

Forum:[Hack Forums](#)

Thread: [Botnet self ddos during two-way communication mitigation theory](#)

blacksmith - May 28, 2020, 10:56 am

To start it off, I'll give you a brief introduction to my WIP attack method: Dynamic attack (yes, I know, I couldn't be bothered to choose a name). The attack collects data from all bots during an attack (mainly failure rates) and makes decisions based on the collected data.

You can use machine learning or the standard DDoS protection approach (reversed). This might not work for CF, but for (nearly?) every other ordinary DDoS protection: Determine the soft-, adjusted-, and hard threshold. Based on said thresholds, you can decide how much power you need and various other unknown variables, such as delay and duration. However, you realize that your botnet is so fucking big that you exceed your C&C server's 10Gbps connection, even though your bots only send an 8-bit-integer over the line. Yeah, that happened, now what? Here's where my untested, took-me-a-few-minutes-to-figure-out theory to mitigate a DDoS attack from your own botnet to your botnet's C&C server (oh the irony) into play.

Just hear me out:
Archiver = Bot

Got it? Well, all you need to do is to look at the picture below:

That's a TON of magic. jk. I don't know what to say at this point as the image explains everything. You can make a few design decision that will (heavily) impact your botnet:
How many nodes do you want to expose?

Do you want to encrypt the relayed data?

Do you want to use compression?

"Woah.. hold on there! How tf is this supposed to impact my botnet?", you may ask. I prepared a few answers for you.

How many nodes do you want to expose? P2P botnet fate, might an okay tradeoff though.

Do you want to encrypt the relayed data? OK, fine, we could sign the data. I didn't figure out another option yet.

Do you want to use compression? No encryption possible (or rather no a notable difference, correct me on that one if I'm wrong here).

4Txe4y33C9zvNhMj - May 29, 2020, 9:36 am

You could compress data first and encrypt later. That would still save bandwidth.

blacksmith - May 29, 2020, 11:42 am

(May 29, 2020 09:36 AM)4Txe4y33C9zvNhMj Wrote: [\[CITE\]](#) You could compress data first and encrypt later. That would still save bandwidth.

Good point. ?

Eye4Eye - May 29, 2020, 1:46 pm

Can you please explain what's a WIP attack?

blacksmith - May 29, 2020, 4:43 pm

(May 29, 2020 01:46 PM)Eye4Eye Wrote: [\[CITE\]](#) Can you please explain what's a WIP attack?

WIP means work in progress.