

00401057	. 8D45 A8	LEA EAX, DWORD PTR SS:[EBP-58]	pStartupInfo
0040105A	. 50	PUSH EAX	CurrentDir = NULL
0040105B	. 6A 00	PUSH 0	pEnvironment = NULL
0040105D	. 6A 00	PUSH 0	CreationFlags = 0
0040105F	. 6A 00	PUSH 0	InheritHandles = TRUE
00401061	. 6A 01	PUSH 1	pThreadSecurity = NULL
00401063	. 6A 00	PUSH 0	pProcessSecurity = NULL
00401065	. 6A 00	PUSH 0	CommandLine = "cmd"
00401067	. 68 30504000	PUSH Malware_.00405030	ModuleFileName = NULL
0040106C	. 6A 00	PUSH 0	CreateProcessA
0040106E	. FF15 04404000	CALL DWORD PTR DS:[&KERNEL32.CreatePro	Timeout = INFINITE
00401074	. 8945 EC	MOV DWORD PTR SS:[EBP-14], EAX	hObject
00401077	. 6A FF	PUSH -1	WaitForSingleObject
00401079	. 8B4D F0	MOV ECX, DWORD PTR SS:[EBP-10]	
0040107C	. 51	PUSH ECX	
0040107D	. FF15 00404000	CALL DWORD PTR DS:[&KERNEL32.WaitForSi	
00401083	. 33C0	XOR EAX, EAX	
00401085	. 98FF	MOV EBP, EBP	

Address	Disassembly	Comment	Registers (FPU)
3401574	85		EAX 00280105
3401575	8BEC	MOV EBP, ESP	EAX 00280105
3401576	8B	PUSH -1, ESP	EAX 00280105
340157C	8B C0404000	PUSH Halware_004040C0	EAX 00000000
3401581	8B C3404000	PUSH Halware_004040C0	EAX 00000000
3401584	64:R1 00000000	MOV EAX, DMWORD PTR FS:[0]	EAX 7FFC0000
3401585	8B C0404000	PUSH Halware_004040C0	EAX 00000000
340158D	64:9225 000000	MOV DMWORD PTR FS:[0], ESP	EAX 00000000
3401590	8BEC 10	SUB ESP, 10	EAX 00000000
3401597	83	PUSH EBX	EAX 00000000
3401598	83	PUSH ESI	EAX 00000000
3401599	83	PUSH EDI	EAX 00000000
340159A	64:58	MOV DMWORD PTR SS:[EBP-10], ESP	EAX 00000000
340159B	FF15 30404000	CALL DMWORD PTR DS:[kernel32.GetVersion]	EAX 00000000
340159C	8B C0404000	PUSH Halware_004040C0	EAX 00000000
340159D	8B C0404000	PUSH Halware_004040C0	EAX 00000000
340159E	8B C0404000	PUSH Halware_004040C0	EAX 00000000
340159F	8B C0404000	PUSH Halware_004040C0	EAX 00000000
34015A0	8B C0404000	PUSH Halware_004040C0	EAX 00000000
34015A1	8B C0404000	PUSH Halware_004040C0	EAX 00000000
34015A2	8B C0404000	PUSH Halware_004040C0	EAX 00000000
34015A3	8B C0404000	PUSH Halware_004040C0	EAX 00000000
34015A4	8B C0404000	PUSH Halware_004040C0	EAX 00000000
34015A5	8B C0404000	PUSH Halware_004040C0	EAX 00000000
34015A6	8B C0404000	PUSH Halware_004040C0	EAX 00000000
34015A7	8B C0404000	PUSH Halware_004040C0	EAX 00000000
34015A8	8B C0404000	PUSH Halware_004040C0	EAX 00000000
34015A9	8B C0404000	PUSH Halware_004040C0	EAX 00000000
34015AA	8B C0404000	PUSH Halware_004040C0	EAX 00000000
34015AB	8B C0404000	PUSH Halware_004040C0	EAX 00000000
34015AC	8B C0404000	PUSH Halware_004040C0	EAX 00000000
34015AD	8B C0404000	PUSH Halware_004040C0	EAX 00000000
34015AE	8B C0404000	PUSH Halware_004040C0	EAX 00000000
34015AF	8B C0404000	PUSH Halware_004040C0	EAX 00000000
34015B0	8B C0404000	PUSH Halware_004040C0	EAX 00000000
34015B1	8B C0404000	PUSH Halware_004040C0	EAX 00000000
34015B2	8B C0404000	PUSH Halware_004040C0	EAX 00000000
34015B3	8B C0404000	PUSH Halware_004040C0	EAX 00000000
34015B4	8B C0404000	PUSH Halware_004040C0	EAX 00000000
34015B5	8B C0404000	PUSH Halware_004040C0	EAX 00000000
34015B6	8B C0404000	PUSH Halware_004040C0	EAX 00000000
34015B7	8B C0404000	PUSH Halware_004040C0	EAX 00000000
34015B8	8B C0404000	PUSH Halware_004040C0	EAX 00000000
34015B9	8B C0404000	PUSH Halware_004040C0	EAX 00000000
34015BA	8B C0404000	PUSH Halware_004040C0	EAX 00000000
34015BB	8B C0404000	PUSH Halware_004040C0	EAX 00000000
34015BC	8B C0404000	PUSH Halware_004040C0	EAX 00000000
34015BD	8B C0404000	PUSH Halware_004040C0	EAX 00000000
34015BE	8B C0404000	PUSH Halware_004040C0	EAX 00000000
34015BF	8B C0404000	PUSH Halware_004040C0	EAX 00000000
34015C0	8B C0404000	PUSH Halware_004040C0	EAX 00000000
34015C1	8B C0404000	PUSH Halware_004040C0	EAX 00000000
34015C2	8B C0404000	PUSH Halware_004040C0	EAX 00000000
34015C3	8B C0404000	PUSH Halware_004040C0	EAX 00000000
34015C4	8B C0404000	PUSH Halware_004040C0	EAX 00000000
34015C5	8B C0404000	PUSH Halware_004040C0	EAX 00000000
34015C6	8B C0404000	PUSH Halware_004040C0	EAX 00000000
34015C7	8B C0404000	PUSH Halware_004040C0	EAX 00000000
34015C8	8B C0404000	PUSH Halware_004040C0	EAX 00000000
34015C9	8B C0404000	PUSH	

[illegible]