Invisible Network Address Translation for Botnets

Aaron Hairsine

Supervisors: Robert Edwards, Ramesh Sankaranarayana

Australian National University

u4671259@anu.edu.au

August 14, 2013
A device connected to the Internet receives information as a series of bits on a medium.

The devices the connect, make up, and pass data through the Internet are under the control of many entities.

Any bit can be changed (or read) by any device the information passes through.
“use a third party computer for the specific purpose of gaining access to a target computer”

“The purpose of this power is to allow ASIO to access the computer of suspected terrorists and other security interests”

“Importantly, the warrant would not authorise ASIO to obtain intelligence material from the third party computer.”

A spokesman for the Attorney-General’s Department - 13 JAN 2013
“use a third party computer for the specific purpose of gaining access to a target computer” Why?

Resources

- Public IP Address
- Legitimate User (someone actually uses it)
- The distribution of the third parties
- Their hardware resources - relatively inexpensive

Reiterating: All networking is just bits on the wire. Any device that the information passes through can change (or read) any of the bits.
Use techniques similar to Source Network Address Translation (SNAT) to utilise an IPv4 address without disruption of the legitimate end devices.
Insert a device, a piece of malware, or configuration change.
Now that you have these resources you can:

- Impersonate legitimate end users
  - Redirect any traffic to appear as if it came from a legitimate end user

- Run your own **state sponsored botnet**.
  - Attack target devices in a highly distributed fashion
It is highly likely that this (or similar) is already being done (Governments like America and China) but we are going to do this now.

1. Provide a **proof of concept** and explore hidden pitfalls
2. Develop countermeasures or **detection techniques**.
3. Explore **plausible deniability** ramifications
Questions?