

Forum: [Hack Forums](#)

Thread: [Batch BYTE order mark](#)

The Phisherman - March 27, 2017, 4:33 am

Hello everyone, just thought I would share a trick that unknown to many, its called a byte order mark, and protects your code from basic text editors, for hex editors, it will do nothing

simply put this at the start of your code

Code ýþ

class save it as normal, if prompted, save in the unicode format

please don't run around telling everyone this or scan on virus total, I may need to, ahem use it

Thanks, any feedback, comment below

zask - March 27, 2017, 8:48 am

(Mar 27, 2017 04:33 AM)The Phisherman Wrote: [\[CITE\]](#) Hello everyone, just thought I would share a trick that unknown to many, its called a byte order mark, and protects your code from basic text editors, for hex editors, it will do nothing

simply put this at the start of your code

Code ýþ

class save it as normal, if prompted, save in the unicode format

please don't run around telling everyone this as I, ahem use it

Thanks, any feedback, comment below

Yup already knew it, put it in the begging of batch file and everything turns Chinese, remove cls and you'll get an error. I made a post on my profile that involved it but no one replied.

JoshuTee - March 27, 2017, 11:41 am

Thanks for sharing, but as @zask pointed out this is pretty known already, nevertheless thanks for contributing!

gogglebot - March 27, 2017, 12:56 pm

I'd never personally heard of this or seen it mentioned before for some reason, interesting share!

?CARUs L?VE?™ - March 27, 2017, 1:36 pm

This is the code for Bouncing Balls

Encoding: USC-2 LE BOM

save as .bat

Code

??????????????????????????+?4???????????????%00????????????????????????4?:????

$$+????????+????????????????????+?????????????+??????????????????\pm?$$

+????????????????????????????????\?

†????4?????????>=????????????????>=??.????????????††????,????????,????????????

†?????:??††????????+??????††††4?????? ††??????????C?..??????
††??????????C?..????????††††4????????‡????
††??????????C?..`??††††4???????? ††????????????????
††????????????????††††4????????
†????????????????????????????+??????††††4????????
††????????????†††††††SM??‡?i???? 5/8 ?????????????????? ††???? 5/8
??SM????‡4????????????????††††SM??‡?i????‡???????????????? ††????
5/8 ??SM???? 5/8 †4????????†?????†††††††SM??‡??? 5/8 SM????
††???????? 5/8 SM??‡??? 5/8 ??††† †????†††???????? ††????????????????
5/8 ? ††????????\††????????+??????4????????||????????†????†††4????
††???????????????? ††????††††4????????+????????????
††????????????††4????????††††????????????????????????????
††††† ††††????????????8????9???????????? ††††‡?i‡?SM 1/3 ?????
††††††????8????9????††††††4???????? ††††††????4? 1/8 ??? 1/8 ?????ix??+?
1/8 ?????||††††††††††††††4????9?`????4????????

gogglebot - March 27, 2017, 6:01 pm

Wow that's quite the effect, is it reversible?

?CARUs L?VE?™ - March 27, 2017, 6:24 pm

(Mar 27, 2017 06:01 PM)gogglebot Wrote: [\[CITE\]](#) Wow that's quite the effect, is it reversible?
I tried, but I didn't try hard :P

b00st3d - March 27, 2017, 6:43 pm

I like it and have never heard of this either. Don't really have a need to encode anything that I can think of but I feel like this is about as close to closed source batch as you can get. I'm bookmarking this thread since I don't know how to save that character as plain text.

SoftAP.bat: <https://pastebin.com/raw/Knr5RBYV>

gogglebot - March 27, 2017, 7:18 pm

(Mar 27, 2017 06:43 PM)b00st3d Wrote: [\[CITE\]](#) I like it and have never heard of this either. Don't really have a need to encode anything that I can think of but I feel like this is about as close to closed source batch as you can get. I'm bookmarking this thread since I don't know how to save that character as plain text.

SoftAP.bat

Code -snip

Indeed I'll be doing the same, I suppose you'd have to give a direct download to any file you want to release with this though?

Or can you copy-paste that jumbled text into notepad, save it, and it still work?

b00st3d - March 27, 2017, 8:25 pm

(Mar 27, 2017 07:18 PM)gogglebot Wrote: [\[CITE\]](#) Indeed I'll be doing the same, I suppose you'd have to give a direct download to any file you want to release with this though?
Or can you copy-paste that jumbled text into notepad, save it, and it still work?
copy paste it to notepad and save as unicode

The Phisherman - March 28, 2017, 3:54 am

Thanks everyone, I thought it was useful, but then again, hex editors do see through it

(Mar 27, 2017 01:36 PM)?CARUs L?VE?™ Wrote: [\[CITE\]](#) This is the code for Bouncing Balls

save as .bat

????+?4????%????4?:???

+????+???? +????+?

+????\?

+???4????>=????>=?•????+????>????..????

+?????:??+????+?????++4???? +????C?..????

+++????C?..????++++4????+????

+++????C?..'???++++4???? +????

+++????++++4????

+????+????+4????

+++????SM???‡i???? 5/8 ????? +++++ 5/8

??SM???‡4????++++SM???‡i????‡???? +++++

5/8 ??SM??? 5/8 †4????+????++++????SM???‡?? 5/8 SM???

+++???? 5/8 SM???‡?? 5/8 ??†? †????++++???? +++++

5/8 ? +++????\?†????+????4????||????†++++4????

+++???? +++++4????+????

+++????†4????++++????

++++? +++++8????9???? +++++‡i?‡SM 1/3 ???†?

++++†????8????9????++++†4???? +++++4? 1/8 ??? 1/8 ?????ix??+?

1/8 ?????||†++++? ++?†++++4???9?´????4????WOW, icarus that is some
high level shit, i have no idea how you did that, but it gave me epilepsy!

didnt bother looking at the source the epilepsy killed me, lol, how did u do that, looks very HQ

EDIT: just looked at sum of ur posts, woh could u show me how to do some of this stuff?

mindblown!

what even is multithreading?

Yeah it is a cool trick.

Is there a way to view normally through its own code with findstr
When the byte order mark is set?

For example findstr searches for a specific phrase within its own code, normally the Byte order mark would interfere with findstr but is there a way to get around that?

THANKS THANKS THANKSTHANKS

(Mar 29, 2017 09:31 PM)dzirione1 Wrote: [\[CITE\]](#) THANKS THANKS THANKSTHANKSNo worries bro!

EDIT: look at this users negative rep, he doesn't mean thanks, he was just spamming to get his 25 post count, shame on you

(Mar 28, 2017 03:54 AM)The Phisherman Wrote: [\[CITE\]](#) Thanks everyone, I thought it was useful, but then again, hex editors do see through it

WOW, icarus that is some high level shit, i have no idea how you did that, but it gave me epilepsy!
didnt bother looking at the source the epilepsy killed me, lol, how did u do that, looks very HQ
EDIT: just looked at sum of ur posts, woh could u show me how to do some of this stuff?
mindblown!

what even is multithreading?

I'm glad you thought so! I will be making more youtube video tutorials, and bouncing balls is one of the videos I have planned. Just keep watching I guess :) oh, and also, questions are important. Ask away

The Phisherman - March 31, 2017, 5:20 am

(Mar 31, 2017 05:10 AM)?CARUs L?VE?™ Wrote: [\[CITE\]](#) I'm glad you thought so! I will be making more youtube video tutorials, and bouncing balls is one of the videos I have planned. Just keep watching I guess :) oh, and also, questions are important. Ask away to start off with, could u explain the concept of multithreading please?

Thanks, I appreciate your time

?CARUs L?VE?™ - March 31, 2017, 5:29 am

(Mar 31, 2017 05:20 AM)The Phisherman Wrote: [\[CITE\]](#) to start off with, could u explain the concept of multithreading please?

Thanks, I appreciate your time

Multithreading can be a tricky subject, I remember it took me some time to wrap my mind around it because the way it works is sort of jarring.

Let me sort of set a visual, if I can...

THREAD 1

Code :Engine

:Engine_loop

parse information from THREAD 2

do something with this information

goto :Engine_loop

exit

THREAD 2

Code :Input

collect input with CHOICE /?

goto :Input

So the idea of multithreading, as you may be able to see from the pseudo-code, is that you can continuously run the main loop, AND collect input, without the script pausing and asking for input. We sort of just want it to pick up information we send if, if we send it any.

For example, games like my [Batch PONG v2](#)

This game is multi-threaded.

It collects input from the user, and still animates the ball flying across the screen.

Hackoo - August 10, 2017, 4:14 am

(Mar 28, 2017 01:56 PM)zask Wrote: [\[CITE\]](#) Yeah it is a cool trick.

Is there a way to view normally through its own code with findstr
When the byte order mark is set?

For example findstr searches for a specific phrase within its own code, normally the Byte order mark would interfere with findstr but is there a way to get around that? If you open it in a HEX editor you'll see how it works - it prepends an FF FE Byte Order Mark (that leads to parse the code as UTF-16 LE in a text editor) + CLS to remove the error message that cmd.exe will throw.

Yes there is a way to do it in batch file instead to use an HEX editor to get back with the original batch file by programming ?
The idea is quite simple :
The prepended line in a HEX editor is
FF FE 26 63 6C 73 0D 0A
As you can see it's 8 characters. Just let PAUSE eat them.
Just save this code as UnObfuscate.bat and drag and drop your Obfuscate batch file over it and It creates a new batch file with 3 underscores appended to the name.

```
UnObfuscate.bat
UnObfuscate.bat (Click to View)Code @echo off &setlocal
if "%~1"==" " exit /b
if /i "%~x1" neq ".bat" if /i "%~x1" neq ".cmd" exit /b
<"%~1" ((for /l %%N in (1 1 8) do pause)>nul&findstr "^">"%~n1____%~x1")
? ? ?
```

(Mar 27, 2017 06:43 PM)b00st3d Wrote: [CITE](#) I like it and have never heard of this either. Don't really have a need to encode anything that I can think of but I feel like this is about as close to closed source batch as you can get. I'm bookmarking this thread since I don't know how to save that character as plain text.

```
SoftAP.bat: https://pastebin.com/raw/Knr5RBYV
The code in plaintext of SoftAP.bat
SoftAP.bat (Click to View)Code cls
@echo off
title SoftAP
CLS
:checkPrivileges
NET FILE 1>NUL 2>NUL
if '%errorlevel%' == '0' ( goto gotPrivileges ) else ( goto getPrivileges )
:getPrivileges
if '%1'=='ELEV' (shift & goto gotPrivileges)
ECHO.
ECHO +=-----+
ECHO + This script requires admin rights in order to create access points.      +
ECHO +=-----+
setlocal DisableDelayedExpansion
set "batchPath=%~0"
setlocal EnableDelayedExpansion
ECHO Set UAC = CreateObject^("Shell.Application"^) > "%temp%\OEgetPrivileges.vbs"
ECHO UAC.ShellExecute "!batchPath!", "ELEV", "", "runas", 1 >> "%temp%\OEgetPrivileges.vbs"
"%temp%\OEgetPrivileges.vbs"
exit /B
:gotPrivileges
:run
```

```

.....
setlocal & pushd .
:start
cls
echo +-----+
call :animate
echo +                +
call :animate
echo + 1.) Create a new AP          +
call :animate
echo +                +
call :animate
echo + 2.) Stop an existing AP      +
call :animate
echo +                +
call :animate
echo + 3.) Show current AP Stats    +
call :animate
echo +-----+
call :animate
echo + 4.) HELP                    +
call :animate
echo +                +
call :animate
echo + 5.) EXIT                    +
call :animate
echo +                +
call :animate
echo +-----+
call :animate
choice /c 12345c /N /M "Please make a selection:
if %errorlevel% == 1 ( goto ap )
if %errorlevel% == 2 ( goto stopAP )
if %errorlevel% == 3 ( goto show )
if %errorlevel% == 4 ( goto help )
if %errorlevel% == 5 ( exit )
if %errorlevel% == 6 ( start & goto start )
:ap
REM Clearing any previous hostednetwork that is still on the machine
echo preparing hosted network...
netsh wlan stop hostednetwork >nul
timeout 1 >nul
netsh wlan set hostednetwork mode=disallow >nul
timeout 1 >nul
cls
echo +-----+
call :animate
echo +SSID:
call :animate
echo +-----+
call :animate
set /p ssid=Please enter an SSID:
cls

```

```

echo +=-----+
call :animate
echo +SSID: %ssid%
call :animate
echo +=-----+
call :animate
set /p key=Please enter a network key:
cls
echo +=-----+
call :animate
echo +SSID: %ssid%
call :animate
echo +
call :animate
echo +Creating your new Access point. Please wait.
call :animate
echo +=-----+
netsh wlan set hostednetwork ssid=%ssid% key=%key% keyUsage=persistent mode=allow
timeout 1 >nul
netsh wlan start hostednetwork
timeout 2 >nul
goto start
:stopAP
cls
echo +=-----+
call :animate
echo + Stopping your Accesspoint
call :animate
echo +=-----+
REM Clearing any previous hostednetwork that is still on the machine
netsh wlan stop hostednetwork >nul
netsh wlan set hostednetwork mode=disallow >nul
taskkill /im mshta.exe
goto start
:show
setlocal enabledelayedexpansion
cls
netsh wlan show hostednetwork
echo.
echo.
echo press any letter or number to return to main menu.
choice /c abcdefghijklmnopqrstuvwxyz0123456789€ /t 5 /d € >nul
if "!errorlevel!" == "37" (
goto show
) else (
endlocal
goto start
)
endlocal
goto start
:animate
ping localhost -n 1 > nul
goto :EOF

```

```

:help
cls
echo +-----+
call :animate
echo + After creating your access point it may be +
call :animate
echo + necessary to make some changes to the virtual +
call :animate
echo + WiFi Miniport Adapter that was created. +
call :animate
echo + +
call :animate
echo + To do this, after the the ap has been created, +
call :animate
echo + open your adapter settings. Find your connection to the internet. +
call :animate
echo + +
call :animate
echo + 1.) Right click select properties. +
call :animate
echo + 2.) Click the 'Sharing' tab. +
call :animate
echo + 3.) Check Allow other network users to connect through this... +
call :animate
echo + 4.) Select your new connection (It should show your SSID in it) +
call :animate
echo + 5.) Click ok +
call :animate
echo + +
call :animate
echo + When finished, press any key to continue +
call :animate
echo +-----+
pause >nul
cls
goto star

```

WOLGA - August 10, 2017, 9:50 am

(Aug 10, 2017 04:14 AM)Hackoo Wrote: [\[CITE\]](#) If you open it in a HEX editor you'll see how it works - it prepends an FF FE Byte Order Mark (that leads to parse the code as UTF-16 LE in a text editor) + CLS to remove the error message that cmd.exe will throw.

Yes there is a way to do it in batch file instead to use an HEX editor to get back with the original batch file by programming ?

The idea is quite simple :

The prepended line in a HEX editor is

FF FE 26 63 6C 73 0D 0A

As you can see it's 8 characters. Just let PAUSE eat them.

Just save this code as UnObfuscate.bat and drag and drop your Obfuscate batch file over it and It creates a new batch file with 3 underscores appended to the name.

UnObfuscate.bat

UnObfuscate.bat [\(Click to View\)](#)Code @echo off &setlocal

```
if "%~1"==" " exit /b
if /i "%~x1" neq ".bat" if /i "%~x1" neq ".cmd" exit /b
<"%~1" ((for /l %%N in (1 1 8) do pause)>nul&findstr "^">"%~n1____%~x1")
? ? ?
Nice explanation about how it works! How does
Code <"%~1" ((for /l %%N in (1 1 8) do pause)>nul&findstr "^">"%~n1____%~x1")work?
```

Hackoo - August 10, 2017, 10:33 am

WOLGA Wrote: [\[CITE\]](#) Code <"%~1" ((for /l %%N in (1 1 8) do pause)>nul&findstr
"^">"%~n1____%~x1")work?I think this code doesn't work on your side ! i'm right ?

WOLGA - August 10, 2017, 10:36 am

(Aug 10, 2017 10:33 AM)Hackoo Wrote: [\[CITE\]](#) I think this code doesn't work on your side ! i'm right ?

Your code works fine. I want to know how it works.

Hackoo - August 10, 2017, 11:28 am

(Aug 10, 2017 10:36 AM)WOLGA Wrote: [\[CITE\]](#) Your code works fine. I want to know how it works.
Code for /l %%N in (1 1 8) do pauseThe prepended line in a HEX editor is FF FE 26 63 6C 73 0D 0A

As you can see it's 8 characters. Just let PAUSE eat them with this loop. like to skip them !

I have another method is to skip the first line and read all lines after this skipping.

And here is the source code with comments :

UnObfuscate.bat

UnObfuscate.bat ([Click to View](#))Code @echo off

Title UnObfuscate the Byte Order Mark trick to show code in plaintext by Hackoo

Color 0A

Rem if the we execute by double clic or if there is no file to drag and drop

:: We go to the error to exit this batch script

if "%~1"==" " goto error

Rem we should drag and drop just *.bat or *.cmd files

if /i "%~x1" neq ".bat" if /i "%~x1" neq ".cmd" goto error

Rem We delete any previous old generated file

if exist "%~n1____%~x1" del "%~n1____%~x1"

Rem in this loop we skip the first line and we edit

:: our file with unicode with this comand CMD /U /C Type

for /f "skip=1 delims=" %%L in ('CMD /U /C Type "%~1") do (

echo %%L

echo %%L >>"%~n1____%~x1"

)

pause>nul & Exit

..*****

..

:Error

Mode con cols=80 lines=3

cls & color 0C

echo(

echo You must drag and drop your ".bat" or your ".cmd" over this batch script

Timeout /T 5 /NoBreak>nul & exit /b

..*****

..