SwRI
SOUTHWEST RESEARCH INSTITUTE

DEFENSE &
INTELLIGENCE
SOLUTIONS
A Division of SwRI

Protecting large organizations and communities through the use of a Honey Community

James Rutherford

16 Nov 2015

Agenda

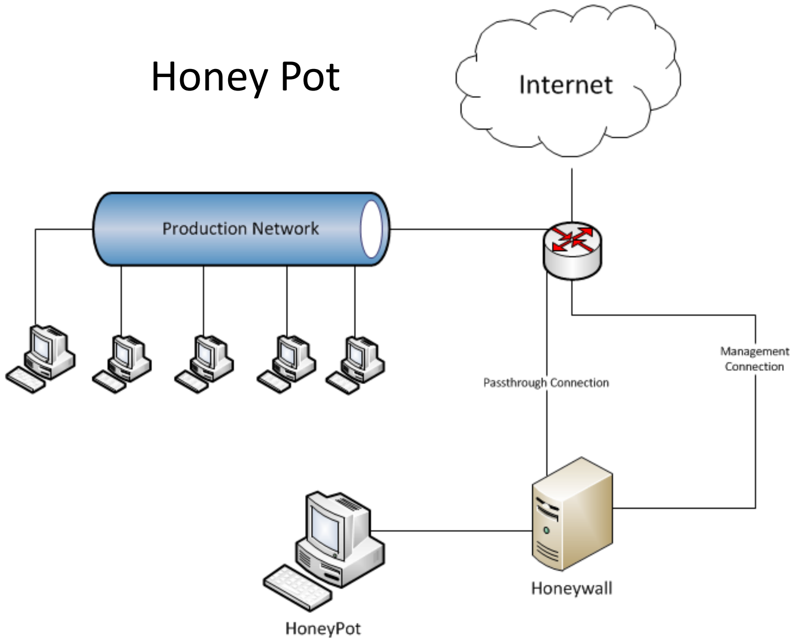
- Overview of the Honey Community
  - – Honey Devices
  - – Data Collected
  - – Observations
- Expanding the Concept
  - – Changes needed
  - – Architecture
  - – Challenges

Participants

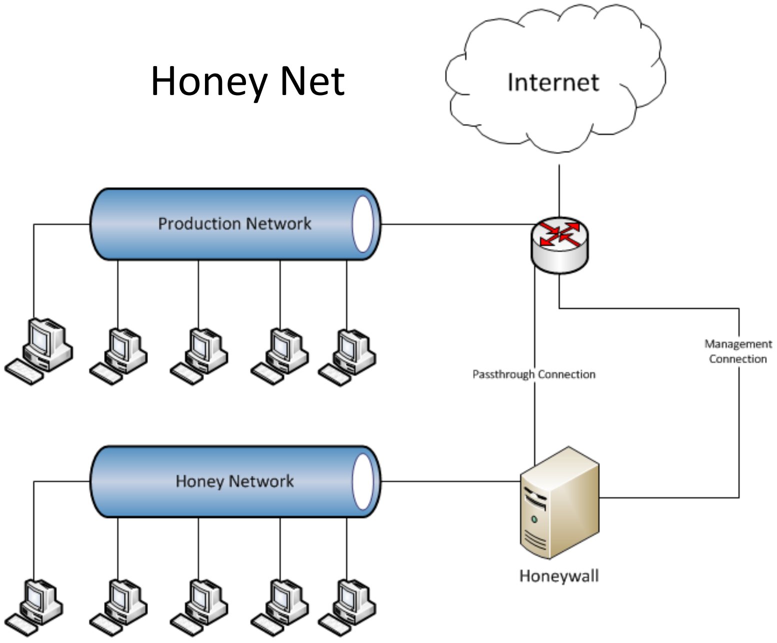
- Southwest Research Institute
  - Defense and Intelligence Solutions
- University of Texas at San Antonio – Center for Information Assurance and Security
  - Dr. Gregory B. White - Director

Honey Devices

Honey Pot



Honey Net



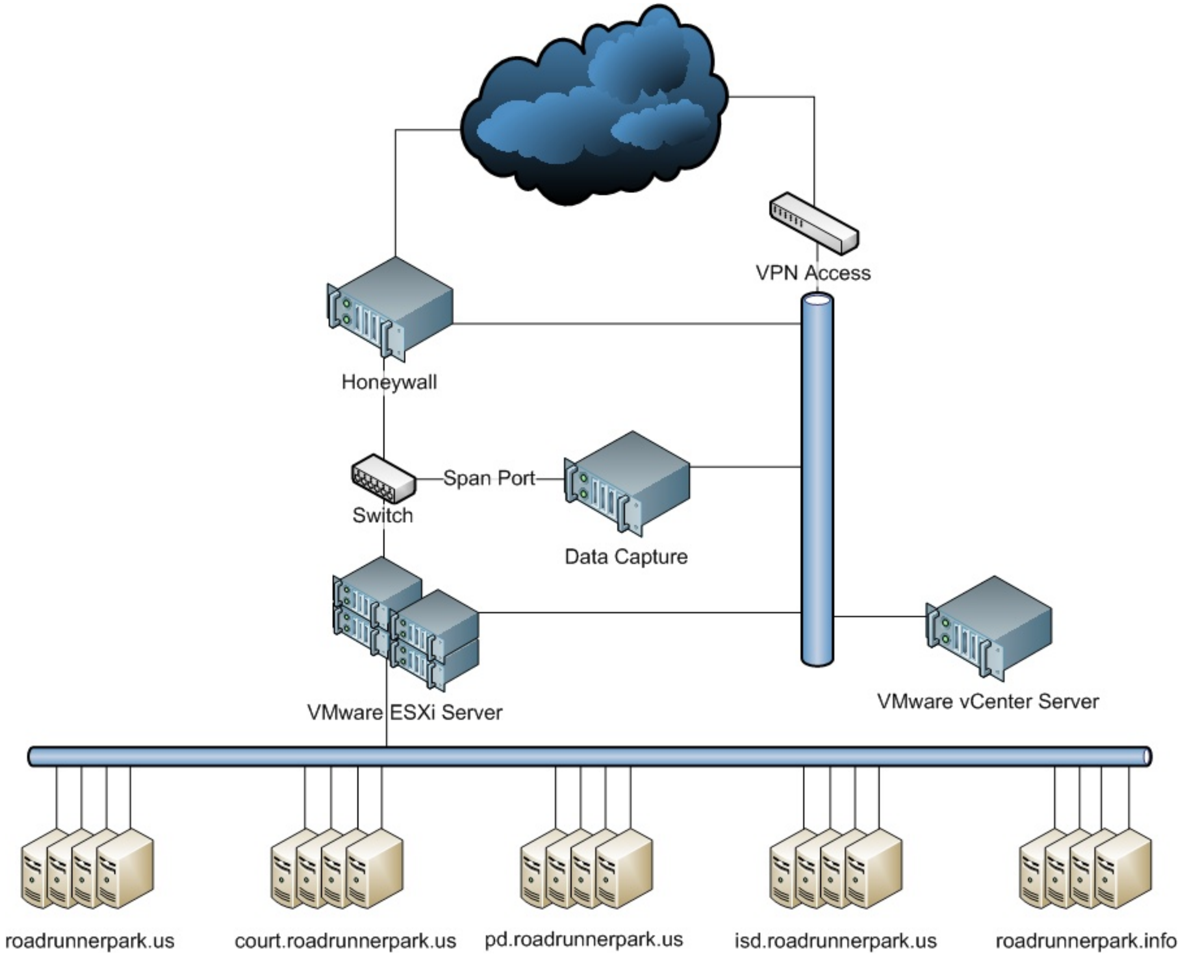
"A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource." – Lance Spitzner, 2003

"It is an architecture of a fishbowl to watch what happens when a network is compromised" – Lance Spitzner, 2005

The Honey Community

- Original Concept
  - – Centrally located (Single IP Address Block)
  - – Limited number of systems
  - – Identical IT structure (OS and Software)
- Ideal for initial concept
  - – Easy data collection
  - – Easy to maintain control of the systems
  - – No information sharing challenges

Honey Community Circa 2012



Honey Community Diagram Circa 2012 as developed by Keith Harrison

Looking across multiple sectors helps

Number of Sectors	Identified Attacks
*	1,402
1	1,430
2	151
3	52
4	16
5	9

Sector	Identified Attacks
Community	2,319
Water and Sewer	369
Criminal Justice	345
Emergency Response	398
Education	381
Commerce	504

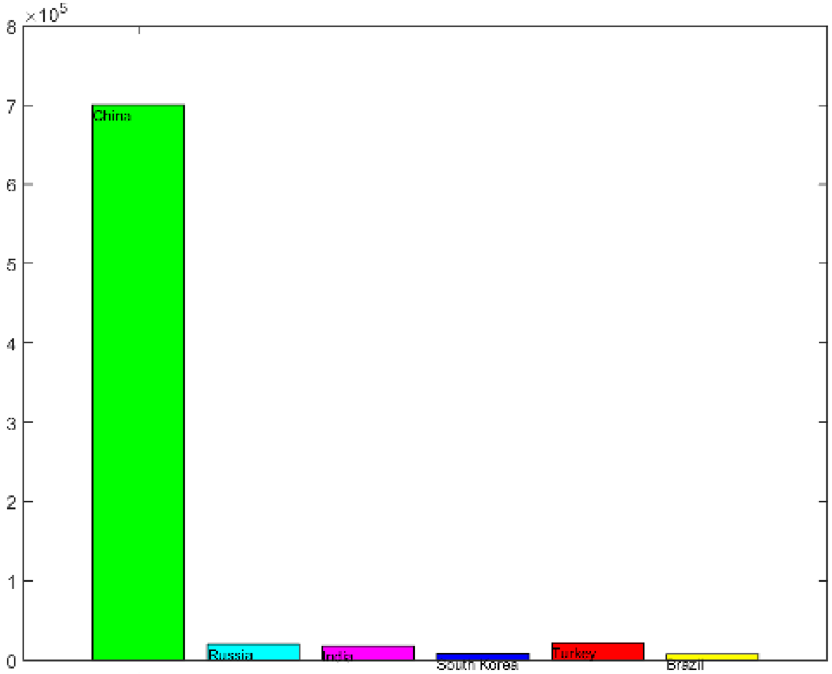
- 3,060 IDS alerts generated by SNORT
- 55% of attacks can be seen as an attack on 1 or more sectors
- 45% of attacks were not attributed to a sector but the effort could be seen across the entire enterprise
- Attacks against 1 sector appeared to re-appear later against another sector

Harrison, Rutherford, and White. "The Honey Community: Use of Combined Organizational Data for Community Protection." *System Sciences (HICSS), 2015 48th Hawaii International Conference on*. IEEE, 2015.

Early Analysis

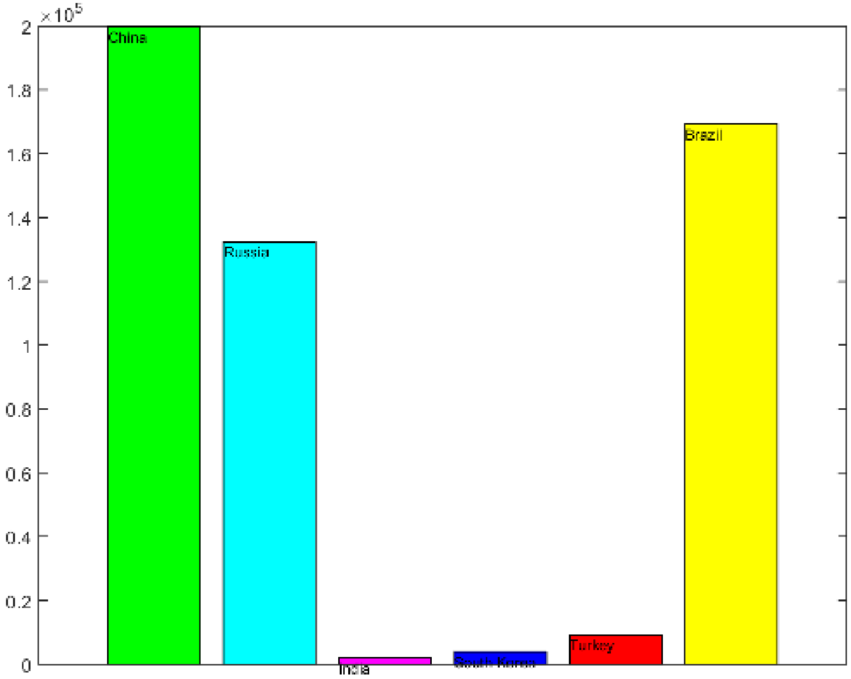
- Attacks and Attackers change over time
- A large number of connections in the known port range
  - Also, a large number in the ephemeral range
  - Walking of the ephemeral ports
- Even though all systems were the same with regard to OS and software they were not all attacked the same

Connection Histogram



2012 Histogram of connections

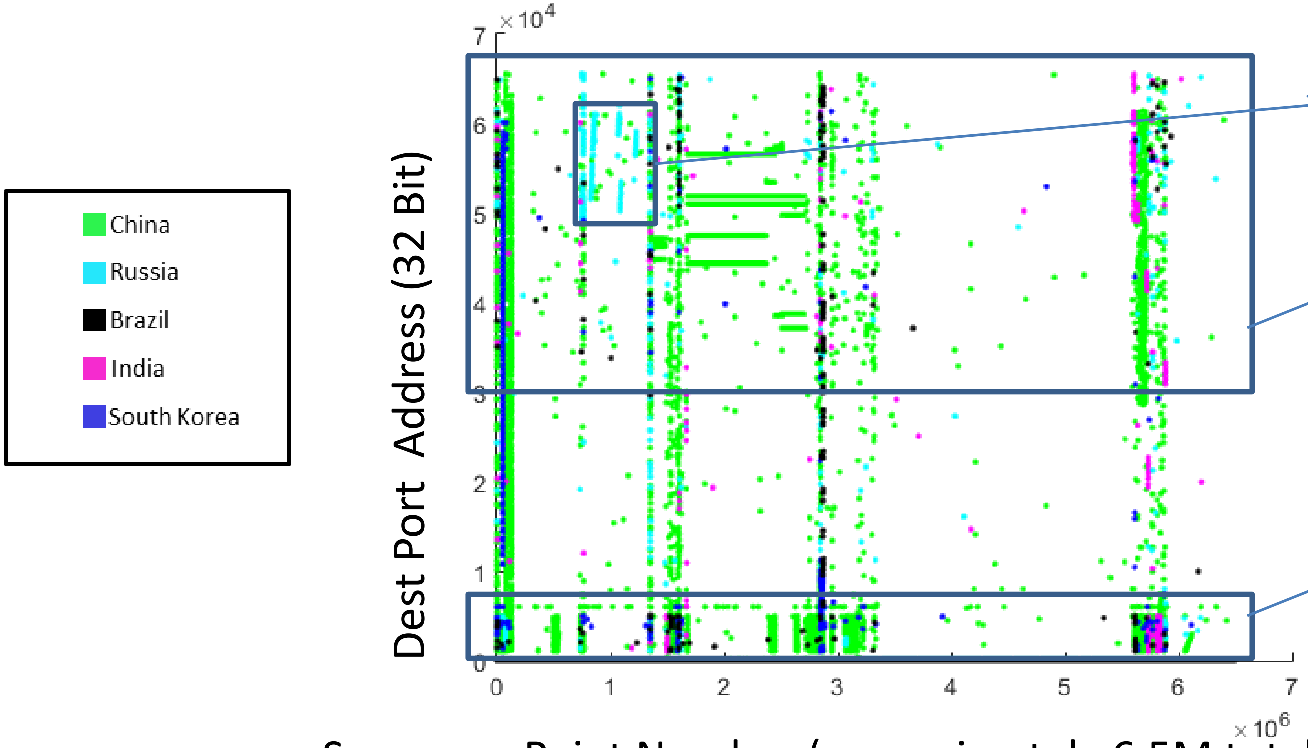
22 -31 August 2012



2014 Histogram of connections

1-13 November 2014

2012 Scatter plot of connections



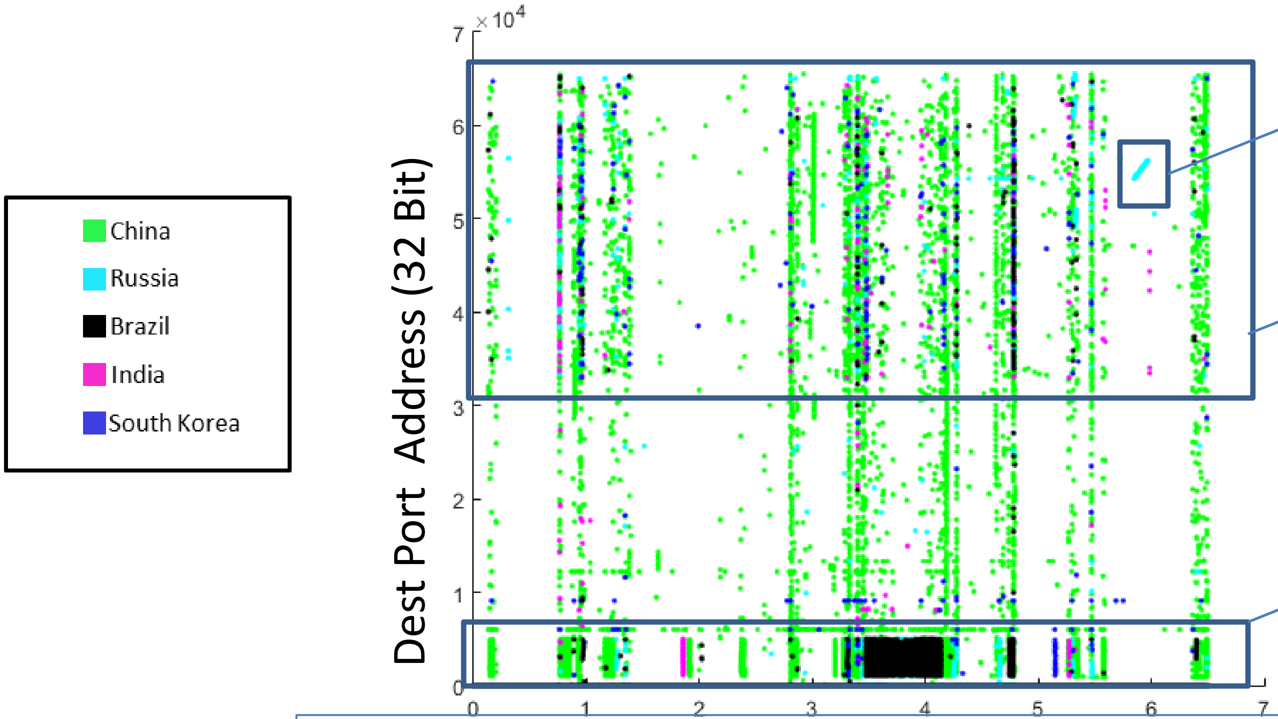
Interesting artifact

Ephemeral Ports

Ports 1-6000

Sequence Point Number (approximately 6.5M total)
22 -31 August 2012

2014 Scatter plot of connections



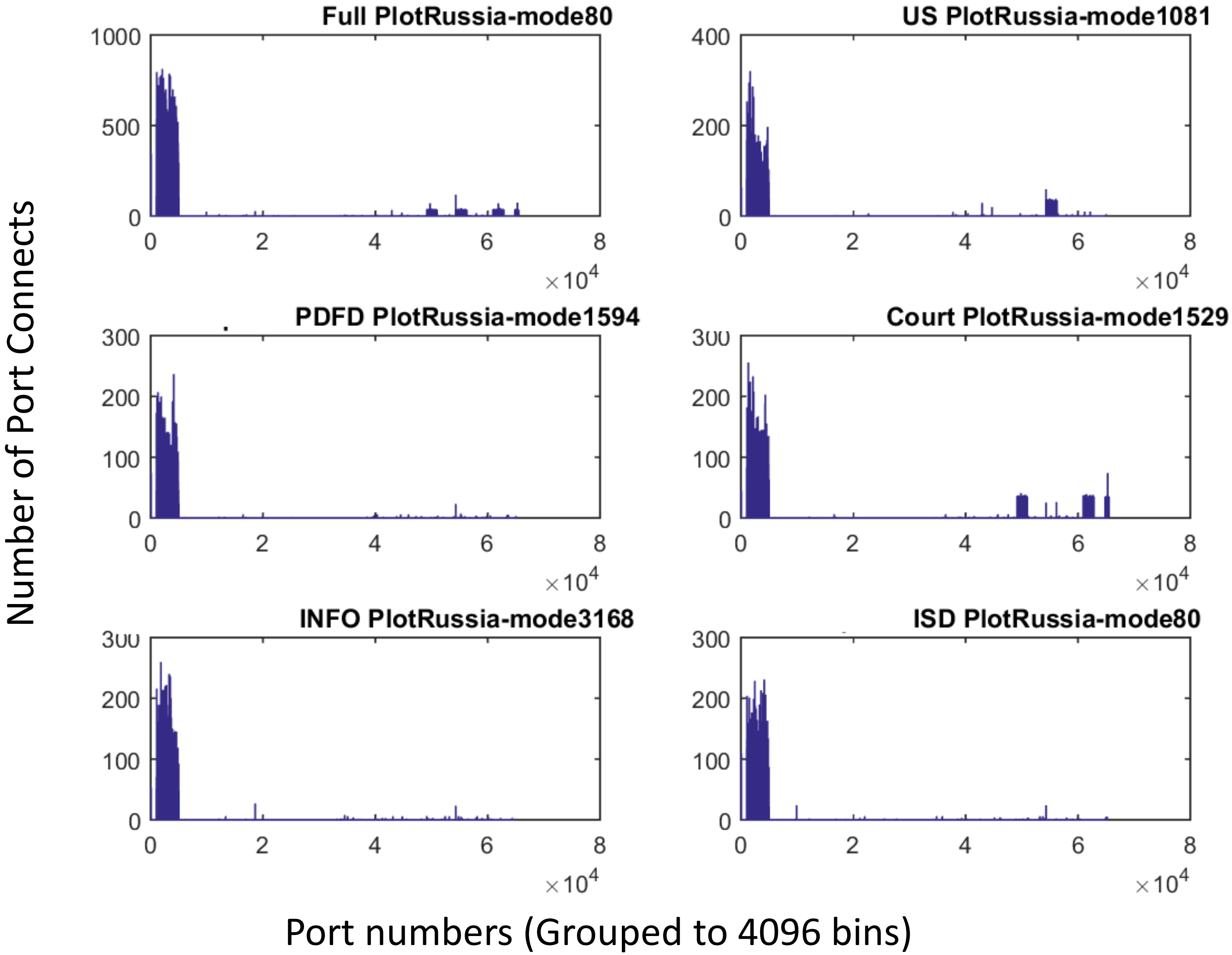
Interesting artifact

Ephemeral Ports

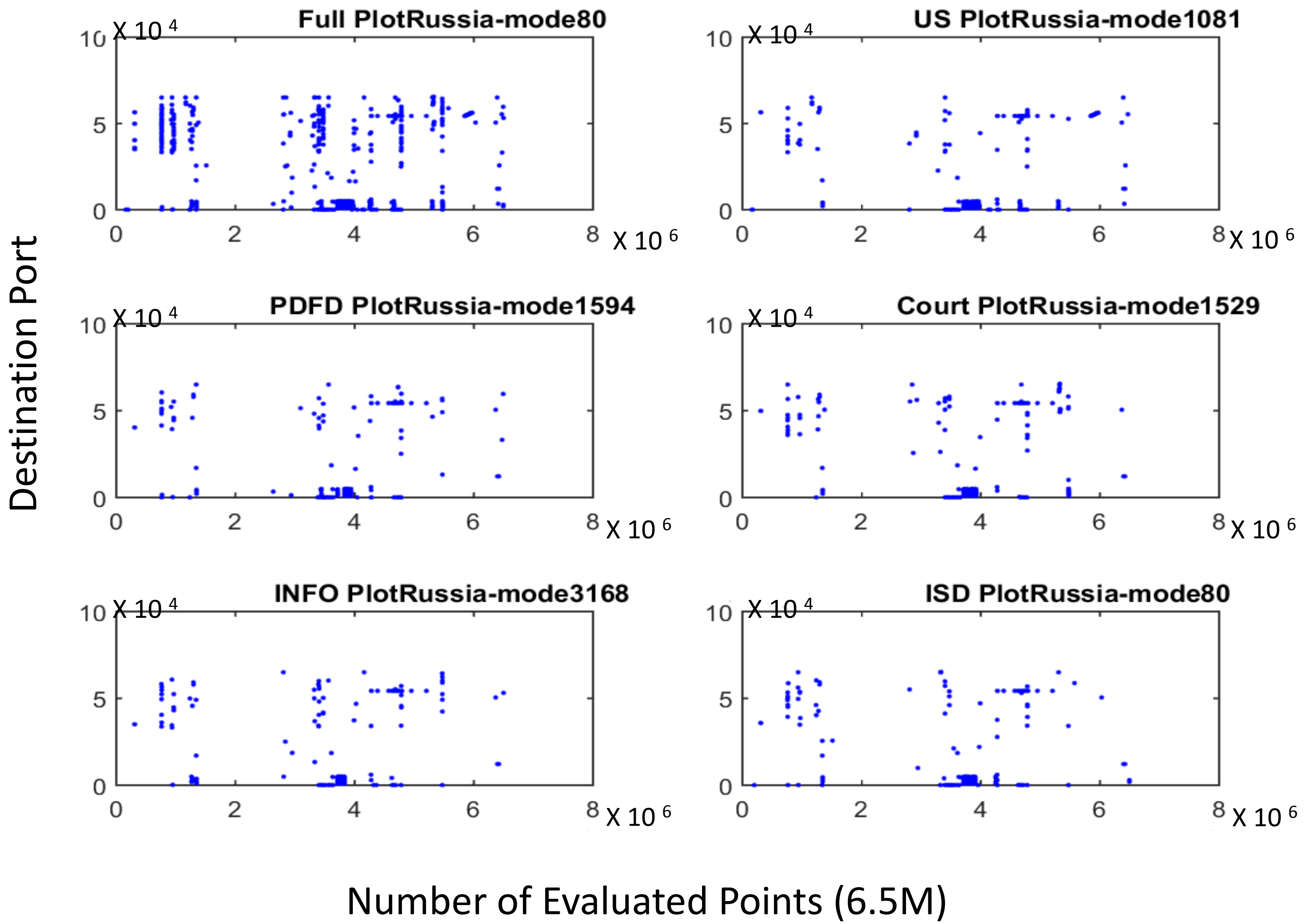
Ports 1-6000

Sequence Point Number (approximately 6.5M total)
1-13 November 2014

Histograms of Connections 2014



2014 Connection Plot



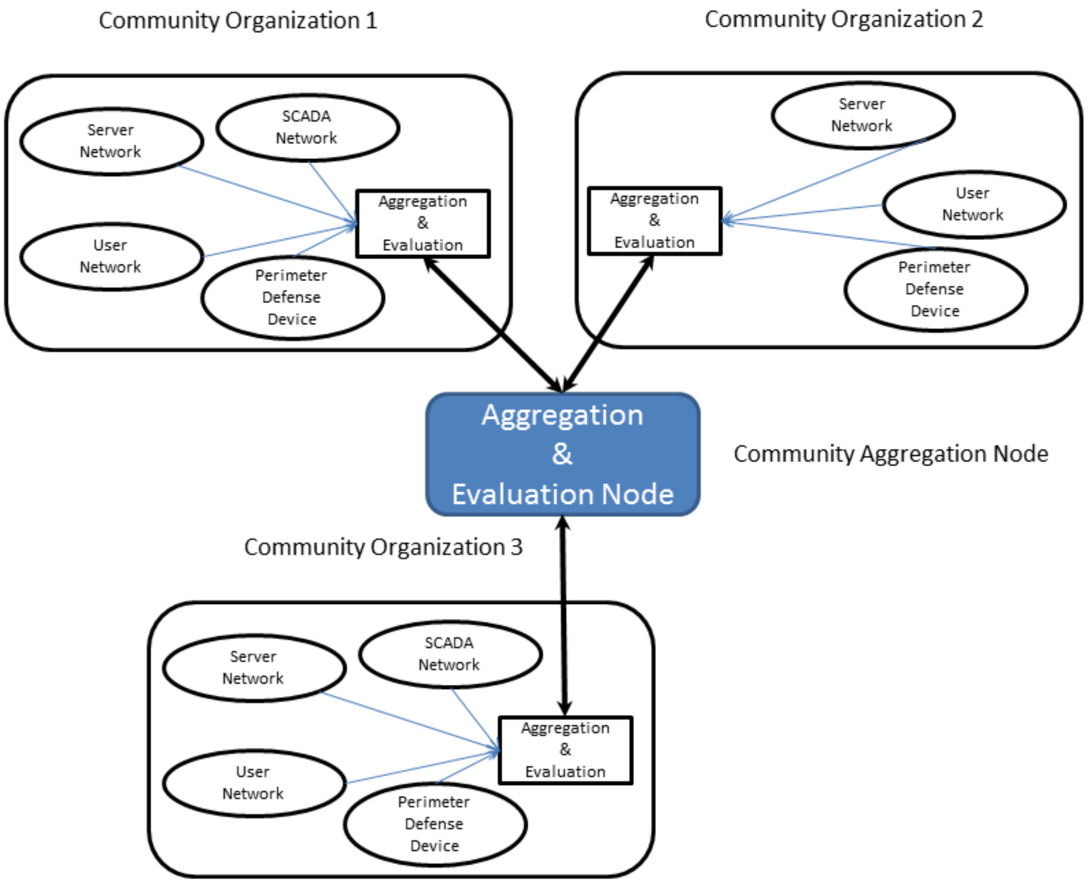
Improvements in the Honey Community Concept

- Current architecture good for collecting research information
  - Proved the basic concept as seen earlier
  - Easy to prove not a real entity
- However, needs to grow to be used in a non-research capability
  - Doesn't represent a real community
  - Won't scale
  - Doesn't take into account existing IT structures

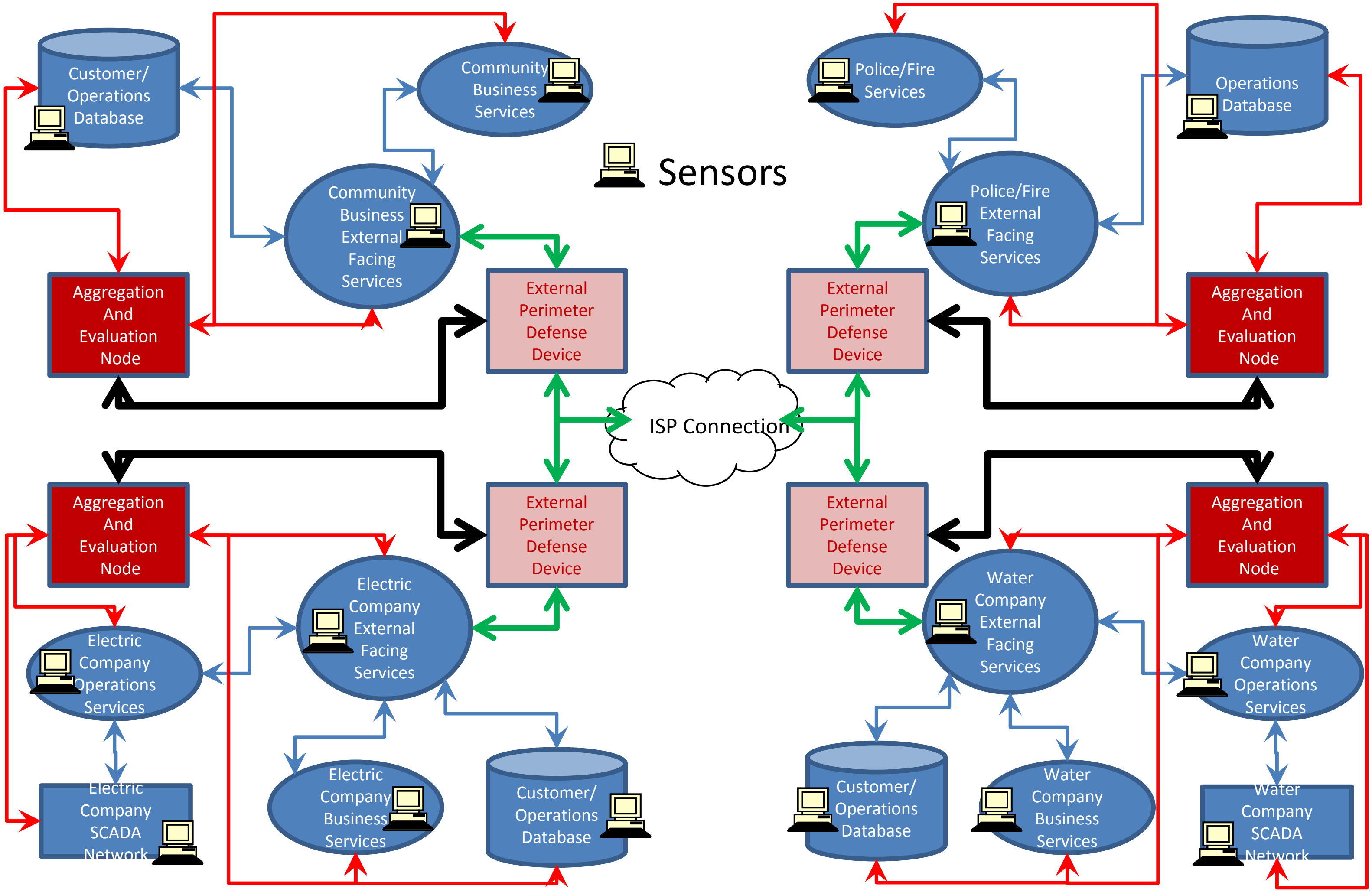
Changes in the Honey Community

- Must work with diverse IT infrastructures
  - Need low cost and easy to maintain sensors
  - Leverage the existing infrastructure
  - Make it difficult for the attackers to adapt
- Must scale both up and down
- Deal with information sharing challenges (contractual, legal, parochial)
- Needs to incorporate both internal sensor and external facing perimeter defense
- Share composited data between parts of the Community to provide better detection and information sharing
- A Taxonomy of cyber attacks comprising the information on attacks
  - Threats – Actors, Techniques
  - Effects - Direct and indirect indicators

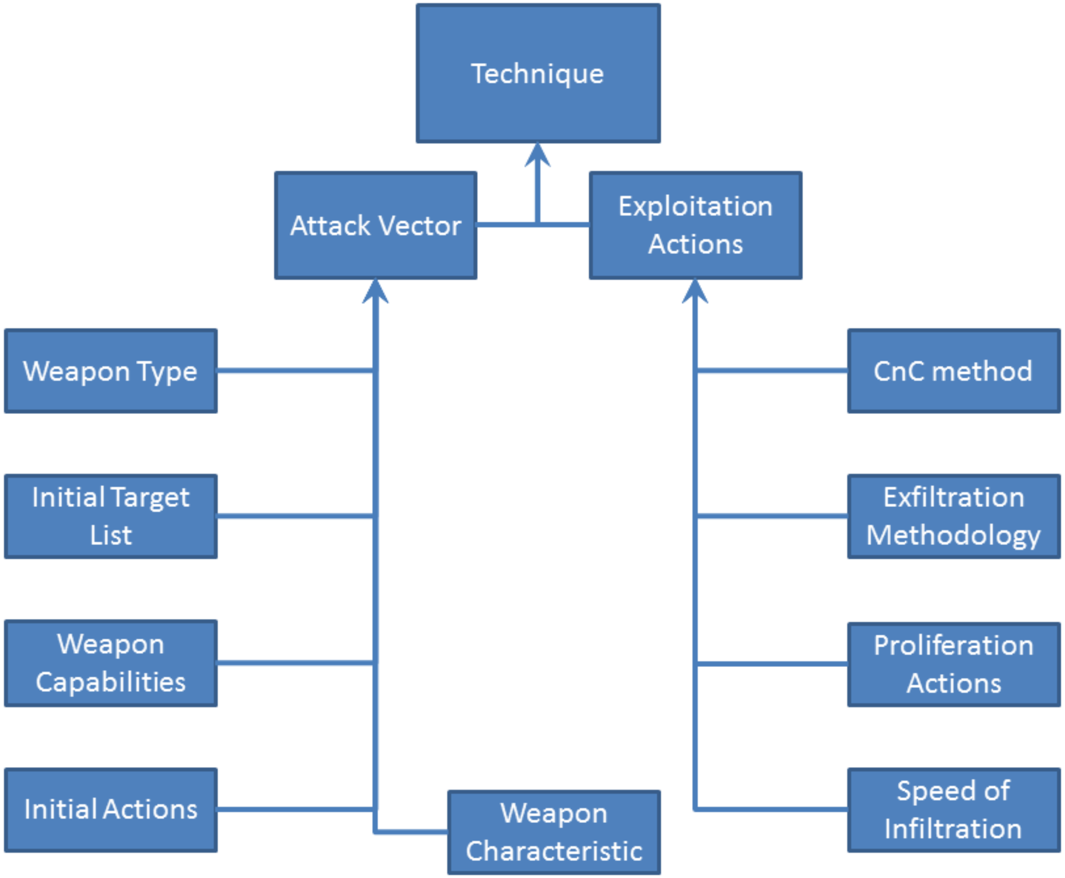
Updated Architecture



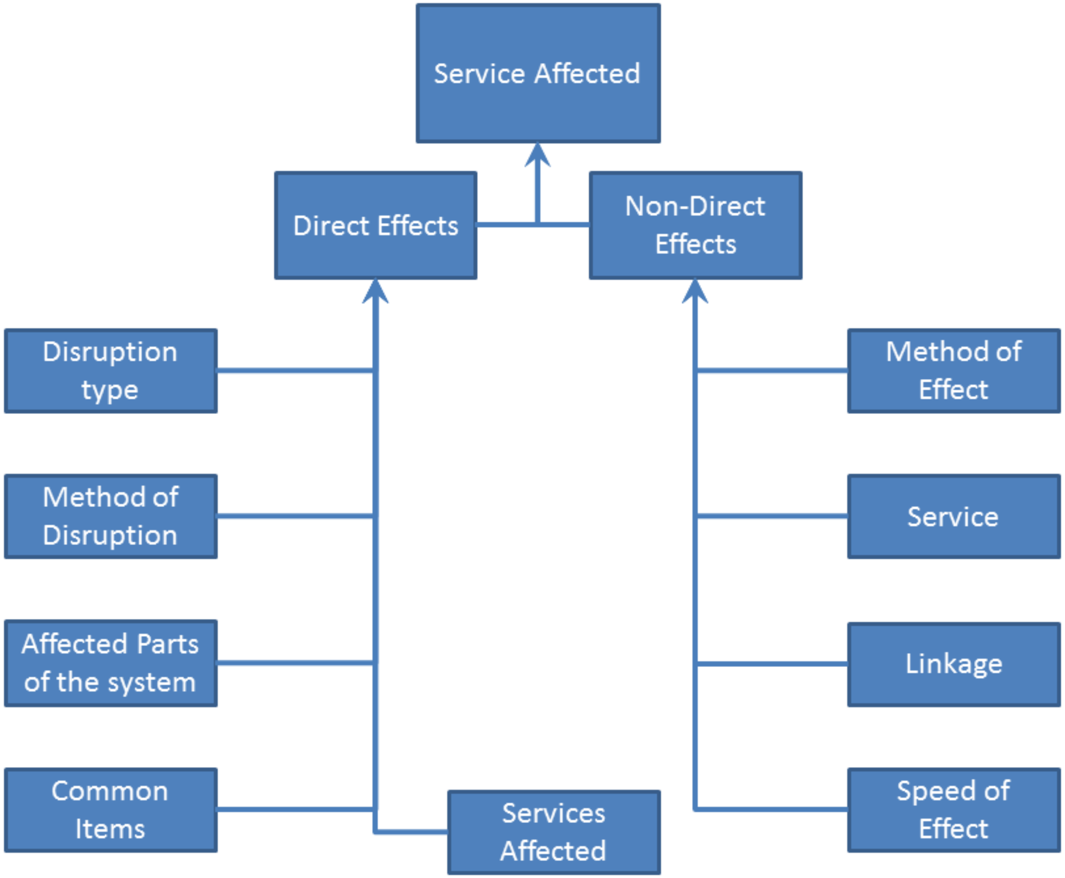
More Detailed


Customer/ Operations Database
Community Business Services
Sensors
Police/Fire Services
Operations Database
Community Business External Facing Services
Police/Fire External Facing Services
Aggregation And Evaluation Node
External Perimeter Defense Device
External Perimeter Defense Device
Aggregation And Evaluation Node
ISP Connection
Aggregation And Evaluation Node
External Perimeter Defense Device
External Perimeter Defense Device
Aggregation And Evaluation Node
Electric Company External Facing Services
Water Company External Facing Services
Electric Company Operations Services
Water Company Operations Services
Electric Company SCADA Network
Electric Company Business Services
Customer/ Operations Database
Customer/ Operations Database
Water Company Business Services
Water Company SCADA Network

Technique


Technique
Attack Vector
Exploitation Actions
Weapon Type
Initial Target List
Weapon Capabilities
Initial Actions
Weapon Characteristic
CnC method
Exfiltration Methodology
Proliferation Actions
Speed of Infiltration

Services Affected


Service Affected

Direct Effects

Non-Direct Effects

Disruption type

Method of Disruption

Affected Parts of the system

Common Items

Services Affected

Method of Effect

Service

Linkage

Speed of Effect

Challenges

- Low cost and low maintenance sensors
  - – Report information in a streamlined format
  - – Prototype developed
- Determining the meta-data that will be acceptable for release by members
- Developing data model and mining techniques to combine the information and report it up and down the chain

QUESTIONS?