VIRUS ANALYSIS 2

Olympic Games

Mikko Hypponen
Data Fellows, Finland

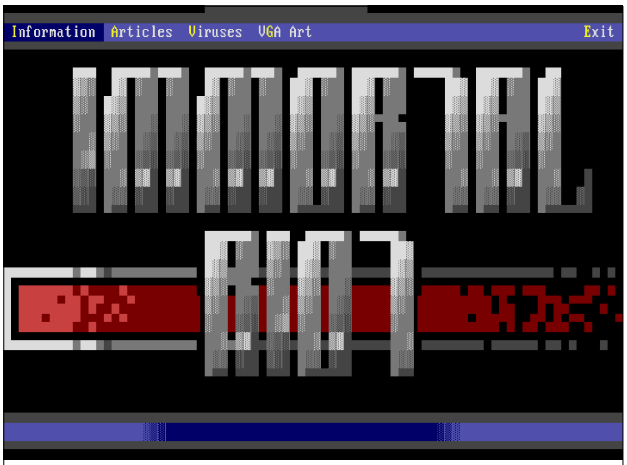
A new virus, known as Olympic (aka Olympic Aids), has featured prominently on the television, on the radio, and in the newspapers of Northern Europe since the beginning of February. Its newsworthy factors are its Olympic-theme activation routine, and suspicions that it had infected the computer systems of the Lillehammer 1994 Winter Olympics. Fortunately this was not the case.

Despite being reported in the wild in Norway, Olympic is not of Norwegian origin: it is made in Sweden by a new virus group which calls itself 'Immortal Riot'.

Into the Undergr ound

Swedish soil seems to provide particularly fertile ground for raising virus groups: clans like Beta Boys, Demoralized Youth, and the Funky Pack of Cyber Punks have been active in Sweden in the past. The latest group of virus writers, Immortal Riot, seems to consist of four members, known only by their aliases, or 'handles'. So far, the group has published and distributed about thirty viruses, most of which are new variants of existing strains. The viruses thus far seen are not examples of technical brilliance; quite the opposite. Most simply crash the computer, or manifest their presence in some other obvious way.

Immortal Riot also publishes an electronic magazine, Insane Reality, containing articles by the group members and their associates, source codes of viruses, and back-patting and back-stabbing of other members of the virus community. The group seems to be little more than an ego trip for this gang of teenagers - it seems to be 'cool' to be a virus writer.



The computer underground gets steadily more organised - Immortal Riot even publishes its own electronic magazine.

Virus Operation

Olympic is a fairly typical COM file infector, which does not remain in memory, and spreads only when an infected file is executed. Its method of searching for files for infection is not very efficient. Once a number of files on the hard disk have been infected, it may take half a minute to find a new victim: such a slowdown is likely to make the virus easier to spot.

When it finds a suitable candidate for infection, the virus first checks the size of that file to ensure that the infected code will be greater than 64 Kbytes, the largest permissible size for a COM file. The first bytes of the file are checked for a jump construct which the virus is about to insert. If found, the virus considers the file already infected and starts to search for another victim. This process is repeated until five files are infected.

The virus does not check the internal structure of the host file when it infects. Thus, EXE files with a COM extension will be infected by the virus. When such a corrupted file is executed, the virus will infects other files on the machine, but is unable to return control to the original program. In most cases, the machine will crash.

The infection process consists of storing the original first three bytes of the file at the file end, replacing them with a jump to a setup routine, which the virus adds to the end of the file. An encrypted version of the virus code is appended to the end of the file, and, finally, the virus adds a short plain-text note and the decryption routine.

Olympic uses a single pseudo-random variable key based on infection time to encrypt its code. The routine uses either the SI or DI register as work-registers in the decryption loop, alternating between infections. Thus, there are only 25 constant bytes between different virus generations. These are located in two different parts of the virus. The encryption method is not truly polymorphic, and is unlikely to cause problems for anti-virus vendors.

Olympic can infect files which have the DOS Read-Only attribute turned on, and will also restore the date and time stamps of infected files. However, files grow in size by 1440 bytes, which is visible in the directory listing. The virus has no directory-stealth routines, as it does not stay resident.

Olmypian Trigger

The virus was programmed to trigger on the day after the start of the 1994 Winter Olympics (12 February), and has a one-in-ten chance of activating after this date. 'Dice-throwing' is done by checking whether the system timer's hundredth-of-seconds field is below 10. The virus does not check the current year. If the trigger conditions are not met, the virus returns control to the host file.

On activation, the virus draws the Olympic circles on the screen, displaying comments on the Games and its mascots, Haakon and Kristin. Next, it overwrites the first 256 sectors of the first hard disk in the system. To ensure destruction, the virus disables Ctrl-C and Ctrl-Break checking during the destruction routine. Finally, the machine hangs.

While the virus overwrites the fixed disk, it thoughtfully displays the Olympic rings - a symbol of cooperation and unity.

Much of Olympic's code resembles that of viruses generated with VCL, up to the point of the standard VCL-like note; a short message in the end of the virus, which is not displayed at all. The virus' note text reads: 'Olympic Aid(s) `94 (c) The Penetrator'. This virus is probably based on VCL-created code, modified to avoid detection by some scanners. As the virus displays a picture before starting to overwrite the disk, aware computer users might be able to switch the machine off before the virus has a chance to overwrite data areas, making recovery much easier.

VCL.Olympic

Aliases:	Olympic Aids.
Type:	Non-resident, parasitic.
Infection:	Files with 'COM' extension.
Self-recognition in Files:	File starts with a JMP to an offset 1443h from the file end.

Hex Pattern:	Due to the short length and large amount of wildcards, this searchstring should be used with care.
	`8D?? 1301 B9AC 0281 ???? ????`
	`??E2 F8C3`

Intercepts:	None.
Trigger:	One in ten chance of overwriting the contents of the fixed disk, on or after 12 February, any year.
Removal:	Specific and generic removal possible under clean system conditions. Recovery of machines affected by trigger routine might be possible with specialist data recovery equipment.