10 Rules:
Zombie Survival Guide

'Zombies' are computers or Internet devices that are under hacker control. Hackers collect vast armies of zombies which they use to launch DDoS attacks.

Remeber the movie **Zombieland**? Here are FlowTraq's rules for being optimally prepared for the ongoing zombie botnet apocalypse. Enjoy!

1. Cardio

When your cyber apocalypse comes, it is best to be in great physical shape. Deploy these defenses today, before you catch your first zombie:

1) ***Visibility everywhere*** Unsampled flow, so you see everything.
2) ***Egress filtering*** Source not in your netblock? Drop it!!

2. Always Double Tap

Prevent re-infection.
The hacker got in once, do you understand how?
Understand the attack vector, and close it off.
That is how you take a zombie down, and keep it down.

3. Beware of Bathrooms

The forgotten machine is as *vulnerable as you'd be to a zombie attack in the bathroom.* Do this religiously:

Educate. Your co-workers
Update. Your operating systems and software
Separate. Your systems and resources

4. "Buckle Up"

Buckle up for safety. Or, in this case "back up" frequently.
When half your network is under hacker control:
Re-image hacked systems, restore data from backup, and get your organization operational again as soon as possible.

5. Travel Light

More stuff on your network, means bigger zombie breeding ground. Follow these two rules:

1) Shut down old hosts ***2) Remove stale permissions***

6. Don't Be A Hero

Don't be a last minute hero working through the night.
Do your legwork, and stay prepared:

1) Hunt for zombies daily.
2) Patch often.
3) Backup frequently.

7. Limber Up

Reserve capacity is king when the zombies start their DDoS attack. It keeps your shop operational while taking down zombies one by one:

1) Bandwidth ***2) Routers*** ***3) CPU***

8. Know Your Way Out

When the going gets tough, make sure you have a tested plan to evade:

1) ***Alternate Internet paths*** 2) ***Offsite data storage***
3) ***Well documented playbooks that can be followed by staff***

9. The Buddy System

Network defense is a human game:
Have buddies who can help (cyber) hunt for zombies.
They may just pick up on patterns that you previously missed!

10. Check Your Back Seat

Once you catch a zombie on your network, stay cool, study it carefully.
Understand their back-channel, and search your network for others.
Only then take them down. All at once.

11. Enjoy The Little Things

Wait, what? *It says "10 Rules", but we'll give you an extra at no charge!* With the constant grind of staying alive in Zombieland, its import to take a moment and smell the roses.
The work is never done because there is always a sequel.
Zombies are always adapting - *Be Prepared*!

Stay Frosty!

FlowTraq