

## Forum:[Hack Forums](#)

Thread: [Python Virus Idea: Dynamic Source Virus](#)

**dberube** - August 21, 2012, 6:06 pm

Python is interpreted. Some may think it is a disadvantage because the source can hardly be hidden and the executable size is considerable. Let me prove you that python can be as powerful as C when you want to create a virus.

Idea : Dynamic Source Virus

Every virus have a static byte compiled source, it can't be modified and it is always present in the executable...

Representation:

Spoiler ([Click to View](#))

But what if we could create a virus with no dependencies and no source included with it?

Here's the idea: we split the virus in multiple parts:

- 1: The "Container", an empty encrypted exe containing an Interpreter and the required module to access the internet. This is what you distribute.
- 2: The "Core", the actual source of the virus, it would be a encrypted text file on a domain. It also contain information about which extra's the container need to download.
- 3: The "extra's", the libraries required to make the virus work , they are encrypted files on a domain.

This is how it would work. On startup, the container open the web page containing the core (hidden of course and over ssl,tls), it decrypt it , install the extra's and interpret the code. For security, everything would be stored in the program memory (or saved in ADS). While this would not protect from detection on execution, it would present many advantages:

Dynamic virus, the user could change the source code at any time without accessing the infected computer

-Intelligent virus, the virus could itself modify his source... evolving

-No detection from av scanning website since no malicious code is inside.

-Reverse engineering more difficult

Representation:

Spoiler ([Click to View](#))

Discuss,share you thought.

**-Max** - August 21, 2012, 7:44 pm

This sounds like a big project, but for what? Who are you targeting? This would be brilliant if it had a purpose. I know I am one to talk, but it is true.

**husky141** - August 21, 2012, 8:06 pm

sounds neat, I might look into something like this ?

**dberube** - August 22, 2012, 4:59 am

(Aug 21, 2012 07:44 PM)Max00355 Wrote: [\[CITE\]](#) This sounds like a big project, but for what? Who are you targeting? This would be brilliant if it had a purpose. I know I am one to talk, but it is true. No one in particular, I was just reading an article about something kinda similar. I used a virus as an example but this could be as useful for a python programmer that do not want to share his source.

For now python is already capable of executing a source code from memory and, about reading a sources from the internet, urllib2(python2) and urllib.request(python3) are already simplifying the process (for security I would strip the needed code from these modules and append it to the container).

Btw:I am currently modifying (rewriting for scratch) my library "txtuplib2" to be able to read text from text-upload because I can't have access to a domain... ???

Edit: I am also writing a script that can parse Html document from memory.

**tweety** - August 22, 2012, 5:44 am

You run into a lot of problems. First, Firewall. Second, if the slave does not have internet connection then the virus won't be able to execute on start up to collect information. Third, if the virus get's found it can be traced back to your domain.

**dberube** - August 22, 2012, 6:01 am

1: The firewall is the main problem...

2: The container will be able to check if the slave have an internet connection. If not, it will loop until a connection is found or exit.

3: Since the virus is a text file, you can upload it to a random text uploading website.

Example (source + release):

This program use this source: <http://www.text-upload.com/read,t11757>

And update it when executed to show how many time it was executed.

minus : <http://minus.com/lbhvRqCdkAAIQC>

Of course, this is far from being a virus.

**Ch1m4zz** - January 27, 2013, 4:40 am

Tweety is right :)

The Firewall will kill it

**framk** - January 27, 2013, 6:50 am

Have you considered the fact that python can be compiled? If you're worried about the source being visible to the victim, simply compile to obfuscate what malicious code is contained within the program. I don't know if auto-updating the program would work, but I understand what you're driving at. Best of luck, brother!

**dberube** - January 27, 2013, 9:01 am

Of course I know. :D

I've analyzed the structure of pyc files for my disassembler and I can say that the protection that the compiled python script offer is so small that it shoudn't considered. Also, by the time I started this thread I found other very usefull techniqe to hide my source (using a .pyd for example (python dll)).

