

## Kortech.cn Botnet Statistics - 16/02/2009 to 31/06/2010

Eric Romang - <http://eromang.zataz.com>

### Kortech.cn Botnet Stats

Total Unique Tier RFIs	39
Total Events	8134
Average Tier RFI Events	208,56
Median Tier RFI Events	25
Min Tier RFI Events	1
Max Tier RFI Events	3520
Total Source IPs	353
Average Tier RFI Source IPs	9,05
Median Tier RFI Source IPs	3
Min Tier RFI Source IPs	1
Max Tier RFI Source IPs	186
Average Tier RFI Lifetime	48,33
Median Tier RFI Lifetime	11
Min Tier RFI Lifetime	0
Max Tier RFI Lifetime	499

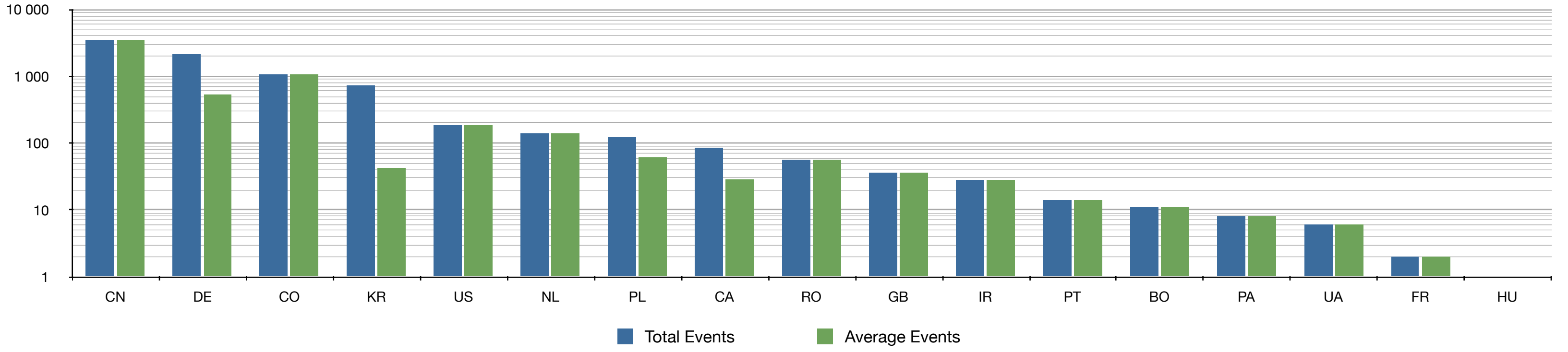
### Kortech.cn Tier RFIs Countries

Country	Total Tier RFIs	Total Events	Average Events	Total Source IPs	Average Source IPs	Events per Tier RFI	Events per Source IP	Source IPs per Tier RFI	Average Lifetime
CN	1	3 520	3 520	186	186	3 520	19	186	499
DE	4	2 127	532	38	10	532	56	10	51
CO	1	1 067	1 067	11	11	1 067	97	11	65
KR	17	725	43	76	4	43	10	4	46
US	1	186	186	5	5	186	37	5	134
NL	1	140	140	9	9	140	16	9	26
PL	2	122	61	9	5	61	14	5	7
CA	3	85	28	8	3	28	11	3	36
RO	1	56	56	1	1	56	56	1	10
GB	1	36	36	1	1	36	36	1	0
IR	1	28	28	2	2	28	14	2	30
PT	1	14	14	1	1	14	14	1	1
BO	1	11	11	2	2	11	6	2	4
PA	1	8	8	1	1	8	8	1	0
UA	1	6	6	1	1	6	6	1	0
FR	1	2	2	1	1	2	2	1	1
HU	1	1	1	1	1	1	1	1	0

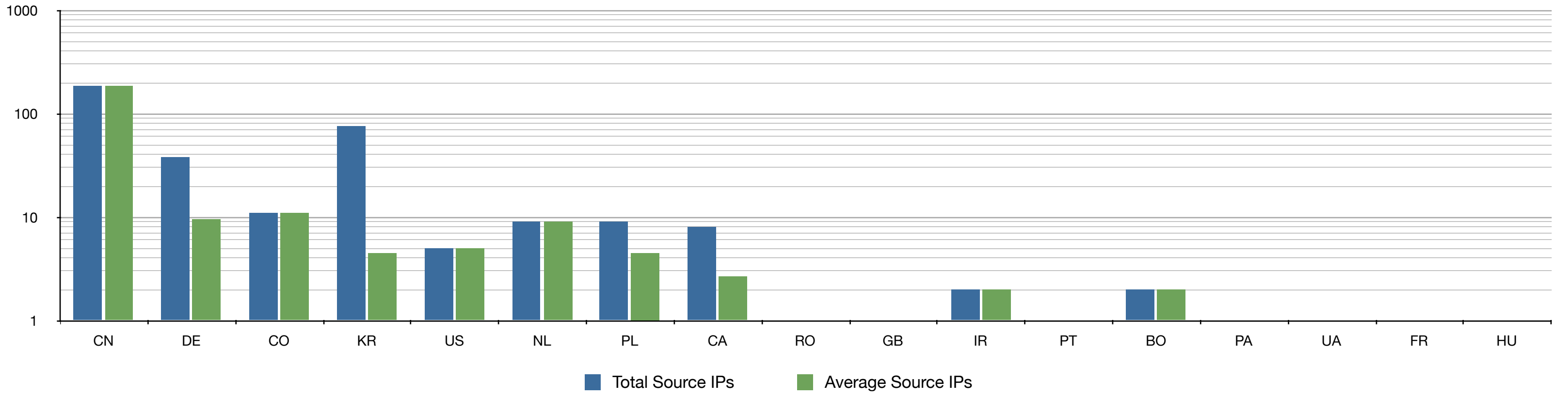
### Kortech.cn Time Frame

Month	02/09	03/09	04/09	05/09	06/09	07/09	08/09	09/09	10/09	11/09	12/09	01/10	02/10	03/10	04/10	05/10	06/10
Total Distinct Tier RFIs	1	4	3	3	4	8	3	3	2	1	7	7	7	10	8	6	6
Total Events	13	71	710	992	725	592	209	104	69	13	142	610	526	1172	347	744	1095
Total Source IPs	3	20	54	41	13	19	16	5	8	3	15	35	28	29	20	32	51
Events per Tier RFI	13	17,75	236,7	330,7	181,3	74	69,67	34,67	34,5	13	20,29	87,14	75,14	117,2	43,38	124	182,5
Events per Source IP	4,333	3,55	13,15	24,2	55,77	31,16	13,06	20,8	8,625	4,333	9,467	17,43	18,79	40,41	17,35	23,25	21,47
Source IPs per Tier RFI	3	5	18	13,67	3,25	2,375	5,333	1,667	4	3	2,143	5	4	2,9	2,5	5,333	8,5

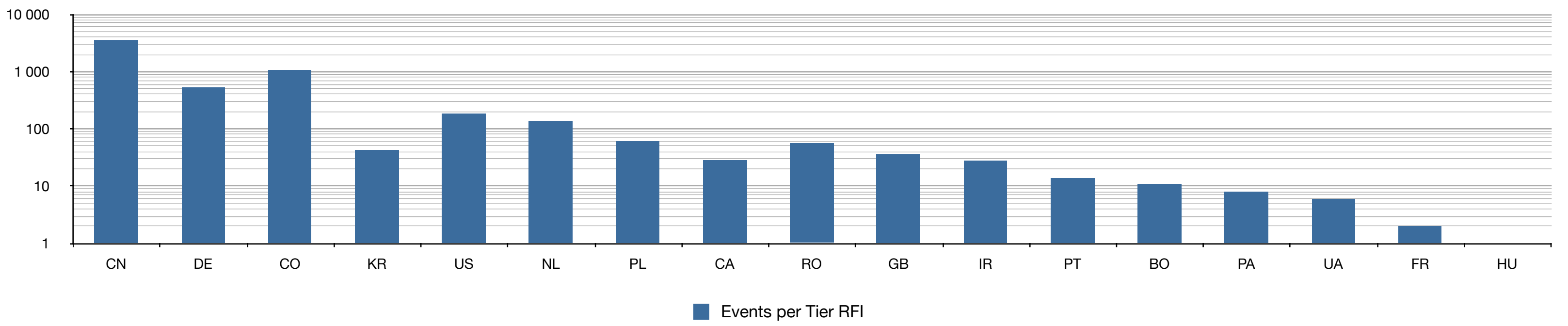
Kortech.cn Botnet Total & Average Events



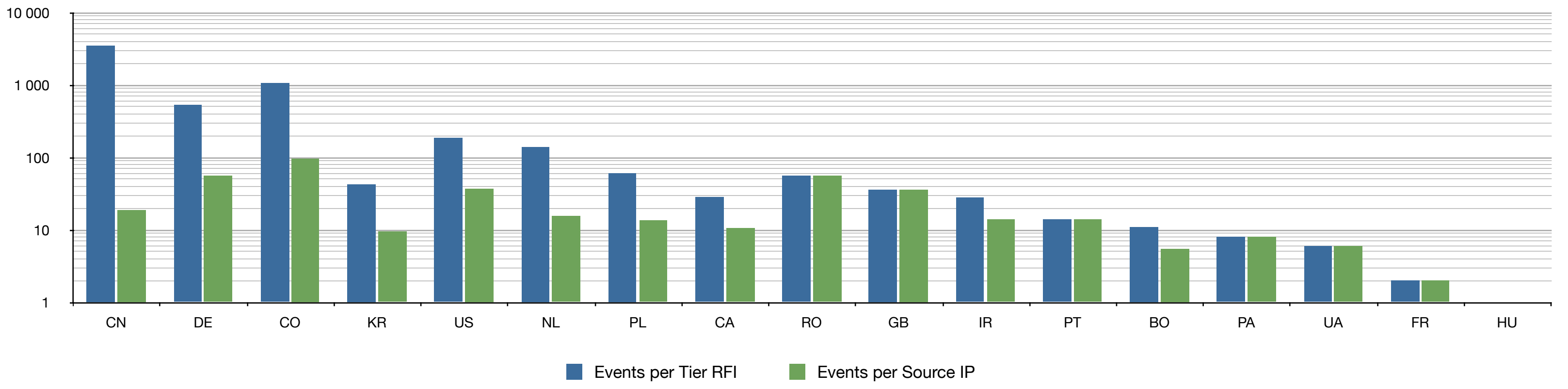
Kortech.cn Botnet Total & Average Source IPs



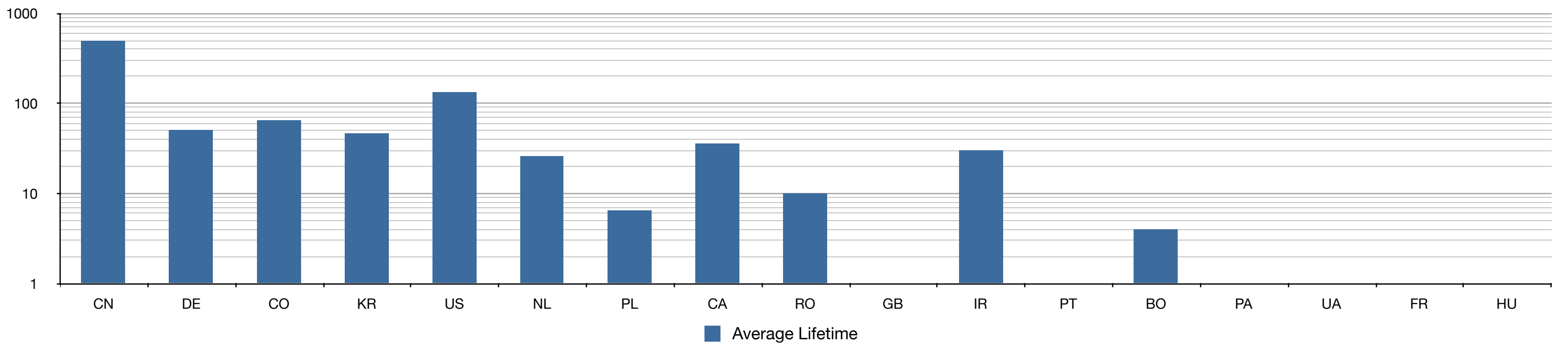
Kortech.cn Botnet Events per Tier RFI



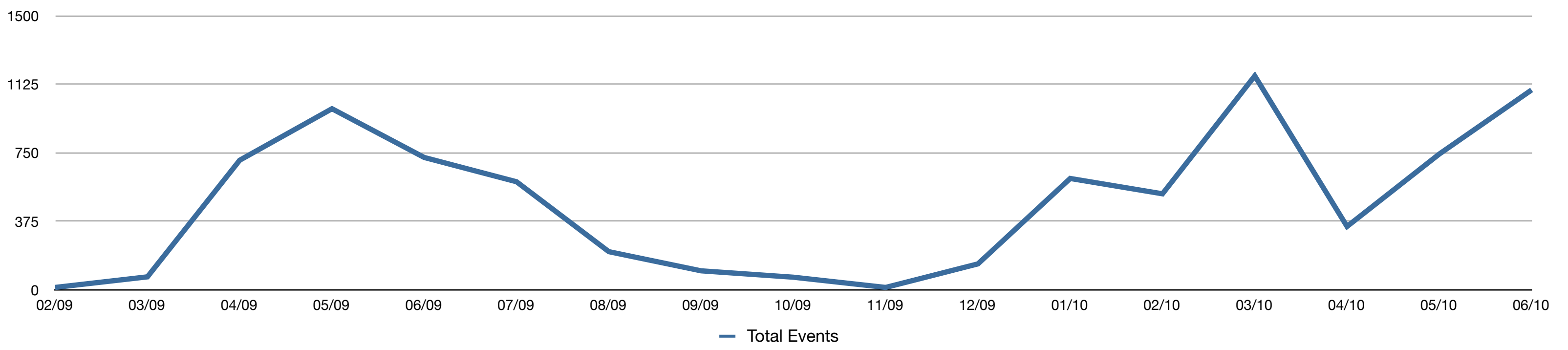
Kortech.cn Botnet Events per Source IP and Events per Tier RFI



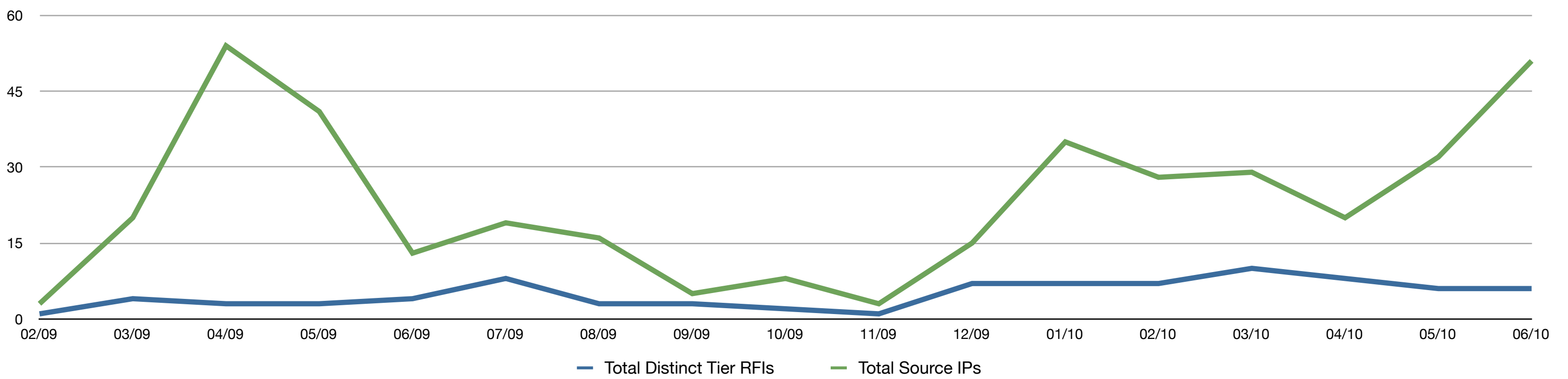
Kortech.cn Botnet Average Lifetime



Kortech.cn Monthly Events



Kortech.cn Monthly Tier RFIs & Source IPs



### Kortech.cn Botnet All Tier RFIs

Tier RFI ID	RFI IP	RFI Country	Events	Source IPs	First seen	Last seen	Lifetime (day's)
15	218.5.74.92	CN	3520	186	16/02/09	30/06/10	499
544	218.38.18.203	KR	10	4	13/03/09	21/03/09	8
637	88.84.128.40	DE	1826	26	20/03/09	08/08/09	141
762	81.12.13.152	IR	28	2	30/03/09	29/04/09	30
920	121.78.70.9	KR	72	11	14/04/09	02/02/10	294
4009	212.40.97.120	HU	1	1	09/06/09	09/06/09	0
1717	211.233.11.27	KR	27	5	29/06/09	23/12/09	177
1725	61.78.62.84	KR	12	1	30/06/09	02/07/09	2
1772	200.105.207.244	BO	11	2	05/07/09	09/07/09	4
1834	85.214.78.119	DE	6	1	10/07/09	11/07/09	1
1894	61.100.181.217	KR	18	4	13/07/09	21/08/09	39
4256	110.45.138.141	KR	1	1	28/07/09	28/07/09	0
2415	125.251.142.142	KR	14	2	12/09/09	12/09/09	0
4276	83.16.182.130	PL	1	1	29/09/09	29/09/09	0
2592	211.203.180.144	KR	14	5	11/10/09	28/10/09	17
2881	72.55.143.249	CA	25	5	06/12/09	01/03/10	85
3346	216.119.103.12	US	186	5	07/12/09	20/04/10	134
2905	201.218.228.226	PA	8	1	09/12/09	09/12/09	0
3015	195.5.163.207	NL	140	9	21/12/09	16/01/10	26
3021	211.239.124.204	KR	13	3	22/12/09	01/03/10	69
3095	121.124.127.34	KR	234	10	01/01/10	23/01/10	22
3179	222.122.26.58	KR	72	7	10/01/10	18/01/10	8
3224	217.168.150.158	GB	36	1	18/01/10	18/01/10	0
1265	200.93.147.154	CO	1067	11	23/01/10	29/03/10	65
3370	210.205.6.233	KR	54	4	04/02/10	05/04/10	60
3527	64.15.152.132	CA	56	2	21/02/10	16/03/10	23
3562	85.119.152.183	DE	7	1	25/02/10	27/02/10	2
3761	125.248.150.84	KR	76	7	18/03/10	20/05/10	63
4229	114.200.199.236	KR	6	1	19/03/10	19/03/10	0
3805	118.129.166.213	KR	46	5	22/03/10	02/04/10	11
1658	85.236.48.245	DE	288	10	27/03/10	26/05/10	60
4699	88.165.81.34	FR	2	1	25/04/10	26/04/10	1
4711	124.49.100.254	KR	3	2	26/04/10	10/05/10	14
4866	211.239.121.168	KR	53	4	10/05/10	16/05/10	6
4990	89.35.219.220	RO	56	1	26/05/10	05/06/10	10
5264	83.16.100.218	PL	121	8	17/06/10	30/06/10	13
5377	62.149.14.44	UA	6	1	28/06/10	28/06/10	0
5392	188.93.234.10	PT	14	1	29/06/10	30/06/10	1
5405	174.142.75.205	CA	4	1	30/06/10	30/06/10	0