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

By coldshell

Archived: 2026-04-05 19:40:04 UTC

This tool helps to deobfuscate nymaim samples.

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

```
 ./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
```

```
 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)
...
...
...
```

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

Source: https://github.com/coldshell/Malware-Scripts/tree/master/Nymaim