

Forum:[Hack Forums](#)

Thread: [\[FUD\] Simple Method To Bypass AV \[PowerShell\]](#)

NYANxCAT - September 29, 2019, 2:10 am

- We will create a Powershell loader using VBS. I tried to make it as simple as I can. Have fun!

[1] Convert your .NET payload to base64

[2] Reverse your base64 string - [URL](#)

[3] FUD - [Scan Result](#)

[!] Copy + Paste = NO FUD

Wikeos123 - September 29, 2019, 2:14 am

I love you NYAN <3 you are the best

tiny cracker - September 29, 2019, 2:15 am

great sharing . NAYA CAT is legend and has good contribution for learning on HF and GitHub. love you dude..

Swado2times - September 29, 2019, 3:07 am

Loading malware which is detected runtime will be bypassed by a Loader? Wow you have defeated every AV in a single blow!

?Onyx? - September 29, 2019, 10:41 am

Awesome man :) commenting here to save this post. Love your contributions :)

naxster - September 30, 2019, 5:32 am

Maybe i'm doing something wrong, but when i saved this as a VBS file i only get errors... :/

The base64 is reversed and everything, still nothing... I get a popup called "Windows Script Host"

naxster - October 2, 2019, 7:40 pm

(Sep 29, 2019 02:10 AM)??` NYAN CAT ?? Wrote: [\[CITE\]](#)

- We will create a Powershell loader using VBS. I tried to make it as simple as I can. Have fun!

[1] Convert your .NET payload to base64

[2] Reverse your base64 string - [Online URL](#)

[3] FUD - [Scan Result](#)

[!] Copy + Paste = NO FUD

Please any help? :(

learner319 - October 3, 2019, 9:11 am

you are the great .Love you brother <3

and77 - October 4, 2019, 4:04 am

Thank you, good luck in the future

twito - October 4, 2019, 8:40 am

How to make cmd completely hidden way , it shows cmd for about 3 seconds

bexpr9 - October 8, 2019, 2:07 am

thank you.

I'll enjoy with this.

You are a good person who gives convenience to many peoples.

Dorothy Gonzales - October 8, 2019, 4:02 pm

not very effective actually because it wont get past AMSI. also using base64 not very stealth at all...stands out like a pineapple because why would anything legit be doing something like this?

if you want to truly be FUD then make it look legit not stand out like something that is obviously shady

One - October 11, 2019, 2:52 pm

Lol when it comes to powershell and base64 all you need is to make the file scantime fud,I will keep saying this till someone gets it

Tyr - January 17, 2020, 12:09 am

(Oct 11, 2019 02:52 PM)One Wrote: [\[CITE\]](#) Lol when it comes to powershell and base64 all you need is to make the file scantime fud,I will keep saying this till someone gets it

THANK YOU. I was reading the replies and laughing, lol.

@OP. Good thread and you put some nice work into it. Highly appreciated.

(Oct 4, 2019 08:40 AM)twito Wrote: [\[CITE\]](#) How to make cmd completely hidden way , it shows cmd for about 3 seconds

What OS are you testing this on, or are you Sandboxie-ing it? This is normal with certain stubs but can be fixed. 3 seconds is a little long though...

4chan.org/bl - January 17, 2020, 2:23 am

its just going to get detected upon runtime lol.

Grüner Baum - January 18, 2020, 2:34 pm

Nyan Cat you really helped me a lot, thank you SO MUCH <3 <3

SIM-4473964 - January 20, 2020, 1:54 am

thanks for the inspiring code ;D

Stanley - February 6, 2020, 2:42 am

I'm Stanley HF's helper bot. This OP (original poster) of this thread wants everyone to see this page and has elected to bump it to the top of the showthread listing. Since HF doesn't want a ton of LQP (Low Quality Posts) this is the best method of bumping your content. There is a small ?yte fee for each bump. Any OP can bump any of their threads on HF from the linked icon on the top of their first post.

If you haven't already read the first post of this thread we encourage you to do so.

Thanks,
Stanley

CasePaste - February 6, 2020, 2:48 am

Cant message you buddy it urgent

SeVC0n - February 15, 2020, 6:17 pm

Sweet! That was really easy. Thanks!

Selling Amazon UK GC - April 4, 2021, 2:47 am

Does anyone know how to do this still? please let me know.

speedyboy17 - April 16, 2021, 8:12 am

Sadly the video is offline :(

ninja137 - April 16, 2021, 10:43 am

Would be interesting to try to add more techniques like this.

Good one