

select section: [news](#) | [calendar](#) | [publications](#) | **encyclopedia** language: [russian](#) | [english](#)



Last update: 8/10/2001

Today: 8/10/2001

- ▶ [Virus News Mail List! Join Right Now!](#)
- ▶ [Click here to bookmark!](#)
- ▶ [Send this page to a friends!](#)

#### VL-Finder v.2




#### Table of Contents

##### 1.AVP Virus Encyclopedia

- 1.1. [File Viruses, DOS](#)
- 1.2. [Boot Viruses](#)
- 1.3. [Multipartite \(File and Boot\) Viruses](#)
- 1.4. [Multi-Platform Viruses](#)
- 1.5. [NewExe Viruses](#)
- 1.6. [Macro Viruses \(Word, Excel, Access, PowerPoint, Amipro and Visio\)](#)
- 1.7. [Virus Constructors](#)
- 1.8. [Windows HLP Viruses](#)
- 1.9. [Java Viruses](#)
- 1.10. [Polymorphic Generators and Generator-based Viruses](#)
- 1.11. [Script Viruses](#)
- 1.12. [Trojan horses](#)
- 1.13. [Internet Worms](#)
- 1.14. [Computer Virus Hoaxes](#)
- 1.15. [Palm](#)
- 1.16. [Malware](#)
- 1.17. [Jokes](#)

#### AVP Virus Encyclopedia

##### Internet Worms

##### Internet E-mail Worms

### I-Worm.Petik.a

This is Internet worm spreading as 8Kb MADCOW.EXE file attached to email messages. To send infected messages the worm uses MS Outlook. The worm also is able to send its copies to IRC channels by affecting mIRC client.

#### First Run

When the worm is start for the first time (if a user clicks on EXE attached to the message, or or being accepted as IRC download) the worm copies itself to two files:

- Windows system directory with Wininet32.exe name
- Windows directory with MadCow.exe name

and registers MadCow.exe file in auto-run section:

- in WIN.INI file, [windows] section, "run=" key - under Win9x
- in system registry in "Run=" key - under WinNT

The worm then creates the C:\WIN32 directory, creates two files in there (DOS batch file and VBS script program):

ENVOIE.BAT - it just spawns ENVOIE.VBS file (next file)  
 ENVOIE.VBS - this script spreads worm with infected messages

While spreading the script connects to MS Outlook and sends infected email messages to all addresses in MS Outlook AddressBook. The messages have:

**Subject:** Pourquoi les vaches sont-elles folles ?  
**Body:** Voila un rapport expliquant la folie des vaches  
**Attachment:** MadCow.exe

#### Second Run

On next start (on next Windows restart) the worm creates its copy with MadCow.exe name in C:\WIN32 directory, and then affects mIRC client in directories:

C:\MIRC\  
 C:\MIRC32\  
 C:\Program Files\MIRC\  
 C:\Program Files\MIRC32\

The affected mIRC client will send worm copy (MadCow.exe file) to all users that join infected channel.

#### Other

The worm creates the registry key: HKLM\Software\Atchoum]

If there is no mIRC client found in the system, the worm creates the MSLS.ICO file in Windows system directory, writes to there an image of imp (devil) and registers as standard icon for EXE files.

The worm also contains the text stings in its body:

IWorm.MadCow par PetiK (c)2000  
 I Love You Maya / Je t'aime

#### Glossary

1. [File attributes](#)
2. [Header of EXE-file \(EXE-header\)](#)
3. [File](#)
4. [Worms](#)
5. [DOS \(Disk Operating System, Operating System\)](#)
6. [EXE-file](#)
7. [FAT \(File Allocation Table\)](#)

#### Related topic

1. [Outside DOS](#)
2. [File Viruses](#)
3. [Virus Incorporation to the Top of File](#)
4. [Virus Incorporation to the End of a File](#)
5. [Virus Incorporation in the Middle of File](#)
6. [File Worms](#)
7. [Incorporating of a Virus into DOS COM and EXE Files](#)
8. [Operating Algorithm of a File Virus](#)
9. [File Viruses](#)
10. [DOS Viruses](#)
11. [Windows Viruses](#)
12. [IRC Worms](#)
13. [IRC Clients](#)
14. [Script Worms](#)
15. [mIRC.Acoragil and mIRC.Simpsalapim](#)
16. [DOS Viruses](#)
17. [Embedding in DOS](#)
18. [Windows Viruses](#)
19. [Detection of a File Virus](#)
20. [Global Access Networks and EMail](#)
21. [Email Conferences, File Servers, FTP and BBS](#)
22. [File Recovery](#)

**VIRUSLIST.COM**

Copyright © 2000  
Kaspersky Lab  
All rights reserved

select section: [news](#) | [calendar](#) | [publications](#) | **encyclopedia** language: [russian](#) | **english**

last update: 8/10/2001  
email: [viruslist@avp2000.com](mailto:viruslist@avp2000.com)