EMBER: A Global Perspective on Extreme Malicious Behavior

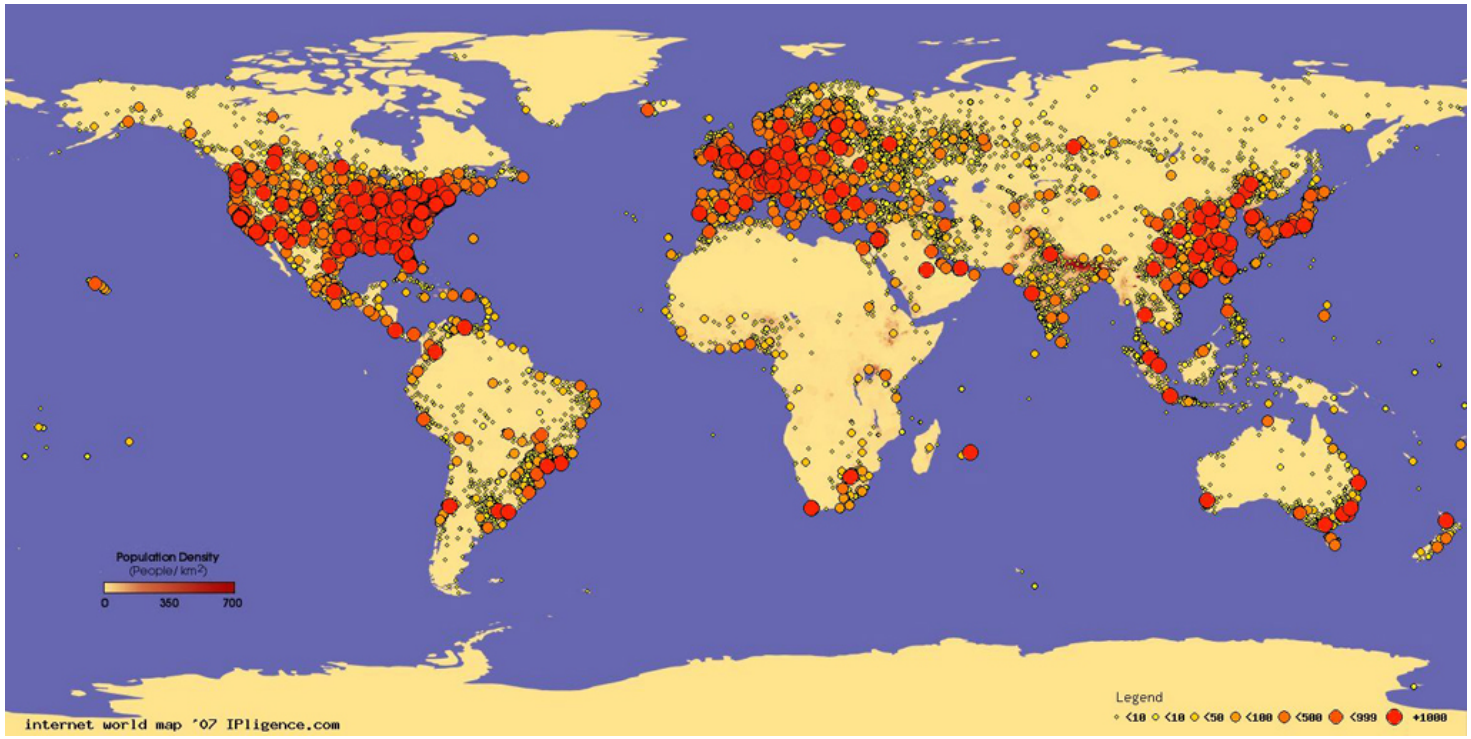
Tamara Yu Richard Lippmann James Riordan Stephen Boyer

MIT Lincoln Laboratory

Wanxin Li

CISC850
Cyber Analytics

Background

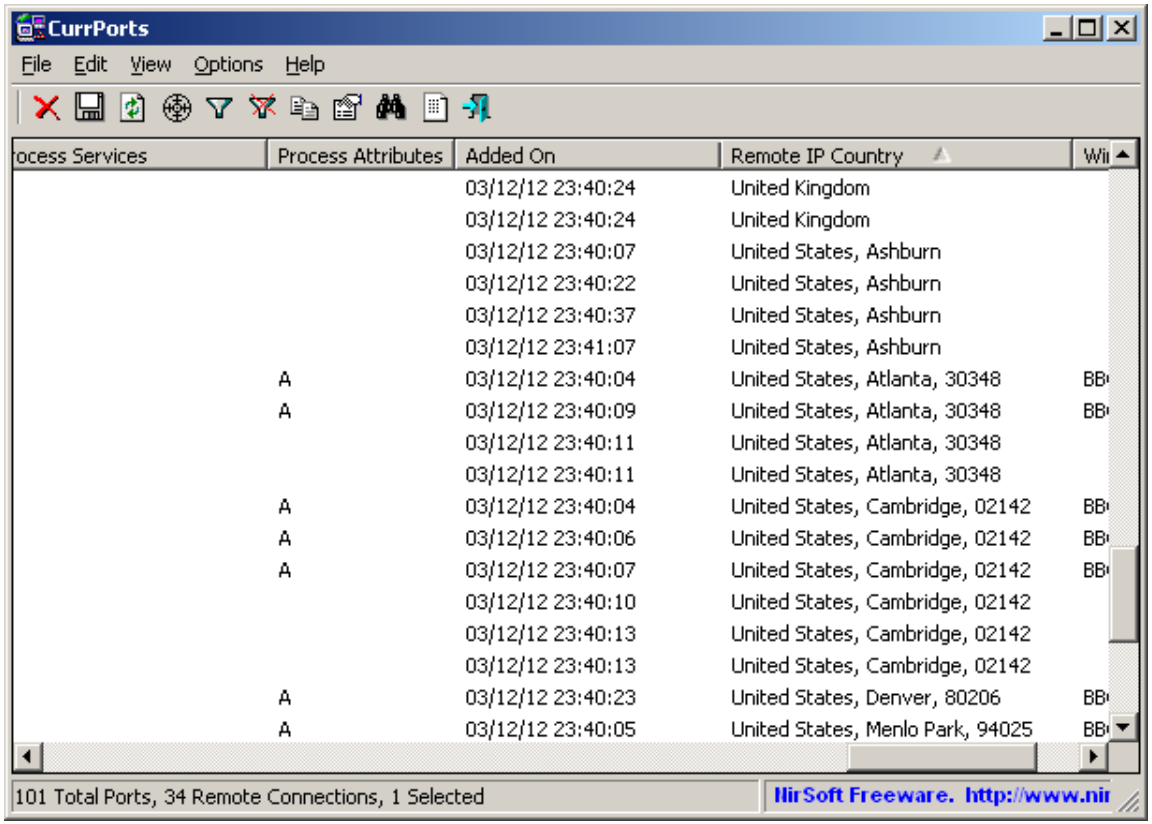

Population Density
(People/ km2)
0
350
700
internet world map '07 IPligence.com
Legend
<10
<10
<50
<100
<500
<999
+1000

Contributions

- Standardized Incidence Rate (SIR);
- Compare malicious activity across cities;
- Using DShield dataset;
- Distribution of SIRs.

Approach

**IP Geo-Location*



MaxMind GeoLite City database

Approach

**City Host Population*

$$N_{city} = Population_{city} \times InternetPenetrationRate_{city}$$

- Data Source:
  - Population Data: GeoNames
  - Internet Penetration Rate: Internet World States

Approach

**Standardized Incidence Rate*

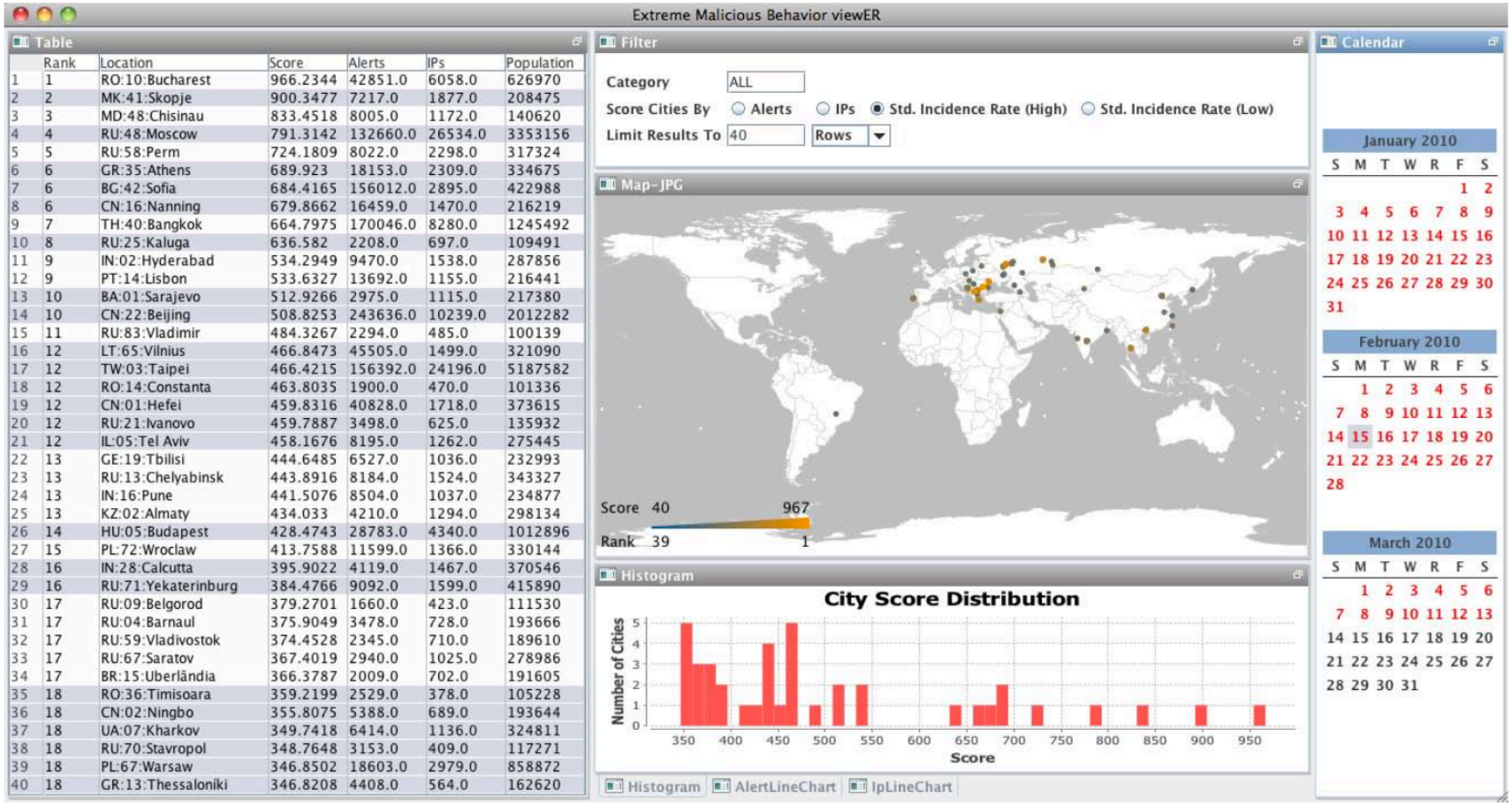
$$SIR_{city} = \frac{IPs_{city}}{N_{city}} \times 100,000$$

Approach

**Adjustments*

	Justification	Mal. IPs	Subtotal
Discarded	No city	30,398	108,680
	No population	77,864	
	Low IPR	418	
Retained	Adjusted IPR	15,717	494,866
		479,149	
Total		603,546	

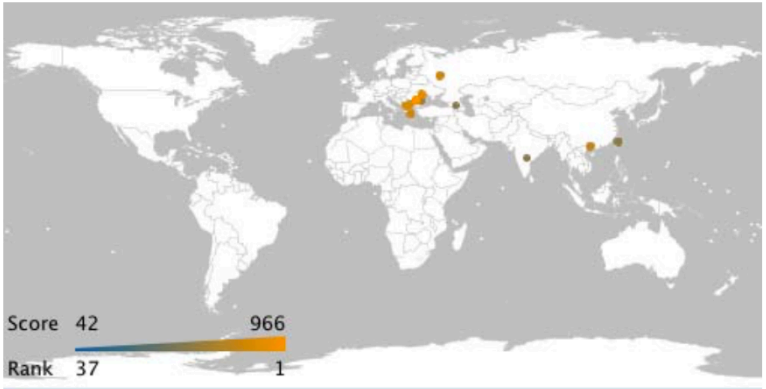
EMBER



	Rank	Location	Score	Alerts	IPs	Population
1	1	RO:10:Bucharest	966.2344	42851.0	6058.0	626970
2	2	MK:41:Skopje	900.3477	7217.0	1877.0	208475
3	3	MD:48:Chisinau	833.4518	8005.0	1172.0	140620
4	4	RU:48:Moscow	791.3142	132660.0	26534.0	3353156
5	5	RU:58:Perm	724.1809	8022.0	2298.0	317324
6	6	GR:35:Athens	689.923	18153.0	2309.0	334675
7	6	BG:42:Sofia	684.4165	156012.0	2895.0	422988
8	6	CN:16:Nanning	679.8662	16459.0	1470.0	216219
9	7	TH:40:Bangkok	664.7975	170046.0	8280.0	1245492
10	8	RU:25:Kaluga	636.582	2208.0	697.0	109491
11	9	IN:02:Hyderabad	534.2949	9470.0	1538.0	287856
12	9	PT:14:Lisbon	533.6327	13692.0	1155.0	216441
13	10	BA:01:Sarajevo	512.9266	2975.0	1115.0	217380
14	10	CN:22:Beijing	508.8253	243636.0	10239.0	2012282
15	11	RU:83:Vladimir	484.3267	2294.0	485.0	100139
16	12	LT:65:Vilnius	466.8473	45505.0	1499.0	321090
17	12	TW:03:Taipei	466.4215	156392.0	24196.0	5187582
18	12	RO:14:Constanta	463.8035	1900.0	470.0	101336
19	12	CN:01:Hefei	459.8316	40828.0	1718.0	373615
20	12	RU:21:Ivanovo	459.7887	3498.0	625.0	135932
21	12	IL:05:Tel Aviv	458.1676	8195.0	1262.0	275445
22	13	GE:19:Tbilisi	444.6485	6527.0	1036.0	232993
23	13	RU:13:Chelyabinsk	443.8916	8184.0	1524.0	343327
24	13	IN:16:Pune	441.5076	8504.0	1037.0	234877
25	13	KZ:02:Almaty	434.033	4210.0	1294.0	298134
26	14	HU:05:Budapest	428.4743	28783.0	4340.0	1012896
27	15	PL:72:Wroclaw	413.7588	11599.0	1366.0	330144
28	16	IN:28:Calcutta	395.9022	4119.0	1467.0	370546
29	16	RU:71:Yekaterinburg	384.4766	9092.0	1599.0	415890
30	17	RU:09:Belgorod	379.2701	1660.0	423.0	111530
31	17	RU:04:Barnaul	375.9049	3478.0	728.0	193666
32	17	RU:59:Vladivostok	374.4528	2345.0	710.0	189610
33	17	RU:67:Saratov	367.4019	2940.0	1025.0	278986
34	17	BR:15:Uberlândia	366.3787	2009.0	702.0	191605
35	18	RO:36:Timisoara	359.2199	2529.0	378.0	105228
36	18	CN:02:Ningbo	355.8075	5388.0	689.0	193644
37	18	UA:07:Kharkov	349.7418	6414.0	1136.0	324811
38	18	RU:70:Stavropol	348.7648	3153.0	409.0	117271
39	18	PL:67:Warsaw	346.8502	18603.0	2979.0	858872
40	18	GR:13:Thessaloníki	346.8208	4408.0	564.0	162620

Case Study

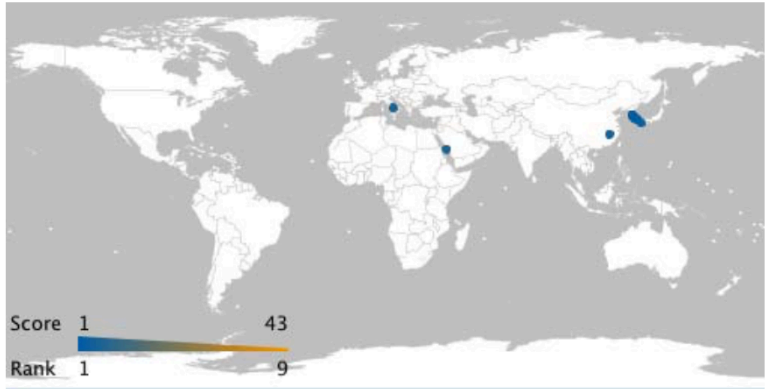
**Extreme Cities*



Table

	Rank	Location	Score	Alerts	IPs	Population
1	1	RO:10:Bucharest	965.9154	44209.0	6056.0	626970
2	2	MD:48:Chisinau	872.5643	5221.0	1227.0	140620
3	3	MK:41:Skopje	814.9658	8197.0	1699.0	208475
4	4	BG:42:Sofia	797.6585	152081.0	3374.0	422988
5	5	GR:35:Athens	780.7574	21325.0	2613.0	334675
6	5	RU:48:Moscow	775.9853	273984.0	26020.0	3353156
7	6	CN:16:Nanning	744.7479	13576.0	1736.0	233099
8	7	RO:14:Constanta	611.826	3334.0	620.0	101336
9	8	TW:03:Taipei	552.4346	145793.0	28658.0	5187582
10	9	IN:02:Hyderabad	517.9673	11132.0	1491.0	287856
11	9	GE:19:Tbilisi	513.7493	7545.0	1197.0	232993

(a)



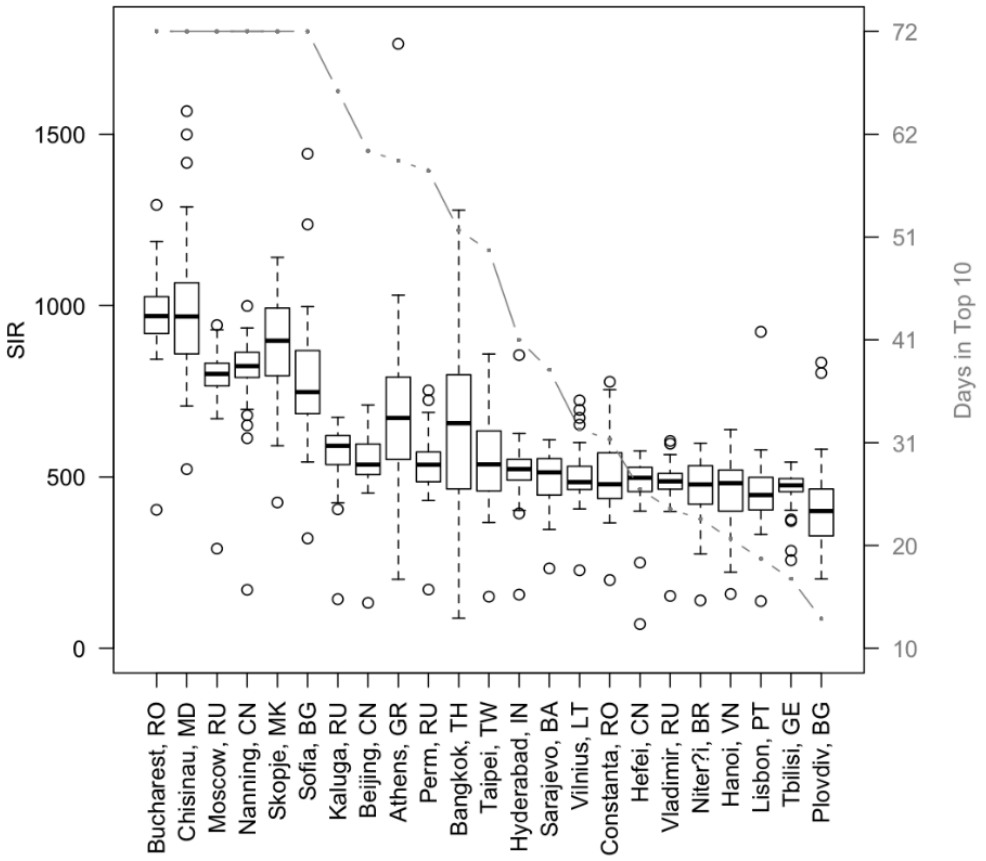
Table

	Rank	Location	Score	Alerts	IPs	Population
1	1	KR:12:Inchon	1.2306	510.0	25.0	2031444
2	1	KR:10:Busan	2.7782	1405.0	79.0	2843523
3	1	KR:19:Daejeon	2.8061	365.0	32.0	1140346
4	1	KR:15:Daegu	3.0242	700.0	60.0	1983935
5	1	JP:07:Kitakyushu	3.5849	163.0	27.0	753146
6	1	KR:12:Incheon	3.8888	1533.0	79.0	2031444
7	1	CN:03:Nanchang	4.0538	83.0	22.0	542692
8	1	KR:13:Bucheon	4.2578	170.0	28.0	657615
9	1	KR:21:Ulsan	4.2993	269.0	32.0	744295
10	1	IT:04:Napoli	4.6939	156.0	24.0	511299
11	1	SA:14:Jeddah	5.5954	303.0	43.0	768476

(b)

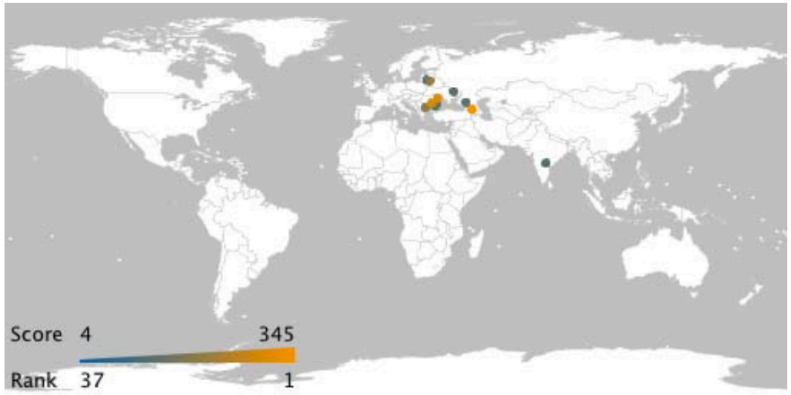
Case Study

**Infection Duration*



Case Study

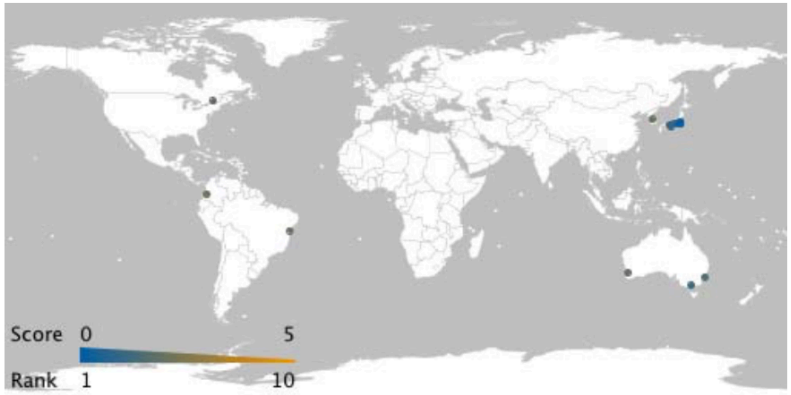
**Persistent Infections*



Table

	Rank	Location	Score	Alerts	IPs	Population
1	1	GE:19:Tbilisi	344.6455	5500.0	803.0	232993
2	2	MD:48:Chisinau	301.5218	2661.0	424.0	140620
3	3	RO:10:Bucharest	296.9839	16852.0	1862.0	626970
4	4	BG:42:Sofia	193.6225	144200.0	819.0	422988
5	4	LT:65:Vilnius	192.7808	9319.0	619.0	321090
6	5	RO:14:Constanta	123.352	1086.0	125.0	101336
7	6	BG:61:Varna	119.3514	930.0	137.0	114787
8	7	RU:70:Stavropol	116.8234	544.0	137.0	117271
9	7	LT:57:Kaunas	115.8722	21618.0	257.0	221796
10	8	UA:07:Kharkov	112.0651	2918.0	364.0	324811
11	8	IN:02:Hyderabad	110.4719	2500.0	318.0	287856

(a)



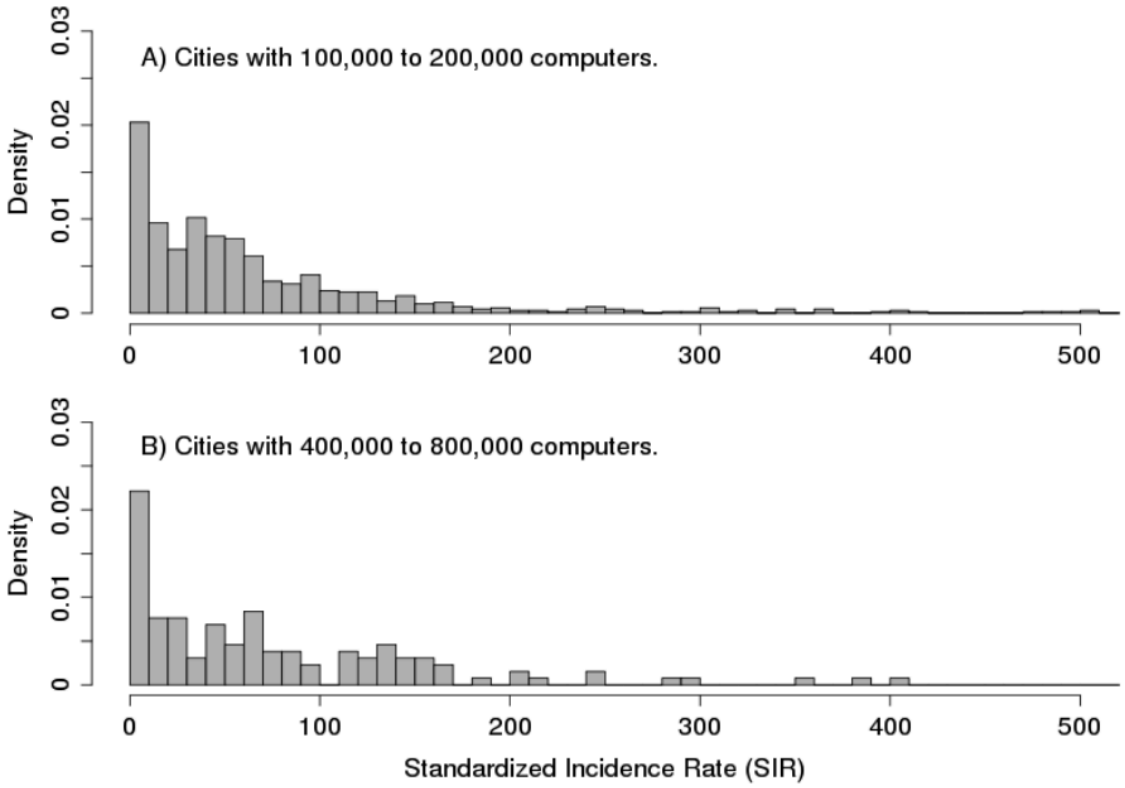
Table

	Rank	Location	Score	Alerts	IPs	Population
1	1	JP:40:Tokyo	0.7951	6360.0	189.0	23767776
2	2	JP:19:Yokohama	1.1857	344.0	32.0	2698731
3	2	JP:32:Osaka	1.4816	165.0	29.0	1957287
4	3	JP:01:Nagoya	1.5715	365.0	26.0	1654425
5	3	AU:07:Melbourne	1.6399	2428.0	49.0	2987900
6	3	AU:02:Sydney	1.9317	3118.0	68.0	3520063
7	4	CA:QC:Montreal	2.124	4232.0	52.0	2448116
8	4	AU:08:Perth	2.2436	655.0	26.0	1158819
9	4	KR:13:Suwon	2.2901	2174.0	22.0	960626
10	4	BR:05:Salvador	2.3859	258.0	22.0	922047
11	4	CO:29:Cali	2.3985	9151.0	26.0	1083982

(b)

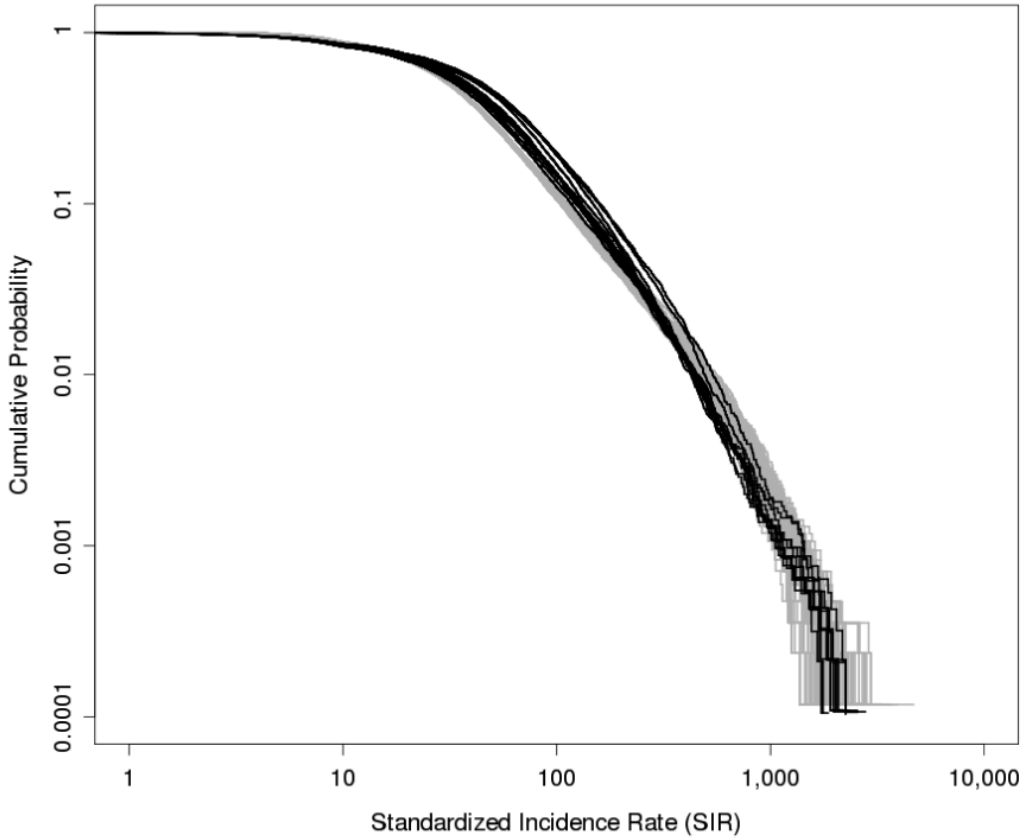
Case Study

**Standardized Incidence Rate Distribution*



Case Study

**Simulation to Explain SIR Distribution*



Conclusions

- EMBER scores cities by SIR.
- Apply EMBER by DShield dataset.
- Worldwide SIR Distribution.

Future Work

- Obtain more accurate geo-location data.
- Improve the estimation of city host population.
- Import IPv6 dataset.