CROWDSTRIKE

Y.A.N.T.

SEBASTIAN ESCHWEILER

CROWDSTRIKE

NYMAIM: THE ANALYST'S SCOURGE

- Nymaim: What has been published?
- Heaven's Gate
- Hybrid Binaries
- Thread Obfuscation

NYMAIM'S FEATURES

- Anti-Sandbox Techniques
- Encrypted Data
- `push [reg]` Obfuscation
- Obfuscation of (Internal) Function Addresses
- Obfuscation of API Function Calls
- [...]

HEAVEN'S GATE

HEAVEN'S GATE

- Mechanism to directly call 64-bit kernel code from 32-bit code
- Nymaim uses it to directly call x64 API functions
- Shellcode style!

HEAVEN'S GATE

- Store and align stack pointer
- Call 64 bit stub
- Clean up, return

```
[...]
call    far ptr 33h:2Ah
mov     esi, eax
xor     eax, eax
cpuid
mov     ax, ds
mov     ss, eax
assume ss:_code
mov     eax, esi
mov     esp, edi
[...]
```

HEAVEN'S GATE – X64 CODE

- Find API function by hash
- Find `jmp rbx` instruction in ntdll
- Convert arguments to `__fastcall`
- Call API function (return to `ea_jmp_rbx`)
- `retf` to 32-bit mode

```
mov     rbp, rbx    ; ea_jmp_rbx
[…]
mov     rcx, [rsp+0]
mov     rdx, [rsp+arg_0]
mov     r8, [rsp+arg_8]
mov     r9, [rsp+arg_10]
call    detourFunction
[…]
retf

detourFunction:
pop     rbx
Push    rbp         ; ea_jmp_rbx!
jmp     r12
```

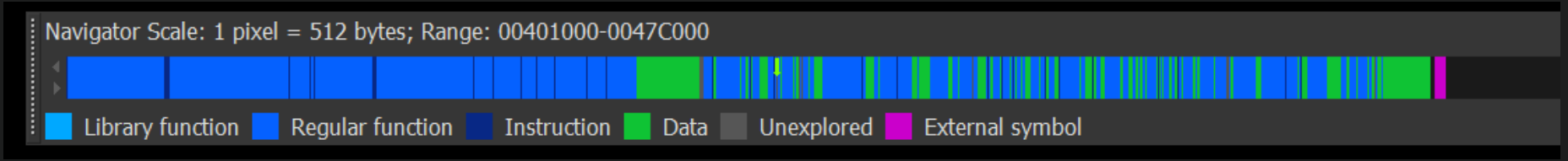
HEAVEN'S GATE – CONCLUSION

- Encrypted code hides itself from static analysis tools
- Shellcode style helps obfuscate origin of call
- Nice way to evade sandbox hooks

HYBRID BINARIES

CROWDSTRIKE

HYBRID BINARIES




```
48                  dec     eax
85 C9               test    ecx, ecx
0F 84 6E AD 02 00   jz      nullsub_153
48                  dec     eax
89 E0               mov     eax, esp
48                  dec     eax
89 58 08            mov     [eax+8], ebx
48                  dec     eax
```

```
test    rcx, rcx
jz      locret_46A8B4
mov     rax, rsp
mov     [rax+8], rbx
mov     [rax+10h], rbp
```

POLYGLOT CODE

```
31 C0 40 90 C3
```

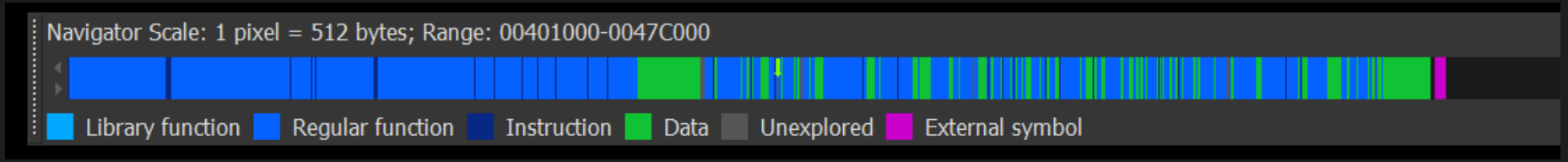
x86

```
31 C0    xor     eax, eax
40       inc     eax
90       nop
C3       retn
```

x64

```
31 C0    xor     eax, eax
40 90    xchg    eax, eax
C3       retn
```

HYBRID BINARIES



THREAD OBFUSCATION

THREAD OBFUSCATION – RECIPE

- 3 ingredients
  - ROP gadget
  - Shellcode
  - Management function

STIR WELL…

- Find ROP gadget (ea_ROP)

```
7C90E2FF    POP EDX
7C90E300    RETN
```

- Generate shell code (ea_Shellcode)

```
00350000    PUSH 2              ; actual lpParameter
00350005    PUSH EDX            ; save original return address
00350006    PUSH 427669h        ; actual thread procedure
0035000B    MOV EAX,49F97Ah     ; address of management function
00350010    CALL EAX
```

- Call CreateThread(ea_ROP, ea_Shellcode)

THREAD OBFUSCATION – CONCLUSION

- Thread obfuscation hides actual thread function
- Once understood, it’s quite easy to recognize Nymaim’s thread creation function

CONCLUSION

CONCLUSION

- Nymaim offers a rich set of obfuscations. Amongst others:
  - Heaven's Gate
  - Hybrid Binaries
  - Thread Obfuscation
- Pay attention to small details that don't make sense
- If you really want to annoy someone, send them a Nymaim sample ;-)