J A M B I

Jambi is a PE infector. The program adds a new section of executable code in all exe files of the current directory. It modifies the EntryPoint field to run before regular execution ; then, returns back to original entry point.

Calls to Windows API are resolved at runtime, getting kernel base address and parsing export table of Kernel32 module.

Injected code is up to you.

Underlying concepts

- Windows API programming
- Virtual address space of Win32 process (exe module, kernel32, ntdll)
- Assembly programming
- Portable Executable (PE) file format
- Code flow

Language

ASM

Ressources

Introduction au format Portable Executable
http://esl.epitech.net/~arnaud/introduction-au-format-portable-executable

MASM32 (Microsoft assembler)
http://www.masm32.com

Iczelion's Win32 Assembly Homepage
http://win32assembly.online.fr

VX Heavens
http://vx.netlux.org

OllyDbg
http://www.ollydbg.de

Debugging tools for Windows
http://www.microsoft.com/whdc/DevTools/Debugging/default.mspx

LordPE
http://esl.epitech.net/~arnaud/lsd/s/pe-tools/lordpe/

Microsoft Portable Executable and Common Object File Format Specification
http://www.microsoft.com/whdc/system/platform/firmware/pecoff.mspx

Intel 64 and IA-32 Architectures Software Developer's Manual
http://www.intel.com/products/processor/manuals/