Malware-Scripts/Nymaim at master · coldshell/Malware-Scripts · GitHub

github.com/coldshell/Malware-Scripts/tree/master/Nymaim

coldshell

coldshell/**Malware-Scripts**

0 Contributors

0 Issues

24 Stars

13 Forks

Nymaim deobfuscation

This tool helps to deobfuscate nymaim samples.

To deobfuscate we use `miasm` for the emulation and `grap` to match graph patterns.

Usage

Patch nymaim and generate an IDA script to rename fonctions:

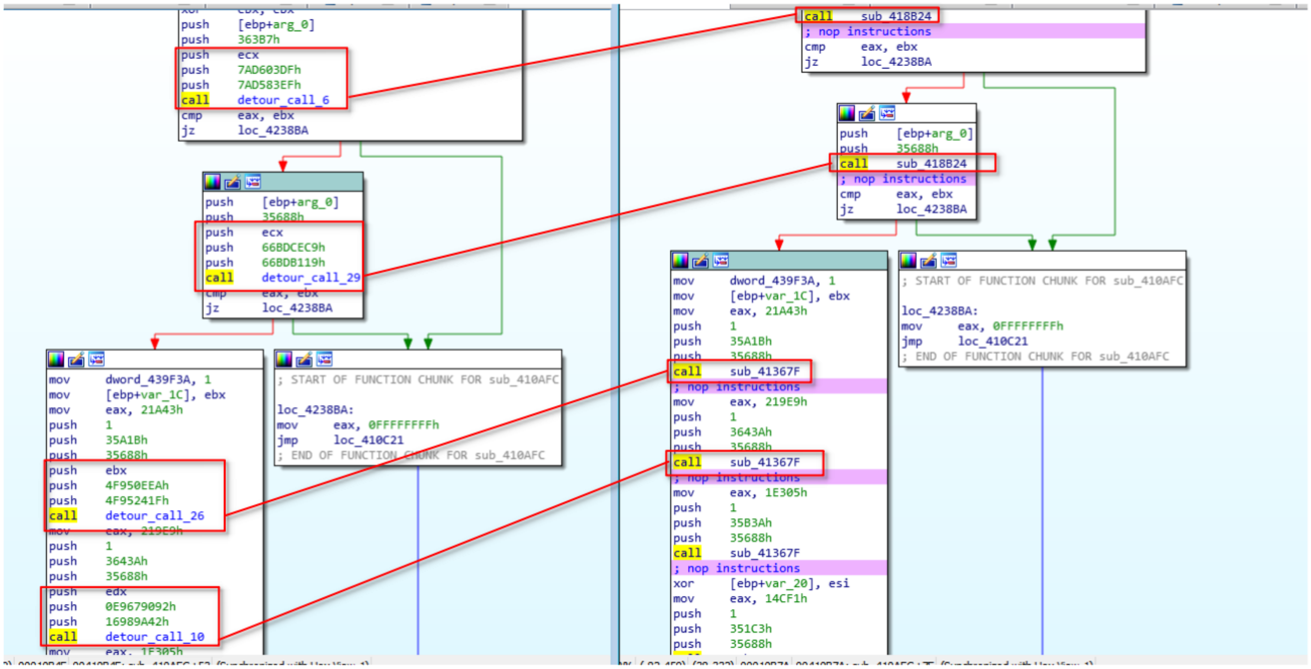
```
./nymaim.py --ida /tmp/nymaim_unpack_2018-03-28.bin

[+] Searching for the pattern push_reg
[i] The graph push_reg was found 1 time(s)
[+] Emulating each call to push_reg
[+] Patching each call to push_reg (can take a while)
[+] Searching for the pattern detour_call
[i] The graph detour_call was found 34 time(s)
[e] No XREFS to the function 0x429537 was found
[+] Emulating each call to detour_call
[+] Patching each call to detour_call (can take a while)
[+] Searching for the pattern detour_jmp
[i] The graph detour_jmp was found 32 time(s)
[e] No XREFS to the function 0x402AC2 was found
[e] No XREFS to the function 0x404A23 was found
[e] No XREFS to the function 0x404EAB was found
[e] No XREFS to the function 0x406A90 was found
[e] No XREFS to the function 0x4081B3 was found
[e] No XREFS to the function 0x40DF3D was found
[e] No XREFS to the function 0x41148D was found
[e] No XREFS to the function 0x419F2C was found
[e] No XREFS to the function 0x41A5B4 was found
[e] No XREFS to the function 0x41FB49 was found
[e] No XREFS to the function 0x42247A was found
[e] No XREFS to the function 0x423A38 was found
[e] No XREFS to the function 0x42477F was found
[e] No XREFS to the function 0x4278C1 was found
[e] No XREFS to the function 0x42914B was found
[e] No XREFS to the function 0x42BFFF was found
[e] No XREFS to the function 0x42F385 was found
[e] No XREFS to the function 0x43212F was found
[+] Emulating each call to detour_jmp
[+] Patching each call to detour_jmp (can take a while)
[+] Creation of an IDA script to rename function: /tmp/nymaim_unpack_2018-03-28.bin_ida.py
[+] Patched nymaim available: /tmp/nymaim_unpack_2018-03-28.bin.clean
```

The generated IDA script look like this:

```
MakeFunction(4214618)
MakeNameEx(4214618, "detour_jmp_0", SN_NOWARN)
MakeFunction(4226729)
MakeNameEx(4226729, "detour_jmp_1", SN_NOWARN)
MakeFunction(4229427)
MakeNameEx(4229427, "detour_jmp_2", SN_NOWARN)
MakeFunction(4261327)
MakeNameEx(4261327, "detour_jmp_3", SN_NOWARN)
MakeFunction(4270551)
MakeNameEx(4270551, "detour_jmp_4", SN_NOWARN)
MakeFunction(4327584)
MakeNameEx(4327584, "detour_jmp_5", SN_NOWARN)
MakeFunction(4327617)
MakeNameEx(4327617, "detour_jmp_6", SN_NOWARN)
MakeFunction(4356652)
...
...
...
```

Before/After:



```
xor     ebx, ebx
push    [ebp+arg_0]
push    363B7h
push    ecx
push    7AD603DFh
push    7AD583EFh
call    detour_call_6
cmp     eax, ebx
jz      loc_4238BA
```

```
push    [ebp+arg_0]
push    35688h
push    ecx
push    66BDCEC9h
push    66BDB119h
call    detour_call_29
cmp     eax, ebx
jz      loc_4238BA
```

```
mov     dword_439F3A, 1
mov     [ebp+var_1C], ebx
mov     eax, 21A43h
push    1
push    35A1Bh
push    35688h
push    ebx
push    4F950EEAh
push    4F95241Fh
call    detour_call_26
mov     eax, 219E9h
push    1
push    3643Ah
push    35688h
push    edx
push    0E9679092h
push    16989A42h
call    detour_call_10
mov     eax, 1E305h
```

```
; START OF FUNCTION CHUNK FOR sub_410AFC

loc_4238BA:
mov     eax, 0FFFFFFFFh
jmp     loc_410C21
; END OF FUNCTION CHUNK FOR sub_410AFC
```

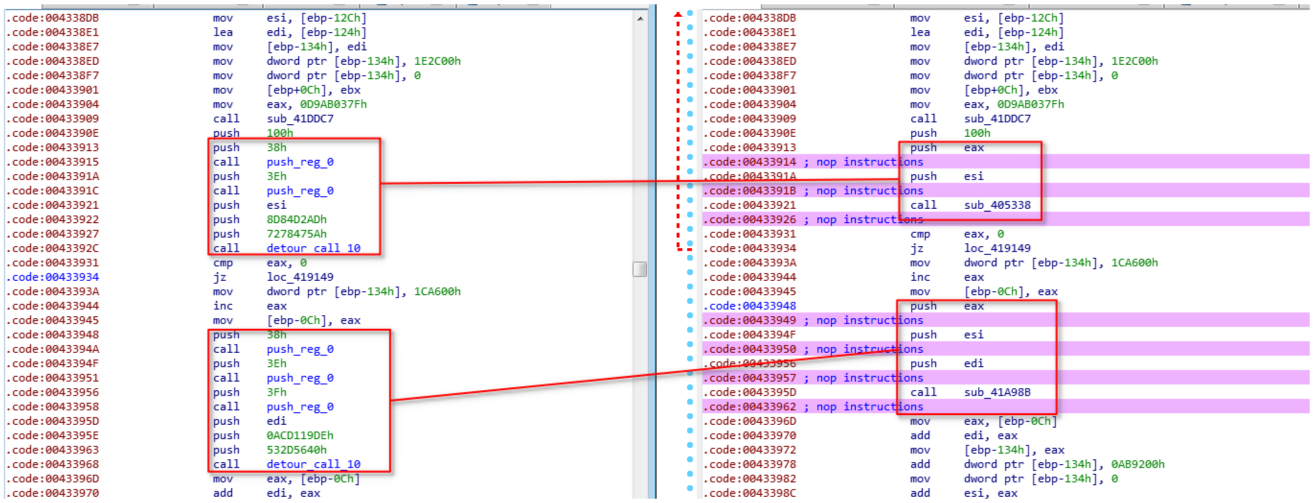
```
call    sub_418B24
; nop instructions
cmp     eax, ebx
jz      loc_4238BA
```

```
push    [ebp+arg_0]
push    35688h
call    sub_418B24
; nop instructions
cmp     eax, ebx
jz      loc_4238BA
```

```
mov     dword_439F3A, 1
mov     [ebp+var_1C], ebx
mov     eax, 21A43h
push    1
push    35A1Bh
push    35688h
call    sub_41367F
; nop instructions
mov     eax, 219E9h
push    1
push    3643Ah
push    35688h
call    sub_41367F
; nop instructions
mov     eax, 1E305h
push    1
push    35B3Ah
push    35688h
call    sub_41367F
; nop instructions
xor     [ebp+var_20], esi
mov     eax, 14CF1h
push    1
push    351C3h
push    35688h
```

```
; START OF FUNCTION CHUNK FOR sub_410AFC

loc_4238BA:
mov     eax, 0FFFFFFFFh
jmp     loc_410C21
; END OF FUNCTION CHUNK FOR sub_410AFC
```



```
.code:004338DB                  mov     esi, [ebp-12Ch]
.code:004338E1                  lea     edi, [ebp-124h]
.code:004338E7                  mov     [ebp-134h], edi
.code:004338ED                  mov     dword ptr [ebp-134h], 1E2C00h
.code:004338F7                  mov     dword ptr [ebp-134h], 0
.code:00433901                  mov     [ebp+0Ch], ebx
.code:00433904                  mov     eax, 0D9AB037Fh
.code:00433909                  call    sub_41DDC7
.code:0043390E                  push    100h
.code:00433913                  push    38h
.code:00433915                  call    push_reg_0
.code:0043391A                  push    3Eh
.code:0043391C                  call    push_reg_0
.code:00433921                  push    esi
.code:00433922                  push    8D84D2ADh
.code:00433927                  push    7278475Ah
.code:0043392C                  call    detour_call_10
.code:00433931                  cmp     eax, 0
.code:00433934                  jz      loc_419149
.code:0043393A                  mov     dword ptr [ebp-134h], 1CA600h
.code:00433944                  inc     eax
.code:00433945                  mov     [ebp-0Ch], eax
.code:00433948                  push    38h
.code:0043394A                  call    push_reg_0
.code:0043394F                  push    3Eh
.code:00433951                  call    push_reg_0
.code:00433956                  push    3Fh
.code:00433958                  call    push_reg_0
.code:0043395D                  push    edi
.code:0043395E                  push    0ACD119DEh
.code:00433963                  push    532D5640h
.code:00433968                  call    detour_call_10
.code:0043396D                  mov     eax, [ebp-0Ch]
.code:00433970                  add     edi, eax
```

```
.code:004338DB                  mov     esi, [ebp-12Ch]
.code:004338E1                  lea     edi, [ebp-124h]
.code:004338E7                  mov     [ebp-134h], edi
.code:004338ED                  mov     dword ptr [ebp-134h], 1E2C00h
.code:004338F7                  mov     dword ptr [ebp-134h], 0
.code:00433901                  mov     [ebp+0Ch], ebx
.code:00433904                  mov     eax, 0D9AB037Fh
.code:00433909                  call    sub_41DDC7
.code:0043390E                  push    100h
.code:00433913                  push    eax
.code:00433914 ; nop instructions
.code:0043391A                  push    esi
.code:0043391B ; nop instructions
.code:00433921                  call    sub_405338
.code:00433926 ; nop instructions
.code:00433931                  cmp     eax, 0
.code:00433934                  jz      loc_419149
.code:0043393A                  mov     dword ptr [ebp-134h], 1CA600h
.code:00433944                  inc     eax
.code:00433945                  mov     [ebp-0Ch], eax
.code:00433948                  push    eax
.code:00433949 ; nop instructions
.code:0043394F                  push    esi
.code:00433950 ; nop instructions
.code:00433956                  push    edi
.code:00433957 ; nop instructions
.code:0043395D                  call    sub_41A98B
.code:00433962 ; nop instructions
.code:0043396D                  mov     eax, [ebp-0Ch]
.code:00433970                  add     edi, eax
.code:00433972                  mov     [ebp-134h], eax
.code:00433978                  add     dword ptr [ebp-134h], 0AB9200h
.code:00433982                  mov     dword ptr [ebp-134h], 0
.code:0043398C                  add     esi, eax
```

Requirements

You will need grap and miasm. For the others dependencies see the `requierments.txt`.