CERIAS

the center for education and research in information assurance and security

Botnet Behavior Analysis

James E. Goldman, Sean C. Leshney*, Bradley J. Nabholz, Deepak R. Nuli, Nicklas R. Peelman

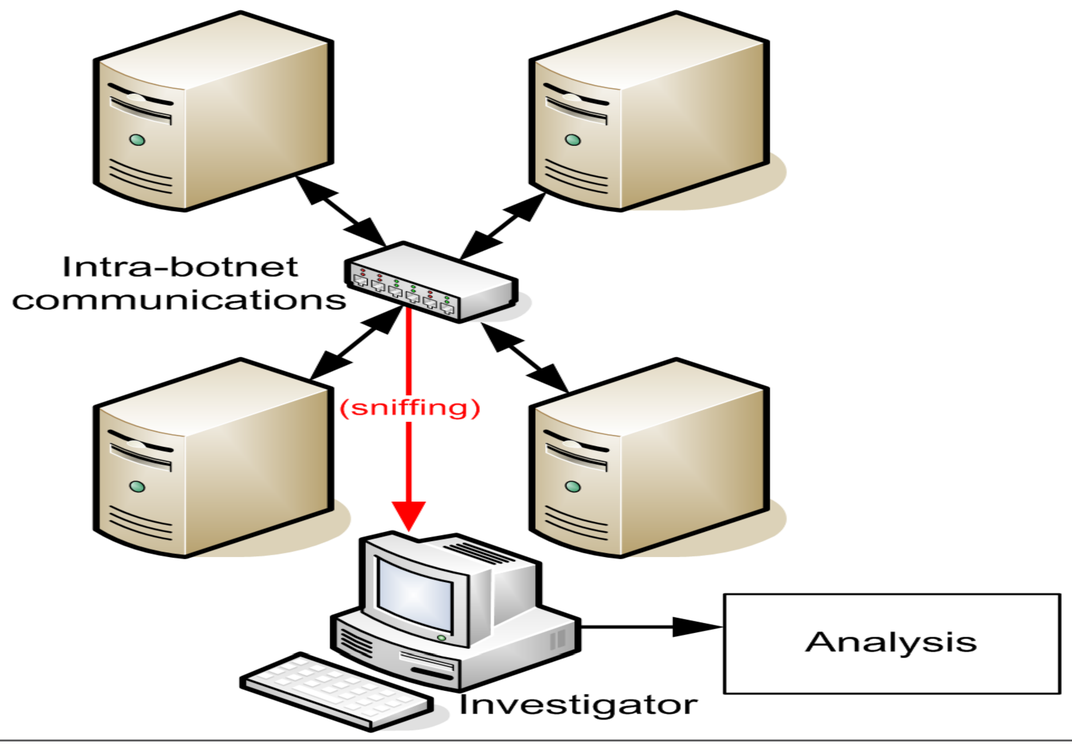
OVERVIEW

As part of current research into malware behavior, the Botnet Analysis Team is developing standardized architectures and processes with which to isolate, observe, and analyze botnets. Botnets are typically used for illegal activities, and are often made up of thousands of compromised computers. Botnet simulation will use a cluster of PCs configured with typical operating system and software configurations used by homes and businesses today.

PROBLEM

Botnets are often used for nefarious purposes, such as the following:

- Large-scale denial-of-service attacks
- Sending unsolicited e-mail (spam)
- Sending fraudulent e-mail (phishing)
- Distributing trojans, worms or viruses
- Distributing pirated media or software
- Facilitating “conventional” criminal activity, by concealing the source of electronic attacks



PROCESS

- In a controlled and isolated environment, launch botnet on cluster of PCs
- Using another workstation to sniff the network or “listen in,” record communications between botnet participants
- Analyze the recorded data for patterns, giving insight into the botnet’s operation and behavior

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center