

Forum:[Hack Forums](#)

Thread: [Polymorphic Example](#)

WOLGA - December 28, 2015, 4:00 pm

Edit: Apparently HackForums breaks the script with its encoding, so I have uploaded the script to here: <http://pastebin.com/raw/yHqUT2fT>

How to use:

1. Save as .bat
2. Run it
3. Notice that the source code varies after every run, while the output remains the same.

Ventriloquism - December 28, 2015, 4:20 pm

Very nice, I've seen a few of these in the past. Definitely something worth experimenting with more.

Gratz on Ub3r btw ? Looks good.

Nakamoto - December 28, 2015, 5:02 pm

Now this is the kind of stuff that this section should be filled with.

WOLGA - December 28, 2015, 5:52 pm

(Dec 28, 2015 05:20 PM)Circuits Wrote: [\[CITE\]](#) Very nice, I've seen a few of these in the past. Definitely something worth experimenting with more.

Gratz on Ub3r btw ? Looks good.

Truly? Can you compare my code to those other ones you've saw?

Ventriloquism - December 28, 2015, 6:19 pm

(Dec 28, 2015 06:52 PM)Qwertyuiopasdfghjklzxc Wrote: [\[CITE\]](#) Truly? Can you compare my code to those other ones you've saw?

Well, I found one source to reference, but it wasn't the one(s) I was looking for...oh well ?

Until I can give you a proper answer, I'll say this. The ones I've seen before in the past are okay, but they aren't anywhere as advanced as your is. Hands down. Where their algorithm is fairly simple, yours is advanced. I recall a lot of the ones I've seen utilize @ symbols at the beginning of every line, which is generated from its engine. Idk...I'll respond soon with proper sources so you can take a look at what I'm judging this by. I would like to add though, that this is probably the best on the BSDaCLI so far. Or at least the ones I've seen. You should expand on this more. Very cool ?

annikk.exe - December 29, 2015, 6:14 am

Hope you remembered to keep backups while you were working on it. :> It's annoying if the code deletes itself!

Looks very HQ. I was having a bad day and then I saw this thread, and now ::purr::

Nakamoto - December 29, 2015, 8:31 am

(Dec 28, 2015 07:19 PM)Circuits Wrote: [\[CITE\]](#) Well, I found one source to reference, but it wasn't the one(s) I was looking for...oh well ?

Until I can give you a proper answer, I'll say this. The ones I've seen before in the past are okay, but they aren't anywhere as advanced as your is. Hands down. Where their algorithm is fairly simple, yours is advanced. I recall a lot of the ones I've seen utilize @ symbols at the beginning of every line, which is generated from its engine. Idk...I'll respond soon with proper sources so you can take a look at what I'm judging this by. I would like to add though, that this is probably the best on the BSDaCLI so far. Or at least the ones I've seen. You should expand on this more. Very cool ?

Actually the method used in this script is quite simple, but at the same time unique. This isn't something you see everyday. I personally have only seen TWO polymorphic batch scripts, this being one of them. I have however seen many claiming to be polymorphic but failed to make the cut, because adding ":" or "REM" to the start of a few lines and removing it from others isn't polymorphism.

Cynoq - December 29, 2015, 2:09 pm

Could someone explain what this batch file really does? I'm interested.

WOLGA - December 29, 2015, 4:34 pm

(Dec 29, 2015 07:14 AM)annikk.exe Wrote: [\[CITE\]](#) Hope you remembered to keep backups while you were working on it. :-> It's annoying if the code deletes itself!

Looks very HQ. I was having a bad day and then I saw this thread, and now ::purr::
I did in fact keep backups, but I added the overwrite method last, so it was pretty safe.

(Dec 29, 2015 03:09 PM)Cynoq Wrote: [\[CITE\]](#) Could someone explain what this batch file really does? I'm interested.

This batch file changes itself while making sure the new version does the same thing using [polymorphism](#).

jahwi - January 6, 2016, 5:44 am

Very nice. This script is a middle finger to those who diss batch.

WOLGA - January 9, 2016, 12:46 pm

I have just received notice that HackForums encoding fucked up my script. Therefore, I have uploaded the working script to pastebin, and updated the OP as well.

Here is the working version: <http://pastebin.com/raw/yHqUT2fT>

unrealirc - January 12, 2016, 5:05 am

Guys may i ask what it is doing i see only changing the key value.

May it be possible to apply that polymorphism to another code after it execute?

i.e.

original code running when finish > polymorph new code replaced

WOLGA - January 14, 2016, 5:50 pm

(Jan 12, 2016 06:05 AM)unrealirc Wrote: [\[CITE\]](#) Guys may i ask what it is doing i see only changing the key value.

May it be possible to apply that polymorphism to another code after it execute?

i.e.

original code running when finish > polymorph
new code replaced

You should also notice that the variable 'epayloadl1' is changing after every execution. That is the cool part.

It is possible but non-trivial to use this polymorphism with larger and more complex scripts.