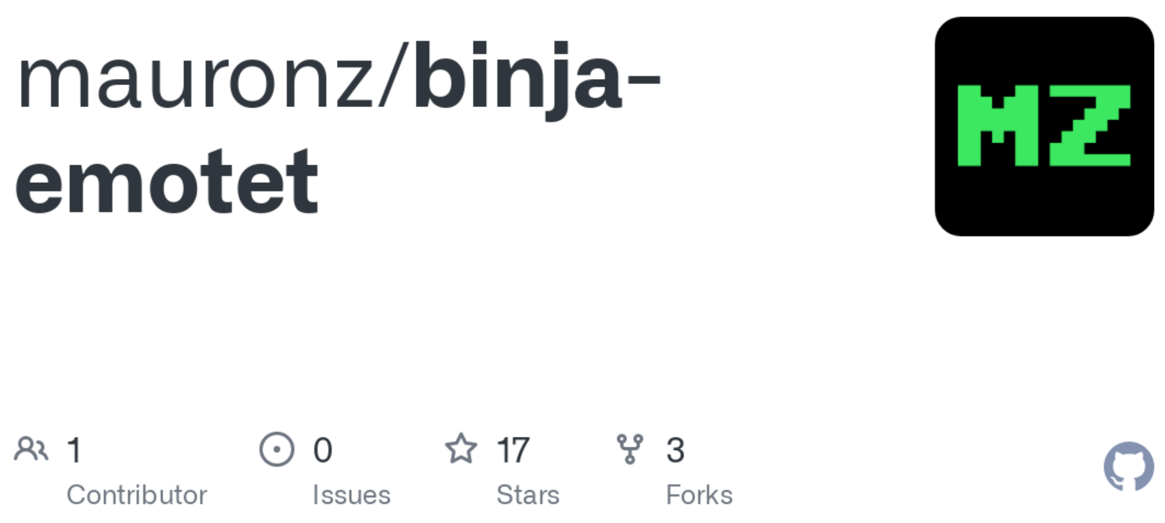
Emotet API+string deobfuscator (v0.1)

github.com/mauronz/binja-emotet

mauronz



mauronz/binja-emotet

1 Contributor

0 Issues

17 Stars

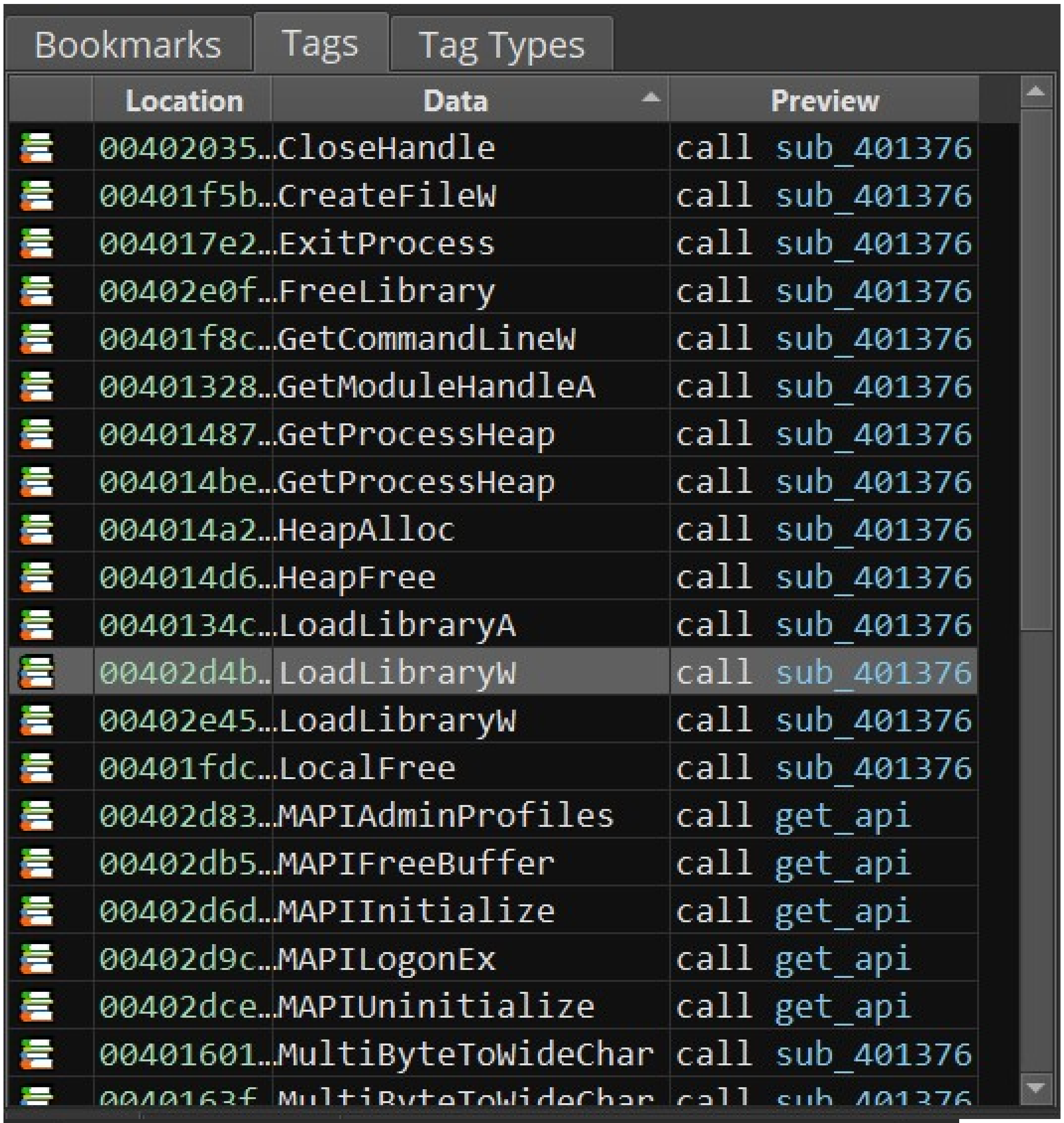
3 Forks

Author: **Francesco Muroni**

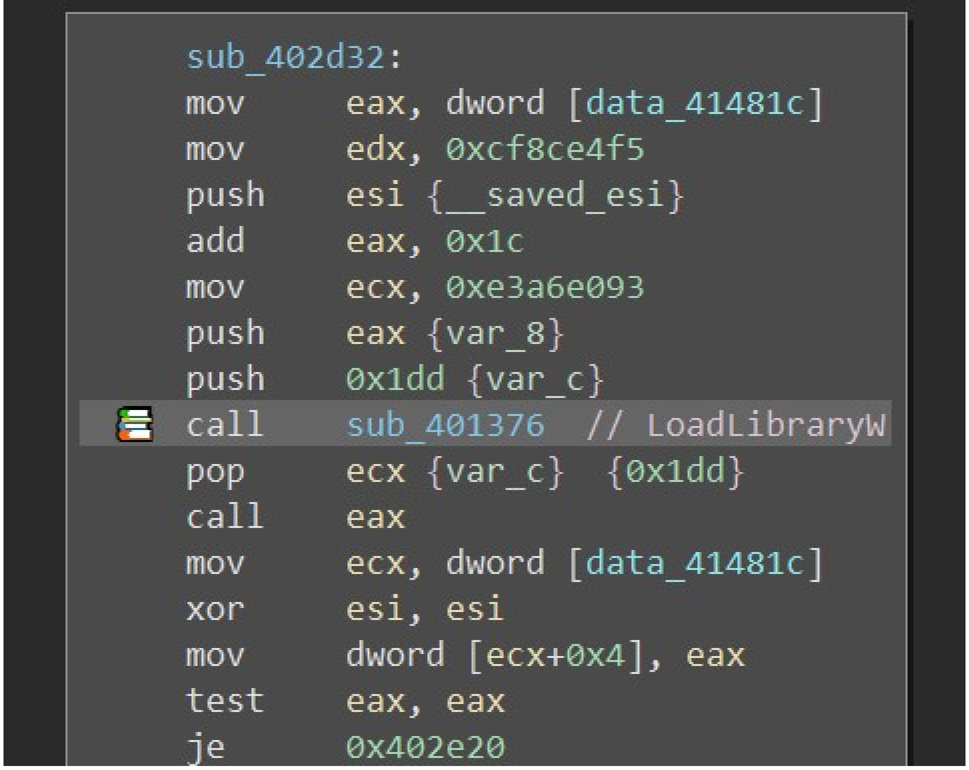
Deobufscate API calls and strings in unpacked Emotet samples.

Description:

Helper plugin for the analysis of unpacked Emotet samples. Locate dynamically imported API functions and add tags to make them easily searchable.

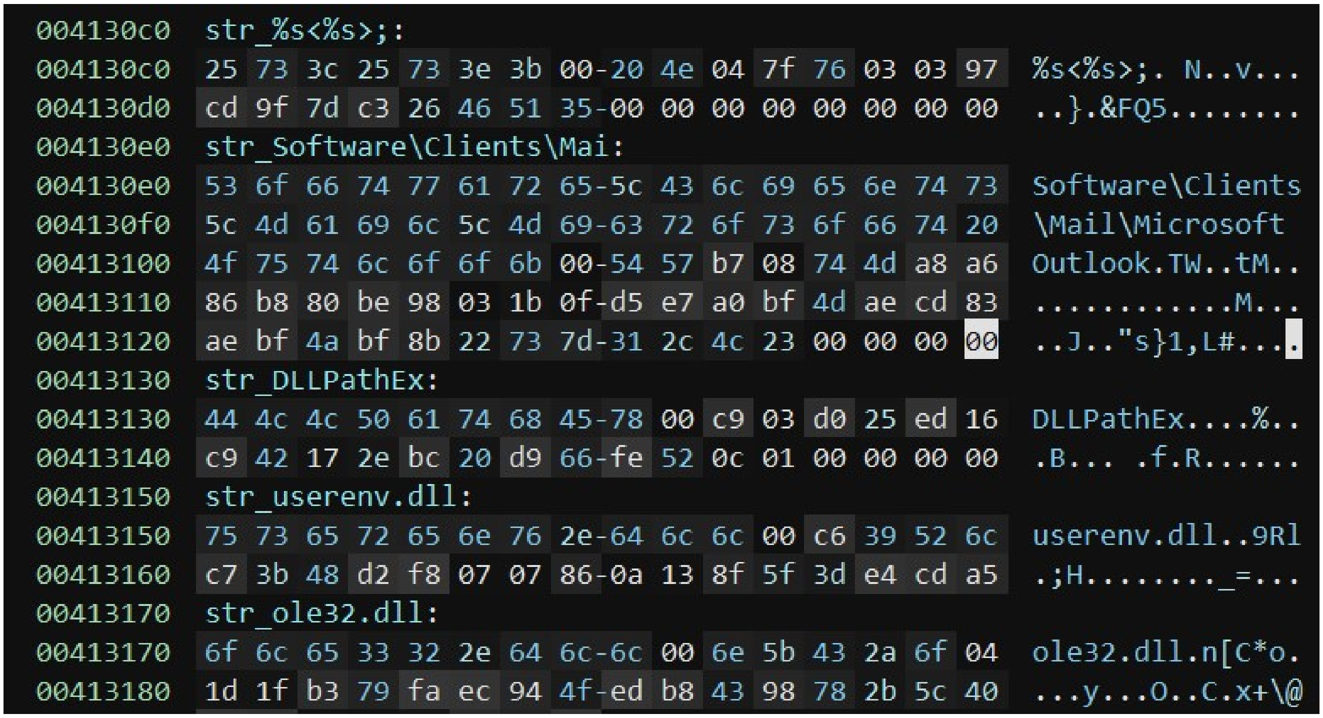


	Location	Data	Preview
	00402035…	CloseHandle	call sub_401376
	00401f5b…	CreateFileW	call sub_401376
	004017e2…	ExitProcess	call sub_401376
	00402e0f…	FreeLibrary	call sub_401376
	00401f8c…	GetCommandLineW	call sub_401376
	00401328…	GetModuleHandleA	call sub_401376
	00401487…	GetProcessHeap	call sub_401376
	004014be…	GetProcessHeap	call sub_401376
	004014a2…	HeapAlloc	call sub_401376
	004014d6…	HeapFree	call sub_401376
	0040134c…	LoadLibraryA	call sub_401376
	00402d4b…	LoadLibraryW	call sub_401376
	00402e45…	LoadLibraryW	call sub_401376
	00401fdc…	LocalFree	call sub_401376
	00402d83…	MAPIAdminProfiles	call get_api
	00402db5…	MAPIFreeBuffer	call get_api
	00402d6d…	MAPIInitialize	call get_api
	00402d9c…	MAPILogonEx	call get_api
	00402dce…	MAPIUninitialize	call get_api
	00401601…	MultiByteToWideChar	call sub_401376
	0040163f…	MultiByteToWideChar	call sub_401376



```
sub_402d32:
mov     eax, dword [data_41481c]
mov     edx, 0xcf8ce4f5
push    esi {__saved_esi}
add     eax, 0x1c
mov     ecx, 0xe3a6e093
push    eax {var_8}
push    0x1dd {var_c}
call    sub_401376  // LoadLibraryW
pop     ecx {var_c}  {0x1dd}
call    eax
mov     ecx, dword [data_41481c]
xor     esi, esi
mov     dword [ecx+0x4], eax
test    eax, eax
je      0x402e20
```

Replace obfuscated strings with their original value.



```
004130c0  str_%s<%s>;:
004130c0  25 73 3c 25 73 3e 3b 00-20 4e 04 7f 76 03 03 97  %s<%s>;. N..v...
004130d0  cd 9f 7d c3 26 46 51 35-00 00 00 00 00 00 00 00  ..}.&FQ5........
004130e0  str_Software\Clients\Mai:
004130e0  53 6f 66 74 77 61 72 65-5c 43 6c 69 65 6e 74 73  Software\Clients
004130f0  5c 4d 61 69 6c 5c 4d 69-63 72 6f 73 6f 66 74 20  \Mail\Microsoft
00413100  4f 75 74 6c 6f 6f 6b 00-54 57 b7 08 74 4d a8 a6  Outlook.TW..tM..
00413110  86 b8 80 be 98 03 1b 0f-d5 e7 a0 bf 4d ae cd 83  ............M...
00413120  ae bf 4a bf 8b 22 73 7d-31 2c 4c 23 00 00 00 00  ..J.."s}1,L#....
00413130  str_DLLPathEx:
00413130  44 4c 4c 50 61 74 68 45-78 00 c9 03 d0 25 ed 16  DLLPathEx....%..
00413140  c9 42 17 2e bc 20 d9 66-fe 52 0c 01 00 00 00 00  .B... .f.R......
00413150  str_userenv.dll:
00413150  75 73 65 72 65 6e 76 2e-64 6c 6c 00 c6 39 52 6c  userenv.dll..9Rl
00413160  c7 3b 48 d2 f8 07 07 86-0a 13 8f 5f 3d e4 cd a5  .;H........_=...
00413170  str_ole32.dll:
00413170  6f 6c 65 33 32 2e 64 6c-6c 00 6e 5b 43 2a 6f 04  ole32.dll.n[C*o.
00413180  1d 1f b3 79 fa ec 94 4f-ed b8 43 98 78 2b 5c 40  ...y...O..C.x+\@
```

License

This plugin is released under a MIT license.

Metadata Version

2