Towards Network Reputation - Analyzing the Makeup of RBLs

Manish Karir, Kyle Creyts, Nathan Mentley
Research and Development
Merit Network Inc.

Outline

- Introduction and Motivation
- Architecture
- Key Components
- Uses of network reputation
- Some initial results
- Conclusions

The Problems

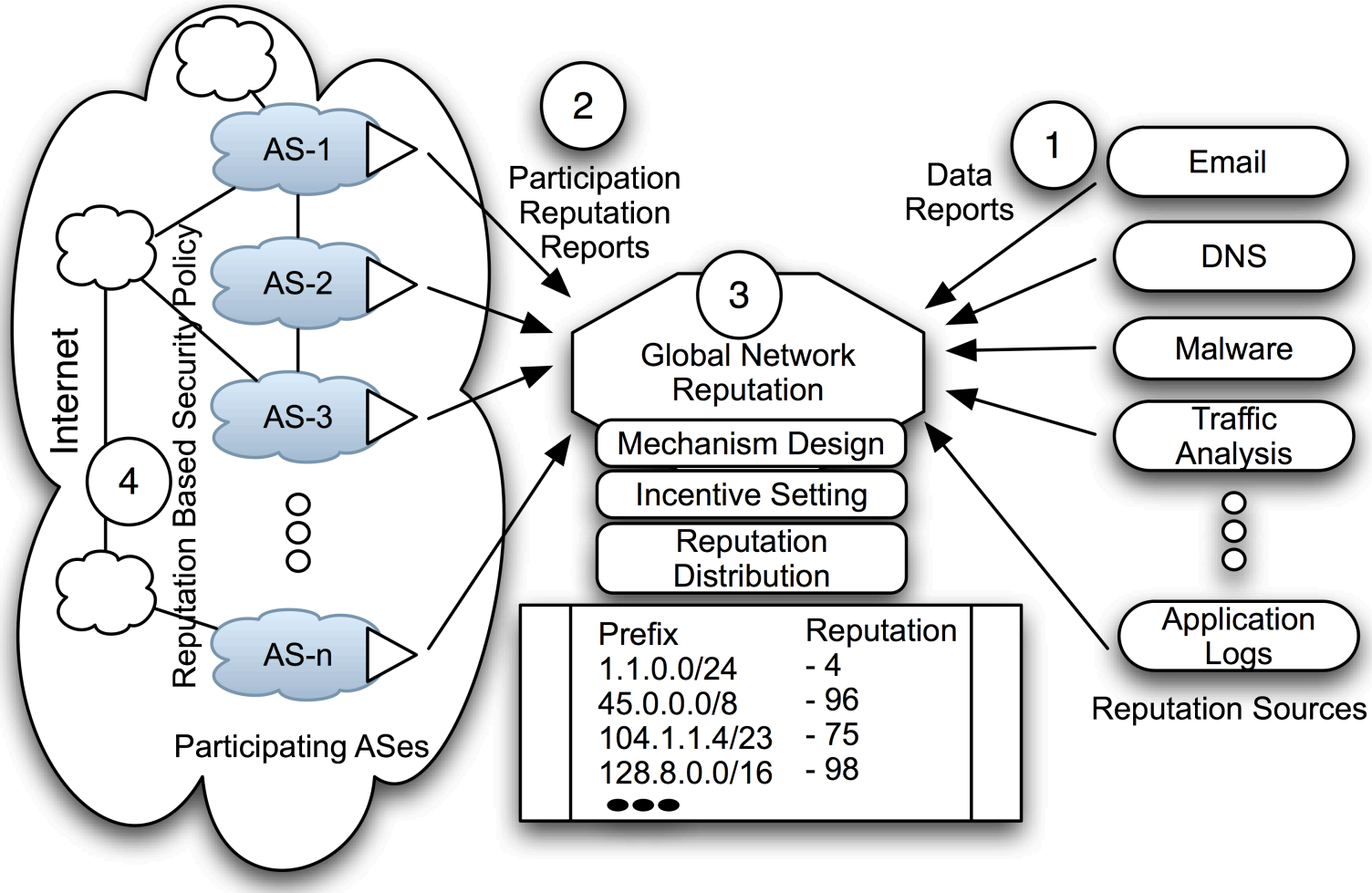
- How do you create incentives for the need to run a clean network
- How do you measure the relative security posture of a given network
- How do you balance the need to communicate with another network with the risks
- How can you estimate the likely hood of malicious activity from another network
- Can you assign a risk metric with a BGP path

➢ *You need to know about the historical and current reputation of networks*

Desired Properties of a Network Reputation System

- Must take into account a wide variety of network data sources (BGP, DNS, Email etc)
- Must be both passive as well as allow for community participation (must NOT allow a person or small groups to collude)
  - Must include both global and local data sources
  - Must create incentives for people to participate and provide local perspectives on network reputation
- Reputation generation must NOT be responsibility of a single entity or single data source
- Must allow operators to merge global reputation with their own local biases before use in a security policy

Architecture



Key Components

1: External Reputation Reports

2: Participation Reports

3: Global Network Reputation System

- Incentive Setting
- Data synthesis and weighting
- Reputation Distribution

4: Security policies based on network reputation

1: External Participation Reports

- Derived from “third-party” data sources such as spam reputation, dns reputation, botnet reputation sources, darknet scanners
- Generally published globally by neutral third parties not generally related with either the host being reported on or the party that is a potential user of this information
- We have lots of *host* reputation information of this type. We can use that to derive and seed network reputation fairly easily

2: Participation Reputation Reports

- Many forms of potential reputation data is not visible at the global level – e.g ssh brute force attacks at an enterprise, www brute force attacks visible in local logs
- Self reporting of suspicious activity originating from various customer blocks
- Reporting on local reputation views of specific networks if requested by overall system

3: Global Reputation Example

Prefix	Reputation Index	TimeStamp	Data Sources
1.1.0.0/16	30	2011-02-13:21:45:22	Scan,Darknet
192.168.5.0/24	92	2011-02-14:11:23:12	Botnet,SPAM
12.5.1.0/24	98	2011-02-21:10:45:12	DNS,Malware
206.142.0.0/14	75	2011-02-13:21:45:22	SSH, Darknet
...	...	...	...

- Aggregate and weight different sources of input based on relative confidence in both data type and the reporting party
- Publish consolidated reputation index in a variety of ways, BGP, xml, rss, etc.

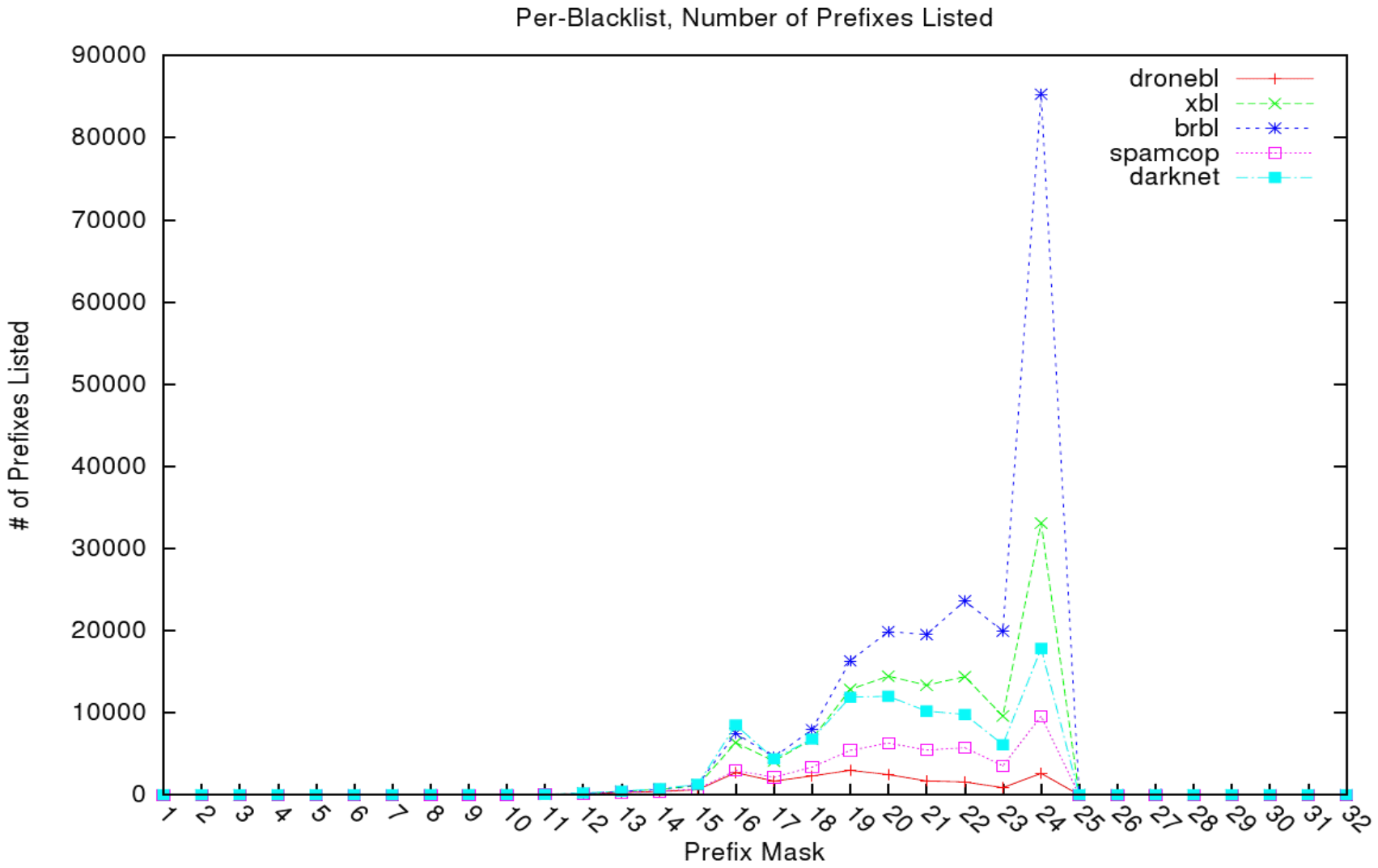
4: Reputation based security policies

- Some Interesting possibilities:
  - BGP – For each path compute the relative reputation over entire path or the lowest hop AS in any path and influence policy to avoid that path
  - SPAM Scoring – use reputation of source in scoring, but more interestingly – bypass other checks if reputation is > 95
  - Inbound Firewall – Allow all traffic to regular servers from sources with reputation > 10 but for reputation < 10 send traffic to alternate servers or services, require additional authentication etc
  - Outbound traffic – disallow traffic to networks with poor reputation
  - Making DPI viable/scalable for more people – normally route traffic for reputation > 30 but for poor reputation sources pass traffic through DPI for further inspection

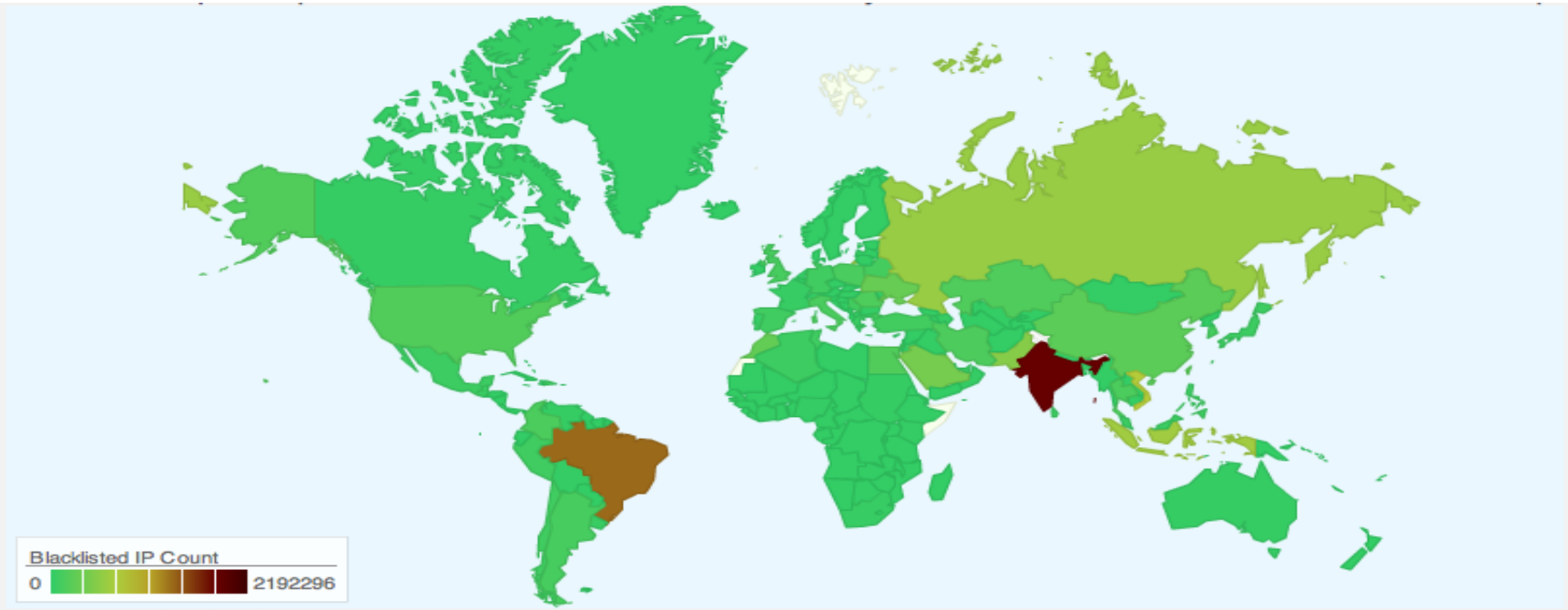
RBL Characterization

RBL	Data Type	Size (# of IPs)
BRBL	SPAM	100M
XBL	SPAM	7.5M
SpamCop	SPAM	290K
Cymru	CC	243
Shadow	CC	1600
DrkScan	Scanner	170K
BruteForce SSH	Application	65K
DroneBL	Misc	40K

RBLs by Prefix



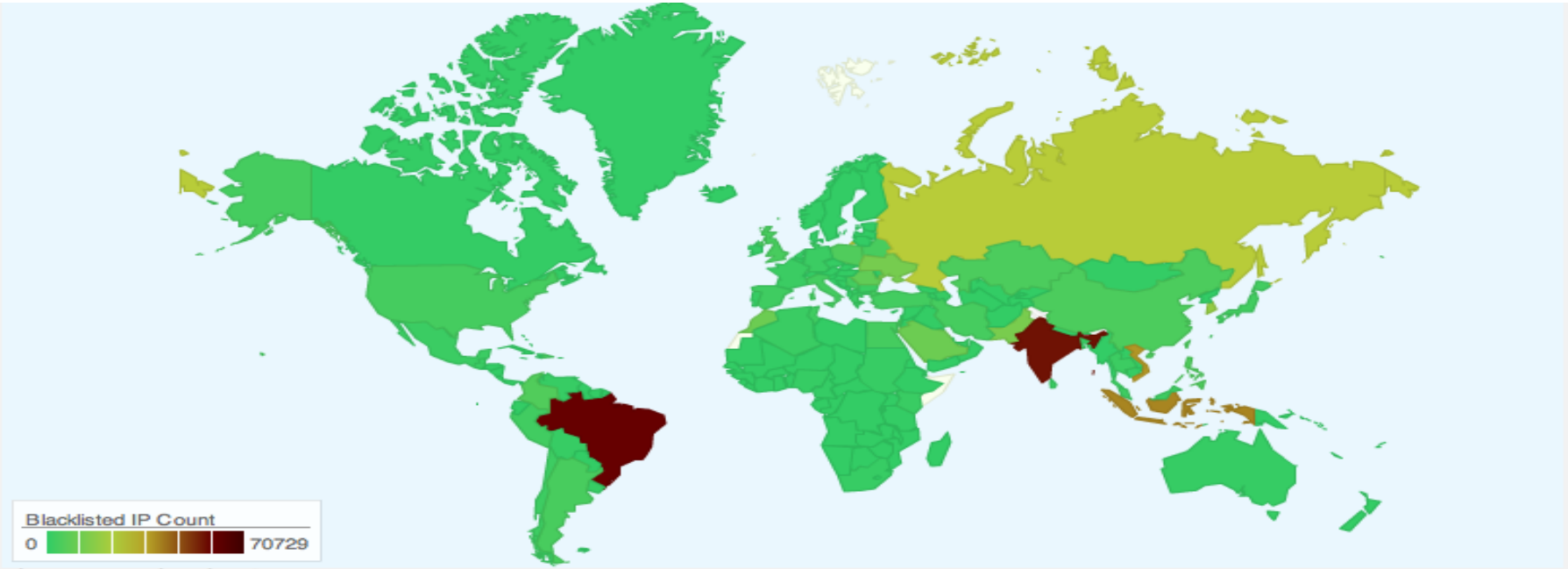
What is in RBLs - XBL



view as a pie chart

	Country Code	Blacklisted IP Count	% of Listed IPs	Country Name
1	IN	2192296	10.40	INDIA
2	BR	1623824	7.70	BRAZIL
3	VN	937838	4.45	VIET NAM
4	ID	794023	3.77	INDONESIA
5	RU	723802	3.43	RUSSIAN FEDERATION
6	PK	602453	2.86	PAKISTAN
7	SA	482391	2.29	SAUDI ARABIA
8	UA	379548	1.80	UKRAINE
9	MA	346907	1.65	MOROCCO
10	CN	290420	1.38	CHINA

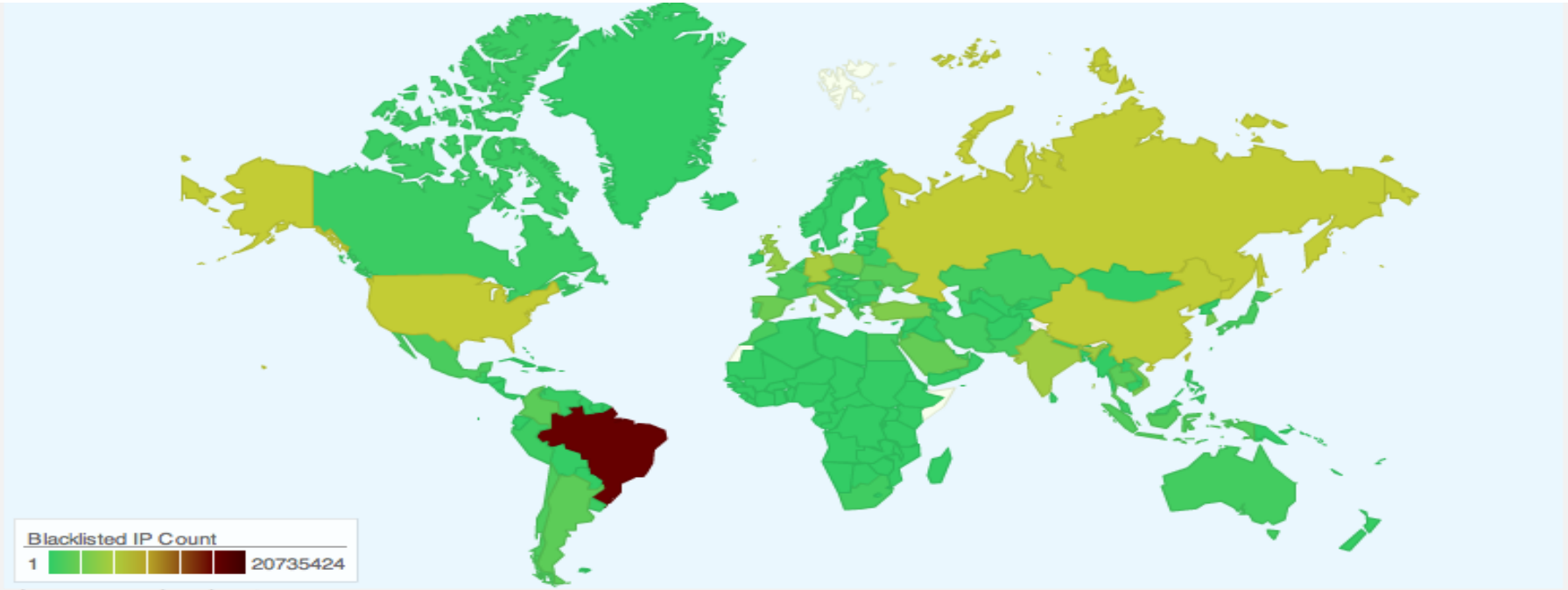
What is in RBLs - SpamCop



view as a pie chart

	Country Code	Blacklisted IP Count	% of Listed IPs	Country Name
1	BR	70729	8.66	BRAZIL
2	IN	67542	8.27	INDIA
3	ID	47500	5.81	INDONESIA
4	VN	44611	5.46	VIET NAM
5	RU	30937	3.79	RUSSIAN FEDERATION
6	KR	22831	2.79	KOREA REPUBLIC OF
7	PK	16185	1.98	PAKISTAN
8	UA	15693	1.92	UKRAINE
9	SA	13294	1.63	SAUDI ARABIA
10	MA	13209	1.62	MOROCCO

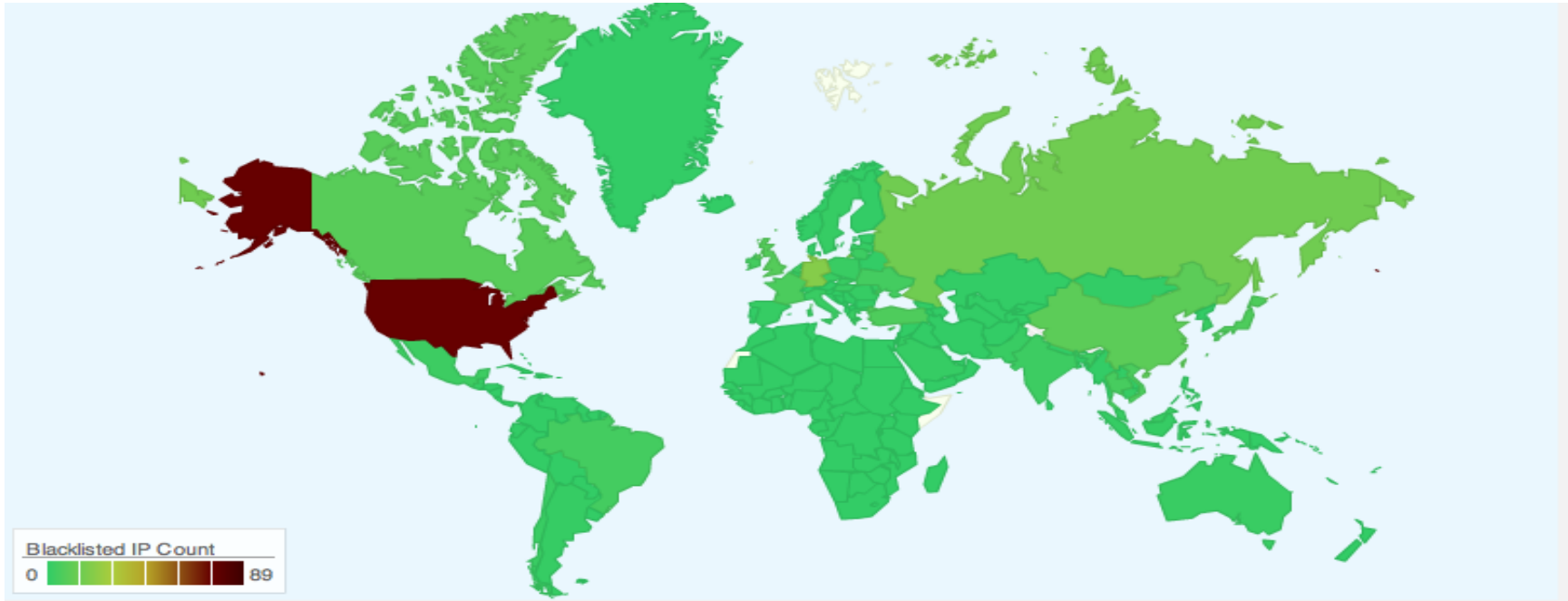
What is in RBLs - BRBL



view as a pie chart

	Country Code	Blacklisted IP Count	% of Listed IPs	Country Name
1	BR	20735424	7.73	BRAZIL
2	US	9794242	3.65	UNITED STATES
3	RU	9643239	3.60	RUSSIAN FEDERATION
4	CN	9552575	3.56	CHINA
5	DE	8080633	3.01	GERMANY
6	IN	7397899	2.76	INDIA
7	GB	6535633	2.44	UNITED KINGDOM
8	IT	5872867	2.19	ITALY
9	TR	5244777	1.96	TURKEY
10	VN	4603300	1.72	VIET NAM

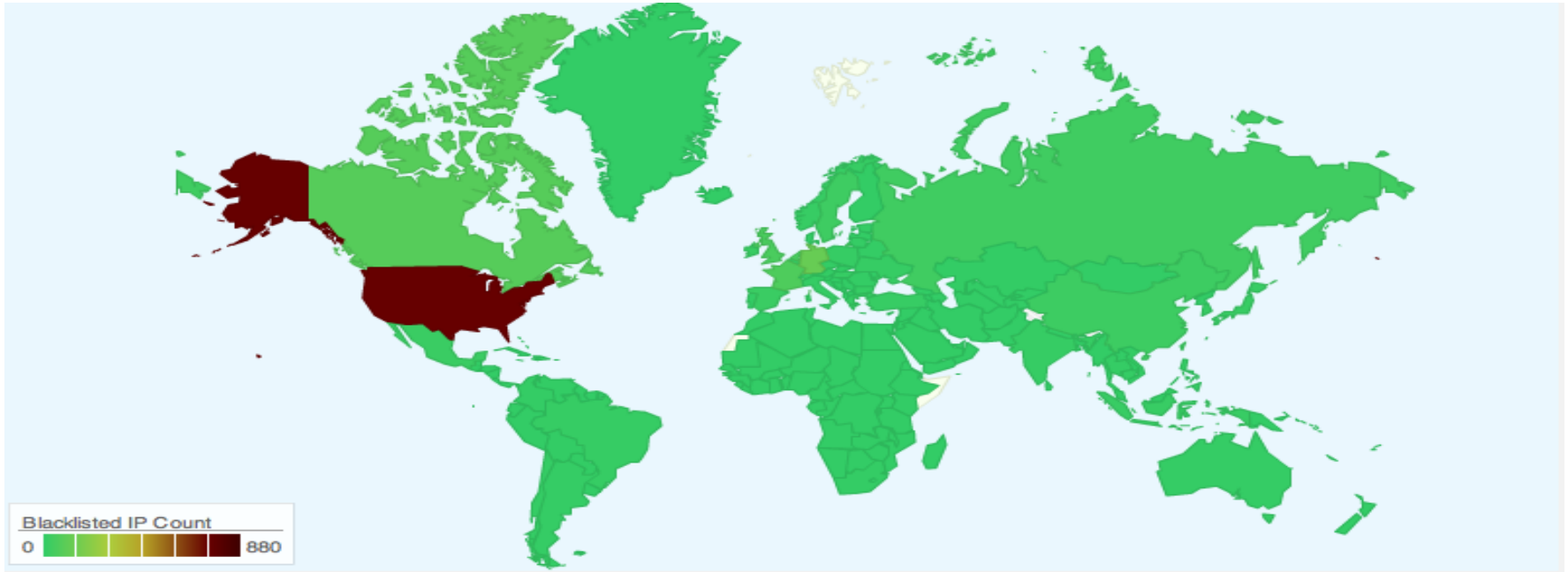
What is in RBLs - cymru



view as a pie chart

	Country Code	Blacklisted IP Count	% of Listed IPs	Country Name
1	US	89	16.67	UNITED STATES
2	DE	24	4.49	GERMANY
3	RU	18	3.37	RUSSIAN FEDERATION
4	CN	12	2.25	CHINA
5	CA	11	2.06	CANADA
6	GB	10	1.87	UNITED KINGDOM
7	HK	9	1.69	HONG KONG
8	TR	8	1.50	TURKEY
9	JP	8	1.50	JAPAN
10	FR	7	1.31	FRANCE

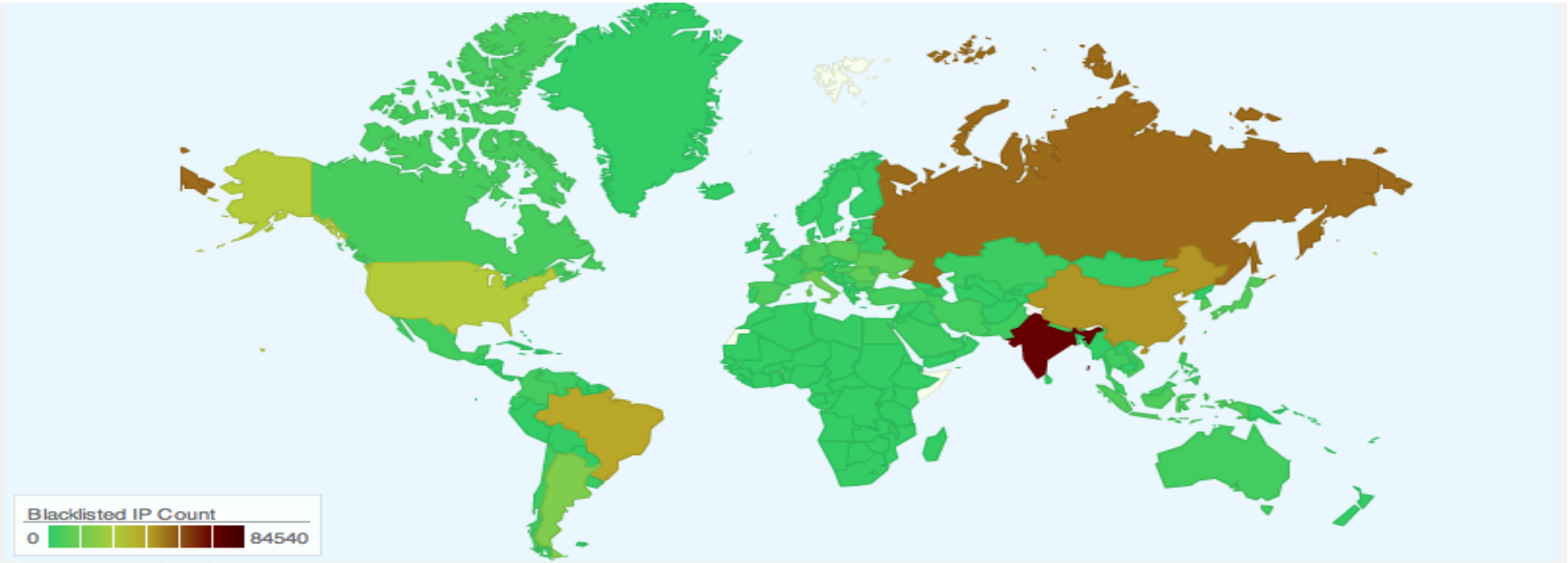
What is in RBLs - ShadowServer



view as a pie chart

	Country Code	Blacklisted IP Count	% of Listed IPs	Country Name
1	US	880	25.49	UNITED STATES
2	DE	151	4.37	GERMANY
3	CA	102	2.95	CANADA
4	FR	78	2.26	FRANCE
5	GB	69	2.00	UNITED KINGDOM
6	NL	66	1.91	NETHERLANDS
7	RU	40	1.16	RUSSIAN FEDERATION
8	SE	34	0.98	SWEDEN
9	CN	29	0.84	CHINA
10	ES	22	0.64	SPAIN

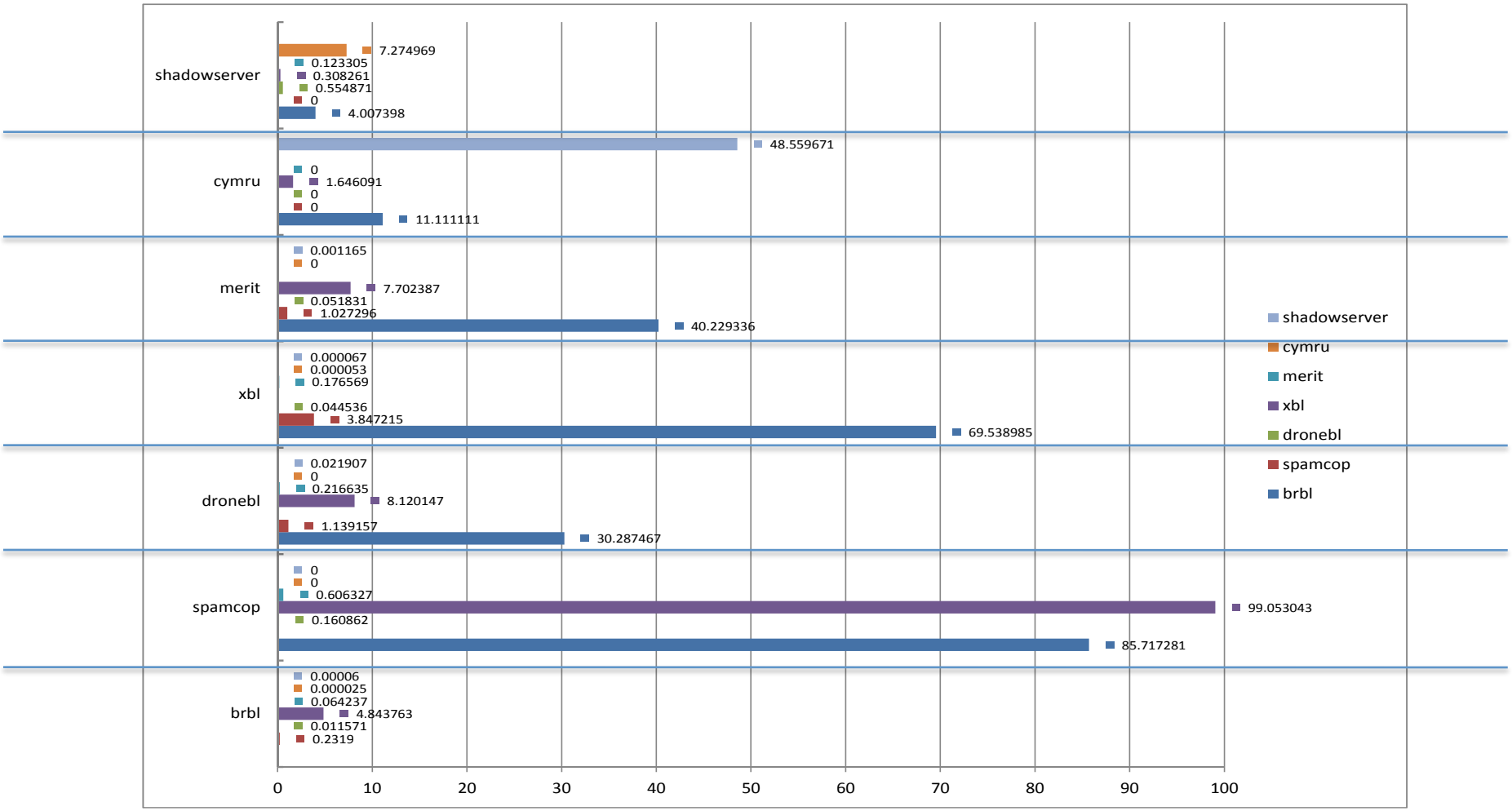
What is in RBLs - DarknetScanners



view as a pie chart

	Country Code	Blacklisted IP Count	% of Listed IPs	Country Name
1	IN	84540	11.33	INDIA
2	RU	62404	8.36	RUSSIAN FEDERATION
3	CN	53570	7.18	CHINA
4	BR	49921	6.69	BRAZIL
5	US	35950	4.82	UNITED STATES
6	TW	24912	3.34	TAIWAN, PROVINCE OF CHINA
7	AR	21436	2.87	ARGENTINA
8	IT	15729	2.11	ITALY
9	RO	12078	1.62	ROMANIA
10	UA	12024	1.61	UKRAINE

RBL Overlaps



RBL BRICs

	Country	IP Count on RBL	% of List		RBL Name
1	BR	9718232	9.04	BRAZIL	brbl
2	BR	30833	10.60	BRAZIL	spamcop
2	BR	635647	8.49	BRAZIL	xbl
2	BR	19136	11.14	BRAZIL	dsbl
4	BR	2321	5.65	BRAZIL	dronebl
1	RU	28857	16.81	RUSSIAN FEDERATION	dsbl
3	RU	2364	5.75	RUSSIAN FEDERATION	dronebl
3	RU	23831	8.19	RUSSIAN FEDERATION	spamcop
3	RU	471500	6.29	RUSSIAN FEDERATION	xbl
5	RU	6981325	6.49	RUSSIAN FEDERATION	brbl
1	IN	1212606	16.19	INDIA	xbl
1	IN	38993	13.40	INDIA	spamcop
6	IN	4719107	4.39	INDIA	brbl
2	CN	2627	6.39	CHINA	dronebl
3	CN	7442328	6.92	CHINA	brbl
8	CN	205017	2.74	CHINA	xbl
10	CN	5202	3.03	CHINA	dsbl

Building Network Reputation- Example

Prefix	XBL	SpmCop	Drknet	RpIdx
59.103.63.0/24	222	3	216	57
59.103.69.0/24	217	8	177	52
202.152.243.0/24	254	154	10	54
83.149.21.0/24	253	124	1	49
85.26.164.0/23	508	229	3	48
85.115.248.0/24	252	81	1	43
83.149.44.0/22	1024	180	64	41
83.149.8.0/23	508	43	76	41
85.26.155.0/24	252	22	38	41
180.245.188.0/22	894	15	0	30

Building Network Reputation- Example

Prefix	Network Owner	**CN**	**RIR**
59.103.63.0/24	PTCL H/Q G-8/4	PK	APNIC
59.103.69.0/24	PTCL H/Q G-8/4	PK	APNIC
202.152.243.0/24	XLNET	ID	APNIC
83.149.21.0/24	OJSC MSSPovol	RU	RIPE
85.26.164.0/23	Volga OJSC GPRS	RU	RIPE
85.115.248.0/24	JSC Vimpelcom	RU	RIPE
83.149.44.0/22	CJSC MegaFon Ctr	RU	RIPE
83.149.8.0/23	MegaFon-Moscow	RU	RIPE
85.26.155.0/24	MegaFon-Moscow	RU	RIPE
180.245.188.0/22	PTTelkom Indonesia	ID	APNIC

Building AS Reputation

Network Reputation

Index
View Stats - Top Networks - Top ASNs
View Dataset Graphs - View Geographical Data

#	ASN ▼	Size ▼	Owner ▼	Index ▼
1	131089	1022	CAT-ISP-4BYTENET-AS-AP CAT TELECOM Public Company Ltd,CAT	52
2	31208	2040	MF-CENTER-AS OJSC MegaFon Network	47
3	18959	6140	AWL-29-AS - The American Way, LLC	45
4	40965	254	NET-UA-AS limited corp	33
5	40775	6140	WIRELESSASPAS1 - Wirelessasperations, LLC	31
6	49908	510	TELEPHANT-AS Telephant Ltd	30
7	22893	12284	CYBERWORLD-INT - Cyber World Internet Services, Inc.	30
8	50604	2046	MEDIASUD-AS SC MEDIA SUD SRL	30
9	20228	12284	PACNET-MX - Pacnet, S.A. de C.V.	29
10	8661	57338	PTK PTK IP/MPLS Network	29
11	23860	16376	ALLIANCE-GATEWAY-AS-AP Alliance Broadband Services Pvt. Ltd.,Alliance Gateway AS,Broadband Services Provider,Kolkata,India	28
12	49817	510	SKIF-TV-AS TRK Skif-TV LLC	27
13	42601	2046	MABNA Gostaresh Ertebatat Mabna (MABNA)	27
14	44798	1022	PERVOMAYSK-AS PP "SKS-Pervomaysk"	27
15	50106	1022	ANTRATSIT-UA-NET PP "SKS-ANTRASIT"	27
16	51858	254	KRAPKO-AS FOP Krapko Olexandr Muhaylovich	27
17	46801	12280	DIALWAVE-INTERNATIONAL - Dialwave International	27
18	8143	16378		27
19	40861	12252	COLONET-SOLUTIONS-ASN - Colo Net Solutions, LLC.	26
20	50948	5106	BEHKOOSH Behkoush Rayaneh Afzar Co.	25
21	51630	1018	SIABAS-AS SIA BUSINESS AVIATION SERVICES	25
22	12327	254	IDEAR4BUSINESS-INTERNATIONAL-LTD IDEAR4BUSINESS INTERNATIONAL LTD	24
23	55812	254	HOAPDI-NET-PH Unit 202 JMR Building Legaspi St	24
24	29117	256	IRC-HISPANO http://www.irc-hispano.es/	24
25	28373	1022	Bajanet Comunicaciones, S.A. de C.V.	24

Displaying Results From 1 to 25

Display 10 Results - Display 25 Results - Display 50 Results - Display 100 Results - Display 200 Results
next

Conclusions

- The goal of the network reputation index is to create a predictive indicator of malicious activity and to allows networks to adjust their own security posture for different networks
- The underlying premise is that network reputation is an indicator of your relative security posture and hence a predictor of future malicious activity
- Initial results and proof-of-concept are promising but a lot of work remains in developing a more convincing method for handling local reputation reports
- Work also underway for developing prototypes that demonstrate the utility of network reputation in security polices