Regional Botnet Detection

Jake Czyz
Research Engineer
Merit Network
jake@merit.edu

Michael Bailey
Research Faculty
University of Michigan
mibailey@eecs.umich.edu

Manish Karir
Director of Research
Merit Network
mkarir@merit.edu

Dave Dittrich
Senior Security Engineer
APL - University of Washington

Michael K. Hamilton
Chief Information Security Officer
City of Seattle

NANOG 49 – San Francisco, CA
Security BOF
2010-06-14

merit NETWORK

Agenda

- Motivation & Vision
- PRISEM
- A Botnet Detection System
- Ongoing and Future Work
- Conclusion

Criticality of Local Government

- Federal gov't wants resilience from all hazards
  - vs. OLD message of "preventing terrorism"
  - Effective first response is key to resilience
- Local government
  - Is first responder, last to leave scene in any disruption
  - Is where 100% of critical infrastructure is deployed
  - Infosec controls neither prioritized nor regulated
  - But, all response services are enabled by IT
- Thus, we have a problem that requires immediate attention

Grand Challenges for State/Local Government Cybersecurity

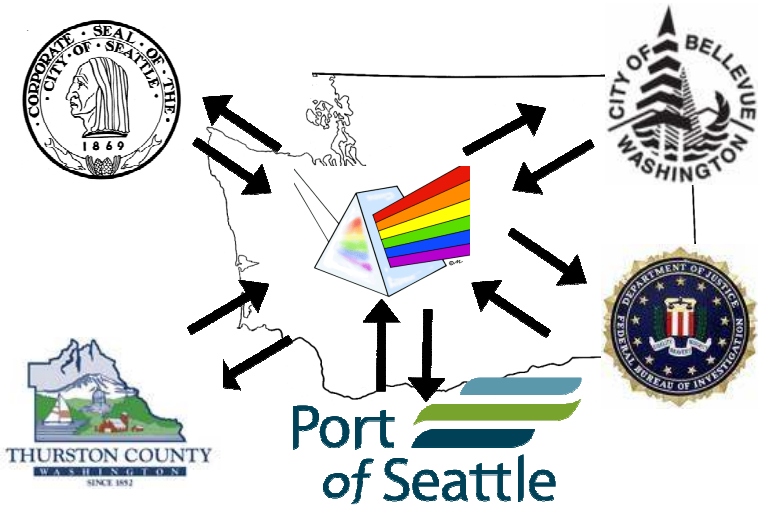
- Antiquated technology and methods (socio-technical problem set, not just technical)
- Under-resourced and overwhelmed
  - Small regional networks often lack the security expertise necessary to take action on the information
  - Metropolitan areas need a “block-watch” model
- Key challenges:
  - **Balancing privacy rights** concerns with gathering & sharing quality cybercrime intelligence
  - Current information sharing methods (phone calls, bulletins, ISACs, portals, notification systems, etc.) fall short (don’t scale, reactive, no aggregation, no situational awareness, classification system sometimes a hindrance)

DHS S&T *STATE & LOCAL* Government Botnet Technology Transfer

Program: DHS S&T RTAP CS 1 - Botnet Detection and Mitigation – Phase 2

Goal: Transition US-CERT technology to local and state governments through the **Public Regional Information Security Event Management (PRISEM)** project

- **Enhance the information security and compliance** status of participant agencies
- Provide a **method for reporting cyber-security event and trend information** to participants, and the intelligence and law-enforcement communities
- Create an operational setting for the **deployment of research**-grade technologies



merit NETWORK

Visions

- **A paradigm for local government security information and action sharing – one also applicable to small ISPs and other resource-constrained networks**
  - Pilot underway involving the University of Washington, City of Seattle, and other local governments
  - Testing processes and agreements to share infosec intelligence while guarding privacy
- **A Community and toolset enabling less-expensive federated security monitoring:**
  - Repository and community around set of open-source free modular tools for botnet detection
  - **http://www.botnets.org**
  - Seeded with an initial set of detectors developed by the University of Michigan and Merit, funded by DHS under PRISEM (the "Botnets System")

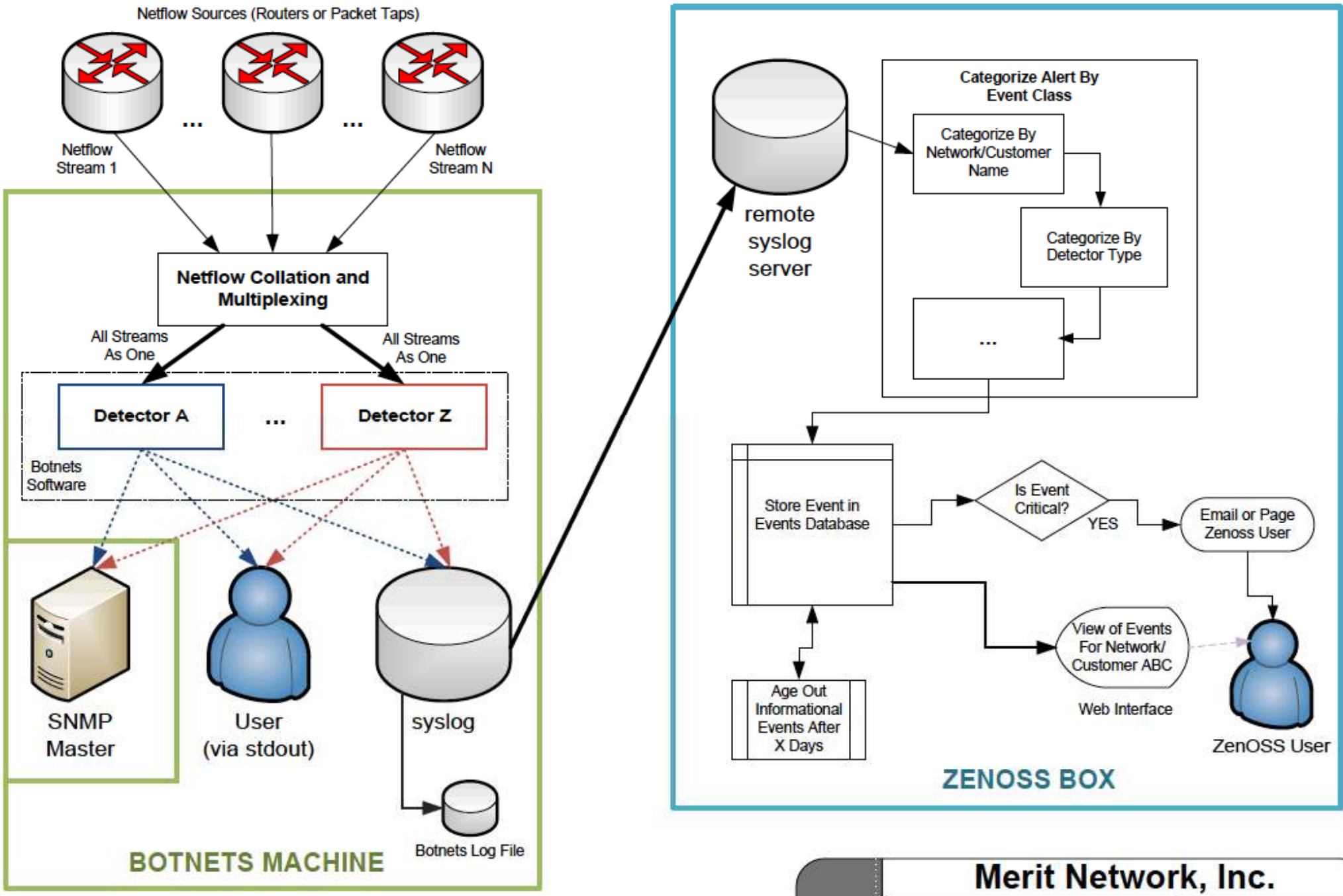
Privacy and Other Concerns PRISEM Pilot Attempts to Address

- These issues **have been a serious obstacle** to similar security info sharing efforts in the past
- Participant-driven governance
- Data retention/destruction fixed by state requirements
- Formal data-sharing agreement
- Notice of privacy practices (we don't want your user data!)
- Data access protocols and security controls

Initial Toolset Overview (the Botnets System)

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

Botnets High-Level System Architecture



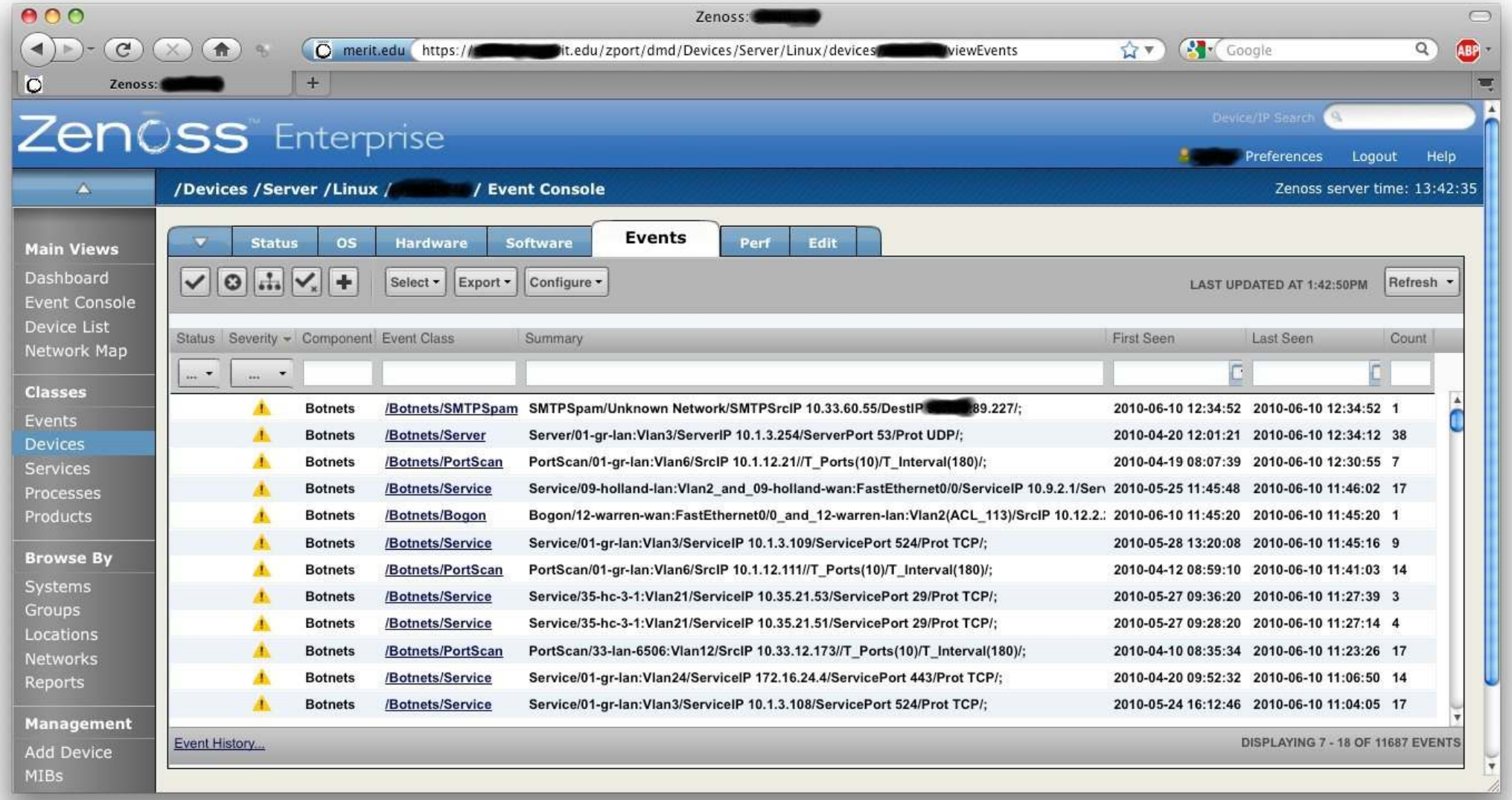
Merit Network, Inc.

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

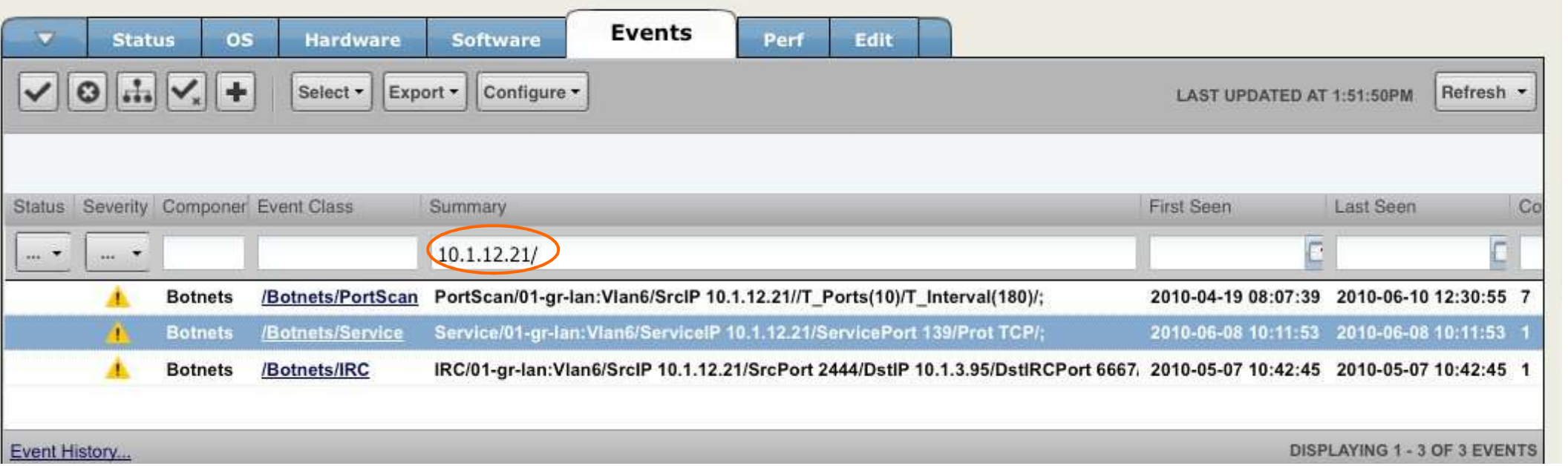
Current Detectors

Detector	Purpose/Features
Blacklist (and shadow, cymru, bogon, darknet derivatives)	Initialized with one or more blacklist or specific IP/prefix; detects traffic destined to addresses in blacklist; Can also help build list of all active IPs on a network
DNS	Reports DNS queries to blacklisted domains (receives syslog from resolvers)
Port Scan	Alerts when more than threshold connections to well-known ports are attempted in threshold seconds by a single source
Syn Flood	Alerts when too many syns are seen within threshold time window to the same destination
SMTP Spam	Flags SMTP server-like behavior, often indicating a compromised host
Service/Server	Flags server services (well known ports) or traffic volume indicative of likely server
IRC	Reports traffic destined to one of the several well-known IRC ports; ignores likely innocuous traffic
Feature	Alerts when a flow matching commandline-specified features is detected (e.g. src/dest ip, src/dest port, protocol, packet count)

Zenoss: a Poor-Man's SEM



Zenoss: a Poor-Man's SEM



Ongoing and Future Work

- Botnets System (detectors) pilot in progress: Sys. Validation by having alerts investigated by actual Merit customer, Davenport University
- Incorporate pilot and user feedback
- Evaluation with other SEM (e.g. Alienvault OSSIM)
- Enhance current & create additional detectors
- **Build a community around core toolset and a repository for maintained open source detectors**

Conclusion: The Trickle Down Effect

- Trickling down NSP-SEC sorts of activities to lower regional and local communities is a challenge
- Sharing and coordinating with peers is only one aspect of the problem, we need to ensure diffusion of both expertise as well as condensed knowledge and alerts to all layers
- State/Regional government structures and issues are similar in nature to the relationship between service providers and customers as well as regional networks and campuses or even a campus and its departments
- Our goal is to create a co-operative environment where groups can share some basic tools, architectures, and knowledge to make it easier to implement a minimal set of current best practices

Thank You!

Other Feedback and Questions

botnets@merit.edu

merit NETWORK

Backup Slides

City/Regional Information Sharing

- How it's done today:
  - Phone calls and personal relationships
  - Online Publications / Blogs and Sites / DHS Daily
  - Portals, ISACs, and more portals; Vendor reports
  - National, State, Regional Notification Systems
- Problems with this way:
  - Personal relationships do not scale; reactive
  - One-way communication, not inter-sector
  - No summary/aggregate; no situational awareness
  - Classification system sometimes a hindrance

Initial Toolset Architecture

- Python 2.6 : Rapid development, readable, maintainable
- Standard python distutils packaging/installation system
- Object-oriented design for better code reuse and quicker detector writing; highly-commented code
- Main Code components:
  - Collectors: netflow5, ascii (csv), syslog
  - BotnetsDetector Superclass:
    - Implements common core features, including: option parsing, whitelisting, history/purge/email, network naming, etc.
  - Subclasses: IrcDetector, Server…, Portscan…, SynFlood…, etc.
- Network operator friendly features
- Runs on Linux (tested on CentOS and Ubuntu)

Glossary

- DHS – Department of Homeland Security
- DHS S&T RTAP CS – DHS Science and Technology Rapid Technology Adaptation Program: Cyber Security
- ISAC – Information Sharing and Analysis Center
- OSSIM – Open Source Security Information Management (by Alienvault)
- PRISEM – Public Regional Information Security Event Management
- SEM – Security Event Management
- SIEM – Security Information and Event Management