Security Reputation Metrics for Hosting Providers

@CSET'15
10 Aug. 2015

TU Delft

Arman Noroozian, Maciej Korzcyński,
Samaneh Tajalizadehkhoob, Michel van Eeten

Reputation Metrics are Hard !

… to make and Interpret properly

Why Metrics ?

TU Delft

- The "Lemons Market" Problem
  - Information Asymmetry
- Consumer / Policy maker/ Law enforcement officer
  - Which provider is better/worse in security?
- The provider (intermediary) itself doesn't know either!
- Erodes incentives to invest in security

Hosting Providers

TU Delft

- Legitimate hosting provider types

Hosting Type	Hardware	Operating System	Software	Abuse Issues
Dedicated	Provider	Customer	Customer	Customer
Managed	Provider	Provider	Provider	Provider or Customer
Reseller	Provider or Customer	Customer or its Client	Customer or its Client	Customer or its Client
Shared	Provider	Provider	Provider	Provider and Customer
Unmanaged	Provider and Customer	Customer	Customer	Customer
Virtual Private Server	Provider	Provider	Customer	Customer

(M3AAWG, Anti-Abuse Best Common Practices for Hosting and Cloud Service Providers. Technical Report March 2015.)

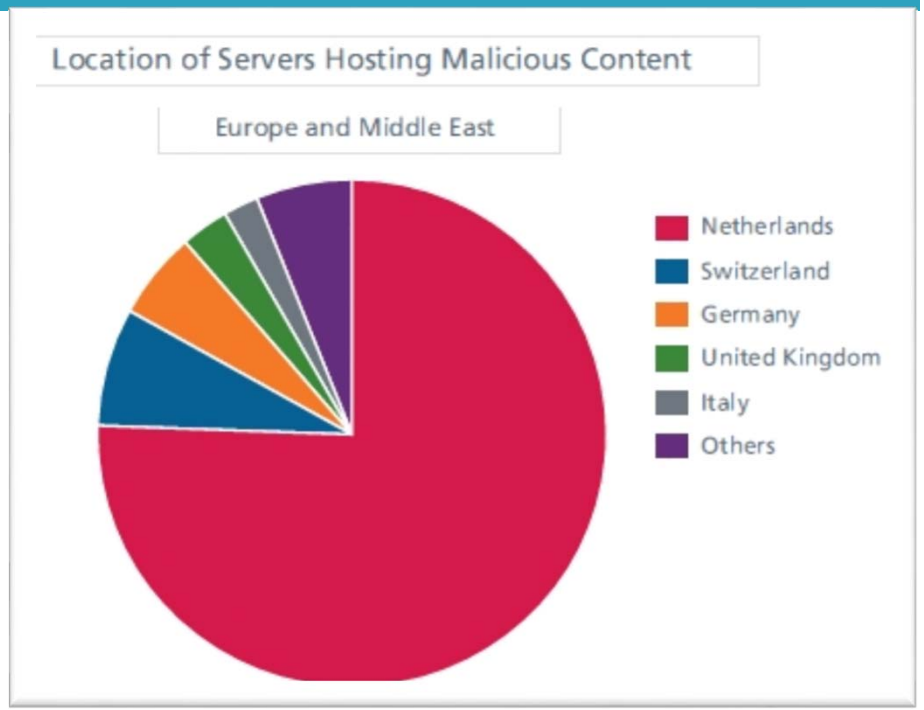
- Bulletproof Hosting!



Concentration of Abuse

TU Delft

- Attractive Pressure points
  - Remediation
  - Policy making



Source: McAfee Threats Report Q2 2012

Concentrations of Abuse (Cont.)

TU Delft

STOP BADWARE (SITES)	F.I.R.E. (COMPOSITE)	PHISHTANK	ZEUSTRACKER (TOP ZEUS C&Cs)	MALWARE DOMAIN LIST (JAN.1-TODAY
ThePlanet.com (AS21844)	ThePlanet.com (AS21844)	NJ INTL INTERNET EXCHANGE (AS16812)	JINGXUN (AS9803)	ThePlanet.com (AS21844)
CHINANET BACKBONE (AS14035)	PAH Inc GoDaddy.com (AS26496)	MetroRED Telecom Services (AS13591)	HANARO Telecom (AS9318)	OVH - OVH (AS16276)
PAH Inc GoDaddy.com (AS26496)	OVH - OVH (AS16276)	RAPIDSWITCH-AS (AS29131)	TTNET (AS9121)	DXTNET BEIJING (AS17964)
N/A	BLUEHOST-AS (AS11798)	CENTROHOST-AS (AS41126)	GR-Vertical Ltd (AS49365)	VEST-EH (AS47560)
eNom Inc. (AS6151)	IPNAP- GigeNET (AS23522)	ThePlanet.com (AS21844)	CHINANET BACKBONE (AS14035)	TTNET (AS9121)
Google Inc. (AS15169)	EcomD-Coloquest/GigeNet (AS32181)	iWeb Technologies Inc. (AS32613)	ThePlanet.com (AS21844)	DIRECT-NET2 - Data Tex (AS4229)
Softlayer Technologies (AS36351)	GNAXNET - Global Net Access (AS3595)	Softlayer Technologies (AS36351)	Network Operations Center (AS21788)	Prombuddetal (AS44107)
Cogent Co/PSI (AS174)	iWeb Technologies Inc (AS32613)	OVH - OVH (AS16276)	CNCNet China Netcom (AS9929)	Chugye-AS-KR (AS23971)
TONET Beijing (AS17431)	Softlayer Technologies (AS36351)	Limestone Networks Inc (AS46475)	Interactive3D (AS49544)	Vital Vital Teknoloji (AS44565)
American Internet Svcs (AS6130)	Bizland-SD - Endurance Intl (AS29873)	SOVAM-AS Golden Telecom (AS3216)	Vital Vital Teknoloji (AS44565)	CHINA TELECOM (AS4134)
<<------->>	<<------->>	<<------->>	<<------->>	<<------->>
ARBOR TOP ASN THREATS	**EMERGING THREATS COMPROMISED IPS**	**EMERGING THREATS RBN**	**SHADOWSERVER (BOT C&CS)**	**GOOGLE SAFEBROWSING**
NJ INTL INTERNET XCHANGE (AS16812)	CHINA TELECOM (AS4134)	Softlayer Technologies (AS36351)	net-0x2a-ukraine (AS48587)	ThePlanet.com (AS21844)
CNIX -AP (AS4847)	Korea Telecom (AS4766)	ThePlanet.com (AS21844)	Ecatel Network (AS29073)	CHINANET BACKBONE (AS14035)
CHINANET BACKBONE (AS14035)	Deutsche Telekom (AS3320)	CHINA TELECOM (AS4134)	Webalta Networks (AS41947)	PAH Inc GoDaddy.com (AS26496)
ThePlanet.com (AS21844)	SBC Internet Services (AS7132)	NETDIRECT-DE (AS28753)	EZZI (AS15149)	Softlayer Technologies (AS36351)
OVH - OVH (AS16276)	PROXAD Free SAS (AS12322)	Hivelocity Ventures Corp (AS29802)	Network Operations Center (AS21788)	MESH GmbH (AS25074)
COLUMBUS-NAP (AS10297)	Telecom Sao Paolo (AS27699)	Leaseweb (AS16265)	CHINA TELECOM (AS4134)	HETZNER ONLINE (AS24940)
Softlayer Technologies (AS36351)	China Network Comm. (AS4837)	HETZNER ONLINE (AS24940)	Interactive3D (AS49544)	VPLS INC (AS35908)
Interiapl (AS16138)	HANARO Telecom (AS9318)	NJIX (AS19318)	SBC Internet Services (AS7132)	Ecatel Network (AS29073)
HINET (AS3462)	National Internet Backbone (AS9829)	Layered Tech (AS22576)	Leaseweb (AS16265)	1&1 Internet AG (AS8560)
AMAZON (AS14618)	CHINANET-BJ-AS-169 (AS4808)	OVH - OVH (AS16276)	Korea Telecom (AS4766)	root eSolutions (AS5577)

Source: http://krebsonsecurity.com/2010/03/naming-and-shaming-bad-isps/

Hoster Size Matters

Top 50 Hosts

A list of the 50 ASes with the highest HE Indexes i.e. the highest observed concentrations of malicious activity.

Autonomous System (AS)
A logical collection of Internet routes, controlled by an organization or ISP.

ASN
Unique number assigned to the AS.

HE Index
HostExploit's quantitative metric, representing the concentration of malicious activity served from an Autonomous System.

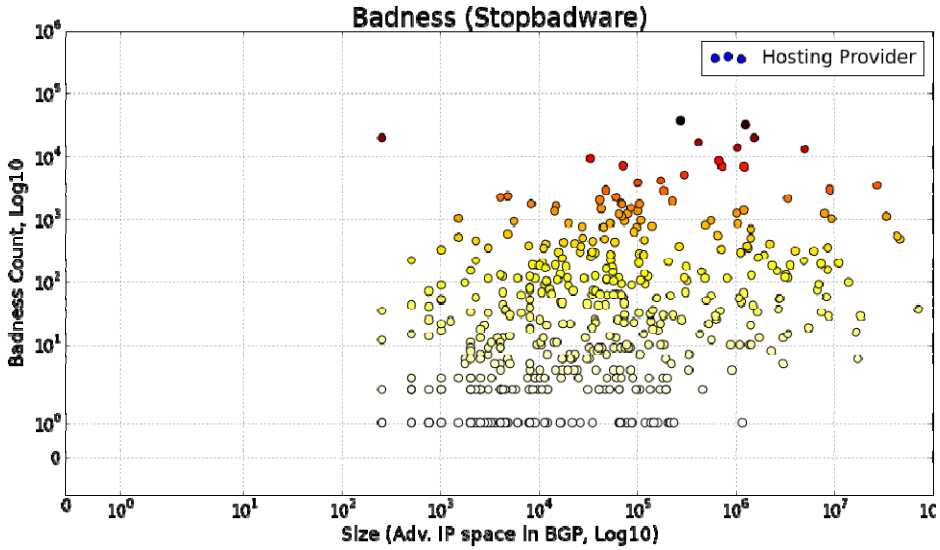
HE Rank	HE Index	ASN	Name	Country	IPs
1	291.22	11042	Landis Holdings Inc	US	28,416
2	289.08	26347	New Dream Network, LLC	US	156,928
3	248.71	33182	HostDime.com, Inc.	US	78,848
4	245.64	31034	Aruba S.p.A.	IT	145,664
5	242.00	29182	ISPsystem	RU	44,544
6	239.48	47583	Hostinger International	US	13,568
7	219.72	13335	CloudFlare, Inc.	US	258,560
8	211.48	12824	home.pl	PL	204,800
9	191.78	25532	Masterhost	RU	77,824
10	191.71	26496	GoDaddy.com, LLC	US	1,768,192
11	187.04	8560	1&1 Internet AG	DE	372,224
12	182.24	16276	OVH Systems	FR	1,079,552
13	180.30	34619	Cizgi Telekomunikasyon	TR	30,208
14	179.01	25504	Vautron Rechenzentrum AG	DE	22,784
15	169.96	46606	Unified Layer	US	648,960
16	168.71	27823	Dattatec.com	AR	12,288
17	166.51	38955	World4You Internet Services	AT	6,400
18	163.94	16265	LeaseWeb B.V.	NL	397,824
19	162.89	29073	Ecatel Network	NL	12,800
20	161.04	40034	Confluence Networks Inc	VG	16,128
21	161.00	48159	Telecommunication Infrastructure	IR	385,728
22	160.02	24940	Hetzner Online AG	DE	705,280
23	159.48	43146	Agava Ltd.	RU	20,736

Source: http://hostexploit.com/downloads/world_hosts_report_201403.pdf

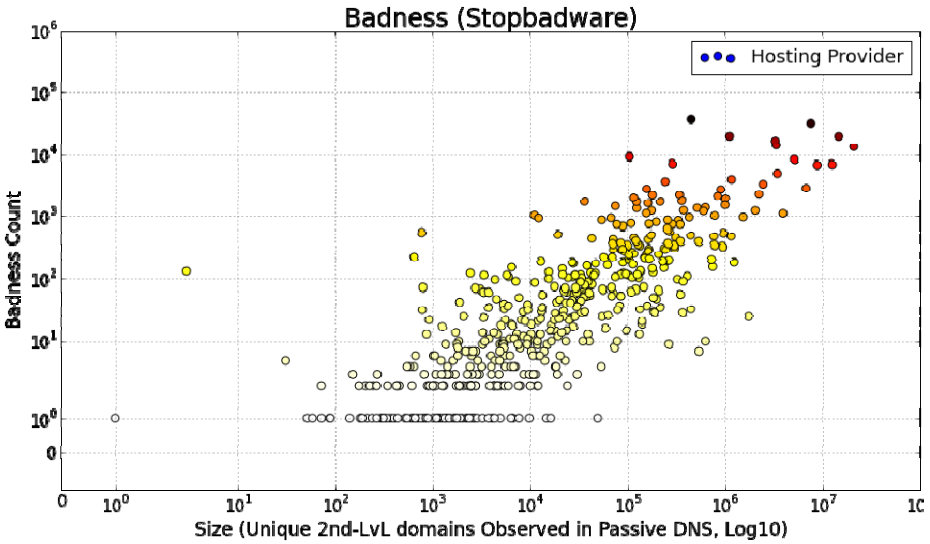
Measures of Size

TUDelft

Advertised IP Space



Hosted 2nd level domains



Indicators of Abuse

TU Delft

Indicators	Why	Challenge
Occurrence of Abuse (How often abused?)	*Signals network hygiene and vulnerability*	*Hard to isolate provider efforts from other factors*
Uptime of abuse (How long abused?)	*Signals effectiveness of abuse handing*	*Hard to measure at scale*

Sensitivity of Metrics

TU Delft

- Choice of abuse data
- Biases and errors in abuse data
- Errors in mapping abuse data
- Biases and errors in size estimation data

TU Delft

A Dutch Case Study

Dutch Police:

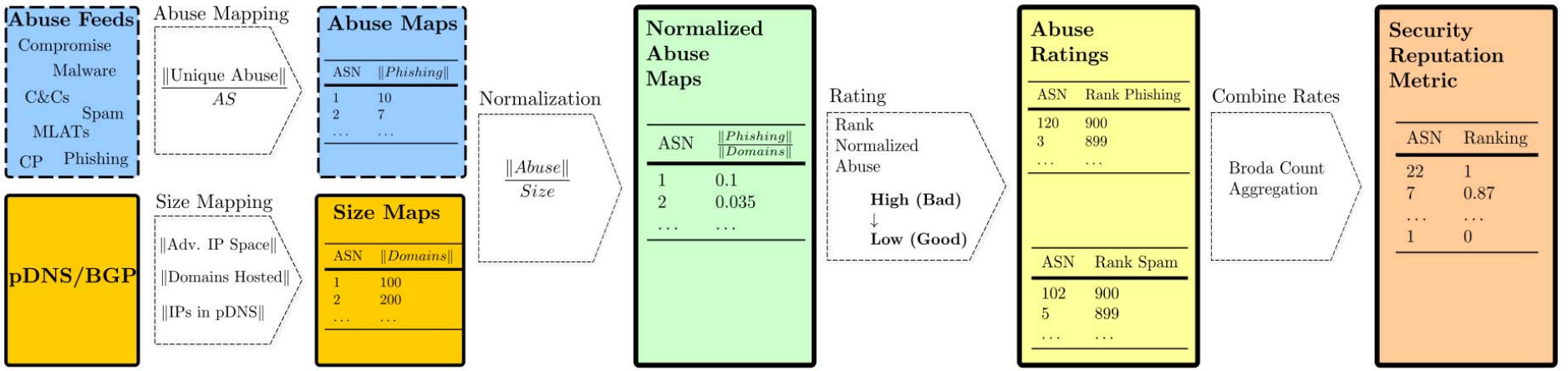
"Who are the worst hosting providers in our jurisdiction?"

Data Sources

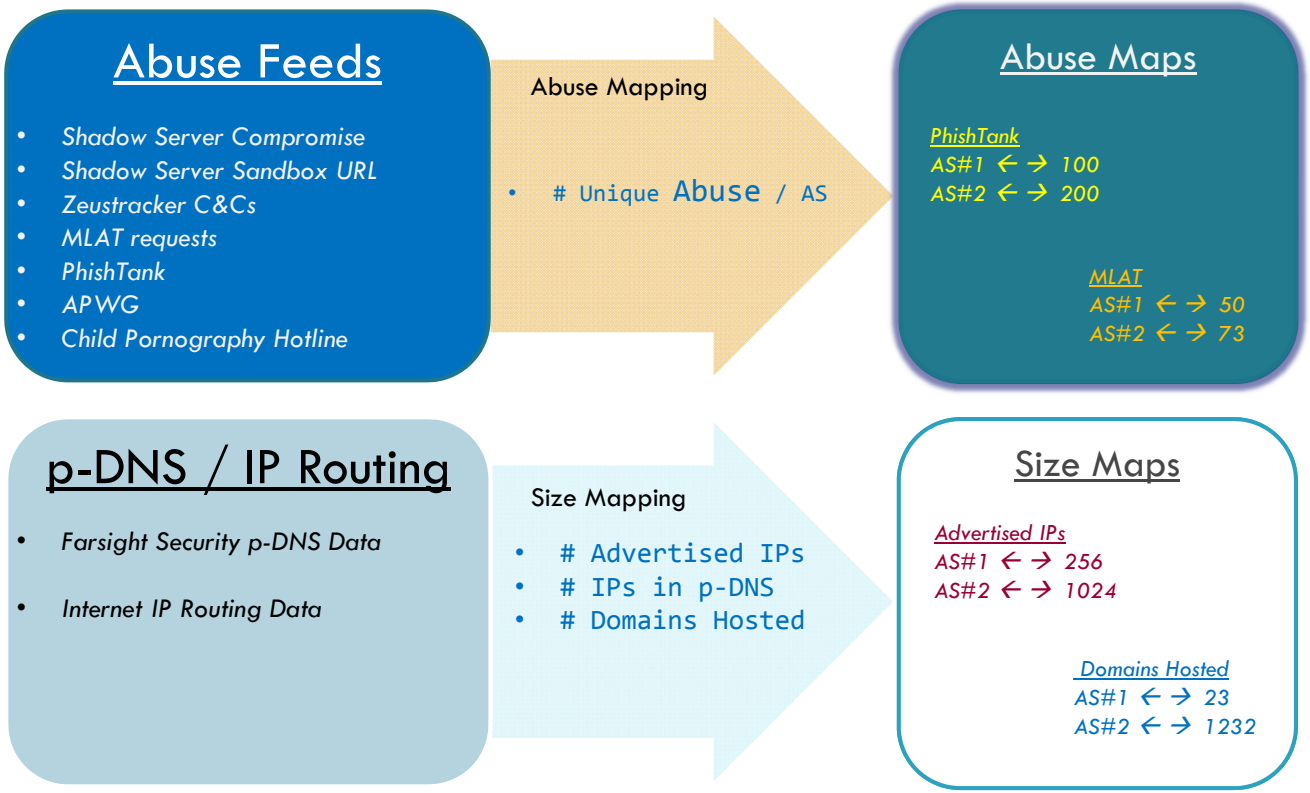
TU Delft

- Abuse
  - StopBadware
  - Shadowserver
    - Compromised servers
    - Outbound malware connections
  - Zeustracker C&Cs (Abuse.ch)
  - Mutual Legal Assistance Treaty (MLAT) requests
  - Dutch child pornography hotline
  - Phishtank
  - Anti-Phishing Working Group
- IP Routing Data
  - Python pyasn library
- Passive DNS (pDNS)
  - DNSDB from Farsight Security
  - 750 million unique 2LDs
  - 93 million unique IPv4 Addresses

Our Methodology

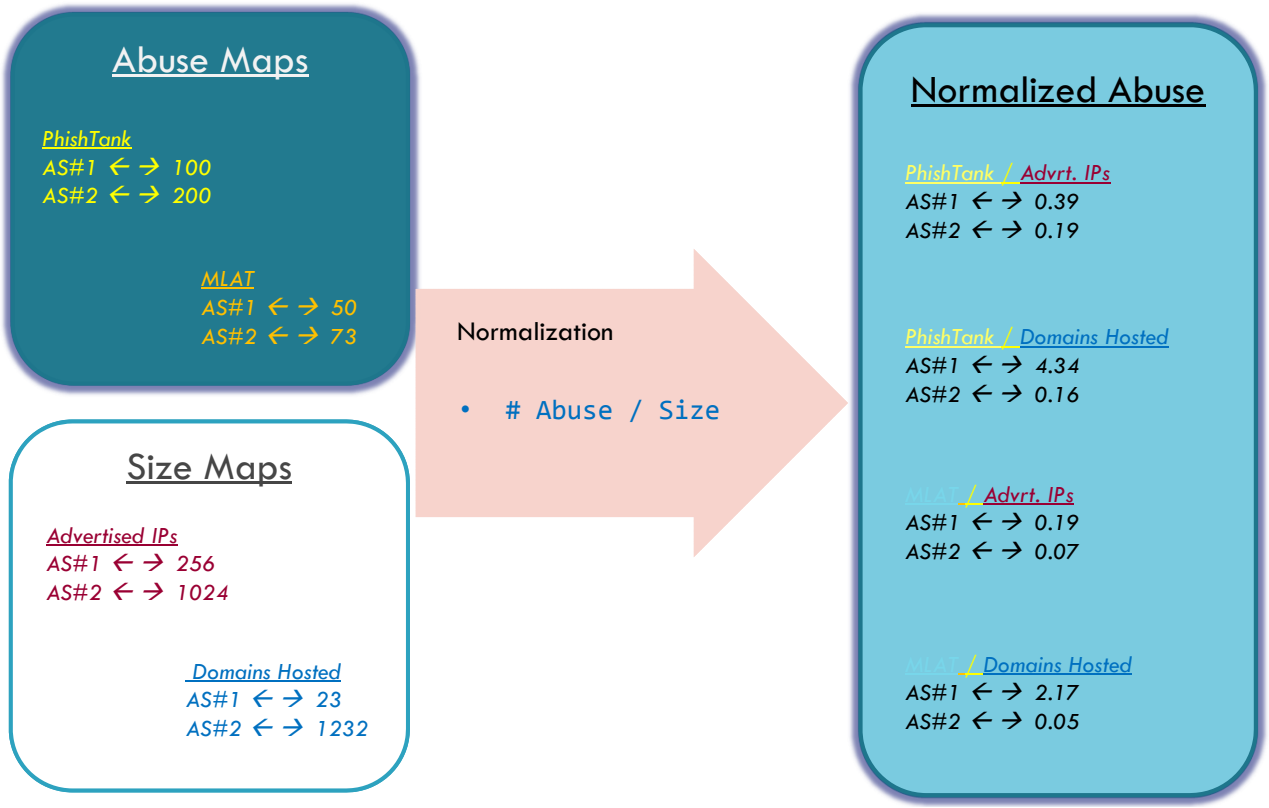


Step 1+2: Mapping



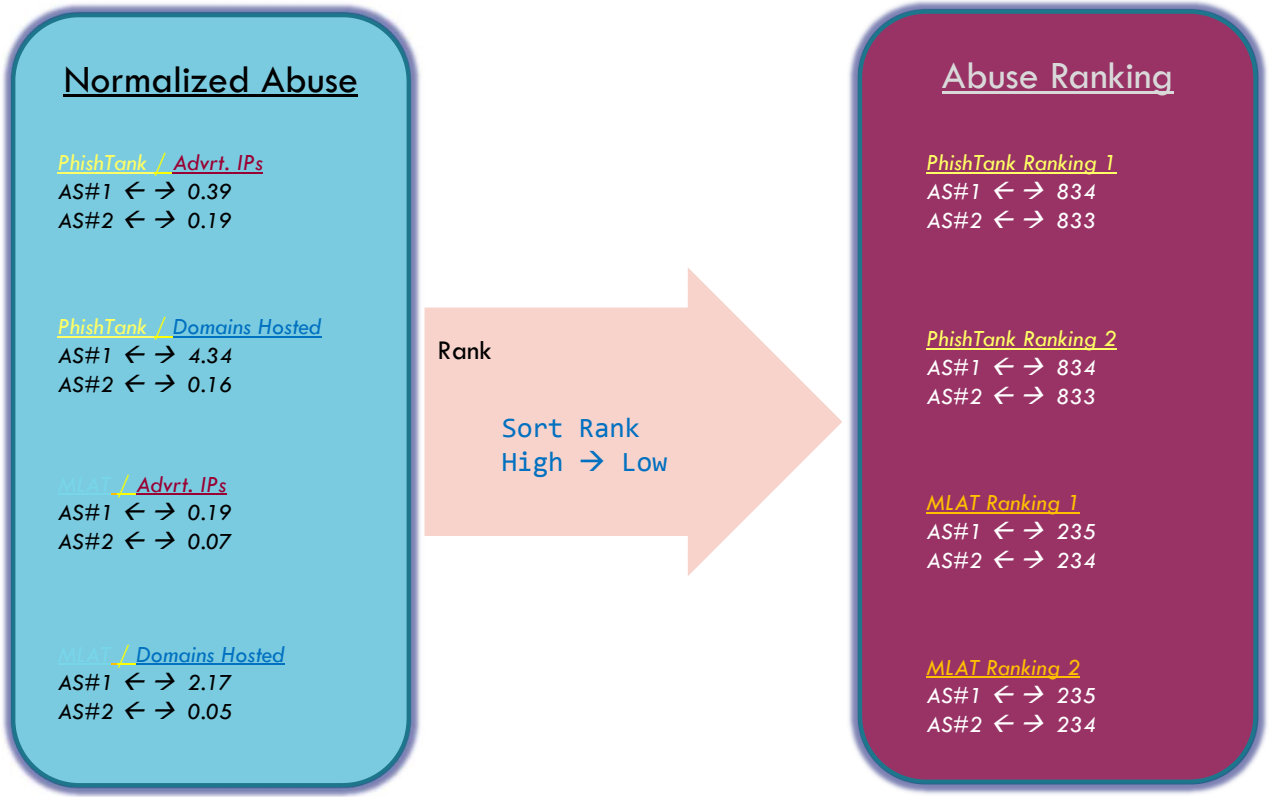
Step 3: Normalization

TU Delft



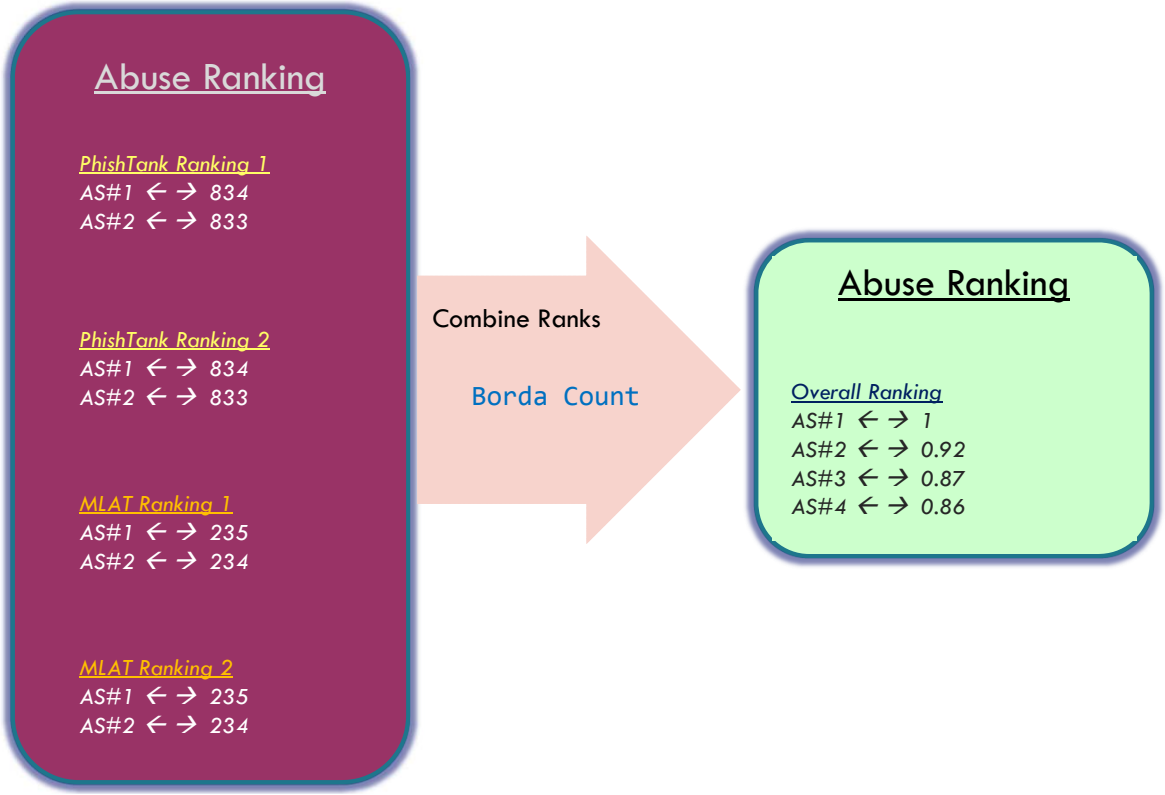
Step 4: Ranking

TU Delft



Step 5: Aggregation

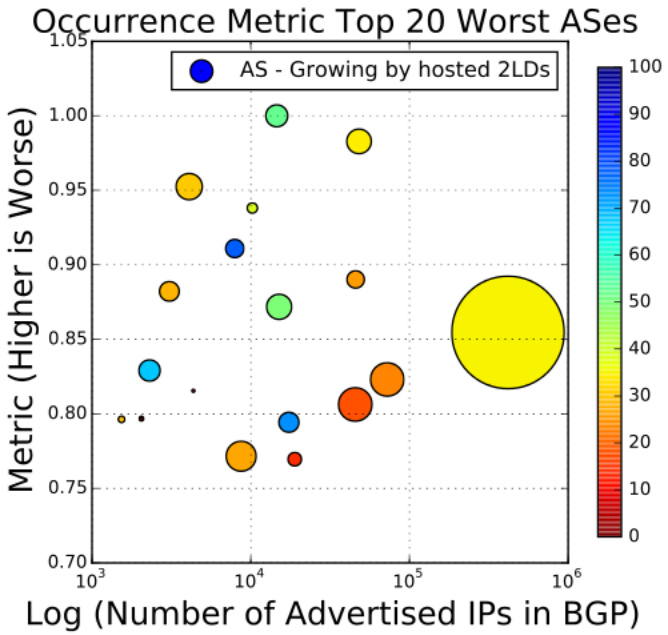
TU Delft



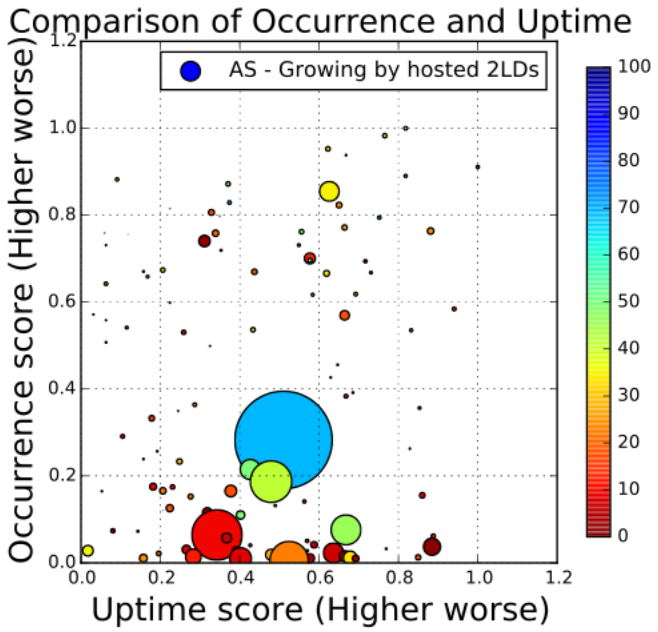
Security Reputation Metrics

TU Delft

20 worst Dutch hosting providers



Abuse Rate vs Cleanup Rate



Abuse Metrics are Hard

TU Delft

- How to measure abuse and remediation
  - What abuse can be observed
  - What does it tell us about remediation efforts
- How to associate it with hosting providers
  - What is a hosting provider
  - How to identify them at scale
- How to control for differences among providers and interpret metric(s)
  - How to take size into account
  - How to take different business models into account
- How to aggregate indicators into a comprehensive metric (set of metrics) ?

Towards better metrics

TU Delft

- How to measure abuse and remediation
  - Increase coverage, add different global abuse feeds
  - Add uptime data (e.g. phishing)
- How to associate it with hosting providers
  - Identify hosting providers from IP ownership data (WHOIS) instead of AS-level routing data (BGP)
- How to control for differences among providers and interpret metric(s)
  - Extract 'profiles' from pDNS data (size, shared hosting, dedicated, non-webdomain)
- How to aggregate indicators into a comprehensive metric (set of metrics) ?
  - More sensitivity analysis of aggregation methods

Thank you for attention

Questions?