## ICCC Internet Outage Detection & Analysis

http://www.caida.org/projects/ioda

<u>Alberto Dainotti</u>, kc claffy, Alistair King Vasco Asturiano, Karyn Benson, Marina Fomenkov, Brad Huffaker, Young Hyun, Ken Keys, Ryan Koga, Alex Ma, Chiara Orsini, Josh Polterock



Center for Applied Internet Data Analysis University of California, San Diego







UC San Diego

# IODA PROJECT

Started in Sep. 2012 with an NSF award from a program to *Transition to Practice* Cybersecurity research

#### Funding also provided by DHS S&T

• **Goal:** prototype an *operational capability* to monitor the Internet 24/7 to detect and analyze, in *near-realtime*, Internet blackouts affecting large networks / geographical areas

Project Website: <u>http://www.caida.org/projects/ioda</u>
Experimental service: <u>https://ioda.caida.org</u>





### BEFORE IODA

methodologies used for post-event manual analysis

 Country-level Internet Blackouts during the Arab Spring

> Dainotti et al. "Analysis of Country-wide Internet Outages Caused by Censorship" ACM Internet Measurement Conference 2011



EGYPT, JAN 2011 GOVERNMENT ORDERS TO SHUT DOWN THE INTERNET

## • Natural disasters affecting the infrastructure

Dainotti et al. "Extracting Benefit from Harm: Using Malware Pollution to Analyze the Impact of Political and Geophysical Events on the Internet" ACM SIGCOMM CCR 2012



Center for Applied Internet Data Analysis University of California San Diego



Japan, Mar 2011 Earthquake of Magnitude 9.0

### OUR METHODOLOGY combining various types of measurements

#### multiple types of sources for inference

- Routing Plane [BGP]
- Data Plane
  - Active probing
  - Passive traffic analysis [IBR]

• meta-data to extract liveness signals for various aggregations (e.g., countries, ASNs)

#### visualize and compare signals



BGP

**IBR** 

### IBR

### "Extracting benefit from harm."

• Use Internet Background Radiation (IBR), mostly generated by malware-infected hosts as a "signal"

INFECTED HOST Randomly Scanning The Internet

IBR

UCSD NETWORK TELESCOPE DARKNET XXX.0.0.0/8





Center for Applied Internet Data Analysis University of California San Diego



### BEFORE IODA

#### post-event manual analysis

4 months of work



Dainotti et al. "Analysis of Country-wide Internet Outages Caused by Censorship" ACM Internet Measurement Conference 2011



Center for Applied Internet Data Analysis University of California San Diego

#### Analysis of Country-wide Internet Outages Caused by Censorship

Alberto Daino ti Claudio Squarcet a Emile Aben Unversity si Napoli Posetori i Plana în: Unversity en 1992 NGC alberte@unina.it squarce@da.uniroma3.it emile.aben@ripe.net Kimbarty C, Clarty Marco Chiosa cADAUGSD Bena îno Jrikenety ke@caida org chiesa@da uniroma3.it Moheie Russo Antonio Pescapé Univesity of Napoli Federico II Unvesity of Napoli Federico II

#### ADJTRACT

In the first manhs of rapial in several Netti partexts and threats of a of these charaptions. In surplus on manipies of to academic resources data, association have p the material physics in an and MaxMind's protooats to determine the within each e-catry or est to BGF announced using publicity available rope. We then analyses performent discution control plane and data to names down which it phonented in a given p datasted what we belie based blocking before disconnection Our net direct outages errainilla

gaographic ortopologia

Categories and 5

C.2.) [Settork Operation] C.2.) [Local and Wide

General Terms

Monument Socialty

Personnine to make digitpresentation dominant menational and endiantibates for bear fluctuated like the test resultied, represents surver presentes under a forpresentes under a for-DICTL Networks 2-4, 2 Copyright 2011 ACM 978



related to protocks in the ensempty The work site of the Mexicup of Communications (see large any) two strated with a randomly provide LOS much gas here the comparation of nonzery 25 at different larges; 15.4° AOUTOP (formulas), 16.4° AOUTOP (for antic), and 11.06° AOUTOP (formulas), 16.4° AOUTOP (for antifer to be derived affects originates of the detectory of the stratetion of packet and , submaring are uppeaket attentions (fitant Mexicup).

and the proceeding of model. On Forenaux 1 the well state of the Egyptian Ministry of Interior (reconstricting) provide state provide the Hell state in the term for the state of the state of the term 1. The term Hell state in the 25 W of the 11 setter. The interior of address was attacked interpretime the flag of the from OSO for 64 S2 CMT. In this case the outmated state tracement and the model is positively proceeding.

#### 52 Libya

3.2.1 Convertee Ldogs's hierarchickness two is a superposed to available tion durality of a polytop from its dyna of two, and its match and connectivity is precised by only two substation cables, both anding in Trapic (19) works to be infrastructure in the duration of by a single, inter-encode, AC Wavely from these relates Alter heating many presence in Large, as its section of the Alter heating in the presence in Large, as its section of the Alter heating in Large, while the section of the Alter heating of the Large Alter Alteret stage. In Cody 2201 over heating in the presence in Large, as its section of the Alter heating.

In failparture different setages in only 2011 over identified and pathols between the (Figure 7) allower the testing interacting the CODE network theorym from Lings broughout in time will excompanying the energies. The pathol lebels is, B and Construct tree allowers disclosed spontees could be all 20 of the terms broaded service attacks discussed in Continue trees. It and 20 of the terms broaded service attacks discussed in Continue COA Toward the signet of the pathoese of the cost is an analy hap participle. Liberatorize of the cost is an

#### 3.2.2 Cutoges insite full

The formers or type loops of during two semiconics right. Figure 15() during a same detailed rine of during two stategies as desarroutly on USAD basespic rights, 10() strong the during sour the main interval in both cases, within a low minute. If our source is a strong right of the during rights are strong of the during the strong right of the during the during the during with another by cases within an interval of the during the contains [Poly profits are manyed by IrANS2 and Mary 2014]. Interview on First profits in *HeNIC* (whetpare) the for-Edoy. The Model and P profits in *HeNIC* (whetpare) the for-Edoy. The Model and P profits in *HeNIC* (whetpare) the for-Edoy. The Model and P profits in *HeNIC* (whetpare) the for-Edoy. The Model and P profits in *HeNIC* (whetpare) the forsion provide the strong profits in *HeNIC* (whetpare) the forle strong provide the strong profits in *HeNIC* (whetpare) the forle strong provide the strong profits in *HeNIC* (whetpare) the forle strong provide the strong profits in *HeNIC* (whetpare) the forhere the strong profits in *HeNIC* (whetpare) the forhere the strong profits in *HeNIC* (whetpare) the strong provide the forsion provide the strong profits in *HeNIC* (whetpare) the forhere the strong provide the st profit annumentality Suffall, which particles stabilises reviews in the Malife lists, Asia and Africa. The covering Det parts also considered 100: Pringer is several other constraints professionarily at the Warmin task. We constraine this maintenal As terms the UCML colored parently, described a significant material of tranbilised with covering, them the interval a significant material transmission of the several parently of the significant for the terms (them Steparstern and help). This lock of Taskayeousli ref. Its indicates a population one curveness same prior to travely conductions are observable and adviate influence of a states, conditions. Travels from this restantic also parathely excitence of advihopment to Edge advisors transmission for advisors of states, conditions. Travels from the total communities from the advisors of the hopment to Edge advisors to the sevents. Confidence to believe to that are filter addingend and the sevents.

Comparing function 1.3.46 and 1.3.00 reports a different between distant lists anti-posision service [17]: the second range the set caticly consoling BOP without diff. The BOP distants expansion Primary 19 result2130.13.0100, cateory matching the sharp forcersion distants halfsel from Linux during according with results are Linyan with over high Adver Merswers [21], that translet appendisantly one local tests, at 2004.22. In control appendionated years, been low, at 2004.22. In control of primary experiments and Edward discourse in which there is a suggest it that a Wavet discourse in which there is a solid-like intergy approvely adapted adapted to be interprint of a singly and acceptant of the interaction were it is not strain primary and dur-



Figure 11: The fractive Lieven concerns the associated radia to UCSD chains contain track they for children of Theor Bod produces in ACP devices Researching and BBC 2007 28 colleven. Now for the secondplane and decopless concerning of concerning the entropy of the sectematic second second second second second second second decomposition of the second second second second second second decomposition of the second second second second second second decomposition of the second second second second second second decomposition of the second second second second second second decomposition of the second second second second second second decomposition of the second second second second second second decomposition of the second second second second second second decomposition of the second second second second second second second decomposition second second second second second second second second second decomposition second se

### IODA GOALS

#### applied research





Center for Applied Internet Data Analysis University of California San Diego

## IODA CHALLENGES

Why this is a tough problem

- refine/extend inference methodologies
- automate inference methodologies
- complex data
- noisy data
- big data
- heterogeneous data
- velocity
- lack of tools
- distributed system
- •visualization for dashboards and data exploration
- lots of infrastructure to maintain/operate
- . . . .
- all with relatively few money/people/time..

#### high-level system view







|0|

#### high-level system view







### BGPSTREAM

#### efficient scalable processing of Internet routing data





### BGPSTREAM IN IODA

32 BGPCorsaro instances processing data from ~500 routers



#### high-level system view







#### high-level system view







#### high-level system view







#### high-level system view









#### high-level system view







#### high-level system view







### IODA SW SPIN OFFS

open-source frameworks of more general utility





### IODA DEMO





Center for Applied Internet Data Analysis University of California San Diego

## TALK/DEMO PURPOSE

feedback/interest

- Pre-release: use it!
- Collect feedback
- Add other data sources



### IODA FUTURE Ongoing work

- day-to-day maintenance to keep it online
- backfill of historical data
- sw/hw infrastructure updates
- more documentation

• make a kafka stream (we already have it. if you're interested) publicly available and share historical datasets through DHS IMPACT



## IODA FUTURE

#### Improvements

- More functionalities in web interface (e.g., add menu selectors of AS/ Country/region)
- Finer geo granularity
  - -Engineering + Research (e.g., improve prefix geolocation)
- Reduce latency (IBR, BGP, active probing)
- Improvements to IBR signals
  - -clean up
  - -detection
  - -systematically validate / evaluate IBR detection (we started at country level)
- IPv6 support



## ONGOING COLLABS

#### Academia, Industry, Government

#### **Collaboration with Industry**



We are collaborating with Comcast researchers, who are using IODA to support their own research on Internet reliability and performance. In addition, Comcast, through their Innovation Fund provided a research grant for the development of visual interfaces to monitor and characterize Internet outages.

cisco. <u>Cisco</u>

We established a collaboration with researchers at Cisco Systems, who are using BGPStream and are collaborating in extending it to support internal and open source projects carried out by Cisco, such as the OpenBMP implementation of the BGP Monitoring Protocol.

#### Public Safety



The Public Safety and Homeland Security Bureau (PSHSB) of the Federal Communications Commission (FCC) has the responsibility for ensuring that communications networks are reliable, resilient and secure. To accomplish this task, the PSHSB developed a data-driven process centered on collecting information on and performing analyses of communication outages. CAIDA had several meetings with the FCC to discuss results of the IODA project, providing the FCC with additional insight into the complexity of Internet outage monitoring and to discuss technology transfer of some of these research results and infrastructure capabilities.

#### Also, research collaborations with networking and poli-sci researchers



### IODA FUTURE Collabs

• Work with John to validate our ``Trinocular" implementation and maybe integrate his data source

- Work with Neil + Rama on combining the micro view with the macro view
- Add other data sources (Merit, VNG, ...)



### THANKS

### ioda.caida.org www.caida.org/projects/ioda

