The Bulgarian and Soviet Virus Factories

Vesselin Bontchev, Director
Laboratory of Computer Virology
Bulgarian Academy of Sciences, Sofia, Bulgaria

It is now well known that Bulgaria is leader in computer virus production and the USSR is following closely. This paper tries to answer the main questions: Who makes viruses there, What viruses are made, and Why this is done. It also underlines the impact of this process on the West, as well as on the national software industry.

1 How the story began.

Just three years ago there were no computer viruses in Bulgaria. After all, these were things that can happen only in the capitalist countries. They were first mentioned in the April issue of the Bulgarian computer magazine *"Komputar za vas"* ("Computer for you") [KV88] in a paper, translated from the German magazine *"Chip"* [Chip]. Soon after that, the same Bulgarian magazine published an article [KV89], explaining why computer viruses cannot be dangerous. The arguments presented were, in general, correct, but the author had completely missed the fact that the majority of PC users are not experienced programmers.

A few months later, in the fall of the same year, two men came in the editor's office of the magazine and claimed that they have found a computer virus. Careful examination showed that it was the `Vienna` virus.

At that time the computer virus was a completely new idea for us. To make a computer program, whose performance resembles a live being, is able to replicate and to move from computer to computer even against the will of the user, seemed extremely exciting.

The fact that "it can be done" and that even "it had been done" spread in our country like wildfire. Soon hackers obtained a copy of the virus and began to hack it. It was noticed that the program contains no "black magic" and that it was even quite sloppily written. Soon new, home–made and improved versions appeared. Some of them were produced just by assembling the disassembly of the virus using a better optimizing assembler. Some were optimized by hand. As a result, now there are several versions of this virus, that were created in Bulgaria — versions with infective lengths of 627, 623, 622, 435, 367, 353 and even 348 bytes. The virus has been made almost two times shorter (its original infective length is 648 bytes) without any loss of functionality.

This virus was the first case. Soon after that, we were "visited" by the `Cascade` and the `Ping Pong` viruses. The later was the first boot–sector virus and proved that this special area, present on every diskette can be used as a virus carrier, too. All these three viruses were probably imported with illegal copies of pirated programs.

2 Who, What & Why.

2.1 The first Bulgarian virus.

At that time both known viruses that infected files (`Vienna` and `Cascade`) infected only COM files. This made me believe that the infection of EXE files was much more difficult. Unfortunately, I made the mistake by telling my opinion to a friend of mine. Let's call him "V.B." for privacy reasons.[1]

The challenge was taken immediately and soon after that I received a simple virus that was able to infect only EXE files. It is now known to the world under the name of `Old Yankee`. The reason for this is that when the virus infects a new file, it plays the "Yankee Doodle" melody.

The virus itself was quite trivial. Its only feature was its ability to infect EXE files. The author of this virus even distributed its source code (or, more exactly, the source code of the program that releases it). Nevertheless, the virus did not spread very widely and even had not been modified a lot. Only a few sites reported to be infected by it. Probably the reason for this was the fact, that the virus was non–resident and that it infected files only on the current drive. So the only possibility to get infected by it was to copy an infected file from one computer to another.

When the puzzle of creating a virus which is able to infect EXE files was solved, V.B. lost his interest in this field and didn't write any other viruses. As far as I know, he currently works in real–time signal processing.

2.2 The T.P. case.

The second Bulgarian virus–writer, T.P., caused much more trouble. When he first heard the idea about a self–replicating program, he was very interested, decided to write his own virus, and he succeeded. Then he tried to implement a virus protection scheme and succeeded again. The next move was to improve his virus to bypass his own virus protection, then to improve the virus protection and so on. That is why there are currently about 50 different versions of his viruses.

Unfortunately, several of them (about a dozen) were quite "successful." They spread world–wide. There are reports about them from all countries of the former Eastern block, as well as from the USA and West Europe.

Earlier versions of these `TP` viruses are known under the name `VACSINA`, because they contain such a string. In fact, this is the name of the virus author's virus protection program. It is implemented as a device driver with this name. The virus merely tries to open a file with this name, which means "Hey, it's me, let me pass."

The latest versions of the virus are best known under the name `Yankee Doodle`, because they play this tune. The conditions on which the tune is played are different with the different versions of the virus — for instance when the user tries to reboot the system, or when the system timer reaches 5 p.m.

[1] *These are the initials of his true name. It will be the same with the other virus writers that I shall mention. Please note, that while I have the same initials (and even his full name resembles mine), we are two different persons.*

All TP viruses are strictly non–destructive. Their author payed particular attention not to destroy any data. For instance, the virus does not infect EXE files for which the true file length and the length of the loadable part as it is present in the EXE header, are not equal. As far as I know, no other virus that is able to infect EXE files works this way.

Also, the virus does not try to bypass the resident programs that have intercepted INT 13h, therefore it takes the risk to be detected by most virus activities monitoring software. The author of the virus obviously could circumvent it — for instance it uses a clever technique, now known as "interrupt tracing" to bypass all programs that have hooked INT 21h. The only reason for not bypassing INT 13h as well, is that this would also bypass all disk casheing programs, thus it could cause damage.

Of course, the fact that the virus is not intentionally destructive does not mean that it does not cause any damage. There are several reports of incompatibilities with other software; or of panicking users, that have formatted their disks; or, at least, damage caused by time loss, denial of computer services, or expenses removing the virus. It is well known, that *"there ain't no such thing as a good virus."*

The TP viruses were not spread intentionally; the cause could be called "criminal negligence." The computer used by T.P. to develope his viruses was also shared by several other people. This is common practice in Bulgaria, where not everyone can have a really "personal" computer to work with. T.P. warned the other users that he is writing viruses, but at this time computer viruses were a completely new idea, so nobody took the warning seriously. Since T.P. didn't bother to clean up after himself, these users got, of course, infected. Unintentionally, they spread the infection further.

When asked about the reason of writing viruses, T.P. replied that he did this in order to try several new ideas; to better learn the operating system and several programming tricks. He is not interested in this field any more — he has stopped writing viruses about two years ago.

2.3 The Dark Avenger.

In the spring of 1989 a new virus appeared in Bulgaria. It was obviously "home–made" and just to remove any doubts about it, there was a string in it, saying `"This program was written in the city of Sofia (C) 1988-89 Dark Avenger."`

The virus was incredibly infectious — when it was in memory, it was sufficient to copy or just to open a file to get it infected. When the user felt that there is a virus in his/her system and, without booting from a non–infected write–protected system diskette, ran an anti–virus program which wasn't aware of this new virus, he usually got all his/her executable files infected.

The idea of infecting a file when it is opened was new and really "successful." Now such viruses are called "fast infectors." This strategy helped the virus to spread world–wide. There are reports from all European countries, from the USA, the USSR, even from Thailand and Mongolia.

On the top of this, the virus was very dangerously destructive. On each 16th run of an infected program, it overwrote a sector on a random place of the disk, thus possibly destroying the file or directory that contained this sector. The contents of the overwritten sector was the first 512 bytes of the virus body, so even after the system has been cleaned up, there were files, containing a string "Eddie lives...somewhere in time!" This was causing much more damage than if the virus was just formatting the hard disk, since the destruction was very unnoticable and when the user eventually discovered it, his backups probably already contained corrupted data.

Soon after that, other clever viruses began to appear. Almost all of them were very destructive. Several contained completely new ideas. Now this person (we still cannot identify him exactly) is believed to be the author of the following viruses:

> Dark Avenger, V2000 (two variants), V2100 (two variants), 651, Diamond (two variants), Nomenklatura, 512 (six variants), 800, 1226, Proud, Evil, Phoenix, Anthrax, Leech...

Dark Avenger has several times attacked some anti–virus researchers personally. The V2000/V2100 viruses claim to be written by "Vesselin Bontchev" and in fact hang the computer when any program, containing this string is run. A slightly modified variant of V2100 (V2100-B) has been used to trojanize version 66 of John McAfee's package VIRUSCAN.

There are reports that Dark Avenger has called several bulletin board systems in Europe and has uploaded there viruses. The reports come from the UK, Sweden, the Netherlands, Greece... Sometimes the viruses uploaded there are unknown in Bulgaria (Nomenklatura, Anthrax). But they are obviously made in our country — they contain messages in Cyrillic. Sometimes Dark Avenger uploads a Trojan program that spreads the virus — not just an infected program. This makes the detection of the source of infection more difficult.

One particular case is when he has uploaded a file called UScan, which, when run, claims to be the "universal virus scanner," written by Vesselin Bontchev. Even the person who has uploaded it, has logged under the name "Vesselin Bontchev." In fact, the program just infected all scanned files with the Anthrax virus.

While the other Bulgarian virus writers seem to be just irresponsible or with childish mentality, the Dark Avenger can be classified as a "technopath." He is a regular user of several Bulgarian bulletin board systems, so one can easily exchange e-mail messages with him. When asked why his viruses are destructive, he replied that "destroying data is a pleasure" and that he "just loves to destroy other people's work."

Unfortunately, no measures can be taken against him in Bulgaria. Since there is no law for information protection, his activities are not illegal there. He can be easily caught by tapping the phones of the BBSes that he uses, but the law enforcement authorities cannot take such measures, since there is no evidence of illegal activities. Alas, he knows this perfectly.

2.4 Lubo & Ian.

Some of the Dark Avenger's viruses proved to be very "successful" and caused real epidemics. That is why they were often imitated by other virus writers, that had no imagination to design their own virus, but were jealous of Dark Avenger's fame. So they just disassembled his viruses (usually the first one) and used parts of it — sometimes without even understanding their purpose. Such is the case with the Murphy viruses.

According to a string in them, they are written by "Lubo & Ian, USM Laboratory, Sofia." These people do exist and they have used their real names. "Lubo" has even been several times interviewed by newspaper's reporters.

They claim that the virus was written for vengeance. They have done some important work for their boss and the latter refused to pay them. That is why they developed the virus in one night and released it. The fact that the virus will spread outside the laboratory just didn't come to their minds. However, this does not explain the developing of the other versions of the same virus (there are at least four variants). Nevertheless, it proves one more time that it is better (and safer, too) to pay the good programmers well...

Besides `Murphy`, these two virus writers have created another virus, called `Sentinel` (5 variants). The only unusual thing with this virus is that it is written in a high–level programming language (Turbo PASCAL), but is not an overwriting or a companion virus as most HLL viruses are. It is able to infect COM and EXE files by appending itself to them and by preserving their full functionality. It is also memory resident, hides the file length increase when the user issues the DIR command, and even mutates.

2.5 The virus writer from Plovdiv.

This man, P.D., claimed that he has written viruses "for fun" and only "for himself" and that he "never releases them." Unfortunately, at least two of them have "escaped" by accident. These are the `AntiPascal-605` and the `Terror` viruses. Especially the latter is extremely virulent and caused a large epidemic in Bulgaria.

P.D. was very sorry for that and submitted examples of all his viruses to the anti–virus researchers so that the respective anti–virus programs be developed — just in case some of these viruses escapes too. These viruses turned out to be quite a few, ranging from extremely stupid to very sophisticated. Here are some of them:

```
XBoot, AntiPascal (5 variants), Tiny (11 variants), Minimal-45,
Terror, Dark Lord, Nina, Gergana, Happy New Year (2 variants), Int 13.
```

P.D. claims that the `Dark Lord` virus (a minor `Terror` variant) is not written by him. The `Tiny` family has nothing to do with the Danish `Tiny` virus (the 163–byte variant of the `Kennedy` virus), and, as well as the `Minimal-45` virus, are written with the only purpose to make the shortest virus in the world.

Now P.D. is not writing viruses any more — because "it is so easy, that it is not interesting," according to his own words. He is currently writing anti–virus programs — and rather good ones.

2.6 The two guys from Varna.

They are two pupils (V.P. and S.K.) from the Mathematical High School in Varna (a town on the Black Sea). They have developed several viruses and continue to do so, producing more and more sophisticated ones. Furthermore, they intentionally spread their viruses, usually releasing them on the school's computers or in the Technical University in Varna. When asked why they write and release viruses, they reply "because it's so interesting!"

The viruses written by them are: `MG` (5 variants), `Shake` (5 variants), `Dir` and `Dir II`. All of them are memory resident and infect files when the `DIR` command is performed.

The last one is an extremely virulent and sophisticated virus — as sophisticated, as The Number of the Beast. It is also a completely new type of virus — it infects nether boot sectors, nor files. Instead, it infects the file system as a whole, changing the information in the directory entries, so that each file seems to begin with the virus.

There is a counter of the number of infected systems in the virus body. There is evidence that V.P. and S.K. collect infected files, copy the contents of the counter and then draw curves of the spread of infection, checking the normal distribution law. They are doing this "for fun."

2.7 W.T.'s case.

W.T. is a virus writer from Sofia, who has written two viruses — WWT (2 variants) and Darth Vader (4 variants). According to his own words, he has done so to test a new idea and to gain access to the Virus eXchange BBS (see below).

The new idea consisted of a virus (Darth Vader) that does not increase file lengths, because it searches for unused holes, filled with zeros, and writes itself there. Also, the virus does not perform any write operations. Instead, it just waits for a COM file to be written to by DOS and modifies the file's image in memory just before the write operation is performed.

W.T. does not write viruses any more, but he is still extremely interested in this field. He is collecting sophisticated viruses and disassembles them, looking for clever ideas.

2.8 The Naughty Hacker.

This virus writer, M.H., is a pupil and also lives in Sofia. He has written several viruses, most of which contain the string "Naughty Hacker" in their body. All of them are non– destructive, but contain different video effects — from display desynchronization to a bouncing ball.

Currently, at least 8 different variants are isolated, but it is believed that even more exist and are spread in the wild. Also, it is believed that M.H. continues to produce viruses. As usual, he is doing so "because it is interesting" and "for fun."

He is also the author of three simple boot sector viruses (BootHorse and two others that are still unnamed).

2.9 Other known virus writers.

The persons listed above are the major Bulgarian virus producers. However, they are not alone. Several other people in Bulgaria have written at least one virus (sometimes more). In fact, making a virus is currently considered there a kind of sport, or a practical joke, or means of self–establishment.

Some of these virus writers have supplied their creations directly to the anti–virus researchers, as if they are waiting for a reward. This happens quite often — probably they expect that the anti–virus researcher, as the best qualified person, will evaluate their creation better. Sometimes the fact that their virus becomes known, is described, and is included in the best anti–virus programs is sufficient for these people and they don't bother to really spread their virus in the wild. So, probably the main reason for these people to produce viruses is the seek of glory, fame, and self–establishment.

Such known Bulgarian virus writers (with the respective names of their viruses given in parentheses) are V.D. from Pleven (`Micro-128`), A.S. and R.D. from Mihajlovgrad (`V123`), I.D. from Trojan (`Mutant`, `V127`, `V270x`), K.D. from Tutrakan (`Boys`, `Warrier`, `Warrior`, `Dream`), and others.

2.10 Unknown Bulgarian virus writers.

Of course, there are also other virus writers, that are not known to the author of this paper. Sometimes it is possible to determine the town where the viruses were developed — usually due to an appropriate string in the virus body, or because the virus wasn't found elsewhere. Some of the viruses are very simple, others are quite sophisticated. Here are examples of such viruses.

- The `Kamikaze` virus has been detected only in the Institute of Mathematics at the Bulgarian Academy of Sciences, Sofia and is probably made there;
- The `Rat` virus, made in Sofia, as it is written in its body;
- The `VFSI` (`Happy Day`) virus has been developed in the Higher Institute of Finances and Economics in Svishtov (a small town on the Danube) by an unknown programmer;
- The `Destructor` virus, probably made in Plovdiv, where it has been first detected;
- The `Parity` virus, probably written in the Technical University, Sofia, since it has not been detected elsewhere;
- The `Tony` file and boot sector viruses, probably created in Plovdiv where they have been first detected;
- The `ETC` virus, detected only in Sofia;
- The `1963` virus, a quite sophisticated one, probably made in the Sofia University;
- The `Justice` virus.

2.11 The Virus eXchange BBS.

About a year ago, the virus writing in Bulgaria entered a new phase. The virus writers began to organize themselves. The first step was the creation of a specialized bulletin board system (BBS), dedicated to virus exchange. The Virus eXchange BBS.

It's system operator (SysOp), T.T. is a student of computer science in the Sofia University. He has established the BBS in his own home. On this BBS, there are two major kinds of files — anti–virus programs and viruses. The anti–virus programs can be downloaded freely.

In order to get access to the virus area, one has to upload there a new virus. However, anyone who uploads a new virus, gets access to the whole virus collection. S/He could then download every virus that is already available, or even all of them. No questions are asked — for instance for what reason s/he might need these viruses.

Furthermore, the SysOp takes no steps to verify the identity of his users. They are allowed to use fake names and are even encouraged to do so. Dark Avenger and W.T., between them are, the most active users, but there are also names like George Bush from New York, Saddam Hussein from Baghdad, Ozzy Ozburn and others.

Since this BBS has already a large collection of computer viruses (about 300), it is quite difficult to find a new virus for it. If one wants badly to get access to the virus area, it is much simpler to write a new virus, instead of trying to find a new one. That is exactly what W.T. did. Therefore, this BBS encourages virus writing.

Furthermore, on this BBS there are all kinds of viruses — some of them as `1260`, `V2P6Z`, `Flip`, `Whale` are considered as extremely dangerous, since they are using several new ideas and clever tricks, which makes them very difficult to be recognized and removed from the infected files. And the Virus eXchange BBS policy makes all these viruses freely available to any hacker that bothers to download them. This will, undoubtedly, lead to the creation of more and more such "difficult" viruses in the near future.

The free availability of live viruses has already given its bitter fruits. It helped to viruses created far away from Bulgaria and not widely spread, to cause epidemics in our country. Such was the case of the `DataLock` virus. It has been created in California, USA and uploaded to the Virus eXchange BBS. A few weeks later it was detected in the Technical University, Sofia. Probably one of the users of the BBS had downloaded it from there and spread it "for fun." In the similar way the `Internal`, `Typo` and `1575` viruses entered our country.

But the free availability of known live viruses is not the most dangerous thing. After all, since they are already known, there already exist programs to detect and probably to remove them. Much more dangerous is the free availability on this BBS of virus source code! Indeed, original source code or well commented virus disassemblies of several viruses are freely available on the Virus eXchange BBS — just as any other live virus. To name a few, there are:

```
Dark Avenger, Old Yankee, Diamond, Amstrad, Hymn, MLTI830, Murphy,
Magnitogorsk, Icelandic, Mix1, Stoned, Jerusalem, Datacrime, Burger,
Armagedon, Oropax, Darth Vader, Naughty Hacker, 512, Vienna, 4096,
Fish#6, Ping Pong, Black Jec, WWT, MG, TSD, BootHorse, Bad Boy,
Leech...
```

Most of them are perfectly assemblable sources.

The publishing of virus source code has proven to be the most dangerous thing in this field. The `Vienna`, `Jerusalem`, `Cascade` and `Amstrad` viruses are the best examples. Their source code has been made publicly available, which led to the creation of scores of new variants of these viruses. The known variants of only these four viruses are about 20 % of all known viruses, which means more than a hundred variants. One can imagine the consequences of making publicly available the source code of all the viruses listed above. In less than a year we probably will be submerged by thousands new variants...

In fact, this process has already begun. The `HIV`, `Migram`, `Kamasya`, `Cemetery` and `Antichrist` viruses have been obviously created by someone who had access to the source of the `Murphy` virus. The `Enigma` virus is clearly based on the `Old Yankee` code. There have been reports about infections with these viruses in one Italian school and an Italian virus writer, known as Cracker Jack is a user of Virus eXchange...

The damage caused by this BBS alone to the rest of the world is big enough. But this is not all. Since possession of "viral knowledge" (i.e., live viruses, virus source code) has always tempted hackers and since the legitimate anti–virus researchers usually exchange such things only between themselves and in a very restricted manner, it is not surprising that similar "virus boards" began to pop up around the world. There are currently such BBSes in the USA, Germany, Italy, Sweden, Czechoslovakia, the UK and the Soviet Union. Stopping their activities is very difficult in legal terms, because the possession, storage or willful downloading of computer viruses usually is not considered as a criminal offence. And it shouldn't be — otherwise the anti–virus researchers themselves will not have a way to exchange virus samples to work with.

The creation of a virus–oriented BBS, the system operator of which supported the writing, spreading and exchanging of virus code didn't go unnoticed in Bulgaria. Almost all virus writers have obtained a modem (a not very easy thing in Bulgaria) and contacted it. Afterwards, they began to contact each other by means of electronic messages on this BBS. They have even created a specialized local conference (local for Bulgaria), in order to keep in touch and to exchange ideas how to write clever viruses. Therefore, they began to organize themselves — a thing that cannot be said about the anti–virus research community in all countries...

3 New ideas.

As it can be seen from the examples above, the whole of Bulgaria has turned into some kind of computer virus developing laboratory, where any capable (or not so capable) pupil/student/programmer is tempted to write his own virus and to test it in the wild. It is not therefore unusual that several completely new ideas were first developed in our country. I shall try to enumerate here some (only the most important) of them.

- The interrupt tracing technique, capable of finding the original handler (in DOS or BIOS) of any interrupt vector, has been first implemented in the `Yankee Doodle` (`TP`) viruses. Later other viruses in the world began to use it (`4096`, `Naughty Hacker`).

- The "fast infectors" — viruses that infect on file opening or even on any file operation were first developed in Bulgaria. The first such virus was the `Dark Avenger`. Now there are a lot of fast infectors. One of them — `1963` — even infects on file deletion.

- The "semi–stealth" viruses — viruses that hide the increasing of the size of the infected files (the `651` virus) or that remove them from the inflected files when one loads them with a debugger (`Yankee Doodle`) both are viruses, made in our country.

- Hiding the true file length usually causes problems, because `CHKDSK` is able to detect the difference between the disk space marked as used in the FAT and the reported file length. Only two Bulgarian viruses in the world are able to handle this problem — `Diamond` and `V2100`.

- The first really "stealth" file infector — the 512 virus was Bulgarian. It is true however, that the idea has been discovered independently almost at the same time in other parts of the world (the 4096 virus from Israel).

- The only known stealth parasitic virus, which "stealthy" features go down to the BIOS level (i.e., it cannot be detected if active in memory even if the infected file is read at sector and not at file level) is the Bulgarian Int13 virus.

- One of the first multi–partite viruses (viruses that are able to infect both files and boot sectors) — the Anthrax virus, has been developed in Bulgaria. It is true, however, that similar ideas can be noticed in the 4096 and GhostBalls viruses, which are developed much earlier. Also, other multi–partite viruses (Virus-101, V-1, Flip, Invader) were created independently almost at the same time (and even earlier) in other parts of the world.

- The idea first used in the Lehigh virus — to place the virus body in an unused part of the file COMMAND.COM has been further developed by several Bulgarian viruses. They all can infect any COM or EXE file (unlike the Lehigh virus) in the usual way, but when they are infecting the command interpreter, they place themselves in an area filled with zeros at the end of the file and thus in this case they do not increase its length. Such viruses are Terror, Naughty Hacker and others.

- The method, mentioned above has been developed even further by other Bulgarian viruses. They have noticed that any sufficiently large area of zeros in any file (not just COMMAND.COM) can be used to hide the virus body. The viruses that use this method are again of Bulgarian origin — Proud, Evil, Phoenix, Rat, Darth Vader... The latter even does not write to the infected files — it leaves this task to DOS. And the Rat virus hides itself into the unused part of the EXE file headers.

- One of the extremely mutating viruses is the Dark Avenger's virus Leech. It can exist in more than 4.5 billion variants. It is true, however, that this is neither the first entirely mutating virus (1260 being the first), nor it has the most flexible mutating mechanism (it is much simpler than V2P6Z).

- A completely new type of computer virus (Dir II) has been developed by two Bulgarian pupils. This virus does not infect neither files, nor boot sectors. Instead, it infects file systems as a whole, or more exactly — directory entries.

- Different tricks to get control without directly hooking the INT 21h vector were developed by several Bulgarian virus writers. The Terror virus places a JMP instruction to its body in the original INT 21h handler in DOS. The viruses from the Phoenix family (800, 1226, Proud, Evil, Phoenix) hook an interrupt that is called by DOS on every file–related function (INT 2Ah, AH=82h). The Dir II virus patches itself in the chain of DOS disk device drivers.

- The first virus, that is able to infect device drivers (SYS files only), is, of course, Bulgarian. This is the Happy New Year (1600) virus.

- The first fully functional parasitic virus, written entirely in a high level language (Turbo PASCAL) is the Bulgarian virus `Sentinel`.

- The Bulgarian virus `Anthrax` is the first virus that is resident in memory only temporary. It removes itself from there after it has infected the first file and then acts as a non–resident virus.

- The shortest memory resident virus in the IBM PC world — only 128 bytes — is again developed in Bulgaria. There are reports about a 108–byte resident virus, also from there, but they are unconfirmed yet.

- The shortest virus in the IBM PC world — only 45 bytes long, is the Bulgarian virus `Minimal-45`. It seems possible, however, to shorten it even further — up to 31 bytes, with a big loss of reliability.

4 Why so many viruses are created in Bulgaria.

Computer viruses are created in all parts of the world, not only in Bulgaria. However, the portion of them that are created in our country is extremely high. Therefore, in the whole world there exist preconditions that make virus writing tempting, but in Bulgaria there exist specific conditions as well.

4.1 Specific reasons for virus writing in Bulgaria.

4.1.1

The first, and most important of all is the *existence of a huge army of young and extremely qualified people, computer wizards, that are not actively involved in the economic life.*

The computerization in Bulgaria began without economical reasons. Since our country was a socialist one, its economics was of administrative type. The economics didn't need to be computerized. In fact, computers and planned economics are quite incompatible — computers help you to produce more in less time and with less effort and money, while the goal of a manager in a planned economics is to fulfil the plan exactly as it is given — for no more and no less time, and with no more and no less money. However, the communist party leaders in Bulgaria decided that we should computerize — mainly to be able to supply computers to the Soviet Union and circumvent the embargo.

While computerization in itself is not a bad thing, we made a very severe mistake. Bulgarian economics was very weak (now it is even weaker), but we had quite a lot skilled people. Therefore, we should not have tried to produce hardware while we had good chances in the software industry, where mainly "brainware" is required. However, Bulgaria did just the opposite. Instead of buying the hardware, we began to produce it (mainly illegal Apple and IBM clones). Instead of producing our own software and to try to sell it in the West, we began to steal Western computer programs, to change some copyright notices in them, and to re–sell them (mainly in Bulgaria, in the Soviet Union, and in the other countries of the former Eastern block).

At that time most Western software was copy protected. Instead of training our skilled people in writing their own programs, we began to train them to break copy protection schemes. And they achieved great success in this field. The Bulgarian hackers are maybe the best in cracking copy protected programs. Besides, they had no real hope in making and selling their own programs, since, due to the total lack of copyright law on computer software, it was impossible to sell more than two or three examples of a computer program in Bulgaria. The rest were copied.

Since the introduction of computers in the Bulgarian offices was not a natural process, but due to an administrative order, very often these computers were not used — they were only considered as an object of prestige. Very often on the desk of a company director, near the phone, stood a personal computer. The director himself almost never used the computer — however sometimes his/her children came to the office to use it — to play games or to investigate its internals.

While the price of personal computers in Bulgaria was too high to permit a private person to have his/her own computer, it was a common practice to use the computer at the office for personal reasons.

At the same time, the computer education was very widely introduced in Bulgaria. Everyone was educated in this field — from children in the kindergartens to old teachers that had just a few years until pension. Since this kind of science is better comprehended by younger brains, it is no wonder that the people, who became most skilled in this field, were very young.

Very young and not morally grown–up. We spent a lot of effort teaching these people how to program, but forgot to educate them in computer ethics. Besides, the lack of respect to the others' work is a common problem in the socialist societies.

4.1.2

The second main reason is the *wide–spread practice of software pirating (which was, in fact, a kind of state policy) and the very low payment of the average programmers.*

As was mentioned above, Bulgaria took the wrong decision in producing computers and stealing programs. There is still no copyright law, concerning computer software there. Because of this, the software piracy was an extremely widespread practice. In fact, almost all software products used were illegal copies. Most people using them have never seen the original diskettes or original documentation. Very often there was no documentation at all.

Since all kinds of programs (from games to desktop publishing systems) were copied very often, this greatly helped for the spread of computer viruses.

At the same time, the work of the average programmer was evaluated very low — there were almost no chances to sell his/her software products. Even now, a programmer in Bulgaria is paid 100 to 120 *times* less than the programmer with the same qualification in the USA.

This caused several young people to become embittered against the society that was unable to evaluate them as it should. There is only one step in the transformation of these young people into creators of destructive viruses. Some of them (e.g., the Dark Avenger) took this step.

4.1.3

The third major reason is the *total lack of legislative against creation and willful distribution of computer viruses and against illegal access and modification of computer information in general.*

Because of the lack of copyright laws on computer software, there is no such thing as ownership of computer information in Bulgaria. Therefore, the modification or even the destruction of computer information is not considered a crime — since no one's property is damaged.

The Bulgarian legislature is hopelessly old in this area. Furthermore, even if the appropriate law is accepted in the future, as a punishing law it will not be able to be applied to crimes, committed before it was passed. Therefore, the virus writers still have nothing to fear of.

That is why, the creation of new computer viruses has become some kind of sport or entertainment in Bulgaria.

4.1.4

The next reason is the *very weak organization of the fight against computer viruses in Bulgaria.*

Just now our country is in a very deep economical crisis. We lack funds for everything, including such basic goods as food and gasoline. At the same time, the organization of the virus fight would require money — for the establishment of a network of virus test centers that collect and investigate computer viruses, centers equipped with the best hardware, centers that are able to communicate between themselves and with the other similar centers in the world in an effective way. Such an effective way is the electronic mail system — and Bulgaria still does its first steps in global computer communications.

All this requires a lot of money — money that our government just does not have now.

4.1.5

Another reason is the *incorrect opinion, that the society has on the computer virus problem.*

Still, the victims of a computer virus attack consider themselves as victims of a bad joke, not as victims of a crime.

4.1.6

The least important reason, in my opinion, is the *availability and the easy access to information of a particular kind.*

All kind of tricks how to fool the operating system circulate among the Bulgarian hackers. Some of them are often published in the computer related magazines. As it was mentioned above, there is even a specialized BBS, dedicated to virus spreading and a special (local to Bulgaria) FidoNet echo, dedicated to virus writing.

Not to mention the well–known file `INTERxyy`, published by Ralf Brown from the USA as shareware. It is very popular in Bulgaria, since it contains, carefully described, a huge number of undocumented tricks.

However, this is not a very important reason. Usually those, who have decided to make a virus already know how to do it, or, at least, can figure it out by themselves. They do not need to take an existing virus and to modify it. The proof is the prevalence of original Bulgarian viruses over the variants of known ones, as well as the fact, that many new ideas for virus writing were first invented and implemented in Bulgaria.

4.2 General reasons.

Since viruses are also created in all the other parts of the world, there should be also some general reasons for this. These reasons are, of course, valid for Bulgaria too. Let's see these general reasons.

4.2.1 Wish for glory.

Every programmer dreams that his/her program gets widely spread and used. A lot of very good programmers write and distribute wonderful software packages for free — with the only intention to have more users using their package.

However, for a program to be used, it has to be good enough. And not every programmer is able to make a program so good that the users will widely use it — even for free.

At the same time, computer viruses do spread very widely, regardless and even against the users' will. So, when a virus writer reads in a newspaper that his virus has been discovered at the other end of the world, he feels some kind of perverted pleasure. Some people write viruses just to see their names (or the names of their viruses) published in the newspapers.

This reason has yet another aspect. In the beginning of the virus era, when the idea of the computer virus was very new, only the very good programmers were able to make a virus. It became a common myth that if you can write a virus, you're a great programmer. This myth might have been justified at the beginning, but now it is completely without sense.

Nevertheless, young hackers began to write viruses — just to prove to their friends and to the rest of the world how good programmers they are. Some of them were really unable to invent something original — that's why they just picked a known virus, modified it a bit and released this new mutation. This explains why there are so many variants of the simplest viruses that were first created — `Brain`, `Jerusalem`, `Stoned`, `Vienna`, `Cascade`... A typical example is the Italian virus writer, who calls himself Cracker Jack.

4.2.2 Simple human curiosity.

One has to admit that the idea of a computer program that is able to spread by its own means, to replicate, to hide from the user (who is believed to maintain the computer under full control), and in general to behave as a real live being is really fascinating.

Just simple human curiosity is sufficient to make some people, if they are young and irresponsible enough, to try to make a computer virus. Some of them do succeed. A greater and greater part, if we consider the amount of last reports for new viruses. Some of them claim that they are writing viruses "only for themselves," "only for fun," and that "they do not spread them."

However, it is often impossible to fully control the spread of a "successful" computer virus. The more clever these viruses are, the greater the probability that they will "escape."

There is an idea to teach students how viruses are made — of course in a very strongly restricted environment. Maybe at least for some this will fulfil their curiosity and they will not be tempted to write their own virus. Maybe if we force every computer science student to learn Dr. Fred Cohen's theorems on the computational aspects of computer viruses, if we administer an exam and ask students to design a virus protection scheme or to help a cluster of users, attacked by a computer virus for a course work — well, maybe in this case these students will have more than enough of the computer virus problem and will not want to hear about it any more — least to make their own viruses.

4.2.3 Easy access to information.

Sufficient information, needed to write a virus can be found easily. This information is often even more accessible than in Bulgaria.

The person that wants to write an average virus needs only to dig in the respective manuals — manuals, which are often not available in Bulgaria. However, the usefulness of the easy access to this information is much greater than the damage, caused by the fact that it is used by the virus writers.

4.2.4 Military interests.

It is often rumoured that the superpowers are working on the problem how to use computer viruses to destroy the enemy computers' software. It is even very probable, that in several countries such research is performed. There are reports on this from the USA, France and the USSR.

This is no wonder — it is the right of every military force to investigate any new idea and to consider the possible usefulness and/or threats it might bring to the national defense.

However, it is quite improbable that the computer viruses can be used for this purpose. Just like the live viruses, the computer ones are able to spread only among individuals with very similar immunotype, i.e. — among compatible computers. The most widely used kinds of personal computers are the IBM PC, Macintosh, Amiga and Atari ST. It is therefore no wonder that the vast majority of existing computer viruses are able to infect only these computers.

In the same time, viruses that infect one kind of computer (say, IBM PC), are unable to spread (or even to run) on another (e.g., a Macintosh). They are usually not able to run even on two different operating systems in one and the same computer. Even a different version of the same operating system might cause big problems to a particular computer virus — up to preventing it to work.

The common personal computers are never assigned important tasks in the army. Therefore, even if a virus infects them, and even if it destroys all the data on all such computers, the caused damage will not be of great importance.

Computers that are used for the really important things, such as rocket leading or cannon aiming, are always specialized ones. Their programs are usually hard–coded and only data can be entered in them. It is not possible to insert an infected IBM PC diskette in the computers that control the NORAD system.

At the same time, the computers that control different important devices are usually incompatible even between themselves. Therefore, even if someone writes a virus for a specialized rocket computer, this virus will not be able to infect the computers of a strategic bomber or even these of a rocket of a different system. So, such virus will not spread very much.

And last, but not least, such virus has to be placed somehow in the enemy's computers. Since, as we saw above, it won't be able to spread from one computer to another of a different kind, obviously someone has to insert it in the victim computer. But if you have access to the enemy's computers, you don't need a virus. You can do the same task easier (and often much better) “manually”, or with a Trojan horse or a logic bomb.

4.2.5 Corporate interests.

It is also often speculated that the large software companies and the producers of anti–virus software make or willfully spread computer viruses.

There is some reason behind this. Indeed the fear of viruses can make the user buy only original software (sometimes — quite expensive), and not to use pirated copies, shareware or freeware. At the same time, companies that produce anti–virus software are interested that their products are sold. And they will be, if the user needs anti–virus protection.

However, it is rather improbable, that a software company (whether producing or not anti–virus software) will take the risk to become known that it willfully spreads viruses. It will be probably boycotted by its users and the losses of income will be much greater than any gains.

As to the producers of anti–virus software, they don't need to write viruses themselves, in order to sell their programs. It is sufficient to use the hype that the media accords to the problem, to mention how many viruses there are and how many of them their wonderful product is able to defeat.

5 The Soviet virus factory and virus writing in the other countries of the former Eastern block.

While Bulgaria was one of the best computerized countries in East Europe, the political, economical, and social conditions in the other countries were (and maybe still are) quite similar. That is why the virus writing and spreading has been developed in these countries too.

Viruses are created in Poland (`W13`, `217`, `583`, `Father Christmas`, `Dot Eater`, `Joker`, `Vcomm`, `Akuku`, `311`, `Hybryd`), in Hungary (`Stone ‘90`, `Filler`, `Monxla`, `Polimer`, `Turbo Kukac`), in Czechoslovakia (the `Antivirus` virus), and even in Yugoslavia (`17Y4`, `Svir`). According to some reports from Romania, there are no viruses written there, but the `W13`, `Yankee Doodle`, `Dark Avenger` and `Stoned` viruses are quite widespread.

However, the country most similar to Bulgaria is, undoubtedly, the Soviet Union. According to the Soviet anti–virus researcher Bezrukov [Bezrukov], the first virus appeared there almost at the same time as in Bulgaria and, by the way, it was the same virus (`Vienna`). So, the preconditions are almost the same as with our country.

There are, however, two main differences: the level of computerization and the number of virus writers.

The level of computerization is still much lower than in Bulgaria. There are much fewer computers per person than in our country. The users are much more isolated, due to the much larger distances. The telephone network is in the same miserable condition, as in Bulgaria. The networks are very few and not widely used. For instance, in Sofia alone there are more FidoNet nodes than in the whole Soviet Union. It is not safe to send floppy disks by regular mail, since they will be probably stolen. All this delays very much the spreading of viruses. Unfortunately, it also delays the distribution of anti–virus products and the information exchange between the anti–virus researchers. For instance, examples of new viruses created there reach the Western anti–virus researchers with huge delays.

Unfortunately, the other factor is much more dangerous. In the USSR there are much more programmers than in Bulgaria and they seem at least as much motivated in creating new viruses.

The virus writing in the Soviet Union is currently in the same state as it was in Bulgaria about three years ago. However, at that time only nine variants of known viruses and one stupid original virus has been created there (6 `Vienna` variants, 3 `Amstrad` variants, and the `Old Yankee` virus). At the first Soviet anti–virus conference in Kiev (mid–November, 1990) more than 35 different viruses of Russian origin were reported.

Some of them were variants of known viruses, while others were completely new. It has been noticed that the Soviet virus writers are less qualified than the Bulgarian ones, but they use a destructive payload in their creations much more often.

Since the reasons of virus writing in the USSR are very similar to those in Bulgaria; since this virus writing occurs in a much larger scale; and since no steps are taken by the authorities in order to stop it, it is possible to predict that in the next few years the Soviet Union will be far ahead of Bulgaria in computer virus creation and that a new, much larger wave of computer viruses will come from there. Probably after a year, several (up to ten) virus writers with the qualification of the Dark Avenger will emerge from there.

6 The impact of the Bulgarian viruses on the West and on the national software industry.

While a huge part of the existing viruses are produced in Bulgaria, a relatively very small part of them spread successfully to the West. Of more than 160 Bulgarian viruses, only very few (`Dark Avenger`, `V2000`, `V2100`, `Phoenix`, `Diamond`, `Nomenklatura`, `Vacsina`, `Yankee Doodle`) are relatively widespread.

At the same time some of them (`Dark Avenger`, `V2000`, `Yankee Doodle`, `Vacsina`) are extremely widespread. According to John McAfee, about 10 % of all infections in the USA are caused by Bulgarian viruses — usually by the `Dark Avenger` virus. In West Europe this virus shares the popularity with `Yankee Doodle` and `Vacsina`.

Of the viruses listed above, the major part are written by the Dark Avenger — all except `Yankee Doodle` and `Vacsina`. Almost all his viruses (in this case — with the exception of `Diamond`, which is the least spread) are extremely destructive. The `Phoenix` and `Nomenklatura` viruses corrupt the FAT in such a subtle way, that when the user notices the damage, there is no way to disinfect the infected files and even to determine which files are damaged. The only way is to reformat the hard disk.

It is difficult to estimate the costs of all damage caused by Bulgarian viruses. There are reports from Germany about a 10,000,000 DM damage, caused only by the `Vacsina` virus. It is probable, however, that these numbers are largely overestimated.

The huge number of known Bulgarian viruses causes also indirect damage to the West community, even if the viruses themselves do not escape from Bulgaria, but only examples of them are supplied to the anti–virus researchers. These researchers have to develop anti–virus programs against these viruses (just in case the latter succeed to spread outside Bulgaria). Therefore, they have to waste their time and efforts. Furthermore, the user is forced to buy new anti–virus programs (or pay for updates of the old ones), in order to feel safe against these viruses.

In the same time, the creation and spreading of Bulgarian viruses causes a lot of damage to the Bulgarian economics. In Bulgaria, the Bulgarian viruses are much more widespread. More than 80 % of about 160 known Bulgarian viruses have been detected in the wild in our country. It is difficult, however, to evaluate, or even to estimate the exact costs of the caused damage, since in Bulgaria the term "property of computer information" simply does not exist in legal sense. It is the same with the cost of this information.

In fact, the creation of computer viruses causes also indirect damage to our economics. First of all, a lot of extremely capable people are wasting their minds to create destructive viruses, instead of something useful. Second, the fact that the Bulgarian programmers use their time to create computer viruses destroys their reputation as a whole. No serious software company accepts to deal with Bulgarian programmers or software companies, because it is afraid that the supplied software might be pirated or might contain a virus.

7 Conclusion.

Virus writing in Bulgaria is an extremely widespread hobby. Most of the major virus writers are known, but no measures can be taken against them. Their work causes a lot of damage to the Western community, as well as to the national economics. Therefore, it is urgent to take legal measures in this direction; measures that will make virus writing and willful spread of computer viruses a criminal act. This is the only way to stop, or at least to reduce the threat.

References

[KV88] Viruses in Memory, Komputar za vas, 4–5, 1988, pp. 12–13 (in Bulgarian)

[KV89] The Truth about Computer Viruses, Vesselin Bontchev, Komputar za vas, 1–2, 1989, pp. 5–6 (in Bulgarian)

[Chip] Die neue Gafahr — Computerviren, Steffen Wernery, Chip, 9, 1987, pp. 34–37 (in German)

[Bezrukov] Computer Virology, Nikolay Nikolaevitch Bezrukov, Kiev, 1991, ISBN 5-88500-931-X (in Russian)