CYBER SECURITY DIVISION
2013 PRINCIPAL INVESTIGATORS'

Cartographic Capabilities for Critical Cyberinfrastructure (C4)

CAIDA/UCSD
PI k claffy

18 September 2013

Homeland Security
Science and Technology

caida
www.caida.org

Team Profile

Cooperative Association for Internet Data Analysis (CAIDA)

- – Founded by PI and Director k claffy
- – Independent analysis and research group
- –15+ years experience in data collection, curation and research
- – located at UC's San Diego Supercomputer Center

Key personnel: Bradley Huffaker, Young Hyun, Marina Fomenkov, Josh Polterock, Ken Keys, Matthew Luckie

Customer Need

Global Cybersecurity Challenges

President Obama has declared that the “cyber threat is one of the most serious economic and national security challenges we face as a nation” and that “America's economic prosperity in the 21st century will depend on cybersecurity.”

To help address these threats, DHS needs:

- New measurement and data collection technologies
- Infrastructure to improve situational awareness
- Better understanding of the structure, dynamics and vulnerabilities of the global Internet

Approach

- Active measurement using Archipelago measurement infrastructure
  - Ongoing measurements
  - Randomly probe entire IPv4 address space at /24 granularity
  - 77 monitors and growing
- Alias resolution measurements
  - Every six months
  - Improved tools and techniques
- Collect and analyze additional data on Autonomous Systems
  - Annotate graph
  - BGP, WHOIS, performance data
  - Financial data

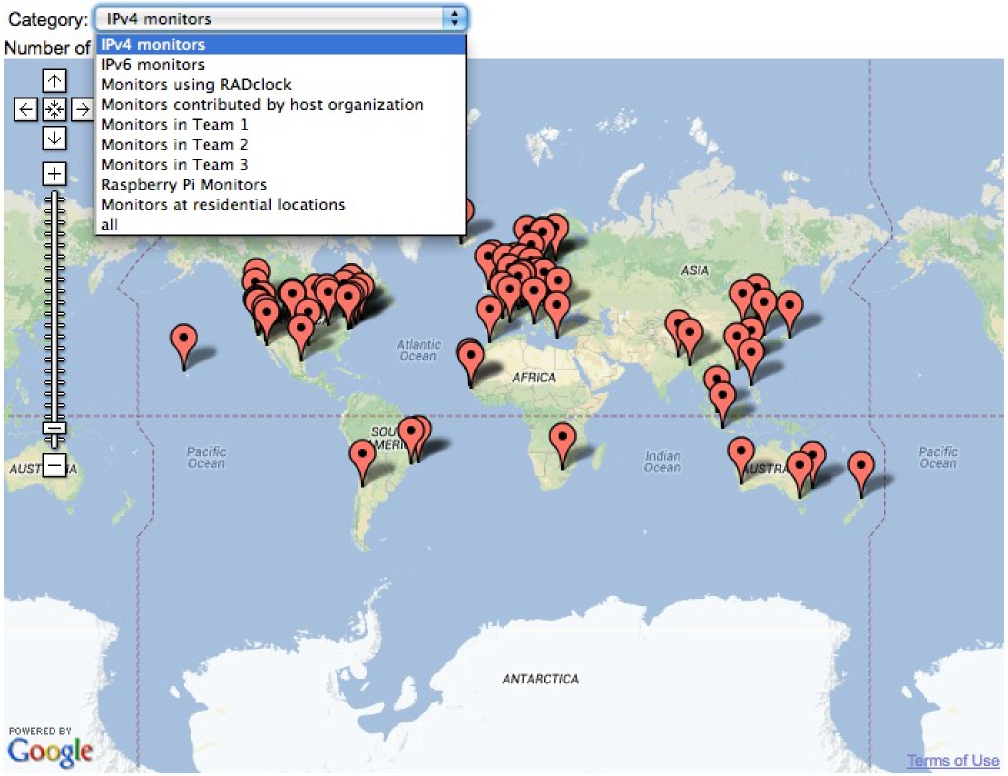
Approach

- Collect, synthesize, curate data into Internet Topology Data Kit (ITDK)
  - Data sources: active IP layer measurement, BGP, DNS (active and passive), geolocation data
  - Derived data: IP paths, AS paths, router aliases, device locations
  - Results: AS relationships, AS paths/links, router locations, router to AS assignments, hostnames, router graphs including nodes and links

Increased coverage of Internet

Task 1: Improve completeness of macroscopic Internet maps

Archipelago Measurement Infrastructure

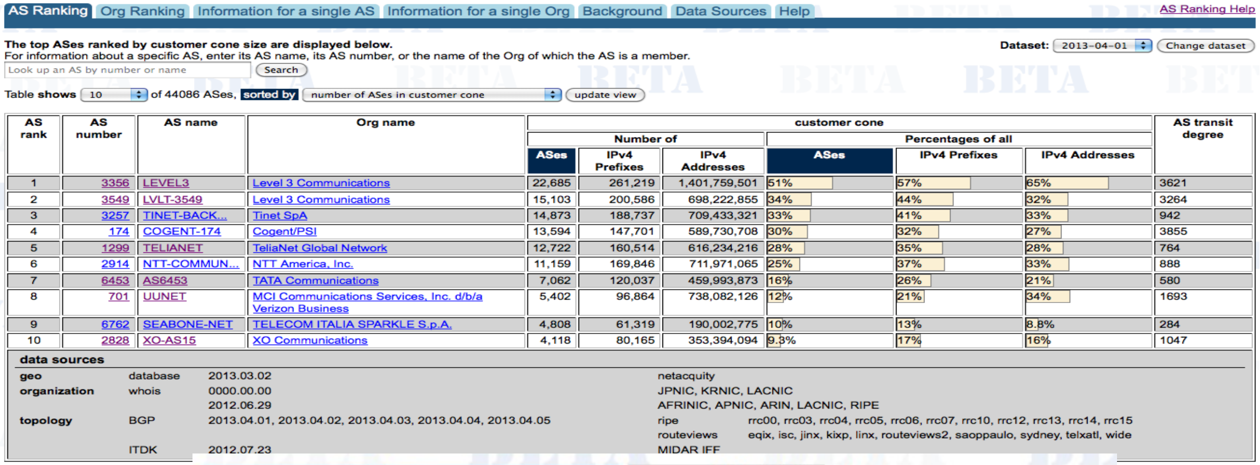


Category: IPv4 monitors

Increased Completeness, Accuracy and Richness of Annotations

Task 2: Increase accuracy of macroscopic Internet maps

AS Ranking of Autonomous Systems



The top ASes ranked by customer cone size are displayed below.
For information about a specific AS, enter its AS name, its AS number, or the name of the Org of which the AS is a member.

Look up an AS by number or name

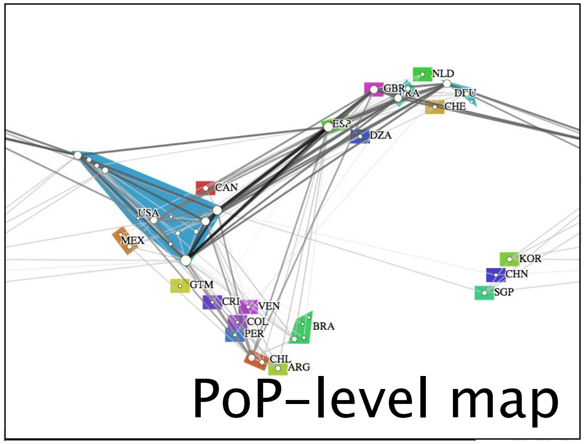
Dataset: 2013-04-01

Table shows 10 of 44086 ASes, **sorted by** number of ASes in customer cone

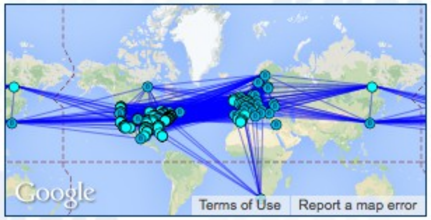
AS rank	AS number	AS name	Org name	customer cone						AS transit degree
				Number of			Percentages of all			
				ASes	IPv4 Prefixes	IPv4 Addresses	ASes	IPv4 Prefixes	IPv4 Addresses	
1	3356	LEVEL3	Level 3 Communications	22,685	261,219	1,401,759,501	51%	57%	65%	3621
2	3549	LVLT-3549	Level 3 Communications	15,103	200,586	698,222,855	34%	44%	32%	3264
3	3257	TINET-BACK...	Tinet SpA	14,873	188,737	709,433,321	33%	41%	33%	942
4	174	COGENT-174	Cogent/PSI	13,594	147,701	589,730,708	30%	32%	27%	3855
5	1299	TELIANET	TeliaNet Global Network	12,722	160,514	616,234,216	28%	35%	28%	764
6	2914	NTT-COMMUN...	NTT America, Inc.	11,159	169,846	711,971,065	25%	37%	33%	888
7	6453	AS6453	TATA Communications	7,062	120,037	459,993,873	16%	26%	21%	580
8	701	UUNET	MCI Communications Services, Inc. d/b/a Verizon Business	5,402	96,864	738,082,126	12%	21%	34%	1693
9	6762	SEABONE-NET	TELECOM ITALIA SPARKLE S.p.A.	4,808	61,319	190,002,775	10%	13%	8.8%	284
10	2828	XO-AS15	XO Communications	4,118	80,165	353,394,094	9.3%	17%	16%	1047

data sources

geo	database	2013.03.02	netacquity	
organization	whois	0000.00.00	JPNIC, KRNIC, LACNIC	
		2012.06.29	AFRINIC, APNIC, ARIN, LACNIC, RIPE	
topology	BGP	2013.04.01, 2013.04.02, 2013.04.03, 2013.04.04, 2013.04.05	ripe	rrc00, rrc03, rrc04, rrc05, rrc06, rrc07, rrc10, rrc12, rrc13, rrc14, rrc15
			routeviews	eqix, isc, jinx, kixp, linx, routeviews2, saopaulo, sydney, telxatl, wide
	ITDK	2012.07.23	MIDAR IFF	



PoP-level map

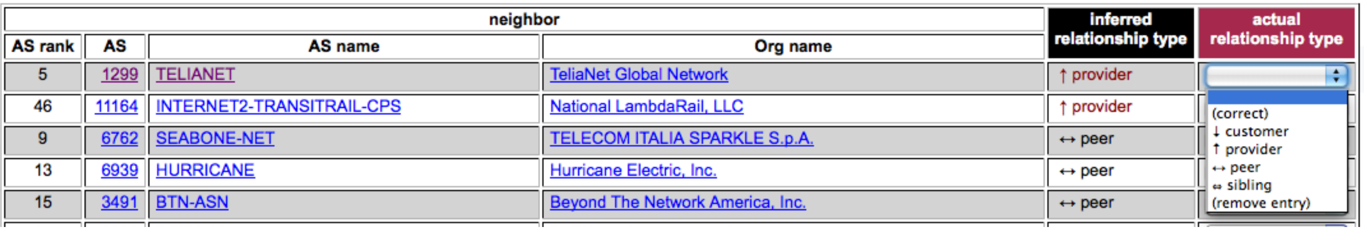


AS number:	174
AS name:	COGENT-174
Org name:	Cogent/PSI
AS rank:	4
Country:	US
Customer cone size:	13,594
AS transit degree:	3,855

0	1	65	3,789
Provider	Sibling	Peer	Customer

Router-level map

Operator feedback

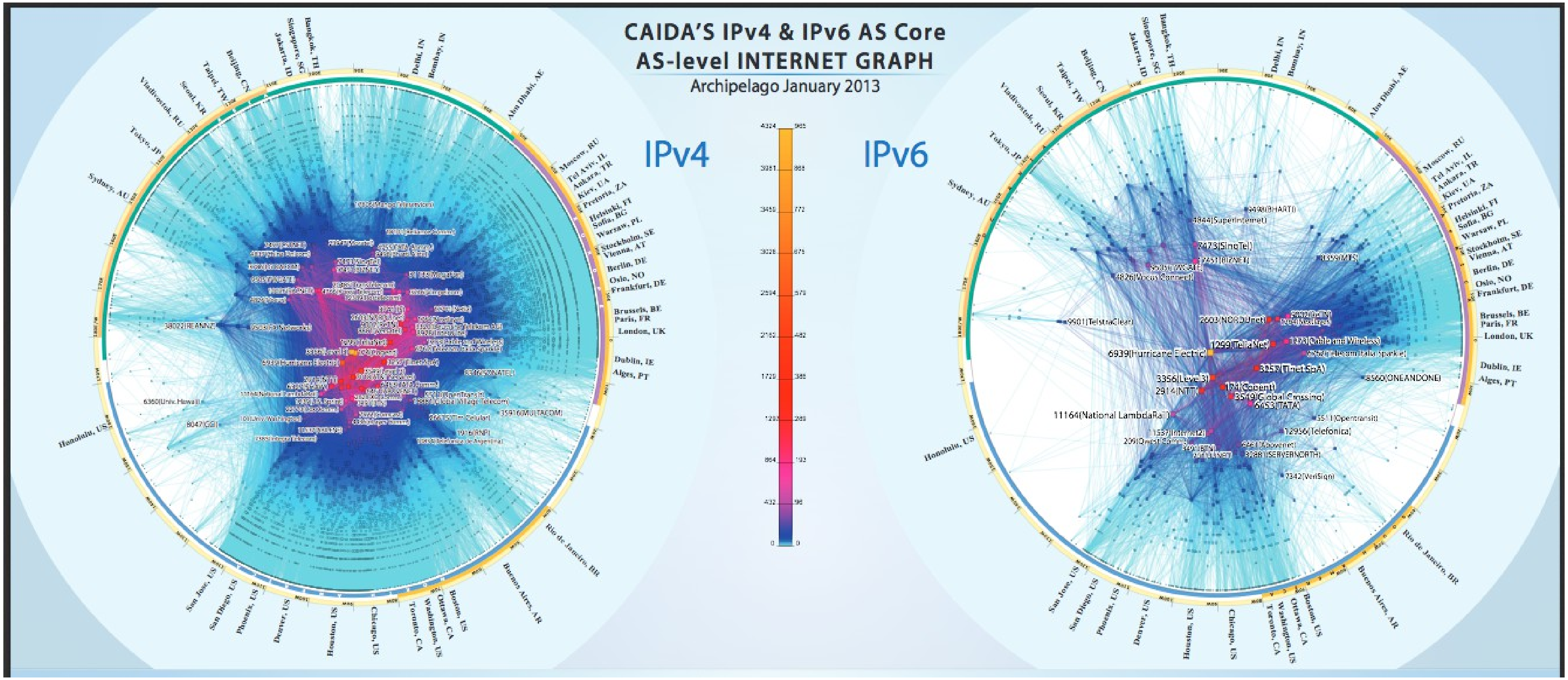


neighbor				inferred relationship type	actual relationship type
AS rank	AS	AS name	Org name		
5	1299	TELIANET	TeliaNet Global Network	↑ provider	
46	11164	INTERNET2-TRANSITRAIL-CPS	National LambdaRail, LLC	↑ provider	
9	6762	SEABONE-NET	TELECOM ITALIA SPARKLE S.p.A.	↔ peer	
13	6939	HURRICANE	Hurricane Electric, Inc.	↔ peer	
15	3491	BTN-ASN	Beyond The Network America, Inc.	↔ peer	

Improved Topology Maps

Task 3: Increase the richness of macroscopic Internet maps

AS Core network visualizations



Benefits

- Improved situational awareness of the Internet through:
  - Increased completeness
    - Increased measurement infrastructure
    - Expanded probing
    - Discovered method to synthesize better Internet topology
  - Increased accuracy
    - Filtered out false link inferences
    - Improved AS business relationships
  - Improved richness of topology maps
    - Better geographical locations
    - Dual maps, aliases resolved with :
      - MIDAR+iffinder – highest confidence aliases with low false positives
      - MIDAR+iffinder+kapar - increased coverage at cost of false positives
    - Increased connectivity at router-level
    - IP, router, PoP, and AS-level

Competition – Related Work

- (We tend to cooperate, complement, or create derivatives of related work rather than compete with it)

- RIPE Atlas (http://atlas.ripe.net/)
- iPlane (http://iplane.cs.washington.edu/data/data.html)
- DIMES (http://www.netdimes.org/new/)
- Renesys (http://www.renesys.com/)
- zMap (https://zmap.io/)

Current Status

- Deliverables
  - Monthly data collection (ongoing)
  - Evaluate experimental traceroute-based Internet topology (Mar 2014)
- Milestones
  - Activated 14 new Ark nodes
  - Evaluated scalable probing algorithms
  - Increased pool of IP addresses for alias resolution
  - Investigated the impact of false link inferences on the router-level, PoP-level, and AS-level graphs
- Schedule – near term
  - Deploy beta-version of interactive intermediate (PoP/city-level) map validation functionality for testing and feedback (Dec 2013)
  - Applied Research Phase through March 2014

Next Steps

- Based on the success of our tech transfer approach on a previous BAA (07-09), we plan to transfer an array of academic research related to homeland security challenges into a production resource of practical utility to DHS needs. We plan to:
  1) release two Internet Topology Data Kits per year;
  2) develop a user-friendly interactive visual interface to topology data and meta-data; and
  3) implement two on-demand topology measurement tools
     1) Topo-on-demand – CLI to Ark platform
     2) https://vela.caida.org/ web-based GUI to Ark platform

Contact Information

k claffy

kc@caida.org

http://www.caida.org/