Strumenti di Base

Ora che avete la teoria in mano ed avete già visto cosa c'è da fare, è bene che cominciate a prendere confidenza con gli strumenti giusti per fa vedere al mondo la nostra "arte"; come minimo sindacale, avrete almeno bisogno di questo Kit di Base:

un analyzer (per riconoscere linguaggi ed eventuali packers/crypters): vi consiglio PEiD, semplice e completo;

- ho raccolto da vari siti i plugins più utili per questo programma ed il pack completo con l'ultima versione lo potete scaricare da qui.

un disassemblatore (per ricostruire il codice meglio possibile): un solo credo, un solo nome, IDA! ;-)

un debugger (per seguire il programma in runtime): due scuole di pensiero si dibattono da anni...

-

SoftIce [ora DriverStudio]: duro e cattivo, il primo debugger serio della storia, per utenti non alle prime armi!

-

OllyDbg: comodo e leggero, consente di soddisfare la maggior parte dei nostri bisogni di reversing. :-)

- plugins e .ini : molta della sua potenza, Olly la deve all'architettura a moduli, e nel corso dei mesi ne ho raccolto una nutrita serie, di cui alcuni abbastanza rari; inoltre, in collaborazione con la UIC (grazie a revenge70 per le segnalazioni!), ho messo a punto il file di configurazione con le opzioni più comuni già impostate ed un syntax highlighting a gusto personale... spero vi piaccia! ;-)

Per scaricare il pack completo (debugger configurato + tutti i plugins) cliccate qui.

un decompilatore (quando avete a che fare con VB e Delphi):

-

SmartCheck (fa anche da debugger): purtroppo non più sviluppato, ma tuttora molto potente ed adatto per rintracciare le procedure associate agli eventi.

- VBDE (decompilatore VB): un po' absoleto, ma con il VB6 ci sa fare.

- DeDe (decompilatore Delphi): il miglior strumento in assoluto per affrontare i figli dell'oracolo!

- un PE Editor (per dumpare i programmi e controllare il PE header): ne segnalo tre, ma ce ne sono a bizzeffe...

- PE Tools: carino, con un sacco di funzioni tra cui il PE Realigner, OEP Sniffer, DumpFixer, PE editing, FullDumper...

- PE Explorer: molto user-friendly, utile anche come Resource Editor.

- Lord PE: storico programma del grande Yoda, che fa ancora la sua porca figura.

- Wark: pregevole creatura di Ntoskrnl e Quake2 (i "Protected-Mode")... complimenti! :-D

un editor esadecimale (per sporcarsi le mani con i bytes!): anche qui c'è l'imbarazzo della scelta, ma personalmente ve ne indico due...

Hiew: vetusto e per DOS, ma velocissimo e ricco di opzioni (ora trova anche le stringhe!)

- Hex Workshop: più moderno, per Windows, ma bisogna abituarsi un po' all'interfaccia per sfruttarlo al massimo.

un patcher (per costruire file che applicano le nostre modifiche):

l'ottimo CodeFusion fa ancora egregiamente il suo dovere, ma in giro potete trovarne anche altri.

una reference (per avere sotto mano la sintassi e la descrizione delle API del linguaggio target):

- MSDN: mamma Micro$oft offre online questo immenso archivio su tutto quello che concerne la programmazione sotto Windows; indispensabile.

- ApiGuide: programmetto molto utile che contiene più di 900 funzioni divise in categorie e con relativi esempi.

La lista qui sopra è soltanto la punta dell'iceberg, giusto i tools più importanti per iniziare a spippolare un po'; per un elenco molto più completo, consultate l'apposito sticky post sul forum della UIC o comunque visitate la sezione Tools per quelli di cui ho fatto il mirror.

Per qualsiasi altro bisogno impellente di tools, recatevi da ProTools o da ExeTools (attualmente non più aggiornato), che sono pieni zeppo di roba, oppure da BiW.