# *ViruBack*

**For Windows 95/98/ME/NT/2000**

- **Overview**
- **ViruBack Win 95/98/ME**
- **ViruBack Win NT/2000**
- **Virus check tips**
- **About**

# *ViruBack*

### Virus attack Backup and Restore Instructions for Win NT/2000

## Preparation before backing up

a) The Recycle Ben is excluded from being backed up but better empty it before making backup(s).
b) For faster backup, better empty all your Windows\Temp and Internet Temp files.
c) Be sure the computer is virus free and you have scanned all drives thoroughly from within Windows also from MS-DOS using a MS-DOS antivirus software after a cold boot. (Please read the Virus checking tips section.)
d) Make a Win 95 or 98 boot disk and make a test run, select to "Full format" floppy and to "Copy System Files". If you don't full format it using a Win95/98 formatting tool then the bootdisk might fail to boot computer.
e) Rename large self extracting EXE downloads extensions, such as Internet explorer 4.0/5.0, Netscape or any large size download that have the .exe extension that you don't want them to be backed up taking more space, but in the same time protect them from being infected. Rename their extension to .ex_ for example.

## Backup Instructions

Open ViruBack, start at the very top and select one of the two backup options, "Drive Backup" or "Windows directory backup".

1) Select to backup the Windows directory or a drive one at a time.

2) Select destination where you would like to save the backup.
Windows backup name should be in MS-DOS 8.3 short name and drive backup have to have the drive letter at the beginning of it.
Example C_DriveV.zip, the C used to identify backup.
Windows backup saved as WinVback.zip, it will be converted to MS-DOS 8.3 short file name format if it is more than eight letters.
Best to keep and save the Windows backup in one of the hard drives, you can store the others in a Zip disk or CDR.

3) Add/Remove extensions wildcards, be sure to leave one space only in between each wildcard, no more and no less.
*.exe *.com *.sys *.doc *.xls *.ppt
Double check that only one space is in between.
*.exe *.com *.sys (executables and system files, a must backup.)
*.doc *.xls *.ppt (Microsoft Office, document, Excel and Power Point).

4) Options:

a) Update backup
A time saver when re-making a backup, it will add new files and replace old with newer files but will not remove any.
Don't select to update if your backup is too old and you have uninstalled many programs, because when restoring it will restore all zipped files and will make path if path not found.

a) Skip Locked Files(not recommended)
It will skip files that are in use.
If not selected and one file is locked, then backup will fail.
To be sure that none are locked, close all applications then press Ctrl+alt+Del, End Task all except, Explorer, Systray and ViruBack before making the backup and you should be OK.

5) Click the backup button and wait, zip has to scan the drive first then it will start zipping.
After Windows backup it will prompt you to copy the Windows restore batch file and necessary restore files to the boot disk.
If you don't have a boot disk ready, then you can do it later by clicking Options\Copy Restore Batch to a Boot Disk.

To update backups:
Double click from list to transfer backup configuration to Source and destination, it will transfer previously selected paths but you still have to Add/Remove extensions again.

# Restore Instructions

## Restoring and Starting Windows

After a virus attack such as the Monkey boot virus nothing would run.
Once you are sure that the antivirus have cleaned the computer, deleted, renamed or removed virus from infected files.
(done by using a MS-DOS antivirus software).

Boot computer with the ViruBack boot disk in the floppy drive to restore the Windows directory first,
once booted, type
**RestWinV**
It will restore all Windows executables.
It will restore NtDetect.com so you can boot computer.
It will restore ViruBack.exe to the ERS directory so you can run it and be able restore the drive(s) executables from within windows.

Above will get Windows started.
Recommend strongly to use the Win & Win\Sys backup in ERS NT or ERS 2000 and restore from a ERS bootdisk if necessary.

## Restoring Drives

After you have restored Windows, only ViruBack.exe can be ran from within windows.

Run ViruBack, start at the very top and select one of the restore Action options.

Double click the the desired backup to be restored from the list then click the Restore Backup button, be sure drive and path the Destination drive are transferred correctly.

# Menus

## Edit Menu

1) To delete a backup, click Edit\Delete backup or right click and select Delete Backup.

2) To remove a listed backup without deleting it, click Edit\Remove from List or right click and select Remove from List.

### Tools Menu

1) **Backup All Fixed Hard Drives and Windows**
   If selected then it will Backup All Fixed Hard Drives and Windows once you click the Backup button.

2) **Make an ERS 9x Boot Disk**.
   Make an ERS 9x boot disk and test it to be sure it boots OK.

3) **Copy Restore Batch file to boot disk**, that will give you another chance to copy batch file, and all required files to the boot disk.
   Pkunzip.exe, Choice.com, Edit.com, Attrib.exe copied from ERS directory.
   NOTE: If you have Win95 950 (1995 release) installed from floppies then Choice.com will not be found in the Windows\Command directory, download at http://www.mslm.com/ersmore.htm

### Option menu

1) **Backup Automatically When ViruBack is Opened**
   You need to set a one permanent directory to store all backups in the "Always use the same directory to store backups." text window, then select this option.
   ViruBack will backup all drives and the Windows directory automatically without prompting.
   The option is good to either manually open Viruback and run all backups without attending it or run it using a Task scheduler such as the one included with ERS.

2) **Open Task Scheduler**
   Open Task Scheduler and schedule it to run Viruback.exe so it will do backups automatically when ever you wish.

3) **Skip Locked Files When UnZipping**
   If there are files that can't be over written then select this option to skip

these files, so you don't get error restoring.

4) **Set ZipTemp Drive**

Zipping needs a Temp working folder to do the work.(about 20% of the backup being backed up).
Be sure there is enough free hard disk space for zipping.
Don't set Zip Temp in a Network computer or non fixed drives.
Change Zip Temp Path if you are backing up a hard drive
and the Zip Temp is in the drive being backed up.

# *ViruBack*

## Virus attack Backup and Restore Instructions for Win 95/98/ME

### Preparation before backing up

a) The Recycle Ben is excluded from being backed up but better empty it before making backup(s).
b) For faster backup, better empty all your Windows\Temp and Internet Temp files.
c) Be sure the computer is virus free and you have scanned all drives thoroughly from within Windows also from MS-DOS using a MS-DOS antivirus software after a cold boot. (Please read the Virus checking tips section.)
d) Make and test run an ERS 9x boot disk, open ERS 9x click Options\Make ERS bootdisk,
e) Rename large self extracting EXE downloads extensions, such as Internet explorer 4.0/5.0, Netscape or any large size download that have the .exe extension that you don't want them to be backed up taking more space, but in the same time protect them from being infected. Rename their extension to .ex_ for example.

### Backup Instructions

Open ViruBack, start at the very top and select one of the two backup options, "Drive Backup" or "Windows directory backup".

1) Select to backup the Windows directory or a drive one at a time.

2) Select destination where you would like to save the backup.
Windows backup name should be in MS-DOS 8.3 short name and drive backup have to have the drive letter at the beginning of it.
Example C_DriveV.zip, the C used to identify backup.
Windows backup saved as WinVback.zip, it will be converted to MS-DOS 8.3 short file name format if it is more than eight letters.
Best to keep and save the Windows backup in one of the hard drives, you can store the others in a Zip disk or CDR.

3) Add/Remove extensions, be sure to leave one space only in between each wildcard, no more and no less.
*.exe *.com *.sys *.doc *.xls *.ppt
Double check that only one space is in between.
*.exe *.com *.sys (executables and system files, a must backup.)
*.doc *.xls *.ppt (Microsoft Office, document, Excel and Power Point).

4) Options:

a) Update backup
A time saver when re-making a backup, it will add new files and

replace old with newer files but will not remove any.
Don't select to update if your backup is too old and you have uninstalled many programs, because when restoring it will restore all zipped files and will make path if path not found.

a) Skip Locked Files(not recommended)
It will skip files that are in use.
If not selected and one file is locked, then backup will fail.
To be sure that none are locked, close all applications then press Ctrl+alt+Del, End Task all except, Explorer, Systray and ViruBack before making the backup and you should be OK.

5) Click the backup button and wait, zip has to scan the drive first then it will start zipping.
After Windows backup it will prompt you to copy the Windows restore batch file and necessary restore files to the boot disk.
If you don't have a boot disk ready, then you can do it later by clicking Options\Copy Restore Batch to a Boot Disk.

To update backups:
Double click from list to transfer backup configuration to Source and destination, it will transfer previously selected paths but you still have to Add/Remove extensions again.

## Restore Instructions

### Restoring and Starting Windows

After a virus attack such as the Monkey boot virus nothing would run.
Once you are sure that the antivirus have cleaned the computer, deleted, renamed or removed virus from infected files.
(done by using a MS-DOS antivirus software).

Boot computer with the ViruBack boot disk in the floppy drive to restore the Windows directory first,
once booted, type
**RestWinV**
It will restore all Windows executables.
It will restore Io.sys, MsDos.sys and the Command.com so you can boot computer.
It will restore ViruBack.exe to the ERS9x directory so you can run it and be able restore the drive(s) executables from within windows.

Above will get Windows started.
Recommend strongly to use the Win & Win\Sys backup in ERS 9x and restore from a ERS 9x bootdisk if necessary.

### Restoring Drives

After you have restored Windows, only ViruBack.exe can be ran from within windows.

Run ViruBack, start at the very top and select one of the restore Action options.

Double click the the desired backup to be restored from
the list then click the Restore Backup button, be sure
drive and path the Destination drive are transferred correctly.

## Menus

### Edit Menu

1) To delete a backup, click Edit\Delete backup or right click and
select Delete Backup.

2) To remove a listed backup without deleting it, click Edit\Remove from List
or right click and select Remove from List.

### Tools Menu

1) **Backup All Fixed Hard Drives and Windows**
If selected then it will Backup All Fixed Hard Drives and Windows once
you click the Backup button.

2) **Make an ERS 9x Boot Disk**.
Make an ERS 9x boot disk and test it to be sure it boots OK.

3) **Copy Restore Batch file to boot disk**, that will give you another
chance to copy batch file, and all required files to the boot disk.
Pkunzip.exe, Choice.com, Edit.com, Attrib.exe copied from ERS directory.
NOTE: If you have Win95 950 (1995 release) installed from floppies then
Choice.com will not be found in the Windows\Command directory, download at
http://www.mslm.com/ersmore.htm

### Option menu

1) **Backup Automatically When ViruBack is Opened**
You need to set a one permanent directory to store all backups in the
"Always use the same directory to store backups." text window,
then select this option.
ViruBack will backup all drives and the Windows directory automatically
without prompting.
The option is good to either manually open Viruback and run all backups
without attending it or run it using a Task scheduler such as the one
included with ERS.

2) **Open Task Scheduler**
Open Task Scheduler and schedule it to run Viruback.exe so it will do
backups automatically when ever you wish.

3) **Skip Locked Files When UnZipping**
If there are files that can't be over written then select this option to skip
these files, so you don't get error restoring.

4) **Set ZipTemp Drive**
Zipping needs a Temp working folder to do the work.(about 20% of the
backup being backed up).
Be sure there is enough free hard disk space for zipping.

Don't set Zip Temp in a Network computer or non fixed drives.
Change Zip Temp Path if you are backing up a hard drive
and the Zip Temp is in the drive being backed up.

# OVERVIEW

This program was made when the Melissa, Papa and the CIH /SpaceFiller viruses started flooding the Internet Mar, 1999.
It could be a nightmare if attacked by a virus and lost all executables then have to reinstall Windows and all programs in your computer just to restore the executables.
Zip files don't get infected unless they are opened and files executed from it.
You may not loose infected files after an antivirus has disinfected them but you will loose infected files creation date, a restore from ViruBack will restore computer original files untouched.

ViruBack will b**ackup files that are most vulnerable** to be infected
*.exe *.com *.sys *.doc *.xls *.ppt
with option to add and remove as you see necessary.

Option to backup the whole drive or the Windows directory.
Drives backup can be restored from within Windows after the Windows directory, computer boot files and Viruback.exe have been restored from a bootdisk to get Windows started.

Each backup could use anywhere from 5 to 150 MB depending how many programs you have installed and type of work that you do.

It will copy one restore batch file RestWinV.bat, Pkunzip.exe, and this program ViruBack.exe to the boot disk that you should have ready.
Running RestWinV.bat from the bootdisk will restore Windows executables and the computer boot files (Io.sys, Command.com and MsDos.sys in Win 95/98/ME) and (Netdetect.com in Win NT/2000).
It also restores ViruBack.exe to the ERS directory so you can run it and be able restore the drive(s) executables from within windows.
Recommend strongly to use the Win & Win\Sys restore in ERS and restore from it if necessary.

You can run all backup using a task scheduler but you need to select options in the Options menu and select/save a permanent backup directory.
There is a Task Scheduler included in ERS 9x but none in ERS NT/2000.
A task Scheduler also included in freeware MiniApps
http://www.mslm.com/free.htm

# Virus Checking Tips

There are many Antivirus software, having only one is not enough.
Because one company could be ahead of the other updating their
antivirus software effectively with the latest viruses.

Always get the latest antivirus updates and make a habit visiting
antivirus homepages. A two week old antivirus is worthless if infected
with a brand new released virus.

If somebody announces a new virus, to be sure it is not a hoax (fake),
visit the antivirus homepages and check.
Also best to search for it using any of the Internet search engines,
**BUT be careful, DON'T visit** unknown homesites to read about the viruses,
because that could be the place that is helping in spreading it. Go to
well known sites that normally stay on top of the latest news.

Normally I would say that viruses are most spread through schools,
colleges, work, friends and family members. But now viruses are getting
spread by Email, check an Email attachment for a virus before opening it
or sending it, simply right click the file and select Virus Scan from the
context menu (not all antivirus software have the option).

**Be ready to fight a virus**

There are many viruses, each damage files, act, symptoms and the
cures are different.
A virus attack doesn't mean it is the end of the world and doesn't mean that
you are going to loose every thing.
With destructive viruses, yes ViruBack is a great help but many antivirus
software can remove the virus from the infected file without deleting it,
but you will loose the file date, they will be dated at the time they
were disinfected, so restoring from ViruBack can restore the files
to their original dates.

One of the worst viruses is the boot Monkey virus, it is very well spread
and chances that every computer will get it some where along the line.
When active it will delete .exe and .com files.
If you suspect a boot virus then shut the computer switch instantly.
Some boot viruses are very aggressive, it will delete all .exe and .com files
in seconds or few minutes and some are not so aggressive, will delete once in
a while and then hide.
The aggressive type is obvious but the hiding type is hard to detect and you
may have to scan two or three times to find it.
To detect a boot virus effectively you need to run a MS-DOS antivirus from
a write protected antivirus bootdisk.

**After checking the computer thoroughly in Windows**:

In Win95/98, insert a brand new floppy formatted with Win95/98 ONLY,
select to copy System Files.
For Win ME use ERS 9x boot disk.
In Win NT/2000, insert a brand new Win95/98 boot disk.

Don't use third party formatting tool because some will not work to make
a Win95/98 boot disk.

Unzip your favorite MS-DOS antivirus to the floppy,
write protect the floppy by sliding the tab upwards, that will prevent any viruses
from entering and infecting the files in the floppy.
To run it, restart computer with boot disk in drive, once booted, type the word
used to run the antivirus in MS-DOS.

Some times a boot virus will not let you boot into a floppy drive or access
a floppy drive, try again and again.

Remember that most viruses don't reside in files only but reside in memory,
and use memory as a central active location to infect other files. A write protected
antivirus boot disk is the best way to disinfect memory.
Before booting from a boot disk, shut computer power completely for about
10 to 20 seconds.

# *ViruBack*

## **ViruBack** For Windows 95/98/ME/NT/2000



Theodore Fattaleh author, programmer and publisher.
All Program Names are Registered Trademarks of their
Respective Owner.
http://www.mslm.com same as
My Email addresses:
2000@msn.com
twf@flash.net
2000ted@csi.com