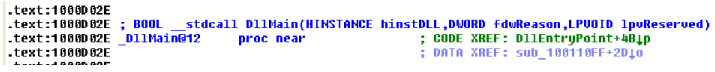
# Analisi statica avanzata con IDA

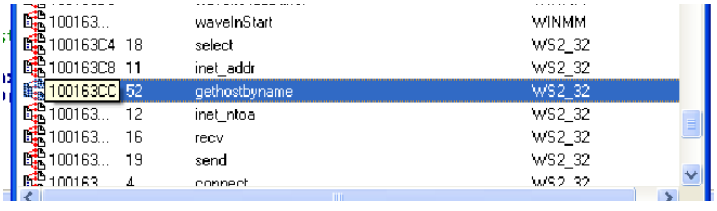
## Ernesto Robles

**Con l'uso di IDA è stata effettuata un'analisi statica avanzata come dall'immagine qui sotto raffigurata possiamo vedere come il tool abbia riconosciuto la funzione MAIN nel codice malware.**

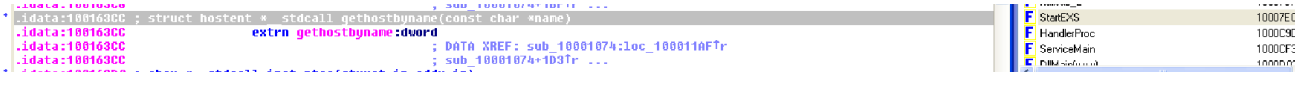




**Nella scheda imports è stato individuato la funzione "gethostbyname" e nelle immagini sottostanti vediamo l'indirizzo della funzione**




**Dopo aver cliccato sulla funzione veniamo inviati alla sezione che raffigura il codice che la compone da cui è possibile dedurre che gethostbyname è una funzione di libreria standard utilizzata per la risoluzione dei nomi di dominio in indirizzi IP in quanto la "hostent" di solito contiene informazioni come l'indirizzo IP associato al nome host, gli alias del nome host e altri dettagli correlati.**

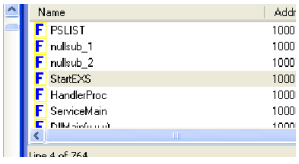



**La funzione alla locazione di memoria 0x10001656 ha 20 variabili locali e 1 parametro come si può vedere dall'immagine**


**Con l'uso di VirusTotal si controlla il file del malware riuscendo ad avere ulteriori informazioni più precise che ci permettono di fare ulteriori considerazioni attraverso**

**l'analisi degli import oppure delle funzioni,le immagini seguenti raffigurano funzioni che verificano il tipo di hardware, versioni del software e creano backdoor.**

```
.text:1000437C        push    eax             ; lpBuffer
.text:1000437D        push    edi             ; nBufferLength
.text:1000437E        call    ds:GetCurrentDirectoryA
.text:10004384        mov     esi, ds:sprintf
.text:1000438A        lea     eax, [ebp+buf]
.text:10004390        push    offset aBackdoorServer ; "\r\n\r\n*****************************\r\n[Ba"...
.text:10004395        push    eax             ; char *
.text:10004396        call    esi ; sprintf
.text:10004398        mov     ebx, [ebp+s]
.text:1000439B        lea     eax, [ebp+buf]
.text:100043A1        push    eax             ; buf
```




```
.text:10004033        mov     [esi+0C0h], eax
.text:10004039        lea     eax, [ebp+var_C]
.text:1000403C        push    eax             ; phkResult
.text:1000403D        push    1               ; samDesired
.text:1000403F        push    0               ; ulOptions
.text:10004041        push    offset aHardwareDescri ; "HARDWARE\\DESCRIPTION\\System\\CentralProc"...
.text:10004046        push    80000002h       ; hKey
.text:1000404B        mov     [ebp+var_14], 8
.text:10004052        call    edi ; RegOpenKeyExA
.text:10004054        lea     eax, [ebp+var_14]
.text:10004057        xor     edi, edi
.text:10004059        push    eax             ; lpcbData
.text:1000405A        lea     eax, [esi+0ACh]
.text:10004060        push    eax             ; lpData
.text:10004061        push    edi             ; lpType
.text:10004062        push    edi             ; lpReserved
.text:10004063        push    offset aMhz     ; "~MHz"
.text:10004068        push    [ebp+var_C]     ; hKey
.text:1000406B        call    ebx ; RegQueryValueExA
.text:1000406D        push    [ebp+var_C]     ; hKey
.text:10004070        call    ds:RegCloseKey
.text:10004076        lea     eax, [ebp+Buffer]
```