Virus Activation Routines

This paper was presented at the EICAR 1995 Conference in Zurich

Mikko Hyppönen
F-Secure Ltd

November 1995

Abstract: This paper categorizes different types of virus activation routines which are found in existing viruses and also discusses what triggers these activation routines. Common viruses are used as examples where possible. This paper also covers why it is important to know what a virus exactly does if you are infected by one. Some horror stories of the worst possible activation routine in a virus are also included. The scope of this paper is limited to PC compatible machines.

Introduction

General public's idea of a computer virus is usually something like "It's a program that destroys data". Strictly, this is not true, for a virus doesn't have to destroy anything in order to be a virus. In fact, most of the known viruses do not format hard drives or overwrite files - or do anything at all in addition to spreading.

All anti-virus support persons know that a lot of the people calling for support are asking "Your program said I have this virus. What does it do?", and the typical answer is: "Nothing. It just replicates".

People often find this surprising, because the destructive or spectacular viruses - naturally - get more publicity than the boring ones which have nothing special about them. Still, roughly half of the known viruses have no activation routines at all. Perhaps the authors of these viruses wanted to make the virus smaller by omitting such routines, or perhaps they reasoned that any activation at all is just going to make the virus discovered earlier. Or perhaps they just didn't have the imagination to think up one.

Common viruses and activation routines

When we look at some of the most common viruses worldwide, we see that most of them have no visible activation feature at all:

- AntiCMOS.A - has an activation routine, which is never executed
- AntiEXE - has an activation routine, which is practically never executed
- DIR_II.A - no activation routine
- Form.A - no activation routine
- Tai-Pan.438 - no activation routine
- Junkie - no activation routine
- Stoned.Empire.Monkey.B - no activation routine
- Stoned.Standard.A - has an activation routine, which is executed very seldom
- Stoned.No_INT.A - no activation routine
- Stealth_Boot.B - no activation routine

WordMacro/Concept - no activation routine

These viruses alone cover currently probably two thirds of all the virus infections worldwide. However, there are viruses with activation features among the most common viruses as well:

- Kampana.A - overwrites part of the hard drive after 400 boots
- Green_Caterpillar.1575 - draws a Caterpillar on screen after 60 days

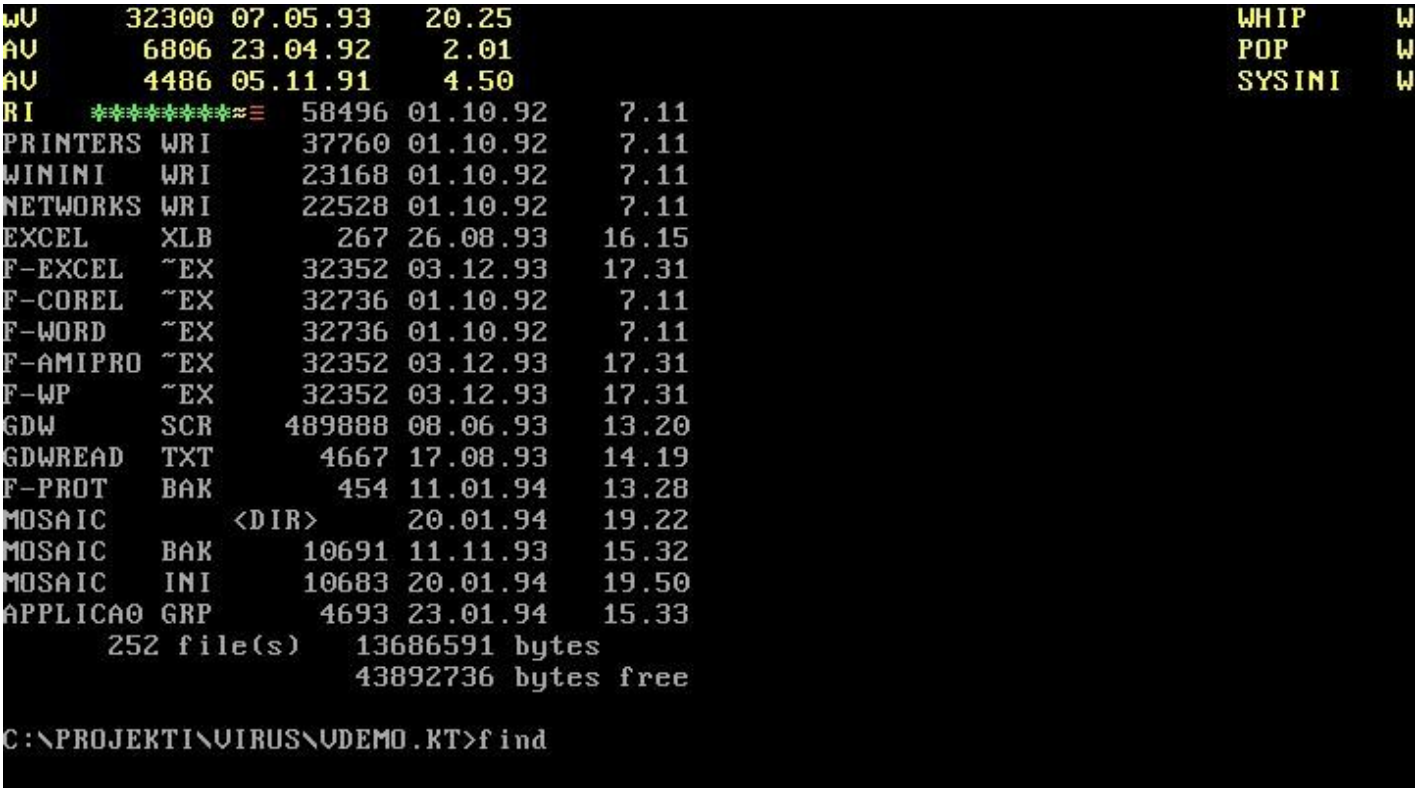


Figure 1: Activation routine of Green_Caterpillar.1575

- Michelangelo - overwrites part of the hard drive on every 6th of March
- Cascade.1701.A - drops letters to the bottom of the screen
- V-Sign - draws an ASCII graphics of a large V after every 64 boots
- Tequila - draws a fractal by random

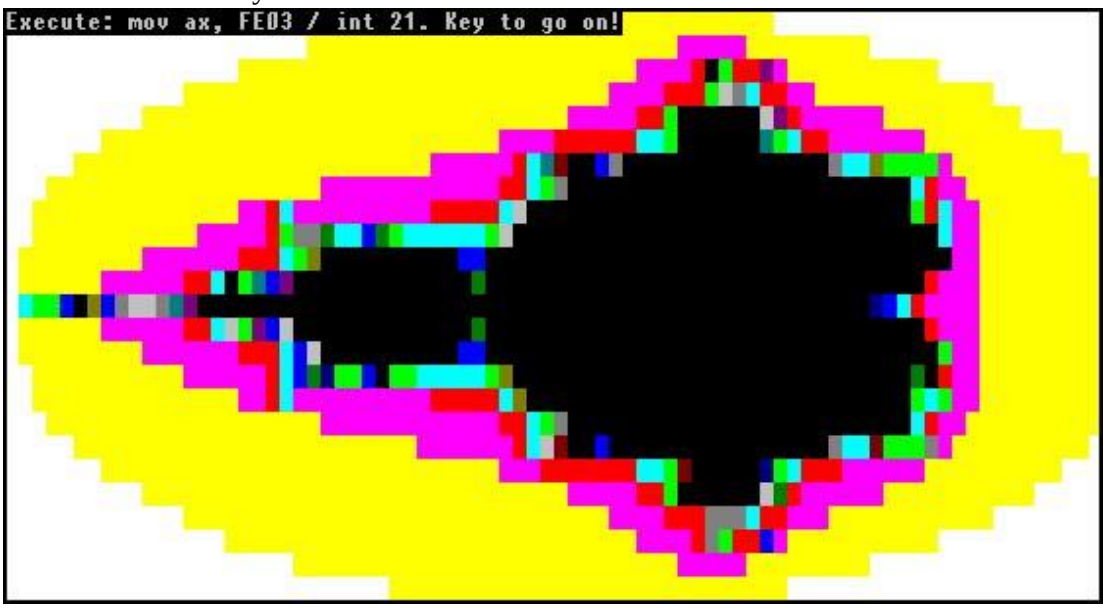


Figure 2: Fractal display of the Tequila virus

Classification

There are no formal classifications rules for different activation routines in viruses. However, we can categorize the routines from known viruses to the following groups:

Data destruction

Destructive activation routines can furthermore be grouped to immediate and gradual.

Examples of immediate destruction include viruses like Michelangelo, Kampana and Natas, which simply overwrite part of the hard drive with a low-level BIOS function. Other viruses with immediate destructive routines will delete or overwrite files instead of overwriting physical sectors.

Gradual destruction is done by viruses such as Ripper or Nomenklatura, which slowly corrupt the data on the hard drive. This is also sometimes called data-diddling. Such corruption is likely to go unnoticed until the corrupted data has been backed up several times. This makes recovering considerably more difficult, and in most cases significant amounts of data is lost for good.

Thankfully, destructive activation routines quite often fail to work due programming errors. It seems that the virus authors are reluctant to test these routines on their own machines.

It is also worth noticing that there are very few destructive viruses on the Macintosh side. This is possibly a result of the different user cultures between users of PC and Mac machines.

Sounds, tunes, speech

There are several viruses which activate by playing tunes through PC speaker. Probably the most common examples are the different Yankee_Doodle variants which activate by playing the Yankee Doodle tune at different times of day. Other viruses just produce beeps and zaps occasionally. There are also some viruses which try to speak - an example of this is the Dreamer virus, which tries to say "Hitler!" through the PC speaker. There exists also viruses which try to utilize a sound card if one is found from the infected PC.

Animations

Viruses which activate with an animation can be further grouped to text-mode and graphical animations. Examples of text-mode animations are the Cascade.1701.A virus, which will drop the characters on-screen to the bottom of the screen or the Walker virus, which will produce a walking man to the screen. Another example is the Vienna.Bua AKA Big Caibua virus, which gathered media attention by producing a text-mode animation of an ejaculating penis on-screen while deleting data on the hard drive.

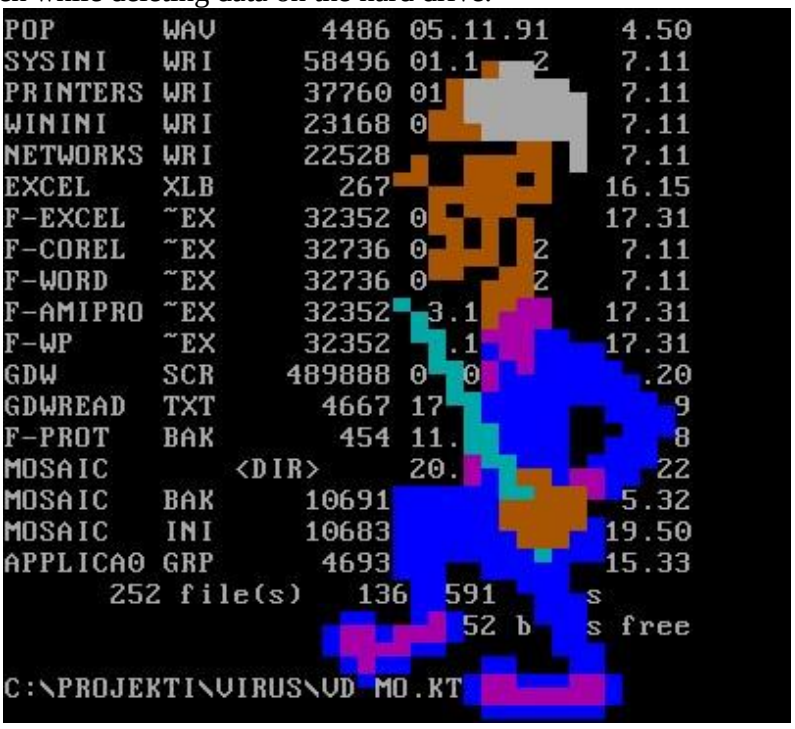


Figure 3: Activation routine of the Walker virus

Graphical activation routines are somewhat rarer, but such are found in viruses like Den_Zuk, which produces a logo on-screen, or the HH&H virus, which shows a quite interesting 3D animation of a bouncing ball build out of small dots.



Figure 4: Activation routine of the Den_Zuko virus

Messages

Viruses which display messages on-screen, include Stoned.Standard.A, which occasionally displays "Your PC is now Stoned!" if the machine is booted from a floppy. Another common virus which has a message to display is the Parity_Boot.B virus, which activates by displaying "PARITY CHECK".

A more interesting display is produced by the Rescue virus, which shows a screen full of nonsense messages.

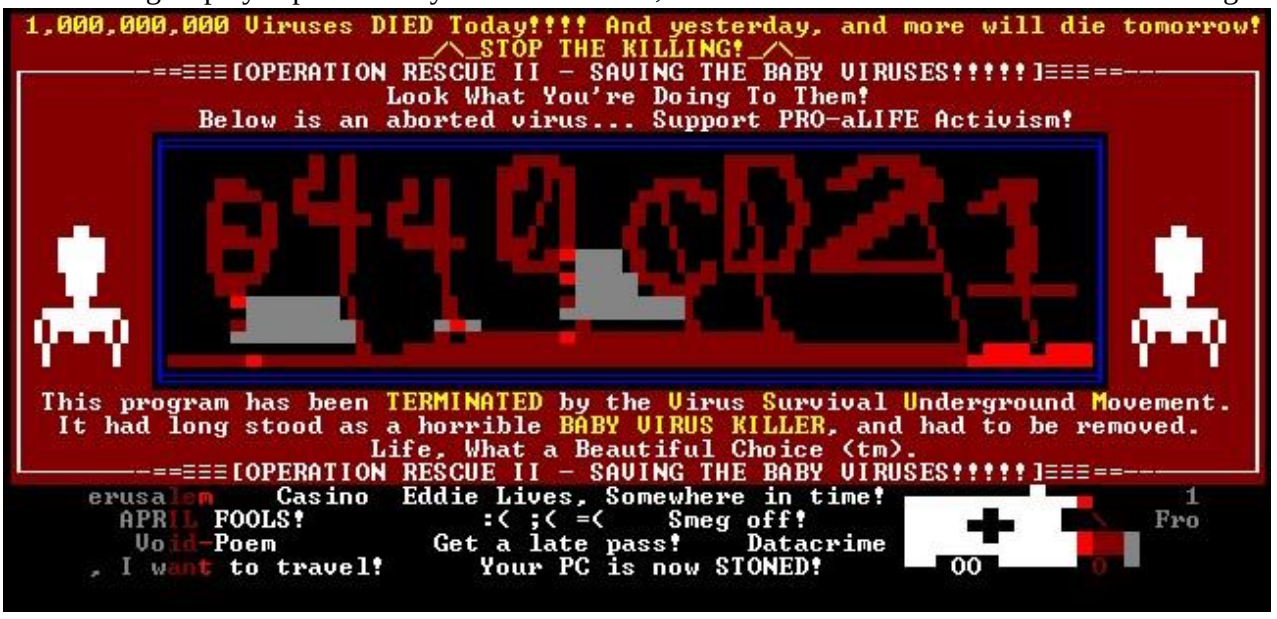


Figure 5: On-screen message shown by the Rescue virus

Interactive activations

Some viruses stop the PC and demand the user of the PC to do something. For example, the Joshi virus will stop the machine on January 5th and demand the user to type "Happy Birthday Joshi" before the machine continues working, and the Casino virus, which will put the user to gamble in a Jackpot game with the stakes being the contents of his hard drive.

Some viruses will demand more effort from the user. The YAM.Math virus will occasionally stop the machine when a program is run and display simple addition or subtraction questions. Execution of the program is denied unless the correct answer is given by the user.

Another similar virus called Peter_II displays the following message:

```
Good morning,EVERYbody,I am PETER II
Do not turn off the power, or you will lost all of the data in Hardisk!!! WAIT
for 1 MINUTES,please...
```

After this, the virus encrypts the whole hard drive. After that, it continues by displaying the following questionnaire:

```
Ok.If you give the right answer to the following questions,
I will save your HD:
```

```
A. Who has sung the song called "I`ll be there" ?
          1.Mariah Carey  2.The Escape Club  3.The Jackson five  4.All  (1-4):
B. What is Phil Collins ?
          1.A singer  2.A drummer  3.A producer  4.Above all(1-4):
C. Who has the MOST TOP 10 singles in 1980`s ?
          1.Michael Jackson  2.Phil Collins (featuring Genesis)
          3.Madonna  4.Whitney Houston(1-4):
```

If the user gives correct answers to every question, the virus decrypts the hard disk and displays the following message:

```
CONGRATULATIONS !!! YOU successfully pass the quiz!
AND NOW RECOVERING YOUR HARDISK ......
```

The user can then continue using the computer normally. However, if incorrect answers are given, the virus will not decrypt the hard disk. Instead, it will just display the following message:

```
Sorry!Go to Hell.Clousy man!
```

Correct answers to the questions are left as an exercise to the reader.

Finally, some viruses invite the user to play a game on the PC. An example of this is the Playgame virus, which displays a simple race game.

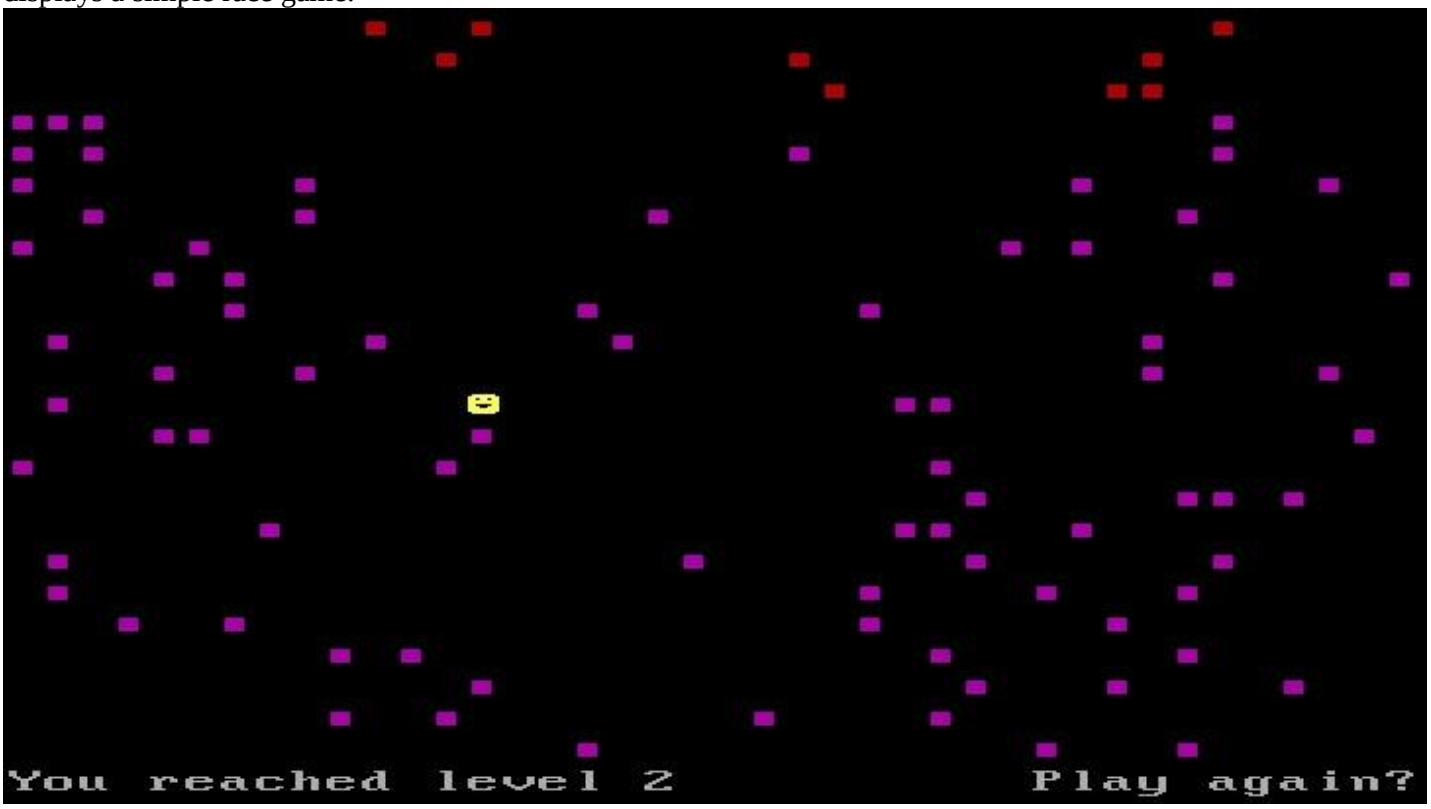


Figure 6: Playfield displayed by the Playgame virus

Fake hardware failures

Some viruses try to simulate a hardware failure. For example, the Azusa virus disables the serial and parallel ports of the machine and Parity_Boot makes it appear as if the machine has faulty memory chips.

In the worst case, user replaces components of his system before he realizes that there is physically nothing wrong in the machine.

Practical jokes

Several viruses play practical jokes with the user. The Jerusalem.Fu_Manchu virus observes what the user is typing, and inserts comments when keywords such as 'Thatcher', 'Reagan' or 'Waldheim' are entered.

The Armagedon virus from Greece checks if a modem is connected to the machine and tries to call out to the local time service when the time is between 5am and 6am. The Fone.688 does a similar thing, except that it calls to X-rated 1-900 phone services in the USA.

Haifa virus inserts two text lines in the middle of DOC files when they are accessed:

```
OOPS!  Hope I didn't ruin anything!!!
Well, nobody reads those stupied DOCS anyway!
```

Similarly, the WordMacro/Nuclear virus adds comments against French nuclear testing in Pacific to the end of documents when they are printed or faxed from Microsoft Word.

Denial of service

Some viruses just try to make the machine unusable. Viruses which overwrite hard drives obviously do this, but good backups provide a fast way to recover from them. Then there are viruses like Monica, which sets the BIOS boot-up password function on (if the BIOS supports this) and sets the password to 'monica'. As there is no way for the user to guess the password, the machine is effectively rendered unusable until CMOS battery is disconnected. In future we will see Flash BIOS -aware viruses, which will cause even more difficult problems.

Triggers

There are several different trigger events, which viruses use to decide when to activate. These include:

- Date or time
- Generation counter of the virus
- Number of keypresses on the keyboard
- Amount of free space on the hard drive
- Amount of minutes the machine has been idle Name
- of an executed program

Basically any event it the PC can be used as a trigger by a virus.

Why it is important to know what a virus does

When you have a real infection in your hands, you probably want to know what the virus in question does. Actually, this information can be crucial, especially in the case of viruses which do gradual corruption.

A virus like One_Half also demonstrates the importance of knowing what a virus does before starting to disinfect it: One_Half is a full stealth virus, which gradually encrypts the contents of the hard drive. The encryption key and counter is kept inside the virus body in the boot sector. If One_Half is removed by overwriting the virus code in the boot sector with a clean one, the components required to decrypt the drive are lost, and the encryption will not be hidden anymore by the stealth routines of the virus. In effect, data on the hard drive is lost due to disinfecting the virus.

Information sources

It would be great to have a single source of information which would describe every computer virus, complete with it's propagation methods and activation routines. Unfortunately, no such reference exists, and will never exist. There are just too many viruses out there and new ones are created too fast.

Today, when several new viruses are found every day, virus experts have limited time to spend with analyzing any single virus. Virus analysis systems are automated as much as possible, and a virus typically only gets a cursory look - which is usually enough to add detection, identification and disinfection. Such analysis will not reveal any special features the virus may contain. For this reason, no anti-virus vendor can provide a complete reference guide for all viruses their product detects.

There are, however, some sources which are useful. These sources typically cover only the most common or otherwise special viruses, but this is usually enough.

These sources include:

- The virus description database of F-PROT Professional antivirus package. Do note that this is not the same as in the shareware version of F-PROT. The emphasis of descriptions are on viruses which are known to be in the wild.
- Virus description service at F-Secure Ltd's Internet World-Wide Web server at http://www.datafellows.com/. This database is based on the same information as in F-PROT Professional antivirus program, but it is constantly updated, and features the possibility to do free searches and browse through the latest updates. This is a free service, which is currently serving several hundreds of description requests every day.
- AVP Virus Encyclopedia. This Russian freeware DOS hypertext program has probably the largest single set of descriptions; there are several thousand viruses described here. Some of the descriptions even include a demo of the actual activation routine. The only problem with AVPVE is that at times the language is a bit difficult to understand - English with Russian accent.
- CARObase is a joint effort by the Computer Antivirus Researcher's Organization to gather technical descriptions of viruses. It currently contains only about 120 descriptions, but the detail and accuracy of those are excellent.
- VTC Computer Virus Catalog is already getting outdated, but it still contains excellent descriptions of over 200 PC viruses, and also covers other platforms, such as Amiga, Atari or Unix.

There are other sources available as well. The popular VSUM Virus Summary can not be strongly recommended due the several errors it contains, but it can be useful as a cross-reference tool when trying to locate a virus which is known by several alias names.

Antivirus programs such as McAfee SCAN, Thunderbyte Antivirus or Dr. Solomon's Antivirus Toolkit do contain brief descriptions, but these are all based on a few basic attributes for each virus, so they don't have details on activation routines. S&S International has also published a book called Virus Encyclopaedia, which has more detailed information.

Future

Worst possible activation routine

What would be the worst possible activation routine that could exist in a virus? Obviously it is not a virus which would just destroy data - incidents like that are relatively unimportant if good backup practices are kept, and gradually corrupting viruses can be found with good integrity checking. But how about a virus which would breach the security and privacy of your system?

The rising popularity of the Internet does indeed bring new risks. Considering the widespread use of the Internet and TCP/IP connections for normal PC workstations, and the amount of Winsock installations in use, several scary visions can be thought of. How about a virus which would open a NNTP connection from your machine and spam every newsgroup in the Usenet news hierarchy, masquerading as you? Or send rude e-mail messages to all addresses found from your e-mail package's alias database. In some e-mail systems, a virus could even use the authentication features to positively identify that the sender is actually you.

Even worse, how about a virus which would wait until a machine with a Winsock connection has been idle for some hours, open a ftp connection to some large public ftp server which has an open area for incoming files and uploads all DOC, XLS and DBF files found from your hard drive - or your network? If the virus were widespread, Internet surfers would make interesting discoveries while going through the confidential files of hundreds or thousands of unsuspecting users.

It's difficult to think of a worse activation routine for a virus. Unfortunately, we will probably see something like this in the future.

Conclusions

There is a wide variety of activation routines found in the current viruses. After all, only the imagination is the limit. There are some scary possibilities which future viruses will probably use in their activation routines to make the life of a computer user miserable.

It's still good to keep in mind that although flashy viruses get all the media attention, most viruses do nothing but replicate.

BIOGRAPHY

Mikko Hypponen is a graduate from the Institute of Information Technology of Helsinki, Finland. He entered the anti-virus field when he switched from being a database developer to a full-time virus specialist in 1990.

Hypponen works as the Support Manager at F-Secure Ltd.

Born in 1969, Hyppönen is currently the youngest member in CARO (Computer Antivirus Researchers Organization).
