

## Forum:[Hack Forums](#)

Thread: [How to make your own personal ULTIMATE Anti-virus!!!](#)

Goku - June 27, 2008, 10:37 pm

Ok, so i was working on this a while back, and IT WORKS!!! aha! ok. so here's the deal. you can't run any .bat or .vbs files with this.

it's a little tricky though, and takes some time, so, sorry guys :(.

anyways, the idea is to remove all your .exe and .com files that have anything to do with dos, including dos itself. by remove, i mean MOVE or COPY. now, windows has an auto-protect feature, that if a file goes missing, it recreates it. so, to by pass that you'll need something like "Lock Folder XP v3.6", which is what i got. i dunno how you'd do it on vista though or anyother version of windows, but if u got xp, u can use it. u can get the serial for it from <http://serials.ws>

so here's the deal, here's a list of the majority of files that you need to copy and hide:

### FILES ([Click to View](#))

append.exe  
ARP.EXE  
at.exe  
attrib.exe  
auditpol.exe  
bcdedit.exe  
bitsadmin.exe  
bootcfg.exe  
cacls.exe  
certreq.exe  
certutil.exe  
change.exe  
chglogon.exe  
chgport.exe  
chgusr.exe  
chkdsk.exe  
chkntfs.exe  
choice.exe  
cipher.exe  
cleanmgr.exe  
clip.exe  
cmd.exe  
cmdkey.exe  
cmstp.exe  
comp.exe  
compact.exe  
convert.exe  
cscript.exe  
debug.exe  
Defrag.exe  
diantz.exe

diskpart.exe  
diskperf.exe  
diskraid.exe  
dispdiag.exe  
doskey.exe  
dosx.exe  
dpapimig.exe  
driverquery.exe  
edlin.exe  
esentutl.exe  
eventcreate.exe  
exe2bin.exe  
expand.exe  
fc.exe  
find.exe  
findstr.exe  
finger.exe  
fltMC.exe  
fontview.exe  
forfiles.exe  
fsutil.exe  
[ftp.exe](#)  
getmac.exe  
gpresult.exe  
gpupdate.exe  
help.exe  
hostname.exe  
icaccls.exe  
ipconfig.exe  
iscsicli.exe  
label.exe  
lodctr.exe  
logman.exe  
logoff.exe  
lpremove.exe  
makecab.exe  
mem.exe  
mountvol.exe  
mrinfo.exe  
msiexec.exe  
mtedit.exe  
nbtstat.exe  
net.exe  
net1.exe  
netcfg.exe  
netsh.exe  
netstat.exe  
nlstfunc.exe  
nslookup.exe  
ocsetup.exe  
odbcconf.exe  
openfiles.exe  
pathping.exe

Ping.exe  
PkgMgr.exe  
PnPUnattend.exe  
PnPUtil.exe  
powercfg.exe  
print.exe  
printui.exe  
qappsrv.exe  
qprocess.exe  
query.exe  
quser.exe  
qwinsta.exe  
rasautou.exe  
rasdial.exe  
rasphone.exe  
recover.exe  
reg.exe  
regini.exe  
regsvr32.exe  
relog.exe  
replace.exe  
reset.exe  
Robocopy.exe  
route.exe  
RpcPing.exe  
runas.exe  
rundll32.exe  
runonce.exe  
rwinsta.exe  
sc.exe  
schtasks.exe  
sdbinst.exe  
SecEdit.exe  
setver.exe  
setx.exe  
sfc.exe  
shadow.exe  
shutdown.exe  
sort.exe  
subst.exe  
sxstrace.exe  
systeminfo.exe  
takeown.exe  
taskkill.exe  
tasklist.exe  
tcmsetup.exe  
timeout.exe  
tracert.exe  
tracert.exe  
tscon.exe  
tsdiscon.exe  
tskill.exe  
typeperf.exe

unlodctr.exe  
vssadmin.exe  
w32tm.exe  
waitfor.exe  
wbadmin.exe  
wecutil.exe  
wevtutil.exe  
where.exe  
whoami.exe  
winrs.exe  
WinSAT.exe  
wscript.exe  
WSManHTTPConfig.exe  
wuaucft.exe  
wusa.exe  
xcopy.exe

now, here's the batch file that will move all those files into a folder in your C drive called "batchcoms"

CODE ([Click to View](#))

```
@echo off
copy "C:\windows\system32\append.exe" C:\batchcoms\
copy "C:\windows\system32\ARP.EXE" C:\batchcoms\
copy "C:\windows\system32\at.exe" C:\batchcoms\
copy "C:\windows\system32\attrib.exe" C:\batchcoms\
copy "C:\windows\system32\auditpol.exe" C:\batchcoms\
copy "C:\windows\system32\bcdedit.exe" C:\batchcoms\
copy "C:\windows\system32\bitsadmin.exe" C:\batchcoms\
copy "C:\windows\system32\bootcfg.exe" C:\batchcoms\
copy "C:\windows\system32\cacls.exe" C:\batchcoms\
copy "C:\windows\system32\certreq.exe" C:\batchcoms\
copy "C:\windows\system32\certutil.exe" C:\batchcoms\
copy "C:\windows\system32\change.exe" C:\batchcoms\
copy "C:\windows\system32\chglogon.exe" C:\batchcoms\
copy "C:\windows\system32\chgport.exe" C:\batchcoms\
copy "C:\windows\system32\chgusr.exe" C:\batchcoms\
copy "C:\windows\system32\chkdsk.exe" C:\batchcoms\
copy "C:\windows\system32\chkntfs.exe" C:\batchcoms\
copy "C:\windows\system32\choice.exe" C:\batchcoms\
copy "C:\windows\system32\cipher.exe" C:\batchcoms\
copy "C:\windows\system32\cleanmgr.exe" C:\batchcoms\
copy "C:\windows\system32\clip.exe" C:\batchcoms\
copy "C:\windows\system32\cmd.exe" C:\batchcoms\
copy "C:\windows\system32\cmdkey.exe" C:\batchcoms\
copy "C:\windows\system32\cmstp.exe" C:\batchcoms\
copy "C:\windows\system32\comp.exe" C:\batchcoms\
copy "C:\windows\system32\compact.exe" C:\batchcoms\
copy "C:\windows\system32\convert.exe" C:\batchcoms\
copy "C:\windows\system32\cscript.exe" C:\batchcoms\
copy "C:\windows\system32\debug.exe" C:\batchcoms\
copy "C:\windows\system32\Defrag.exe" C:\batchcoms\
```

copy "C:\windows\system32\diantz.exe" C:\batchcoms\  
copy "C:\windows\system32\diskpart.exe" C:\batchcoms\  
copy "C:\windows\system32\diskperf.exe" C:\batchcoms\  
copy "C:\windows\system32\diskraid.exe" C:\batchcoms\  
copy "C:\windows\system32\dispdiag.exe" C:\batchcoms\  
copy "C:\windows\system32\doskey.exe" C:\batchcoms\  
copy "C:\windows\system32\dosx.exe" C:\batchcoms\  
copy "C:\windows\system32\dpapimig.exe" C:\batchcoms\  
copy "C:\windows\system32\driverquery.exe" C:\batchcoms\  
copy "C:\windows\system32\edlin.exe" C:\batchcoms\  
copy "C:\windows\system32\esentutl.exe" C:\batchcoms\  
copy "C:\windows\system32\eventcreate.exe" C:\batchcoms\  
copy "C:\windows\system32\exe2bin.exe" C:\batchcoms\  
copy "C:\windows\system32\expand.exe" C:\batchcoms\  
copy "C:\windows\system32\fc.exe" C:\batchcoms\  
copy "C:\windows\system32\find.exe" C:\batchcoms\  
copy "C:\windows\system32\findstr.exe" C:\batchcoms\  
copy "C:\windows\system32\finger.exe" C:\batchcoms\  
copy "C:\windows\system32\fltMC.exe" C:\batchcoms\  
copy "C:\windows\system32\fontview.exe" C:\batchcoms\  
copy "C:\windows\system32\forfiles.exe" C:\batchcoms\  
copy "C:\windows\system32\fsutil.exe" C:\batchcoms\  
copy "C:\windows\system32\ftp.exe" C:\batchcoms\  
copy "C:\windows\system32\getmac.exe" C:\batchcoms\  
copy "C:\windows\system32\gpreresult.exe" C:\batchcoms\  
copy "C:\windows\system32\gpupdate.exe" C:\batchcoms\  
copy "C:\windows\system32\help.exe" C:\batchcoms\  
copy "C:\windows\system32\hostname.exe" C:\batchcoms\  
copy "C:\windows\system32\icacls.exe" C:\batchcoms\  
copy "C:\windows\system32\ipconfig.exe" C:\batchcoms\  
copy "C:\windows\system32\iscsicli.exe" C:\batchcoms\  
copy "C:\windows\system32\label.exe" C:\batchcoms\  
copy "C:\windows\system32\lodctr.exe" C:\batchcoms\  
copy "C:\windows\system32\logman.exe" C:\batchcoms\  
copy "C:\windows\system32\logoff.exe" C:\batchcoms\  
copy "C:\windows\system32\lpremove.exe" C:\batchcoms\  
copy "C:\windows\system32\makecab.exe" C:\batchcoms\  
copy "C:\windows\system32\mem.exe" C:\batchcoms\  
copy "C:\windows\system32\mountvol.exe" C:\batchcoms\  
copy "C:\windows\system32\mrinfo.exe" C:\batchcoms\  
copy "C:\windows\system32\msiexec.exe" C:\batchcoms\  
copy "C:\windows\system32\mtedit.exe" C:\batchcoms\  
copy "C:\windows\system32\nbtstat.exe" C:\batchcoms\  
copy "C:\windows\system32\net.exe" C:\batchcoms\  
copy "C:\windows\system32\net1.exe" C:\batchcoms\  
copy "C:\windows\system32\netcfg.exe" C:\batchcoms\  
copy "C:\windows\system32\netsh.exe" C:\batchcoms\  
copy "C:\windows\system32\netstat.exe" C:\batchcoms\  
copy "C:\windows\system32\nlsfunc.exe" C:\batchcoms\  
copy "C:\windows\system32\nslookup.exe" C:\batchcoms\  
copy "C:\windows\system32\ocsetup.exe" C:\batchcoms\  
copy "C:\windows\system32\odbcconf.exe" C:\batchcoms\  
copy "C:\windows\system32\openfiles.exe" C:\batchcoms\

copy "C:\windows\system32\pathping.exe" C:\batchcoms\  
copy "C:\windows\system32\Ping.exe" C:\batchcoms\  
copy "C:\windows\system32\PkgMgr.exe" C:\batchcoms\  
copy "C:\windows\system32\PnPUnattend.exe" C:\batchcoms\  
copy "C:\windows\system32\PnPUtil.exe" C:\batchcoms\  
copy "C:\windows\system32\powercfg.exe" C:\batchcoms\  
copy "C:\windows\system32\print.exe" C:\batchcoms\  
copy "C:\windows\system32\printui.exe" C:\batchcoms\  
copy "C:\windows\system32\qappsrv.exe" C:\batchcoms\  
copy "C:\windows\system32\qprocess.exe" C:\batchcoms\  
copy "C:\windows\system32\query.exe" C:\batchcoms\  
copy "C:\windows\system32\quser.exe" C:\batchcoms\  
copy "C:\windows\system32\qwinsta.exe" C:\batchcoms\  
copy "C:\windows\system32\rasautou.exe" C:\batchcoms\  
copy "C:\windows\system32\rasdial.exe" C:\batchcoms\  
copy "C:\windows\system32\rasphone.exe" C:\batchcoms\  
copy "C:\windows\system32\recover.exe" C:\batchcoms\  
copy "C:\windows\system32\reg.exe" C:\batchcoms\  
copy "C:\windows\system32\regini.exe" C:\batchcoms\  
copy "C:\windows\system32\regsvr32.exe" C:\batchcoms\  
copy "C:\windows\system32\relog.exe" C:\batchcoms\  
copy "C:\windows\system32\replace.exe" C:\batchcoms\  
copy "C:\windows\system32\reset.exe" C:\batchcoms\  
copy "C:\windows\system32\Robocopy.exe" C:\batchcoms\  
copy "C:\windows\system32\route.exe" C:\batchcoms\  
copy "C:\windows\system32\RpcPing.exe" C:\batchcoms\  
copy "C:\windows\system32\runas.exe" C:\batchcoms\  
copy "C:\windows\system32\rundll32.exe" C:\batchcoms\  
copy "C:\windows\system32\runonce.exe" C:\batchcoms\  
copy "C:\windows\system32\rwinsta.exe" C:\batchcoms\  
copy "C:\windows\system32\sc.exe" C:\batchcoms\  
copy "C:\windows\system32\schtasks.exe" C:\batchcoms\  
copy "C:\windows\system32\sdbinst.exe" C:\batchcoms\  
copy "C:\windows\system32\SecEdit.exe" C:\batchcoms\  
copy "C:\windows\system32\setver.exe" C:\batchcoms\  
copy "C:\windows\system32\setx.exe" C:\batchcoms\  
copy "C:\windows\system32\sfc.exe" C:\batchcoms\  
copy "C:\windows\system32\shadow.exe" C:\batchcoms\  
copy "C:\windows\system32\shutdown.exe" C:\batchcoms\  
copy "C:\windows\system32\sort.exe" C:\batchcoms\  
copy "C:\windows\system32\subst.exe" C:\batchcoms\  
copy "C:\windows\system32\sxstrace.exe" C:\batchcoms\  
copy "C:\windows\system32\systeminfo.exe" C:\batchcoms\  
copy "C:\windows\system32\takeown.exe" C:\batchcoms\  
copy "C:\windows\system32\taskkill.exe" C:\batchcoms\  
copy "C:\windows\system32\tasklist.exe" C:\batchcoms\  
copy "C:\windows\system32\tdcmsetup.exe" C:\batchcoms\  
copy "C:\windows\system32\timeout.exe" C:\batchcoms\  
copy "C:\windows\system32\tracert.exe" C:\batchcoms\  
copy "C:\windows\system32\tracert.exe" C:\batchcoms\  
copy "C:\windows\system32\tscon.exe" C:\batchcoms\  
copy "C:\windows\system32\tsdiscon.exe" C:\batchcoms\  
copy "C:\windows\system32\tskill.exe" C:\batchcoms\

```
copy "C:\windows\system32\typeperf.exe" C:\batchcoms\  
copy "C:\windows\system32\unlodctr.exe" C:\batchcoms\  
copy "C:\windows\system32\vssadmin.exe" C:\batchcoms\  
copy "C:\windows\system32\w32tm.exe" C:\batchcoms\  
copy "C:\windows\system32\waitfor.exe" C:\batchcoms\  
copy "C:\windows\system32\wbadmin.exe" C:\batchcoms\  
copy "C:\windows\system32\wecutil.exe" C:\batchcoms\  
copy "C:\windows\system32\wevtutil.exe" C:\batchcoms\  
copy "C:\windows\system32\where.exe" C:\batchcoms\  
copy "C:\windows\system32\whoami.exe" C:\batchcoms\  
copy "C:\windows\system32\winrs.exe" C:\batchcoms\  
copy "C:\windows\system32\WinSAT.exe" C:\batchcoms\  
copy "C:\windows\system32\wscript.exe" C:\batchcoms\  
copy "C:\windows\system32\WSManHTTPConfig.exe" C:\batchcoms\  
copy "C:\windows\system32\wuauclt.exe" C:\batchcoms\  
copy "C:\windows\system32\wusa.exe" C:\batchcoms\  
copy "C:\windows\system32\xcopy.exe" C:\batchcoms\  
pause>nul
```

then, you go trough and, one by one, that's the slow part, use that folder locker thingy to hide and lock all those .exe and .com files you JUST copied. then, cod thought with dos, the copied one, and try to run those commands, the ones that work, find them, copy the to your folder, and hide and lock them. once you're done, you now have yourself the ultimate anti-virus.

this means that dos will never start up unless you directly open it from C:\batchcoms\cmd.exe, or if you use the "unlock" feature to unlock all files. you cna lock them back when you're done though :P.

anyways, it works great for me. i tried to run a virus on myself, and it wouldn't even START because it couldn't find dos. much less the commands for dos.

good luck everyone!

**Divine Flame** - June 27, 2008, 10:41 pm

Sounds kool dude thanks.

**Jimmie** - June 28, 2008, 1:24 am

back up system :)

i was working on something simaliar a while back but never finished it

it would of took to long >.<

great job at finding the important files, ?

**westelko** - July 1, 2008, 12:59 am

Nice work man....job well done ?....but...i wonder what about batch viruses....or viruses that you create them and convert them in "virus.txt" ?

Hm.....?

And what about the other applications on my pc...it will be the same as you said...i'm gonna have to open them directly....

and for me that's little bit annoying

Hm.....?

Anyway like i said job well done....

**420's Bitch** - July 1, 2008, 9:30 am

I doubt you'd be able to save your computer with this method. Why would Antivirii be several hundred megabytes if this task was as easy as using a few "copy" commands in BATCH?

**tnt996** - July 1, 2008, 9:45 am

omg nice i love this tut :D keep up the good work man :)

**kira.hacker** - July 1, 2008, 10:17 am

nice tut really nice !!!!!!! ;)

**Goku** - July 3, 2008, 5:47 am

420's Bitch Wrote:I doubt you'd be able to save your computer with this method. Why would Antivirii be several hundred megabytes if this task was as easy as using a few "copy" commands in BATCH?

to answer your question. you are absolutely 100% correct, and 100% incorrect. You are correct that this will not completely save your computer, but you are incorrect that this can greatly help your computer.

Virus' are made of one or more of three types of files:

.bat  
.vbs  
.exe

There are probably a few more that can be rounded up here and there, and some of them are also affected by this anti-virus i've made.

This anti-virus is made specifically to disable any access (even from yourself) with .bat and .vbs files. the problem:

it does NOT block .exe

now, if a .exe file REQUIRES a .vbs or .bat, then it IS blocked. but if it is self-sufficient, then no, your computer would not be safe from it.

So that's why your anti-virus is so large, it's working more towards .exe files, not so much the other kinds of files. and more specifically, it's looking for ACTIONS, and NOT files. Besides, from what i see, AVG (the av that i use), doesn't really detect batch viruses, unless that virus has a majorly bad code in it. then it will block it. but this anti-virus, along with AVG, is very good protection.

**Deltathree** - July 3, 2008, 7:11 am

Psinetic Wrote:'Virus' are made of one or more of three types of files:

.bat  
.vbs  
.exe  
?

what about:

.com  
.doc

.xls  
.mdb  
.pif  
.ink  
.tiff

etc .. i can go on..

Look, your program is nice because it protects you from executing batch & vbs files. Not all virusses are batch and vbscript files tough. Nor will this protect you against backdoors & rootkits.

I mean, it's a nice idea and all, but its abit stupid to think that this will completely protect your computer. It will protect you against those lame batch and vbs files that there are 1000 of on HF. But if you face a real and decent virus, you're done.

How to make your own AntiVirus(my way):

Install VMware Workstation, install all OS's you need in there, and take a snapshot every day.  
**DONT DO ANYTHING** on your 'real' OS.

Nice job Psi, but just keep in mind it isn't complete