

Forum: [Hack Forums](#)

Thread: [How do most IRC bots work \(specifically perl bots\)?](#)

Decompress - March 5, 2015, 3:45 pm

I guess I'll post this here because it seems like everyone in the botnet section are skids and don't actually know how these things work.

"I'm curious how most IRC bots work, specifically these "perl bots" everyone is talking about. In all honestly, I'm way too lazy to look through the source code and would like someone to simply break it down for me.

From what I understand, this is how they work:

- An exploit is used to breach the machine in question and malware is installed.
- Said malware connects to the C&C server and joins a preset channel, usually setting its nickname to contain information about the compromised machine such as it's operating system.
- Once in a channel, the malware listens for commands. If it recognizes a command, it checks if the user who initiated the command has sufficient privileges e.g. if they're an administrator and if they are then perform the task that corresponds with the command.

Is that it? Or is there other stuff to it as well?

Anything I missed out on or should know about?

Additionally, what are the pros and cons of using desktop computers as bots vs using rooted servers? Thanks for your help.

EDIT: Also, what's all the fuss about bots written in perl? What makes perl better than C?"

(Re: <https://hackforums.net/showthread.php?tid=4716943>)

Mouse? - March 6, 2015, 10:57 am

That's the jist of it. There's not much else to it besides the commands themselves, methods of hiding itself from the user of the infected device, and other internals. Pros and cons of using desktop computers vs servers? Well, that 'skid' (I assume that's who you're talking about) isn't wrong. If you're DoSing from a server, it's probably doing a better job than some home connection lol. Not to mention their hardware is more powerful (the only thing I cared about regarding using botnets was cryptocurrency mining.)

And as for the Perl thing, beats me. I'm not an experienced Perl user but I do know that Perl is more popular for networking. Using Perl for a little while, I can say that the syntax and modules favour networking in a beautiful way, so it might just be a popularity thing. I refuse to say that Perl is "better" than C

Decompress - March 7, 2015, 5:42 pm

(Mar 6, 2015 11:57 AM)Rodaxoleaux Wrote: [\[CITE\]](#) That's the jist of it. There's not much else to it besides the commands themselves, methods of hiding itself from the user of the infected device, and other internals. Pros and cons of using desktop computers vs servers? Well, that 'skid' (I assume that's who you're talking about) isn't wrong. If you're DoSing from a server, it's probably doing a better job than some home connection lol. Not to mention their hardware is more powerful (the only thing I cared about regarding using botnets was cryptocurrency mining.)

And as for the Perl thing, beats me. I'm not an experienced Perl user but I do know that Perl is more popular for networking. Using Perl for a little while, I can say that the syntax and modules favour networking in a beautiful way, so it might just be a popularity thing. I refuse to say that Perl is "better" than C

Thanks for your reply. I'm still confused as to why perl bots are favored over C/C++ bots as well. Someone said it's because embedded devices such as routers, switches, IP cameras, etc. usually don't come with a perl interpreter installed, so using perl bots kind of weed out shitty embedded devices from joining your botnet.

Brasil - *March 19, 2015, 8:13 pm*

Writing a perl bot takes less time than with C/C++. With CPAN someone has already made everything, you just need to import the code, put some of it in the correct order and MAGIC you have a bot. With C/C++ you need to reinvent the wheel, axel, bearing, and everything else. Just my \$0.02.