The Botnets System: Network-wide malicious traffic detection

Jake Czyz
Research Engineer
jake@merit.edu

MJTS Meeting
2010-04-07

merit NETWORK

Agenda

- Background Concepts
- System Overview
- System Infrastructure
- Software Architecture
- Detectors and Features
- Brief Demo
- Limitations and Future Work

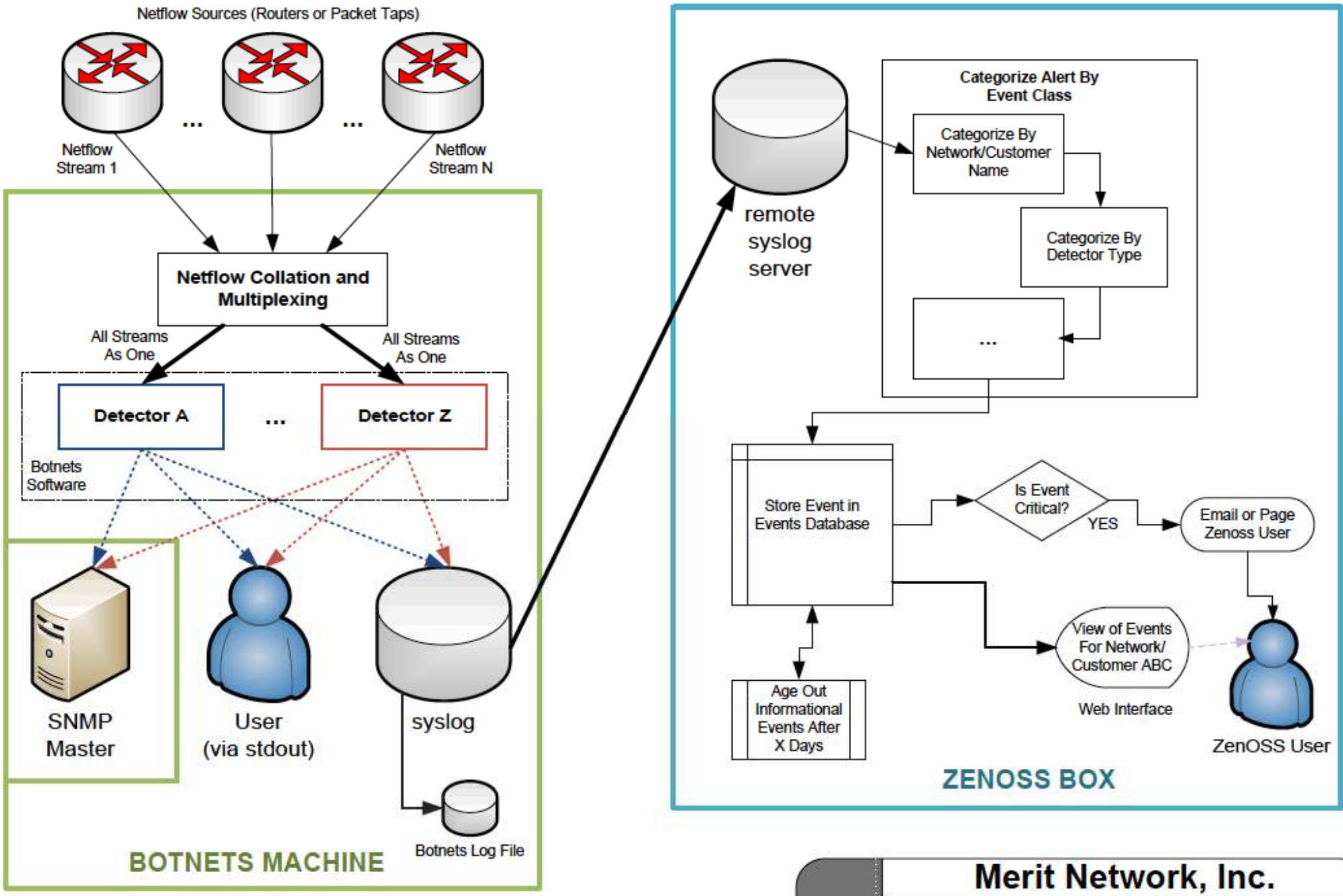
Background Concepts

- **netflow**
  - Records of IP flows (src ip, dst ip, src port, dst port, packets, bytes, tcp flags, etc.)
  - Generated by routers (usually sampled) or packet taps that get a mirror of the traffic
  - Used by ISPs and large networks for traffic accounting
- **botnets**
  - networks of compromised hosts used for DDOS, spam, and other nefarious purposes

System Overview

- Python-based software that implements several standalone malicious network traffic detectors
- Able to detect suspicious traffic related to botnets or other anomalous activity
- Passive
- Scalable
- Flexible
- Hackable
- Free (as in both beer *and* freedom)

Botnets High-Level System Architecture



Merit Network, Inc.

J.Czyz - jake@merit.edu | 2010-03-22

Software Architecture

- Python 2.6 : Rapid development, highly readable and maintainable code
- Object-oriented design for better code reuse and quicker detector writing
- Main Code components:
  - BotnetsDetector Superclass:
    - Implements most features, including: option parsing, whitelisting, history/purge/email, network naming, etc.
  - Subclasses:
    - IrcDetector, PortscanDetector, SynFloodDetectror, etc.
  - Logging module:
    - Can log to stdout, syslog, snmp
- Per-detector unit tests that read netflow from CSV files

Software Architecture

- Standard python distutils packaging/installation system
  - i.e. `python setup.py install`
- Tested on:
  - CentOS 5.4 (32 and 64 bit)
  - Ubuntu 8.04 (32 bit)
  - Should work on most modern Linux distros
- No current plans for a Windows version
- Extensive internal comments for easy modification
- Network operator friendly features

Current Detectors

Detector	Purpose/Features	Issues
Blacklist (and shadow, cymru, bogon, darknet derivitives)	initialized with one or more blacklist or specific IP/prefix; detects traffic destined to addresses in blacklist; Can help build list of all active IPs	Need separate script / manual download of cymru & shadow files; Lots of positives inside ISP depending on bogon filtering poilcy
IRC	Simply reports traffic destined to one of the several well-known IRC ports; ignores likely innocuous traffic	High false positive rate due to legitimate IRC traffic
Port Scan	Alerts when more than threshold well-known ports are connected to in threshold seconds by a single source	Could be more efficient
Syn Flood	Alerts when too many syns are seen within threshold time window to the same destination	Could be more efficient
SMTP Spam	Flags SMTP server-like behavior, often indicating a compromised host	Early alpha status
Service/Server	Flags server services	Early alpha status

Brief Live Demo

Limitations

- Shallow packet inspection
- An unsampled netflow stream is needed for the system to be most useful
- High sensitivity => Lots of alerts
- Beta software
- Better system performance validation needed

Future Work

- Overall System Tasks
  - Pilot in progress: Sys. Validation by having alerts investigated by actual Merit customer
  - Characterization and estimation of alert volumes
  - Web page for open sourcing of code & Release software into the wild
- Future detectors: beaconing detector, IP scan detector
- Future Features we're working on or thinking about:
  - Richer summary information emailed during the periodic purge
  - More details about events leading to alerts written to disk for each
  - Additional non-netflow detector types (e.g. distributed brute-force attack detection via centralized syslog parsing; perhaps active probing)

Acknowledgements

- System was designed and written by Eric Vander Weele and Jake Czyz, with some code contributed by a UM CSE undergraduate course project
- Leadership by: Manish Karir (Merit) and Michael Bailey (UM)
- Funding comes from the Department of Homeland Security (DHS)

Questions?

Thank You!