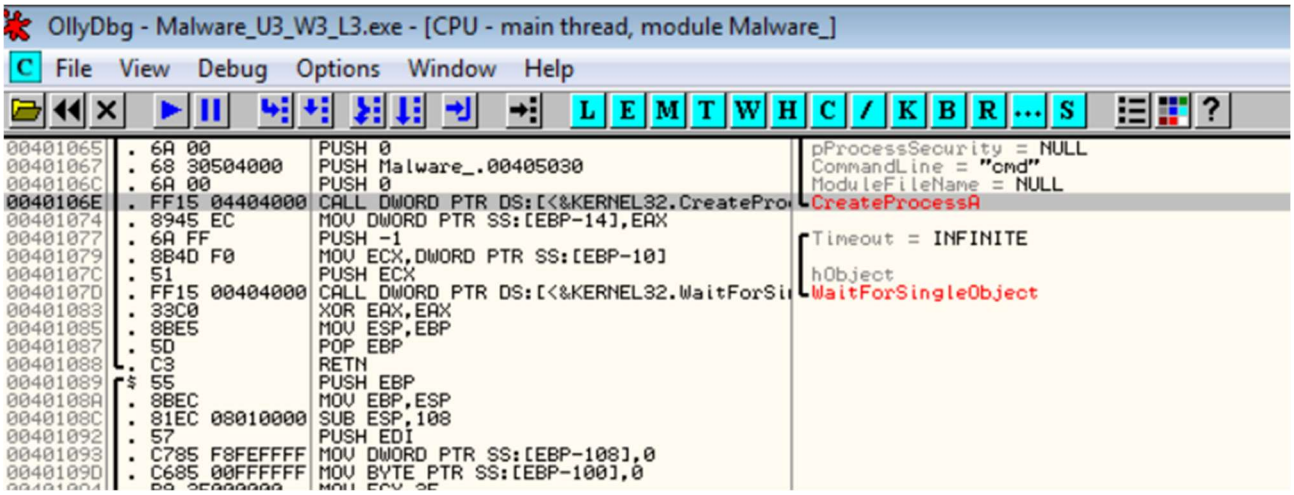
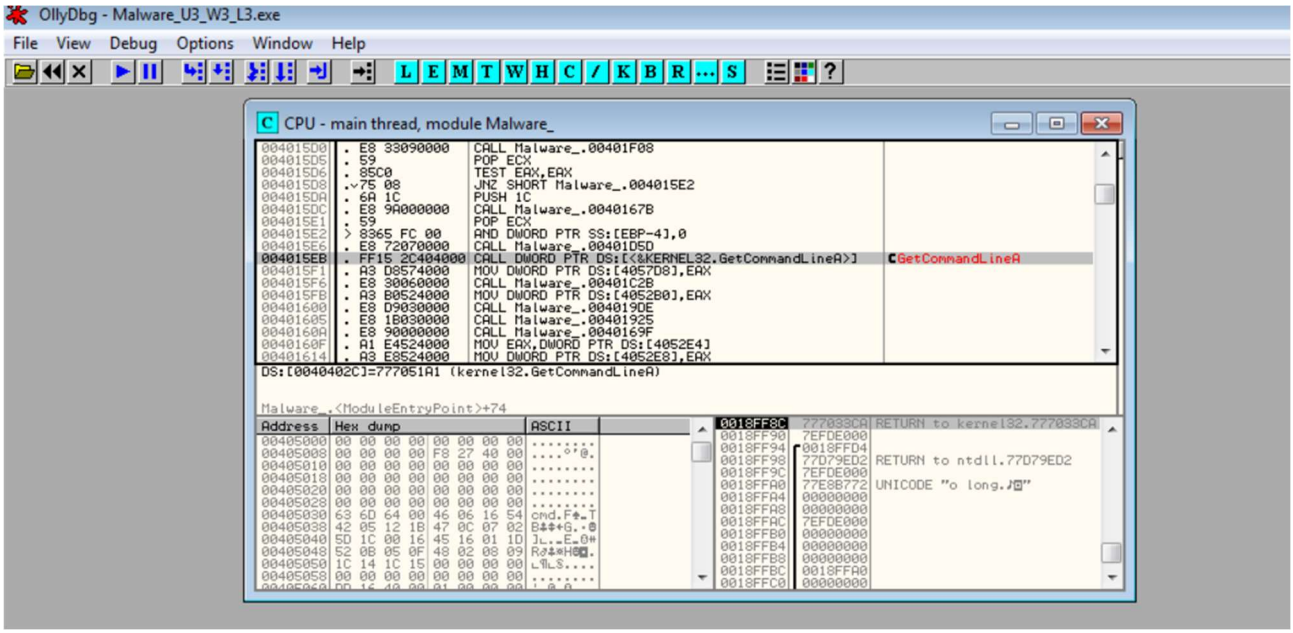
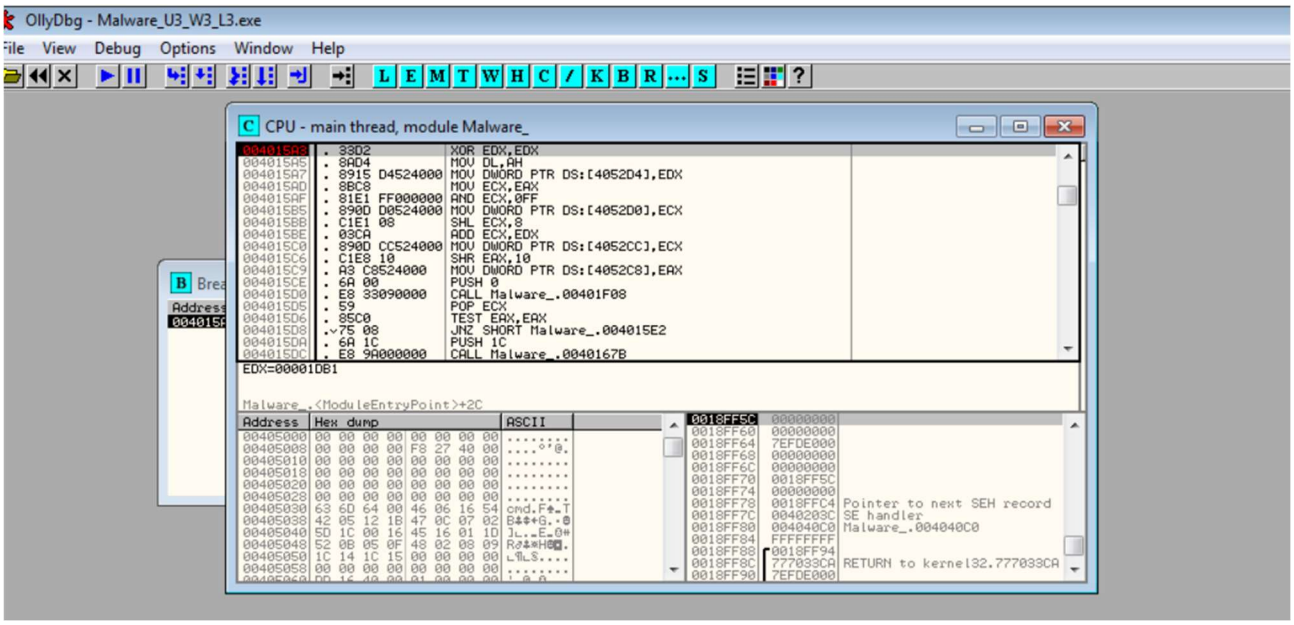
Traccia:

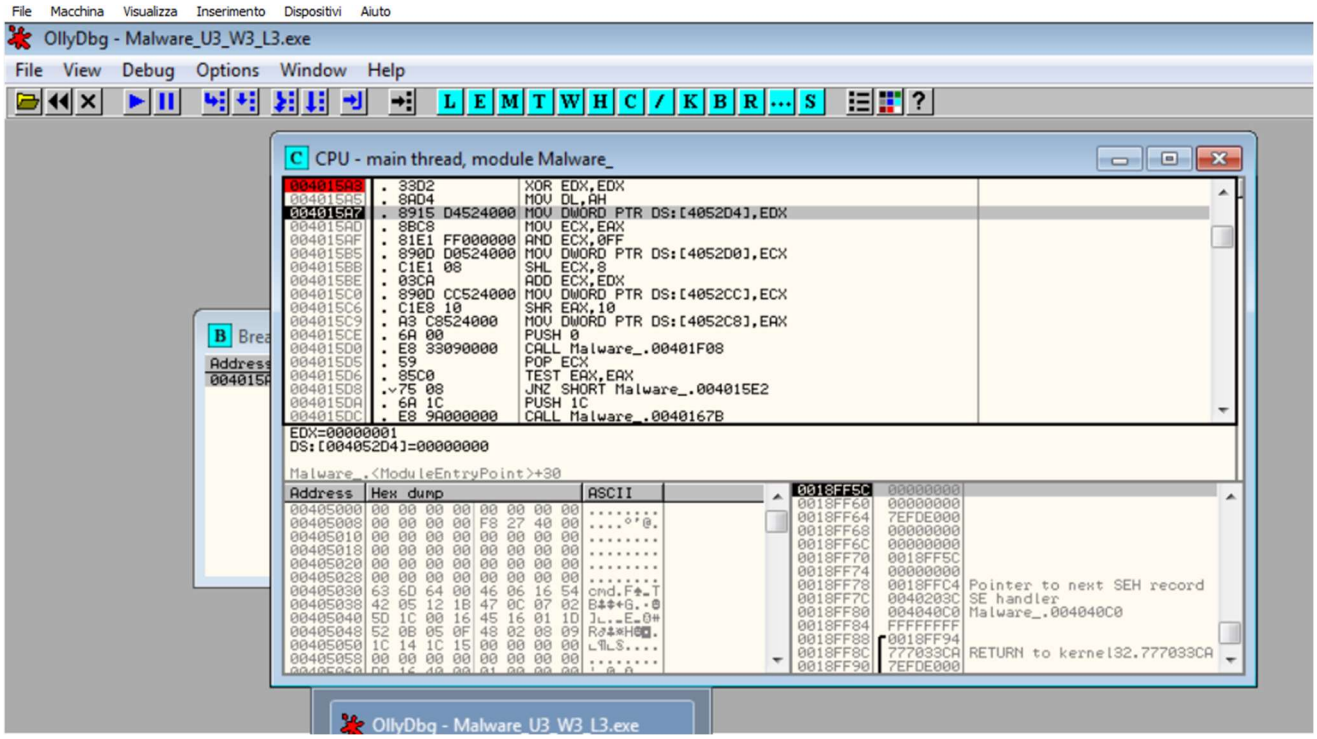
Fate riferimento al malware: Malware_U3_W3_L3, presente all'interno della cartella Esercizio_Pratico_U3_W3_L3 sul desktop della macchina virtuale dedicata all'analisi dei malware. Rispondete ai seguenti quesiti utilizzando OllyDBG. All'indirizzo 0040106E il Malware effettua una chiamata di funzione alla funzione «CreateProcess».

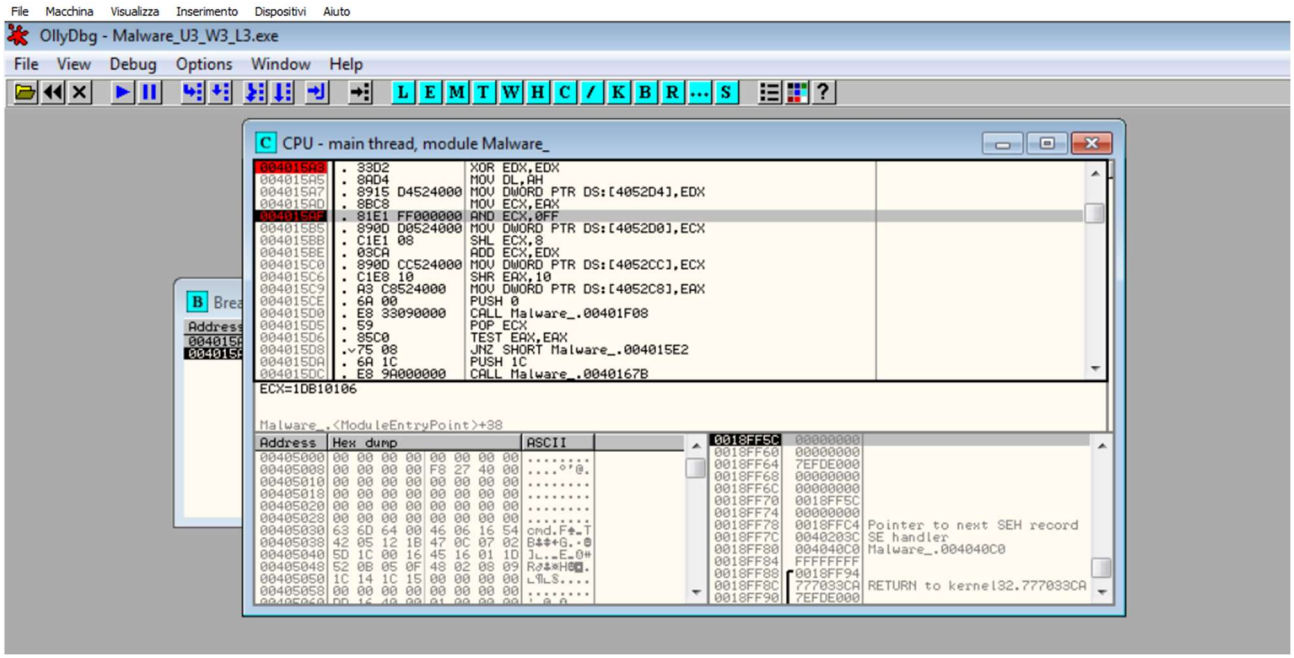
1. Qual è il valore del parametro «CommandLine» che viene passato sullo stack?
2. Inserite un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX?
3. Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX motivando la risposta.
4. Che istruzione è stata eseguita?
5. Inserite un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX?
6. Eseguite uno step-into. Qual è ora il valore di ECX? Spiegate quale istruzione è stata eseguita.

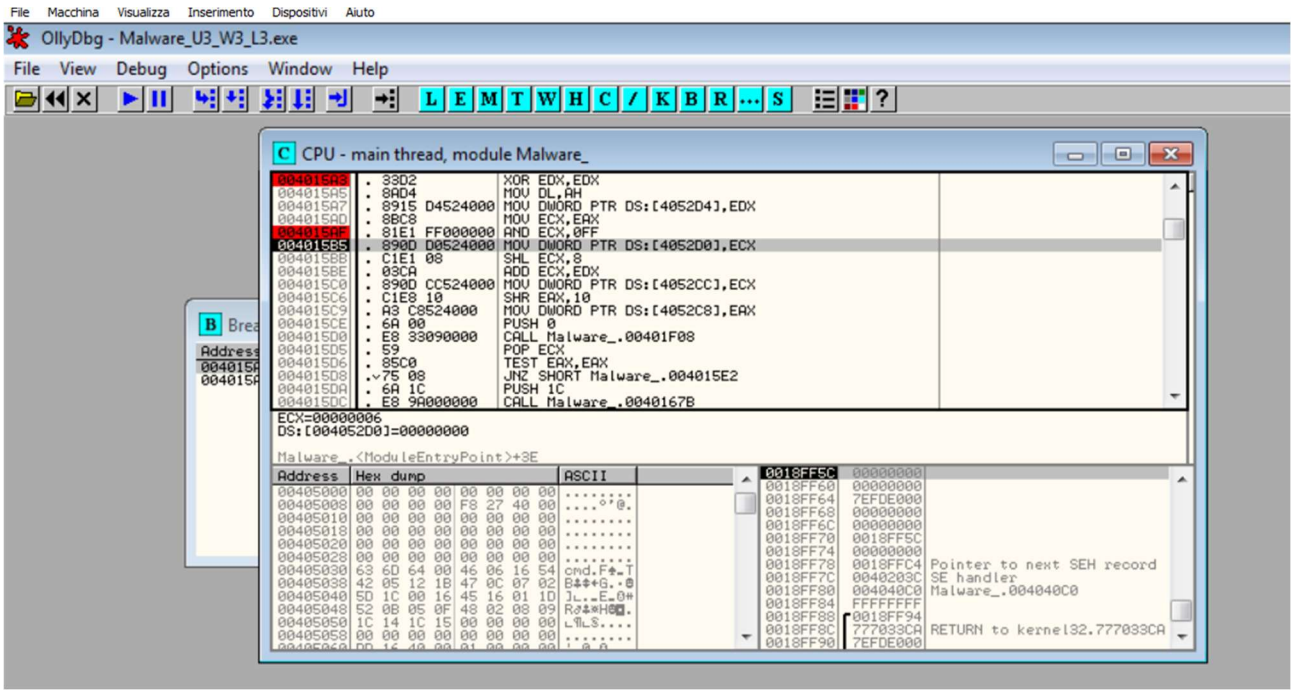





OllyDbg - Malware_U3_W3_L3.exe
File View Debug Options Window Help
CPU - main thread, module Malware_
004015A8 . 33D2 XOR EDX,EDX
004015AA . 8AD4 MOV DL,AH
004015A7 . 8915 D4524000 MOV DWORD PTR DS:[4052D4],EDX
004015AD . 8BC8 MOV ECX,EAX
004015AF . 81E1 FF000000 AND ECX,0FF
004015B5 . 890D D0524000 MOV DWORD PTR DS:[4052D0],ECX
004015BB . C1E1 08 SHL ECX,8
004015BE . 03CA ADD ECX,EDX
004015C0 . 890D CC524000 MOV DWORD PTR DS:[4052CC],ECX
004015C6 . C1E8 10 SHR EAX,10
004015C9 . A3 C8524000 MOV DWORD PTR DS:[4052C8],EAX
004015CE . 6A 00 PUSH 0
004015D0 . E8 33090000 CALL Malware_.00401F08
004015D5 . 59 POP ECX
004015D6 . 85C0 TEST EAX,EAX
004015D8 .v75 08 JNZ SHORT Malware_.004015E2
004015DA . 6A 1C PUSH 1C
004015DC . E8 9A000000 CALL Malware_.0040167B
EDX=00001DB1
Malware_.<ModuleEntryPoint>+2C
Address Hex dump ASCII
00405000 00 00 00 00 00 00 00 00 ....
00405008 00 00 00 00 F8 27 40 00 ....°'@.
00405010 00 00 00 00 00 00 00 00 ....
00405018 00 00 00 00 00 00 00 00 ....
00405020 00 00 00 00 00 00 00 00 ....
00405028 00 00 00 00 00 00 00 00 ....
00405030 63 6D 64 00 46 06 16 54 cmd.F♠_T
00405038 42 05 12 1B 47 0C 07 02 B♣$+G.•☻
00405040 5D 1C 00 16 45 16 01 1D]L..E.☺↔
00405048 52 0B 05 0F 48 02 08 09 R♂♣☼H☻◘.
00405050 1C 14 1C 15 00 00 00 00 L¶LS....
00405058 00 00 00 00 00 00 00 00 ....
0018FF5C 00000000
0018FF60 00000000
0018FF64 7EFDE000
0018FF68 00000000
0018FF6C 00000000
0018FF70 0018FF5C
0018FF74 00000000
0018FF78 0018FFC4 Pointer to next SEH record
0018FF7C 0040203C SE handler
0018FF80 004040C0 Malware_.004040C0
0018FF84 FFFFFFFF
0018FF88 0018FF94
0018FF8C 777033CA RETURN to kernel32.777033CA
0018FF90 7EFDE000


File Macchina Visualizza Inserimento Dispositivi Aiuto
OllyDbg - Malware_U3_W3_L3.exe
File View Debug Options Window Help
CPU - main thread, module Malware_
004015A8 . 33D2 XOR EDX,EDX
004015AA . 8AD4 MOV DL,AH
004015A7 . 8915 D4524000 MOV DWORD PTR DS:[4052D4],EDX
004015AD . 8BC8 MOV ECX,EAX
004015AF . 81E1 FF000000 AND ECX,0FF
004015B5 . 890D D0524000 MOV DWORD PTR DS:[4052D0],ECX
004015BB . C1E1 08 SHL ECX,8
004015BE . 03CA ADD ECX,EDX
004015C0 . 890D CC524000 MOV DWORD PTR DS:[4052CC],ECX
004015C6 . C1E8 10 SHR EAX,10
004015C9 . A3 C8524000 MOV DWORD PTR DS:[4052C8],EAX
004015CE . 6A 00 PUSH 0
004015D0 . E8 33090000 CALL Malware_.00401F08
004015D5 . 59 POP ECX
004015D6 . 85C0 TEST EAX,EAX
004015D8 .v75 08 JNZ SHORT Malware_.004015E2
004015DA . 6A 1C PUSH 1C
004015DC . E8 9A000000 CALL Malware_.0040167B
EDX=00000001
DS:[004052D4]=00000000
Malware_.<ModuleEntryPoint>+30
Address Hex dump ASCII
00405000 00 00 00 00 00 00 00 00 ....
00405008 00 00 00 00 F8 27 40 00 ....°'@.
00405010 00 00 00 00 00 00 00 00 ....
00405018 00 00 00 00 00 00 00 00 ....
00405020 00 00 00 00 00 00 00 00 ....
00405028 00 00 00 00 00 00 00 00 ....
00405030 63 6D 64 00 46 06 16 54 cmd.F♠_T
00405038 42 05 12 1B 47 0C 07 02 B♣$+G.•☻
00405040 5D 1C 00 16 45 16 01 1D]L..E.☺↔
00405048 52 0B 05 0F 48 02 08 09 R♂♣☼H☻◘.
00405050 1C 14 1C 15 00 00 00 00 L¶LS....
00405058 00 00 00 00 00 00 00 00 ....
0018FF5C 00000000
0018FF60 00000000
0018FF64 7EFDE000
0018FF68 00000000
0018FF6C 00000000
0018FF70 0018FF5C
0018FF74 00000000
0018FF78 0018FFC4 Pointer to next SEH record
0018FF7C 0040203C SE handler
0018FF80 004040C0 Malware_.004040C0
0018FF84 FFFFFFFF
0018FF88 0018FF94
0018FF8C 777033CA RETURN to kernel32.777033CA
0018FF90 7EFDE000
OllyDbg - Malware_U3_W3_L3.exe


File Macchina Visualizza Inserimento Dispositivi Aiuto
OllyDbg - Malware_U3_W3_L3.exe
File View Debug Options Window Help
CPU - main thread, module Malware_
004015A3 . 33D2 XOR EDX,EDX
004015A5 . 8AD4 MOV DL,AH
004015A7 . 8915 D4524000 MOV DWORD PTR DS:[4052D4],EDX
004015AD . 8BC8 MOV ECX,EAX
004015AF . 81E1 FF000000 AND ECX,0FF
004015B5 . 890D D0524000 MOV DWORD PTR DS:[4052D0],ECX
004015BB . C1E1 08 SHL ECX,8
004015BE . 03CA ADD ECX,EDX
004015C0 . 890D CC524000 MOV DWORD PTR DS:[4052CC],ECX
004015C6 . C1E8 10 SHR EAX,10
004015C9 . A3 C8524000 MOV DWORD PTR DS:[4052C8],EAX
004015CE . 6A 00 PUSH 0
004015D0 . E8 33090000 CALL Malware_.00401F08
004015D5 . 59 POP ECX
004015D6 . 85C0 TEST EAX,EAX
004015D8 .v75 08 JNZ SHORT Malware_.004015E2
004015DA . 6A 1C PUSH 1C
004015DC . E8 9A000000 CALL Malware_.0040167B
ECX=1DB10106
Malware_.<ModuleEntryPoint>+38
Address Hex dump ASCII
00405000 00 00 00 00 00 00 00 00 ....
00405008 00 00 00 00 F8 27 40 00 ....°'@.
00405010 00 00 00 00 00 00 00 00 ....
00405018 00 00 00 00 00 00 00 00 ....
00405020 00 00 00 00 00 00 00 00 ....
00405028 00 00 00 00 00 00 00 00 ....
00405030 63 6D 64 00 46 06 16 54 cmd.F♠-T
00405038 42 05 12 1B 47 0C 07 02 B♣↕←G.•@
00405040 5D 1C 00 16 45 16 01 1D]∟..E-☺↔
00405048 52 0B 05 0F 48 02 08 09 R♪♣☼H☻◘○
00405050 1C 14 1C 15 00 00 00 00 ∟¶∟§....
00405058 00 00 00 00 00 00 00 00 ....
0018FF5C 00000000
0018FF60 00000000
0018FF64 7EFDE000
0018FF68 00000000
0018FF6C 00000000
0018FF70 0018FF5C
0018FF74 00000000
0018FF78 0018FFC4 Pointer to next SEH record
0018FF7C 0040203C SE handler
0018FF80 004040C0 Malware_.004040C0
0018FF84 FFFFFFFF
0018FF88 0018FF94
0018FF8C 777033CA RETURN to kernel32.777033CA
0018FF90 7EFDE000


File Macchina Visualizza Inserimento Dispositivi Aiuto
OllyDbg - Malware_U3_W3_L3.exe
File View Debug Options Window Help
CPU - main thread, module Malware_
004015A3 . 33D2 XOR EDX,EDX
004015A5 . 8AD4 MOV DL,AH
004015A7 . 8915 D4524000 MOV DWORD PTR DS:[4052D4],EDX
004015AD . 8BC8 MOV ECX,EAX
004015AF . 81E1 FF000000 AND ECX,0FF
004015B5 . 890D D0524000 MOV DWORD PTR DS:[4052D0],ECX
004015BB . C1E1 08 SHL ECX,8
004015BE . 03CA ADD ECX,EDX
004015C0 . 890D CC524000 MOV DWORD PTR DS:[4052CC],ECX
004015C6 . C1E8 10 SHR EAX,10
004015C9 . A3 C8524000 MOV DWORD PTR DS:[4052C8],EAX
004015CE . 6A 00 PUSH 0
004015D0 . E8 33090000 CALL Malware_.00401F08
004015D5 . 59 POP ECX
004015D6 . 85C0 TEST EAX,EAX
004015D8 .v75 08 JNZ SHORT Malware_.004015E2
004015DA . 6A 1C PUSH 1C
004015DC . E8 9A000000 CALL Malware_.0040167B
ECX=00000006
DS:[004052D0]=00000000
Malware_.<ModuleEntryPoint>+3E
Address Hex dump ASCII
00405000 00 00 00 00 00 00 00 00 ....
00405008 00 00 00 00 F8 27 40 00 ....°'@.
00405010 00 00 00 00 00 00 00 00 ....
00405018 00 00 00 00 00 00 00 00 ....
00405020 00 00 00 00 00 00 00 00 ....
00405028 00 00 00 00 00 00 00 00 ....
00405030 63 6D 64 00 46 06 16 54 cmd.F♠-T
00405038 42 05 12 1B 47 0C 07 02 B♣↕←G.•@
00405040 5D 1C 00 16 45 16 01 1D]∟..E-☺↔
00405048 52 0B 05 0F 48 02 08 09 R♪♣☼H☻◘○
00405050 1C 14 1C 15 00 00 00 00 ∟¶∟§....
00405058 00 00 00 00 00 00 00 00 ....
0018FF5C 00000000
0018FF60 00000000
0018FF64 7EFDE000
0018FF68 00000000
0018FF6C 00000000
0018FF70 0018FF5C
0018FF74 00000000
0018FF78 0018FFC4 Pointer to next SEH record
0018FF7C 0040203C SE handler
0018FF80 004040C0 Malware_.004040C0
0018FF84 FFFFFFFF
0018FF88 0018FF94
0018FF8C 777033CA RETURN to kernel32.777033CA
0018FF90 7EFDE000