, tid 2436)
OK
00001000 00401000: .idata:rtcSin
General registers
EAX
EBX
ECX
EDX
ESI
EDI
EBP
ESP
EIP
EFL
Modules
Path
C:\Documents and Settings\Administr
C:\WINDOWS\system32\kernel32.d
Threads
Decimal Hex State
2436 984 Ready
Hex View-1
Stack view


DEBUGGING

EVER HEARD OF.. kernel33.dll ?



CYPHORT

Dynamic API Loading

... Crap.

CYPHORT™

```
                public start
1128 start:
1128 push    offset VB_Header
112D call    ThunRTMain
112D ; ---------------------------
1132 dw 0
1134 align 8
1138 dd 30h, 40h, 0
1144 dd 74BAC62Dh, 42AB33F9h, 0C616C69Bh
1158 dd 10000h, 410000h, 7818A4h, 74616C
1178 dword_401178 dd 31CCFFh, 0A27DAA02h
1178
1178 dd 0C1368748h, 0EEBB0B68h, 0AD4F3AD
1178 dd 93h, 8 dup(0)
11D0 dd 83F200h, 834600h, 0F0000h, 74696
11D0 dd 0E010Dh, 6972754Bh, 616D7265h, 6
11D0 dd 746C00h, 78DE00h, 0DE4D4200h, 78h, 36000000h, 28000000h, 78000000h
11D0 dd 9000004h, 1000000h, 1800h, 0A8000000h, 78h, 3 dup(0)
1244 dd 0FF000000h, 19h dup(0FFFFFFFFh), 2A7C7C2Ah, 9AAh, 26Ah dup(0BC00BC00h)
```

Trace window

Thread	Address
00000F54	kernel32.dll:kernel32_CreateProcessW
00000F54	kernel32.dll:kernel32_CreateProcessW
00000F54	kernel32.dll:kernel32_CreateProcessW
00000F54	kernel32.dll:kernel32_CreateProcessW
00000F54	kernel32.dll:kernel32_CreateProcessW

CYPHORT

BACK TO STEALTH MODE

POST VB6 PACKER

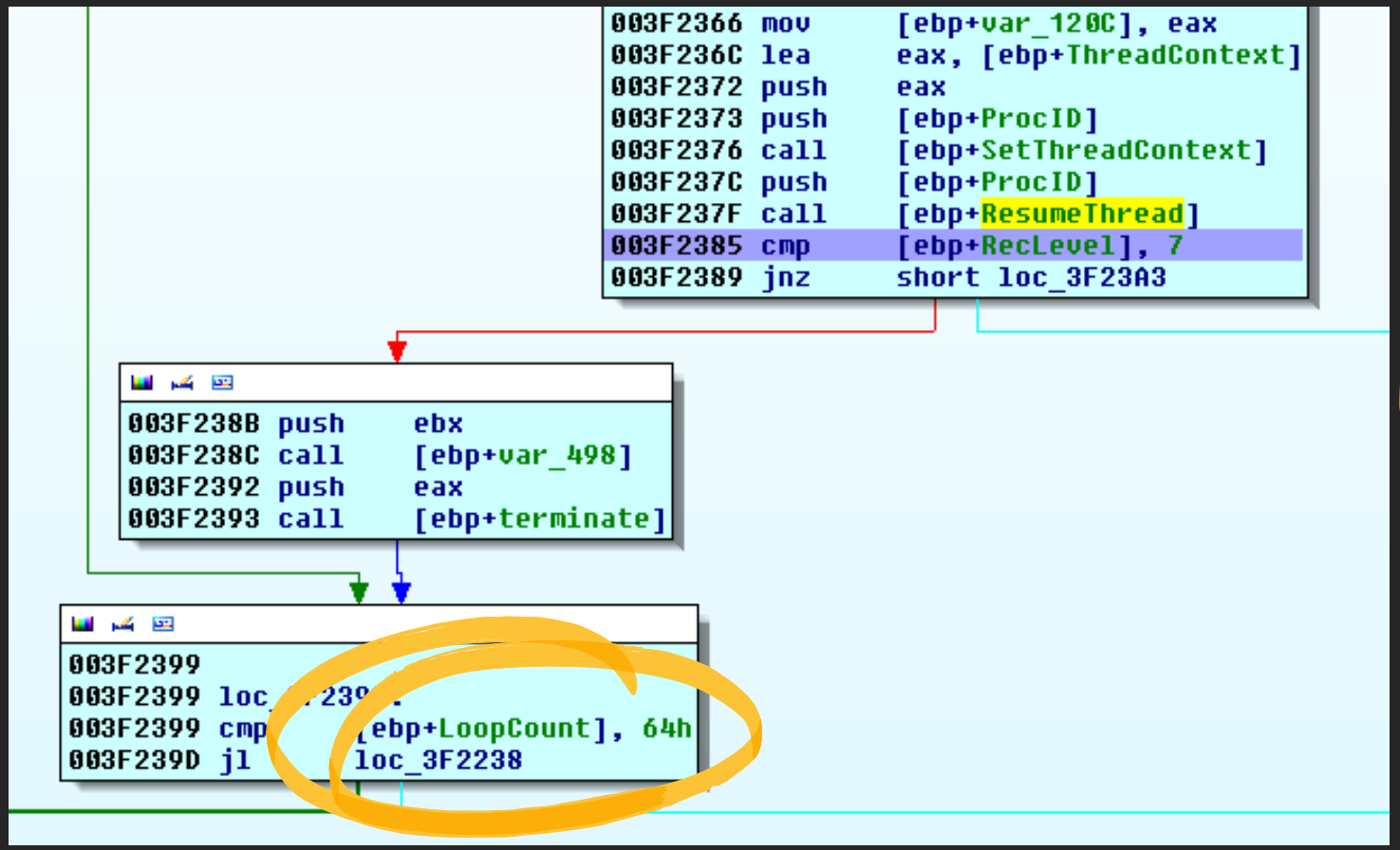
```
NRWConfig.exe:004022A0 ; ---------------------------
NRWConfig.exe:004022A0 push    ebp
NRWConfig.exe:004022A1 mov     ebp, esp
NRWConfig.exe:004022A3 sub     esp, 1Ch
NRWConfig.exe:004022A6 push    esi
NRWConfig.exe:004022A7 xor     esi, esi
NRWConfig.exe:004022A9 mov     [ebp-0Ch], esi
NRWConfig.exe:004022AC mov     [ebp-4], esi
NRWConfig.exe:004022AF mov     [ebp-8], esi
NRWConfig.exe:004022B2 call    near ptr unk_402230
NRWConfig.exe:004022B7 call    near ptr unk_4021BE
NRWConfig.exe:004022BC cmp     eax, esi
NRWConfig.exe:004022BE jz      loc_4023A2
NRWConfig.exe:004022C4 lea     ecx, [ebp-4]
NRWConfig.exe:004022C7 push    ecx
NRWConfig.exe:004022C8 push    eax
NRWConfig.exe:004022C9 lea     esi, [ebp-8]
NRWConfig.exe:004022CC call    near ptr unk_4018CD
NRWConfig.exe:004022D1 pop     ecx
NRWConfig.exe:004022D2 pop     ecx
NRWConfig.exe:004022D3 test    eax, eax
NRWConfig.exe:004022D5 jz      loc_4023A2
NRWConfig.exe:004022DB mov     esi, [ebp-4]
NRWConfig.exe:004022DE mov     al, [esi]
NRWConfig.exe:004022E0 cmp     al, 10h
NRWConfig.exe:004022E2 ja      loc_4023A2
NRWConfig.exe:004022E8 push    ebx
```

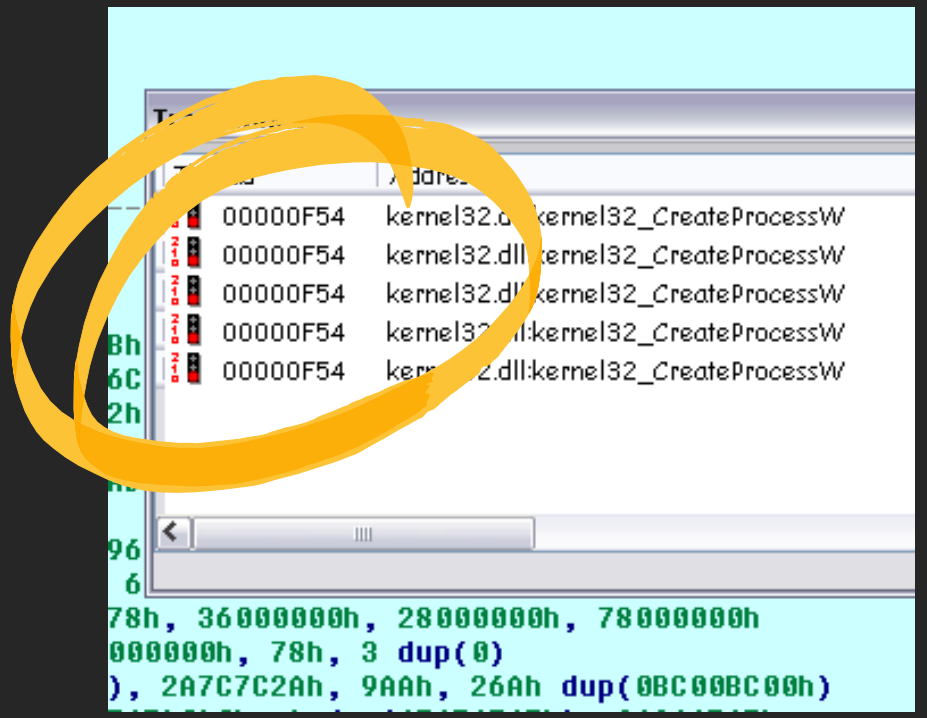
POST C++ PACKER

```
0040228B public start
0040228B start proc near
0040228B
0040228B var_1C= byte ptr -1Ch
0040228B var_C= dword ptr -0Ch
0040228B var_8= dword ptr -8
0040228B var_4= dword ptr -4
0040228B
0040228B push    ebp
0040228C mov     ebp, esp
0040228E sub     esp, 1Ch
00402291 push    esi
00402292 xor     esi, esi
00402294 mov     [ebp+var_C], esi
00402297 mov     [ebp+var_4], esi
0040229A mov     [ebp+var_8], esi
0040229D call    WalkProcesses
004022A2 call    Path_setup_dat
004022A7 cmp     eax, esi
004022A9 jz      loc_40238C
```

```
004022AF lea     ecx, [ebp+var_4]
004022B2 push    ecx
004022B3 push    eax
004022B4 lea     esi, [ebp+var_8]
004022B7 call    ReadAFile
004022BC pop     ecx
004022BD pop     ecx
004022BE test    eax, eax
004022C0 jz      loc_40238C
```

CYPHORT





C++ PACKER

VB6 PACKER

CYPHORT

THANK YOU!

Marion Marschalek

CYPHORT

marion@0x1338.at
0x1338.blogspot.co.at
@pinkflawd