Table of Contents

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 registeres 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

Page Top

Glossary

Related topic

last update: 8/10/2001
email: viruslist@avp2000.com