

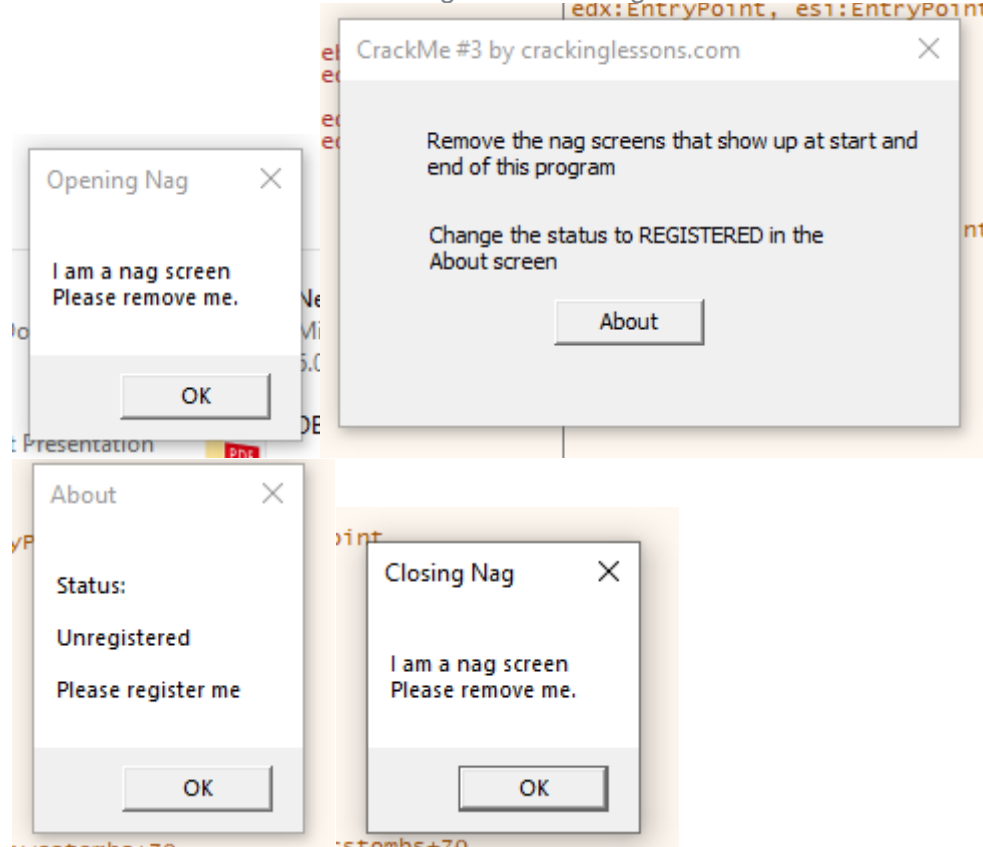
Crack me 3:

Objective:

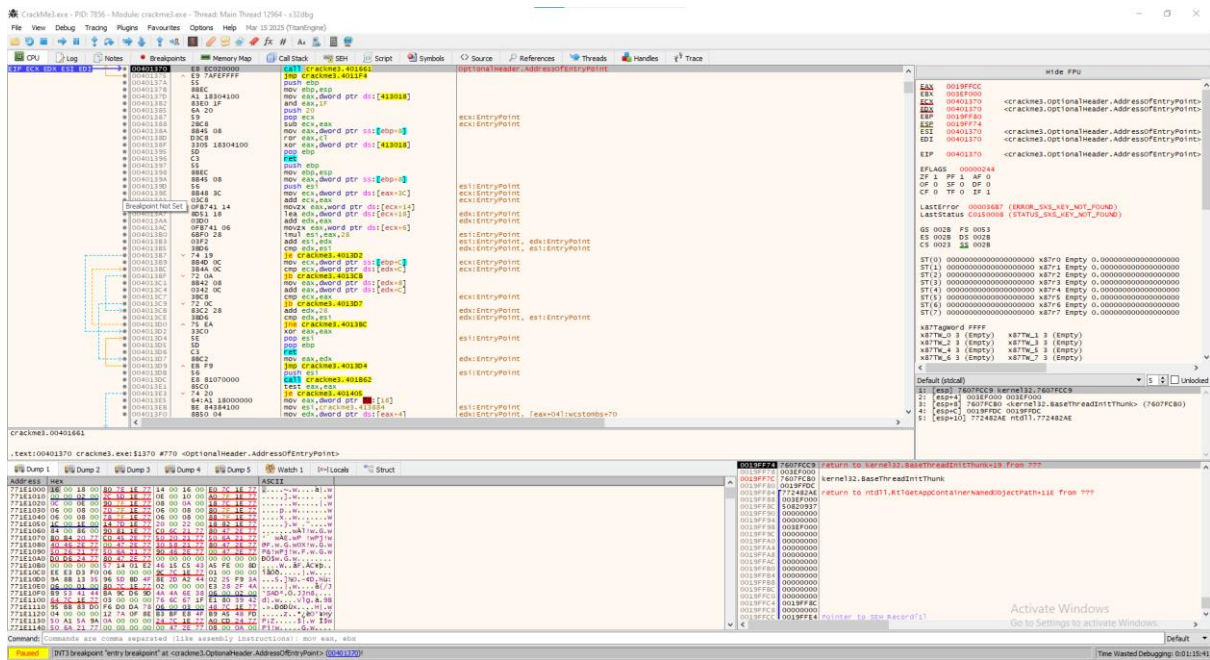
1. Remove the 2 nag screens – one at startup and one at close of program.
2. In the About screen – change status to Registered.

Solution:

Run crackme3.exe to notice strings in box of nag screens and About screen.

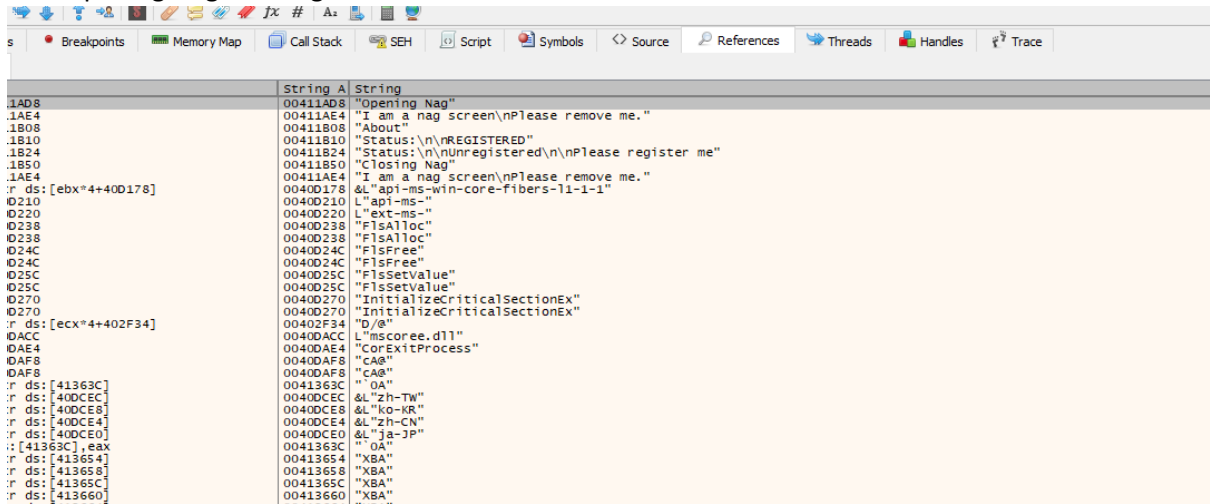


Open crackme3.exe in x32dbg tool.

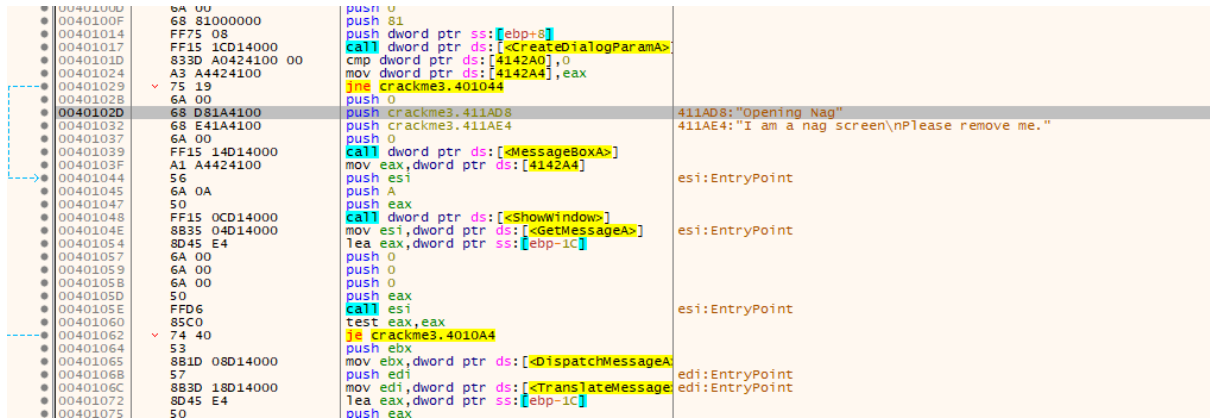


Opening nag:

Find Opening Nag in String references



Double click to see code in CPU:



Trace code above and below, pay attention on this line 'jne crackme3.401044', this code is jump not equal through MessageBoxA of string "Opening Nag, I am a nag..." to address 00401044.

00401029	75 19	jne crackme3.401044	
0040102B	6A 00	push 0	
0040102D	68 D81A4100	push crackme3.411AD8	411AD8:"Opening Nag"
00401032	68 E41A4100	push crackme3.411AE4	411AE4:"I am a nag screen\nPlease remove me."
00401037	6A 00	push 0	
00401039	FF15 14D14000	call dword ptr ds:[<MessageBoxA>]	
0040103F	A1 A4424100	mov eax,dword ptr ds:[4142A4]	
00401044	56	push esi	esi:EntryPoint
00401045	6A 0A	push A	
00401047	50	push eax	
00401048	FF15 0CD14000	call dword ptr ds:[<ShowWindow>]	
0040104E	8B35 04D14000	mov esi,dword ptr ds:[<GetMessageA>]	esi:EntryPoint
00401054	8D45 E4	lea eax,dword ptr ss:[ebp-1C]	
00401057	6A 00	push 0	

Need to change this one to je – jump equal to 00401044 ignoring these opening nag.

00401029	74 19	je crackme3.401044	
0040102B	6A 00	push 0	
0040102D	68 D81A4100	push crackme3.411AD8	411AD8:"Opening Nag"
00401032	68 E41A4100	push crackme3.411AE4	411AE4:"I am a nag screen\nPlease remove me."
00401037	6A 00	push 0	
00401039	FF15 14D14000	call dword ptr ds:[<MessageBoxA>]	
0040103F	A1 A4424100	mov eax,dword ptr ds:[4142A4]	
00401044	56	push esi	esi:EntryPoint

Closing nag:

Do it again with Closing nag

00401101	FF35 A4424100	push dword ptr ds:[4142A4]	
00401107	FF15 0CD14000	call dword ptr ds:[<ShowWindow>]	
0040110D	6A 00	push 0	
0040110F	68 501B4100	push crackme3.411B50	411B50:"Closing Nag"
00401114	68 E41A4100	push crackme3.411AE4	411AE4:"I am a nag screen\nPlease remove me."
00401119	6A 00	push 0	
0040111B	FF15 14D14000	call dword ptr ds:[<MessageBoxA>]	
00401121	6A 00	push 0	
00401123	FF15 10D14000	call dword ptr ds:[<PostQuitMessage>]	
00401129	33C0	xor eax,eax	
0040112B	5D	pop ebp	
0040112C	C2 1000	ret 10	

Trace code above and below to find the line jump, but no line has comparison to jump so we need to highlight 00401107 to 0040111BB (content of MessageBoxA of Closing nag) and fill with NOPs (no operation) to ignore Closing nag.

00401107	90	nop
00401108	90	nop
00401109	90	nop
0040110A	90	nop
0040110B	90	nop
0040110C	90	nop
0040110D	90	nop
0040110E	90	nop
0040110F	90	nop
00401110	90	nop
00401111	90	nop
00401112	90	nop
00401113	90	nop
00401114	90	nop
00401115	90	nop
00401116	90	nop
00401117	90	nop
00401118	90	nop
00401119	90	nop
0040111A	90	nop
0040111B	90	nop
0040111C	90	nop
0040111D	90	nop
0040111E	90	nop
0040111F	90	nop
00401120	90	nop
00401121	6A 00	push 0
00401123	FF15 10D14000	call dword ptr ds:[<PostQuitMessage>]
00401129	33C0	xor eax,eax

About screen:

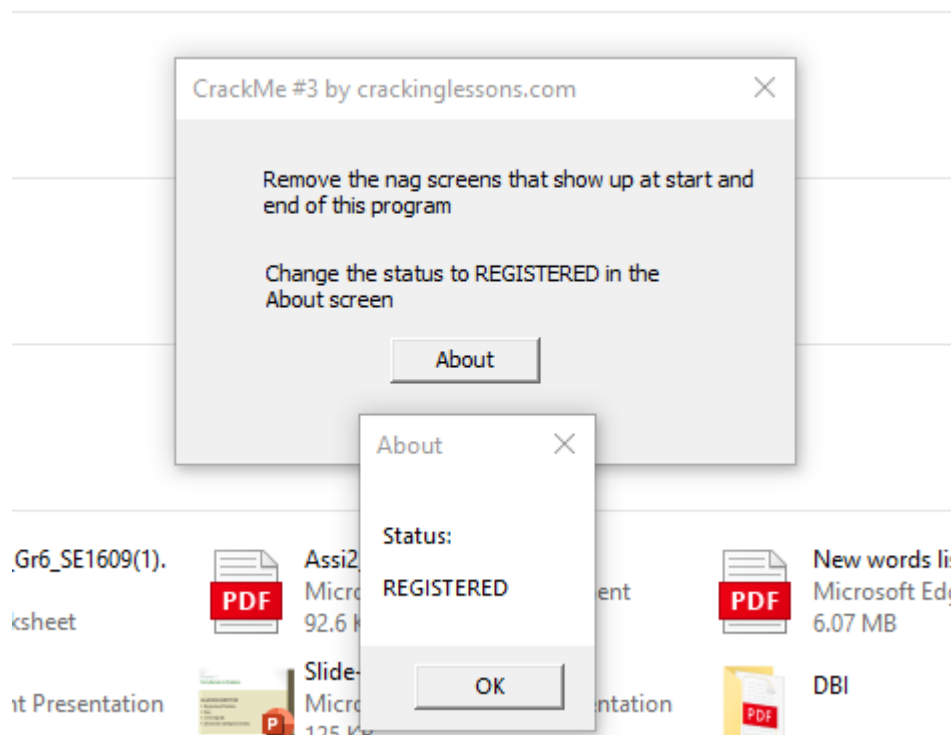
Then trace to About screen:

004010CD	68 081B4100	push crackme3.411B08	411B08: "About"
004010D2	3905 A0424100	cmp dword ptr ds:[4142A0], eax	
004010D8	74 12	je crackme3.4010EC	
004010DA	68 101B4100	push crackme3.411B10	411B10: "Status:\n\nREGISTERED"
004010DF	50	push eax	
004010E0	FF15 14D14000	call dword ptr ds:[<MessageBoxA>]	
004010E6	33C0	xor eax, eax	
004010E8	5D	pop ebp	
004010E9	C2 1000	ret 10	
004010EC	68 241B4100	push crackme3.411B24	411B24: "Status:\n\nUnregistered\n\nPlease register me"
004010F1	6A 00	push 0	
004010F3	FF15 14D14000	call dword ptr ds:[<MessageBoxA>]	

Notice line "je crackme3.4010EC", this mean jump equal to push string "Unregistered..." and call MessageBoxA, while we find out address 004010DA has string "Registered". We need to change "je crackme3.4010EC" to "je crackme3.4010DA" to display Registered status.

004010CD	68 081B4100	push crackme3.411B08	411B08: "About"
004010D2	3905 A0424100	cmp dword ptr ds:[4142A0], eax	
004010D8	74 00	je crackme3.4010DA	
004010DA	68 101B4100	push crackme3.411B10	411B10: "Status:\n\nREGISTERED"
004010DF	50	push eax	
004010E0	FF15 14D14000	call dword ptr ds:[<MessageBoxA>]	

After change 3 objective, we patch file and run again to check the consequence.



Done!

Convert file clamav to yara with the command:

```
(khanhNNHE191159@ kali)-[~/Downloads]
$ ls
BIG_FAT_WARNING.txt  clamav.py  clamscn.exe  clamsrc.ndb  COPYING  COPYING.getopt  COPYING.lzma  COPYING.unrar  libclamav.dll  package.01.ful.7
clamav  clamav.py  clamscn.bat  conversion_peid.log  COPYING.bz2  COPYING.regex  COPYING.rlib  libclamav.patch  sigbase.sig
clamav_to_yara.py  clameid.py  clamsrc.ldb  conversion_signsrc.log  COPYING.file  COPYING.llvm  COPYING.sha256  daily.cvd  package  Test

(khanhNNHE191159@ kali)-[~/Downloads]
$ sudo python2 clamav_to_yara.py -f clamsrc.ndb -o clamsrc.yara

#####
Malware Analyst's Cookbook - ClamAV to YARA Converter 0.0.1
#####

[+] Read 2291 lines from clamsrc.ndb

[+] Wrote 2287 rules to clamsrc.yara

(khanhNNHE191159@ kali)-[~/Downloads]
$ ls
BIG_FAT_WARNING.txt  clameid.ndb  clamsrc.ldb  conversion_signsrc.log  COPYING.getopt  COPYING.regex  daily.cvd  package.01.ful.72
clamav  clameid.py  clamsrc.ndb  COPYING  COPYING.LGPL  COPYING.sha256  libclamav.dll  sigbase.sig
clamav_to_yara.py  clamscn.exe  clamsrc.yara  COPYING.bz2  COPYING.llvm  COPYING.unrar  libclamav.patch  Test
clamfier.py  clamsrc.bat  conversion_peid.log  COPYING.file  COPYING.lzma  COPYING.zlib  package

(khanhNNHE191159@ kali)-[~/Downloads]
$
```

```

(khanhNNHE191159@kali) ~/Downloads
$ yara -r clamsrch.yara /home

rfc3548_Base_64_Encoding_with_URL_and_Filename_Safe_Alphabet__8_byt_ASC_62_ /home/kali/.mozilla/firefox/14/{0e6ea333-e688-46a3-be80-4916d87ddf72}.final
rfc3548_Base_64_Encoding_with_URL_and_Filename_Safe_Alphabet__8_byt_ASC_62_ /home/kali/.mozilla/firefox/0/{9e054843-7ac3-4fbe-a6a6-82719c6add50}.final
rfc3548_Base_64_Encoding_with_URL_and_Filename_Safe_Alphabet__8_byt_ASC_62_ /home/kali/.mozilla/firefox/64/{9afde2e5-158a-486b-b190-36fc539014a4}.final
padding_used_in_hashing_algorithms__0x80_0__0__8_byt_64_ /home/kali/.mozilla/firefox/8ryv4mda.
padding_used_in_hashing_algorithms__0x80_0__0__8_byt_64_ /home/kali/.mozilla/firefox/8ryv4mda.
padding_used_in_hashing_algorithms__0x80_0__0__8_byt_64_ /home/kali/.mozilla/firefox/8ryv4mda.
padding_used_in_hashing_algorithms__0x80_0__0__8_byt_64_ /home/kali/.mozilla/firefox/8ryv4mda.
padding_used_in_hashing_algorithms__0x80_0__0__8_byt_64_ /home/kali/.mozilla/firefox/8ryv4mda.
padding_used_in_hashing_algorithms__0x80_0__0__8_byt_64_ /home/kali/.mozilla/firefox/8ryv4mda.
Binary_arithmetic_decoder_LPSTable__T264_cabac_range_lps__8_byt_256_ /home/kali/.mozilla/firefox/8ryv4mda.
libavcodec_ff_zigzag_direct__8_byt_64_ /home/kali/.mozilla/firefox/8ryv4mda.default-esr/gmp-gmpe
Bit_count_256__popcount_tab_population_count__8_byt_256_ /home/kali/.mozilla/firefox/8ryv4mda.
libavcodec_H_26L_H_264_AVC_JVT_14496_10_lps_range__8_byt_256_ /home/kali/.mozilla/firefox/8ryv4mda.
Simbin_Race_WTCC_files_encryption_version_2__8_byt_STR_16_ /home/kali/Downloads/sigbase.sig
GS_SDK_challenge_response_algorithm_default_key__8_byt_STR_32_ /home/kali/Downloads/sigbase.sig
anti_debug_WINICE_BR__8_byt_STR_9_ /home/kali/Downloads/sigbase.sig
Bzip2_signature__8_byt_STR_6_ /home/kali/Downloads/sigbase.sig
anti_debug_SOFTICE1__8_byt_STR_8_ /home/kali/Downloads/sigbase.sig
rotor_German_Enigma__8_byt_STR_26_ /home/kali/Downloads/sigbase.sig
GS_SDK_challenge_response_algorithm_Soldier_of_Anarchy_key__8_byt_STR_32_ /home/kali/Downloads/sigbase.sig
PADDINGXXPPADDING__8_byt_STR_16_ /home/kali/Downloads/sigbase.sig
PSCHF__Pukall_Stream_Cipher_Hash_Function__8_byt_STR_16_ /home/kali/Downloads/sigbase.sig
anti_debug_IsDebuggerPresent__8_byt_STR_17_ /home/kali/Downloads/sigbase.sig
PADDINGXXPPADDING__8_byt_STR_16_ /home/kali/Downloads/clamscan.exe
anti_debug_IsDebuggerPresent__8_byt_STR_17_ /home/kali/Downloads/clamscan.exe

```


Create a new rule file called custome.yara and cat to see:

```
(khanhNNHE191159@kali)-[~/Downloads]
$ cat custome.yara
rule ConditionsExample {
strings:
$string1 = "hello"
$string2 = "hello"
$string3 = "hello"
condition:
any of them
}
global rule GlobalRuleExample {
condition:
filesize < 2MB
}
rule NumberStringsExample {
strings:
$hello = "hello"
condition:
#hello ≥ 5
}
rule CheckImage {
strings:
$a = {89 50 4e 47 0d 0a 1a 0a}
condition:
any of them
}

(khanhNNHE191159@kali)-[~/Downloads]
$
```

Test yara rules:

```
(khanhNNHE191159@kali)-[~/Downloads]
$ yara -r custome.yara /home/kali/Downloads/Test
GlobalRuleExample /home/kali/Downloads/Test/Clam_HelloWorld.ndb
ConditionsExample /home/kali/Downloads/Test/test.txt
GlobalRuleExample /home/kali/Downloads/Test/test.txt

(khanhNNHE191159@kali)-[~/Downloads]
$
```

Here we see yara's report for the rule we created as follows: ConditionExample means that yara has detected that the test.txt file matches the rule we provided and contains the string "hello" in there. In addition, other files will match yara's GlobalRuleExample.