JPRS-CST-90-010
10 APRIL 1990


# JPRS Report

# Science & Technology

## China

### Computer Viruses: Two Generations

# Science & Technology

## CHINA

## Computer Viruses: Two Generations

*JPRS-CST-90-010* *10 April 1990*

CONTENTS

## Analyses of, Methods for Countering Computer Viruses

### Immunization Against 'Brain' Virus

*90CF0128A Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 39, 11 Oct 89 p 44*

[Article by Lei Jun [7191 6511], Department of Computer Science, Wuhan University: "Vaccination Against the Brain Virus"]

[Text] Editor's note: The primary computer virus currently appearing in computer circles within China is a benign virus—the "ball virus" [or "Ping-Pong" virus], against which many computer users have developed vaccination, detection, and elimination software. We have received many letters from readers following up on our issue No 28 of this year that was dedicated to publishing a number of articles on computer viruses [see JPRS-CST-89-022, 10 Oct 89, special issue]. These letters have analyzed contributing factors, detection, and eradication of the ball virus, as well as methods of vaccination, and at the same time, new viruses have been discovered. For this reason, this paper has once again arranged for a special issue on computer viruses. We do so on the one hand to provide even more information regarding computer viruses to users who find themselves troubled by these problems, as well as to sound the alarm to those who have yet to be attacked by viruses and to provide some means of prevention. We also want to appeal to the many computer users, that our colleagues in the computing profession should organize to draw up pertinent tactics by which to control or eliminate the production or spread of computer viruses. [End of note.]

Following upon the ball virus, one called "Brain" (or "Pakistani Brain") has appeared in China.

This virus is benign, but it is also possible that it could destroy disk files. The Brain virus has several unique characteristics: all volume labels on disks affected by Brain are changed to read "(C) Brain." By listing the directory, the user can determine whether the disk has been infected by Brain. Brain takes over the disk boot sector, where in that infected boot sector one can see such information as "BRAIN COMPUTER SERVICES" and "E-PAKISTAN," which is how the name "Brain" or "Pakistani Brain" has come into being.

The source code for Brain is more than 3K, but only one-half of that runs. Brain occupies three clusters, changing those clusters to "bad" clusters, and the user can employ PC Tools to see a disk MAP diagram (the position of the Brain virus on the disk is not fixed).

Generally speaking, Brain resides in the higher range of RAM, interrupting any read operation. During those read operations, Brain first determines whether the read is of a boot sector, and if a boot sector is not being read first, then Brain determines whether the fourth and fifth bytes have the value '1234' ('1234' is the Brain virus marker, and it is stored as '3412'). If not, it then infects the disk. Brain looks for three successive free clusters, puts the original boot sector into the first of these clusters, and stores part of the virus in the disk boot sector, putting the remainder in the other empty clusters. If the disk is full, it abandons the infection. With only one free cluster, Brain will occupy that cluster, then write over the next two clusters. In this way, if those two clusters are part of a file, the file can no longer be run (or read or written onto); this is also one way in which many users have come to know of the Brain virus. Brain stores the original boot sector address in five successive bytes beginning with the ninth byte of the new boot sector. The contents of the five bytes beginning at the eighth byte in the Brain-infected disk boot sector appended to this article are 0327000100, that is, side 1, track 27, and sector 3. If the system is infected with the Brain virus, when a user reads in the boot sector, what is read is the correct boot sector. Brain is deceptive here. When removing Brain, it is best to initialize with an uninfected disk.

If you cannot determine which disk has not been infected, use DEBUG to alter the interrupt vector of INT 13H, changing it to F000:EC59 (F000:EC59 is the interrupt routine for INT 13H in the ROM).

The principles of Brain and the ball virus are largely the same, so the method of eradication is also similar.

The eradication is done as follows:

```
<1>   A>COPY CON BRAIN.V
A
MOV       AX, 0201      ; READ operation
MOV       BX, 1000      ; buffer address
MOV       CX, 2703      ; contents of 8th and 9th bytes of boot sector
MOV       DX, 0001      ; contents of 11th and 12th bytes
INT       13            ; read the correct boot module
INT       3
G
RIP
100
A 100
MOV       AX, 0301      ; WRITE operation
G                       ; write to first sector of track 0 on side 0
Q
^Z
<Z>   A>DEBUG <BRAIN.V
```

```
1AE8:0100  FA E9 4A 01 34 12 00 03-27 00 01 00 00 00 00 20  ..J 4...'......
1AE8:0110  20 20 20 20 20 20 57 65-60 63 6F 6D 65 20 74 6F        Welcome to
1AE8:0120  20 74 68 65 20 44 75 6E-67 65 6F 6E 20 20 20 20   the Dungeon
1AE8:0130  20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20
1AE8:0140  20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20
1AE6:0150  20 28 63 29 20 31 39 38-36 20 42 61 73 69 74 20   (C) 1986 Basit
1AE8:0160  26 20 41 6D 6A 61 64 20-28 70 76 74 29 20 40 74  & Amjad (pvt) Lt
1AE8:0170  64 2E 20 20 20 20 20 20-20 20 20 20 20 20 20 20  d.
1AE8:0180  20 42 52 41 49 4E 20 43-4F 4D 50 55 54 45 52 20   BRAIN COMPUTER
1AE8:0190  53 45 52 56 49 43 45 53-2E 2E 37 33 30 20 4E 49  SERVICES..730 NI
1AE8:01A0  5A 41 4D 20 42 4C 4F 43-4B 20 41 4C 4C 41 4D 41  ZAM BLOCK ALLAMA
1AE8:01B0  20 49 51 42 41 4C 20 54-4F 57 4E 20 20 20 20 20   IQBAL TOWN
1AE8:01C0  45 20 50 41 48 49 53 54-41 4E 2E 2E 50 48 4F 4E  E-PAKISTAN..PHON
1AE8:01D0  45 20 3A 34 33 30 37 39-31 2C 34 34 33 32 34 38  E :430791,443248
1AE8:01E0  2C 32 38 30 35 33 30 3E-20 20 20 20 20 20 20 20  ,280530.
1AE8:01F0  20 20 42 65 77 61 72 65-20 6F 66 20 74 68 69 73    Beware of this
1AE8:0200  20 56 49 52 55 53 2E 2E-2E 2E 2E 43 6F 6E 74 61  VIRUS.....Conta
1AE8:0210  63 74 20 75 73 20 66 6F-72 20 76 61 63 63 69 6E  ct us for vaccin
1AE8:0220  61 74 69 6F 6E 2E 2E 2E-2E 2E 2E 2E 2E 2E 2E 2E  ation...........
```

**Figure 1. A Portion of the Brain Virus Boot Code**

```
 Volume in drive B is  (c) Brain
 Directory of B:\

VE       EXE      5824   7-07-89          7:00p
VP       EXE     19328   7-07-89          7:00p
V1A      EXE     19232   7-07-89          7:00p
V1B      EXE     21328   7-07-89          7:00p
L        COM        74   8-25-89          2:05a
PRO      LOC     17040   1-01-80         12:38a
PAS          <DIR>       9-06-89          1:50p
STEP         <DIR>       9-06-89          1:50p
TREEINFO NCD        59   9-06-89          1:51p
        9 File(s)          137216 bytes free
```

**Figure 2. A Listing of the Directory of an Infected Disk**

If the boot portion read is not the correct boot portion, it is possible that the disk has previously been infected by another virus. Overlapping infection by viruses can made eradication extremely complex. Yet a better method is to write in a correct boot portion from the appropriate DOS disk, and then to use the DOS SYS command.

Recovering "bad clusters" is easy. Just use the Advanced version of Norton Utilities to change the "bad clusters" to "available."

The viruses currently making the rounds in China are benign, but we must heighten our awareness and closely watch any abnormal situation in our systems so that we might discover a virus as early as possible, thereby reducing our losses.

Concurrently, we should speed up development of general-purpose vaccination programs.

## Banking System Viruses

*90CF0128B Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 39, 11 Oct 89 p 46*

[Article by Yao Shuanghong [1202 7175 1347], People's Construction Bank of China, Changzhou Center Branch: "An Invasion of 'Viruses'? How Banking Microcomputers Are To Cope"]

[Text] In May of this year [1989], we discovered, when running bank accounting-system software written in dBASE III on a "Yangzi 0520," that intermingled with normal display to the screen was a white dot looking like a ping-pong ball jumping around in a pattern something like a sine wave. At the same time, the working efficiency of the computer showed a clear decrease, and when printing on the printer, the screen could even lose its display or the machine would lock up. When restarted, the hard disk would boot normally, but we discovered that some data on the hard disk had been lost. After the appropriate modifications, and after running normally for more than 20 hours, these same faults would reappear. Using the CHKDSK command to inspect the hard disk, we discovered that there were 1,024 bytes of bad sectors. When we ran DIR to inspect the "3070" 24-pin dot-matrix Chinese character driver, ALL24P.EXE, we discovered that the length of this program had increased by 648 bytes over the original version. Referring to the relevant documents, we diagnosed our situation as infection by a virus affecting the operating system and the shell. Because the machine was then monitoring accounts and we could not delay our work, we took the following measures:

1. We first booted the machine using a system disk on which the write-protect hole had been covered (to prevent infection by the virus). We then used the COPY or BACKUP command to copy off the hard disk any data that had not been backed up on floppies.

2. Using the YZ0520 high-level diagnostic disk to boot the system, we did a low-level format of the hard disk. Using the FDISK command to create a DOS partition on the hard disk, we then used the command FORMAT/S/V to format the DOS segment.

3. We installed the CC-DOS operating system, dBASE III, and the software we were using.

4. We copied in the database, then retrieved data from the hard disk.

It only took 2-3 hours to do these things, and we were able to eradicate the virus. So far, this computer has not been reinfected, and it has worked normally.

Looking back on it, the method we used would also be effective for certain other operating-system and shell viruses. This is because this kind of virus does not infect data files with the .DBF extension, or if so, it definitely does not then become a source of infection. Whether the method could also be effective for invasive and source-code viruses remains to be seen.

We can see from the process just described that there is no mystery about computer viruses, and this is because they are a form of software. When eliminating a virus, there is no need whatsoever to use physical means to do so. Naturally, by the time a virus is discovered it will have caused a certain amount of damage for us computer users and will have affected our normal work. But even so, taking preventive measures is the best plan with which to deal with viruses for us banking computer personnel, and we should always be doing the following:

1. We must back up system software; we must back up databases at periodic intervals; ideally, we must back up dynamic information databases daily to floppies; and we must keep those back-up floppies for a year. Doing this is also an effective means of dealing with use of a computer to undertake theft.

2. Don't carelessly copy software on operations computers; examine floppies whose origins are unclear; and to whatever extent possible, do not use application software on floppies interchangeably among different machines, which precaution could prevent the spread of infection.

3. Don't carelessly install new software on an operations computer, and forbid the use of any game software on an operations computer.

4. Make use of existing virus detection software and methods, and periodically a corresponding check of a computer hard disk so that a virus might be discovered promptly.

5. As soon as it is discovered that a computer has become infected, if the type of virus is not clear and there is no effective eradication software, you can demagnetize or reformat a hard disk and floppies used on that machine.

As long as we can have a clear understanding of computer viruses, can strengthen usage management of computers, and regularly educate operators in safe use of computers, we can certainly deal with the invasion of computer viruses.

## Adding Passwords to Hard Disks

*90CF0128C Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 39, 11 Oct 89 p 46*

[Article by Shi Fensu [4258 1164 6204], Ningxia Institute of Computer Technology: "The Method Using a Computer Virus Program To Add Passwords to Hard Disks"]

[Text] The methods by which passwords are assigned to hard disks was outlined in CHINA COMPUTERWORLD in issues 88.22, 88.43, and 89.18, and these methods may be largely divided into two kinds: the first places a command file in the automatically executing file AUTOEXEC.BAT; the second puts a password identification routine into the COMMAND.COM file.

Comparing the two, we find the second is quite reliable, but where it is insufficient is in the fact that with so many versions of DOS being used, the COMMAND files are not the same, so the address of the password identification processing routine that is added will differ with the different contents of the COMMAND file. This approach would not be convenient for a user not familiar with assembly language.

Computer viruses have been spreading rapidly recently among many microcomputers in China (especially the Ping-Pong virus), and this paper has already addressed the problem in its 89.28 special issue, in which it provided some ways to eradicate and vaccinate against viruses.

Although computer viruses are reprehensible because they get in the way of our normal computer use, after we have understood their operating principles, we can then make effective use of them ourselves.

As far as computers with hard disks infected with the Ping-Pong virus are concerned, with only a minor modification of the virus program, we can achieve the two goals in one of getting rid of and vaccinating against the virus, and also providing passwords for a hard disk.

One portion of the Ping-Pong virus is stored in the disk boot sector, and another portion is placed among some sectors marked as in "bad" clusters.

When a computer is booted, the virus program from the boot sector and relevant parameters are installed in RAM at 0000:7C00, from where it is executed, and at which time the virus accomplishes the following actions:

1. It requests 2K of space in highest RAM, then relocates itself and relevant parameters to that area. It then passes control to the pertinent addresses of the original boot code for execution.

2. Another portion of the virus and the normal boot sector are read into pertinent areas of RAM.

3. The entry point for the INT 13H interrupt routine is altered, then the normal boot routine is run.

With only a minor modification to the virus program, beginning in step 3, we can keep the virus from modifying the INT 13H pointer, and can then add a handling routine to identify passwords. When we then pass to execution of the normal boot routine, we will have achieved our previously stated goal. For the specific modifications, please see the listing provided. It should be explained that the alteration just described is done

```
C>DEBUG
-L 100 2 0 1
-A 0173
098A:0173  JMP     01D0
098A:0175  DB 0D,0A,"Please input password:",0
098A:018E  DB "12345",0
098A:0194  DB 0,0,0,0,0,0
-A 01D0
098A:01D0  PUSH    CS
098A:01D1  POP     ES
098A:01D2  MOV     AH,0F
098A:01D4  INT     10
098A:01D6  MOV     AH,00
098A:01D8  INT     10
098A:01DA  MOV     SI,7C75
098A:01DD  LODSB
098A:01DE  AND     AL,7F
098A:01E0  JZ      01EB
098A:01E2  MOV     AH,0E
098A:01E4  MOV     BX,0007
098A:01E7  INT     10
098A:01E9  JMP     01DD
098A:01EB  MOV     SI,7C94
098A:01EE  MOV     CX,0005
098A:01F1  PUSH    CX
098A:01F2  MOV     AH,00
098A:01F4  INT     16
098A:01F6  CMP     AH,00
098A:01F9  JZ      01FD
098A:01FB  MOV     [SI],AL
098A:01FD  MOV     AH,0E
098A:01FF  MOV     BX,0007
098A:0202  MOV     AL,3F
098A:0204  INT     10
098A:0205  INC     SI
098A:0207  POP     CX
098A:0208  LOOP    01F1
098A:020A  MOV     SI,7C8E
098A:020D  MOV     DI,7C94
098A:0210  MOV     CX,0005
098A:0213  REPZ
098A:0214  CMPSB
098A:0215  JZ      0224
098A:0217  INC     BYTE PTR [7DF7]
098A:021B  CMP     BYTE PTR [7DF7],03
098A:0220  JNZ     01D2
098A:0222  JMP     0222
098A:0224  MOV     AH,0F
098A:0226  INT     10
098A:0228  MOV     AH,00
098A:022A  INT     10
098A:022C  MOV     DL,[7DF8]
098A:0230  JMP     0000:7C00
098A:0235
-W 100 2 0 1
-Q
```

**Listing of Modification**

when a hard disk has been infected (as to whether a virus is present, please see the diagnostic methods described in issue 89.28 of this paper).

Password length is 5 bytes (it can be the numbers 0-9, as well as lowercase letters), and as each keystroke is pressed a '?' is displayed on the screen.

A user may choose any password he likes, requiring only that the '12345' that appears as the command at address :018E of the listing be modified to reflect the bytes chosen.

Since the version of DOS is not relevant, as soon as a hard disk has been infected by the Ping-Pong virus, the virus program is always the same, so this way of adding passwords to a hard disk is quite general-purpose. This method actually puts the password handling routine in place before the normal boot routine is executed.

## Method for Eliminating Viruses

*90CF0128D Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 39, 11 Oct 89 p 50*

[Article by Liu Guangqi [0491 0342 1142]: "A Convenient Way To Eliminate a Computer Virus"]

[Text] Issues 20 and 23 of CHINA COMPUTERWORLD published such articles as "Computer Virus Programs Discovered One After Another in China" [see JPRS-CST-89-014, 18 Jul 89, pp 46-47] and "Software Tool Developed for Detection, Eradication of Computer Viruses" [see JPRS-CST-89-018, 22 Sep 89, pp 75-76]. I used the content of those articles in a preliminary attempt to deal with the virus phenomenon in my office. I relate this here so that others might learn from my experience.

### Posing the Question

We copied onto a floppy in our IBM PC XT a floppy disk from outside the office, then copied it and viewed the files contents (not knowing the disk carried a virus), after which we displayed the contents of relevant files on the hard disk. When we ran the applications files involved (on both floppies and the hard disk), on about the 20th occasion the notorious little ball appeared on our screen, bouncing up and down, and we were simply unable to deal with our application program. Using the directory and file allocation command CHKDSK, we checked both the floppy and the hard disk, discovering that there were bad sectors on the floppy (just as described in your reports), while the bad sectors on the hard disk (not always the same) were listed at 2,048 bytes or 2,732 bytes, etc.

### Analysis of the Problem

Because this is a benign virus, there was no damage to the machine and the operating system, the only problem being the "random" appearance on the screen of the moving ball when running application software, and in no time, the application program would become unmanageable. But when we rebooted the operating system, we could again run the application software. From the point of view of disk space allocation, the virus would create 1,024-byte bad sectors (on the floppy), and 2,048- and 2,732-byte bad sectors (on the hard disk, where the size varied). During read operations, the virus would be made resident in RAM from the floppy (or hard disk), causing the virus to rapidly replicate. Could we reallocate the disk space to recover the bad sector space that had been made off-limits, thereby getting rid of the virus? The answer was "yes."

### The Specific Method

After we cold-booted (and warm-booted) from drive A: with an operating system that had (definitely) not been

infected, we took out the floppy and inserted a floppy with the virus. We inserted a pre-formatted back-up disk in drive B: (being sure it did not have the virus), then used the COPY command to copy the designated files from disk A to disk B (we could not use DISKCOPY or the all-inclusive command COPY A:*.* B), after which we once again inserted the operating system disk in A: and rebooted. We used the CHKDSK command to check the disk in B:, finding no 1,024-byte bad sectors. We put the copied virus disk into drive B:, then used the format command FORMAT B: to format the disk in B:. We once again used CHKDSK B: to check, but could not find any bad sectors on the disk in B:. We had therefore attained our goal of eliminating the virus. This disk was then available as a back-up disk. By repeating the operations just described, you can recover a floppy disk that has had the virus. The principles are the same for eliminating the virus from a hard disk, so I will not repeat.

After use over the intervening period, the recovered disks have never again experienced an outbreak of virus.

## Dealing With the Ping-Pong Virus

*90CF0128E Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 39, 11 Oct 89 p 50*

[Article by Wu Xiangcun [2976 4382 2625] and Xie Dong [6200 2639], Qinghua University: "Diagnosis, Analysis, and Eradication of the Ball Virus in the DOS Environment"]

[Text] The appearance and continuing proliferation of computer viruses has already and continues to generate tragedies in computer applications circles, and at the same time, they have posed a new challenge for computer workers.

### I. The Symptoms and Threat of Viruses

Comparatively speaking, the Ping-Pong virus is considered benign (i.e., it does not destructively alter and delete disk files), but it seriously affects the normal operation of programs. After contact with this virus during a read or write operation, a small ball bouncing along an accurate sine-wave form will make a mess of the display, rendering it unintelligible. When in Chinese-character mode (graphics mode), the situation is more serious, and the operator must reboot the system. With larger programs, longer operating times, and more frequent disk operations, the chances of setting off this virus get greater, and the damage it causes will be all the more extensive.

### II. The Diagnosis and Analysis of the Virus

Take a careful look at the disk map of storage space, and if you discover that there are one or more bad sectors, it is quite possible that this disk has been infected by a virus. After booting with a system disk that is infected (either floppy or hard disk), the virus program resides in RAM, and the computer is now able to transmit the virus, and all working disks will become infected. Moreover, the latter half of the virus program is hiding in the first marked bad sector, while the front half has modified the data in sector 1 of track 0 on side 0 of an infected disk, that is, the data comprising the boot sector.

1. The complete virus totals 1,024 bytes, occupying two sectors of disk space, and these two sectors are not contiguous, so there is no harm in having a V1 and V2 [the first and second parts of the virus, respectively] occupying first sector 1 of track 0 on side 0 (the boot sector) and replacing the normal boot routine, then having V2 stored in a random sector somewhere else on the disk (which is determined by the transmission process). The next sector after V2 happens to be the remainder of the normal boot sector. The cluster composed of these two sectors is marked as a bad cluster in the FAT [File Allocation Table], for which reason it will not be overwritten with another program file.

2. The initializing and installation process of the virus program

After a PC has been booted, the ROM routines use the boot system to read the data on sector 1 of track 0 on side 0 of the boot disk (either A: or C:) into RAM at 0000:7C00, after which there is a jump to this RAM address, beginning execution of the program commands just read into memory. If the boot disk is not damaged, what is read into RAM at that point is the normal booting routine, following upon which, the task is to successively read in and execute three system files: IBMBIO.COM, IBMDOS.COM, and COMMAND-.COM. At this point, the normal boot is complete. If there is a virus on the disk, things become more complex. At that time, what the ROM-routine boot system reads into RAM at 0000:7C00 is V1. After V1 gains control, it runs the following operations: it copies the V1 module into the highest possible RAM address, to where it shifts and continues execution; it reads V2 from the disk into RAM right behind the V1 sector; and it reads the normal boot sector auxiliary portion right behind V2, into RAM at 0000:7C00, overwriting in the process the sector occupied by V1. It then modifies the INT 13 interrupt vector of the normal boot routine, causing it to point at the V1 module in highest RAM, and after which it passes control back to 0000:7C00 to begin execution of the normal DOS boot process. At that time, the virus program has completed its installation in highest RAM, and it cannot be easily overwritten.

We can see from this that the virus is buried deep within the lowest level of the system, and that it has completed its installation even before the DOS system is booted, which makes it highly secretive and stubborn.

3. The virus transmission process and display trigger

As we have just said, the virus has modified the normal INT 13 interrupt vector to point to the virus routine, that is, to the virus transmission routines and display trigger routines that have been inserted into the front part of the normal INT 13 service routines. Whenever

there is a read/write operation to the disk, then the virus transmission routine and display trigger routine will be executed. The function of the virus transmission route is to copy V1 to the boot sector of the disk, copy V2 to the first sector of the disk, and then to mark the corresponding positions in the FAT as bad clusters, which prevents the virus program from being overwritten. The function of the virus display trigger program is first to determine whether certain conditions have been met, and if so, it then alters the INT 8 interrupt vector to point to the routine module that bounces the ball on the screen. As is well known, INT 8 is the clock hardware interrupt, which occurs about 18 times per second. As soon as triggered and the INT 8 interrupt vector has been altered, the ball will bounce interminably on the screen. The only way the user has of stopping this phenomenon (temporarily) is to reboot the system. There is no other way. The more frequent the read/write operations, the greater is the chance of triggering the display, and even though that might not have yet happened, it will have seriously affected the speed of the disk read/write operations.

### III. The Elimination of the Virus and Suppression of Its Transmission

Reboot the system with an undamaged system disk. After formatting new disks and disks without files of value, copy important files from the virus disks onto these formatted disks (generally speaking, data disks that have been infected will not transmit the virus, but it is another story if you mistakenly try to boot a data disk thinking it is a system disk, something that will happen occasionally). It is then effective to reformat the virus disks as a way of eliminating the virus, but this is a lot of work. To eliminate the hard-disk virus in this way is really troublesome. With that in mind, we have especially developed a software tool, CKV-1, to eliminate the virus, and this has proved successful. Within a minute, the disk can be restored to its pre-infected state, and it can be periodically used to rid the user of the trouble caused by this computer virus.

## National Statistics System Virus

*90CF0128F Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 39, 11 Oct 89 p 52*

[Article by Jiang Guozhong [1203 0948 1813], Computing Center, Dalian Municipal Bureau of Statistics: "Analysis of the Computer Virus Prevalent in the National Statistical System"]

[Text] Since computer viruses were first discovered in the United States, computer viruses have spread throughout the world, and this phenomenon has gained a great deal of attention from world computer circles. The first page of COMPUTERWORLD 89.20 reported that "computer viruses are continuing to be discovered in China," and as confirmation of this fact, computer viruses have again appeared in China recently, in particular, a virus that has infected many computers in the national statistics system.

All M24 microcomputers at the Dalian Municipal Bureau of Statistics have been infected by a computer virus prevalent in the national statistical system, a virus that can infect IBM PC and compatible computers running MS-DOS. Although on infected computers this virus does not damage programs and data on the computer floppy or hard disks, when doing normal data processing (such operations as data input, printing, or gathering data), a small ball will occasionally appear to bounce around on the screen, and it looks as though many ping-pong balls are bouncing on a ping-pong table. These balls on the display will bounce interminably, disrupting normal operations of the microcomputer, until the system is reset or turned off.

This virus is quite infectious, so it is quickly transmitted. If one places an uninfected disk into the drive of an infected computer, it is possible the disk will become infected. Therefore, floppy disks that have been used on an infected machine, then transferred to another machine, could be transmitting the virus to that other machine. The floppy disk is the primary medium for the propagation of viruses among microcomputers. Because all M24 microcomputers at the Computing Center were infected, when we used these machines for writing or copying the annual-report programs for the 1988 Annual Report of the City of Dalian, and released these annual-report programs to counties and cities in our jurisdiction, we thereby caused all microcomputers throughout the city and in the administrative districts to be infected with this virus.

I analyzed infected disks using DEBUG and discovered those areas where infected disks differed from those not infected, then looked for what caused the virus.

### 1. The Boot Record Had Been Modified

The boot record of the DOS operating system is composed of four parts: a) a jump to coded instructions; b) a business identifier; c) a basic input/output parameter module; and d) an initialization code section. The boot record is a rather stable part of the DOS operating system, only changing in different versions of DOS as system files change their size or position, but even then they are not entirely different. The jump code and initialization code sections in the boot records of infected disks are completely different from the boot record supplied in the DOS operating system.

### 2. There Are Bad Clusters Marked in the File Allocation Table (FAT)

The FAT of an infected disk is marked as having bad clusters (bad sectors). By analysis, I discovered that there is no physical damage to the disk, but rather that the designation is man-made.

### 3. The Contents of the Infected Disk Bad Sectors

At the disk positions corresponding to the bad clusters as marked, the first sector has information, but not that provided by DOS; this is the man-made virus, interfering with normal operations of the computer, and showing as a small ball rolling around on the screen. The contents of the second sector includes the boot record provided by the DOS operating system.

Because the boot record has been modified by the virus, when on an infected MS-DOS system the FORMAT/S command is used to format a floppy, the system states that the floppy had no bad sectors; but when you boot from that floppy, the system will not run normally.

The boot record provided by the DOS system is used to initialize DOS, and it includes the minimum number of routines necessary to read in and initialize the various primary parts of the operating system. On power-up or warm boot, the ROM BIOS initialization routines read the first record (the boot record) from the floppy in drive A: into a standard position in RAM (the address is 31744, or 7C00h), and after doing so, the ROM BIOS passes the control at that address over to the boot routine, and the boot routine checks to see whether two hidden files are on the disk—IO.SYS and MSDOS.SYS. If so, those files are read into a specific location beginning at 0060:0000. Control is then transferred to that address, which is IO.SYS.

The boot record of an infected disk does not have the same contents as those provided by the normal DOS system, and therefore its boot process is as follows: the ROM BIOS initialization routines pass control to the boot routine, which then does not first read the files IO.SYS and MSDOS.SYS into RAM, but rather looks for the bad disk cluster mark 'FF7' in the FAT. Having found the two sectors on the floppy corresponding to the information listed in the bad clusters mark, it reads them into RAM. This is how the virus enters RAM, and after reading in the contents of the bad sectors, the contents of the infected boot record are written to the boot region of the hard disk, where bad cluster marks are created in the hard disk FAT. The boot contents provided by the virus and the DOS operating system are written into positions on that disk corresponding to those bad cluster marks. This is why, when an infected DOS disk is used to boot the microcomputer, the virus can be transmitted to an uninfected hard disk.

This kind of computer virus works simply by modifying the boot record of the DOS operating system as provided through a floppy or hard disk, where bad cluster marks are created for the FAT; the two sectors on the floppy disk that correspond to those marked as bad are written into the boot sectors provided by both the virus and the normal DOS system, and the contents of the file directory area are not changed. No files on the floppy are damaged. To see whether a microcomputer has been infected by this virus, one can run the CHKDSK command supplied by the DOS operating system. When used on a floppy, there will be bad sectors in 1,024 bytes on an infected disk, while when used on a hard disk, there will be 8,192 bytes of bad sectors.

The way to remove this virus is to use a special program or DEBUG and directly write the DOS supplied boot record into the corresponding sector of an infected floppy or hard disk. This way, a normal boot record is built on an infected disk, which then destroys the condition necessary to introduce the virus source from an infected disk into RAM.

Because files on an infected disk are not damaged, the average computer user can simply disinfect hard disks and floppies, the specific steps for which are as follows:

### 1. A Way To Disinfect a Floppy

First, set up a subdirectory on the hard disk; then, copy all files on the infected floppy to this subdirectory with the command A>COPY *.* C:. Next, use the normal DOS operating system (the MS-DOS operating system provided with the infected M24 micro) to reformat the infected floppy disk, then recopy the files in the hard-disk subdirectory back to the floppy with the command C>COPY *.* A:. Working this way, the virus on the floppy will be eliminated, and files will have been protected. Please note that you cannot accomplish this operation in the root directory of the hard disk, because then the floppy disk would be reinfected.

### 2. A Way To Disinfect a Hard Disk

There are many opportunities by which a hard disk can become infected. Booting a computer by means of the DOS operating system will infect the hard disk. Copying files from an infected floppy to the hard-disk root directory or to a subdirectory will also infect the hard disk. Before disinfecting a hard disk, one must first copy all files in a hard-disk root directory one wishes to preserve onto floppies. When processing of the desired back-up files is complete, one can use the FORMAT C: /S command to reformat the hard disk, which eliminates the hard-disk virus.

An important step after removing the virus from both floppies and hard disks concerns how to prevent reinfection with the virus. My recommendation is to be more diligent in management of commonly used disks, and do the necessary inspection of floppies coming from other units before use. If a virus is discovered, one should immediately take the required steps to prevent the virus from spreading, report to the required authorities of the relevant departments or organizations, and eliminate the virus to reduce the effects of the virus to an absolute minimum.

## Another Virus Elimination Technique

*90CF0128G Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 39, 11 Oct 89 p 54*

[Article by Ge Qinge [5514 0530 7245] and Wang Jin [3769 2516], Maritime Command Automation Workstation: "A Simple Method for Virus Elimination"]

[Text] The Ping-Pong virus appearing these days in China infects IBM PC and compatibles running MS-DOS. When an infected computer is used, a small ball will roll around interminably on the screen beginning at a certain time. It looks like a ping-pong ball bouncing

```
NAME    XCBT
STACK   SEGMENT PARA STACK 'STACK'
STAPN   DB 100 DUP  (0)
TOP     EQU LENGTH STAPN
STACK   ENDS
DATA    SEGMENT PARA PUBLIC 'DATA'
BUF1    DB 1024 DUP (0)
BUF2    DB 1024 DUP (0)
JSQ     DW 1024
DATA    ENDS
CODE    SEGMENT PARA PUBLIC 'CODE'
ASSUME CS:CODE, DS:DATA, SS:STACK
START:
        MOV     AX, DATA
        MOV     DS, AX
        MOV     AX, STACK
        MOV     SS, AX
        MOV     AX, TOP
        MOV     SP, AX
        MOV     WORD  PTR  JSQ, 1024
        MOV     AL, 0
        MOV     CX, 4
        MOV     DX, 1
        MOV     BX, OFFSET  BUF1
        INT     25H
        JB      EXIT
        POPF
        MOV     SI, OFFSET  BUF1
        MOV     DI, OFFSET  BUF2
AA:
        MOV     AX, WORD  PTR  [SI]
        MOV     BX, AX
        AND     BX, 0FFFH
        CMP     BX, 0FF7H
        JNZ     AA1
        AND     AX, 0F000H
        MOV     WORD  PTR [SI], AX
        MOV     WORD  PTR [DI], AX
AA1:
        MOV     AX, WORD  PTR [SI] [1]
        MOV     BX, AX
        AND     BX, 0FFF0H
        CMP     BX, 0FF70H
        JNZ     AA2
        AND     AX, 000FH
        MOV     WORD  PTR [SI] [1], AX
        MOV     WORD  PTR [DI] [1], AX
AA2:
        ADD     SI, 3
        ADD     DI, 3
        SUB     WORD  PTR  JSQ, 3
        CMP     WORD  PTR  JSQ, 3
        JAE     AA
        MOV     AL, 0
        MOV     CX, 4
        MOV     DX, 1
        MOV     BX, OFFSET  BUF1
        INT     26H
        POPF
EXIT:
        MOV     AH, 4CH
        INT     21H
CODE    ENDS
        END     START
```

unobstructedly on a ping-pong table, which goes on until the system is reset or turned off. This virus affects not only what is displayed on the screen, but also reduces the running efficiency of the computer. By analyzing and comparing disks both with the infecting program and without, we have found a simple way to eliminate this virus.

**How the Virus Program Stores Itself**

The virus program has no file name and is therefore not included in the directory area, and its position on the disk is random. By analyzing the File Allocation Table (FAT), we discovered that infected disks always have a "bad cluster" (the cluster signifier in the FAT is FF7). Therefore, this "bad cluster" is not actually physical damage to the disk, but rather is just a man-made 'FF7' bad cluster mark in the FAT, which keeps other application programs from overwriting it. The virus program is then stored in this bad cluster, its size about 1,024 bytes.

**How To Eradicate the Virus**

Knowing the position of the virus routines on the disk, one need only restore the FAT 'FF7' bad cluster indicator to '000', the indication that no bad clusters are allocated, then use COPY to copy another application program onto this disk. This allocates that cluster to another program, which eliminates the virus.

**A Specific Example**

Following is printed a specific program for eradicating the virus on the floppy disk; one need only insert the infected floppy into the A: drive and run this program immediately.

Some explanation:

1. The FAT comprises one 12-bit entry (1.5 bytes) for each cluster on a disk;

2. The method is the same for hard disks as that above, but the FAT occupies eight sectors;

3. Note: there is an alternate copy of the FAT that is of equivalent size.

## Eradicating the DOS Virus

*90CF0128H Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 39, 11 Oct 89 p 54*

[Article by Huang Lianhua [7806 0494]: "How To Eliminate the DOS Virus"]

[Text]

**I. The Infection Process**

The virus is transmitted during disk reads. Because DOS disk read/writes are accomplished through INT 13h, an infected DOS system INT 13h has been modified. That modification includes insertion of a transmission routine before the INT 13h routine. During each DOS disk read, the virus routine checks the disk to be read to see whether it has been infected, and if not, the read-disk process will automatically transmit the virus to the new disk without affecting system operations.

The virus is loaded into RAM together with DOS during boot time, where the boot sector of an infected DOS has been modified without changing the system files.

The boot process is as follows:

1. The ROM BIOS reads the boot sector into RAM at 0000:7C00, then executes the code at that address;

2. The code at 0:7C00—7DFF is moved to 97C0:7C00, and execution is shifted to that location (97C0h is an address in 640K-byte RAM);

3. During execution, the virus routines (one sector) are read into 97C0:7E00;

4. The original DOS boot sector is read into 0000:7C00;

5. The entry address for INT 13h is changed to 97C0:7C00;

6. Execution shifts to 0000:7C00 to enter the original DOS boot.

Steps 2-6 are added by the infected DOS.

**II. A Method of Eradication**

Now that we know how the virus is transmitted, it is not difficult to get rid of it. There is a comparatively simple way to eliminate the fifth step in the boot process. In this way, although DOS will be infected, it will not be transmitted, nor will it be "set off," and at the same time, we recover our original operating efficiency. Use of the following method will also determine whether disk has been "infected."

The method (C: is used in this example; for A:, change '2' to '0'):

```
C>DEBUG

-L 100 2 0 1
-D 100
```

This displays the contents of memory, and if the cell at 101 is 1Ch, then the disk has been infected and the following procedure must be taken. If there is a different value at 101, the disk has not been infected and one may exit.

```
-F 17C 185 90
-W 100 2 0 1
-Q
```

**III. How To Set Off the Virus**

The condition for setting off the virus is when having twice read the same disk, the clock counter value satisfies a particular logic state. This is a phenomenon that appears by modification of the clock hardware interrupt INT 08. Therefore, the more often the disk is read, the more easily the virus is triggered. A simple prevention method is to write-protect disks to be read as much as possible. If the disk has been infected, use of the method described above will provide "immunization" forever!

## More on the Ping-Pong Virus

*90CF0128I Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 39, 11 Oct 89 p 56*

[Article by Li Shengjun [2621 0524 6511], People's Bank of China, Yiyang Branch: "One Experience in Getting Rid of the Round-Dot Virus"]

[Text] We brought back a GW [Great Wall] BIOS 3.00 system disk from Xi'an. The day after we had booted this disk on our PC XT, just as we were gathering and processing data and copying files, a round dot jumped out from the upper left corner of our screen, and then began moving toward the center. As the dot kept bouncing, it gradually formed a sine-wave pattern, after which, the screen became a jumbled mess of round dots; in addition, one small round dot moved around the four corners of the screen. During this process, the program continued to run, but very slowly.

We knew from this event that we were seeing a computer virus.

Therefore, we looked at our operations record, from which we determined that the source of the virus was the GW BIOS 3.00 system disk.

We then used DEBUG to look at the boot sector, where we discovered a change in that sector, and using PCTOOLS, we checked the system information, discovering that system RAM capacity was now less than 640K bytes (with each read-in of the virus, RAM reduces by 2K bytes). By initializing a virus system and reading disks with it, the virus is transmitted to normal disks. If we used a newly formatted normal disk to check the boot sector under an infected system, we see that the virus immediately infects the disk, which then changes the normal boot sector.

To get rid of the virus, we read over the articles concerning the Ping-Pong virus in this newspaper, and tried the virus elimination methods described in the [No 28] 19 July 1989 special issue, but did not succeed. For example, by using the JD1987.COM of Jiang Mingfu [3068 2494 1381] we could only achieve vaccination, not the elimination of the virus; we tried using the method of Gao Guoming [7559 0948 2494], whose instructions were not clearly set out, and which generated system hard-disk errors.

normal boot sector

```
-d 280 2ff
08FF:0280  0D 0A 4E 6F 6E 20 53 79-73 74 65 6D 20 64 69 73   ..Non System dis
08FF:0290  6B 20 6F 72 20 64 69 73-6B 20 65 72 72 6F 72 0D   k or disk error.
08FF:02A0  0A 52 65 70 6C 61 63 65-20 61 6E 64 20 73 74 72   .Replace and str
08FF:02B0  69 6B 65 20 61 6E 79 20-6B 65 79 20 77 68 65 6E   ike any key when
08FF:02C0  20 72 65 61 64 79 0D 0A-00 0B 0A 44 69 73 6B 20    ready.....Disk
08FF:02D0  42 6F 6F 74 20 66 61 69-6C 75 72 65 0D 0A 00 69   Boot failure....
08FF:02E0  62 6D 62 69 6F 20 20 63-6F 6D 30 69 62 6D 64 6F   bmbio  com0ibmdo
08FF:02F0  73 20 20 63 6F 6D 30 00-00 00 00 00 00 00 55 AA   s  com0.......U*
-q
```

virus boot sector

```
-d 280 2ff
08FF:0280  A3 F5 7D 88 36 F9 81 E9-08 01 C3 81 3E 0B 80 00   #u}.6y..i...c.....
08FF:0290  02 75 F7 80 3E 0D 80 02-72 F0 88 0E 0E 80 A0 10   .uw.>...rP.... . .
08FF:02A0  80 98 F7 26 16 80 03 C8-88 20 00 F7 26 11 80 05   ..w&...H8 .w&...
08FF:02B0  FF 01 88 00 02 F7 F3 03-C8 89 0E F5 7D A1 13 7C   ..i..WS.H..U}!.|
08FF:02C0  2B 06 F5 7D 8A 1E 0D 7C-33 D2 32 FF F7 F3 40 88   +.u}...|3R2.ws@.
08FF:02D0  F8 80 26 F7 7D FB 3D F0-0F 76 05 80 0E F7 FD 04   x.&w}{=p.v...w}.
08FF:02E0  BE 01 00 8B 1E 0E 7C 4B-89 1E F3 7D C6 06 B2 7E   >.....|K..s}F.2
08FF:02F0  FE EB 0D 01 00 0C 00 01-00 90 02 00 57 13 55 AA    k..........W.U*
```

Finally, having done much exploration, we looked again at Gao Guoming's method, from which we obtained the following way to eliminate the virus and vaccinate against it. The specific steps are as follows (using DOS 2.00, where the A: drive is the example):

1. Boot from a normal DOS 2.00 system disk (the normal disk should first be write protected);

2. From A:, call up DEBUG: A>DEBUG;

3. Read the boot sector of an infected disk into RAM: -L 10 0 0 0 1;

4. Look at the final 16 bytes of the boot sector to see whether it is infected. If normal, you will see in the display to the right such things as 'COM'; -D 2F 0 2FF;

5. If truly infected, look at the contents at bytes 2F9 and 2FA to calculate the sector numbers corresponding to the original normal boot sector. Done this way, 2FA has the high eight bits, while 2F9 has the lower eight bits, and from this you will get a four-digit hexadecimal value, to which you add 1 and consider as 'b';

6. -L 1 0 00 b1;

7. Look at the contents of sector number 'b' to see whether it is truly a boot sector, -D 2F 02 FF;

8. If so, set the value 5713 at 2FC 2FD to add the vaccination marker, -E 2FC 5713;

9. After determining that the boot sector is correct, do a write-disk operation, -W100 0 0 1;

10. -q.

By this time, the virus will have been eliminated and you will have put into place a function protecting you from the Ping-Pong virus. After rebooting the system, use PCTOOLS to view the system and ensure that the virus has truly been eliminated from the system. We used this method to fundamentally eliminate the virus from all infected disks.

It is important to note that:

1. When 'b' is not the correct boot sector, you may not proceed as described above.

2. If you use this method on falsely attributed bad sectors not yet recovered, you will not necessarily find all the boot sectors.

3. While on this subject, if you start the machine with a normal system disk, you will not be disturbed while running the system by the virus display.

4. The following figure compares a normal boot sector with the contents of the virus boot sector:

## Virus Diagnosis, Treatment Software

*90CF0128J Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 39, 11 Oct 89 p 56*

[Article by Di Yulai [3695 3768 0171]: "Diagnosis and Treatment Software for Computer Viruses"; refers to information window on page 58]

[Text] According to current reports from relevant sources in China, the virus most commonly affecting IBM PC XT computers is the "small ball" virus. The symptoms of computer systems that fall prey to infection by this virus appear as: a ball-shape that moves around on the screen, regular programs cannot continue executing, printers then engaged in printing interrupt their

printing, and in particular, it is possible that computer local-area-networked systems will suffer harmful consequences.

To diagnose and treat this virus, the Computer Department of North China Jiaotong University has developed a computer virus diagnostic and treatment package for the IBM PC XT series and their compatibles, within which package are three programs: for virus diagnosis and detection, for virus inducement, and for treating and vaccinating against viruses. In less than 1 minute, a disk can be checked for the existence of a virus, and can then be treated; after treatment, the disk will never again be infected by that virus.

## New Series of Anti-Virus Programs

*90CF0128K Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 39, 11 Oct 89 p 56*

[Article by Min Ji [7044 6060]: "Wonder Drug for Computer Viruses—the Youlong [1429 7893] Series of Anti-Viral Programs"]

[Text] The Planning Commission Information Center of the city of Sanming in Fujian Province has analyzed many computer viruses, studying such computer-virus processes as booting, transmission, activation, and disabling effects [see JPRS-CST-89-024, 1 Nov 89, p 15] and they have come up with the "Youlong Series of Anti-Virus Programs." These anti-virus programs can counter such benign and malignant viruses and "cold" viruses prevalent in China as the Small Ball Virus, the File Virus, and the Hard Disk Virus.

Benign viruses are offensive viruses, but they do not damage the data on computer systems; the viruses simply interfere with the man-machine interface. For example:

When the Small Ball Virus is triggered, it appears as a small bouncing ball. Malignant viruses do damage and can destroy data in computers or on floppy or hard disks. The Cold Virus has a malignant nature, but does not damage anything.

When the Hard Disk Virus is triggered, the system that is currently running is not affected, but on the next booting of the system, the hard disk becomes useless, and the boot goes into ROM BASIC.

## Guarding Against Virus Spread

*90CF0128L Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 39, 11 Oct 89 p 58*

[Article by Lao [0525]: "Beware of the Spread of Computer Viruses"]

[Text] Note: Computer viruses have appeared in many places in China, and they have come under close scrutiny by many computer personnel. On the one hand, these personnel have analyzed and eliminated viruses (but that virus elimination still greatly worries users since it is only a holding action), and after that analysis have also developed vaccination programs corresponding to the different viruses, which is an active prevention measure. On the other hand, they have attacked the channels of transmission of the viruses through administrative or organizational means, and in this respect, Shanghai leads the way. They have made an excellent attempt, which can serve as an example for other cities and units. Coincident with this, the Shanghai methodology poses a question for us, namely, should we establish a national organization for the prevention and eradication of computer viruses, or should we formulate pertinent laws to protect the interests of the computer-using public? [End of note.]

One after the other, Shanghai computer users have been discovering computer viruses, a trend that continues to evolve. To this end, the Shanghai Municipality Electronic Information Systems Office of Applications Dissemination and the Municipality Bureau of Public Security have jointly issued communications requesting all concerned units to look closely into the transmission of computer viruses.

It is understood that among viruses already discovered in Shanghai, the majority are propagated among IBM PCs and compatibles. The virus will appear at a certain time during the execution of a program, at which time a spot of light will bounce around on the screen, which reduces the processing speed of the current program. Although it has not been discovered that this virus damages original data, the virus is capable of self-replication. The bulletins point out common ways for viruses to invade systems: through use of floppy disks contaminated outside the immediate environment; through use of infected computers brought in from elsewhere; and through electronic communications over computer networks. Blocking these paths of virus propagation is an effective way of preventing invasion by virus. In consideration of this purpose, the bulletins request that all computer users: 1) diligently inspect microcomputers and floppy disks used within this organization system to determine whether virus infection has occurred. Measures should be taken for those microcomputers and disks that have been infected, they should be isolated, the virus should be eliminated as quickly as possible, and the source of the virus should be sought; 2) write-protect all system disks and important application software that has not been infected, then carefully archive these, pay attention to their storage, and unless they are distribution disks, never use floppies to boot a hard disk; 3) be careful in the use of public and shared software, never run programs whose origins are unclear, do not arbitrarily copy software from other people, and do not carelessly use software (including the many game software programs) from other machines on microcomputers within this system.

The bulletins particularly request retailers in Shanghai to be responsible for the hardware and software products

they sell, ensuring that they never contain viruses. To most quickly deal with the situation regarding the propagation of computer viruses in Shanghai, to aid in adopting measures, and to effectively treat, detect, and eliminate computer viruses, a computer virus "epidemic information" reporting system has been set up in Shanghai. As soon as users discover viruses, they should immediately make these reports through the levels of the administrative system. Regarding prevention and treatment, detection, and elimination of computer viruses, each unit should communicate with others whatever good experience, methods, and techniques it has, as well as any good suggestions.

## More Virus Detection Software

*90CF0128M Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 39, 11 Oct 89 p 58*

[Article by Lin Jieheng [2651 2638 3874] and Zhao Lijun [6392 0448 6511], Department of Computing, North China Jiaotong University: "Software for the Rapid Detection and Elimination of Viruses"]

[Text] During May and June of this year [1989] several IBM PC and 0520 microcomputers in our unit were discovered on several occasions to have one of two computer viruses. Characteristics common to both these viruses are: sometime after the computers have begun operation, a small light spot (diameter of about 1 mm) appears on the screen. The spot moves randomly about the screen, and as soon as it hits a Chinese character, it erases half of that character, or, the Chinese character will be entirely erased, which makes the computer impossible to use normally. But the two viruses have differences, too. The movement of the light spot for one virus traces the shape of a sine wave of various amplitudes, and it only erases Chinese characters. The pattern of movement of the light spot of the other virus has no regularity, and after it erases a Chinese character, it gradually leaves some small round dots (of about 3 mm diameter) stationary in an empty part of the screen. These dots are distributed irregularly about the entire screen.

After the appearance of the two viruses [known as Ping Pong and Ping Pong-B, respectively] just described, these phenomena only disappear if one turns off the machines and reboots. But after another period of operation, the virus can appear again quite quickly.

To eradicate these two viruses, we have now come up with special software, which has such functions as rapid detection (diagnosis) and elimination of these viruses. In less than half a minute, this program will give an accurate response in virus diagnosis of a floppy or hard disk: this disk "has a virus," or this disk "has no virus." This software is also fast when eradicating viruses from infected hard disks or floppies—it is done in 20 seconds.

## New Series of Virus Detection Tools

*90CF0128N Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 39, 11 Oct 89 p 58*

[Article by Xi Hongyu [1153 4767 1342]: "Beijing University Department of Mechanics Develops Series of Tools for Computer Virus Detection and Vaccination"]

[Text] Not long after the Department of Mechanics at Beijing University brought out tools by which users could detect, eliminate, and vaccinate against the common "small ball" virus and a shell-type "malignant" virus [see JPRS-CST-89-018, 22 Sep 89, pp 75-76], they have now also developed a series of "computer virus detection and vaccination tools" that can be used to detect some typical viruses already spreading abroad—such viruses as Brain, Lehigh, Marijuana, and dBASE. The threat from these viruses is quite great; most of them will destroy all files on a disk, and some have been designed to destroy data files. Some have a long incubation period (dBASE for example lies dormant for 90 days). These tools are interactive through a window menu display, which means the user need not have special knowledge; all he must do is follow the screen prompts for safe and convenient usage.

## Two New Viruses Reported

*90CF0128O Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 39, 11 Oct 89 p 58*

[Article by Peng Xiaoming [1756 2556 2494], Computer Laboratory, Air Force Radar Academy: "Two More New PC Viruses"]

[Text] The computer virus is a computer program that is powerfully destructive and infectious. Since their discovery in the United States, various viruses have been discovered one after the other throughout the world. Publications have even been reporting on these in China at present (the "round-dot" [or "Ping-Pong"] virus is epidemic on IBM PC's, XT's, and AT's). We, too, have recently come across two new PC viruses: "Chirper" and "Snowball." Their infectiousness and destructiveness are both in excess of and less than those characteristics of the "round-dot" virus.

The characteristics of the Chirper are: when it goes into effect, the speaker on the PC emits a continuous stream of noise of differing frequencies. We first discovered this in a PC laboratory of a college, where not long after students had begun working there, several computers came down with it one after the other. For a time, the eerie noise rose and fell, and was really quite dreadful. Like the round-dot virus, Chirper can greatly slow down the efficiency of a computer, and it is also quite infectious.

The characteristics of Snowball are: when the infected computer is turned on, the virus enters RAM together with DOS, and whenever a disk is read or written to, the virus is transmitted to this disk and a new free disk cluster will be occupied by the virus, then marked as a "bad" cluster. This is how Snowball gets larger and larger, until it has used all disk space. Because this virus has no obvious "triggering" characteristic (that is, no round dot will appear, nor will any noise), it is quite difficult to discover, and it is also quite destructive.

The transmission mechanisms for these two viruses are similar to that of the Round-Dot Virus, even to the extent of some of the code, and it is presumed that the

perpetrator has essentially modified the Round-Dot Virus. If you use whatever methods you use to deal with the Round-Dot Virus, they will have little effect. We have developed antibody software for each of these—the Round-Dot, Chirper, and Snowball. This software can accurately distinguish the different kinds of virus, then effect a radical cure.

## Treatment for Computer Viruses

*90CF0128P Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 40, 18 Oct 89 pp 66, 68*

[Article by Xie Xiaoquan [6200 1420 0356], Institute 706, Ministry of Aeronautics and Astronautics Industry: "The Treatment and Prevention of Computer Viruses"]

[Text]

### Prevention and Treatment

To date, there have not been developed any effective, yet general-purpose methods or products to prevent and treat computer viruses. This is due to the shared and transmitted natures of computer system information, as well as to the universality of information interpretation, all of which provide the conditions by which computer viruses are transmitted. There are many different kinds of computer virus, but there is currently no complete, systematic understanding of them, and existing methods and products to prevent and treat computer viruses are all addressed to computer viruses of a specific kind.

Prevention and treatment of computer viruses must first detect the existence of said viruses in the system. To determine whether a known program P is a virus, one must learn whether P is able to infect other programs, and this is a question that cannot be precisely determined. We use an ambivalent program example proposed by the noted scholar F. Cohen to explain this problem.

If we suppose a decision process D, when it determines that program P is a virus, it returns a value of "true" (that is, DCP = true).

```
Virus ambivalent program (CV) :=
{...
main routine :=
{if ~D (CV) then
      {execute "infect subroutine";
      if "trigger subroutine" returns a value
      then execute "damage subroutine";
      }
      goto next;
      }
      }
```

In this ambivalence program, if the decision process D decides that the program CV is a virus, then the "infect subroutine" is not run; that is, CV will not infect other programs, therefore CV is not a virus. Conversely, if D decides that CV is not a virus and CV does infect other programs, obviously, CV is, too, a virus, and these two conclusions both generate contradictions under the conditions of the decisions of the decision process D; therefore, a precise determination of the virus nature is not a question that can be determined.

In addition, F. Cohen has proposed four methods for the prevention and treatment of computer viruses from a theoretical standpoint:

#### 1. The Basic Isolation Method

There is information sharing in a system, and so there is the danger of virus infection. Eliminate information sharing, and the system will be "isolated," and viruses cannot propagate in via information from outside (naturally, neither can viruses within this system propagate out), and this isolation strategy is the most fundamental way to prevent and treat computer viruses. Obviously, too, it would not be easy for this method to catch on.

#### 2. The Excision Method

Based on the transfer relations of a particular information flow, users may be divided into closed sets or non-closed sets, all in close relation to this information flow. In this way, certain restrictions are adopted for the information flow, and, consequently, the system is correspondingly divided into individual unique subsystems. The virus, then, will not be transmitted between subsystems, but can only be transmitted within a particular subsystem.

#### 3. The Flow Model Method

Set up a threshold for distances traveled by the information flow, by which action a preventive mechanism can be erected using information that has exceeded a certain distance threshold, information that might possess a certain danger.

#### 4. Restricted Interpretation Method

No fixed interpretation model will become infected by viruses, but because its interpretation also uses write operation routines, it can become infected. For example, the microcode in a computer is fixed, but because it is interpreted by machine code routines, it can become infected. Therefore, a certain degree of immunization can be achieved by restricting the interpretation of the program statements.

Generally speaking, the methods used on microcomputers to prevent and cure computer viruses include the following: regular check of the length of executable programs and the date stamps to see whether they have changed; caution against computer game programs, programs that come from bulletin boards external to the

present environment, and electronic mail; a regular check of the interrupt vectors in the system; and monitor disk accesses.

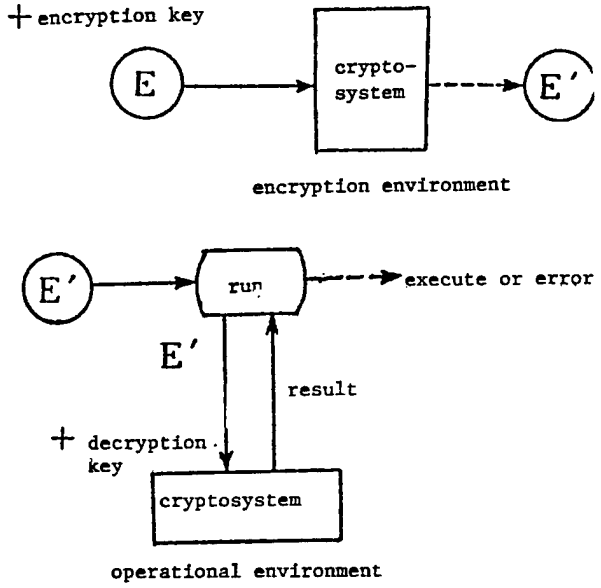
Computer viruses propagate through modification of executable files, and therefore, by protecting the integrity of information in executable files, one can discover and inhibit the propagation of viruses. There are two ways to prevent the modification of executable files: 1) provide executable files that do not permit any alterations; and 2) before a program runs, check whether this executable file has been modified. The first method can be implemented by storing executable files in read-only storage devices; for the second method may be used encrypted executable files, or, by checksums on record codes. We now describe the encryption and code-checksum methods separately.

### 1) The Encryption Method

By use of the encryption method, we can guarantee the information integrity of executable files, also using that fact to detect the propagation of viruses, and by which action we remove the potential threat of viruses. This is shown in the following diagrams:

The executable file E generates E' by means of the encryption system. During operations, E' is sent to the encryption system for decryption, after which it is executed to obtain the actual results. If the operation fails, this shows that the executable file has been modified after encryption. Therefore, executable files that are run-encrypted can reveal potential danger (whether or not the danger is a virus).

There are two considerations here: one is when all executable files in a system are without viruses and are



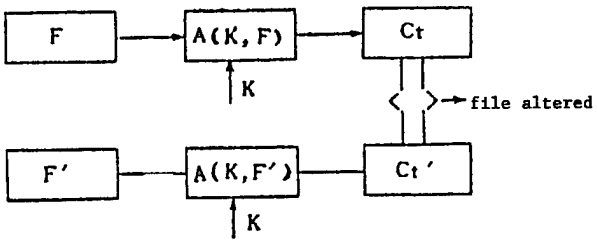

encryption-protected. When a virus is introduced that intends to infect executable files, this mechanism can detect that virus and suppress further danger from it; second, if before encryption a virus already resides within an executable file, this mechanism then cannot detect the existence of that virus. The virus will remain hidden, and as far as the effects are concerned, its behavior will be like that of the traditional Trojan Horse programs.

Use of this method depends upon which type of encryption system is selected, and especially upon the management of the encryption and decryption keys.

### 2) Code-Checksum Method

From the traditional point of view, using integrity mechanisms to protect information will avoid the illegal creation, deletion, and modification of that information. The code-checksum technique is used to determine the integrity of information for which a protection mechanism has not been established.

Code checksums are generated from interaction between a user key (KD) and the information file, where by checking the code checksums for equality before and after use, the integrity of the file information can be checked. This is shown in the diagram below:




Under a key K, apply the discrimination algorithm A(K,F) to the legal file F, generating a checksum Ct, by which one can know that it is an image at time t and algorithm A(K,F) under F. After a certain amount of time, one may consider F as F', at which time use the algorithm A(K,F') under key K on F' to generate the checksum Ct'. If in a comparison of Ct and Ct', the two are not identical, this shows that F has been modified, that is, it is possible that it has been infected by a virus.

The characteristics of the code-checksum method are: it must be comparatively easy to derive Ct from (K,F); it is very difficult to derive K from the acknowledged (F,C); when there is no K, it is also very difficult to solve for a code checksum Ct' for a non-acknowledged file F' from the acknowledged (F,C); to be useful, the length of the code checksum Ct must be less than the length [F ]of file F. That is:

(F,K) $\rightarrow$ Ct is easy, but Ct $\rightarrow$ F', F $\rightarrow$ K, F $\rightarrow$ Ct, Ct $\rightarrow$ F, Ct $\rightarrow$ K, and (F,Ct) $\rightarrow$ K are difficult.

What we mean here by "easy" is that by using a known algorithm, we can accomplish this task within a reasonable amount of time, and by "difficult" we mean that there is currently no known algorithm of this sort, which means that we cannot solve this problem within a reasonable amount of time.

The code-checksum method can be based upon the RSA [Rivest-Shamir-Adleman] encryption system for repeated implementation of encoding. To this end, the RSA encryption system acts as a random number generator.

**Conclusion**

Methods for developing effective and convenient prevention and cure for computer viruses will be a major direction for development in research on computer viruses. At present, people have come up with three "vaccines" for computer virus prevention and cures: one keeps viruses from invading a computer system, a second can detect a virus vaccine in a system, and the third can eliminate the virus vaccine from a system.

People have also conceived of mechanisms in compilers and assemblers to prevent and cure computer viruses, which would enable the executable programs so generated to have anti-virus capabilities.

On the legal front, laws should be established regarding the computer virus problem, and this would also be an effective protection against the propagation of computer viruses. Work has begun on this abroad, and China should also make an effort to set up relevant rules and regulations to prohibit the creation and propagation of computer viruses.

## Can Ping-Pong Virus Harm Floppy Drives?

*90CF0128Q Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 41, 25 Oct 89 p 28*

[Article by Gao Guoming [7559 0948 2494], Computing Center, Southwest Aluminum Processing Plant: "Does the 'Round-Dot' Virus Harm Floppy Disk Drives?"]

[Text] The Round-Dot Virus that is currently epidemic definitely does not harm floppy disk drives, nor does it harm disks. But it can create the false impression of having damaged a floppy drive or disk, which has led to misunderstandings.

A colleague told me about the PC-compatible, with two floppy drives, which his unit had just bought. Computer viruses had already invaded their computer system, but they had no way of knowing this. Consequently, when they were formatting system disks, they discovered that the formatted system disks always failed to boot, and they exchanged these disks for new ones, but the outcome was always the same for both drives A: and B:. His colleagues then suspected that the problem was floppy-drive damage, and they put in a third new drive, with identical results. They later decided that perhaps the problem was that a virus had damaged the floppy drives, which was then damaging the floppy disks.

What follows is an analysis of how the Round-Dot Virus could have caused the problems just discussed.

When a computer system is infected with the Round-Dot Virus and the FORMAT /S command is run, the following situation occurs. The formatting process consists of first initializing the entire disk, then writing the disk boot module into sector 0 [this should be "sector 1"] of side 0 (on the floppy), after which it goes on to initialize the File Allocation Table (FAT) and the file directory area. If there was the trailing '/S' parameter, then the FAT and file directory are read in preparation for storing the system files: IBMBIO.COM, IBMDOS.COM, and COMMAND.COM. It is when reading the disk operating system, before IBMBIO.COM is written, that the virus begins part of its activity. It first writes the second part of the virus and the normal boot sector into the first cluster of the file area—sectors 0Ch and 0Dh, and then the first part of the virus is written to sector 0 side 0. Only after this can it write IBMBIO.COM, and as everyone knows, there are several conditions for a DOS system disk boot to be successful, among which is that IBMBIO.COM must be written into the first contiguous sectors of the first cluster in the files area before the system can boot normally.

By analyzing the process just described, it will be easy for people to see why there is a false appearance of damage to floppy drives and disks. We now look at the way to run the FORMAT /S command normally while within a virus environment, and this is also a way to eliminate the virus.

Whether or not the current system has a virus, the following command can always be executed to format a single-sided system disk.

A>FORMAT B: /S/1 <enter>

After successful formatting, this single-sided system disk will not have a virus (and this is not limited to a particular DOS version). Rebooting under the new system disk, there will no longer be a virus in RAM, and at this time, the FORMAT /S command can again be used to format a system disk; this disk will not only boot successfully, it will also be without the virus.

This is because the Round-Dot Virus does not infect disks that are formatted with fewer than two sectors per cluster. That is why, if a disk formatted in accordance with the method just described can boot, that proves that the floppy drives and disks are all right. Please note, too, that there is a 3M floppy disk currently on the market that has mildew spots. If one is not careful using those disks, it is possible to soil the drive heads, which would keep the drives from working properly. If this proves to be the case, you can use a cleaning disk to cleanse the heads two or three times, which will restore the drives to normal condition. This is not the same situation as the virus phenomenon, so please treat each differently. It is also recommended when using new diskettes or diskettes that have been stored for a long time, please check

carefully for signs of mold. This could avoid dirtying the drive heads and affecting normal operation.

## Getting Rid of Game Viruses

*90CF0128R Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 41, 25 Oct 89 p 28*

[Article by Xiao Ping [5135 1627], Finance Department, China State Shipbuilding Corporation: "Using LOWFORM.EXE To Eliminate Viruses From Microcomputer Games"]

[Text] The Chinese-character printer driver 3.COM and 24X24 dot-matrix print font library CLIB24 were just as always in the 0520C-H hard-disk directory, but when 3.COM was run, it displayed the message: "There is no font library file C:CLIB24, so you cannot use this module." There was therefore no way to print Chinese characters, but other operations were all quite normal. Not only did we not discover any trouble when running the diagnostic program DIAGSTAR.COM, but whether we recopied 3.COM and CLIB24 from prepared back-up disks or changed their positions on the hard disk, or recopied GWBIO.COM, GWDOS.COM, COMMAND-.COM, and GWINT16.COM, or even used FDISK.COM and FORMAT.COM to repartition and reformat the hard disk, we still had that trouble. This was a problem that occurred universally on IBM PC, XT, AT, 0520C-H, and compatibles after certain game programs had been run (editor's note: among viruses that have been discovered to date, most have had to do with game software).

The problem just described occurred after this particular computer had run the game "Ball" (B.EXE on the games disk), and then occasionally during copies to the hard disk from the floppy or when running GWINT16.COM, the ball from the game would suddenly appear, bouncing back and forth on the screen. It had no effect on English text, but when it struck Chinese characters it would be like in the game where the graphics square "eats." At these times, the computer would operate normally, but when the ball had appeared, it would never go away, and even CLS could not get rid of it—there was only the reboot.

Because of the eccentricity or playfulness of the problem just described, the chance appearance of the game ball, and the "stronger" nature of its activity after its appearance, we had no choice but to call it a "virus." After analysis, we could see that while executing, the game would do some writing in the hard-disk boot sector record, which caused an error during the check on the existence of 3.COM and CLIB24. It also wrote the virus program into sector 17, side 0, track 410 of the hard disk (we used the MAP address image function of PCTOOLS to see that this was marked as a bad disk portion), and then during certain operations, the virus would be triggered...

We used the random cylinder hard-disk physical formatter LOWFORM.EXE to resolve our problem, by which we got rid of the game virus.

Our method was as follows:

1. A>LOWFORM

1) Drive no. (1-2): select 1;

2) Interleave (2-9): select 2;

3) Among the 12 hard-disk models presented, select 1 (i.e., Miniscribe 3438, NEC5126); the capacity of this disk is 30 megabytes;

4) Select cylinder: 615, head: 4, sector: 17;

5) Split into 2 logical units? (Y/N), select N (just one unit);

6) Enter drive defect table? (Y/N), select Y;

7) Press <ESC> to quit output;

8) Press Y to begin physical format.

2. A>FDISK, select 1 to set up one unit;

3. A>FORMAT C: /S/V

4. A>COPY A:*.* C: to copy the system disk onto the hard disk.

At this point, you may boot the hard disk, and the computer will have returned to normal.

## Disinfection Measures From Fujian

*90CF0289A Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 43, 8 Nov 89 p 2*

[Article by You Long [1429 7893]: "Fujian Province Computer Society Does Full-Scale Survey and Research on Measures for 'Disinfection'"]

[Text] The Fujian Province Computer Society has been commissioned by the Province Office for Electronics Promotion and the Provincial Bureau of Public Security to undertake a province-wide survey of the situation regarding computer viruses, to gather and study methods of eliminating viruses, and to assist appropriate units with their disinfection. Their survey showed that: 1) through numerous specialized technical seminars held by the Computer Society, a majority of users have come to a basic understanding of how to distinguish and prevent viruses, and the "small ball virus" that has spread throughout the country during spring and summer has been largely brought under control; 2) the various viruses that have thus far been discovered have been benign or "cold viruses," failing to maliciously damage the computer system. But there are still some users who have not gained this knowledge of viruses, and who are reformatting disks as a way of eliminating viruses, which wastes a lot of manpower and funds; 3) some management users are emphasizing education in

professional morality among personnel in the computer lab, are restricting booting of systems from floppies brought in from outside, are not permitting the playing of computer games, and are rationalizing the allocation of hard-disk resources, and have thereby escaped the virus invasion; 4) it is worth noting that a significant number of users let it be known that their computers have become infected from floppy disks brought in by college interns. The survey also discovered that some students have created new viruses by altering the "small ball virus" triggering procedure. Infection symptoms are sprouting up all over the place, some even capable of great damage to hard disks. For this reason, there has been a loud cry to pertinent departments for stronger monitoring, and to formulate pertinent policies and rules by which to restrict troublemakers from intentionally introducing, creating, and disseminating viruses.

Recently, the group in the province Computer Society that worked on virus analysis has developed an "XY-Class Virus Prevention and Cure Program"; this program can completely treat and prevent such "boot record viruses" as the "small ball" and the "hard-disk" virus that originate in a hard-disk boot record [i.e., leader record]. The successful development of this program is an attack technologically on the curious and irresponsible who would create viruses, and it will have a positive influence on the effective prevention and control of viruses.

## Virus Discovered at Medical University

*90CF0289B Beijing RENMIN RIBAO [PEOPLE'S DAILY] in Chinese 15 Dec 89, Overseas Ed., p 4*

[Article by Zeng Liming [2582 0448 2494]: "University in Beijing Discovers Computer 'Virus'"]

[Text] Some of the PCs and Changcheng [i.e., Great Wall] 0520-CH computers at Beijing Medical University recently experienced problems. It was determined after evaluation by experts that they had become infected by the "small ball" computer virus.

This computer virus is actually a program, one that can store itself inside another program, repeatedly replicating then disseminating itself, until finally it has infected other programs. This process, then, is just like a virus replicating itself within an organism until it appears to have caused an illness, which is why people call them viruses.

The one that has appeared in Beijing Medical University computers has also appeared in many institutions of higher learning and research departments throughout Beijing. As the experts tell us, this "small ball" virus primarily infects 8086 and 8088 CPU microcomputer systems, and when the virus is triggered, problems occur with the screen. When this gets serious, the machine locks up.

According to statistics, the "small ball" virus has been discovered at all prefectural, municipal, and provincial bureaus of statistics in the jurisdiction of the Bureau of Statistics for 21 provinces and municipalities. This situation has attracted the close scrutiny of computer circles in China. Concerned specialists are warning computer managers and users to be careful and to take effective preventive measures, and they have developed countermeasures. They are now writing various programs for users to detect, eliminate, and vaccinate against viruses.

## Virus Analysis/Automatic Processing System

*90CF0289C Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 50, 27 Dec 89 p 2*

[Article by Zou Hai [6760 3189]: "A 'System for the Analysis of Computer Viruses and the Automatic Handling Thereof' Achieves High Acclaim From Experts"]

[Text] A "System for the Analysis of Computer Viruses and the Automatic Handling Thereof" that can do rapid and accurate diagnosis of the Ball computer virus, as well as eliminate it, has been successfully developed by the Office of Computers at the Jiangxi Publishing Bureau. It recently passed a technical evaluation arranged by the Jiangxi Science and Technology Commission, when it received high praise from experts.

This system uses the means by which the virus replicates and spreads itself, and gets rid of the virus with the principle of "fighting fire with fire." The system sets up a uniform format with a disk cluster number and sector numbers, offering a "three-point determination" diagnostic scheme, and providing an excellent full-screen menu-driven user interface. Much of the thinking and implementation algorithms that went into the design of this system are of a high standard. The system runs on IBM PCs and compatibles.

## Ping-Pong Virus Eradication

*90CF0289D Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 50, 27 Dec 89 pp 52-54*

[Article by Zhao Shuaimao [6392 3764 0602], Henan Province, Office of Coal: "Three Steps Toward Getting Rid of the Round-Dot Computer Virus"]

[Text] There are at present many different ways to prevent the spread of computer viruses or to eliminate them, but some among those ways simply keep the virus program from being triggered again, thereby having no vaccination function; if one is just a little careless, there is still the possibility of reinfection. And some methods do not recover the space from the two boot sectors that had been occupied by the virus. The bad sector mark that can be seen using the MAP command of PCTOOLS can give a person the feeling that some mistake has been made.

In my opinion, the following three steps should be taken in dealing with the computer round-dot virus:

1. Recover the proper boot record (namely, the disk boot sector);

2. Add vaccination, so that after this process, neither a hard disk nor a floppy disk will be reinfected by this particular virus;

3. Recover the two boot sectors that had been taken over by the virus (that is, alter the FAT [File Allocation Table] entry of 'FF7' to '000').

Here are the methods for diagnosing and treating the virus:

**I. Determination of the Existence of a Virus (Diagnostics)**

Diagnosis of the existence of a virus can be accomplished with either DEBUG or PCTOOLS, as both can be used to examine disk mapping and to check for differences in boot records. Using the PCTOOLS MAP command, you will see the bad sector sign 'X' on disks that have been infected, but this marker is not in a set position (that is, there has been no set time that the disk has become infected). A mapping of an infected disk is shown in Figure 1; that for an uninfected disk is shown in Figure 2 (it is the map of the infected disk, but after elimination of the virus).

The following notes involve DEBUG for diagnosis and treatment. It is also possible to use PCTOOLS, but that is not covered here.

You can see using DEBUG that there is a great difference in the last 128 bytes of the boot sector between an

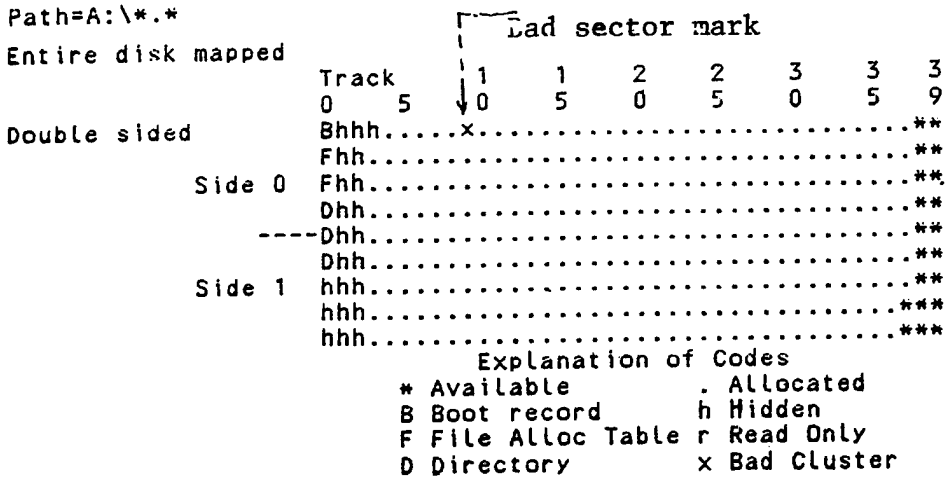



Figure 1

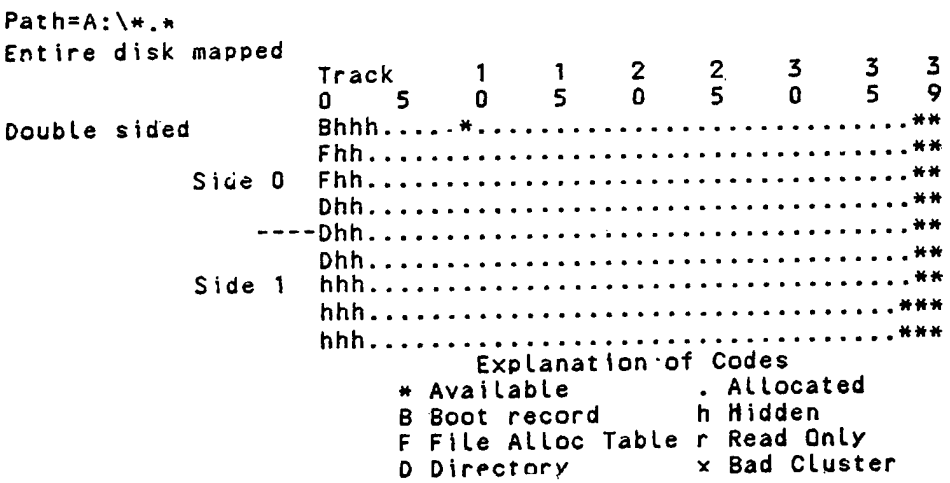



Figure 2

infected and an uninfected disk. This technique does not require reading assembly-language code. To use it, insert a disk having the DEBUG.COM file into drive A:.

A>DEBUG

-L 100 0 0 1 (here, the DEBUG L command reads the disk boot sector into RAM)

The ASCII portion of the last 128 bytes of an uninfected disk has some readable English text (later versions of DOS will have more than 128 bytes like this), but the ASCII portion of the final 128 bytes in the boot sector of an infected disk will have random symbols.

The final 128 bytes of an uninfected boot sector is shown in Figure 3 using the D command.

Figure 4 below that shows the last 128 bytes in the boot sector of an infected disk.

Looking closely, we can see that the hexadecimal code of bytes 506-508, among the 512 bytes in the boot sector (the boot record in sector 0), gives the location of the sector number containing the virus code. Bytes 509-510 contain the symbol for the round-dot virus—'1357'. During the transmission process for this virus, it is first determined whether this '1357' exists on a particular disk. If there is none, the boot sector is first modified, then a portion of the virus code is moved together with the original boot sector to the first free sector on the disk, when the "bad sector" indicator 'FF7' is added. This is to ensure that later data will not cover over the data in this sector.

Therefore, if you can determine in which sector is the virus, then the next sector will be the proper boot sector. In the example above, the virus code is in sector A2H ('H' signifying hexadecimal numbers), so the proper boot sector number is A3H (i.e., A2 + 1 = A3).

**II. Methods of Treatment**

After it has been determined that a virus exists, DEBUG can then be used in the following manner:

1. To recover the proper boot sector;

2. To install a vaccination marker.

We will continue to use the infected disk discussed above as an example. Since we already know that the sector number of the proper boot sector is A3H, we can use the L command to read that sector into RAM, where we change the two bytes at 509-510 to read '5713' (this is actually the value '1357', but in this computer the high byte follows the low), and then finally we use the W command to write the contents of this sector into sector 0 (that is, we overwrite the boot sector that has had the virus). Steps of this operation (while at the computer):

A>DEBUG

-L 1000 A3 (read the contents of the proper boot sector into RAM from sector A3H)

-E2FC

0F00:02FC00.5700.13 (modify the bytes at 509-510 in this sector to be '5713', which is a vaccination mark)

-W100001 (write this sector into sector 0)

3. Recover the usable space from the two sectors occupied by the virus

```
-D 280 2FF
0F00:0280  0D 0A 4E 6F 6E 2D 53 79-73 74 65 6D 20 64 69 73   ..Non-System dis
0F00:0290  6B 20 6F 72 20 64 69 73-6B 20 65 72 72 6F 72 0D   k or disk error.
0F00:02A0  0A 52 65 70 6C 61 63 65-20 61 6E 64 20 73 74 72   .Replace and str
0F00:02B0  69 6B 65 20 61 6E 79 20-6B 65 79 20 77 68 65 6E   ike any key when
0F00:02C0  20 72 65 61 64 79 0D 0A-00 0D 0A 44 69 73 6B 20    ready.....Disk
0F00:02D0  42 6F 6F 74 20 66 61 69-6C 75 72 65 0D 0A 00 69   Boot failure...i
0F00:02E0  62 6D 62 69 6F 20 20 63-6F 6D 30 69 62 6D 64 6F   bmbio  com0ibmdo
0F00:02F0  73 20 20 63 6F 6D 30 00-00 00 00 00 00 00 55 AA   s  com0.......U*
```

**Figure 3**

```
-D 280 2FF
0F00:0280  A3 F5 7D 8B 36 F9 81 E9-08 01 C3 81 3E 0B 80 00   #u}.6y.i..C.>...
0F00:0290  02 75 F7 80 3E 0D 80 02-72 F0 8B 0E 0E 80 A0 10   .uw.>...rp.... .
0F00:02A0  80 98 F7 26 16 80 03 C8-88 20 00 F7 26 11 80 05   ..w&...H8 .w&...
0F00:02B0  FF 01 BB 00 02 F7 F3 03-C8 89 0E F5 7D A1 13 7C   ..;..ws.H..u}!.|
0F00:02C0  2B 06 F5 7D 8A 1E 0D 7C-33 D2 32 FF F7 F7 F3 40   +.u}...|3R2.ws@.
0F00:02D0  F8 80 2e F7 7D FB 3D F0-0F 76 05 80 0E F7 7D 04   x.&w}{=p.v...w}.
0F00:02E0  BE 01 00 86 1E 0E 7C 4B-89 1E F3 7D C6 06 B2 7E   >.....|K..s}F.2~
0F00:02F0  FE EB 0D 01 00 0C 00 01-00 A2 00 00 57 13 55 AA   ~k.......".."W.U*
```

Virus mark

Sector number in which virus resides

**Figure 4**

Knowing the sector numbers where the virus routine resided, we can use a formula to convert the bad sector mark 'FF7' in the corresponding position of the FAT.

The conversion formula is as follows:

360KB floppy: S = 2C + 8

10-megabyte hard disk: S = 8C + 33

20-megabyte: S = 16C + 49

(S is the sector number, C the cluster number)

And we already know that the virus is at sector A2H:

A2H = AX16 + 2X16 = 162 (convert hexadecimal to decimal)

C = S-8/2 = (162-8)/2 = 77 (calculate the cluster number from the sector number)

77X1.5 rounds to 115, which is 73h (round the cluster number after multiplication by 1.5, then convert to hexadecimal)

73h + 100h = 173h (because when loading into the FAT, this is generally done beginning at 100h, so 100h must be added for accuracy)

-L100012 (call the FAT sector into RAM)

-E173

0F00:01737F.0FFF.00 (use the E command to modify the two bytes beginning at 173, remembering that the high and low bytes are reversed; at completion of this adjustment, the 'FF7' has changed to '000')

-W100012 (write to disk the modified FAT, noting that the command parameter is identical to that of the L command)

With completion of the steps just described, use the DIR command to see that 1,024 bytes of free space have been added to the disk.

The preceding discussion has referred to floppies, but the procedure is the same for a hard disk, the only difference being the use of a different drive designation. For editions of DOS at 3.1 and below, this procedure will work for all users.

## Interview With Anti-Virus Programmer

*90CF0289E Beijing KEJI RIBAO [SCIENCE AND TECHNOLOGY DAILY] in Chinese 31 Dec 89 p 4*

[Article by Li Jian [2621 1696]: "The Good Doctor for Eliminating Computer Viruses"]

[Text] Since the world discovery of computer viruses in 1986, hundreds of thousands of computers have been invaded by them. At the end of last year, some units in China also began discovering computer viruses, causing work at many computers to be disturbed and much material to be mysteriously damaged. This has led to discussions of virus variations among computer operations personnel, and some newspapers have alarmedly warned of computer viruses spreading throughout China. For a while, the situation was quite tense. But people can now relax a little, for Lecturer Xi Hongyu of the Department of Mechanics at Beijing University has isolated two kinds of computer virus among those that have been discovered in China, and he has written programs to detect and to vaccinate against these viruses. To stop an epidemic and further spread, the Department of Mechanics at Beijing University has recently decided to provide the virus detection program free of charge to anyone. It was for that reason that I especially wanted to interview Xi Hongyu, the author of this program.

Xi Hongyu is from Changzhou in Jiangsu Province, quite youthful in appearance, and he is a graduate of this Department of Mechanics.

"Our department was formerly called the 'Department of Mathematics and Mechanics,' and I was primarily a math student. I regularly used computers as a student, and so after graduating, my chief interest turned in that direction."

He having brought up the subject, I could not help but address the topic at hand: "What are these computer viruses, anyway?" He replied: "Computer viruses are actually programs written by people, but they have two particular functions. One is that they can automatically reproduce and propagate themselves, and the other is that they can disrupt the normal operation of a computer; the ill-intentioned ones among them can be quite destructive indeed. Some are such that on a certain day they will suddenly destroy all directories; some will only damage files after several incidents of infection; with still others, as soon as your computer becomes infected, a line of text appears: 'The most wonderful thing has happened: your computer has been taken over by a virus.' Some people have linked a virus to their names, and as soon as their name clears, the virus begins to work. On 3 November [1988], the U.S. ARPANET computer network was attacked by viruses with the result that more than 6,000 terminals and networked computers in the Pentagon and NASA could not work. The United States dispatched thousands of computer specialists, who spent several days before they could get the computers working again, and direct losses alone reached millions of dollars."

It would appear that whether involving national-defense construction or scientific research, there is great danger from these viruses. So, how did they come about?

"As far as the idea is concerned, that began during the mid-1970's. In 1975, a science fiction story was published in the United States called "The Attack-Wave Knights," in which this idea occurred. In the early 1980's, the concept of computer viruses began to appear. And in 1986, two Pakistani youths made the first virus because their software was being regularly pirated by

others. That was a malignant virus, capable of destroying an entire directory of files, or even trashing all files completely. There was another that was benign, as it would only make a mark on your disk and some extraneous patterns on your screen, not generally damaging your files. But it did take up time on the computer."

What about the viruses discovered in China—were they harmless or pernicious? This undoubtedly is of great concern to computer users.

"There are both kinds. But the two now found most often have been isolated, and we have made programs for detection, recovery, and vaccination; we can even recover some of the files that are damaged. There are no signs on these two viruses, and we cannot tell where they were created. But all signs are that they were brought in from abroad, as they are not like things done here."

That infected machines and disks can be cured and protected will certainly bring relief to people, so the situation is good after all. But what about the viruses that have yet to be discovered and for which we have no means of protection—can we avoid infection by them?

"Infection by a virus is primarily through networks and disks. It is seldom that discovery can be made as soon as infection has occurred, and the just-infected machine can become a new source of infection. It is therefore best to not use software of uncertain origins, and when running software on the computers of others, it is best to place write-protect tabs on one's own disks. In addition, from the point of view of the state, we should come up with software laws as quickly as possible, by which we could both protect the copyrights of software authors, and also clearly prohibit the creation and transmission of damaging software."

Finally, he quite pointedly told me that "Without the rule of law, we cannot fundamentally solve this problem." I believe that what he said is quite true and quite worthy of our attention.

## Additional Antivirus Measures, New Virus Reported

### Ball Virus Diagnosis/Treatment Software Package Released

*90CF0336A Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 4, 24 Jan 90 p 18*

[Article by Shi Bingkun [4258 3521 0981]: "Ball Virus Diagnosis and Treatment Package"]

[Text] The computer department of North China Jiaotong University recently released the Ball-Virus Treatment and Diagnosis Software Package for the IBM PC/XT series and their compatibles, to deal with a computer virus that is now widespread.

The software package consists of four programs: a "virus diagnosis" program, a "virus activation" program, a "virus treatment and inoculation" program, and a "comprehensive diagnosis and treatment" program.

**1. The Virus Diagnosis Program**

This program checks floppy-disk or hard-disk drives A, B and C to determine whether they have been infected with the virus. If the computer displays the message "NO" and beeps, then the disk has been infected; if it displays the message "OK" and does not beep, the disk has not been infected.

**2. The Virus Activation Program**

This program is used to check computer systems while in operation. When this program is run, if the screen displays a bouncing ball or flashes, the virus has been induced to become active, indicating that the boot disk (floppy disk or hard disk) carries the virus and has introduced it into the computer system: thus it may flare up at any time and the system disk must be disinfected before it can be used. If the system crashes or the above images do not appear on the screen, then the boot disk does not carry the virus.

**3. The Virus Treatment and Vaccination Program**

A DOS system disk free of the virus is used to reboot, and disks that have been shown by the above two programs to carry the virus are then disinfected and vaccinated. The screen displays the message "Disk to be disinfected"; the user must insert the appropriate disk and enter the drive number (A, B, C or D). The virus will then be eliminated from the disk. Disks with DOS version 2.X can be vaccinated, making them immune to this particular virus; disks with DOS version 3.X can be disinfected but cannot be vaccinated. Disks that are not infected should not be treated with the program.

**4. The Comprehensive Diagnosis and Treatment Program**

This software immediately checks the disks in drives A, B and C of any IBM PC/AT or compatible and displays a message indicating which disks, if any, carry the virus. In IBM PC/XT's and compatibles the program indicates only whether or not the system contains the virus.

In either type of PC, the program eliminates the virus from internal storage and becomes resident until the computer is turned off. Operation of other programs is not affected when the program is resident.

### 'Computer Virus Doctor' Software Released

*90CF0336B Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 4, 24 Jan 90 p 18*

[Article by Gao Yuqian [7559 3022 0051]: "'Computer Virus Doctor' Version 1.10 Software Released in Shanghai"]

[Text] Frequent invasions by computer viruses have come to the notice of the authorities. In Shanghai, in

addition to special notices requesting units with computers to report any outbreaks of viruses to the relevant offices, active measures have been taken to protect against and eliminate viruses, and methods for doing so have been disseminated to all users. The "Computer Virus Doctor Version 1.10" software developed by the Shanghai Shaped Steel Pipe Works has come into wide use in the system subordinate to the Shanghai Metallurgical Office, and has produced noteworthy results.

Directed against the main computer viruses now spreading, this software, written in assembly language, combines diagnosis, treatment and vaccination. It is capable of identifying, treating and vaccinating against the "ball (round-dot) virus"—the most prevalent domestic type—as well as the Stone virus, in IBM PC's and compatibles. The ball virus creates a bouncing ball on the CRT display; the Stone virus displays no outward symptoms, but damages parts of the FAT [file allocation table] and FDT [function description table], causing serious loss of software or data. The software can also treat the Pakistani Brain virus. It is capable of diagnosing the Brain virus rapidly; in addition, it outputs a warning in the case of suspect disks on which the virus cannot immediately be diagnosed. When a disk has been diagnosed as carrying the Brain virus, the Stone virus or the ball virus, the software asks whether the virus should be eliminated, and if so instructed, it selects the appropriate program and eliminates the virus from the disk. In the case of floppy disks that have been found to be free of the virus, the software immediately outputs the message that the disk is a virus-free PC-DOS disk. The software can vaccinate your disk against the standard ping-pong ball virus. On-the-spot diagnosis of user disks brought to applications training classes has produced excellent results. The developers state that they are continuing research in order to expand the range of viruses that can be diagnosed and eradicated and to provide better user service.

## Malignant Virus Reported by Second Artillery Corps Unit

*90CF0336C Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 4, 24 Jan 90 p 18*

[Article by Li Zhaolin [2621 0340 2651]: "Another Malignant Virus"]

[Text] Recently, a unit of the Second Artillery Corps found that the hard disks of seven of its IBM PC/XT computers or compatibles with DOS 2.X operating systems could not be made to operate normally except after booting with a floppy disk. Use of DEBUG.COM and PC TOOLS.EXE for a comprehensive examination of the hard disks indicated that the only abnormality was damage to the fifth sector of the FAT (but not the system boot sector), preventing normal use of certain software. But when they used a specially written program to read out the main boot sector, they unexpectedly discovered that it had been replaced by a different program. Analysis of this program indicated that it was a previously unknown malignant virus [called the "Marijuana" or "Stone" virus; see series of articles later in this special issue].

This very cleverly written virus took up only 420 bytes. The entire virus program inserted itself into the floppy-disk boot sector of the hard-disk main boot sector and copied the hard-disk partition table into the virus program. This improved its concealment, because DEBUG-.COM, FDISK.COM and similar hard-disk utilities were incapable of detecting the virus or any abnormal activity. The virus is more contagious than the ping-pong virus, because if an infected nonsystem floppy disk is used to boot the computer, the hard disk is infected at the moment of booting. After infection, the virus mercilessly destroys the directory area of floppy disks or the FAT area of hard disks under DOS 2.X. It also can leave behind incurable "after-effects," so that the arduous labor of many persons may be destroyed in an instant. Worse still, false "expression" portions are written into the virus program to fool anyone who tries to analyze the program into following false branches. The virus makes use of the operating system's supervisory functions to fool the unsuspecting DOS and damage the hard-disk main boot sector, so that the hard disk cannot be booted. After this destructive action, if a healthy floppy disk is used to boot the computer (so that the virus is not present in on-board RAM), the same effect will be produced, making the virus even more mysterious. It produces different virus storage formats on floppy disks and on DOS 2.0 and 3.0 hard disks, so that the virus is transmitted in a variety of complex ways. As a result, unless the virus is diagnosed quickly, so that the disk can be vaccinated to suppress its transmission, the consequences are unthinkable. The operating principles of the virus program were therefore analyzed and a virus elimination and vaccination program and methods of alleviating or curing the after-effects were developed. Our unit's damaged computers have now been fully restored to normal operation.

## Software for Eliminating Ping-Pong Virus Developed by Military Unit

*90CF0336D Beijing JISUANJI SHIJI [CHINA COMPUTERWORLD] in Chinese No 4, 24 Jan 90 p 18*

[Article by Zheng Min [6774 2404]: "Software for Eliminating the Ping-Pong Virus"]

[Text] The Automation Work Station of the Guangzhou Military Region headquarters has developed software to eradicate the "ping-pong ball" virus, the first virus from which the military region has suffered.

Last May and June [1989], during technical exchange with outside organizations, the Automation Work Station of the Guangzhou Military Region headquarters became infected with the ping-pong virus. This was the

first instance of a computer virus in the Guangzhou Military Region. The virus causes a small ball to appear on the computer screen and to move like a ping-pong ball. This produced garbage on the screen, wasted computer system space, and decreased the operating efficiency of user programs; in addition, the virus spread to other computers via disks, which seriously affected the normal operation of computer equipment. To deal with the situation, the Automation Work Station quarantined equipment infected with the virus in order to stop its spread, and organized a technical team, which, after 2 months of analysis, research and testing, found that the ping-pong-ball virus primarily altered the disk-read/write and clock-interrupt calling programs in order to propagate and to trigger its activity. The group therefore developed specific software to eliminate the ping-pong-ball virus.

## Analysis, Prevention of Round-Dot Virus

*90CF0336E Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 4, 24 Jan 90 p 26*

[Article by Yang Limin [2799 4539 3046], Computer Laboratory, West Shanghai Motor Transport Company: "The Round-Dot Virus: Analysis and Protection"]

[Text] The round-dot virus is a domestically prevalent virus of IBM PC/XT's and AT's. The author's analysis of the virus program indicates that it has a distinctive organization and characteristics.

The virus program follows specific laws in the physical areas of a magnetic disk. This is because the virus needs to propagate, and wants to do so without executing specific files on disk. Most virus creators make the boot sector of the disk the head of the virus. In terms of their mechanism of propagation, such viruses can be divided into three parts. This first part is the head section, the virus' boot section, whose main function is to read the entire virus into RAM and to prepare for its spread and expression. The head of the virus program is stored in side 0, cylinder 0, sector 1 of the disk and takes up 512 bytes. The second part is the virus' infective body, and the third is its pathogenic body. The main programs for these two parts are stored in some cluster of the disk, where they occupy 1K or 2K bytes, depending on the number of sectors per cluster. As a rule, this cluster is flagged in the FAT as a bad cluster (FF7) in order to prevent its being destroyed or overwritten by some other program. This cluster number's true starting logical sector number, when the disk is infected, is written into and stored in the data field of the virus head; the real boot routine and the disk parameter list are relocated to the cluster's second logical sector.

Because the initial boot is performed with a disk contaminated with the virus, the DOS program is not entered into the proper addresses in on-board RAM, and the DOS service routine cannot be used to service the virus, so that its only recourse is to use the BIOS interrupt service programs in EPROM. The INT 13 interrupt routine is one of the keys to the virus program's propagation and expression. When the virus head in side 0, cylinder 0, sector 1 is read into RAM, it first is stored at the top of memory. It then reads the other two parts of the virus from the cluster concealed by the FF7 flag to the top of RAM, where it has allocated 2K of space for their use. Because it has altered the data on RAM capacity in the memory data area, the transient storage area and data area at the top of DOS do not overlap the area in which it is stored.

The main process by which the virus program propagates and expresses its symptoms has two key elements. First, the virus program alters the INT 13 interrupt vector so that the normal INT 13 interrupt routine first executes the virus program stored at the top of RAM. INT 13 is the most extensively and frequently used routine in microcomputers, so that it is the fastest means of virus spread and expression. The other key is that the virus alters the INT 8 interrupt vector, so that the CPU accesses the expression part of the virus program at a frequency of 18.2 times a second. As a consequence, execution of the normal program is continually repeated by the interrupt or becomes impossible. But the INT 8 step will be altered by the virus and produce its symptoms only if the INT 13 interrupt is called at a particular clock time.

Flow charts of the three parts of the round-dot virus are given below.

Analysis indicates that the round-dot virus program has four distinctive characteristics:

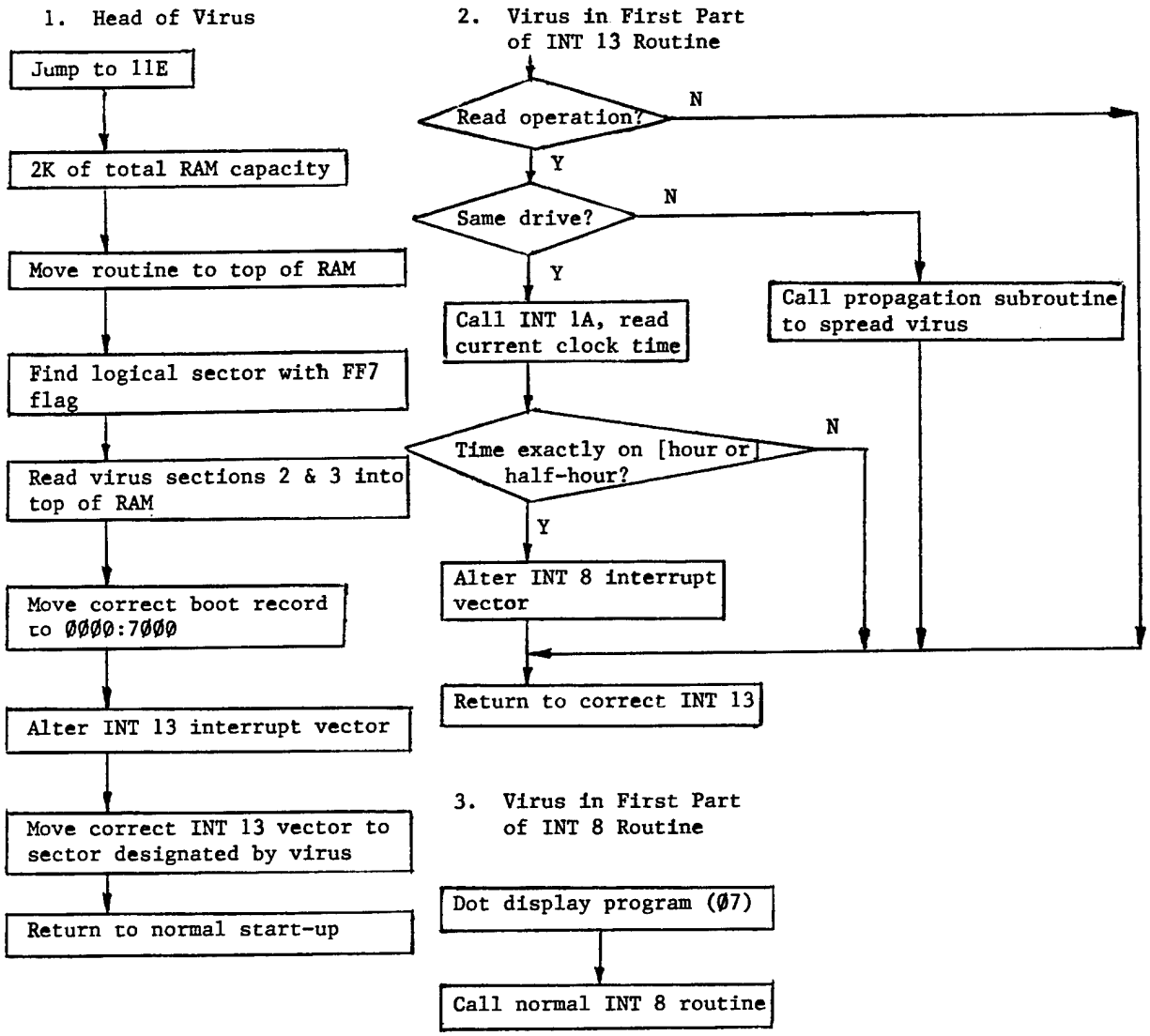
1. The data communications area at the beginning of the virus program consists of only 28 bytes, while that at the front of the normal boot routine occupies 42 bytes. Thus the virus program's first statement is JMP 011E, for which the corresponding machine code is EB1C.

2. The head sector of the virus program always ends with 571355AA (it usually is a sequence of four bytes beginning with 1FC); the normal boot sector always ends in 000055AA.

3. Owing to the action of the virus program, the byte stored at 0000:0413 in RAM gives the total amount of RAM minus 2K; this can be checked with the PC TOOLS utility.

4. The INT 13 interrupt vector should be F000:EC59, but after infection it is XXXX:7CD0.

The above analysis suggests several methods of eliminating or preventing the virus. Procedures of this kind have already been published in JISUANJI SHIJIE of 19 July 1989, and we will not repeat them here. Instead, we will describe a simple method of eliminating the round-dot virus suited to the needs of the general user. Because the virus' head end is essential to its propagation and expression, it is possible to use the DOS boot program to overwrite it on infected disks. The virus program thus




becomes unable to alter the INT 13 interrupt vector, which eliminates its means of propagation and expression. The bad-cluster flag in the FAT is not corrected; but this represents a loss of at most one cluster, which is negligible in overall terms.

If your computer exhibits the round-dot virus on booting, you may proceed as follows:

1. Insert a normal, uninfected DOS boot disk into the drive and perform a warm boot.

2. At the A> prompt, type SYS C:.

3. Start DOS again on the hard disk, which will then be restored to normal.

Preventive measures begin with the steps described in JISUANJI SHIJIE for 29 July 1989. A very important question is how to vaccinate the computer and disks. The writer's investigations indicate that the immunization of the computer involves the INT 13 interrupt vector. Once DOS has been started normally, the best thing is to make sure that the INT 13 vector is normal; this is done by inspecting its value. If an error is found, then the correct value must be restored. The mechanism of disk immunization involves the flag 1357 at the end of the boot area: provided that the disk has this flag, the round-dot virus cannot be transmitted.

Although the round-dot virus is benign, it still can do a great deal of harm, and computer personnel must maintain

a high level of vigilance and perform effective inspection and protective measures in order to assure operating safety.

## New Viruses, Including 'Marijuana' Virus, Reported; Countermeasures Described

### Situation in Fujian Province

*40080015A Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 5, 7 Feb 90 pp 38-39*

[Article by Su Wurong [5685 2976 2837] of the Fujian Province Computer Society: "Once and for All, We Need To Prevent and Treat Computer Viruses"]

[Summary] A report on the spread of computer viruses in Fujian Province was delivered by the Fujian Province Computer Society on 15 August 1989 to an all-province commission. From feedback to this report, we can observe the following:

(1) The main virus outbreaks in the province include those of the "ball virus," the "hard-disk virus," and several variations on these. At the very least, over 50 percent of the computers—namely, IBM PC XT's, Great Wall 0520's and their compatibles—in the province have caught the ball virus.

(2) The majority of computer users in the province have learned the basic principles of diagnosis, prevention, and treatment of computer viruses. The ball-virus outbreak, which spread over the province last spring and summer, is now basically under control.

(3) Some have felt that use of tools such as DEBUG and PC TOOLS to eradicate the viruses and immunize disks is difficult. They want easier and more practical anti-virus software.

(4) Certain users are still having difficulty eliminating the viruses from some compatibles, 286's, and Great Wall 0520's, as well as from different versions of the DOS operating system (such as DOS3.2 and 3.3).

(5) Some users are still employing the formatted-hard-disk method to eliminate viruses. This has wasted great amounts of manpower and financial resources.

(6) There are some more intelligent computer-room managers and workers who have discontinued the use of floppy-disk boot systems, the running of software with an unknown history, and the running of game software on office computers. This has kept them from being invaded by the viruses.

(7) Some users have reported that their computers have been infected by floppy disks brought in by college students. Some, having employed the revised "ball-virus" elucidation program, have created new viruses—the ball-virus variants. These variant viruses have symptoms that are numerous and varied; some have even manifested latent destructive power against hard-disk resources.

Variants of the "ball virus" that have become known include the following:

(1) The explosive virus: at the time of outbreak, small ball(s) appear on the screen, gradually spread, and can "explode" in bursts of light.

(2) The meteor virus: at the time of outbreak, a "meteor" flashes by on the screen and quickly disappears. After about 15 minutes of normal computer operation, however, the meteor returns.

(3) The apple virus: in Chinese-character operating systems, the message "I want to eat an apple" appears on the screen about every half-hour. Normal operation returns after the three characters Pingguo qing ["Apple, please"] are input.

(4) The cipher virus: with encoded hard disks, each time the disk is booted, a password character needs to be typed in; otherwise, when a floppy disk is booted, there is no way to insert the hard disk. The rules of the password are: Taking the 26 letters of the [English] alphabet as a sequence, use the rotational algorithm "back one, forward three." For example, if the last password was "D," the current one will be "C," the next one will be "F," and the one after that will be "E."

(5) The alarm virus: about every 15 minutes, an alarm sound goes off. System data is not affected.

(6) The noise [or chirper] virus: at an unspecified time, a continuous stream of piercing sound is emitted. System data is not affected.

(7) The AIDS virus: within a very short time after the letters A, I, D, and S are input (not necessarily contiguously) with the keyboard, all data stored on the disk is lost. For example, with the Pinyin inputting format, if the two characters zidong ["automatic"] are to be input, the keyboard keys that need to be pressed, as luck would have it, are "AI6DS5"; this activates the virus.

(8) The snowball virus: each time a read/write operation is carried out with a hard disk, the virus is transmitted to this disk and a new available cluster is invaded by the virus and marked as a "bad" cluster. Thus the name snowball—the virus uses up more and more hard-disk space until it has rolled over the entire disk, now useless.

In addition to the "ball virus" and its variants, the "Pakistani Brain" virus (indicated by a new volume mark of ["at" symbol] BRAIN on infected disks), the "Marijuana" (or "Stone") virus (the message "Your PC is now stoned!" is displayed on the screen at the time of outbreak), the "Jew" [or "Israeli"] virus (which breaks out on Friday the 13th, and is therefore also called the "Black Friday" virus), and other viruses have invaded Fujian Province.

## Analysis, Elimination of 'Marijuana' Virus

*40080015B Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 5, 7 Feb 90 pp 40, 42*

[Article by Li Wei [2621 5633] of Bureau No 11, Ministry of Public Security: "Analysis, Elimination of Another New Virus, the 'Marijuana' Virus, That Has Appeared in China"]

[Summary] Recently, a new virus called the "Marijuana" virus or "Stone" virus has broken out on personal computers at a number of institutions of higher learning and scientific research institutes. As opposed to the "ball virus," a benign virus that broke out last year, the new virus falls in the malignant category. It can infect all microcomputers running under the DOS operating system, can destroy system files, and can result in lost user data files.

Source. The "Marijuana" virus was discovered in New Zealand in the second half of 1988. At the time of triggering, the statement "Your PC is now stoned! ...LEGALISE MARIJUANA!" appears on the screen. According to our analysis, the particular type of "Marijuana" virus that has been discovered in China came from Hong Kong. We have obtained disks infected with the virus from some of the units involved, analyzed them, and reached the conclusion that the virus is a malignant one: it has the ability to hide, is transmissible, and is destructive. Although the "Marijuana" virus has so far not spread over China to the extent that the "ball virus" has, we cannot afford to take the matter lightly, and strongly recommend that management take proper safety measures to prevent the virus from spreading further.

Diagnostic techniques. Under the DOS system, the virus program generally resides in the disk boot sector in the COMMAND.COM instruction. One can use DEBUG or PC TOOLS to determine if a disk has or has not been infected. The steps to follow are given below:

### 1. First, Understand Normal DOS Boot Program Characteristics for the Disk

a. The boot program for floppy disk A has these characteristics:

(1) The first command is a jump command: "JMP xx".

(2) The next one is a disk I/O parameter list, the floppy-disk root list.

(3) The final approximately 128 bytes of the boot sector always generate the following English message when a booting error is made: "No—system disk or disk error. Replace and strike any key when ready."

(4) The last two bytes have the bootstrap marker "55AA."

b. The hard-disk main leader record and the placement of the partition table:

When the hard disk is formatted, on hard-disk head 0, cylinder 0, sector 1, a "hard-disk partition table" and main leader record are set up. So that different operating systems can jointly use the disk space, the disk can be partitioned into four independent areas, of which one is the DOS partition for bootstrapping. The allocation structure is as follows:

Hard-disk head 0, cylinder 0, sector 1
00H—main leader record (240 bytes)
0F0H—all zeroes (206 bytes)
1BEH—1st partition table (16)
1CEH—2nd partition table (16)
1DEH—3rd partition table (16)
1EEH—4th partition table (16)
1FEH—55H
AAH

### 2. Diagnosing the "Marijuana" Virus

First, use a normal DOS system disk (A disk) to boot; make sure that the system operates under a non-infected environment.

a. Disk A audit

A>DEBUG

—L 100 0 0 1; read disk A boot sector

—U 100 107; display first and second commands: "JMP 0700:0005" "JMP 00A1"

—D28A 2B7; display "Your PC is now stoned...LEGALISE MARIJUANA!"

If your floppy-disk audit conforms with the previous conditions, then you can be certain that your PC has caught the "Marijuana" virus.

b. Hard-disk audit

Because the virus can infect the hard disk's main boot sector, but not infect the DOS partition boot sector, the hard-disk main boot sector is concealed; one cannot use DEBUG to read/write, and the following operations must therefore be carried out:

A>DEBUG

—R IP; set up IP register

:100

—A 100; begin assembly

xxxx: 0100: MOV DX, 0080
MOV CX, 0001
MOV BX, 0200
MOV AX, 0201

xxxx: 010c: INT 13; read hard-disk cylinder 0, head 0, sector 1

—G=100 10E; execute above assembly program

—U 200 207; display "JMP 07CO: 0005"

—D 38A 3B7; display "Your PC is now stoned!"

"LEGALISE MARIJUANA!"

Via the above operations, one can determine whether or not the virus is present.

**Symptoms of, Harm Caused by Marijuana Virus**

**I. Symptoms**

1. Use of the Marijuana program replaces the original boot routine.
2. The revised INT 13 pointer causes the INT 13 to stay right in the virus program.
3. The original boot program residing in the floppy disk will be: track 0, head 1, sector 3; for hard disks, it will be: cylinder 0, head 0, sector 7.
4. When initiating with an infected hard disk, doing a read/write to disk A will infect disk A.
5. At a specific time, the screen displays the information that the system has been infected with the Marijuana virus.

**II. Harm**

This virus is malignant: it can spread, remain dormant, and is destructive.

Since this virus loads the original DOS boot program into the sectors allotted to system files, it is allocated as follows:

Floppy disks: For low-density disks (9 sectors/track), logical sector 0BH is loaded into the final sector of the root directory area. For high-density disks (15 sectors/track), logical sector 11H is loaded into the root directory area.

Hard disks: Logical sector 06H is loaded into the FAT [file allocation table] space.

From the above, it is apparent that the "Marijuana" virus conceals itself in the loading operation of the original DOS boot routine; it damages the system's FAT or root directory, thus destroying system files, leading to loss of user files, and possibly even leading to system crash.

**Elimination of the Marijuana Virus**

After completing the two-step diagnosis for the virus, carry out the following operations:

First, use a normal DOS system disk (A disk) to boot; make sure that the operation is performed in a non-virus-infected environment. Then, insert a floppy disk infected with the virus into the B drive.

a. Floppy-disk virus elimination

A>DEBUG

—L 100 1 Ob 1; read B-disk track, head 1, sector 3 (low-density logical sector number 0bh), read the resident DOS boot program into RAM zone 100.

—d 100 2ff; audit is or is not of DOS boot program

—w 100 1 0 1; write B-disk track 0, head 0, sector 1, recover proper DOS boot. (Marijuana virus is now eliminated.)

b. Hard-disk virus elimination

After the two-step diagnosis, carry out the following operations:

A>DEBUG

—R IP; set up IP pointer

:100

—A 100; begin assembly

xxxx: 0100: MOV DX, 0080

MOV CX, 0007

MOV BX, 0200

MOV AX, 0201

INT 13; read hard-disk cylinder 0, head 0, sector 7 into RAM position 200, read original hard-disk main boot.

MOV DX, 0080

MOV CX, 0001

MOV BX, 0200

MOV AX, 0301

xxxx: 011a: INT 13; write hard-disk cylinder 0, head 0, sector 1, recover hard-disk main boot program.

—G=100 11C; execute above [assembly] program (Virus is now eliminated)

Because the "Marijuana" virus destroys the floppy-disk root directory and a sector in the hard-disk FAT, it can lead to loss of some user data files, and precludes use of the FAT sector. With the appropriate measures, one can restore the root directory and FAT, and reclaim use of the particular sector. This project is relatively complex, requiring a thorough understanding of disk structure and the DOS operating system, and will not be detailed here.

## Prevention, Treatment of 'Marijuana' Virus

*40080015C Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 5, 7 Feb 90 p 41*

[Article by Xi Hongyu [1153 4767 1342] of the Mechanics Department, Beijing University: "Analysis, Prevention, Treatment of Marijuana Virus"]

[Summary]

**I. Analysis of the Virus**

The "Marijuana" virus belongs in the operating-system category of viruses; it resides in the physical sectors of a

disk, such as side 0, track 0, sector 1. If an infected disk is used as a boot disk, the virus after the booting resides in on-board RAM (and takes up 2Kbytes of space); moreover, it becomes part of the operating system. Any floppy disk inserted thereafter in the A drive can catch the virus.

Since the virus' 1A5H-1B7H position has the words "LEGALISE MARIJUANA!" it has come to be called the "Marijuana" virus. Below is a mapping of the BOOT area of a 360K floppy disk after infection:

The virus is relatively small; its effective length is only that of the 1B7H byte. It is also relatively simple, residing only in the disk service interrupt routine (INT 13H). It hides in the disk's first physical sector: side 0, track 0, sector 1. For floppy disks, this sector is the disk's BOOT area, and can be audited with PC TOOLS and similar utilities. For hard disks, however, this area is usually not the first logical sector, but rather is the disk's main boot sector. It does not belong to the logical sectors of the C disk or D disk, and cannot therefore affect them via read/write operations.

A hard disk will assuredly catch the virus after an infected floppy disk is used for booting. In addition, in one-eighth of the cases, the computer's internal buzzer emits a sound, and in the upper left corner of the screen, the message "Your PC is now stoned!" is displayed.

The newly added contents of the INT 13H is part of the virus. When a read/write is done with a disk in the A drive, the A-drive motor is in a start-up state, and A-drive disks not covered with a write-protect tag can be infected. Finally, it returns to execution of the original normal INT 13H routine.

In order to preserve the boot sector of the original disk, the virus moves it to other positions on the disk. For floppy disks, the virus hides the original BOOT sector in disk side 1, track 0, sector 3; for hard disks, the virus stores the original main boot sector in disk side 0, track 0, sector 7.

The virus examines the disk's boot space, and if this sector's first four bytes are the same as those of the virus itself—namely, EAH, 05H, 00H, and C0H—then it knows that the disk has already been infected and it will thus not need to infect it again.

Furthermore, the virus uses up to three BIOS internal-memory [i.e., on-board RAM] low-address data, which are:

0000: 0413—total capacity of internal memory; 1024 bytes = 1Kbyte is taken as the count unit, taking up 1 byte.

0000: 043F—disk-drive motor switching state, occupying 1 byte.

0000: 046C—computer's internal clock count, taking up 4 bytes.

## II. Symptoms of, Harm Caused by Virus

When the DIR statement is input after a floppy disk has been infected, one can see that several files in the root directory have been lost; also, in the middle or at the end of the directory, an obviously abnormal file will be listed.

Infected hard disks almost always do not manifest obvious symptoms, and can operate normally. Use of PC TOOLS and other tools to examine the boot area will not permit detection of any abnormality. When this infected hard disk is then used for initialization, the virus can then reside in the computer's internal memory. Also, if one inserts a floppy disk into the A drive and does a read/write, the disk can catch the infection. The worst condition with hard disks is when the virus destroys the FAT and/or the boot sector, preventing subsequent use of the hard disk as a system boot disk. Also, after a floppy-disk initialization, one sometimes cannot change to the C disk: the display shows that the C disk does not exist, and there is no way to access the C files. Using the DOS FORMAT instruction, even the FDISK command, does not restore the files.

Path:A:

Absolute seotor 00000,Svstem BOOT

| Displaoement | --- | --- | --- | --- | --- | --- | Hex codes | | | --- | --- | --- | --- | --- | --- | --- | ASCII value |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0000(0000) | EA | 05 | 00 | 00 | 07 | 19 | 99 | 00 | 00 | 71 | 2A | 00 | F0 | E4 | 00 | 80 | + q* |
| 0016(0010) | 9F | 00 | 70 | 00 | 00 | 1E | 50 | 80 | F0 | 02 | 72 | 17 | 80 | F0 | 04 | 73 | \| ^P r s |
| 0384(0180) | 03 | 33 | DB | FE | C1 | CD | 13 | EB | 05 | 07 | 59 | 6F | 75 | 72 | 20 | 50 | 3 : Your P |
| 0400(0190) | 43 | 20 | 69 | 73 | 20 | 6E | 6F | 77 | 20 | 53 | 74 | 6F | 6E | 65 | 64 | 21 | c is now Stoned! |
| 0416(01A0) | 07 | 00 | 0A | 0A | 00 | 40 | 45 | 47 | 41 | 40 | 49 | 53 | 45 | 20 | 4D | 41 | LEGALISE MA |
| 0432(0180) | 52 | 49 | 4A | 55 | 41 | 4E | 41 | 21 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | RIJUANA! |

The following table shows the sector allocations for three kinds of floppy disks:

| | BOOT | FAT1 | FAT2 | Root directory space | Data space | No. of sectors/track |
|---|---|---|---|---|---|---|
| 360K disk | 0 | 1-2 | 3-4 | 5-11 | 12- | 9 |
| 320K disk | 0 | 1 | 2 | 3-9 | 10- | 8 |
| 1.2M disk | 0 | 1-7 | 8-14 | 15-20 | 29[sic] | 15 |

Infection of a 320K disk can spell disaster for the files stored on it, for there is no way to restore them. When the root directory for the 1.2Mbyte high-density disks increasingly used with 286 and more powerful computers exceeds 2x16=32 items, abnormal phenomena can appear. To avoid the destruction of the "Marijuana" virus when employing high-density disks, assuming a need to store over 30 files or records, it is best to use a subdirectory to store data.

With respect to hard disks, if disk side 0, track 0, sector 7 is the main area for storing system data, then the files on that disk can be destroyed. The CHKDSK instruction can be used to detect "bad" clusters on an infected disk.

### III. Immunization Against the Virus

Although elimination of the virus is relatively easy [see preceding article], immunization against the virus is somewhat more difficult. For non-system boot disks, under virus-free conditions, one needs to force the address of the boot sector's first four bytes to become EAH, 05H, 00H, and C0H, respectively. For system disks, one needs to rewrite the hard disk's main boot sector, which can be accomplished even with already infected hard disks. Replace 0CCH-0D2H in the boot sector with 90H; this will prevent the virus from again altering the INT 13H interrupt pointer and infecting the disk. Then replace 0BDH-0BFH with 90H (the NOP dummy instruction); this will prevent the virus from taking up residence again in internal memory. VC-HARD.EXE in the ViruCide software series that we have developed can be used for mass recovery of files on the vast majority of hard disks, to avoid losses from reformatted hard disks.

## Detoxification of Stone Virus

*40080015D Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 5, 7 Feb 90 p 42*

[Article by Yan Long [7027 7893] and Xia Xiaodong [1115 2556 2639] of the Software Engineering Institute, Beijing Aerospace University: "Detoxification of the Stone Virus"]

[Summary]

### I. Loading and Detection of the Stone Virus

In floppy disks infected with the Stone virus, the BOOT sector has already been replaced with the virus program, and the contents of the original BOOT sector have been placed into a certain sector in the root directory. To determine whether or not the floppy disk has been infected, one can simply use DEBUG, PC TOOLS, NU or other tools to perform an audit of the disk's BOOT sector (side 0, track 0, sector 1), and if the message "Your PC is now stoned!" appears in the BOOT sector, this indicates that the floppy disk has been infected; if otherwise, the disk has not caught the virus, but this does not eliminate the presence of other viruses [elsewhere on the disk].

Using a common tool to determine if a hard disk has the Stone virus is very difficult, because of the virus' great ability to hide. The virus gets loaded into head 0, cylinder 0, sector 1 (i.e., the 446 bytes of the hard disk's main leader record) of the hard disk's physical sectors. The common tools can only check the hard disk's BOOT sector, FAT space, and ROOT space; there is thus no way to determine if the disk has been infected. If the NU tool is used to audit head 0, cylinder 0, sector 1 of the physical sectors, one can find the same information as with an infected floppy-disk BOOT sector: the original hard-disk main leader record has been moved to head 0, cylinder 0, sector 7 of the physical sectors. If the hard disk has not been infected, the disk's main leader record is normal.

### II. Transmission of the Stone Virus

Common read/write operations performed on a computer with an infected hard disk will transmit the virus to the floppy disk; furthermore, the floppy disk itself can then be a medium for further spread of the virus. The transmission has a certain randomness to it, however; in the initial stages of infection, very little further transmission takes place, but in later periods transmissibility increases. If infected floppy disks are used to boot a non-infected computer, then soon afterwards, all disks used in that computer for reading and writing can be infected.

### III. Detoxification of the Stone Virus

Detoxification or eradication of the Stone virus from a computer here means the restoration of all the disk files revised by the virus. To detoxify a floppy disk on a computer that has not been infected (or a computer that is booted with an uninfected floppy disk), after backing up the files contained on the floppy disk, format the infected floppy disk, and then copy the backed-up contents onto the floppy disk as soon as possible.

If one needs to retain the floppy-disk boot routine, floppy-disk detoxification entails the recovery of the original BOOT sector contents copied by the virus into the ROOT space; it also entails moving the revised sectors in the ROOT space to an empty file directory to be determined by formatting (see specific procedure in Program 1 below).

Since the virus is loaded into the hard disk's main leader record, a system transfer or a common hard-disk formatting does not change the main leader record, hence the phenomenon whereby infected hard disks, after formatting, still have the virus—yet another aspect of the malicious nature of the Stone virus. Practical detoxification of a hard disk requires taking the contents of the main leader record (head 0, cylinder 0, sector 7 of the physical sectors) moved by the virus into the hard disk's physical sectors, and copying those contents into head 0, cylinder 0, sector 1 of the physical sectors occupied by the virus (specific procedure is given in Program 2 below).

**IV. Notice on the Stone Virus**

It is estimated that many floppy disks have been infected by the virus, and readers should be extremely careful about floppy disks used to boot their computers; use of write-protect tags is mandatory.

We invite colleagues to comment on the accompanying programs, which are written in the C language.

## Four Viruses Discovered in Jiangsu

*40080015E Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 5, 7 Feb 90 p 44*

[Article by Zhao Yujie [6392 3768 3381]: "Four Computer Viruses Discovered in Jiangsu Province"]

[Text] An investigation has revealed that Jiangsu Province has been invaded by four kinds of virus: the round-dot virus, the snowball virus, the noise [i.e., chirper] virus, and the data-destroying type of virus. In the round-dot virus, after switch-on, 1-3-mm-diameter white spheres appear on the screen, and if they collide with Chinese characters, the latter can be cut off or lost altogether, the computer's operating speed slows down, and the computer can lock up. With the snowball virus, each time a read/write is done, the disk is infected once; this process is repeated until all the available disk space is taken over by the virus. With the noise virus, a short time after switch-on, the computer emits a strange noise continuously; moreover computer operation is interfered with. The preceding three types of virus are benign, but the fourth type—the data-destroying type—is malignant. Files on floppy disks and hard disks can be eliminated, and there may be no way to restore them; part of the data is lost or tampered with, and one cannot use the computer.

It has been revealed that the outbreak has been caused by imported game software and by already infected floppy disks and computers, or by network hook-ups. Blocking the [network] transmission paths is an effective way of preventing the virus. Infected computers should be quarantined.

## Integrated Virus-Elimination Software Package Developed

*40080016A Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 8, 28 Feb 90 p 2*

[Article by Hou Jinjun [0230 6930 6511]: "Xidian University Develops Computer-Virus-Elimination Integrated Software Package"]

[Summary] Domestic software previously released for the elimination of computer viruses has all been unifunctional—these products have been unable to eradicate a variety of viruses from different kinds of disks and files. Now, however, with the "GC" integrated computer-virus-elimination software package recently developed by Xidian University [formerly Northwest Institute of Telecommunications Engineering] in Xian, users can eliminate the "Marijuana," "Ball," "Jew" [or "Israeli"], "Raindrop," and other viruses currently prevalent in IBM PC's and compatibles throughout China.

Via a multi-window menu-driven format, the user can select the appropriate type of virus to be eliminated from a floppy disk or hard disk. In addition, this software package can provide "vaccination" against the "Ball Virus" for disks on which the virus has already been eliminated. Trials by several units—including the Ministry of Machine-Building and Electronics Industry's [MMEI] Economic Regulation Department and Education Department, and the Air Force's Institute of Telecommunications Engineering—have demonstrated the product's efficacy.

## Over 1,000 Qinghua University Microcomputers Infected by Viruses

*40080011A Beijing BEIJING KEJI BAO [BEIJING SCIENCE AND TECHNOLOGY NEWS] in Chinese 24 Jan 90 p 3*

[Unattributed article: "Over 1,000 Microcomputers Infected by Viruses; Users Urge Immediate Measures To Effect a Radical, Permanent Cure"]

[Summary] According to an article in the 31 December 1989 issue of the Qinghua University newspaper XIN QINGHUA, the reporter learned from the School of Information Science, the CAI [computer aided instruction] laboratory, and other university units that large-scale computer virus infections have broken out this semester among the IBM-series microcomputers at the university, and moreover that the viruses are tending to spread to higher-level computers. The viruses have seriously interrupted normal teaching, research, and administrative work and have caused losses that cannot be made up. A large number of computer users are calling

Program 1

```
CSEG    SEGMENT PARA 'CODE'
        ASSUME  CS:CSEG,DS:CSEG
        ASSUME  ES:CSEG,SS:STACK
FDUS    PROC    FAR
        PUSH    DS
        XOR     AX,AX
        PUSH    AX
;
        MOV AH,0
        MOV DL,0
        INT 13H
;
        MOV AX,0201H
        MOV DX,0101H
        MOV CX,0003H
        MOV BX,SEG STONE
        MOV ES,BX
        MOV BX,OFFSET STONE
        INT 13H
;
        MOV AX,0301H
        MOV DX,0001H
        MOV CX,0001H
        MOV BX,SEG STONE
        MOV ES,BX
        MOV BX,OFFSET STONE
        INT 13H
;
        MOV BX,SEG ROOTD
        MOV ES,BX
        MOV BX,OFFSET ROOTD
        MOV AX,0301H
        MOV DX,0101H
        MOV CX,0003H
        INT 13H
;
        RET
FDUS    ENDP
STONE   DB  512 DUP(0)
ROOTD   DB  16 DUP(0,31 DUP(0F6H))
CSEG    ENDS
;
STACK   SEGMENT PARA STACK 'STACK'
        DB      256 DUP(0)
STACK   ENDS
        END
```

Program 2

```
CSEG    SEGMENT PARA 'CODE'
        ASSUME  CS:CSEG,DS:CSEG
        ASSUME  ES:CSEG,SS:STACK
HDUS    PROC    FAR
        PUSH    DS
        XOR     AX,AX
        PUSH    AX
;
        MOV AH,0
        MOV DL,80H
        INT 13H
;
        MOV AX,0201H
        MOV DX,0080H
        MOV CX,0007H
        MOV BX,SEG STONE
        MOV ES,BX
        MOV BX,OFFSET STONE
        INT 13H
;
        MOV AX,0301H
        MOV DX,0080H
        MOV CX,0001H
        MOV BX,SEG STONE
        MOV ES,BX
        MOV BX,OFFSET STONE
        INT 13H
;
        RET
HDUS    ENDP
STONE   DB  512 DUP(0)
CSEG    ENDS
;
STACK   SEGMENT PARA STACK 'STACK'
        DB      256 DUP(0)
STACK   ENDS
        END
```

on authorities for immediate measures to eradicate the viruses and to guarantee healthy operation of computers.

The main characteristics of the viruses discovered at the university are as follows: "frenzied copying" [fengkuang kaobei], or automatic, ceaseless copying of files; automatic addition or deletion of files by a bug called the "marijuana virus"; a phenomenon called "the Israeli," which breaks out most often on a Friday or on the 13th of the month; a [ping-pong] ball rolling around on the screen; chirping [emission of high-frequency sounds]; image flicker; etc.

In addition to interfering with normal computer operation, the viruses have caused irreparable damage. According to an official at the CAI lab, the virus broke out as an IBM 386 optical disk for mathematics test questions was being loaded. Not only was operation impossible, 30Mbytes of working space were totally lost.

When the reporter asked what corrective measures were being taken, an official responded that some higher authorities need to develop better ethics and habits by not playing computer games on computers used for instruction and calculation, and what's more by not running floppy disks bearing a virus; and all computer administrative units should increase their supervision of the use of floppy disks and put an end to the spread of infected disks. The official also recommended that—in view of the fact that there are some who are very fond of creating and transmitting viruses—appropriate government departments should pass legislation to severely punish computer crime.

## Jiangxi Researcher Tackles Three Kinds of Virus

*40080014A Beijing GUANGMING RIBAO [GUANGMING DAILY] in Chinese 6 Feb 90 p 1*

[Article by Wang Shaoxiong [3769 4801 7160]: "Zou Zhenquan Successively Solves Problems of Three Kinds of Computer Virus"]

[Summary] The computer virus analysis and automatic processing system developed by the Computer Office of the Jiangxi Province Publishing Affairs Management Bureau recently [December 1989] passed appraisal in Nanchang [see "Virus Analysis/Automatic Processing System Developed" elsewhere in this special issue]. Heading a team of four in developing this system was 42-year-old Assistant Researcher Zou Zhenquan [6760 2182 2938], who began tackling the problem in the first half of 1989. Now, less than 2 months after this system for diagnosing and eliminating the "small ball" virus was accredited, Zou has also developed a "Marijuana" computer virus automatic processing system and a "Pakistani [Brain]" virus automatic processing system. Currently, over 30 types of computer virus have been discovered worldwide, and four or five have been found in China.

At a meeting held in Beijing in early January and attended by representatives of the State Science and Technology Commission, the China Artificial Intelligence Society, the State Commission of Science, Technology and Industry for National Defense, the Chinese Academy of Sciences' Space Science and Applications Research Center, Institute 15 of the Ministry of Machine-Building and Electronics Industry, and other organizations, Zou reported on his [first] system and gave an on-site demonstration. Noted Chinese computer expert Professor Tu Xuyan [3205 1645 1750], Researcher Gong Weishu [1362 4850 2873], Senior Engineer Zong Bahai [1350 2149 3189], Associate Researcher Shi Weisan [0670 3956 0005], and others gave the [first] system very high praise, commenting that its diagnostic accuracy was high, its operation in eliminating viruses is safe, that it is suitable to a wide variety of computers, and that it is easy and convenient to use. It should generate significant social and economic benefits and is recommended for dissemination throughout China.

## Games Cause Computer Viruses

*40100034A Beijing CHINA DAILY in English 2 Mar 90 p 3*

[Text] The use of computer games has been blamed for the current outbreak of computer viruses spreading in Shanghai, and China Science News has appealed for a ban on the playing of these games on office computers.

With the wider use of computers in China, many users have bought or copied games and play them in their leisure time.

A signed article in the Beijing-based newspaper said a recent random check in Shanghai showed that nearly 90 percent of the computer games carried viruses.

Last year, Shanghai Public Security Bureau and the Shanghai computer popularization office jointly issued a circular to cut the ways of spreading viruses, but with little effect. (CD News)

## Panic Over Computer Viruses in Taiwan

*40080005A Beijing JISUANJI SHIJIE [CHINA COMPUTERWORLD] in Chinese No 43, 8 Nov 89 p 12*

[Unattributed article: "Panic Over Computer 'Viruses' Spreads Throughout Taiwan"]

[Summary] Computer viruses have now caused a serious menace to personal computers (PC's) in Taiwan. According to businessmen in Taiwan, the situation is so severe that at least 50 percent of the 700,000 PC's in Taiwan may have caught a virus. The viruses are meticulously designed programs which can engulf a computer's entire memory and cause the PC to stop working, and frequently take the form of a "time bomb"—a [logic] bomb set to unleash its attack on the computer at a certain time and to cause PC paralysis. Spread of the viruses is by insertion of an infected floppy disk into a

disk drive, or by the presence of a virus in a PC network; in the latter case, other computers in the network can readily catch the virus.

According to dispatches from foreign press agencies, a "Columbus Day" virus (also called Data Crime 123) and a "Black Friday" virus have recently caused worldwide alarm. According to data received from computer merchants in Taiwan, the Hungch'i [1347 2759] Company has estimated that 70 to 80 percent of Taiwan's PC's have caught a virus that is incubating in the computers. A spokesman for the Shent'ung [4377 6639] Company has stated that the "Russian Block" [Eluosi fangkuai] game software is especially dangerous. At least 30 types of virus are now spreading over Taiwan, including a "native-born" [bentuhua] virus; an adaptation of the "Black Friday" virus called the "Happy Sunday" virus, where the words "Happy Sunday" actually appear on the computer screen; a version of the "Columbus Day" virus; and a "Two Tigers" virus, where, after destroying the computer [data], the virus causes a loud song "Two Tigers" to be played.

Foreign Broadcast Information Service (FBIS) and Joint Publications Research Service (JPRS) publications contain political, economic, military, and sociological news, commentary, and other information, as well as scientific and technical data and reports. All information has been obtained from foreign radio and television broadcasts, news agency transmissions, newspapers, books, and periodicals. Items generally are processed from the first or best available source; it should not be inferred that they have been disseminated only in the medium, in the language, or to the area indicated. Items from foreign language sources are translated; those from English-language sources are transcribed, with personal and place names rendered in accordance with FBIS transliteration style.

Headlines, editorial reports, and material enclosed in brackets [ ] are supplied by FBIS/JPRS. Processing indicators such as [Text] or [Excerpts] in the first line of each item indicate how the information was processed from the original. Unfamiliar names rendered phonetically are enclosed in parentheses. Words or names preceded by a question mark and enclosed in parentheses were not clear from the original source but have been supplied as appropriate to the context. Other unattributed parenthetical notes within the body of an item originate with the source. Times within items are as given by the source. Passages in boldface or italics are as published.

## SUBSCRIPTION/PROCUREMENT INFORMATION

The FBIS DAILY REPORT contains current news and information and is published Monday through Friday in eight volumes: China, East Europe, Soviet Union, East Asia, Near East & South Asia, Sub-Saharan Africa, Latin America, and West Europe. Supplements to the DAILY REPORTs may also be available periodically and will be distributed to regular DAILY REPORT subscribers. JPRS publications, which include approximately 50 regional, worldwide, and topical reports, generally contain less time-sensitive information and are published periodically.

Current DAILY REPORTs and JPRS publications are listed in *Government Reports Announcements* issued semimonthly by the National Technical Information Service (NTIS), 5285 Port Royal Road, Springfield, Virginia 22161 and the *Monthly Catalog of U.S. Government Publications* issued by the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402.

The public may subscribe to either hardcover or microfiche versions of the DAILY REPORTs and JPRS publications through NTIS at the above address or by calling (703) 487-4630. Subscription rates will be provided by NTIS upon request. Subscriptions are available outside the United States from NTIS or appointed foreign dealers. New subscribers should expect a 30-day delay in receipt of the first issue.

U.S. Government offices may obtain subscriptions to the DAILY REPORTs or JPRS publications (hardcover or microfiche) at no charge through their sponsoring organizations. For additional information or assistance, call FBIS, (202) 338-6735,or write to P.O. Box 2604, Washington, D.C. 20013. Department of Defense consumers are required to submit requests through appropriate command validation channels to DIA, RTS-2C, Washington, D.C. 20301. (Telephone: (202) 373-3771, Autovon: 243-3771.)

Back issues or single copies of the DAILY REPORTs and JPRS publications are not available. Both the DAILY REPORTs and the JPRS publications are on file for public reference at the Library of Congress and at many Federal Depository Libraries. Reference copies may also be seen at many public and university libraries throughout the United States.