IoC Analysis: CrackMe01.exe

Información

Tipo:	PE	**Firma:**	Microsoft Visual C++ VC8 Microsoft Visual C++
Bits:	x32	**Arquitectura:**	X86
Endiness:	little	**Entry point:**	0x13cc
Image Address:	0x1000		

Hashes

MD5	4c235ddd021665752054d2c9a8cefd71
SHA1	29a2ae98de1d4d18ec39890ed9b96b81196ddf5b
SHA256	c9b5b22f8f98031252253487cd7622756dfbb03bd011dd9394bfa2212969c183

Otros Hashes:

Imphash MD5	EE9CC9973AFC3F4EC7C40AC58BAC53C3
SSDeep	192:Xej799E4mwHjOM3IIv/rPoNN7E5pz67VSkGPk:Xu77nmqj17/2N78kGM
TLSH	T181124B03FE514963CB998BF4253395EEC1BBB7234B916253B7BB95464B35160E00304F

Secciones/segmentos

Nombre	Dirección
.text	0x401000
.rdata	0x402000
.data	0x403000
.rsrc	0x404000
.reloc	0x405000

Cadenas de interés

yVjtU	YYuQb	,tkuj	EQPyYYe
VhuftUj			
uytvt	EUEMj	Hola bienvenido al primer reto.	Reto superado, guarda la password para las respuestas
Pista en https://www.youtube.com/watch?v=Zz6rp3Qn3_c			
C:\Users\IEUser\source\repos\RetosIniciales\Release\CrackMe01.pdb	GCTL	Hmemset	Xexit
jterminate			
UnhandledExceptionFilter	mSetUnhandledExceptionFilter	GetCurrentProcess	TerminateProcess
IsProcessorFeaturePresent			
MQueryPerformanceCounter	GetCurrentProcessId	GetCurrentThreadId	GetSystemTimeAsFileTime
cInitializeSListHead			
IsDebuggerPresent	xGetModuleHandleW		

Símbolos

Nombre	Dirección	Tipo
__current_exception_context	0x0	SymbolType.TYPE_FUNCTION
__current_exception	0x0	SymbolType.TYPE_FUNCTION
memset	0x0	SymbolType.TYPE_FUNCTION
_except_handler4_common	0x0	SymbolType.TYPE_FUNCTION
_set_fmode	0x0	SymbolType.TYPE_FUNCTION
__stdio_common_vfprintf	0x0	SymbolType.TYPE_FUNCTION
gets	0x0	SymbolType.TYPE_FUNCTION
__acrt_iob_func	0x0	SymbolType.TYPE_FUNCTION
__p__commode	0x0	SymbolType.TYPE_FUNCTION
_c_exit	0x0	SymbolType.TYPE_FUNCTION
_exit	0x0	SymbolType.TYPE_FUNCTION
_initialize_onexit_table	0x0	SymbolType.TYPE_FUNCTION
_cexit	0x0	SymbolType.TYPE_FUNCTION
_crt_atexit	0x0	SymbolType.TYPE_FUNCTION
_seh_filter_exe	0x0	SymbolType.TYPE_FUNCTION
terminate	0x0	SymbolType.TYPE_FUNCTION
__p___argv	0x0	SymbolType.TYPE_FUNCTION
_set_app_type	0x0	SymbolType.TYPE_FUNCTION
_register_thread_local_exe_atexit_callback	0x0	SymbolType.TYPE_FUNCTION
__p___argc	0x0	SymbolType.TYPE_FUNCTION
_register_onexit_function	0x0	SymbolType.TYPE_FUNCTION
exit	0x0	SymbolType.TYPE_FUNCTION
_initterm_e	0x0	SymbolType.TYPE_FUNCTION
_initterm	0x0	SymbolType.TYPE_FUNCTION
_get_initial_narrow_environment	0x0	SymbolType.TYPE_FUNCTION
_initialize_narrow_environment	0x0	SymbolType.TYPE_FUNCTION
_configure_narrow_argv	0x0	SymbolType.TYPE_FUNCTION
_controlfp_s	0x0	SymbolType.TYPE_FUNCTION

__setusermatherr	0x0	SymbolType.TYPE_FUNCTION
_configthreadlocale	0x0	SymbolType.TYPE_FUNCTION
_set_new_mode	0x0	SymbolType.TYPE_FUNCTION
GetSystemTimeAsFileTime	0x0	SymbolType.TYPE_FUNCTION
SetUnhandledExceptionFilter	0x0	SymbolType.TYPE_FUNCTION
GetCurrentProcess	0x0	SymbolType.TYPE_FUNCTION
TerminateProcess	0x0	SymbolType.TYPE_FUNCTION
IsProcessorFeaturePresent	0x0	SymbolType.TYPE_FUNCTION
GetModuleHandleW	0x0	SymbolType.TYPE_FUNCTION
IsDebuggerPresent	0x0	SymbolType.TYPE_FUNCTION
InitializeSListHead	0x0	SymbolType.TYPE_FUNCTION
UnhandledExceptionFilter	0x0	SymbolType.TYPE_FUNCTION
GetCurrentThreadId	0x0	SymbolType.TYPE_FUNCTION
GetCurrentProcessId	0x0	SymbolType.TYPE_FUNCTION
QueryPerformanceCounter	0x0	SymbolType.TYPE_FUNCTION
__current_exception_context	0x0	SymbolType.TYPE_FUNCTION
__current_exception	0x4	SymbolType.TYPE_FUNCTION
memset	0x8	SymbolType.TYPE_FUNCTION
_except_handler4_common	0xc	SymbolType.TYPE_FUNCTION
_set_fmode	0x10	SymbolType.TYPE_FUNCTION
__stdio_common_vfprintf	0x14	SymbolType.TYPE_FUNCTION
gets	0x18	SymbolType.TYPE_FUNCTION
__acrt_iob_func	0x1c	SymbolType.TYPE_FUNCTION
__p__commode	0x20	SymbolType.TYPE_FUNCTION
_c_exit	0x24	SymbolType.TYPE_FUNCTION
_exit	0x28	SymbolType.TYPE_FUNCTION
_initialize_onexit_table	0x2c	SymbolType.TYPE_FUNCTION
_cexit	0x30	SymbolType.TYPE_FUNCTION
_crt_atexit	0x34	SymbolType.TYPE_FUNCTION
_seh_filter_exe	0x38	SymbolType.TYPE_FUNCTION
terminate	0x3c	SymbolType.TYPE_FUNCTION
__p___argv	0x40	SymbolType.TYPE_FUNCTION
_set_app_type	0x44	SymbolType.TYPE_FUNCTION
_register_thread_local_exe_atexit_callback	0x48	SymbolType.TYPE_FUNCTION
__p___argc	0x4c	SymbolType.TYPE_FUNCTION
_register_onexit_function	0x50	SymbolType.TYPE_FUNCTION
exit	0x54	SymbolType.TYPE_FUNCTION
_initterm_e	0x58	SymbolType.TYPE_FUNCTION
_initterm	0x5c	SymbolType.TYPE_FUNCTION
_get_initial_narrow_environment	0x60	SymbolType.TYPE_FUNCTION
_initialize_narrow_environment	0x64	SymbolType.TYPE_FUNCTION
_configure_narrow_argv	0x68	SymbolType.TYPE_FUNCTION
_controlfp_s	0x6c	SymbolType.TYPE_FUNCTION
__setusermatherr	0x70	SymbolType.TYPE_FUNCTION
_configthreadlocale	0x74	SymbolType.TYPE_FUNCTION
_set_new_mode	0x78	SymbolType.TYPE_FUNCTION
GetSystemTimeAsFileTime	0x7c	SymbolType.TYPE_FUNCTION
SetUnhandledExceptionFilter	0x80	SymbolType.TYPE_FUNCTION
GetCurrentProcess	0x84	SymbolType.TYPE_FUNCTION
TerminateProcess	0x88	SymbolType.TYPE_FUNCTION
IsProcessorFeaturePresent	0x8c	SymbolType.TYPE_FUNCTION
GetModuleHandleW	0x90	SymbolType.TYPE_FUNCTION
IsDebuggerPresent	0x94	SymbolType.TYPE_FUNCTION
InitializeSListHead	0x98	SymbolType.TYPE_FUNCTION
UnhandledExceptionFilter	0x9c	SymbolType.TYPE_FUNCTION
GetCurrentThreadId	0xa0	SymbolType.TYPE_FUNCTION
GetCurrentProcessId	0xa4	SymbolType.TYPE_FUNCTION
QueryPerformanceCounter	0xa8	SymbolType.TYPE_FUNCTION
KiUserExceptionDispatcher	0x1014	SymbolType.TYPE_FUNCTION
_fmode	0x1018	SymbolType.TYPE_FUNCTION
_commode	0x101c	SymbolType.TYPE_FUNCTION
_acmdln	0x1020	SymbolType.TYPE_FUNCTION
_wcmdln	0x1024	SymbolType.TYPE_FUNCTION
UnresolvableJumpTarget	0x1028	SymbolType.TYPE_FUNCTION
UnresolvableCallTarget	0x102c	SymbolType.TYPE_FUNCTION

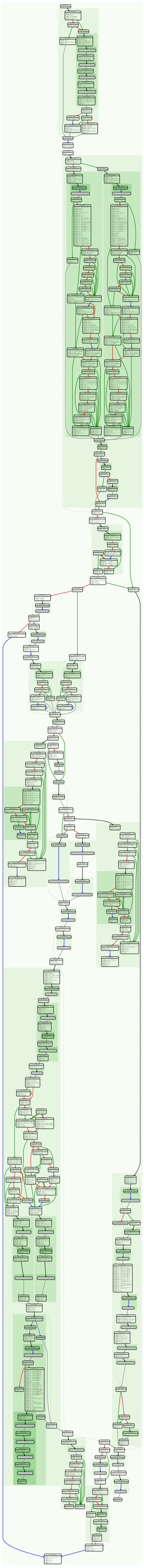
Funciones

Nombre	**Dirección**	**Hash SSDeep**
sub_401000	0x401000	3:3TSx3z7V4Rs:jSR/Vcs
sub_401010	0x401010	6:vh5ThDxWBGp71bA2T2COpgGt9wNhWsE9EY/NuQOr2udFm2TuLJ2XV:vh5TnWy71E2atgGt9w/WsyEtQqNdc2ey
sub_401040	0x401040	48:5NmI+TTNtNsGxOBOZWOZU1PGAt/G5L4N39Gz:5Nv+TtsGxOoZ1ZU1PGA1G5LK39Gz
sub_401174	0x401174	3:9shJF52TFVVT+UK5V13+WKQKhHVfTsAHj6LpGVR0FAVdMVR9hExbPA0ZURLvVMhh:9IJF52TRTOGQw5ThD4pGv7M79hEJPbZf
sub_401185	0x401185	12:vhW4gb6JyEEE7XPzot2LgGDXNfUOBE15jSWwyEgUPoGqknBADTJ68J6wjMEwwyEs:5W4etibrDddBGlz2qTA34b7UzKs
sub_401230	0x401230	3:FJ0dQxZXAK:FJkQxZXV
sub_401238	0x401238	3:FJ0dR5AVdfwNQ3AE9J2dMWcCn:FJk/owE9EMWcCn
sub_4012f5	0x4012f5	12:eiUR/AtwsdOzuI9/WXeW0P5ciUVdoSjE/mWRdobOEIDFPfUPWXfN7nedEgDMrgeo:e1AZsj9eLyccXcO9DFF82NHdEMe7
sub_4012ff	0x4012ff	3:vsABRdL2gSQ2TjlL:vhLdV2T5L
sub_401371	0x401371	3:3TQdLL57gvIK+xkKX56E3+xkKX54d4vjwv7nJFASKAGt6W+AE9J2dLhKVhrGACn:jQdX57gQzp5Hup5djg7nJ/bGt9/E9E9n
sub_401385	0x401385	6:jAVJj7EgfwZVgJ+iG0TVedMdg7uQKFEp57nQxdX57s7gW60VDAaA8OIHJd:EJj7ffU+NV8dWg7udEX7n0p73W6013L
_start	0x4013cc	24:TM7ruOPGdDGbVZzzVYSRgkdENa7T84Rl5:TM7rumGdkBJgkOa7TP5
sub_4013d6	0x4013d6	6:vh5ThDxMg2Tuo7bA2TSZAA2TAE9A2TD8XV:vh5Tcg2So7E2BA2cyA2Ha
sub_401416	0x401416	24:bxxC8LWjEZiWom6L+ziTS+vHrrv1uE8GmnUfA7x7uzxsUstCUiKus:0rzP1p62Kus
sub_4014f7	0x4014f7	12:vh5TwX7hW7pQu/+MF3l2OTF3urf8mzSqp7NSGr8+mXNj8vGNX0Y8hN:55TwM7quT3QOJ3urf8meq7kHOC0vhN
sub_40153b	0x40153b	6:vhWXgEJPbZpXsSshp5ItzcK3F5QOrsVsdwt03RvEJPLbT17PbZAsK:vhWXgApIXIWyQqsCwtCBUPDAZ
sub_40156d	0x40156d	6:vh5ThDy7y0ToA7+VTh1J6KTKTUqT5vX8XlXj6UqTYvBMkmlXSOfn:vh5TI75o/p6KTKTUmB8oUmYvCkmwOf
sub_4015a6	0x4015a6	12:vh5T2gFbZdhWy7ZWN1zl4xPTsYAFxg/62lMs2los2lEs2l9s2a0s2TJ/QlAWN3zN:55TtFboOA1R+hVyuKLLNKAADVFJK4
sub_40162d	0x40162d	12:vsb72MUOO7srX2g+tQuOrDPsv7uiHp73W6013oDquOsrX70Ri/0GtTEXAKdQu86i:pMUOLGOuOpiHeYDqu3watTSQu8KM8e7
sub_401692	0x401692	3:3TSxkKX57gvIK+xkKX54d4vRJ2yQ4d4hEFI5xJAKn:jSp57gQzp5dRJKAI5DVn
sub_4016a5	0x4016a5	3:3TAVJWKp7Eo1v7NfDDrAFM9jdLL57s7wvW6KvVDArGAEVOBVOrO6JPV:jAVJj7Eot7uildX57s7gW60VDAaA8OIr

sub_4016c1	0x4016c1	3:vsAHVfTsAHj6wiVdLkUAExbPA0ZUTBYclXZVFgJ+ie2AsVT+TBQMh8IIsjdLDwvt:vh5ThDwgEJPbZKeclXrFgJ+iy0TsWMhY
sub_4016de	0x4016de	6:vh5ThD/gJ+VThIA0ZKMKg7bErAgJ+iNE/00T/o7bEmlXSKA0lXV:vh5T2gUZKdg7grNNED/o7gmwgP
sub_401706	0x401706	6:vh5ThDy2TxV8u7kshodMvv9gVbHkMlvwApdWiL3bJLF574DXSeSdWiL3bJLF574x:vh5TI2lSu7LodQvq+fSBbFj74OeSBbF8
sub_401733	0x401733	3:vsAHVfTsAHj6f5Rv7eeUdfxLnSdYXfqLAvhd+ESKXlXV:vh5ThDQ7bEpLSdWiLSdTtlXV
sub_401748	0x401748	12:vh5TmpG37KYG77hyA2S+X7X7X7a2E7a2A7bhSoyA2KXX7qO71W7b:55TmpdAPS+Z0xPKXlo
sub_401795	0x401795	12:8p2/WsNXVEzR9WN0PLPWK/xYE2j5AUbWN0PLPc82nL62j7p3AFE2nL62jK:8UeeXVEjA1KJk1AUbARLLVHpw1LVW
sub_4017e0	0x4017e0	3:Q8XAK:Q8XV
sub_4017e3	0x4017e3	3:Q8MyshdPV:Q8uZ
sub_4017e7	0x4017e7	3:3TSx3z/vFn:jSRZn
sub_4017ed	0x4017ed	3:vsVLQtkSQ2TM0s:vZc2TMV
sub_4017f9	0x4017f9	3:3TTgdn:jA
sub_4017fc	0x4017fc	3:vsV2VD+VmVvD+VeM0dMP3U36ExbPLJVT+dBAxibMVdQpws:vXNVrMkMP3c6EJPLbTiWibEQpZ
sub_40181d	0x40181d	3:v:v
sub_401820	0x401820	3:3TSx3z1VvF:jSRxVvF
sub_401826	0x401826	6:FJkY/EdX5QOryBSQBG3QOrs5oQedX5QOryBSQ+QOrs5XVn:oXpQqykQEQqs5o1pQqykQ+Qqs5XVn
sub_401843	0x401843	3:Q8GoXQ2TCkyg4K:Q8a2TCxgd
sub_40184f	0x40184f	3:3TSx3z0n:jSRk
sub_401855	0x401855	3:3TSx3z0ZAK:jSR4
sub_40185b	0x40185b	3:vsAHVfTsAHj6LpGVRhHdCKsVFAVdMVR9hExbPA0ZUdERAGdLL57e4:vh5ThD4pGvhx7M79hEJPbZEERAGdX57n
sub_401874	0x401874	12:w5673qPJ/yEu57Z7Os7ZAg7LJH7/P7zG3WourPo17BjSX7A7YthSg7G7G8XQIv7Z:wvsl9JDFzHf8AIZkAz7If7hiJxwP6b
sub_401975	0x401975	3:gkR+Swn:gD
sub_40197a	0x40197a	6:vBMg2TVZEJPbZflGsjdXKpwtP/TFjdX5QOv/+vatDbTFhRXptWP/Tht2hhtu0Z7H:vCg2RZAtFawzvpQu/+itDPvVjWP7ht+f
sub_4019bd	0x4019bd	3:vsVnLvGgiSQ2TuX0s:vGer2TuEs
sub_4019c9	0x4019c9	12:vh5TnWsNnp7fyGTDfSdZlVTD53rKXdzGD9oTC9jHd9s2LfRr9s2Lgs:55TWe5aZP5rKNzA3
sub_401a1f	0x401a1f	3:iEX52Tzd45QRs:iEX52TzdVRs
sub_401a27	0x401a27	6:vhxhWBnDUFkNxp9n5NnpjWb60UzbDTEdhA9XsdG2TkFnpjWb60UzbD/OIEyj6:vhxhWhDLzpHNnpQ60UznGhAF8G2QnpQV
sub_401a53	0x401a53	6:vhxhWBnyFrFkQA9k/NnpjWb60UzcEdhA9Xe3FGdG2TkFnpjWb60UzeOIEyj6:vhxhWhjQA2/NnpQ60UznhAFe3MG2QnpR
sub_401a8e	0x401a8e	3:oGrRA7+joFsJ:oGrg+EFsJ
sub_401a96	0x401a96	3:oGrRA7+ibp0s34Ek:oGrg+ibpV3u
sub_401aa8	0x401aa8	3:FJ0dyon:FJkRn
sub_401ab1	0x401ab1	3:KGRFzn:KGRN
sub_401ab6	0x401ab6	3:qSKp6u4Dc4:etOc4
sub_401ac2	0x401ac2	3:Vv:d
sub_401ac5	0x401ac5	3:r1n:r1
sub_401ac8	0x401ac8	3:3TwvE45EcfJ+hd4wJNKVhrGAEVOeVOBVOr8VJ0YVVbGtvF:jgEG1J+JJNKXaA8OKOI8VJHVbGtd
sub_401ad8	0x401ad8	6:vh5ThDxWBGp7g1dMlVK7f930/u7ff7NgWWxXkJaV1cmXV:vh5TnWy7gjkK7ZAu7X7NgW60Jy+4
sub_401b07	0x401b07	48:5NLa0bnUHwQ07nWxANggMho6ZP18Wp2PHH4CmP1No4L0xuNm7W4UVRUMW5in:5NxQAZfMBDU2yikuf9jUMWy
sub_401cd7	0x401cd7	3:Q8GoXQ2TUJ8nXAK:Q8a2TUJIF
__current_exception	0x401ce3	3:gXQ2TD:gXQ2TD
__current_exception_context	0x401ce9	3:gXQ2TP:gXQ2TP
memset	0x401cef	3:gXQ2T+:gXQ2T+
_except_handler4_common	0x401cf5	3:gXQ2Tk:gXQ2Tk
_seh_filter_exe	0x401cfb	3:gXQ2Trn:gXQ2Trn
_set_app_type	0x401d01	3:gXQ2T4n:gXQ2T4n
__setusermatherr	0x401d07	3:gXQ2TV:gXQ2TV
_configure_narrow_argv	0x401d0d	3:gXQ2Tln:gXQ2Tln
_initialize_narrow_environment	0x401d13	3:gXQ2TZn:gXQ2TZn
_get_initial_narrow_environment	0x401d19	3:gXQ2T4n:gXQ2T4
_initterm	0x401d1f	3:gXQ2Tp:gXQ2Tp
_initterm_e	0x401d25	3:gXQ2TN:gXQ2TN
exit	0x401d2b	3:gXQ2TB:gXQ2TB
_exit	0x401d31	3:gXQ2TK:gXQ2TK
_set_fmode	0x401d37	3:gXQ2Tin:gXQ2Tin
__p___argc	0x401d3d	3:gXQ2Tgn:gXQ2Tgn
__p___argv	0x401d43	3:gXQ2Tin:gXQ2Ti
_cexit	0x401d49	3:gXQ2T64:gXQ2T64
_c_exit	0x401d4f	3:gXQ2TW:gXQ2TW
_register_thread_local_exe_atexit_callback	0x401d55	3:gXQ2TEn:gXQ2TEn
_configthreadlocale	0x401d5b	3:gXQ2Tt:gXQ2Tt
_set_new_mode	0x401d61	3:gXQ2TM:gXQ2TM
__p__commode	0x401d67	3:gXQ2Tr:gXQ2Tr
_initialize_onexit_table	0x401d6d	3:gXQ2Tu:gXQ2Tu
_register_onexit_function	0x401d73	3:gXQ2TB:gXQ2TB
_crt_atexit	0x401d79	3:gXQ2Tfn:gXQ2Tfn
_controlfp_s	0x401d7f	3:gXQ2Txn:gXQ2Txn
terminate	0x401d85	3:gXQ2THn:gXQ2THn
IsProcessorFeaturePresent	0x401d8b	3:gXQ2TJn:gXQ2TJn
sub_401d91	0x401d91	12:vh5TnGtfS2nTGX7W7kvV7gX7CdPaL7kazTGbdO++fJSYjefszoRTG2:55TGt1KcuNbd7+fcoeqoA2
__current_exception_context	0x500000	
__current_exception	0x500004	
memset	0x500008	
_except_handler4_common	0x50000c	
_set_fmode	0x500010	
__stdio_common_vfprintf	0x500014	
gets	0x500018	
__acrt_iob_func	0x50001c	
__p__commode	0x500020	
_c_exit	0x500024	
_exit	0x500028	
_initialize_onexit_table	0x50002c	
_cexit	0x500030	
_crt_atexit	0x500034	
_seh_filter_exe	0x500038	
terminate	0x50003c	
__p___argv	0x500040	
_set_app_type	0x500044	
_register_thread_local_exe_atexit_callback	0x500048	
__p___argc	0x50004c	
_register_onexit_function	0x500050	
exit	0x500054	
_initterm_e	0x500058	

_initterm	0x50005c
_get_initial_narrow_environment	0x500060
_initialize_narrow_environment	0x500064
_configure_narrow_argv	0x500068
_controlfp_s	0x50006c
__setusermatherr	0x500070
_configthreadlocale	0x500074
_set_new_mode	0x500078
GetSystemTimeAsFileTime	0x50007c
SetUnhandledExceptionFilter	0x500080
GetCurrentProcess	0x500084
TerminateProcess	0x500088
IsProcessorFeaturePresent	0x50008c
GetModuleHandleW	0x500090
IsDebuggerPresent	0x500094
InitializeSListHead	0x500098
UnhandledExceptionFilter	0x50009c
GetCurrentThreadId	0x5000a0
GetCurrentProcessId	0x5000a4
QueryPerformanceCounter	0x5000a8
UnresolvableCallTarget	0x60102c

Control-Flow graph



Estado del proceso

EMU CFG: OK
Nodos CFG: 336

FAST CFG: OK
Vertices CFG: 519