

Forum:[Hack Forums](#)

Thread: [Is Build Your Own Botnet good for beginners?](#)

Ink_Glade - August 6, 2023, 7:29 am

Ages ago I stumbled upon BYOB and it seemed cool but I didn't know tech back then, now that I'm getting into cybersecurity etc. I'm wondering if It's good for beginners learning botnets or if some other alternative is better. I'd rather it be free.

osn64698 - August 6, 2023, 8:39 am

"Counter-Measure Against Antivirus: avoids being analyzed by antivirus by blocking processes with names of known antivirus products from spawning" -

Shit will never work, handle rights are stripped within kernel callbacks, unless you remove them (Via actual driver exploitation) you won't be able to open an av process, let alone prevent it from spawning lmao.

"Encrypt Payloads To Prevent Analysis: the main client payload is encrypted with a random 256-bit key which exists solely in the payload stager which is generated along with it" -

No shit. This was good in 2008, nowadays there is emulation

There is actually no reason to write malware in Python unless you are completely degenerate. If you want to be good at what you do, learn the proper language.

If 5 years ago people would have told you to learn "C/ASM", today I think the best languages are probably "C++/ASM".

C is ugly, and there are multiple reasons why most modern anti-viruses are written in a language like C++ and not C. (Unless you have to use C, like in driver development)

Ink_Glade - August 6, 2023, 2:00 pm

(Aug 6, 2023 08:39 AM)osn64698 Wrote: [\[CITE\]](#) "Counter-Measure Against Antivirus: avoids being analyzed by antivirus by blocking processes with names of known antivirus products from spawning" -

Shit will never work, handle rights are stripped within kernel callbacks, unless you remove them (Via actual driver exploitation) you won't be able to open an av process, let alone prevent it from spawning lmao.

"Encrypt Payloads To Prevent Analysis: the main client payload is encrypted with a random 256-bit key which exists solely in the payload stager which is generated along with it" -

No shit. This was good in 2008, nowadays there is emulation

There is actually no reason to write malware in Python unless you are completely degenerate. If you want to be good at what you do, learn the proper language.

If 5 years ago people would have told you to learn "C/ASM", today I think the best languages are probably "C++/ASM".

C is ugly, and there are multiple reasons why most modern anti-viruses are written in a language

like C++ and not C. (Unless you have to use C, like in driver development)
Alright thanks!