

Forum:[Hack Forums](#)

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

Decompress - March 5, 2015, 1:49 pm

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?

PolarBeats - March 5, 2015, 7:53 pm

well some bots use proxies or tor to connect to the C&C to help hide the servers location, also rooted servers usually run on linux and servers usually have a decent bandwidth speeds so they have stronger ddos, however it is easier to get lots of desktop computers then it is to get rooted servers (usually).