



ASSEMBLY - MALWARE

♦ .text:00401000	push	ebp	
♦ .text:00401001	mov	ebp, esp	
♦ .text:00401003	push	ecx	
♦ .text:00401004	push	0	; dwReserved
♦ .text:00401006	push	0	; lpdwFlags
♦ .text:00401008	call	ds:InternetGetConnectedState	
♦ .text:0040100E	mov	[ebp+var_4], eax	
♦ .text:00401011	cmp	[ebp+var_4], 0	
♦ .text:00401015	jz	short loc_40102B	
♦ .text:00401017	push	offset aSuccessInterne	; "Success: Internet Connection\n"
♦ .text:0040101C	call	sub_40105F	
♦ .text:00401021	add	esp, 4	
♦ .text:00401024	mov	eax, 1	
♦ .text:00401029	jmp	short loc_40103A	
.text:0040102B	; -----		
.text:0040102B			

CREAZIONE DELLE VARIABILI "STACK"

LE VARIABILI SONO PASSATE SULLO STACK "CALL"

VENGONO CONTROLLATE CON UN IF

RISPOSTA, CONNESSIONE RIUSCITA

VIENE RICHIAMATO SUB:40105F "INIDIRIZZO DI MEMORIA" PER ESEGUIRE ALCUNE OPERAZIONI