GADING

majalah akademik itm, cawangan pahang.

Bil. 4 Jilid 1 Jul/Dis 1989

daftar isi :

VIRUS ATTACKS!

by Dianne Cheong Lee Mei

You don't have to be doing anything wrong to get hit. But you can spread it unwittingly while carrying out your legitimate business, that is computing. It makes its presence on a floppy disk. Then it installs itself in the computer's RAM. Hence, the computer is bugged!

Rogue programs or sets of instructions that can secretly be spread among computers are known as viruses and they are disruptive softwares. They caused growing alarm among computer users. Viruses got their name because the mimic in the computer world the behaviour of biological viruses.

Viruses can travel either over a computer network or on an infected disk passed by hand between computer users. Once the infection has spread, the virus might do something as benign as displaying a simple message on a computer screen or as destructive as erasing the data on an entire disk. Pirate software and games package are viewed as a major source of viruses. So do watch out for computer diskettes from unknown sources!

Public domain systems like bulletin boards also are susceptible to virus infection. Unsuspecting individuals PC users can innocently download an infected program, lend the contaminated floppy disks to others and the cycle starts.

Booting from a carrier diskette would result in creating a vicious cycle of infection. Vandals and mischief makers, often known as hackers, who write viruses are usually brillant low-level programmers who find it a challenge cracking complicated computer codes. The appraoch which they usually take involves one of the two approaches. Either the use of a 'trapdoor' in a program or of a 'logic' bomb.

A trapdoor is a deliberate break in the course of a program. Using this gap the criminal can then insert additional instructions which may totally disrupt the system. The logic bomb is triggered either by some combination of events in the system, for example a praticular individual signing on to the system, or by a given date and time being reached. The bomb then obliterates all the stored data or otherwise destroys the files.

There are many strains of viruses. Some are malicious and some are not. Microcomputer users in Thailand are facing widespread infections from the so-called 'Israeli' virus. Several computer vendors admitted that they had found that several of their PCs with the 'Israeli' virus which is spread after it attaches itself to an executable program and then that program is run in another microcomputer. The virus then installs itself in the computer's RAM and any subsequent files that are executed

becomes infected. Each time an infected program is run, it increases in size by just over 1.8kb and in time the computer begins to slow down or the program becomes too large to be run. This computer virus is also known as the 'Friday the 13th virus' since the virus deleted files on October 13,1989.

In Hong Kong, three varieties of viruses have been identified. Stone, Bouncing Ball and Brain attack the boot sector of a disk and passes into the computer's RAM when the system is switched on. When a user carried out a read operation such as DIR, DIR/W or CHKDSK, the virus infects the new disk.

The three viruses are regarded as less malign than viruses which infect the operating systems or general purpose programs of computers. However, they could mutate and randomly destroy hard disks.

Stone occupies the master boot sector of a hard disk or the Disk Operating System (DOS) boot sector of a diskette. In a hard disk it will usually move into the directory area of the disk destroying the directory information. It leaves the first 32 files on a disk intact but destroys all the following files. A message on the computer screen saying "Your PC is Stoned - Legalise marijuana!" is the first indication many users will have that they have been infected with Stone. An antidote program developed by Hong Kong Polytechnic , called Stonebreaker is used to cure the infected disks. A second program called Flushot allows forewarning of new and different virus attacks.

The brain virus was written by Amjad and Basit Farooq of Lahore, Pakistan in 1985 to protect their medical software program. It was intended only as anti-piracy device for their medical package and was therefore non-malicious. But then it can facilitate those who wanted to use the virus maliciously.

Brain occupies unused sectors of a disk and destroys data by moving into adjacent sectors. The Bouncing Ball makes the computer seize up at random times and displays a bouncing ball on the computer screen.

Bouncing Ball, Stone and Brain take up 1, 2 and 3Kb of RAM respectively. Their presence on a floppy disk can be detected on a personal computer with the Microsoft DOS by using the command CHKDSK A:. The memory available on a good disk will be commensurately larger. A software package such as Norton Utilities can also be used to detect a virus on a hard disk. The package is used to check the absolute sector and the DOS boot sector of the disk.

In Malaysia, 3 other strains of virus have also been identified : C Brain, Y.C.I.E.R.P and DENZUK. They to attack the boot sector of a disk and pass into the RAM when the system is switched on. C Brain gives thhe message "Welcome to

the Dungeon C 1986 Brain" while the strain Y.C.I.E.R.P can be detected by the command DIR or DIR/W. The message 'The volume in Drive A (or B) is Y.C.I.E.R.P.' will be displayed.

Rebooting the system disk by presssing CTRL-ALT-DEL the computer screen which display the word 'DENZUK' simply shows the diskette is infected with DENZUK!

Another known killer program, Datacrime I and II was reported to have activated a trail of destruction in Europe on October 13, 1989. An expert has warned that both strains of Datacrime could surface here in one to two years time. Computer users in Asia did not report any presence of Datacrime after the ill-fated Friday the 13th.

Datacrime originated in Holland March, 1989. One strain increases the size of the COM files while the other increases the size of both the COM and the EXE files. A virus detector, Virscan was used to scan all the files for this virus. Datacrime is reported to have already affected 100000 computers in Holland and paralysed Sweden's postal service computer network.

Less than a week after the Datacrime debacle, a non-damaging worm called Wank worm was discovered. It displays anti-nuclear messages on the screens of affected terminals. 50 of the more than 15000 scientific computers and workstations that are hooked up to the space Physics Analysis Network which links universities and government research facilities were affected. The worm causes a message to flash onto the display of an affected system that reads: "Worm Against Nuclear Killers. Your System Has been Officially Wanked". The worm was spotted by security engineers searching the network for evidence of the Datacrime virus.

Some viruses are time bomb attacks. A time bomb program called Halloween named after the Western festival, when according to folklore, the dead rise from their graves for a day was supposed to be activated on October 31, 1989.

There are least 4 viral strains programmed to be activated in the near future. These are:-

1. Sys -B - performs a hard disk format on any Friday 13th after 1990 and does relatively no damage.

2. Jerusalem -D - destroys the File Allocation Table (FAT) of a disk on every Friday the 13th after 1990.

3. Jerusalem -E - identical to the D variety except activation is on any Friday the 13th after 1992.

4. Clone - B - corrupts the FAT when it is booted after May 5, 1992 and

5. Century Virus (also called Oregon Virus) - activation date is January 1, 2000 : erases both FATs on all connected drives and writes to sectors on attached devices. On completion, displays a message, "Welcome to the 21st century".

KEEPING BUGS AT BAY

Are we helpless against computer viruses and should we treat viruses as a prank very much like an April Fool's joke?

Virus writing is a criminal issue. It is not civil nor legal. It is an outsider tampering with an assest - information. However, writing a virus into a sofftware as an anti-piracy device is not necessary the right way to prevent copyright infringement.

While it is relatively easier to isolate and develop vaccines as a preventive measure for computer viruses than pathogenic viruses, some computer viruses are irreversible. This means that once the virus has attacked or bombed there is no looking back. Destroyed data and programs remain destroyed.

On the other hand, if the virus is reversible then a cure can be written to resolve the data. This kind of reverse engineering would take an Assembly language programmer anywhere, from hours to months to generate the code required to counter the virus program. But in the process, the company affected by the virus would have lost precious time and money in the damage done and in its efforts trying to undo the situation.

Computer viruses today are a phenomena that is already well-known. They get into computer systems through loose security and can be prevented if sufficient care and vigilance are exercised. EDP should be the front-line watchdog. They need to assume the responsibility of impressing upon their other colleagues the necessity of maintaining discipline in their computing habits. In short, physical and administrative methods are more effective than any software solution.

Users can guard themselves against 'casual computing' as an anti-viral prevention. Below are some suggestions:

* Always verify a disk the first time it is being used;
* Put write protect tabs in the floppy disks if data is not written on them;
* Check computer's memory when booting up system;
* Backup files;

* Store programs and data on separate directories or disk to avoid saving a virus during a backup;
* Practice installing anti-virus programs such as Flushot, Vaccine, Vaccinate and Virscan into the computer hard disk so that it will automatically check and test for virus;
* program the need for passwords;
* Write-protect own programs. For example, sofware designed to be copied only once usually onto the hard disk and then the program would disallow further copying.

However, if your disk or system is infected, do seek professional help or engage a virus recovery service!

REFERENCE

1. *Asia Computer Weekly, July 10-23, 1989, pg. 3*
2. *Asia Computer Weekly, Sept 18 - Oct 1, 1989, pg. 13*
3. *Asia Computer Weekly, Oct 30 - Nov 12, 1989, pg. 1, 9*
4. *Asia Computer Weekly, Nov 13 - 26, 1989*