From: dave aitel
To: counter_botnet_RFC
Subject: Botnets
Date: Wednesday, June 14, 2017 10:35:30 AM

There are two real possibilities for combating botnets on the Internet. One is to play core-wars, which requires legal setups that allow us to launch beneficial worms which patch vulnerabilities. I can see most policy-types shaking their heads at how difficult this would be to do, but it is a technically workable option. It's also workable in policy with some effort.

The other method is to build a resilient internet - by which we do not mean an internet free of vulnerabilities, but one free of centralized choke points that can be targeted by massive traffic attacks.

DNS is the primary pain-point, but also one the government likes having around because it allows for centralized governmental control. Imagine if everyone was on a decentralized domain system, and the FBI could not "seize" domains. This is the price you pay for resilience. To be fair, I don't think we (as the US Government) really want it. But that IS the real solution. :)

What straight up is not going to work is instituting liabilities for having vulnerable systems or selling vulnerable systems, trying to enforce a global filtering system across the internet, requiring that systems get patched (which is largely irrelevant aside from being technically impossible), or somehow trying to block information about how to build or run botnets using export controls.

Dave Aitel
CEO
Immunity, Inc.