

Forum:[Hack Forums](#)

Thread: [Rose in Pure Batch script](#)

?CARUs L?VE?™ - July 26, 2026, 3:38 pm

Hello!

Been a long time since I've posted, but I have something cool to show again. This is 100% batch script. Enjoy!

<https://github.com/IcarusLivesHF/Batch-Script-Projects/tree/main/rose>

? loading encrypted image...

Tha Sneak - July 26, 2026, 6:19 pm

Excellent work, most people don't realize how powerful batch script can truly be especially when you include other command line applications with it.

Some of the most powerful malware removal tools created were made with batch script calling various powerful command line utilities that had an important role for each piece. Since you're interested in batch scripting I'll send you the source codes.

You'll be amazed as batch scripting in my opinion has always been an art of its own.

TooBuck - August 1, 2026, 9:12 am

The fact that this can even be accomplished in batch blows my mind. Very cool! And that script...good Lord! Super complex!

Tha Sneak - August 1, 2026, 9:20 am

(Aug 1, 2026 09:12 AM)TooBuck Wrote: [\[CITE\]](#) The fact that this can even be accomplished in batch blows my mind. Very cool! And that script...good Lord! Super complex!

If you want to check out more complex scripting take a look at ComboFix's source code. All you have to do is right click the exe file and extract it. It uses a combination of numerous command line tools using batch files for everything. When I first started learning batch files I loved them until I met PowerShell now me and PowerShell are best friends.

Here is a snippet of the code:

Quote:@ECHO OFF

TITLE ComboFix

COLOR 17

@CD /D "%~DP0"

@CALL VerCF.bat

@(

TYPE myNul.dat > ..\TestPrivs.txt

)>N_ \%random% 2>&1 ||(

START PEV EXEC %~DP0NIRCMD.%cfExt% EXEC SHOW %COMSPEC% /c %0

EXIT

```
)
@DEL /A/F ..\TestPrivs.txt

@IF EXIST chcp.bat CALL chcp.bat >N_ \%random% 2>&1
@IF EXIST F3m0.mrk EXIT
@TYPE myNul.dat >F3m0.mrk
SET "PATHEXT=.%cfExt%;%pathext%"

IF EXIST ComboDel.txt DEL /A/F ComboDel.txt

IF DEFINED username IF EXIST "%username%.user.cf" CALL setpath.bat >N_ \%random% 2>&1

IF DEFINED username IF NOT EXIST "%username%.user.cf" (
SET "Combobatch-by=[%username%]"
CALL SetEnvmt.bat >N_ \%random% 2>&1
)

IF NOT DEFINED username CALL setpath.bat >N_ \%random% 2>&1
CALL Lang.bat >N_ \%random% 2>&1

@ECHO.%Line1%

:: IF NOT DEFINED ChkSum (
:: @PEV -rtf -c:#@SET chksum=#5# .\md5sum.pif -output:md501.bat
:: @ECHO.@>> md501.bat
:: @CALL md501.bat
:: @DEL /A/F md501.bat
:: )>N_ \%random% 2>&1

REM IF EXIST FixCSet.dat %KMD% /C CSet.cmd >N_ \%random% 2>&1

SWREG QUERY "hklm\system\select" /v "current" >CurrentCS00
SED -r "/.* !/d; s!/00/; s/^[0-9]*(...) .*/@SET ControlSet=ControlSet\1\nSET
CS00=HKEY_LOCAL_MACHINE\system\\ControlSet\1\\Services/" CurrentCS00 >CCS.bat
CALL CCS.bat
DEL /A/F CurrentCS00 PathX

@SWREG ADD "hkcu\software\microsoft\windows\currentversion\policies\system" /v
"disableregistrytools" /t reg_dword /d 0 >N_ \%random% 2>&1
@IF NOT EXIST Vista.krl SWREG ACL "hklm\software\microsoft\windows
nt\currentversion\windows" /RE:F /Q

REGT /S creg.dat >N_ \%random% 2>&1
REGT /S CregC.dat >N_ \%random% 2>&1

IF EXIST LspFixed.reg REGT /S LspFixed.reg
@IF NOT EXIST Vista.krl SWREG ACL "hklm\software\microsoft\windows
nt\currentversion\windows" /DE:F /Q
IF EXIST SysRan GOTO END
IF NOT DEFINED username TYPE myNul.dat >SysRan
```

```

IF EXIST embedded.key @(
PEV -k rundll32.exe >N_\\%random% 2>&1
SWREG null query hkcr\clsid /s /f >embedded
SED "/.{H;$!d;};x;\nhkey_classes_root\clsid\{.*}\\storage\*\1\n\!d;" embedded >temp00
SED -r "/"^
+reg_name .* /\!d;s///s/.*/\nhkey_local_machine\software\microsoft\windows\currentversion\polic
ies\explorer\run\]\x22&x22=-/" temp00 >>CregC.dat
SED "/.{H;$!d;};x;/start_function.*WLEntry/\!d;" embedded >temp01
SED -r "/^( file_(name|expand|path) .* |$)/\!d;s///" temp01 >temp02
SED -r ":a; $!N;s/\n(.)/ \1/ta;P;D;s/^ //" temp02 >temp03
SED -r -f embedded.sed temp03 >temp04
SED "/ /d" temp04 >temp05
FINDSTR -MIF:temp05 "exefile\shell\open\command"
PEV -r -tpmz -s=113664 "%system%\*" or "%system%\drivers\*" or "%temp%\*" -output:temp06
FINDSTR -MIF:temp06 "exefile\shell\open\command"
)>>d-del2A.dat 2>N_\\%random%
DEL /A/F/Q temp0? L_Beep00 >N_\\%random% 2>&1

```

```

IF EXIST auxx.bat (
%KMD% /C auxx.bat
DEL /A/F auxx.bat
)>N_\\%random% 2>&1

```

```

IF EXIST Foreign.dat FOR /F "TOKENS=*" %%G IN ( Foreign.dat ) DO @IF EXIST "%~G"
MOVE /Y "%~G" "%~G.vir" >N_\\%random% 2>&1

```

```

IF EXIST Mad.dat FOR /F "TOKENS=*" %%G IN ( Mad.dat ) DO @(
GREP -Lisq windbg48 "%~G" >d-del2A.dat &&(
SWREG DELETE "hkml\system\currentcontrolset\services\%~NG"
SWREG ACL "hkml\system\currentcontrolset\enum\root\%~NG" /GE:F /P /Q
SWREG DELETE "hkml\system\currentcontrolset\enum\root\%~NG"
@ECHO.Legacy_%~NG>>SvcTarget.dat
@ECHO.-----\%~NG>>SvcTarget.dat
)||
REGT /S "\QooBox\Quarantine\Registry_backups\services_%~NG.reg.dat"
DEL /A/F "\QooBox\Quarantine\Registry_backups\services_%~NG.reg.dat"
PEV SC start "%~NG"
)>N_\\%random% 2>&1

```

```

ECHO.::::>>rootkit.dat
IF EXIST d-del4AV.old (
GREP -Fisvf rootkit.dat d-del4AV.old >whitedir01
FOR /F "TOKENS=*" %%H IN ( whitedir01 ) DO @IF EXIST "%~H" (PEV -rtf -t!o "%~H"
>>d-del2A.dat) ELSE ECHO."%~H">>drev.dat
)
GREP -sq :\\ Rootkit.dat || DEL /A/F Rootkit.dat

```

```

IF EXIST d-del3AA.dat @(

```

```
FOR /F "TOKENS=*" %%G IN ( d-del3AA.dat ) DO @IF EXIST "%%~G"
ECHO."%%~G">>d-del2A.dat
DEL /A/F d-del3AA.dat 2>N_\\%random%
)
```

```
IF EXIST Navipromo.dat FOR /F "TOKENS=*" %%G IN ( Navipromo.dat ) DO @%KMD% /C PEV
-rtf "%system%\*" and { "%%~G.exe" or "%%~G*.dat" } >>d-del2A.dat
```

```
DEL /A/Q %systemdrive%\qoobox\lastrun\d-del4AV.oldt whitedir0? Mad.dat Navipromo.dat N_\\*
>N_\\%random% 2>&1
```

```
GREP -Fli t1.jfglass.net "%commonProgFiles%\*" >>d-del2A.dat 2>N_\\%random%
FINDSTR -MIR Q.Q.2.0.0.7...T.e.n.c.e.n.t...H.e.l.p.e.r "%commonstartup%\*.lnk" >>d-del2A.dat
2>N_\\%random%
```

```
PEV -rtf -t!o -s+52000 -s-60000 "%system%\?????.dll" | FINDSTR -MF:/ QqHelperJ.dll temp00
>>d-del2A.dat 2>N_\\%random%
```

```
SED "1!d;s/.*\\/" whitedir.dat >whitedir00
```

```
IF EXIST Xorer (
TYPE Xorer >>d-del2A.dat
PEV -rtf "%CommonStartup%\~.exe*.exe" >>d-del2A.dat
PEV -rtf "%Startup%\~.exe*.exe" >>d-del2A.dat
DEL /A/F Xorer 2>N_\\%random%
)
```

```
IF EXIST d-del2AAA.dat TYPE d-del2AAA.dat >> d-del2A.dat && DEL /A/F d-del2AAA.dat
%systemdrive%\qoobox\lastrun\2AAA.dat 2>N_\\%random%
```

```
SETLOCAL
@SET SESSIONNAME=
@SET CLIENTNAME=
@SET COMPUTERNAME=
@SET HOMEDRIVE=
@SET HOMEPATH=
@SET J2D_D3D=
@SET NUMBER_OF_PROCESSORS=
@SET OS=
@SET PROCESSOR_ARCHITECTURE=
@SET PROCESSOR_IDENTIFIER=
@SET PROCESSOR_LEVEL=
@SET PROCESSOR_REVISION=
@SET PROMPT=
@SET USERDOMAIN=
@SET USERNAME=
```

```
IF EXIST d-del2A.dat FOR /F "TOKENS=*" %%G IN ( d-del2A.dat ) DO @IF EXIST "%%~G" IF
NOT EXIST "%%~G\" (
```

```

PEV -k "%~G"
%KMD% /D /C MoveIt.bat "%~G"
IF EXIST "%~G" (
    ECHO.%~G . . . %Fail2Delete%>>drev.dat
) ELSE ECHO."%~G">>drev.dat
)>N_ \%random% 2>&1

IF EXIST x64d-del2A.dat FOR /F "TOKENS=1* DELIMS= " %%G IN ( x64d-del2A.dat ) DO @IF
EXIST "%~H" IF NOT EXIST "%~H\" (
    %KMD% /D /C MoveIt.bat "%~H"
    IF EXIST "%~H" (
        ECHO.%~G . . . %Fail2Delete%>>x64drev.dat
    ) ELSE ECHO."%~G">>x64drev.dat
)>N_ \%random% 2>&1

IF EXIST d-del2b.dat FOR /F "TOKENS=*" %%G IN ( d-del2b.dat ) DO @IF EXIST "%~G" (
    RD "%~G" >N_ \%random% 2>&1
    IF EXIST "%~G" RD /S/Q "%~G" >N_ \%random% 2>&1
    IF EXIST "%~G" (
        ECHO.%~G . . . %Fail2Delete%>>drevF.dat
    ) ELSE ECHO."%~G">>drevF.dat
)>N_ \%random% 2>&1

IF EXIST x64d-del2b.dat FOR /F "TOKENS=1* DELIMS= " %%G IN ( x64d-del2b.dat ) DO @IF
EXIST "%~H\" (
    RD "%~H" >N_ \%random% 2>&1
    IF EXIST "%~H" RD /S/Q "%~H" >N_ \%random% 2>&1
    IF EXIST "%~H\" (
        ECHO.%~G . . . %Fail2Delete%>>x64drevF.dat
    ) ELSE ECHO."%~G">>x64drevF.dat
)>N_ \%random% 2>&1

IF NOT EXIST W6432.dat (
    PEV -rtf and { %system%\* or %systemroot%\* } -preg".*\\(con|prn|aux|null|pt[1-9]|com[1-9])\....$"
-output:temp01
    FOR /F "TOKENS=*" %%G IN ( temp01
    ) DO @CATCHME -I "\QooBox\Quarantine\catchme.log" -Z
"\QooBox\Quarantine%\systemdrive:~,1%~PG_%~NG_%~XG.zip" -e "%~G"
>N_ \%random% &&(
    ECHO.%~G>>drev.dat
)
)

ENDLOCAL

DEL /A/Q %systemdrive%\qoobox\lastrun\d-del?* %systemdrive%\qoobox\lastrun\catch_k* temp0?
N_* >N_ \%random% 2>&1
IF EXIST drev.dat TYPE drev.dat >\qoobox\lastrun\drev_.dat 2>N_ \%random%
IF EXIST drevF.dat TYPE drev.dat >\qoobox\lastrun\drev_F.dat 2>N_ \%random%

```

```

IF EXIST RenV2Move.dat (
FOR /F "TOKENS=1* DELIMS= " %%G IN ( RenV2Move.dat ) DO @IF EXIST "%%~G" (
SWXCACLS "%%~G" /OA
SWXCACLS "%%~G" /GA:F /Q
ATTRIB -H -S "%%~G"
MOVE /Y "%%~G" "%%~H"
IF NOT EXIST "%%~G" ECHO."%%~G" ---^^^> "%%~H">>RenVMoved.dat
)
DEL /A/F RenV2Move.dat
)>N_ \%random% 2>&1

IF EXIST v-files.dat FOR /F "TOKENS=*" %%G IN ( v-files.dat ) DO @IF EXIST "%%~G" DEL /A/F
"%%~G" 2>N_ \%random%
SWXCACLS %sysdir%\drivers\etc\hosts /GE:F /Q
DEL /A/F/Q %sysdir%\drivers\etc\hosts >N_ \%random% 2>&1
ECHO.127.0.0.1 localhost>%sysdir%\drivers\etc\hosts

DEL /A/F/Q %system%\perflib_perfdata_*.dat >N_ \%random% 2>&1
IF EXIST %systemroot%\erdnt\CF_undo.bat DEL /A/F %systemroot%\erdnt\CF_undo.bat
2>N_ \%random%
IF EXIST "%Systemroot%\windows.ext\" (
RD "%Systemroot%\windows.ext"
IF EXIST "%Systemroot%\windows.ext\" RD /S/Q "%Systemroot%\windows.ext"
)>N_ \%random% 2>&1

SWREG ACL "hkml\software\microsoft\windows nt\currentversion\winlogon\notify" /RS /Q
SWREG ACL "hkml\software\microsoft\windows nt\currentversion\winlogon\notify" /I ENABLE /Q

IF NOT DEFINED username exit

:END

```

TooBuck - August 1, 2026, 9:21 am

(Aug 1, 2026 09:20 AM)Tha Sneak Wrote: [\[CITE\]](#) If you want to check out more complex scripting take a look at ComboFix's source code. All you have to do is right click the exe file and extract it. It uses a combination of numerous command line tools using batch files for everything. When I first started learning batch files I loved them until I met PowerShell now me and PowerShell are best friends.

I always thought I was proficient in batch (do a lot of on-the-fly scripting at work) but seeing stuff like this is mind boggling. Thanks for the resource!

Tha Sneak - August 1, 2026, 9:33 am

(Aug 1, 2026 09:21 AM)TooBuck Wrote: [\[CITE\]](#) I always thought I was proficient in batch (do a lot of on-the-fly scripting at work) but seeing stuff like this is mind boggling. Thanks for the resource!

No problem, if you ever need any batch help let me know. :)

Anonymnuk - September 8, 2026, 7:01 pm

one word... WOW! I've done a LOT of stuff like this but never this HQ with the ascii art.... holy shit bro nice work!

Thalion - September 9, 2026, 12:25 pm

Beautiful!

You, sir, are the Leonardo da Vinci of batch scripting (or Leonardo da Batch in Italian, if we want to be funny).

:^)

CyberXero - September 9, 2026, 12:46 pm

Picasso, Picasso

Anonymuk - September 24, 2026, 9:38 am

Holy shit! That's actually impressive in the amount of detail that you were able to put out. Great job!