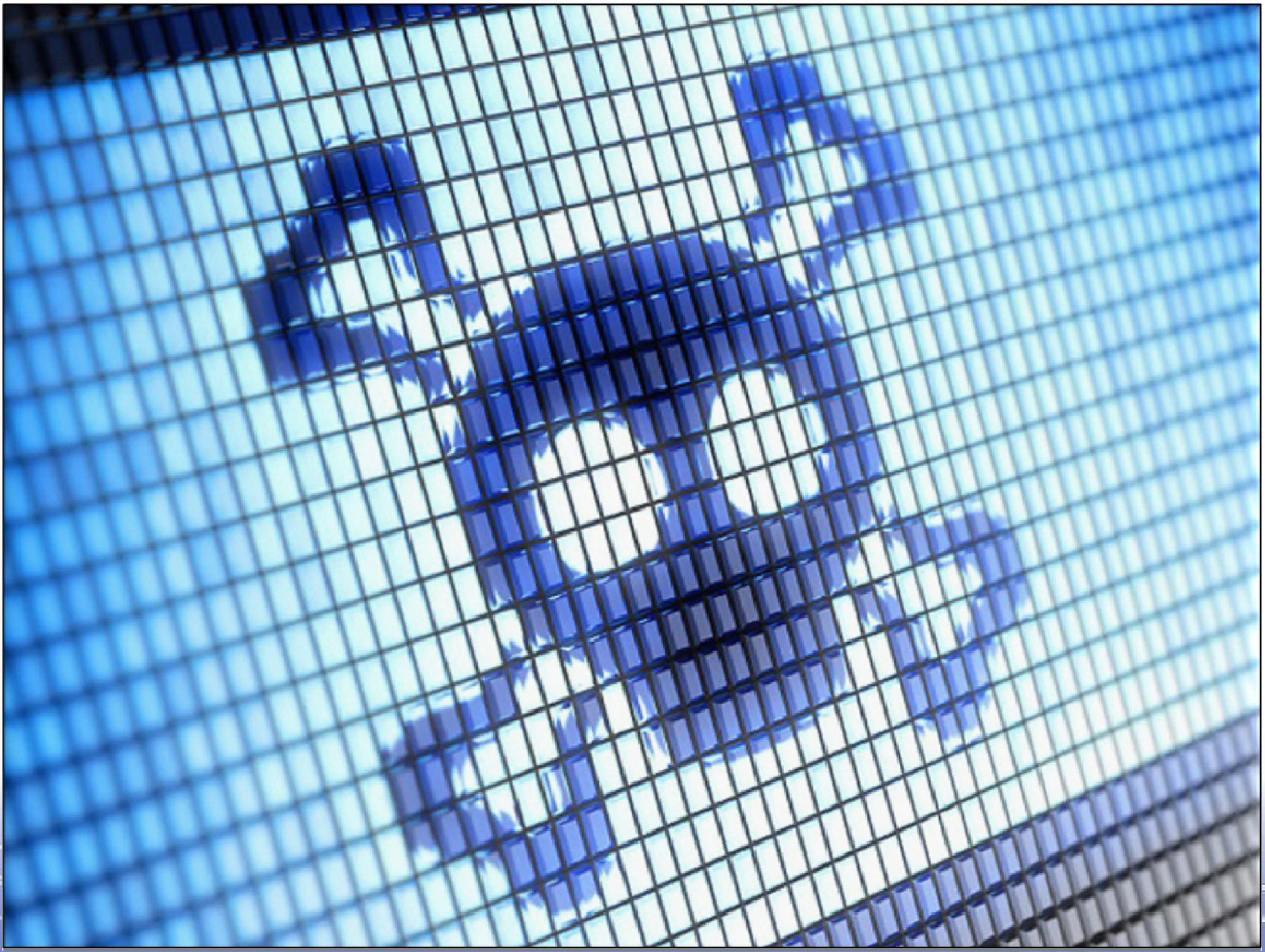
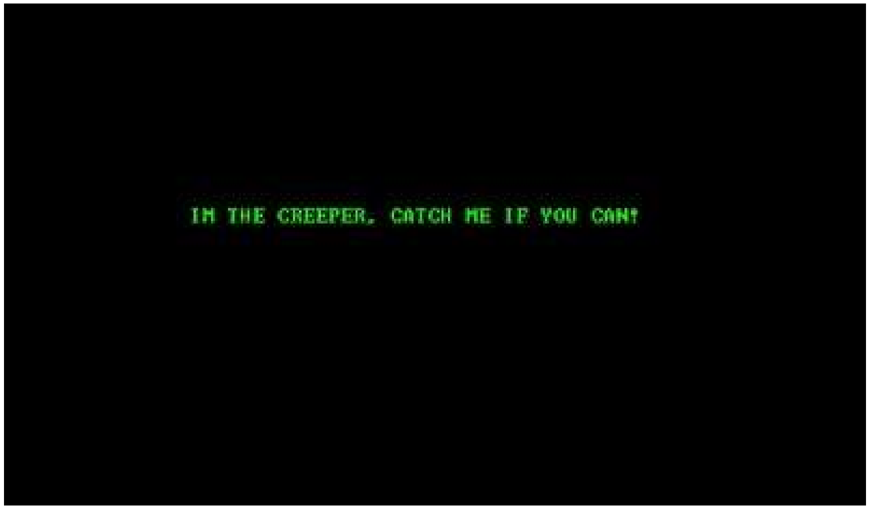


Översikt

- Från creeper till z-bot
- Vad malware gör bra samt dåligt
- QA till malware skrivare
- Anti-debug, Anti-instrumentering
- Framtid



```
IM THE CREEPER, CATCH ME IF YOU CAN!
```

“Welcome to the Dungeon ©”

- 1971 – Creeper
- 1986 – Brain
- 1988 – Morris
- 1991 – Michaelangelo
- 2000 – I Love you
- 2007 - Zeus/Citadel/z-bot

Map
Sat
Ter
Earth
Finland
Iceland
Russia
Canada
China
North Atlantic Ocean
Libya
Mali
Niger
Chad
Sudan
R Congo
Madagasc
Indian Ocean
South Atlantic Ocean

Idag i siffror

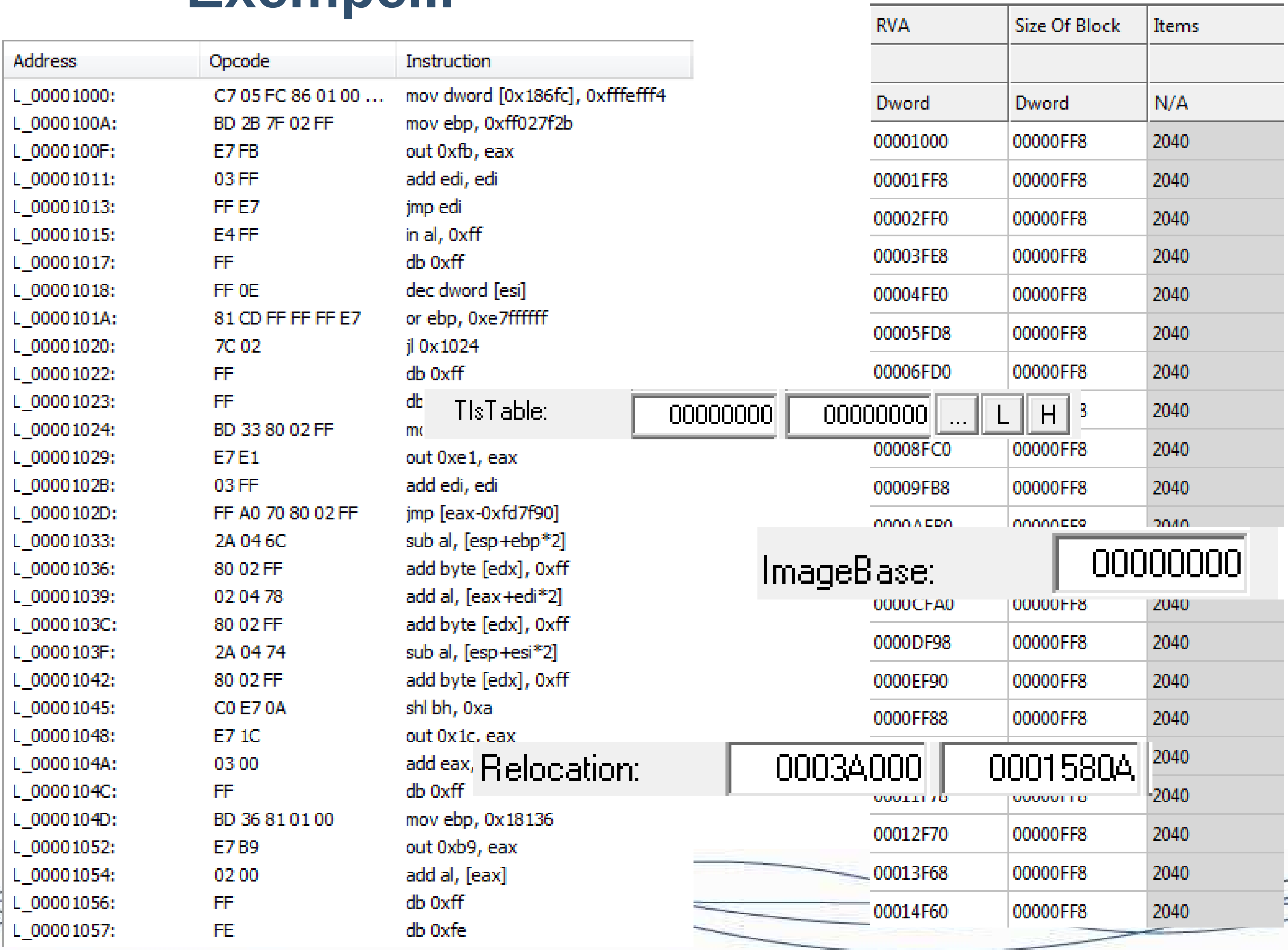
Strategier för..

- ..spridning
- ..att undgå detektering

De mindre bra tecknen?

- Importer
- Imagebase
- Entrypoint
- Sektioner
- Strängar
- Entropi
- API-anrop

Exempel..



```
Address          Opcode              Instruction
L_00001000:      C7 05 FC 86 01 00 ...  mov dword [0x186fc], 0xfffefff4
L_0000100A:      BD 2B 7F 02 FF      mov ebp, 0xff027f2b
L_0000100F:      E7 FB               out 0xfb, eax
L_00001011:      03 FF               add edi, edi
L_00001013:      FF E7               jmp edi
L_00001015:      E4 FF               in al, 0xff
L_00001017:      FF                  db 0xff
L_00001018:      FF 0E               dec dword [esi]
L_0000101A:      81 CD FF FF FF E7   or ebp, 0xe7ffffff
L_00001020:      7C 02               jl 0x1024
L_00001022:      FF                  db 0xff
L_00001023:      FF                  db
L_00001024:      BD 33 80 02 FF      mo
L_00001029:      E7 E1               out 0xe1, eax
L_0000102B:      03 FF               add edi, edi
L_0000102D:      FF A0 70 80 02 FF   jmp [eax-0xfd7f90]
L_00001033:      2A 04 6C            sub al, [esp+ebp*2]
L_00001036:      80 02 FF            add byte [edx], 0xff
L_00001039:      02 04 78            add al, [eax+edi*2]
L_0000103C:      80 02 FF            add byte [edx], 0xff
L_0000103F:      2A 04 74            sub al, [esp+esi*2]
L_00001042:      80 02 FF            add byte [edx], 0xff
L_00001045:      C0 E7 0A            shl bh, 0xa
L_00001048:      E7 1C               out 0x1c, eax
L_0000104A:      03 00               add eax,
L_0000104C:      FF                  db 0xff
L_0000104D:      BD 36 81 01 00      mov ebp, 0x18136
L_00001052:      E7 B9               out 0xb9, eax
L_00001054:      02 00               add al, [eax]
L_00001056:      FF                  db 0xff
L_00001057:      FE                  db 0xfe
```

RVA	Size Of Block	Items
Dword	Dword	N/A
00001000	00000FF8	2040
00001FF8	00000FF8	2040
00002FF0	00000FF8	2040
00003FE8	00000FF8	2040
00004FE0	00000FF8	2040
00005FD8	00000FF8	2040
00006FD0	00000FF8	2040
[illegible]	[illegible]	2040
00008FC0	00000FF8	2040
00009FB8	00000FF8	2040
0000AFB0	00000FF8	2040
[illegible]	[illegible]	[illegible]
0000CFA0	00000FF8	2040
0000DF98	00000FF8	2040
0000EF90	00000FF8	2040
0000FF88	00000FF8	2040
[illegible]	[illegible]	2040
00011F78	00000FF8	2040
00012F70	00000FF8	2040
00013F68	00000FF8	2040
00014F60	00000FF8	2040

TlsTable: 00000000 00000000

ImageBase: 00000000

Relocation: 0003A000 0001580A

Vad malware gör bra/dåligt

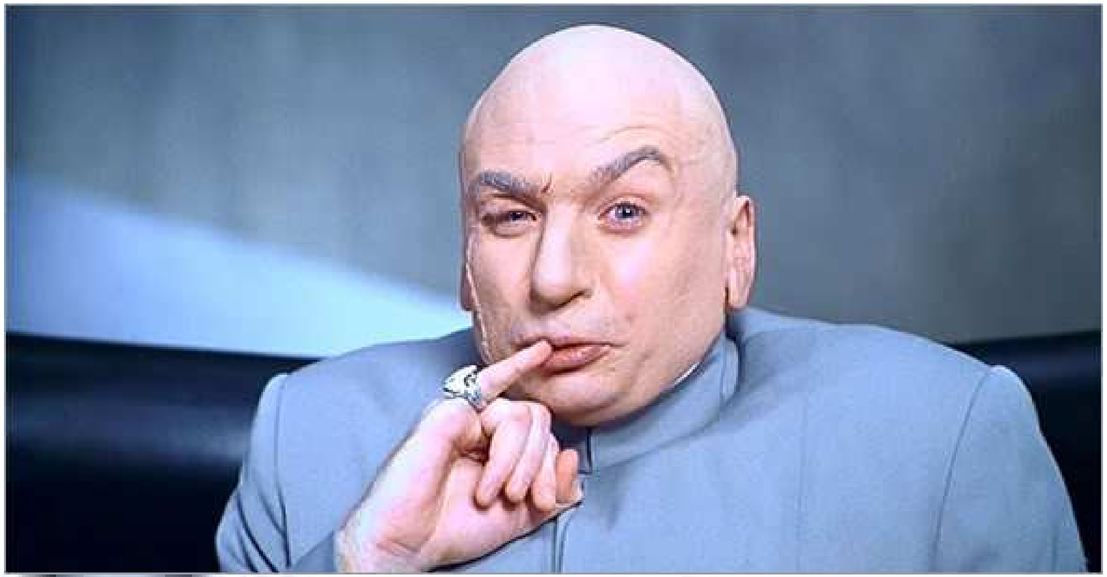
- Majoriteten använder sig av packers
  - Triviala/droppers
- Utnyttjar svagaste länken
- Krypto
- Sårbarheter
- Miljö
- Modulärt
- Skydd
- MITB
- Alltid steget före

SOCIAL ENGINEERING SPECIALIST

Because there is no patch for human stupidity

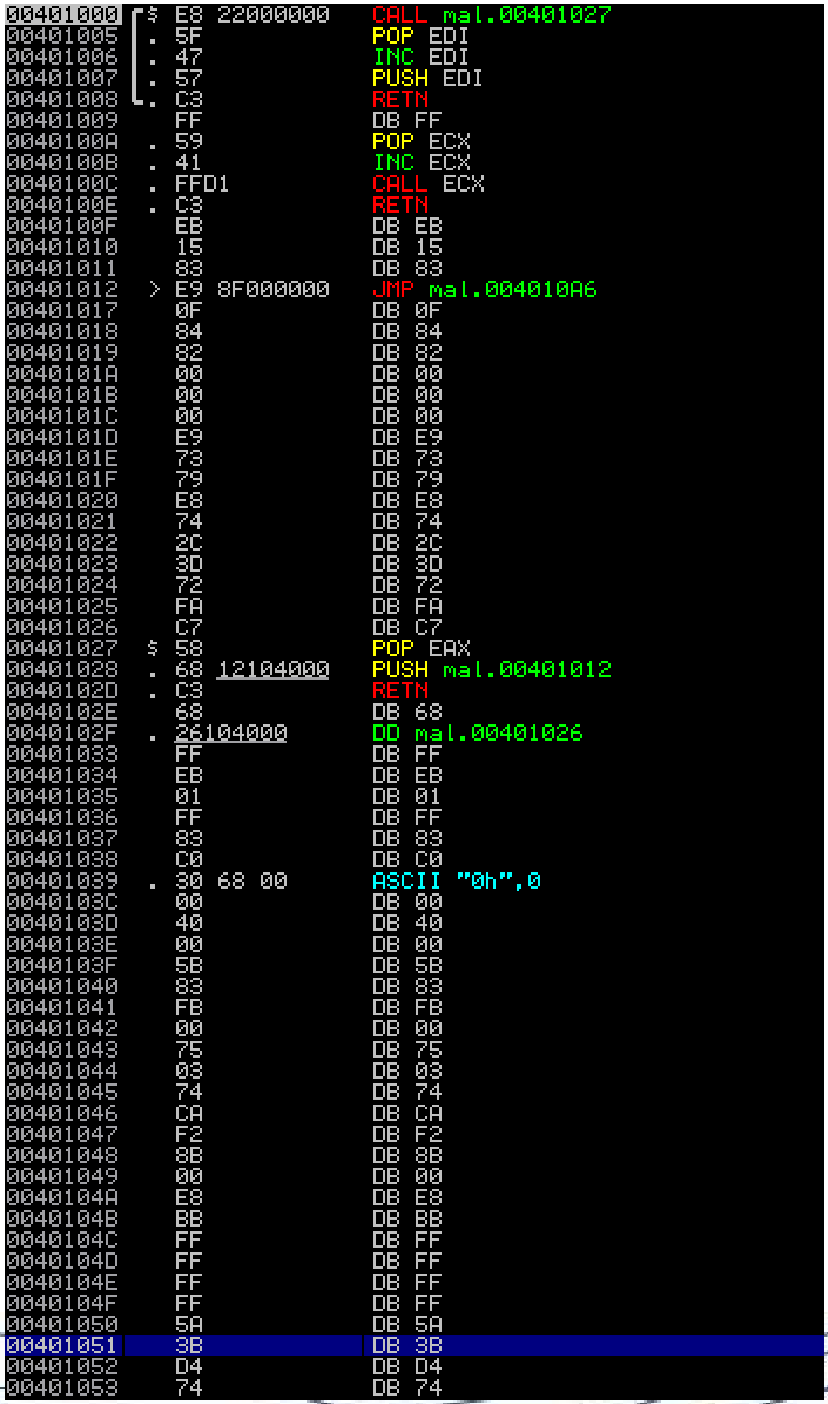
Quality Assurance för malwareskrivaren

- Obfuskering
- Krypto
- Kommunikation
- Dropper
- Anti-Debug/instrumentering/dumpning



Obfuskering

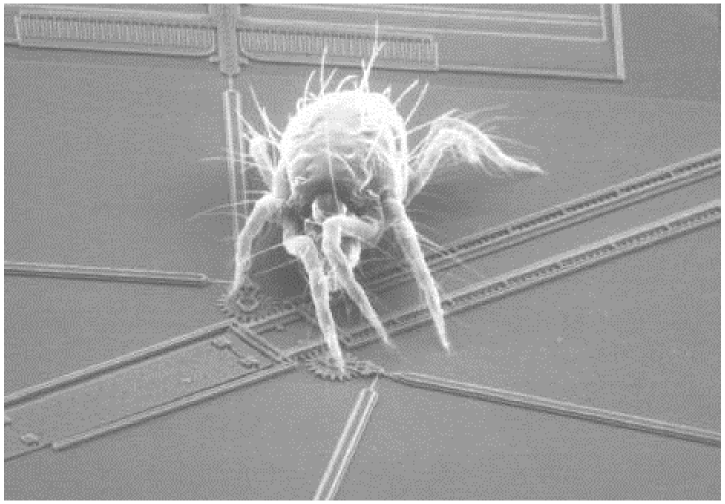
- Skräpkod
  - Felaktig disassemblering
  - Svår läst
- Virtuell maskin
  - P-Code
  - Tungt

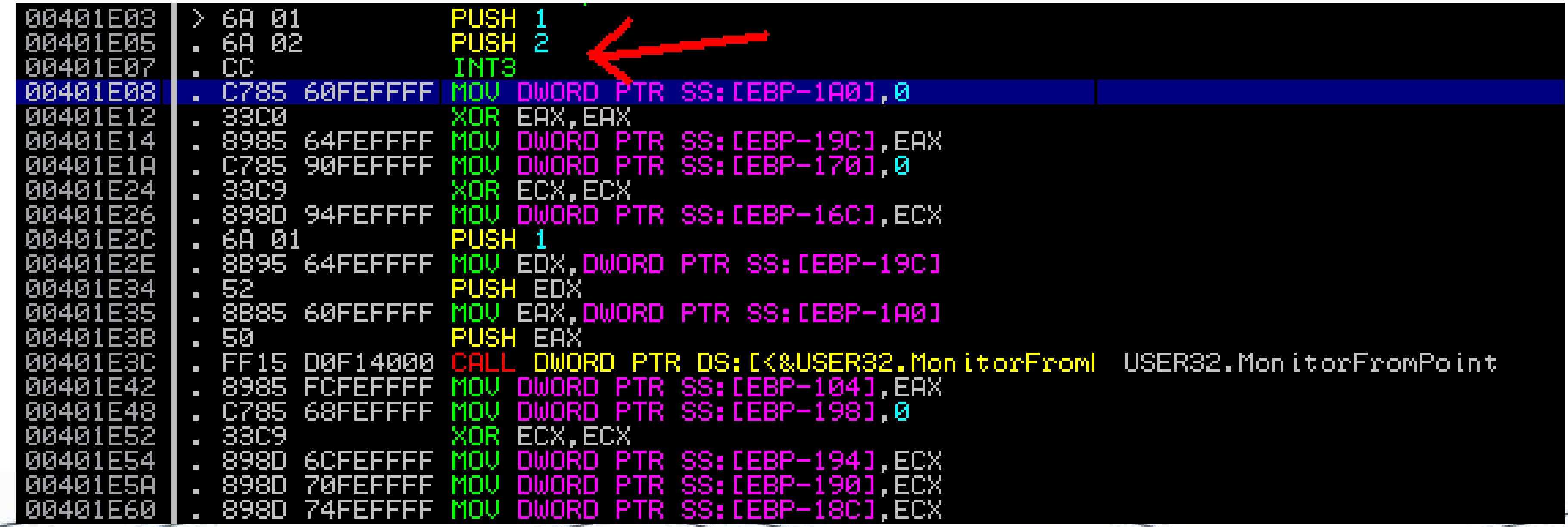


```
00401000 ┌$ E8 22000000     CALL mal.00401027
00401005 │. 5F              POP EDI
00401006 │. 47              INC EDI
00401007 │. 57              PUSH EDI
00401008 └. C3              RETN
00401009    FF              DB FF
0040100A  . 59              POP ECX
0040100B  . 41              INC ECX
0040100C  . FFD1            CALL ECX
0040100E  . C3              RETN
0040100F    EB              DB EB
00401010    15              DB 15
00401011    83              DB 83
00401012  > E9 8F000000     JMP mal.004010A6
00401017    0F              DB 0F
00401018    84              DB 84
00401019    82              DB 82
0040101A    00              DB 00
0040101B    00              DB 00
0040101C    00              DB 00
0040101D    E9              DB E9
0040101E    73              DB 73
0040101F    79              DB 79
00401020    E8              DB E8
00401021    74              DB 74
00401022    2C              DB 2C
00401023    3D              DB 3D
00401024    72              DB 72
00401025    FA              DB FA
00401026    C7              DB C7
00401027  $ 58              POP EAX
00401028  . 68 12104000     PUSH mal.00401012
0040102D  . C3              RETN
0040102E    68              DB 68
0040102F  . 26104000        DD mal.00401026
00401033    FF              DB FF
00401034    EB              DB EB
00401035    01              DB 01
00401036    FF              DB FF
00401037    83              DB 83
00401038    C0              DB C0
00401039  . 30 68 00        ASCII "0h",0
0040103C    00              DB 00
0040103D    40              DB 40
0040103E    00              DB 00
0040103F    5B              DB 5B
00401040    83              DB 83
00401041    FB              DB FB
00401042    00              DB 00
00401043    75              DB 75
00401044    03              DB 03
00401045    74              DB 74
00401046    CA              DB CA
00401047    F2              DB F2
00401048    8B              DB 8B
00401049    00              DB 00
0040104A    E8              DB E8
0040104B    BB              DB BB
0040104C    FF              DB FF
0040104D    FF              DB FF
0040104E    FF              DB FF
0040104F    FF              DB FF
00401050    5A              DB 5A
00401051    3B              DB 3B
00401052    D4              DB D4
00401053    74              DB 74
```

Nanomites

- Conditional jumps
- Anti-Debug
- Anti-Instrumentering





```
00401E03  > 6A 01          PUSH 1
00401E05  . 6A 02          PUSH 2
00401E07  . CC             INT3
00401E08  . C785 60FEFFFF  MOV DWORD PTR SS:[EBP-1A0],0
00401E12  . 33C0           XOR EAX,EAX
00401E14  . 8985 64FEFFFF  MOV DWORD PTR SS:[EBP-19C],EAX
00401E1A  . C785 90FEFFFF  MOV DWORD PTR SS:[EBP-170],0
00401E24  . 33C9           XOR ECX,ECX
00401E26  . 898D 94FEFFFF  MOV DWORD PTR SS:[EBP-16C],ECX
00401E2C  . 6A 01          PUSH 1
00401E2E  . 8B95 64FEFFFF  MOV EDX,DWORD PTR SS:[EBP-19C]
00401E34  . 52             PUSH EDX
00401E35  . 8B85 60FEFFFF  MOV EAX,DWORD PTR SS:[EBP-1A0]
00401E3B  . 50             PUSH EAX
00401E3C  . FF15 D0F14000  CALL DWORD PTR DS:[<&USER32.MonitorFroml  USER32.MonitorFromPoint
00401E42  . 8985 FCFEFFFF  MOV DWORD PTR SS:[EBP-104],EAX
00401E48  . C785 68FEFFFF  MOV DWORD PTR SS:[EBP-198],0
00401E52  . 33C9           XOR ECX,ECX
00401E54  . 898D 6CFEFFFF  MOV DWORD PTR SS:[EBP-194],ECX
00401E5A  . 898D 70FEFFFF  MOV DWORD PTR SS:[EBP-190],ECX
00401E60  . 898D 74FEFFFF  MOV DWORD PTR SS:[EBP-18C],ECX
```

Code Stealing

- Anti-dump
- Kräver analys

Anti-Emulering

- Windows API
- Detour

```
kernel32_CreateFileA
ntdll_RtlInitAnsiString
ntdll_RtlAnsiStringToUnicodeString
ntdll_RtlMultiByteToUnicodeN
kernel32_CreateFileW
ntdll_RtlInitUnicodeString
ntdll_RtlIsDosDeviceName_U
ntdll_RtlInitUnicodeStringEx
ntdll_wcslen
ntdll_RtlDetermineDosPathNameType_U
ntdll_RtlEqualUnicodeString
ntdll_RtlDosPathNameToNtPathName_U
ntdll_wcslen
ntdll_RtlAllocateHeap
ntdll_RtlEnterCriticalSection
ntdll_RtlCompareMemoryUlong
ntdll_RtlFillMemoryUlong
ntdll_RtlGetNtGlobalFlags
ntdll_RtlLeaveCriticalSection
ntdll_RtlAcquirePebLock
ntdll_RtlEnterCriticalSection
ntdll_RtlDetermineDosPathNameType_U
ntdll_RtlAcquirePebLock
ntdll_RtlEnterCriticalSection
ntdll_RtlUpcaseUnicodeChar
ntdll_RtlReleasePebLock
ntdll_RtlLeaveCriticalSection
ntdll_RtlDetermineDosPathNameType_U
ntdll_memmove
ntdll_RtlReleasePebLock
ntdll_RtlLeaveCriticalSection
ntdll_NtCreateFile
ntdll_KiFastSystemCall
ntdll_RtlFreeHeap
ntdll_RtlEnterCriticalSection
ntdll_RtlCompareMemory
ntdll_RtlGetNtGlobalFlags
ntdll_RtlFillMemoryUlong
ntdll_RtlLeaveCriticalSection
ntdll_RtlFreeHeap
```

Integritetskontroller

- Detours
- Loaded Modules
- Signaturer

Framtid

- -1
- $$$
- Mobiler
- Höjda krav
- Användarvänlighet