

Forum:[Hack Forums](#)

Thread: [Concepts/ideas for what a virus should do?](#)

Infamia - January 6, 2017, 5:05 pm

FTP MODULE

MAIN MODULE

My apologies if it isn't the most readable thing; it's not meant to be, it's a virus after-all, I don't really know what to add on. It connects to an FTP server and uploads every file on the Desktop by ZIPing it into one and sending it off; think of it now I think I should just do it via iterations rather- so if the user cancels it, I'll still get some files.

Anyone mind adding some ideas or something? It uses a ROT13 type of cipher but it increments the letter by 1 or minus 1, to encrypt/decrypt you call lambda functions dec/enc.

This is all hard-coded, so it's kind of hard to change.

ideas ideas pls

Goodies - January 6, 2017, 7:16 pm

Do not write malware in Python.

The server can be, though. There are some great frameworks that let you design your own protocol. Highly recommend twisted or asyncio.

Infamia - January 7, 2017, 6:38 am

(Jan 6, 2017 08:16 PM)Goodies Wrote: [\[CITE\]](#) Do not write malware in Python.

The server can be, though. There are some great frameworks that let you design your own protocol. Highly recommend twisted or asyncio.

Oh, I kind of tried to design a virus regardless in Python; and then to mask it up- of course as you can see- I used a simple hard-coded cipher which is solved and then executed.

I understand it's interpreted and open-source, but I enjoy it's syntax and general fluidity.

Also what'd'ya mean by server? The FTP server? I don't really get how it could do much.

Goodies - January 7, 2017, 1:08 pm

No. By "server" I'm referring to the C&C server that the malware connects to. Malware should not be written in such a high level language. It should be very low level. Dropper written in C/C++ or ASM. Something I'm working on is 100% ASM and is entirely positionally independent meaning it can migrate from process to process.

Infamia - January 7, 2017, 5:31 pm

(Jan 7, 2017 02:08 PM)Goodies Wrote: [\[CITE\]](#) No. By "server" I'm referring to the C&C server that the malware connects to. Malware should not be written in such a high level language. It should be very low level. Dropper written in C/C++ or ASM. Something I'm working on is 100% ASM and is entirely positionally independent meaning it can migrate from process to process.

Ooh, OK. I get you, I think I'll recode the virus to interface with a C/D server somehow, perhaps let Python run a cgi-bin server secretly and let me upload C/D scripts which can be executed on the

machine.

Of course this solely relies on if the person has GCV/MinGW, else I can just provide a nasm.exe and rename it; then execute Assembly scripts.

Tbh I could do anything.

Goodies - January 7, 2017, 6:56 pm

(Jan 7, 2017 06:31 PM)Infamia Wrote: [\[CITE\]](#) Ooh, OK. I get you, I think I'll recode the virus to interface with a C/D server somehow, perhaps let Python run a cgi-bin server secretly and let me upload C/D scripts which can be executed on the machine.

Of course this solely relies on if the person has GCV/MinGW, else I can just provide a nasm.exe and rename it; then execute Assembly scripts.

Tbh I could do anything.

Depending on exactly what you're attacking, good malware is generally very portable to different kinds of architectures and operating system versions. I'm currently working on something that is a pure ASM stager that will download and map into memory various DLLs based on the process/system architecture.

Python is both the web server that gives the file to be downloaded and the C&C server that gives commands, but the DLLs are in C++ and the stager is in ASM.

Infamia - January 7, 2017, 7:16 pm

(Jan 7, 2017 07:56 PM)Goodies Wrote: [\[CITE\]](#) Depending on exactly what you're attacking, good malware is generally very portable to different kinds of architectures and operating system versions. I'm currently working on something that is a pure ASM stager that will download and map into memory various DLLs based on the process/system architecture.

Python is both the web server that gives the file to be downloaded and the C&C server that gives commands, but the DLLs are in C++ and the stager is in ASM.

I think I'll stick with Windows purely because I know its file structure better and what to do around the system. I think my main languages would be C, ASM, Python. A mix of super-high, low-ish and pure low.

My idea is to just access other program's memory and completely fuck it up by writing 'DICK' everywhere slowly. Also take PNGs and corrupt them, and if I can change the Windows startup logo to a big cock or something.

Then alas' I'll try to overwrite the MBR and remove winsock.DLL and then peace out.