Virus Code… Revealed

The text files included with this document were obtained by disassembling code from an infected system folder (for Scores), and an infected application (for nVIR). This was performed using DisAsm, by Bob Arning, Version 2.0, released April 86.

I've had this utility for some time, downloaded from Compuserve, but didn't really get into it until I got into an assembler class at school. Now that I have some idea of what the instructions are, and the what and why of code segments, I've gotten curious to see the guts of the viruses that have been dogging my work area as of late. I'm NOT doing this to encourage some asshole to create a new and inproved model.

Comparing the code generated against previous efforts breaking down commercial applications, it looks pretty clean, with DisAsm seeming to catch all the labels and operands.

The nVIR virus code segments are all in one neat package, so the labeled file is all you need.

The Scores virus consists of three INITs, one atpl, and one DATA file. The virus parts can be found together in an infected System file, but it was easier for the disassembler to pick up the pieces from the external files the virus hides copies of it's components in. You should be able to find the text files for the following:

INIT ID 6
INIT ID 10
INIT ID 17
atpl ID 128
DATA ID 4001

If you've read about any of the symtoms of these little monsters, you'll be able to note some of the code segments that cause them. My main interest was to find the code that causes nVIR to say "Don't Panic" at boot up if MacInTalk is installed.

Personally, now that I've had experence disinfecting a few machines, these jewels aren't the swamp things I thought they would be, nothing a good battery of anti-virus tools and a half hour can't handle. That said, lemme add that if there are any hot-shot programmers who want to do something anti-social, write a better copy protection buster, my xxxx game needs it.

CMH