

Forum:[Hack Forums](#)

Thread: [zw0scura | Dropper | Stub size 4Kb | API Encryption | native C++ Stub | Free](#)

zw0scura - March 2, 2015, 10:46 am

I have started a little Project for my self just a simple Dropper, only for Download and Execute a File. The Stub is coded in C++ and some inline ASM, i also include an API Encryption (CallApiByName), the API strings are encrypted with a simple XOR, also i have a Section encryption included there also use XOR for encrypt and decrypt the code. In the Stub are 2 main Sections .Stub and .Code, in the .Stub is the decrypt routine, this decrypt the .Code Section with an XOR Key from the resources at runtime. In the .Code Section is the Download Thread this loads the settings like URL, Filename, CmdArgs from the resources and download the File from the URL with InternetReadFile and saves it to the User temp Folder and run it after with ShellExecute. The Stub dont need the a Visual C++ Runtime Lib its coded in native C++ and the size its only 4,5Kb with the settings !!!

The Builder was created with C# and only encrypt the .Code Section of the Stub and add the settings to the resources of the Stub.

Screenshot of the Builder:

Yes, I know that the Dropper dont have many functions, for now its just a little Project, when some people like it i would add some function here a list of the possible functions

RunPE

Multi File Download

Binder

PE Injector (to Inject the Dropper in a other PE File)

Other Encryption

Save the Config in a Section instead resources

Icon Changer

Assembly Changer

This is just a list of function that I can add in the future when someone like it. When someone have

an idea to a function that i should add please Post below or PM me.

I dont have tested this many, so when someone have a problem please pm me.

Builder Scan Result:

Spoiler ([Click to View](#))

[[IMG](http://www.refud.me/results/415561b240392aa562c442faec42f03c.png)]<http://www.refud.me/results/415561b240392aa562c442faec42f03c.png>[[IMG](#)]

For the Download link please [PM](#) me!

2iceofficial - *May 23, 2016, 3:29 am*

Please a download will do alot of help thanks!

gravitex - *September 3, 2016, 2:36 am*

hm, this seems like is has alot of potential!

good luck :)

bloodh00t1 - *October 17, 2016, 12:19 pm*

look great mate goinn the right way

arne543 - *November 9, 2016, 12:26 pm*

could i get the link pls :)

LanMan - *November 10, 2016, 2:07 am*

Funny i just finished almost the same project as you. ASM payload into a C host, hidden winapi call and hooking Sleep to call the decrypted payload. ?

Currently 763bytes for the full exe with url, and 0/56 ?

Trying to reduce it even more without corrupting the PE format

Edit: Oops should have looked at the dates before posting.