

CATCH ME IF YOU CAN



**HUNTER
HUNTED
and HAUNTED**

YOUR HUNTER TODAY

Marion Marschalek



ANALYST

aims to detect

MALWARE

MALWARE

aims to detect

ANALYST

LEVELS of SOPHISTICATION

Mass Malware

Sophisticated Malware

Toolified Malware

APT Malware

aAPT Malware

EPT Malware

?

```
jA[jZZ+
PP9E u
9E WW
tHHt*Ht#
uJSSR
SSSSS
AVs, please add that string to your signatures.
bad allocation
Unknown exception
mscoree.dll
CorExitProcess
R6008
    not enough space for arguments
R6009
    not enough space for environment
R6010
    abort() has been called
R6016
```

while some are not all that sophisticated

SIMULATION

VIRTUALIZATION

STATIC ANALYSIS

DISASSEMBLING

DEBUGGING

**ARTIFICIAL
INTELLIGENCE**

SIMULATION

VIRTUALIZATION

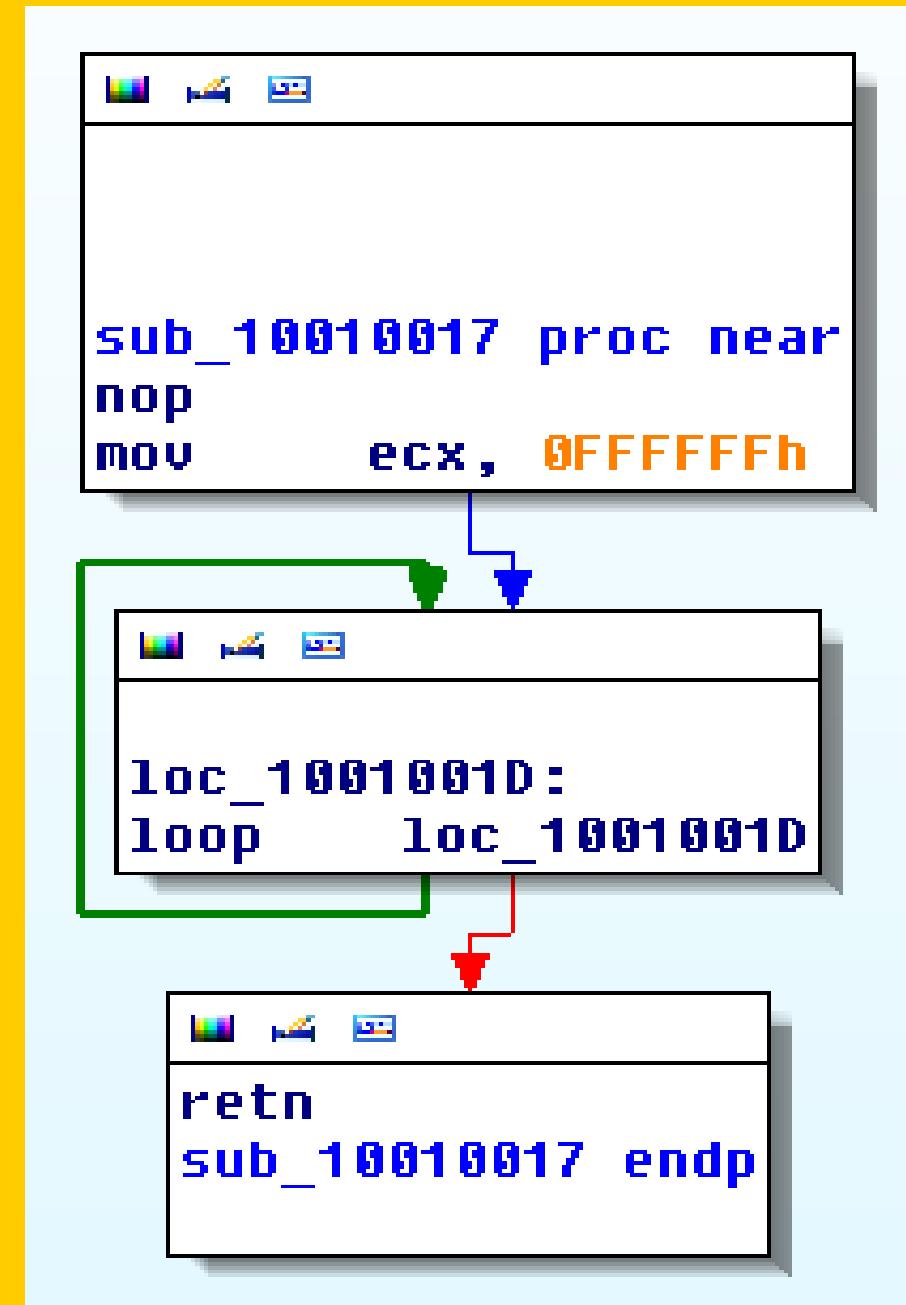
STATIC ANALYSIS

DISASSEMBLING

DEBUGGING

ARTIFICIAL

INTELLIGENCE



SIMULATION

VIRTUALIZATION

STATIC ANALYSIS

DISASSEMBLING

DEBUGGING

ARTIFICIAL

INTELLIGENCE

```
2:003F2610 mov    [ebp+var_44], 'U'
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 mou    byte ptr [ebp+var_201], bl
```

SIMULATION

VIRTUALIZATION

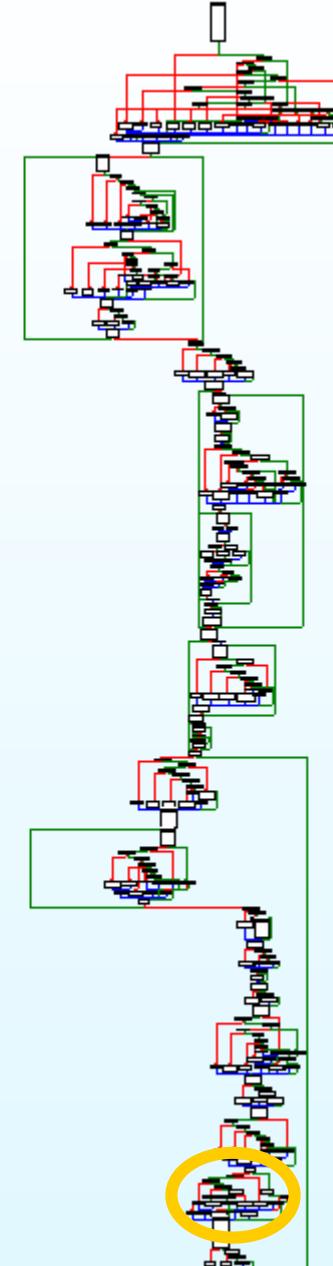
STATIC ANALYSIS

DISASSEMBLING

DEBUGGING

ARTIFICIAL

INTELLIGENCE



SIMULATION

VIRTUALIZATION

STATIC ANALYSIS

DISASSEMBLING

DEBUGGING

ARTIFICIAL

INTELLIGENCE

01047
01047 loc_401047 ; CODE XREF:
01047 0F 84 FF FF FF FF jz near ptr loc_401047+5
0104D 00 68 43 add [eax+43h], ch
01050 22 15 90 58 31 05 and 01, 05:53158900
01056 00 30 add [eax+0], dh
01058 40 inc eax
01059 00 B9 00 00 00 10 add [ecx+10000000h], bh

01045 3B C0 cmp eax, eax
01045 ;
01047 0F db 0Fh
01048 84 FF FF FF dd 0FFFFF84h
0104C ;
0104C FF 00 inc dword ptr [eax]
0104E 00 42 22 15 00 push 001E2242h
01053 58 pop eax
01054 31 05 00 30 40 00 xor dword_403000, eax
0105A B9 00 00 00 10 mov ecx, 10000000h

SIMULATION

VIRTUALIZATION

STATIC ANALYSIS

DISASSEMBLING

DEBUGGING

ARTIFICIAL

INTELLIGENCE

00401C80	push	ebp
00401C81	mov	ebp, esp
00401C83	push	0FFFFFFFh
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

• • •

The screenshot shows a debugger interface with assembly code. The code starts with a push instruction for the stack frame pointer (ebp). It then pushes the current stack pointer (esp) onto the stack. A constant value (0xFFFFFFFF) is pushed onto the stack. The offset of the SEH handler (_WinMain@16_SEH) is pushed onto the stack. The value in eax is moved to the fs register at offset 0. The value in eax is then pushed onto the stack. The stack pointer (esp) is then adjusted by 24h (36 bytes). The code then branches to a label named loc_401D98. Inside this block, it moves the value in ecx to eax. It then calls the value in ecx. It moves the value in eax to ecx. It moves the value in eax to the memory location [ebp + __\$EHRec\$.pNext]. It then moves the value in ecx to the stack (large fs:0). It pops edi from the stack. It then pops esi from the stack. It pops ebx from the stack. It moves the stack pointer (esp) to the value in ebp. It then pops the value in ebp from the stack. Finally, it returns with a value of 10h.

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

SIMULATION

VIRTUALIZATION

STATIC ANALYSIS

DISASSEMBLING

DEBUGGING

ARTIFICIAL

INTELLIGENCE

A close-up photograph of a zebra's coat, showing its characteristic black and white stripes. The stripes are thick and irregular, creating a complex pattern. The background is a solid yellow.

RANDOMNESS

THE ANCIENT ART OF BYPASSING ANTI-ANALYSIS



PEBBeingDebugged Flag: IsDebuggerPresent()	Encryption and Compression
PEBNtGlobalFlag, Heap Flags	Garbage Code and Code Permutation
DebugPort: CheckRemoteDebuggerPresent() / NtQueryInformationProcess()	Anti-Disassembly
Debugger Interrupts	Misdirection and Stopping Execution via Exceptions
Timing Checks	Blocking Input
SeDebugPrivilege	ThreadHideFromDebugger
Parent Process	Disabling Breakpoints
DebugObject: NtQueryObject()	Unhandled Exception Filter
Debugger Window	OllyDbg: OutputDebugString() Format String Bug
Debugger Process	Process Injection
Device Drivers	Debugger Blocker
OllyDbg: Guard Pages	TLS Callbacks
Software Breakpoint Detection	Stolen Bytes
Hardware Breakpoint Detection	API Redirection
Patching Detection via Code Checksum Calculation	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>

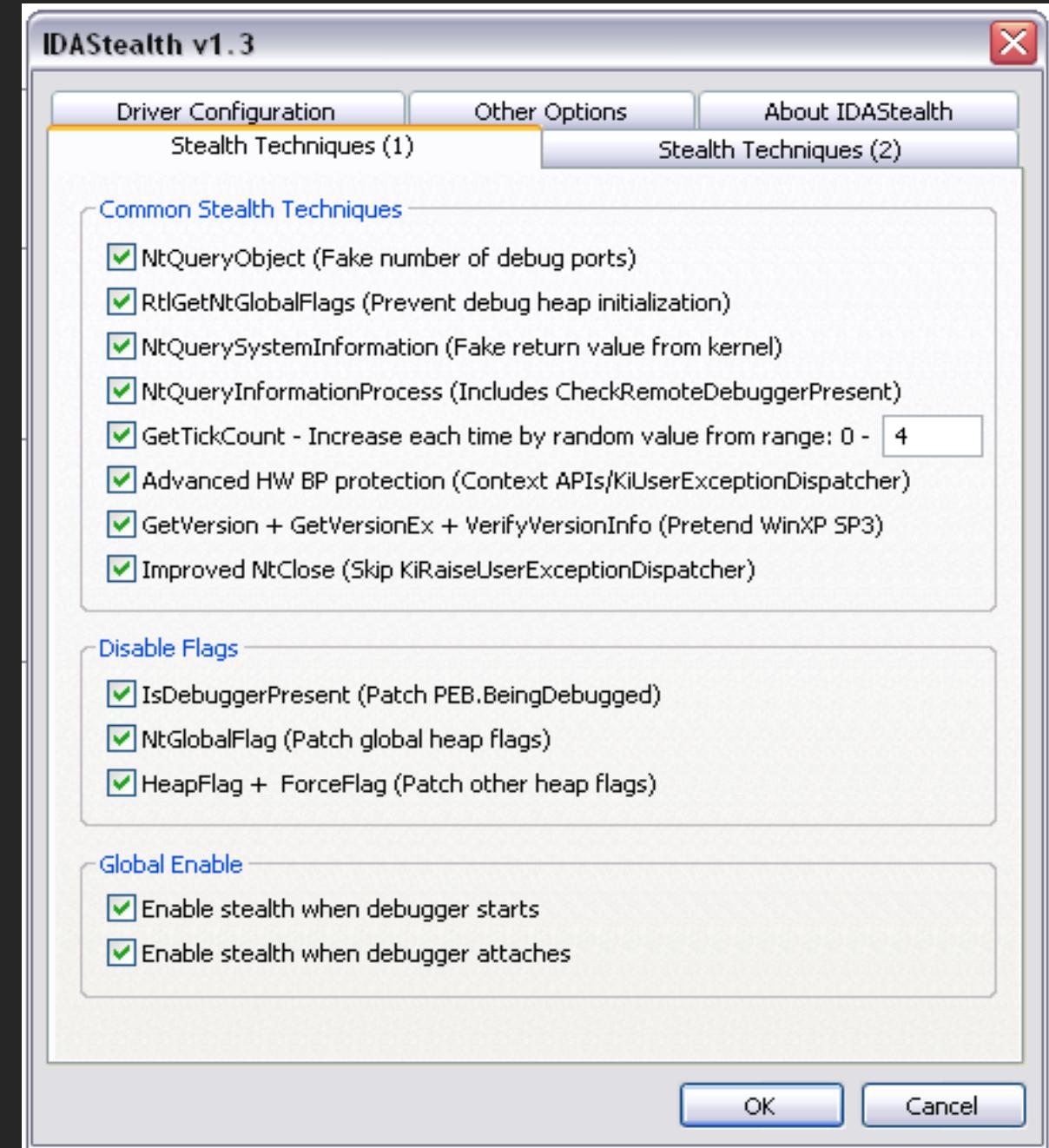
**SCIENTIFIC BUT NOT ACADEMICAL OVERVIEW OF MALWARE ANTI-DEBUGGING,
ANTI-DEBUGGING AND ANTI-VM TECHNIQUES [Branco, Barbosa, Neto]**

<http://research.dissect.pe/docs/blackhat2012-paper.pdf>

VIRTUAL MACHINE DETECTION ENHANCED [Rin, EP_XOFF]

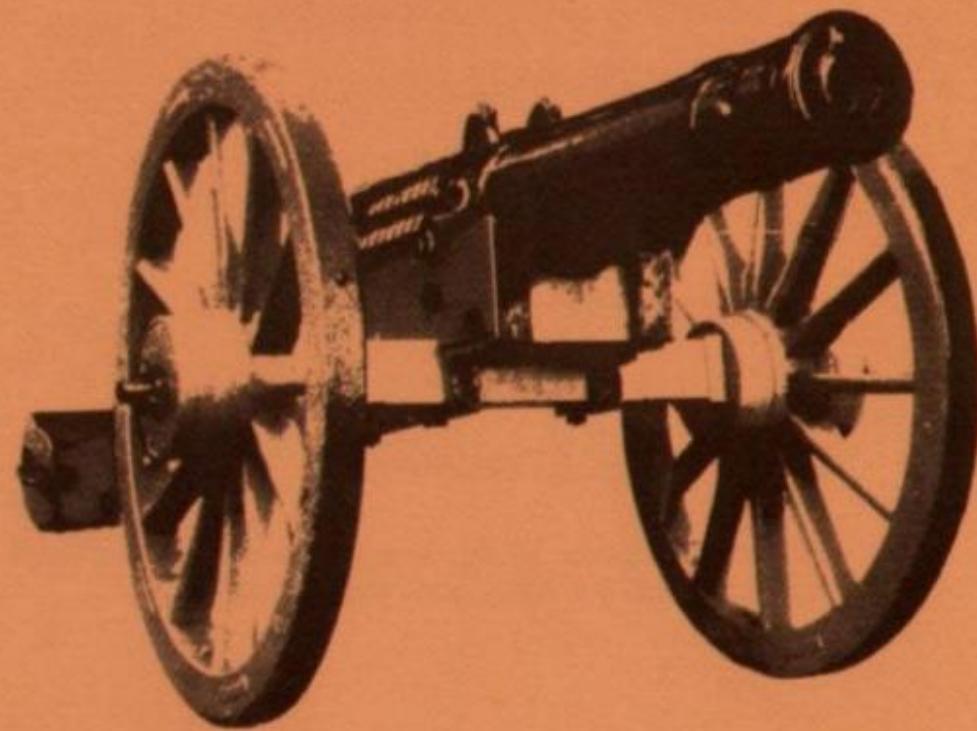
<http://www.heise.de/security/downloads/07/1/1/8/3/5/5/9/vmde.pdf>

AWESOMENESS IMPLEMENTED



80	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
70	NRWConfig.exe	1364	RegQueryValue	HKCU\Control Panel\Desktop\MultiUILanguageId	NAME NOT FOUND Length: 256
43	NRWConfig.exe	1364	RegCloseKey	HKCU\Control Panel\Desktop	SUCCESS
60	NRWConfig.exe	1364	RegCloseKey	HKCU	SUCCESS
20	NRWConfig.exe	1364	CreateFile	C:\WINDOWS\system32\comctl32.dll	SUCCESS Desired Access: General
36	NRWConfig.exe	1364	CreateFileMapping	C:\WINDOWS\system32\comctl32.dll	SUCCESS SyncType: SyncTypeDefault
50	NRWConfig.exe	1364	QueryStandardHandle	C:\WINDOWS\system32\comctl32.dll	SUCCESS AllocationSize: 618.49
71	NRWConfig.exe	1364	CreateFileMapping	C:\WINDOWS\system32\comctl32.dll	SUCCESS SyncType: SyncTypeDefault
90	NRWConfig.exe	1364	CreateFile	C:\WINDOWS\system32\comctl32.dll.124.Manifest	NAME NOT FOUND Desired Access: General
73	NRWConfig.exe	1364	CreateFile	C:\WINDOWS\system32\comctl32.dll.124.Config	NAME NOT FOUND Desired Access: General
08	NRWConfig.exe	1364	CloseFile	C:\WINDOWS\system32\comctl32.dll	SUCCESS
15	NRWConfig.exe	1364	RegOpenKey	HKCU	SUCCESS Desired Access: Read
33	NRWConfig.exe	1364	RegOpenKey	HKCU\Control Panel\Desktop	SUCCESS Desired Access: Read
15	NRWConfig.exe	1364	RegQueryValue	HKCU\Control Panel\Desktop\SmoothScroll	NAME NOT FOUND Length: 144
28	NRWConfig.exe	1364	RegCloseKey	HKCU\Control Panel\Desktop	SUCCESS
10	NRWConfig.exe	1364	RegCloseKey	HKCU	SUCCESS
06	NRWConfig.exe	1364	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\WS2HELP.dll	NAME NOT FOUND Desired Access: Read
99	NRWConfig.exe	1364	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\WS2_32.dll	NAME NOT FOUND Desired Access: Read
09	NRWConfig.exe	1364	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\HideDebugger.dll	NAME NOT FOUND Desired Access: Read
72	NRWConfig.exe	1364	ReadFile	C:\Program Files\NDA\plugins\HideDebugger.dll	SUCCESS Offset: 99.328, Length: 1024
65	NRWConfig.exe	1364	ReadFile	C:\Program Files\NDA\plugins\HideDebugger.dll	SUCCESS Offset: 132.096, Length: 1024
12	NRWConfig.exe	1364	ReadFile	C:\Program Files\NDA\plugins\HideDebugger.dll	SUCCESS Offset: 66.560, Length: 1024
47	NRWConfig.exe	1364	ReadFile	C:\Program Files\NDA\plugins\HideDebugger.dll	SUCCESS Offset: 168.960, Length: 1024
80	NRWConfig.exe	1364	ReadFile	C:\Program Files\NDA\plugins\HideDebugger.dll	SUCCESS Offset: 201.728, Length: 1024
36	NRWConfig.exe	1364	ReadFile	C:\Program Files\NDA\plugins\HideDebugger.dll	SUCCESS Offset: 33.792, Length: 1024
18	NRWConfig.exe	1364	RegOpenKey	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters	SUCCESS Desired Access: Maximum
16	NRWConfig.exe	1364	RegQueryValue	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\WinSock_Registry_Version	SUCCESS Type: REG_SZ, Length: 4
12	NRWConfig.exe	1364	RegQueryValue	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\WinSock_Registry_Version	SUCCESS Type: REG_SZ, Length: 4
56	NRWConfig.exe	1364	RegOpenKey	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9	SUCCESS Desired Access: Maximum
04	NRWConfig.exe	1364	RegQueryValue	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Serial_Access_Num	SUCCESS Type: REG_DWORD, Length: 4
08	NRWConfig.exe	1364	RegQueryValue	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Serial_Access_Num	SUCCESS Type: REG_DWORD, Length: 4
04	NRWConfig.exe	1364	RegOpenKey	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\00000005	NAME NOT FOUND Desired Access: Maximum
05	NRWConfig.exe	1364	RegQueryValue	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Next_Catalog_Entry	SUCCESS Type: REG_DWORD, Length: 4
94	NRWConfig.exe	1364	RegQueryValue	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Num_Catalog_Entry	SUCCESS Type: REG_DWORD, Length: 4
87	NRWConfig.exe	1364	RegOpenKey	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries	SUCCESS Desired Access: Maximum
26	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

UPATRE

SMALL | NASTY | THORNY | standardmalwareofftheself

PROTECTION

PACKER

PAYOUT

ANTI-SIMULATION

The image shows a debugger interface with two windows displaying assembly code. The top window shows the main function body, and the bottom window shows the end of the function. A yellow oval highlights a specific instruction in the middle window.

Top Window (Main Function Body):

```
0040142A
0040142A
0040142A
0040142A ; MMRESULT __stdcall acmMetrics_0(HACMOBJ hao, UINT uMetric, LPUOID pMetric)
0040142A acmMetrics_0 proc near
0040142A     mov     WndClass.hIcon, eax
0040142F     push    0                 ; pMetric
00401431     push    0                 ; uMetric
00401433     push    hao              ; hao
00401439     call    ds:acmMetrics
0040143F     cmp    eax, 5             ; HSYSERR_INVALIDHANDLE
00401442     jz     short locret_401446
```

Bottom Window (Function End):

```
00401444 add     al, [edx]
00401446 locret_401446:
00401446     retn
00401446 acmMetrics_0 endp
00401446
```

A yellow oval highlights the instruction `00401444 add al, [edx]`. A red arrow points from the instruction at address `0040143F` up to the highlighted instruction. A green arrow points down from the highlighted instruction to the `retn` instruction at address `00401446`.

WINDOW CONFUSION

and implicit breakpoint detection

The image shows two windows from a debugger. The top window displays the assembly code for the `decrypt_n_jumptab` procedure. The bottom window shows the entry point code.

Top Window (Procedure Code):

```
00401451
00401451
00401451
00401451 decrypt_n_jumptab proc near
00401451
00401451 var_4= dword ptr -4
00401451
00401451 xor     esi, esi
00401453 add    esi, offset unk_40100F
00401459 xor     edi, edi
0040145B add    edi, esi
0040145D mov    ebx, eax
0040145F add    ebx, 6
00401462 mov    eax, 30h
00401467 mov    edx, fs:[eax]
0040146A push   edx
0040146B push   0
0040146D mov    ecx, 34Ch
```

A large yellow checkmark is drawn over the instruction `mov edx, fs:[eax]`.

Bottom Window (Entry Point Code):

```
00401472
00401472 loc_401472:
00401472 mov     al, [esi]
00401474 sub     al, bl
00401476 stosb
00401477
0040147A dec     ecx
0040147B cmp     ecx, 0
0040147E jnz     short loc_401472
```

A large yellow circle highlights the `stosb` instruction. A green bracket points from the `var_4= dword ptr -4` declaration in the top window to the `stosb` instruction in the bottom window. A blue arrow points from the `start 40100F` label in the bottom window back up to the `decrypt_n_jumptab` procedure in the top window.

WANNABE

TIMING DEFENCE

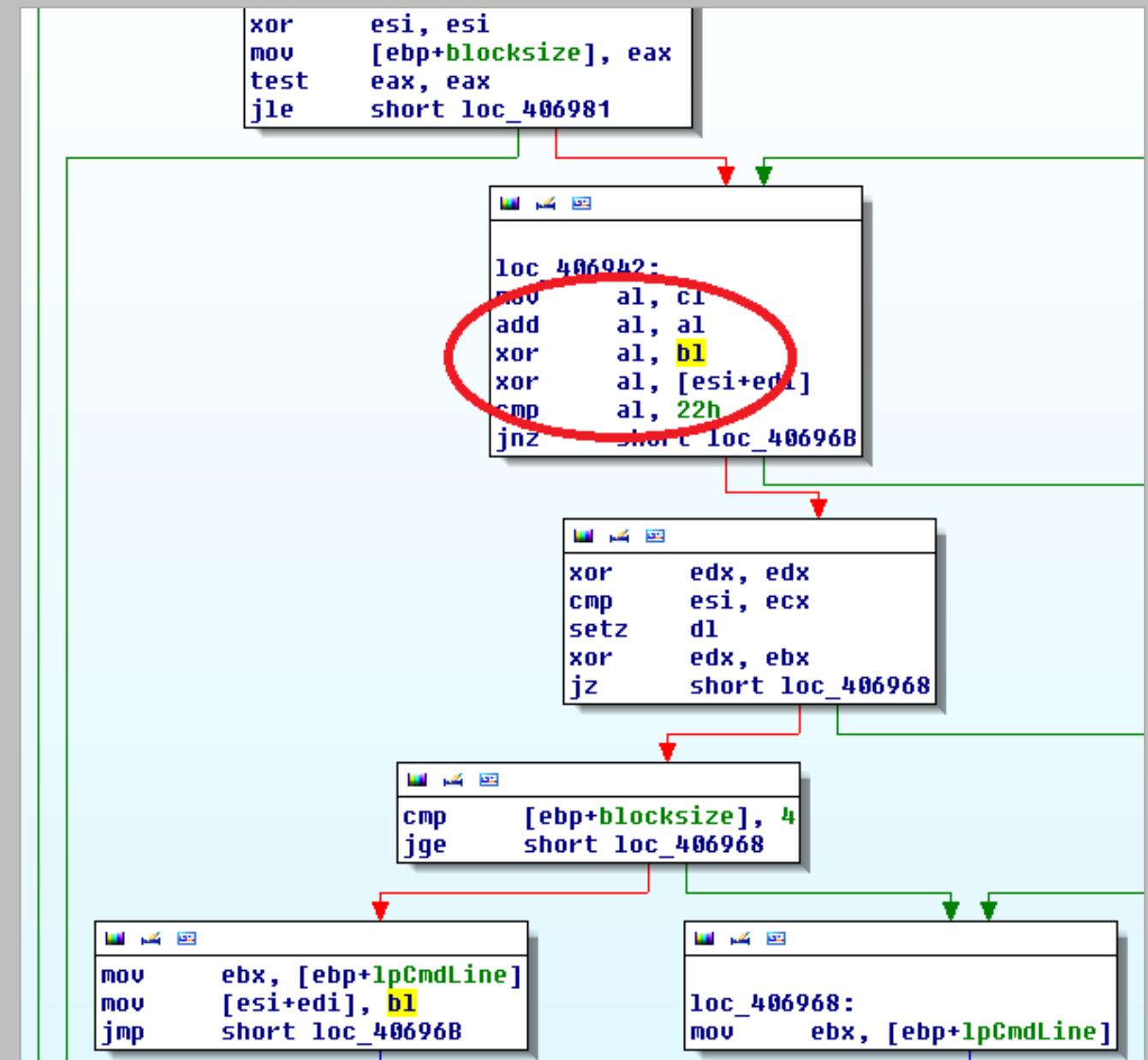
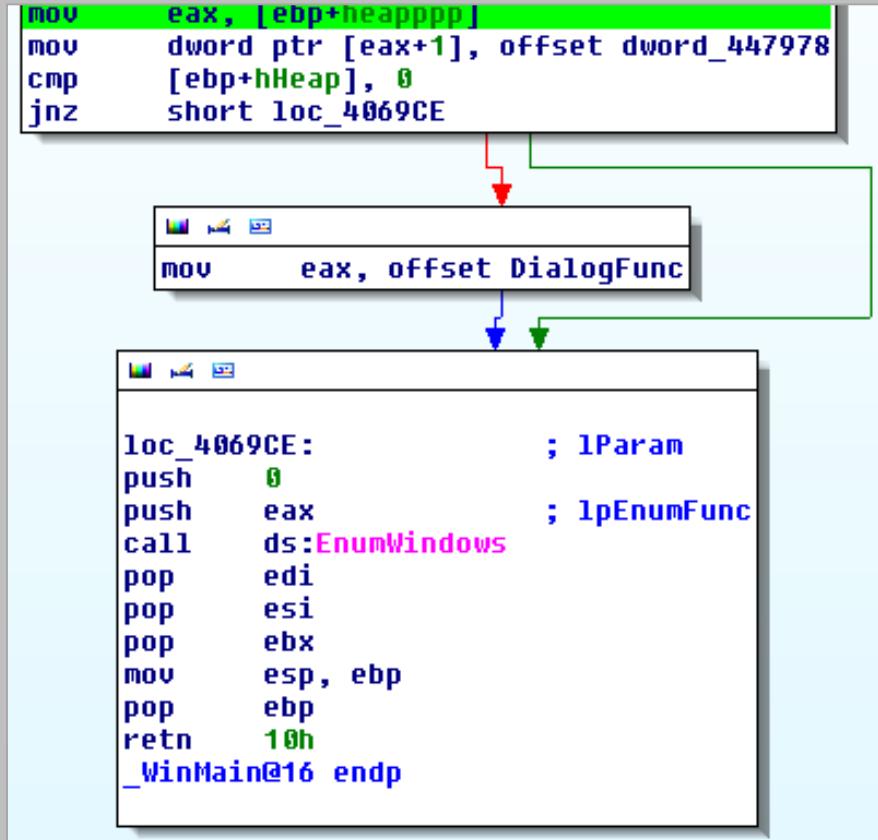
```
.text:00401111 mov    bl, ds:byte_40118F
.text:00401122 rdtsc
.text:00401123 push   eax
.text:00401124 mov    bh, [esi]
.text:00401125 mov    [edi], bh
.text:00401127 inc    edi
.text:00401128
.text:00401128 loc_401128:
.text:00401129 inc    esi
.text:0040112A inc    esi
.text:0040112B push   eax
.text:0040112C mov    al, [esi]
.text:0040112D stosb
.text:0040112E
.text:0040112F loc_40112F:
.text:0040112F add    [edi-1], bl
.text:00401132 pop    eax
.text:00401133 loop   loc_401128
.text:00401134 location_rdtsc endp
.text:00401135
.text:00401136 rdtsc
.text:00401137 nnn   edx
.text:00401138 sub    eax, edx
.text:00401139 sub    esp, 18h
.text:0040113D push   0
.text:0040113F push   heap_40304D
.text:00401145 call   dword ptr ds:acmStreamOpen
.text:00401145 ...
```

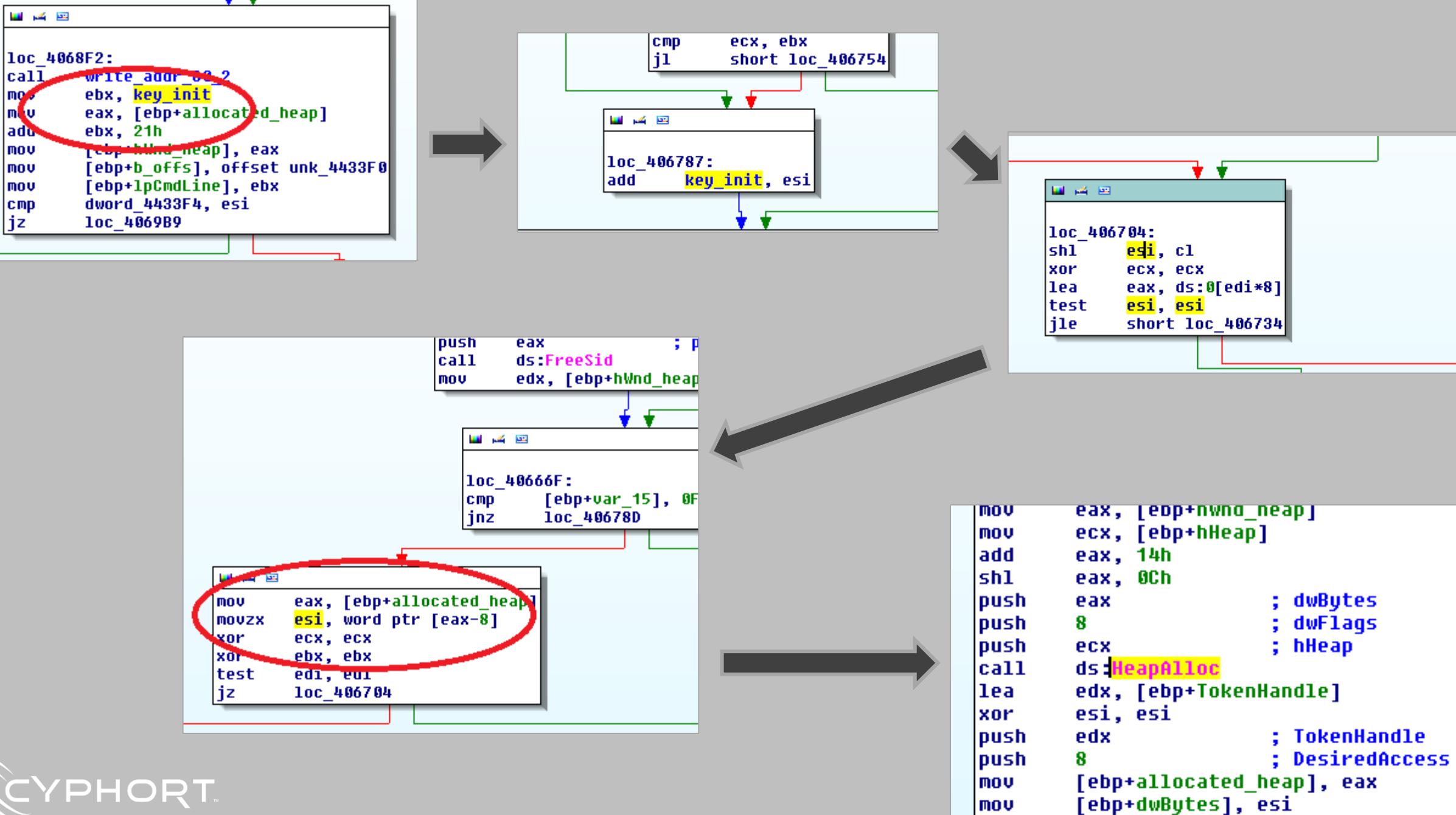
CITADEL

IDA Stealth Bruteforcing

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

Let's start at the end





WITH DEBUGGER

Hex View-1

009A0640	08	00	C8	00	00	01	00	00	EE	FF	EE	FF	00	00	00	00
009A0650	00	00	9A	00	00	40	00	00	00	00	9A	00	26	00	00	00
009A0660	80	06	9A	00	00	60	9C	00	04	00	00	00	01	00	00	00
009A0670	88	05	9A	00	00	00	00	00	98	46	9B	00	00	00	00	00
009A0680	03	28	08	00	60	07	18	00	00	00	00	00	00	00	00	00
009A0690	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009A06A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009A06B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009A06C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009A06D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

WITHOUT DEBUGGER

Hex View-1

009A0640	08	00	C8	00	00	01	00	00	EE	FF	EE	FF	00	00	00	00
009A0650	00	00	9A	00	00	40	00	00	00	00	9A	00	26	00	00	00
009A0660	80	06	9A	00	00	60	9C	00	04	00	00	00	01	00	00	00
009A0670	88	05	9A	00	00	00	00	00	88	46	9B	00	00	00	00	00
009A0680	01	28	08	00	34	01	08	00	00	00	00	00	00	00	00	00
009A0690	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009A06A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009A06B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009A06C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
009A06D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

```
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;
```

CVE-2014-1776

.html

vshow.swf

Heap Preparation

Timer Registration

cmmon.js

Eval (something)

Prepare ROP Chain

Corrupt Memory

Fill SoundObject with Shellcode

Invoke SoundObject.toString()

SNEAKY EXPLOIT BEING SNEAKY



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;
```

ALMOST WONDERFUL wonderfl



世界初！穴埋めで解く HTML5実力テスト応用編！3つのコースが加わりパワーアップしました！

wonderfl build Flash online

Welcome, Penny.Ullmayer • codes • users • games • events • tags • Q&A • wonderfl?

code search GO + Start to Write Code

Penny.Ullmay..

flash on 2014-5-25

forked:0 favorite:0 lines:75 license: MIT License modified: 2014-06-04 19:21:18

Embed <script type="text/javascript"> Tweet 0 Like 0 Preview Fullscreen

Code Fullscreen

```
1 package {
2     import flash.display.Sprite;
3     public class Tope extends Sprite {
4
5         private var m_dump7:String = "5467eba5baab6c9d94532121";
6         private var m_keys:String = "2eb31f09e9a77a0fde5a1a23ef";
7         private var m_trg:String = "42ee4b892986a326ea5aad10179";
8
9         public function Tope()
10        {
11
12             decode(this.m_trg).toString();
13        }
14
15
16         private function hexToIntArray(param1:String) : Vector<int>
17        {
18             var _loc_2:* = null;
19             var _loc_3:* = param1.length;
20             var _loc_4:* = 0;
21             var _loc_5:Vector<int> = new Vector<int>(_loc_3 / 2);
22             var _loc_6:* = 0;
23             while(_loc_4 < _loc_3)
24             {
25                 _loc_2 = _loc_3 - _loc_4;
26                 _loc_6 = _loc_2 % 16;
27                 _loc_5[_loc_4] = _loc_6;
28                 _loc_4++;
29             }
30
31             return _loc_5;
32        }
33
34         private function hexToString(param1:String) : String
35        {
36             var _loc_2:String = "";
37             var _loc_3:int = param1.length;
38             var _loc_4:int = 0;
39             var _loc_5:Vector<int> = hexToIntArray(param1);
40             while(_loc_4 < _loc_3)
41             {
42                 _loc_2 += _loc_5[_loc_4];
43                 _loc_4++;
44             }
45
46             return _loc_2;
47        }
48
49        public function encode():String
50        {
51            var _loc_2:String = "";
52            var _loc_3:int = m_trg.length;
53            var _loc_4:int = 0;
54            var _loc_5:Vector<int> = hexToIntArray(m_trg);
55            while(_loc_4 < _loc_3)
56            {
57                _loc_2 += _loc_5[_loc_4];
58                _loc_4++;
59            }
60
61            return _loc_2;
62        }
63
64    }
```

▶ Play

Fork Edit Download

```
private var delay:uint = 1000;
private var snd:Sound;
private var m_dump7:String = "5467eba5baab6c9d945321215d4f075251af2717b30cde85bdcede9d17bfb6eff2aa25e9b34ad7a1670ab5abc27b1";
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){}
```

MIUREF

and it's packer

Once upon a time ...

Visual Basic 6.0

Microsoft, 1998

Object-based / event-driven

Rapid Application Development

Replaced by VB.NET

End of support in 2008



VB6 IS NOT DEAD



```
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 4505AF07h, 74CD8DB4h, 0F9961AA2h, 4D765813h, 3F4F90BDh
dd 05304B4h, 33AD4F3Ah, 11CF6699h, 0AA000CB7h, 93D36000h
dd 5D72EF40h, 0
dd 0FCFB302Eh, 1068A0FAh, 838A7h, 0B571332Bh, 505C3A43h
dd 72676F72h, 46206D61h, 73656C69h, 63694D5Ch, 6F736F72h
dd 50207466h, 61757369h, 7453206Ch, 6F696475h, 3942565Ch
dd 40565C38h, 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↓
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↓
; .text:00401580↓ ...
dd offset dword_401820
dd 0FFFFFFFh, 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
134Ch, 401384h, 4022C8h, 2 dup(0)
33AD4EF2h, 11CF6699h, 0AA0000CB7h, 93D36000h
```

... FC C8 13 76 ...



23:14:14,4220474 msgbox Just c... 356 Thread Exit
23:14:14,4246438 msgbox Just c... 356 Thread Create
23:14:14,4540749 msgbox Just c... 356 Thread Exit
23:14:14,4654225 msgbox Just c... 356 Thread Create
23:14:14,4688433 msgbox Just c... 356 Thread Exit
23:14:14,4716808 msgbox Just c... 356 Thread Create
23:14:14,4999919 msgbox Just c... 356 Thread Exit
23:14:14,5031882 msgbox Just c... 356 Thread Create
23:14:14,5308285 msgbox Just c... 356 Thread Exit
23:14:14,5338636 msgbox Just c... 356 Thread Create
23:14:14,5621018 msgbox Just c... 356 Thread Exit
23:14:14,5652441 msgbox Just c... 356 Thread Create
23:14:14,5938656 msgbox Just c... 356 Thread Exit
23:14:14,5990288 msgbox Just c... 356 Thread Create
23:14:14,6096176 msgbox Just c... 356 Thread Exit
23:14:14,6127552 msgbox Just c... 356 Thread Create
23:14:14,6402246 msgbox Just c... 356 Thread Exit
23:14:14,6433384 msgbox Just c... 356 Thread Create
23:14:14,6715177 msgbox Just c... 356 Thread Exit
23:14:14,6746130 msgbox Just c... 356 Thread Create
23:14:14,7027163 msgbox Just c... 356 Thread Exit
23:14:14,7057066 msgbox Just c... 356 Thread Create
23:14:14,7339756 msgbox Just c... 356 Thread Exit
23:14:14,7369989 msgbox Just c... 356 Thread Create
23:14:14,7496653 msgbox Just c... 356 Thread Exit
23:14:14,7522760 msgbox Just c... 356 Thread Create
23:14:14,7811637 msgbox Just c... 356 Thread Exit
23:14:14,7840959 msgbox Just c... 356 Thread Create
23:14:14,8120361 msgbox Just c... 356 Thread Exit
23:14:14,8150728 msgbox Just c... 356 Thread Create
23:14:14,8457767 msgbox Just c... 356 Thread Exit
23:14:14,8489293 msgbox Just c... 356 Thread Create
23:14:14,8744842 msgbox Just c... 356 Thread Exit
23:14:14,8774748 msgbox Just c... 356 Thread Create
23:14:14,9058229 msgbox Just c... 356 Thread Exit
23:14:14,9091638 msgbox Just c... 356 Thread Create
23:14:14,9369000 msgbox Just c... 356 Thread Exit
23:14:14,9479070 msgbox Just c... 356 Thread Create
23:14:14,9532359 msgbox Just c... 356 Thread Exit
23:14:14,9583558 msgbox Just c... 356 Thread Create
23:14:14,9835663 msgbox Just c... 356 Thread Exit
23:14:14,9864320 msgbox Just c... 356 Thread Create
23:14:15,0147691 msgbox Just c... 356 Thread Exit
23:14:15,0198035 msgbox Just c... 356 Thread Create
23:14:15,0462237 msgbox Just c... 356 Thread Exit
23:14:15,0489528 msgbox Just c... 356 Thread Create
23:14:15,0938244 msgbox Just c... 356 Thread Exit
23:14:15,0964739 msgbox Just c... 356 Thread Create
23:14:15,1252326 msgbox Just c... 356 Thread Exit
23:14:15,1278078 msgbox Just c... 356 Thread Create
23:14:15,1567950 msgbox Just c... 356 Thread Exit
23:14:15,1595716 msgbox Just c... 356 Thread Create
23:14:15,1880112 msgbox Just c... 356 Thread Exit
23:14:15,1907691 msgbox Just c... 356 Thread Create
23:14:15,2187741 msgbox Just c... 356 Thread Exit
23:14:15,2228550 msgbox Just c... 356 Thread Create
23:14:15,2502068 msgbox Just c... 356 Thread Exit
23:14:15,2530460 msgbox Just c... 356 Thread Create

SISYDYNAMIC

SUCCESS Thread ID: 2536, User Time: 0.0000000, Kernel Time: 0.0000000
SUCCESS Thread ID: 2344
SUCCESS Thread ID: 2344, User Time: 0.0000000, Kernel Time: 0.0000000
SUCCESS Thread ID: 2420
SUCCESS Thread ID: 2420, User Time: 0.0000000, Kernel Time: 0.0000000
SUCCESS Thread ID: 3912
SUCCESS Thread ID: 3912, User Time: 0.0000000, Kernel Time: 0.0000000
SUCCESS Thread ID: 3784
SUCCESS Thread ID: 3784, User Time: 0.0000000, Kernel Time: 0.0000000
SUCCESS Thread ID: 2916
SUCCESS Thread ID: 2916, User Time: 0.0000000, Kernel Time: 0.0000000
SUCCESS Thread ID: 1800
SUCCESS Thread ID: 1800, User Time: 0.0000000, Kernel Time: 0.0000000
SUCCESS Thread ID: 584
SUCCESS Thread ID: 584, User Time: 0.0000000, Kernel Time: 0.0000000
SUCCESS Thread ID: 3740
SUCCESS Thread ID: 3740, User Time: 0.0000000, Kernel Time: 0.0000000
SUCCESS Thread ID: 2784
SUCCESS Thread ID: 2784, User Time: 0.0000000, Kernel Time: 0.0000000
SUCCESS Thread ID: 2516
SUCCESS Thread ID: 2516, User Time: 0.0000000, Kernel Time: 0.0000000
SUCCESS Thread ID: 3796
SUCCESS Thread ID: 3796, User Time: 0.0000000, Kernel Time: 0.0000000
SUCCESS Thread ID: 3208
SUCCESS Thread ID: 3208, User Time: 0.0000000, Kernel Time: 0.0000000
SUCCESS Thread ID: 3780
SUCCESS Thread ID: 3780, User Time: 0.0000000, Kernel Time: 0.0000000
SUCCESS Thread ID: 1892
SUCCESS Thread ID: 1892, User Time: 0.0000000, Kernel Time: 0.0000000
SUCCESS Thread ID: 2608
SUCCESS Thread ID: 2608, User Time: 0.0000000, Kernel Time: 0.0000000
SUCCESS Thread ID: 2560
SUCCESS Thread ID: 2560, User Time: 0.0000000, Kernel Time: 0.0000000
SUCCESS Thread ID: 3284
SUCCESS Thread ID: 3284, User Time: 0.0000000, Kernel Time: 0.0000000
SUCCESS Thread ID: 3284
SUCCESS Thread ID: 3284, User Time: 0.0000000, Kernel Time: 0.0000000
SUCCESS Thread ID: 3016
SUCCESS Thread ID: 3016, User Time: 0.0000000, Kernel Time: 0.0000000
SUCCESS Thread ID: 2016
SUCCESS Thread ID: 2016, User Time: 0.0000000, Kernel Time: 0.0000000
SUCCESS Thread ID: 212
SUCCESS Thread ID: 212, User Time: 0.0000000, Kernel Time: 0.0000000
SUCCESS Thread ID: 600
SUCCESS Thread ID: 600, User Time: 0.0000000, Kernel Time: 0.0000000
SUCCESS Thread ID: 856
SUCCESS Thread ID: 856, User Time: 0.0000000, Kernel Time: 0.0000000
SUCCESS Thread ID: 2896
SUCCESS Thread ID: 2896, User Time: 0.0000000, Kernel Time: 0.0000000
SUCCESS Thread ID: 3236
SUCCESS Thread ID: 3236, User Time: 0.0000000, Kernel Time: 0.0000000
SUCCESS Thread ID: 2648
SUCCESS Thread ID: 2648, User Time: 0.0000000, Kernel Time: 0.0000000
SUCCESS Thread ID: 3876
SUCCESS Thread ID: 3876, User Time: 0.0000000, Kernel Time: 0.0000000
SUCCESS Thread ID: 3864
SUCCESS Thread ID: 3864, User Time: 0.0000000, Kernel Time: 0.0000000
SUCCESS Thread ID: 3864
SUCCESS Thread ID: 3864, User Time: 0.0000000, Kernel Time: 0.0000000
SUCCESS Thread ID: 3536
SUCCESS Thread ID: 3536, User Time: 0.0000000, Kernel Time: 0.0000000
SUCCESS Thread ID: 2096

VB Decompiler v9.2

File Tools Plugins Help

FileName: C:\Documents and Settings\Administrator\Desktop\generic.tar\msgbox_just_cuckoo.exe

P-Code

Project

- Forms
- q
- UserControls

Code

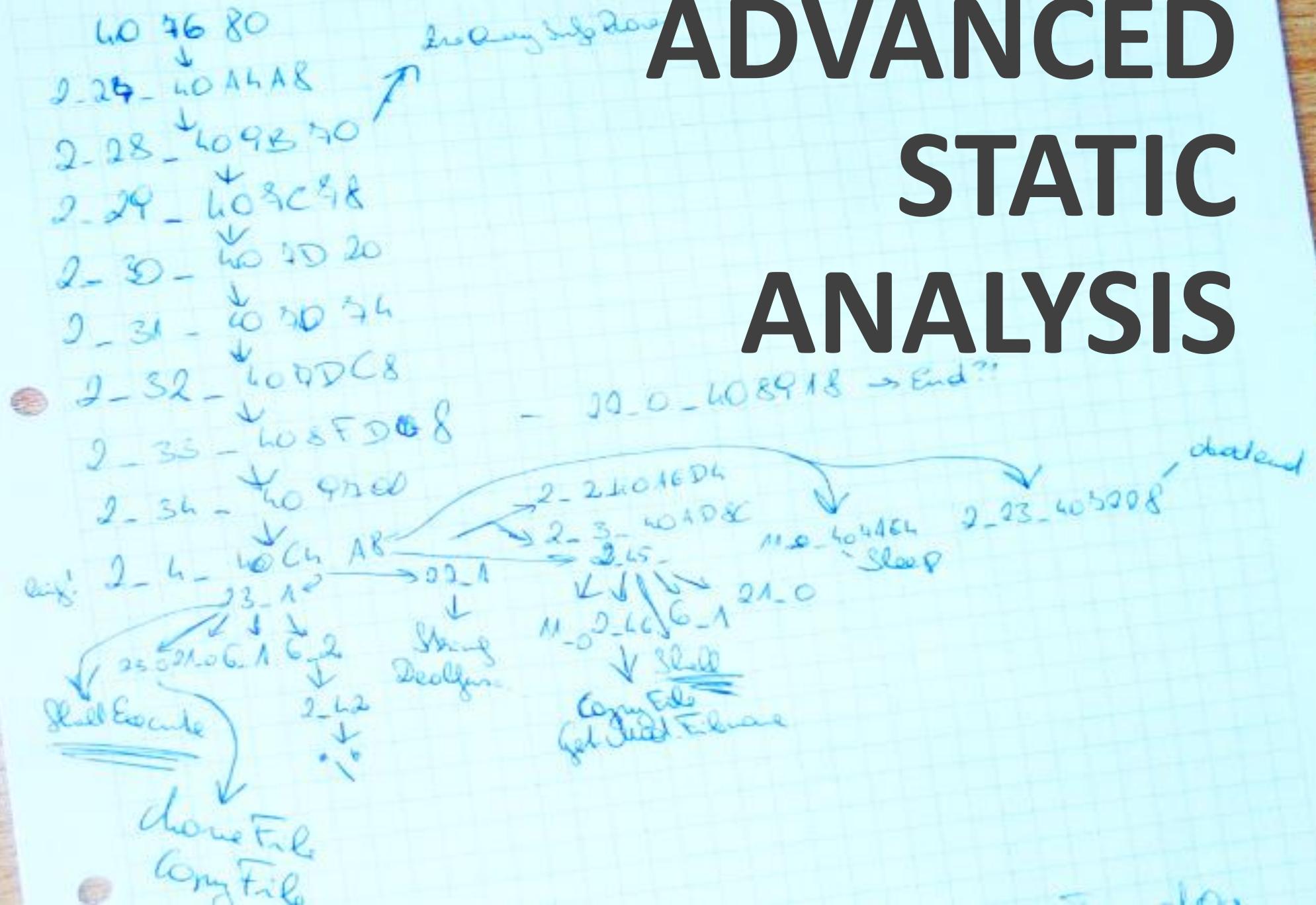
- q
 - Proc_0_0_407680
- BDe
- DA
 - Proc_2_0_4084B0
 - Proc_2_1_420CAC
 - Proc_2_2_40A6D4
 - Proc_2_3_40AD8C
 - Proc_2_4_40C4A8
 - Proc_2_5_40F8A8
 - Proc_2_6_4086B8
 - Proc_2_7_4083AC
 - Proc_2_8_407104
 - Proc_2_9_407710
 - Proc_2_10_407ED4
 - Proc_2_11_4289CC
 - Proc_2_12_40D358
 - Proc_2_13_40A7FC
 - Proc_2_14_4082BC
 - Proc_2_15_408534
 - Proc_2_16_4081D8
 - Proc_2_17_408F14
 - Proc_2_18_41B2EC
 - Proc_2_19_5A3C
 - Proc_2_20_4_118
 - Proc_2_21_4_158
 - Proc_2_22_4CD0
 - Proc_2_23_407228
 - Proc_2_24_4076C0
 - Proc_2_25_4070CC
 - Proc_2_26_409E60
 - Proc_2_27_40A4A8
 - Proc_2_28_409B70
 - Proc_2_29_407C78

P-Code

```
loc_41A606: var_F4 = CStr(var_CC(0))
loc_41A64D: Proc_2_36_40ABF8(var_CC, var_A4, Proc_21_0_408748(CStr(&H3A), 0), -1)
loc_41A65C: var_108 = CStr(var_CC(0))
loc_41A67B: If (Len(var_F4) > 3) Then
loc_41A86F: ReDim var_274(0 To -1)
var_1C8 = Proc_21_0_408748(CStr(&H47)) & Proc_21_0_408748(CStr(&H65)) & Proc_21_0_408748(CStr(&H74)) & Proc_21_0_408748(CStr(&H4))
var_1F8 = var_1C8 & Proc_21_0_408748(CStr(&H72)) & Proc_21_0_408748(CStr(&H72)) & Proc_21_0_408748(CStr(&H65)) & Proc_21_0_40874
var_228 = var_1F8 & Proc_21_0_408748(CStr(&H74)) & Proc_21_0_408748(CStr(&H50)) & Proc_21_0_408748(CStr(&H72)) & Proc_21_0_40874
var_258 = var_228 & Proc_21_0_408748(CStr(&H63)) & Proc_21_0_408748(CStr(&H65)) & Proc_21_0_408748(CStr(&H73)) & Proc_21_0_40874
var_134 = Proc_21_0_408748(CStr(&H6B), CLng(AscW(var_108))) & Proc_21_0_408748(CStr(&H65), 1) & Proc_21_0_408748(CStr(&H72)) & P
var_164 = var_134 & Proc_21_0_408748(CStr(&H65)) & Proc_21_0_408748(CStr(&H6C)) & Proc_21_0_408748(CStr(&H33)) & Proc_21_0_40874
var_26C = var_164 & Proc_21_0_408748(CStr(&H2E)) & Proc_21_0_408748(CStr(&H64)) & Proc_21_0_408748(CStr(&H6C)) & Proc_21_0_40874
PropBag.WriteProperty(var_26C, var_258 & Proc_21_0_408748(CStr(&H49)) & Proc_21_0_408748(CStr(&H64)), var_274)
Erase var_274
var_110 = var_B8
ReDim var_274(0 To 2)
var_274(0) = &H1FOFFF
var_274(1) = False
var_274(2) = var_110
var_1C8 = Proc_21_0_408748(CStr(&H4F)) & Proc_21_0_408748(CStr(&H70)) & Proc_21_0_408748(CStr(&H65)) & Proc_21_0_408748(CStr(&H6
var_1F8 = var_1C8 & Proc_21_0_408748(CStr(&H72)) & Proc_21_0_408748(CStr(&H6F)) & Proc_21_0_408748(CStr(&H63)) & Proc_21_0_40874
var_134 = Proc_21_0_408748(CStr(&H6B), var_110) & Proc_21_0_408748(CStr(&H65), var_B8) & Proc_21_0_408748(CStr(&H72)) & Proc_21_
var_164 = var_134 & Proc_21_0_408748(CStr(&H65)) & Proc_21_0_408748(CStr(&H6C)) & Proc_21_0_408748(CStr(&H33)) & Proc_21_0_40874
var_20C = var_164 & Proc_21_0_408748(CStr(&H2E)) & Proc_21_0_408748(CStr(&H64)) & Proc_21_0_408748(CStr(&H6C)) & Proc_21_0_40874
PropBag.WriteProperty(var_20C, var_1F8 & Proc_21_0_408748(CStr(&H73)) & Proc_21_0_408748(CStr(&H73)), var_274)
Erase var_274
var_2F4 = var_B8
var_B8 = GetModuleFileNameW(AscW(var_108))
ReDim var_274(0 To 4)
var_274(0) = var_2F4
var_274(1) = CLng(Proc_21_0_408748(CStr(&H4F), var_8 & Proc_21_0_408748(CStr(&H34), "cH", var_2F4)) & var_F4)
var_274(2) = &H
var_274(3) = &H
var_274(4) = CVar(GetModuleFileNameW(var_B8))
var_1C8 = Proc_21_0_408748(CStr(&H77)) & Proc_21_0_408748(CStr(&H68)) & Proc_21_0_408748(CStr(&H69)) & Proc_21_0_408748(CStr(&H7
var_1F8 = var_1C8 & Proc_21_0_408748(CStr(&H50)) & Proc_21_0_408748(CStr(&H72)) & Proc_21_0_408748(CStr(&H6F)) & Proc_21_0_40874
var_228 = var_1F8 & Proc_21_0_408748(CStr(&H65)) & Proc_21_0_408748(CStr(&H73)) & Proc_21_0_408748(CStr(&H73)) & Proc_21_0_40874
var_258 = var_228 & Proc_21_0_408748(CStr(&H65)) & Proc_21_0_408748(CStr(&H6D)) & Proc_21_0_408748(CStr(&H6F)) & Proc_21_0_40874
var_140 = Proc_21_0_408748(CStr(&H4B)) & Proc_21_0_408748(CStr(&H65)) & Proc_21_0_408748(CStr(&H72)) & Proc_21_0_408748(CStr(&H6
var_170 = var_140 & Proc_21_0_408748(CStr(&H6C)) & Proc_21_0_408748(CStr(&H33)) & Proc_21_0_408748(CStr(&H32)) & Proc_21_0_40874
```

Decompiled OK

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

Local Win32 debugger

IDA View-EIP, Call Stack, Breakpoints, General registers, Modules, Threads, Hex View-EAX, Stack view

Structures

Break

Trace window

EAX 7FFD2084 ↳ debug006:unk_7FFD2084
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_just_cuckoo.exe 00400000 00040000
C:\Program Files\IDA\plugins\HideDebugger.dll 10000000 000510
C:\WINDOWS\System32\uxtheme.dll 5AB70000 00038C
C:\WINDOWS\System32\netapi32.dll 5B860000 00055C
C:\WINDOWS\System32\comct132.dll 5D090000 0009AC
C:\WINDOWS\System32\faultrep.dll 69450000 00160
C:\WINDOWS\System32\wappwp.dll 71AA0000 00008C

DEB
U
G
G
I
N
G

Hex View-EAX

Stack view

UNKNOWN 7C912EF1: ntdll.dll:ntdll_RtlEqualUnicodeString+56

UNKNOWN 0001039E: debug001:0001039E

UNKNOWN 0001040E: debug001:0001040E

UNKNOWN 7C800041: kernel32.dll:7C800041

UNKNOWN 0145EC78: Stack[00000F24]:0145EC78

Output window

Flush buffers, please wait...ok

AU: idle | Down | Disk: 4GB |

Edit Jump Search View Debugger Options Windows Help



IDA View-EIP, General registers, Modules, Threads, Hex View-1, Stack view



Structures

Enums



General registers

EAX	↳
EBX	↳
ECX	↳
EDX	↳
ESI	↳
EDI	↳
EBP	↳
ESP	↳
EIP	↳
EFL	↳

Modules

Path
C:\Documents and Settings\Administrat
C:\WINDOWS\system32\kernel32.c

Threads

Decimal	Hex	State
2436	984	Ready

DEBUGGING

```
.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.)
.idata:00401000 ; Offset to data section: 00001000
.idata:00401000 ; Flags: 00000020: T executable P readable
.idata:00401000 ; Alignment : default
.idata:00401000 ; Import : MSUB
.idata:00401000 ; Segments : Ext
.idata:00401000 ; .idata:00401000
.idata:00401000 rtcSin dd 72A1CB7Fh
.idata:00401000 ; DATA XREF: .text:00401132jr
.idata:00401000 ; .text:00428C4410
.idata:00401000 rtcCos dd 72A1CBA8h
.idata:00401000 ; DATA XREF: .text:0040112Cjr
.idata:00401000 rtcRgb dd 72A1CC8Dh
.idata:00401000 ; DATA XREF: .text:004010EAjr
.idata:00401000 rtcCharValueBstr dd 72A2710Bh
.idata:00401000 ; DATA XREF: .text:0040111Ajr
.idata:00401018 rtcBstrFromChar dd 72A20F81h
.idata:00401018 ; DATA XREF: .text:00401180jr
.idata:00401014 NethCallEngine dd 72A43B68h
.idata:00401018 rtcLowerCaseVar dd 72A275A0h
.idata:0040101C rtcTrimBstr dd 72A27601h
.idata:00401020 __vbaCopyBytes dd 72A1A0F3h
.idata:00401024 rtcVarFromFormatVar dd 72A3642Bh
.idata:00401028 rtcEnvironBstr dd 72A1DB60h
.idata:00401032 rtcSwitch dd 72A1DD91h
.idata:00401030 rtcIsMissing dd 72A1D6FDh
.idata:00401034 rtcMsgBox dd 72A1D132h
.idata:00401038 rtcMidCharBstr dd 72A26FE2h
.idata:0040103C rtcSpaceBstr dd 72A27DB9h
.idata:00401040 EVENT_SINK_AddRef dd 72A09B74h
.idata:00401044 rtcUpperCaseBstr dd 72A27F8Ah
.idata:00401048 rtcIsNull dd 72A1C9B4h
.idata:0040104C rtcIsNumeric dd 72A1C9CAh
.idata:00401050 __imp_DllFunctionCall dd 7294A0FDh
.idata:00401054 rtcCommandVar dd 72A1DE02h
.idata:00401058 rtcPPMT dd 72A368A9h
.idata:0040105C EVENT_SINK_Release dd 72A09B87h
.idata:00401060 rtcShell dd 72A8CE69h
.idata:00401064 EVENT_SINK_QueryInterface dd 72A09A85h
.idata:00401068 __vbaExceptHandler dd 72A247DFh
.idata:0040106C rtcReplace dd 72A389C4h

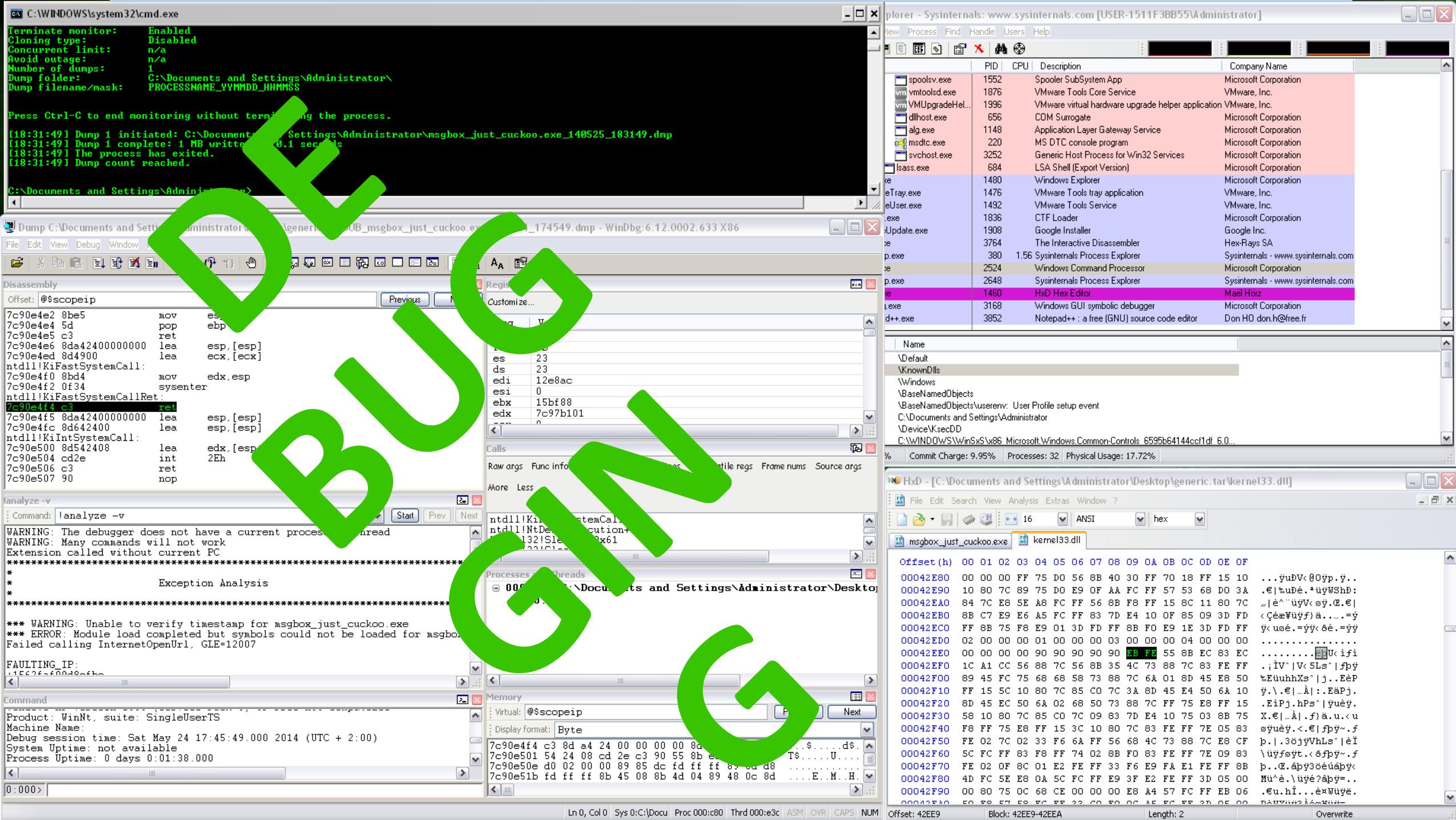
```

00001000 00401000: .idata:rtcSin

Stack view

0110h 68 20 20 40 60 80 F8 F0 FF FF FF FF 00 00 00 00 00 00 b Q F=

0001110h J 02 82 868



EVER HEARD OF.. kernel33.dll ?

Offset(h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	...
00042E80	00 00 00 FF 75 D0 56 8B 40 30 FF 70 18 FF 15 10	...ýuDV<0Oýp.ý..
00042E90	10 80 7C 89 75 D0 E9 0F AA FC FF 57 53 68 D0 3A	.€ %uDé.^üýWSHd:
00042EA0	84 7C E8 5E A8 FC FF 56 8B F8 FF 15 8C 11 80 7C	/ è^"üýV<øý.€
00042EB0	8B C7 E9 E6 A5 FC FF 83 7D E4 10 0F 85 09 3D FD	<ÇéæVüýf}ä....=ý
00042EC0	FF 8B 75 F8 E9 01 3D FD FF 8B F0 E9 1E 3D FD FF	ý< uøé.=ýý< ðé.=ýý
00042ED0	02 00 00 00 01 00 00 00 03 00 00 00 04 00 00 00
00042EE0	00 00 00 00 90 90 90 90 90 EB FE 55 8B EC 83 ECEBU<ifi
00042EF0	1C A1 CC 56 88 7C 56 8B 35 4C 73 88 7C 83 FE FF	.;IV^ V<5Ls^ fpý
00042F00	89 45 FC 75 68 68 58 73 88 7C 6A 01 8D 45 E8 50	%EüuhhXs^ j..EèP
00042F10	FF 15 5C 10 80 7C 85 C0 7C 3A 8D 45 E4 50 6A 10	ý.\.€ _À :.EäPj.
00042F20	8D 45 EC 50 6A 02 68 50 73 88 7C FF 75 E8 FF 15	.EiPj.hPs^ ýuèý.
00042F30	58 10 80 7C 85 C0 7C 09 83 7D E4 10 75 03 8B 75	X.€ _À .f}ä.u.<u
00042F40	F8 FF 75 E8 FF 15 3C 10 80 7C 83 FE FF 7E 05 83	øýuèý.<.€ fpý~.f
00042F50	FE 02 7C 02 33 F6 6A FF 56 68 4C 73 88 7C E8 CF	b. .3öjýVhLs^ èI
00042F60	5C FC FF 83 F8 FF 74 02 8B F0 83 FE FF 7E 09 83	\üýføyt.<ðfpý~.f
00042F70	FE 02 0F 8C 01 E2 FE FF 33 F6 E9 FA E1 FE FF 8B	b..€.âpý3öéúâpý<
00042F80	4D FC 5E E8 0A 5C FC FF E9 3F E2 FE FF 3D 05 00	Mü^è.\üýé?âpý=..
00042F90	00 80 75 OC 68 CE 00 00 00 E8 A4 57 FC FF EB 06	.€u.hî...èxWüýe.
00042FA0	50 F0 F2 F0 FC FF 22 C0 F0 A5 FC FF 2D 05 00

Offset: 42EE9

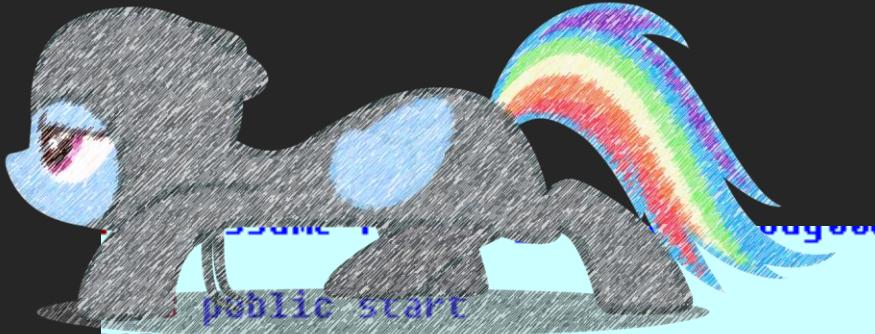
Block: 42EE9-42EEA

Length: 2

Overwrite

Dynamic API Loading

... Crap.



```
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, 41000h, 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, 69727548h, 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(0FFFFFFFh), 2A7C7C2Ah, 9AAh, 26Ah dup(0BC00BC00h)
```

Trace window		
Thread	Address	
2	00000F54	kernel32.dll:kernel32_CreateProcessW

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  
NRWConfig.exe:004022F0 add    esp, 1Ch
```

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
```

```
003F2366 mov [ebp+var_120C], eax
003F236C lea eax, [ebp+ThreadContext]
003F2372 push eax
003F2373 push [ebp+ProcID]
003F2376 call [ebp+SetThreadContext]
003F237C push [ebp+ProcID]
003F237F call [ebp+ResumeThread]
003F2385 cmp [ebp+RecLevel], 7
003F2389 jnz short loc_3F23A3

003F238B push ebx
003F238C call [ebp+var_498]
003F2392 push eax
003F2393 call [ebp+terminate]

003F2399 loc_3F2399
003F2399 cmp [ebp+LoopCount], 64h
003F239D jl loc_3F2238
```

C++ PACKER

```
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
00000F54 kernel32.dll:kernel32_CreateProcessW

003F2399 loc_3F2399
003F2399 cmp [ebp+LoopCount], 64h
003F239D jl loc_3F2238
```

VB6 PACKER

THANK YOU!

Marion Marschalek



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

