

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] View Binary Data of Simple Programs - Get Free Stuff \[Tutorial\]](#)

Example - February 13, 2012, 5:09 pm

I didn't see a thread in this section regarding the viewing of binary data of simple programs that try to take your information. This includes keyloggers, SMTP mailers, and others.

I am not responsible if you use this for bad boy things.

This tutorial will simply explain how you can easily just right-click a simple logging/stealing program - and potentially obtain the creator's identity and stealer/logger info.

NOTE: This is for the most simplest of programs that are not crypted.

NOTE2: Always be safe when downloading infected programs. Run in a virtual environment for maximum safety.

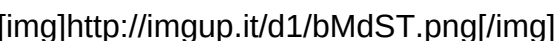
NOTE3: You will also need some type of program to view the construct of programs. Like HEX Workshop or something.

STEP 1:

Find a nice fake program. I hypothetically personally prefer the "Free Microsoft Point Generator" programs.

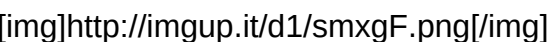
You can find a huge amount of fake software on Youtube.

Most of the time, the video will have the download to the program in the video description.

Spoiler [\(Click to View\)](#)http://imgup.it/d1/bMdST.png[/img]

STEP 2:

Download the program.

Spoiler [\(Click to View\)](#)http://imgup.it/d1/smxgF.png[/img]

STEP 3:

Open up said fake program with your binary data viewer/hex editor.

STEP 4:

Scroll through data until you find something juicy. Good data will be in the middle or bottom-sometimes.

Here we find that the original creator of this was on a user account named, "Jamie."

Spoiler [\(Click to View\)](#)http://imgup.it/d1/hg9vC.png[/img]

You can also find the telltale signs of the compiler they used and such.

Oh look! That info that I typed in is being sent to his email! Oh look! There's his email and password!

Spoiler ([Click to View](#))

Furious` - February 13, 2012, 7:10 pm

About "Jamie" that you found, this only happens when you compile your application as Debug. Most of the people don't know that, it's called debug directory. If you compiled your application as Release this Directory won't exist.

Sanst - February 13, 2012, 7:14 pm

Going to get into this stuff, I guess this helped but it wasn't very descriptive lol,

Thanks though.

Edit: Found a gmail with this, but either he changed his pass or somebody else got to it first :(

subzer00 - February 15, 2012, 12:44 pm

Although the pictures didn't work for me (Not sure why).

This feels like a whaling tutorial when you use bintext (I think that's the program) to look at the program.

@sanst You gotta look for videos that were recently created, last week or so and you can most likely get to it.

theisnophie - February 16, 2012, 9:27 pm

Interesting tutorial. I heard about this reengineering viruses sort of but did not know it was this simple sounding at least.

Infinity. - February 17, 2012, 12:29 am

All seemed so shitty while opening some program in hex workshop but never thought of getting this kind of info

Thanks mate!

domondon1 - February 19, 2012, 12:48 am

Wow!!! i try this men later..hahaha..thank you

Orphan Crippler - August 13, 2015, 10:29 am

man this tut helped a lot thank you!!

sneezing panda - August 14, 2015, 2:44 pm

Holy shit.. a 3 1/2 year gravedig.. why would you do this....

