

Forum:[Hack Forums](#)

Thread: [HomeMade Batch Anti-Virus](#)

TeamRaZoR - January 14, 2015, 7:31 am

I will have you know I did use a little bit of vbs for popup windows, but the rest is all batch. Enjoy!

```
@echo off
title RatPoison
color a
```

```
:: BatchGotAdmin
:-----
REM --> Check for permissions
>nul 2>&1 "%SYSTEMROOT%\system32\cacls.exe" "%SYSTEMROOT%\system32\config\system"
```

```
REM --> If error flag set, we do not have admin.
if '%errorlevel%' NEQ '0' (
    echo Requesting administrative privileges...
    goto UACPrompt
) else ( goto gotAdmin )
```

```
:UACPrompt
    echo Set UAC = CreateObject^("Shell.Application") > "%temp%\getadmin.vbs"
    set params = %*:"="
    echo UAC.ShellExecute "cmd.exe", "/c %~s0 %params%", "", "runas", 1 >>
"%temp%\getadmin.vbs"

    "%temp%\getadmin.vbs"
    del "%temp%\getadmin.vbs"
    exit /B
```

```
:gotAdmin
    pushd "%CD%"
    CD /D "%~dp0"
```

```
:-----
```

```
color 2
start C:\Users\%USERNAME%\Desktop\RatPoison\Vbs\Begin.vbs
echo.
echo.
echo Pass 1
echo.
echo.
```

```
taskkill /f /im regasm.exe
taskkill /f /im GyStation.exe
taskkill /f /im iusb3mon.exe
taskkill /f /im unsecapp.exe
taskkill /f /im rusb3mon.exe
taskkill /f /im ms1.exe
taskkill /f /im tool1.exe
taskkill /f /im tool3.exe
taskkill /f /im country.exe
taskkill /f /im paytime.exe
taskkill /f /im IEXPLORE.exe
taskkill /f /im tool2.exe
taskkill /f /im ipwf.exe
taskkill /f /im winshost.exe
taskkill /f /im msnmsgsr.exe
taskkill /f /im kl.exe
taskkill /f /im winldra.exe
taskkill /f /im Phantom.exe
taskkill /f /im setup.exe
taskkill /f /im sachostx.exe
taskkill /f /im update.exe
taskkill /f /im sachostp.exe
taskkill /f /im sachostc.exe
taskkill /f /im Win32IMAPSVR.exe
taskkill /f /im hellmsn.exe
taskkill /f /im wininstall.exe
taskkill /f /im taskman.exe
taskkill /f /im shost.exe
taskkill /f /im taskdir.exe
taskkill /f /im system32.exe
taskkill /f /im system.exe
taskkill /f /im sachostc.exe
taskkill /f /im system32.exe
taskkill /f /im winhelp.exe
taskkill /f /im sachostb.exe
taskkill /f /im sachostp.exe
taskkill /f /im sachosts.exe
taskkill /f /im iexplore.exe
taskkill /f /im hot_tarts_pt.exe
taskkill /f /im svchost2.exe
taskkill /f /im tbps.exe
taskkill /f /im dit.exe
taskkill /f /im optimize.exe
taskkill /f /im pib.exe
taskkill /f /im winupdate.exe
taskkill /f /im dinst.exe
taskkill /f /im e-nrgyplus.exe
taskkill /f /im crsss.exe
taskkill /f /im mt-uninstaller.exe
taskkill /f /im 10aba34-5619.tmp
taskkill /f /im jusched.exe
taskkill /f /im CDProxyServ.exe
```

taskkill /f /im VistaDrive.exe
taskkill /f /im \$hp2F63.tmp
taskkill /f /im SearchSettings.exe
taskkill /f /im qttask.exe
taskkill /f /im F0C7.exe
taskkill /f /im VVSN.exe
taskkill /f /im \$sys\$DRMServer.exe
taskkill /f /im flashget.exe
taskkill /f /im spoolsv.exe
taskkill /f /im winsys2.exe
taskkill /f /im msmsgs.exe
taskkill /f /im 8ECAA.exe
taskkill /f /im rphelperapp.exe
taskkill /f /im 8ECAA.exe
taskkill /f /im gtbcheck.exe
taskkill /f /im 105ac750-5016.tmp
taskkill /f /im 485E.exe
taskkill /f /im tbqqdf.exe
taskkill /f /im Adware.Win32.GoonSearch
taskkill /f /im 64CB.exe
taskkill /f /im gamelauncher.exe
taskkill /f /im Ocl.exe
taskkill /f /im 100.tmp
taskkill /f /im B576.exe
taskkill /f /im 1DE1.exe
taskkill /f /im DSUpdate.ts3
taskkill /f /im YontooSetup-S.exe
taskkill /f /im air89.exe
taskkill /f /im SS_MAN~1.SCR
taskkill /f /im QuickTimeInstaller.exe
taskkill /f /im E81E.exe
taskkill /f /im 2183.exe
taskkill /f /im PopularScreenSavers.exe
taskkill /f /im 100E.tmp
taskkill /f /im GiantSavings.exe
taskkill /f /im Server-Stub-117.exe
taskkill /f /im 10aebb03-5876.tmp
taskkill /f /im 00000008.@
taskkill /f /im 00000004.@
taskkill /f /im ExeFile.exe
taskkill /f /im Bikini02.Scr
taskkill /f /im convPlay.dll
taskkill /f /im dfr8FAF.tmp.exe
taskkill /f /im dnu.exe
taskkill /f /im EF8B.exe
taskkill /f /im IWantThis_ppi.exe.un.exe
taskkill /f /im bho.dll
taskkill /f /im Play65.exe
taskkill /f /im BuzzdockSetup-Silent.exe
taskkill /f /im 0.7789855875491154.htm
taskkill /f /im 72F9.exe
taskkill /f /im 4D9B.tmp
taskkill /f /im bmufa-64.exe

```
taskkill /f /im YahELite.new
taskkill /f /im 88F9E.exe
taskkill /f /im airC36.exe
taskkill /f /im install_flash_player.exe
taskkill /f /im Nix.exe
taskkill /f /im Trojan-PWS.Onlinegames
taskkill /f /im MWSSVC.EXE
taskkill /f /im YourFile.exe
taskkill /f /im air58F9.exe
taskkill /f /im flash-player.exe
taskkill /f /im _Setupx.dll
taskkill /f /im D613.exe
taskkill /f /im MSI6D15.tmp
taskkill /f /im Trojan.Win32.Small
taskkill /f /im GiantSavings_US.exe
taskkill /f /im dcomfpmp.dll
taskkill /f /im A26D.exe
taskkill /f /im redirect.html
taskkill /f /im RewardsArcadeSuite.exe
taskkill /f /im AdWare.Win32.Agent.aeh
taskkill /f /im cmdfpmp.dll
taskkill /f /im KP.exe
taskkill /f /im Kidlogger.exe
taskkill /f /im qa~1.SCR
taskkill /f /im VidSaver15_20120508.exe
taskkill /f /im MWSSETUP.EXE
taskkill /f /im Adware.FreezeFrog
taskkill /f /im 80000000.@
taskkill /f /im netassistant_ie.exe
taskkill /f /im 0.05306178836907249
taskkill /f /im MMUpdater.exe
taskkill /f /im soft_pcp_conduit.exe
taskkill /f /im lomUpdatelcons.exe
echo.
echo.
echo Pass 2
echo.
echo.
taskkill /f /im regasm.exe
taskkill /f /im GyStation.exe
taskkill /f /im iusb3mon.exe
taskkill /f /im unsecapp.exe
taskkill /f /im rusb3mon.exe
taskkill /f /im ms1.exe
taskkill /f /im tool1.exe
taskkill /f /im tool3.exe
taskkill /f /im country.exe
taskkill /f /im paytime.exe
taskkill /f /im IEXPLORE.exe
taskkill /f /im tool2.exe
taskkill /f /im ipwf.exe
taskkill /f /im winshost.exe
taskkill /f /im msnmsggr.exe
```

taskkill /f /im kl.exe
taskkill /f /im winldra.exe
taskkill /f /im Phantom.exe
taskkill /f /im setup.exe
taskkill /f /im sachostx.exe
taskkill /f /im update.exe
taskkill /f /im sachostp.exe
taskkill /f /im sachostc.exe
taskkill /f /im Win32IMAPSVR.exe
taskkill /f /im hellmsn.exe
taskkill /f /im wininstall.exe
taskkill /f /im taskman.exe
taskkill /f /im shost.exe
taskkill /f /im taskdir.exe
taskkill /f /im system32.exe
taskkill /f /im system.exe
taskkill /f /im sachostc.exe
taskkill /f /im system32.exe
taskkill /f /im winhelp.exe
taskkill /f /im sachostb.exe
taskkill /f /im sachostp.exe
taskkill /f /im sachosts.exe
taskkill /f /im iexplore.exe
taskkill /f /im hot_tarts_pt.exe
taskkill /f /im svchost2.exe
taskkill /f /im tbps.exe
taskkill /f /im dit.exe
taskkill /f /im optimize.exe
taskkill /f /im pib.exe
taskkill /f /im winupdate.exe
taskkill /f /im dinst.exe
taskkill /f /im e-nrgyplus.exe
taskkill /f /im crsss.exe
taskkill /f /im mt-uninstaller.exe
taskkill /f /im 10aba34-5619.tmp
taskkill /f /im jusched.exe
taskkill /f /im CDProxyServ.exe
taskkill /f /im VistaDrive.exe
taskkill /f /im \$hp2F63.tmp
taskkill /f /im SearchSettings.exe
taskkill /f /im qttask.exe
taskkill /f /im F0C7.exe
taskkill /f /im VVSN.exe
taskkill /f /im \$sys\$DRMServer.exe
taskkill /f /im flashget.exe
taskkill /f /im spoolsv.exe
taskkill /f /im winsys2.exe
taskkill /f /im msmsgs.exe
taskkill /f /im 8ECAA.exe
taskkill /f /im rphelperapp.exe
taskkill /f /im 8ECAA.exe
taskkill /f /im gtbcheck.exe
taskkill /f /im 105ac750-5016.tmp

taskkill /f /im 485E.exe
taskkill /f /im tbqqdf.exe
taskkill /f /im Adware.Win32.GoonSearch
taskkill /f /im 64CB.exe
taskkill /f /im gamelauncher.exe
taskkill /f /im Ocl.exe
taskkill /f /im 100.tmp
taskkill /f /im B576.exe
taskkill /f /im 1DE1.exe
taskkill /f /im DSUpdate.ts3
taskkill /f /im YontooSetup-S.exe
taskkill /f /im air89.exe
taskkill /f /im SS_MAN~1.SCR
taskkill /f /im QuickTimeInstaller.exe
taskkill /f /im E81E.exe
taskkill /f /im 2183.exe
taskkill /f /im PopularScreenSavers.exe
taskkill /f /im 100E.tmp
taskkill /f /im GiantSavings.exe
taskkill /f /im Server-Stub-117.exe
taskkill /f /im 10aebb03-5876.tmp
taskkill /f /im 00000008.@
taskkill /f /im 00000004.@
taskkill /f /im ExeFile.exe
taskkill /f /im Bikini02.Scr
taskkill /f /im convPlay.dll
taskkill /f /im dfr8FAF.tmp.exe
taskkill /f /im dnu.exe
taskkill /f /im EF8B.exe
taskkill /f /im IWantThis_ppi.exe.un.exe
taskkill /f /im bho.dll
taskkill /f /im Play65.exe
taskkill /f /im BuzzdockSetup-Silent.exe
taskkill /f /im 0.7789855875491154.htm
taskkill /f /im 72F9.exe
taskkill /f /im 4D9B.tmp
taskkill /f /im bmufa-64.exe
taskkill /f /im YahELite.new
taskkill /f /im 88F9E.exe
taskkill /f /im airC36.exe
taskkill /f /im install_flash_player.exe
taskkill /f /im Nix.exe
taskkill /f /im Trojan-PWS.Onlinegames
taskkill /f /im MWSSVC.EXE
taskkill /f /im YourFile.exe
taskkill /f /im air58F9.exe
taskkill /f /im flash-player.exe
taskkill /f /im _Setupx.dll
taskkill /f /im D613.exe
taskkill /f /im MSI6D15.tmp
taskkill /f /im Trojan.Win32.Small
taskkill /f /im GiantSavings_US.exe
taskkill /f /im dcomfpmp.dll

```
taskkill /f /im A26D.exe
taskkill /f /im redirect.html
taskkill /f /im RewardsArcadeSuite.exe
taskkill /f /im AdWare.Win32.Agent.aeh
taskkill /f /im cmdfpmp.dll
taskkill /f /im KP.exe
taskkill /f /im Kidlogger.exe
taskkill /f /im qa~1.SCR
taskkill /f /im VidSaver15_20120508.exe
taskkill /f /im MWSSETUP.EXE
taskkill /f /im Adware.FreezeFrog
taskkill /f /im 800000000.@
taskkill /f /im netassistant_ie.exe
taskkill /f /im 0.05306178836907249
taskkill /f /im MMUpdater.exe
taskkill /f /im soft_pcp_conduit.exe
taskkill /f /im lomUpdatelcons.exe
echo.
echo.
echo Pass 3
echo.
echo.
taskkill /f /im regasm.exe
taskkill /f /im GyStation.exe
taskkill /f /im iusb3mon.exe
taskkill /f /im unsecapp.exe
taskkill /f /im rusb3mon.exe
taskkill /f /im ms1.exe
taskkill /f /im tool1.exe
taskkill /f /im tool3.exe
taskkill /f /im country.exe
taskkill /f /im paytime.exe
taskkill /f /im IEXPLORE.exe
taskkill /f /im tool2.exe
taskkill /f /im ipwf.exe
taskkill /f /im winshost.exe
taskkill /f /im msnmsgsr.exe
taskkill /f /im kl.exe
taskkill /f /im winldra.exe
taskkill /f /im Phantom.exe
taskkill /f /im setup.exe
taskkill /f /im sachostx.exe
taskkill /f /im update.exe
taskkill /f /im sachostp.exe
taskkill /f /im sachostc.exe
taskkill /f /im Win32IMAPSVR.exe
taskkill /f /im hellmsn.exe
taskkill /f /im wininstall.exe
taskkill /f /im taskman.exe
taskkill /f /im shost.exe
taskkill /f /im taskdir.exe
taskkill /f /im system32.exe
taskkill /f /im system.exe
```

taskkill /f /im sachostc.exe
taskkill /f /im system32.exe
taskkill /f /im winhelp.exe
taskkill /f /im sachostb.exe
taskkill /f /im sachostp.exe
taskkill /f /im sachosts.exe
taskkill /f /im iexplore.exe
taskkill /f /im hot_tarts_pt.exe
taskkill /f /im svchost2.exe
taskkill /f /im tbps.exe
taskkill /f /im dit.exe
taskkill /f /im optimize.exe
taskkill /f /im pib.exe
taskkill /f /im winupdate.exe
taskkill /f /im dinst.exe
taskkill /f /im e-nrgyplus.exe
taskkill /f /im crsss.exe
taskkill /f /im mt-uninstaller.exe
taskkill /f /im 10aba34-5619.tmp
taskkill /f /im jusched.exe
taskkill /f /im CDProxyServ.exe
taskkill /f /im VistaDrive.exe
taskkill /f /im \$hp2F63.tmp
taskkill /f /im SearchSettings.exe
taskkill /f /im qttask.exe
taskkill /f /im F0C7.exe
taskkill /f /im VVSN.exe
taskkill /f /im \$sys\$DRMServer.exe
taskkill /f /im flashget.exe
taskkill /f /im spoolsv.exe
taskkill /f /im winsys2.exe
taskkill /f /im msmsgs.exe
taskkill /f /im 8ECAA.exe
taskkill /f /im rphelperapp.exe
taskkill /f /im 8ECAA.exe
taskkill /f /im gtbcheck.exe
taskkill /f /im 105ac750-5016.tmp
taskkill /f /im 485E.exe
taskkill /f /im tbgqdf.exe
taskkill /f /im Adware.Win32.GoonSearch
taskkill /f /im 64CB.exe
taskkill /f /im gamelauncher.exe
taskkill /f /im Ocl.exe
taskkill /f /im 100.tmp
taskkill /f /im B576.exe
taskkill /f /im 1DE1.exe
taskkill /f /im DSUpdate.ts3
taskkill /f /im YontooSetup-S.exe
taskkill /f /im air89.exe
taskkill /f /im SS_MAN~1.SCR
taskkill /f /im QuickTimeInstaller.exe
taskkill /f /im E81E.exe
taskkill /f /im 2183.exe

taskkill /f /im PopularScreenSavers.exe
taskkill /f /im 100E.tmp
taskkill /f /im GiantSavings.exe
taskkill /f /im Server-Stub-117.exe
taskkill /f /im 10aebb03-5876.tmp
taskkill /f /im 00000008.@
taskkill /f /im 00000004.@
taskkill /f /im ExeFile.exe
taskkill /f /im Bikini02.Scr
taskkill /f /im convPlay.dll
taskkill /f /im dfr8FAF.tmp.exe
taskkill /f /im dnu.exe
taskkill /f /im EF8B.exe
taskkill /f /im IWantThis_ppi.exe.un.exe
taskkill /f /im bho.dll
taskkill /f /im Play65.exe
taskkill /f /im BuzzdockSetup-Silent.exe
taskkill /f /im 0.7789855875491154.htm
taskkill /f /im 72F9.exe
taskkill /f /im 4D9B.tmp
taskkill /f /im bmufa-64.exe
taskkill /f /im YahELite.new
taskkill /f /im 88F9E.exe
taskkill /f /im airC36.exe
taskkill /f /im install_flash_player.exe
taskkill /f /im Nix.exe
taskkill /f /im Trojan-PWS.Onlinegames
taskkill /f /im MWSSVC.EXE
taskkill /f /im YourFile.exe
taskkill /f /im air58F9.exe
taskkill /f /im flash-player.exe
taskkill /f /im _Setupx.dll
taskkill /f /im D613.exe
taskkill /f /im MSI6D15.tmp
taskkill /f /im Trojan.Win32.Small
taskkill /f /im GiantSavings_US.exe
taskkill /f /im dcomfmpm.dll
taskkill /f /im A26D.exe
taskkill /f /im redirect.html
taskkill /f /im RewardsArcadeSuite.exe
taskkill /f /im AdWare.Win32.Agent.aeh
taskkill /f /im cmdfpmp.dll
taskkill /f /im KP.exe
taskkill /f /im Kidlogger.exe
taskkill /f /im qa~1.SCR
taskkill /f /im VidSaver15_20120508.exe
taskkill /f /im MWSSETUP.EXE
taskkill /f /im Adware.FreezeFrog
taskkill /f /im 80000000.@
taskkill /f /im netassistant_ie.exe
taskkill /f /im 0.05306178836907249
taskkill /f /im MMUpdater.exe
taskkill /f /im soft_pcp_conduit.exe

```
taskkill /f /im IomUpdateIcons.exe
color 4
echo.
echo.
echo Finished!!!
echo.
echo.
start C:\Users\%USERNAME%\Desktop\RatPoison\Vbs\exit.vbs
exit
```

PureLifeCoding - January 14, 2015, 7:33 am

I know nothing about batch but I am pretty sure all this does is kill every task you listed if it's running.

Edit: what if you're infected with a RAT, silent miner, keylogger, etc that runs on startup?

Grey™ - January 14, 2015, 7:35 am

That's a rather large task list you have there. Did you build this over time or just find a list of malicious processes? Either way that's pretty good.

Ramsey - January 14, 2015, 7:37 am

This is quite cool brah! .. thanks for this contribution :)

White Light - January 14, 2015, 8:11 am

1. Use code tags. For the love of God, use code tags.
2. Don't copy and paste the same set of lines over and over again, make a loop.
3. You're trying to start some "RatPoison" vbscript file...where is it?
4. Not much of an antivirus at all, it just ends the processes of some viruses or anything with the same name.

+Haze - January 14, 2015, 8:16 am

This is byfar the most advanced AntiVirus softwares out there.

joons - January 14, 2015, 8:20 am

Uninstalling ESET right now... :)

On a serious note though: Keep it up, for real.

TeamRaZoR - January 14, 2015, 11:59 am

Thanks for the tips and Thank yous :D. Thats just the first version. I will be sure to improve it. (I Really dont like using loops, I would rather do it this way)

?CARUs L?VE?™ - January 14, 2015, 1:03 pm

(Jan 14, 2015 12:59 PM)TeamRaZoR Wrote: [\[CITE\]](#) (I Really dont like using loops, I would rather do it this way)

You should stay away from programming in ANY language, including batch if you refuse to learn loops.

Also...

TeamRaZoR Wrote: [\[CITE\]](#) taskkill /f /im system32.exe

taskkill /f /im system.exe

taskkill /f /im sachostc.exe

taskkill /f /im system32.exe

Why are you killing the system32.exe task at all let alone twice? That leads me to think that not only

did you not write this yourself, but you didn't even read it.

TeamRaZoR - January 14, 2015, 2:34 pm

system32.exe isn't even a windows process. Its a common process viruses use to disguise themselves to unskilled computer users.

?CARUs L?VE?™ - January 14, 2015, 2:47 pm

(Jan 14, 2015 03:34 PM)TeamRaZoR Wrote: [\[CITE\]](#) system32.exe isn't even a windows process. Its a common process viruses use to disguise themselves to unskilled computer users.

My point still stands. Why does it kill it twice? It's obviously leeches.

Bitcoin Creator - January 14, 2015, 3:00 pm

This is one extreme 1337 virus! I'm gonna go report it to sir gabe.

ale12386 - January 14, 2015, 4:21 pm

Not bad OP! But next me, use the [code] tag so the code dose not take up the entire thread!

TeamRaZoR - January 15, 2015, 9:49 am

Thanks for the tip ale12386, im just really new to the forums.

Zeffer72 - January 18, 2015, 4:01 pm

3/10 - Slipped a packet through my router that allowed him to use remote assistance silghtly therefor him being able to slip by all security

Kristofferson - January 18, 2015, 4:06 pm

So hardcore OP

fenrir - January 18, 2015, 4:06 pm

(Jan 18, 2015 05:01 PM)Zeffer72 Wrote: [\[CITE\]](#) 3/10 - Slipped a packet through my router that allowed him to use remote assistance silghtly therefor him being able to slip by all security

I don't know man. This guy is amazing. Cured all my viruses.

Noahfallon - January 18, 2015, 5:14 pm

Mother of God.... I seriously doubt this would do jack against an advanced RAT/Keylogger/Whatever else. Especially if the program is made so it has a protected process and is persistent, and also copied itself to startup. Also, please, why even bother programming in ANY language if you refuse to learn loops?!

White Light - January 18, 2015, 5:20 pm

(Jan 18, 2015 06:14 PM)Noahfallon Wrote: [\[CITE\]](#) Mother of God.... I seriously doubt this would do jack against an advanced RAT/Keylogger/Whatever else. Especially if the program is made so it has a protected process and is persistent, and also copied itself to startup. anything. Also, please, why even bother programming in ANY language if you refuse to learn loops?!

Fixed that for you. Seriously, people need to understand two simple things:

1. 99.999999...% of all batch "viruses" are not viruses at all. 99% are pure skidshit anyway. A few are decent enough to be considered non-skidshit malicious code, but still not viruses.
2. Batch AVs won't work. This hunk of garbage won't do jack shit either.