

# VIRUS ANALYSIS 3

## Olivia

Péter Szor  
Data Fellows

The Olivia virus was found in the wild in April 1997: first reports in the wild came from three different countries – Taiwan, Poland and Hungary. In a now-familiar fashion, it was distributed over the Internet, like so many other viruses before it.

Several infected files and droppers have been uploaded to a Taiwanese FTP site. One of these, RAR25C.EXE, claimed to be a new beta version of the popular archive utility, RAR, from Russia. When this self-extracting executable is run, it unpacks two other files, RAR.CFG and RAR.EXE. RAR.EXE is a dropper for Olivia.2374.

When RAR.EXE is executed by the user, it displays the error message: 'Not enough memory. Program aborted.' The user will therefore not suspect that anything is amiss, and is bound to think: 'Just the usual beta again, let's wait until the fix comes.' But the virus is already resident.

The popularity of the Internet appears to be changing the face of the virus problem in East European countries. Prior to 1996, Hungary, for example, had problems with new viruses from Romania, Slovakia, Poland, Russia and of course from Bulgaria. Viruses sometimes entered Eastern Europe from such West European countries as Germany and Sweden. There were also many cases from the Far East, including such incidents as viruses being 'imported' from Taiwan as 'OEMs' with a dozen infected PC clones.

The Internet became big business in East European countries, where large computer networks did not exist before the early 1990s. The situation as regards piracy is also getting better, which creates a new set of problems. Private individuals are trying to get the best shareware and, of course, the latest versions available. This means that a virus writer can reach his goal easily by uploading his latest, even buggy code to some sites in a hack or beta version package.

The Olivia virus family is one of the most recent examples of this trend. Although Olivia.2734 has obviously been written by a newcomer to the field, it nevertheless shows several interesting ideas in its infection mechanism and activation routine.

### Initial Infection

When an infected EXE file is executed, the decryptor takes control immediately. This is not, however, the case with COM infections. When a COM file is infected, the virus follows some of the instructions in the victim's code and calls its decryptor from there.

Olivia's first trick appears almost at the beginning of its code. The virus makes a division by zero after changing the Int 0h (Exception) vector to point into the decryptor first. This routine uses the stack frequently, as well as 286 instructions, thus creating code which is both anti-emulating and anti-debugging. The decryptor is based on a random 8-bit XOR key, but it is not polymorphic, only oligomorphic. Although some of the indexes change, it is still possible to pick up a search-string.

When the virus code is decrypted, Olivia disables the resident parts of *Norton AntiVirus* and *Microsoft AntiVirus*. Next, it executes an anti-emulation trap. It calls Int 11h (equipment determination interrupt) and checks that the return value in AX is not zero. In this manner, Olivia is able to detect most of the heuristic analysers which are based on emulation but which do not pay attention to this particular interrupt. The virus returns to DOS if the return value is zero.

Olivia's next action is to check the date: if it is 10 April or 23 December the virus calls its payload; otherwise it checks for its presence in memory. The 'Are you there?' call is Int 21h AX=3DA0h, BX=1980h.

If, on return from the call, the BX and CX registers are set to 1979h and 1223h respectively, the virus assumes it is already active in memory and returns control to the host program. If the BX and the CX registers do not contain these values, Olivia manipulates the MCB and copies itself to the allocated memory area. Then it hooks Int 21h. Finally, control returns to the host program.

### Infection of Files

Olivia infects COM and EXE files as they are run or renamed, or as their attributes are changed. First, the virus clears the attributes of the file; then, it opens it for read. Next, it obtains the System File Table Entry of the victim and checks its time-stamp – files with time-stamps set to 60 seconds are assumed to be already infected.



平平, 生日快樂! By André '97/1/30

**Figure 1:** Olivia's message, displayed in traditional Chinese characters, translates as: 'Ping Ping, Happy Birthday!'

If the time-stamp is not set to 60 seconds, the virus changes the file access mode in the System File Table and checks the extension of the file there, too. If the extension is COM, the virus uses its exclude list with files named 4DOS, COM-MAND, and VT, which it will not infect.

However, if the extension is EXE, the virus uses a different exclude list, which contains the names WIN, EMM386, SSCAN, TB, and CHKDSK.

Since the file WIN.COM (which launches *Windows 3.x*) has a COM extension, this check will fail, and the virus will infect that file. There is no known reason for the presence of 'VT' in the COM file exclude list, and 'SSCAN' stands for Super Scan, a local product.

If the victim has a COM extension the virus uses a special function which reads 4 bytes in a loop from the beginning of the victim and checks for E9h (JMP), EBh (JMP short), 90h (NOP), F8h (CLC), F9h (STC), FAh (CLI), FBh (STI), FCh (CLD), and FDh (STD) each time.

If one of the above instructions is found, the virus moves to the location of the next instruction. If this instruction is in the last 64 bytes of the program, the virus will not infect that file.

This means, therefore, that the virus will not infect most goat files. However, if the last instruction was not in the last 64 bytes, the virus will modify the host program at this location. More specifically, it uses the 64h (286 Push) opcode to push a word value to the stack, then executes a C3h (RET), which will give control to the virus code. This can prevent heuristic analysis if the emulator is not able to handle 286 opcodes correctly. This technique, called 'inserting', also makes disinfection more difficult.

Then Olivia modifies its decryptor, encrypts the virus body, and adds itself to the end of the COM file. The decryptor is only oligomorphic, but the virus writer is not far from writing a full polymorphic virus. Since the virus does not check the size of the COM files before infection, the infected COM files can be bigger than 64KB and will fail to execute. All these facts tell us that the virus writer is a beginner at his job.

Since the virus has stealth capabilities, the change to file size is not visible: Olivia changes the return values of Find First, Find Next functions by subtracting 2374 from the infected file size field – this is why the virus changes the file stamp to 60 seconds at the end of the file infection.

In the case of EXE files, Olivia does not pay special attention to the file structure; the result being that it will infect standard goat files.

### Payload

The virus calls its payload when the date is 10 April or 23 December (the year is irrelevant). First, Olivia checks that the PC has an active hard drive, by examining the

CMOS. Then it checks for an installed CD-ROM drive. If a CD-ROM is available, Olivia opens the drive and displays this message:

```
please put a love music CD into your CD-ROM
and pass any key to continue...
```

Then it waits for a keypress. If the user puts an audio CD into the CD-ROM drive and presses any key the virus closes the drive and starts to play it.

Next, it changes the video mode and displays a message onscreen which contains Chinese characters (see Figure 1). The translation of the text is: Ping Ping, Happy Birthday! The characters are traditional Chinese ones, normally used in mainland China.

Olivia then disables the keyboard, and then it clears the contents of the CMOS. Finally, it overwrites the hard drive, using memory address FFFFh:0 as the sector image.

The virus has an additional message, never displayed:

```
Olivia Virus 7.5β By André (C)TRAN TECH United
Groups
```

### Summary

Olivia.2374 shows that a virus written by a beginner can spread far and wide if some infected files are available from the Internet. People should be extremely careful in handling material downloaded from the 'net.

Those who do not take precautions are likely not only to lose data from their home PC, but also to create problems for their company. Free software does not necessarily mean virus-free software.

Olivia	
Alias:	CDROM.
Type:	Resident, stealth, oligomorphic.
Infection:	COM, EXE.
Self-recognition:	60 seconds marker in files.
Hex Pattern in Files:	C08E D8FF 3600 00FF 3602 0068 ???? 8F06 0000 8C0E 0200
Hex Pattern in Memory:	CD16 E800 0033 C0CD 110B C075 04B4 4CCD 2144
Payload:	Plays Audio CD, displays messages, overwrites the CMOS and the hard drive on 10 April and 23 December.
Removal:	Recover affected files from backup or replace with original.