Infection on the computer

Head File

Creating a key in Software\\Microsoft\\Windows \\CurrentVersion\\Run for the trigger.

file_tmp.txt

Transition launched by batch file

Auto-decompression of files by induction...

Viruses are recorded in the register.

Virus ready to be launched

Encrypted copy of the virus is created

file_tmp.txt
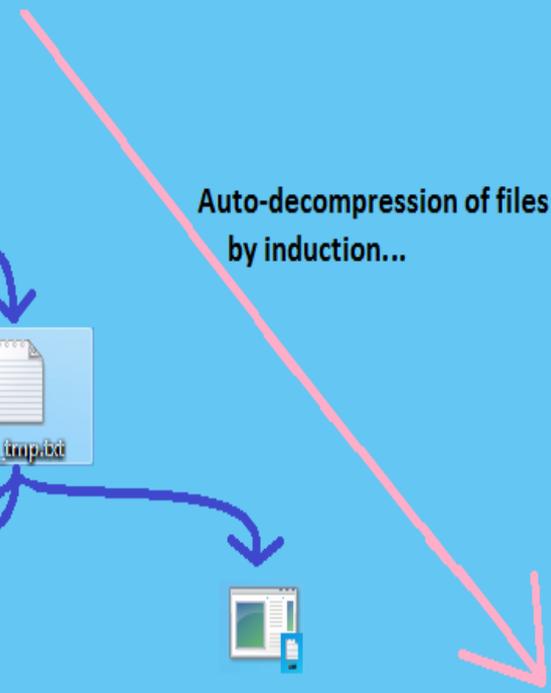
Legend :

Launching process

Writes in the register

Creation of file

Virus file

Auto decompression file

file_tmp.txt

Encrypted virus file

Temporary File

Registry key

Encrypted Registry key

Batch file to run other programs

How works the virus in its final k-ary form :

Launch taskkill.exe
by a system call

The new process is killed

List of current
processes

Virus killed by an
another process

If the file of the virus is
not here, its copy
is decrypted and relaunched

Detection of the loss
of a virus.

Launching by batch

Launch

Self-detection

Legend :

Launching processus

Detection of loss of processes

Reading information
in the register

Auto detection of
viruses

Checks the list of current processes

Kills the process

Understanding about
the authorization to
restart the missed
process

Circle of self-checking
viruses to revive one which
has been attacked

Detection of the arrival
of a new process

Batch file to run
other programs

Virus file

Security program
(eg antivirus).

Taskkill.exe

Encrypted registry
key

Encrypted virus file

New process