

Il valore del parametro CommandLine passato allo stack e successivamente alla funzione CreateProcessA è "cmd" ovvero il comando per ottenere il controllo di una shell su windows.

00401056	52	PUSH EDI	pProcessInfo
00401057	8045 A8	LEA EAX, DWORD PTR SS:[EBP-58]	pStartupInfo
00401058	5A	PUSH EAX	CurrentDir = NULL
00401059	6A 00	PUSH 0	Environment = NULL
0040105A	6A 00	PUSH 0	CreationFlags = 0
0040105B	6A 00	PUSH 0	InheritHandles = TRUE
0040105C	6A 00	PUSH 0	ThreadSecurity = NULL
0040105D	6A 00	PUSH 0	pProcessSecurity = NULL
0040105E	6A 00	PUSH 0	CommandLine = "cmd"
0040105F	6A 00	PUSH 0	ModuleFileName = NULL
00401060	6A 00	PUSH 0	kernel32.CreateProcessA
00401061	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.CreateProcessA>]	
00401062	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.CreateProcessA>]	

Mettendo un breakpoint all'indirizzo "004015A3" possiamo notare come il valore dei suoi registri EH ed EL siano rispettivamente "0A" e "28".

00401593	56	PUSH ESI	Registers (FPU)
00401594	57	PUSH EDI	EAX 00000000
00401595	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	ECX 77FD0000
00401596	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	EDX 00000000
00401597	52	PUSH EDI	EBX 77FD0000
00401598	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	ESP 0012FF94
00401599	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	EBP 0012FFC0
0040159A	52	PUSH EDI	ESI FFFFFFFF
0040159B	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	EDI 7C910208 ntdll!7C910208
0040159C	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	EIP 00000000
0040159D	52	PUSH EDI	
0040159E	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
0040159F	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015A0	52	PUSH EDI	
004015A1	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015A2	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015A3	52	PUSH EDI	
004015A4	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015A5	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015A6	52	PUSH EDI	
004015A7	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015A8	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015A9	52	PUSH EDI	
004015AA	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015AB	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015AC	52	PUSH EDI	
004015AD	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015AE	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015AF	52	PUSH EDI	
004015B0	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015B1	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015B2	52	PUSH EDI	
004015B3	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015B4	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015B5	52	PUSH EDI	
004015B6	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015B7	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015B8	52	PUSH EDI	
004015B9	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015BA	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015BB	52	PUSH EDI	
004015BC	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015BD	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015BE	52	PUSH EDI	
004015BF	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015C0	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015C1	52	PUSH EDI	
004015C2	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015C3	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015C4	52	PUSH EDI	
004015C5	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015C6	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015C7	52	PUSH EDI	
004015C8	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015C9	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015CA	52	PUSH EDI	
004015CB	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015CC	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015CD	52	PUSH EDI	
004015CE	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015CF	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015D0	52	PUSH EDI	
004015D1	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015D2	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015D3	52	PUSH EDI	
004015D4	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015D5	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015D6	52	PUSH EDI	
004015D7	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015D8	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015D9	52	PUSH EDI	
004015DA	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015DB	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015DC	52	PUSH EDI	
004015DD	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015DE	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015DF	52	PUSH EDI	
004015E0	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015E1	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015E2	52	PUSH EDI	
004015E3	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015E4	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015E5	52	PUSH EDI	
004015E6	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015E7	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015E8	52	PUSH EDI	
004015E9	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015EA	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015EB	52	PUSH EDI	
004015EC	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015ED	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015EE	52	PUSH EDI	
004015EF	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015F0	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015F1	52	PUSH EDI	
004015F2	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015F3	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015F4	52	PUSH EDI	
004015F5	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015F6	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015F7	52	PUSH EDI	
004015F8	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015F9	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015FA	52	PUSH EDI	
004015FB	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015FC	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015FD	52	PUSH EDI	
004015FE	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015FF	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	

Ma eseguendo uno "step-into" otteniamo come valore 0 in tutti i bit dato che la comparazione logica bit a bit XOR applicata a due oggetti simili da come risultato 0.

00401594	83EC 10	SUB ESP, 10	Registers (FPU)
00401595	56	PUSH ESI	EAX 00200105
00401596	57	PUSH EDI	ECX 00200105
00401597	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	EDX 00000000
00401598	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	EBX 77FD0000
00401599	52	PUSH EDI	ESP 0012FF94
0040159A	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	EBP 0012FFC0
0040159B	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	ESI FFFFFFFF
0040159C	52	PUSH EDI	EDI 7C910208 ntdll!7C910208
0040159D	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	EIP 00401595 Halware_00401595
0040159E	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
0040159F	52	PUSH EDI	
004015A0	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015A1	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015A2	52	PUSH EDI	
004015A3	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015A4	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015A5	52	PUSH EDI	
004015A6	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015A7	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015A8	52	PUSH EDI	
004015A9	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015AA	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015AB	52	PUSH EDI	
004015AC	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015AD	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015AE	52	PUSH EDI	
004015AF	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015B0	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015B1	52	PUSH EDI	
004015B2	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015B3	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015B4	52	PUSH EDI	
004015B5	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015B6	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015B7	52	PUSH EDI	
004015B8	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015B9	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015BA	52	PUSH EDI	
004015BB	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015BC	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015BD	52	PUSH EDI	
004015BE	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015BF	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015C0	52	PUSH EDI	
004015C1	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015C2	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015C3	52	PUSH EDI	
004015C4	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015C5	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015C6	52	PUSH EDI	
004015C7	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015C8	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015C9	52	PUSH EDI	
004015CA	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015CB	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015CC	52	PUSH EDI	
004015CD	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015CE	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015CF	52	PUSH EDI	
004015D0	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015D1	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015D2	52	PUSH EDI	
004015D3	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015D4	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015D5	52	PUSH EDI	
004015D6	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015D7	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015D8	52	PUSH EDI	
004015D9	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015DA	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015DB	52	PUSH EDI	
004015DC	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015DD	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015DE	52	PUSH EDI	
004015DF	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015E0	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015E1	52	PUSH EDI	
004015E2	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015E3	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015E4	52	PUSH EDI	
004015E5	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015E6	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015E7	52	PUSH EDI	
004015E8	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015E9	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015EA	52	PUSH EDI	
004015EB	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015EC	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion>]	
004015ED	52	PUSH EDI	
004015EE	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	
004015EF	FF15 30404000	CALL DWORD PTR DS:[<&kernel32	