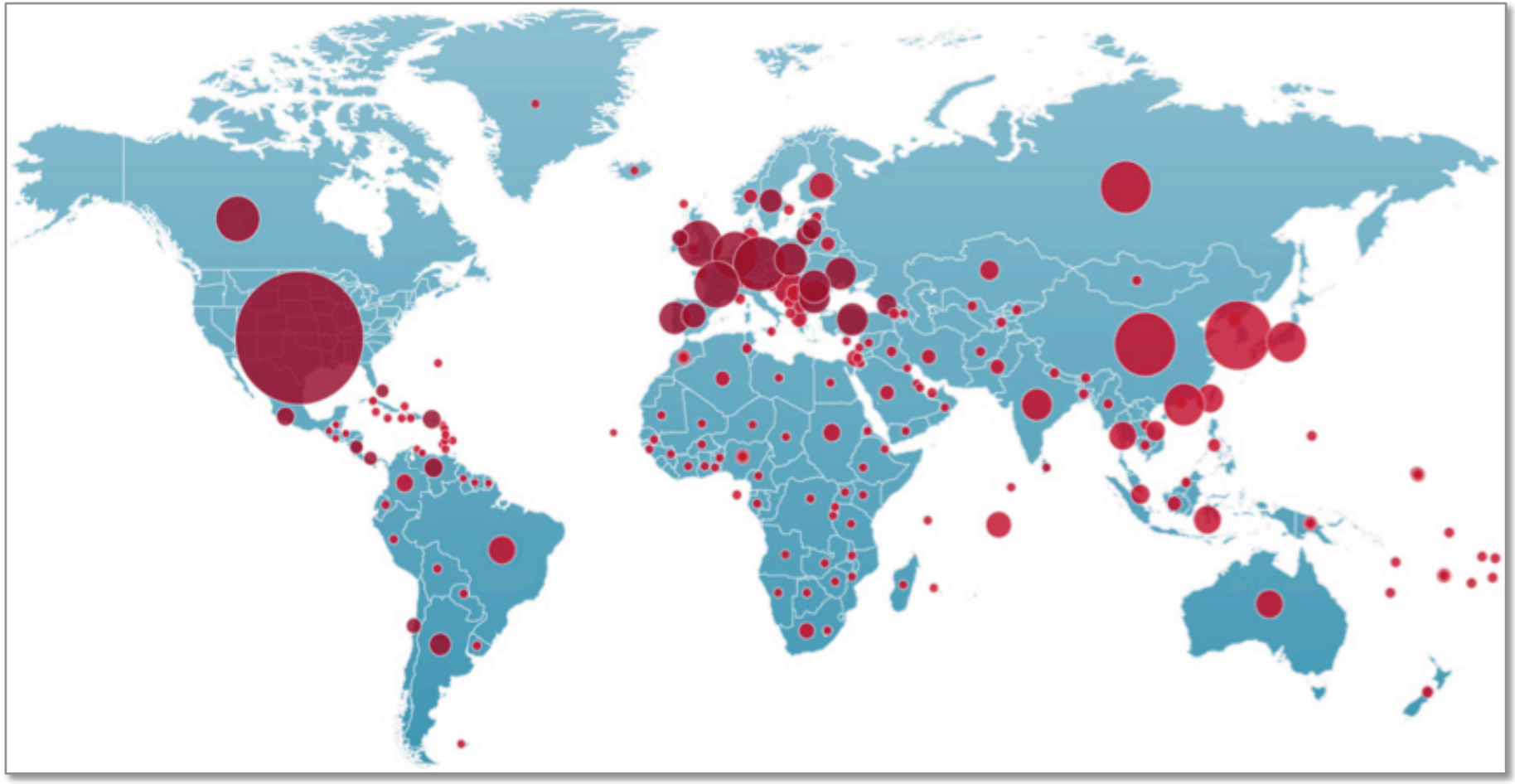
FireEye

Leviathan: Command and Control Communications on Planet Earth

Dr. Kenneth Geers
2501
Kevin Thompson
FireEye

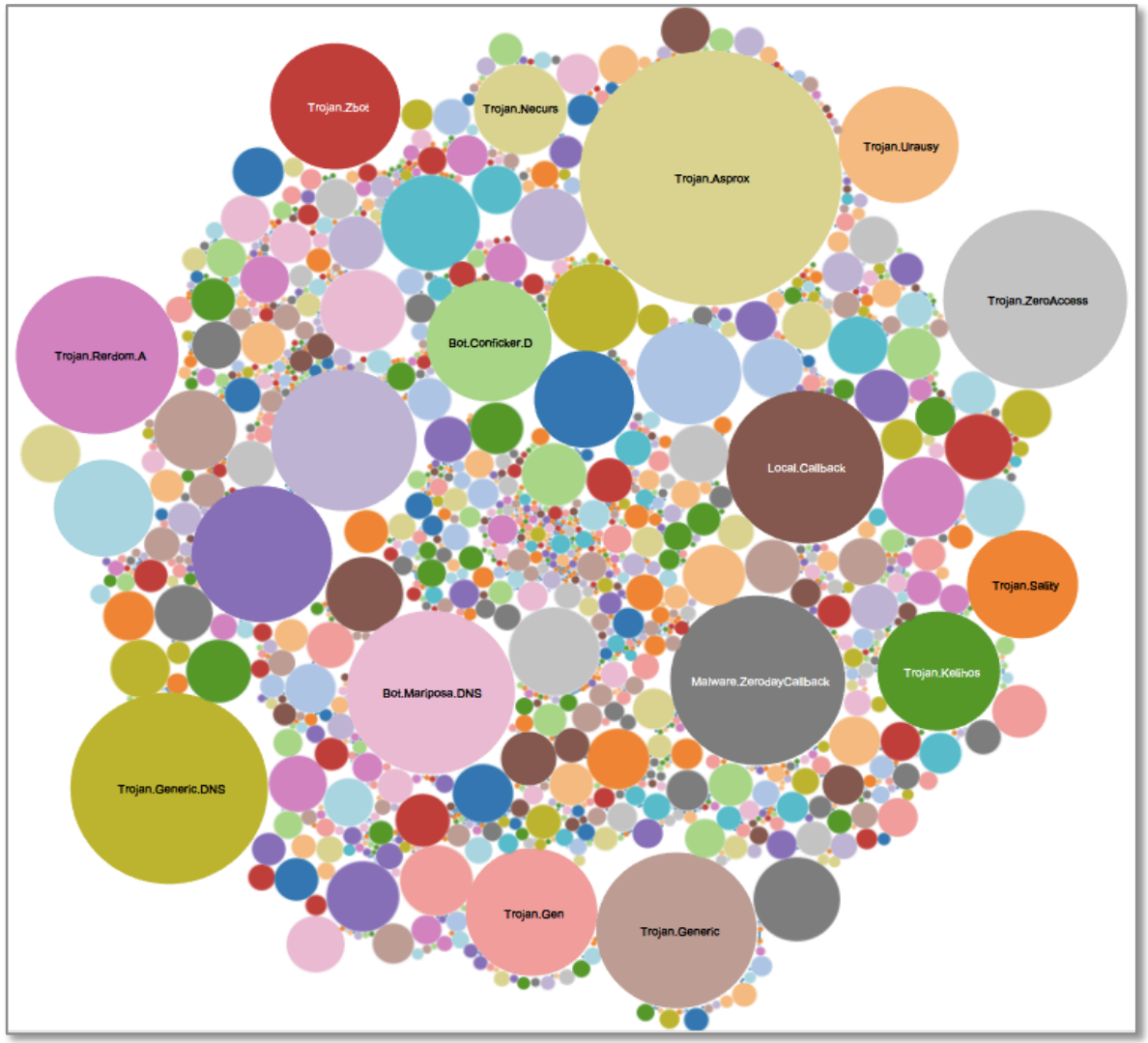
Leviathan

Worldwide malware ecosystem



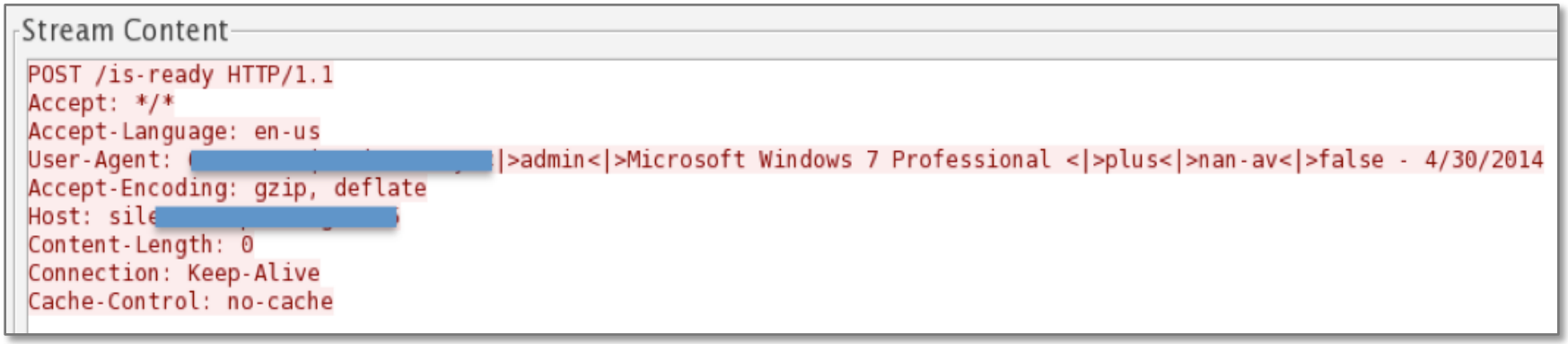
FireEye

C2 malware signatures



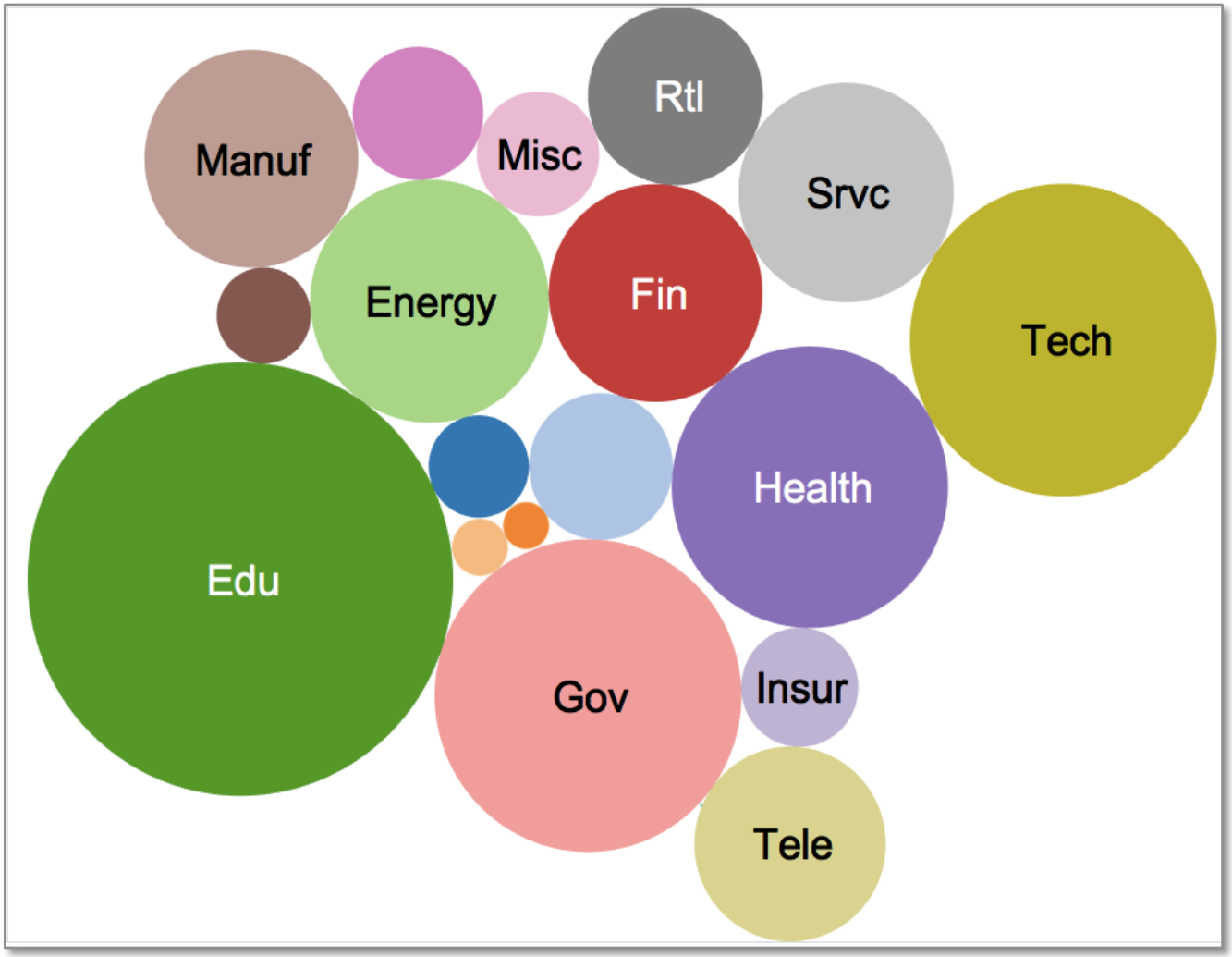
FireEye

Tactics, techniques, and procedures



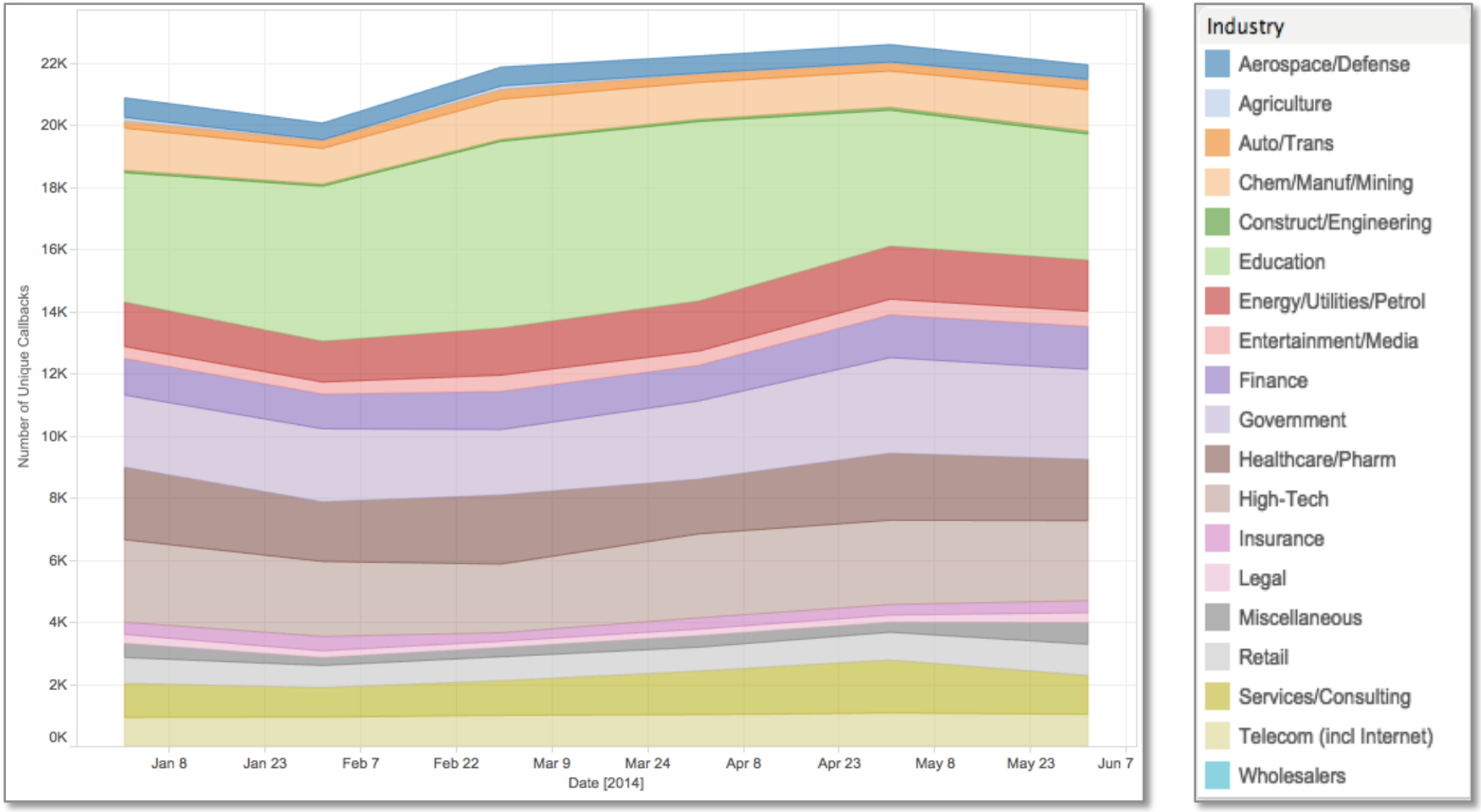
lv|'|'|
2YLZgNin2KrZgNmEINmF2YDYo9is2YDZiNixXzQwMENENTEw|'|'|
Remote PC|'|'|admin|'|'|2013-04-22|'|'|USA|'|'|Win XP Professional SP2 x86|'|'|No|'|'|0.5.0E|'|'|..|'|'|
QzpcV0lORE9XU1xzeXN0ZW0zMlxjbWQuZXhl|'|'|[endof]

Every industry vertical owned



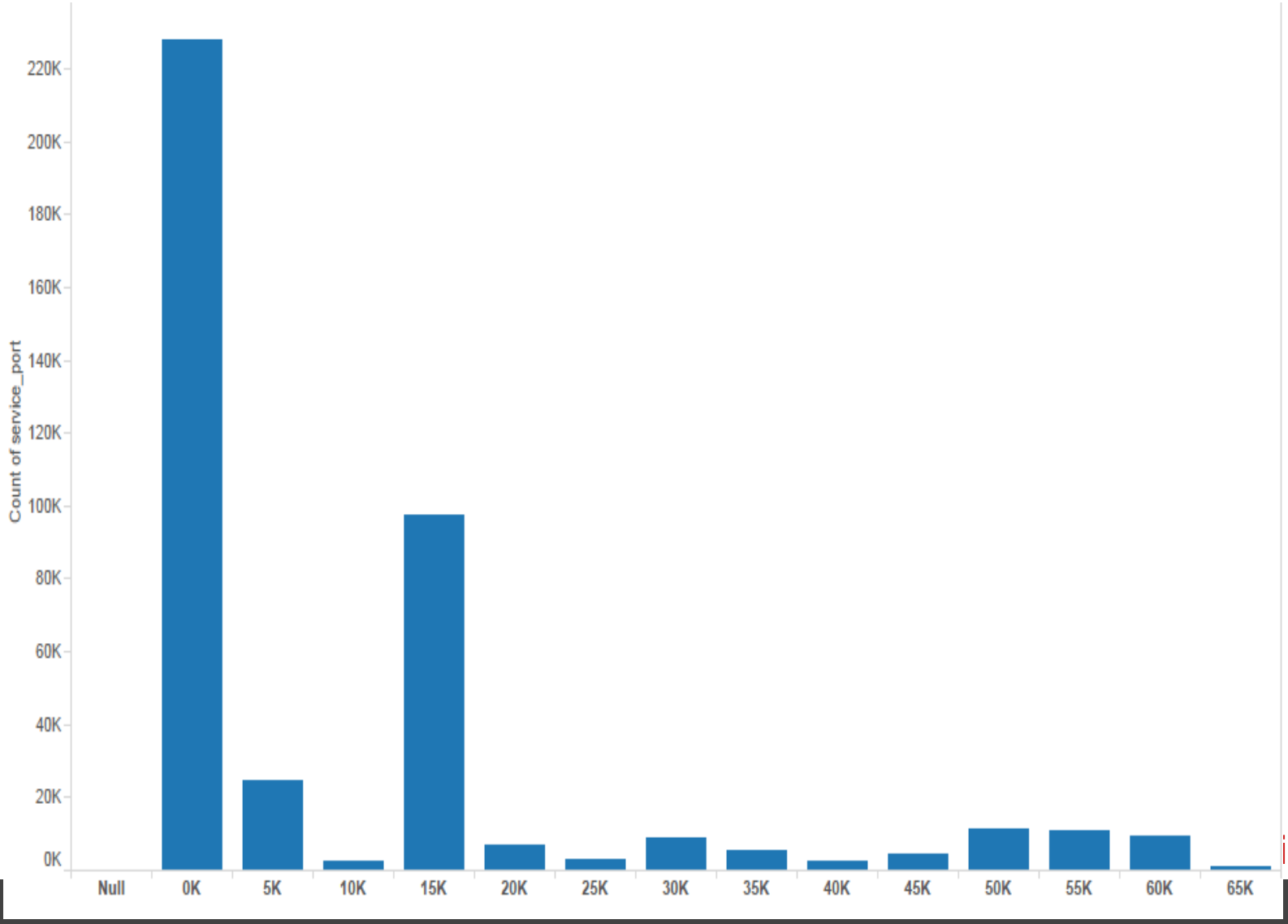
FireEye

Callbacks: ebb and flow



FireEye

Knock Knock


Count of service_port
220K
200K
180K
160K
140K
120K
100K
80K
60K
40K
20K
0K
Null
0K
5K
10K
15K
20K
25K
30K
35K
40K
45K
50K
55K
60K
65K

Hiding in Plain Site

- Vertical Analysis: Education
  - *Library*
  - *CS department*
  - *School of Law*
- Vertical Analysis: Government
- Country to Country
- Less talk, more rock:
  - For 2013 - APT 2.49, Non 5.92
  - For 2014 - APT 1.6, Non 12.10

FireEye

Hiding in plain “site”

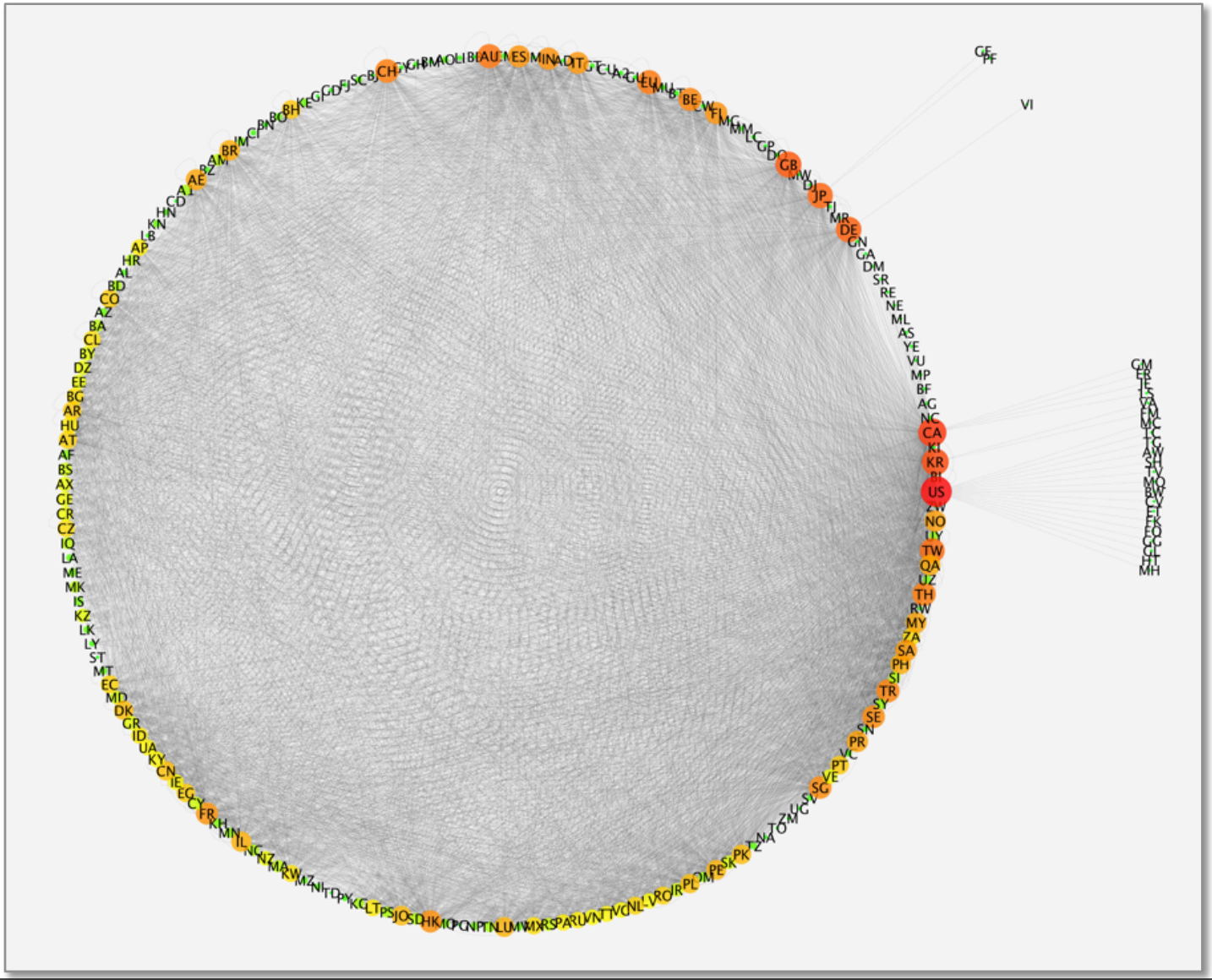
- *Unique initial CnC communications:*
- *200+ variants of google (gooqle)*
- *200+ variants of firefox (firefoxupdata)*
- *50+ variants of Facebook (faceboak)*
- *100’s of Microsoft related variants (microsocft, windosw)*
- *Spoofed security or AV sites*

FireEye

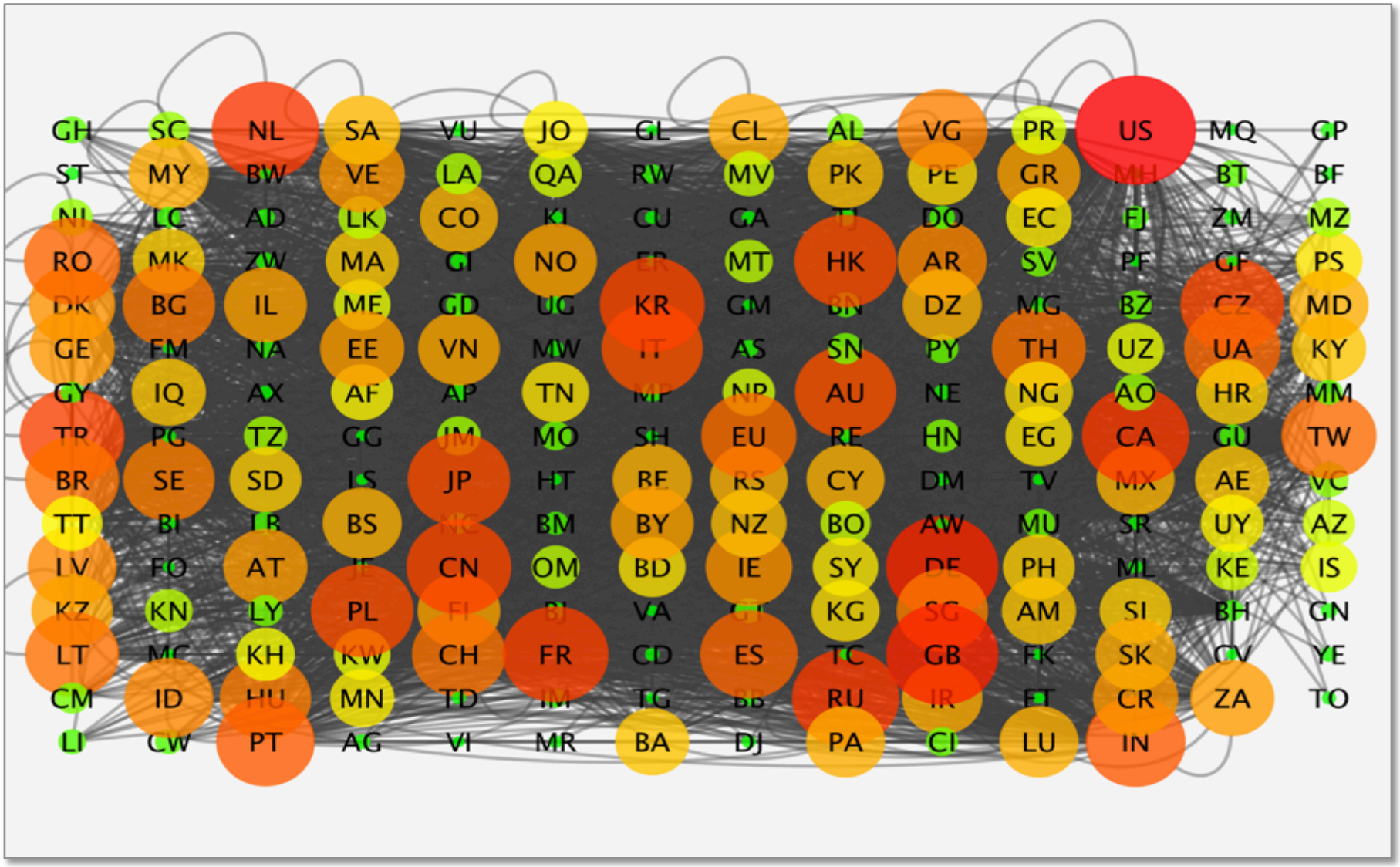
Semantic signatures

FireEye

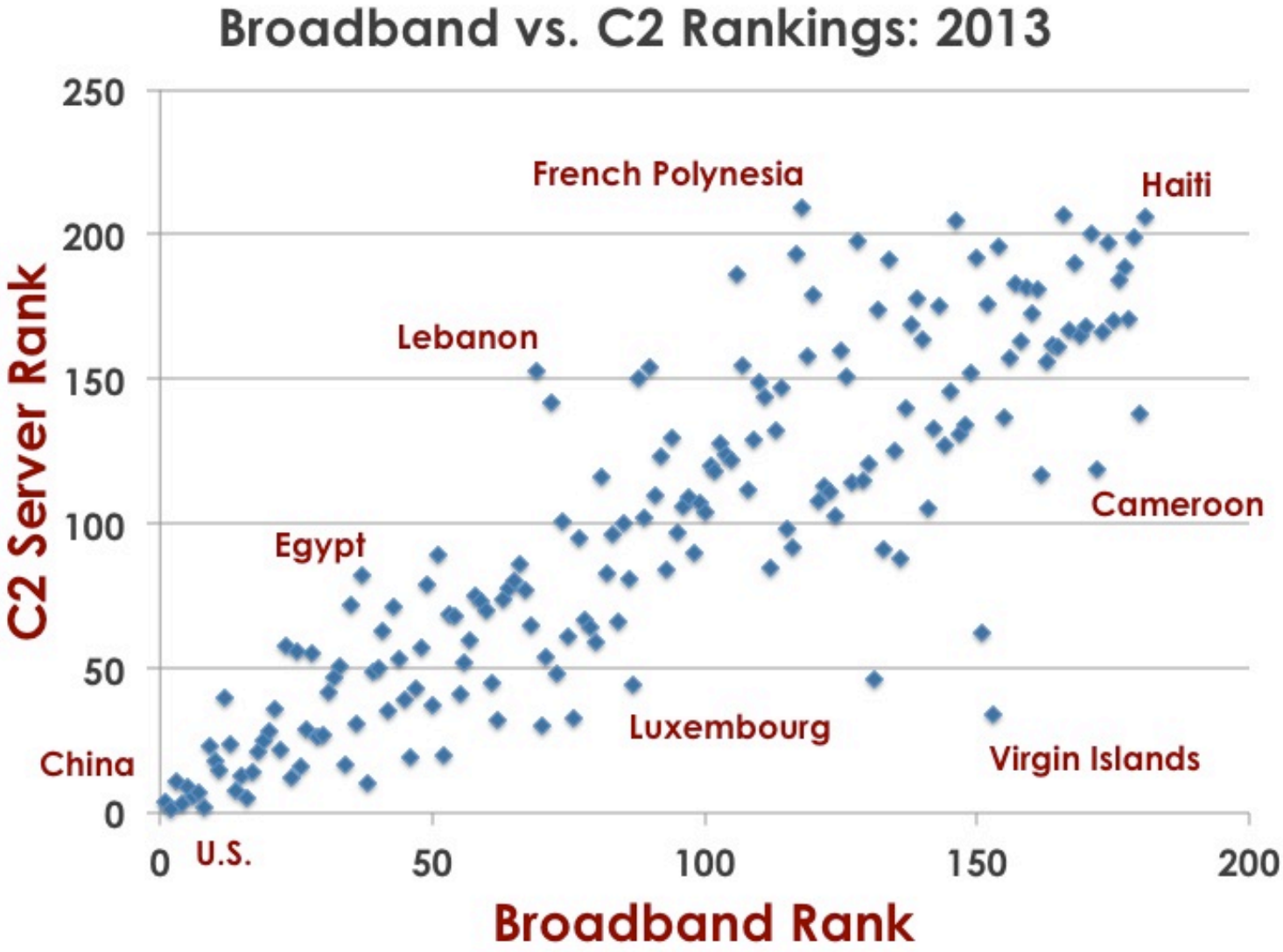
World C2 network map



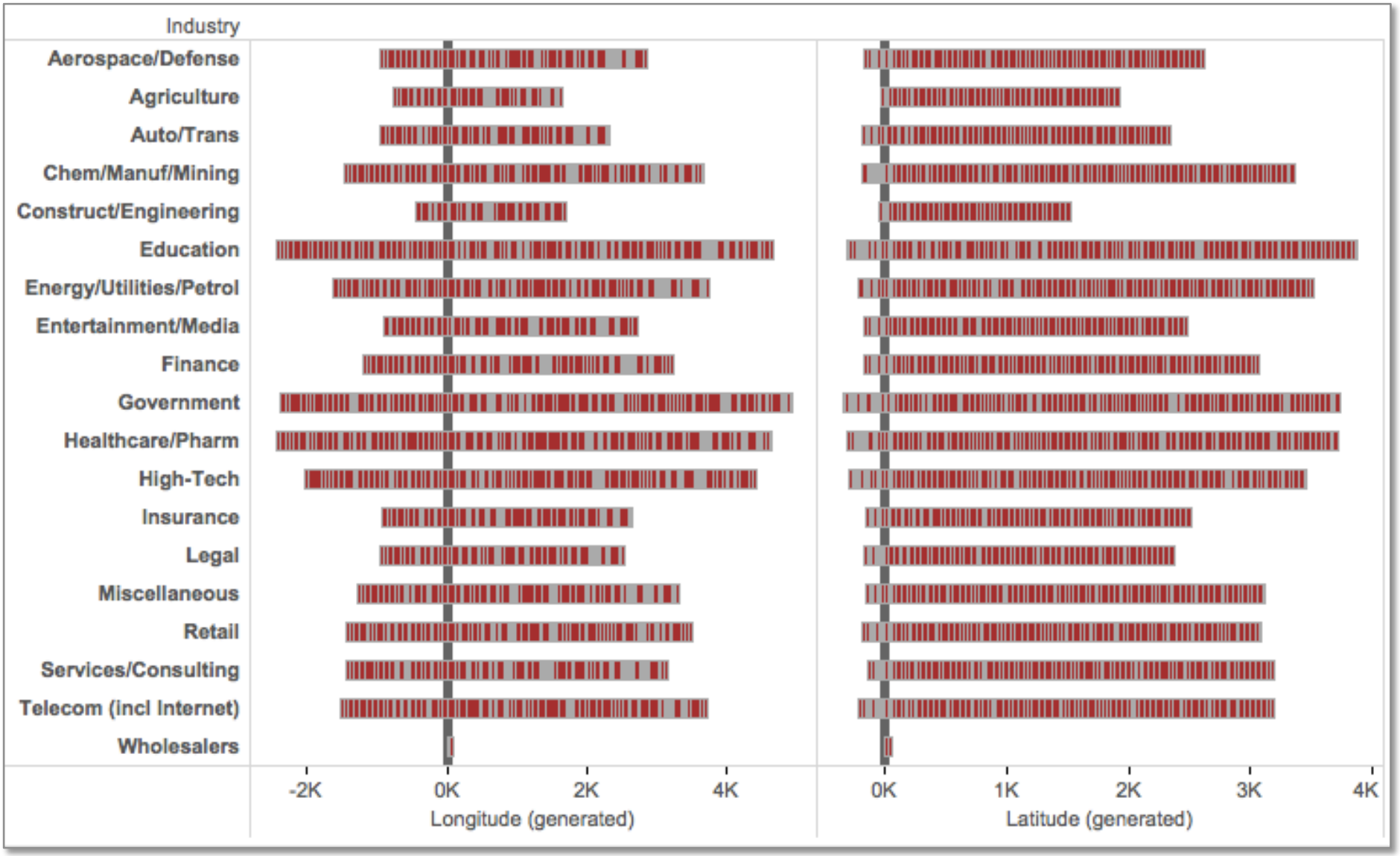
World C2 network heatmap



Connectivity and malware



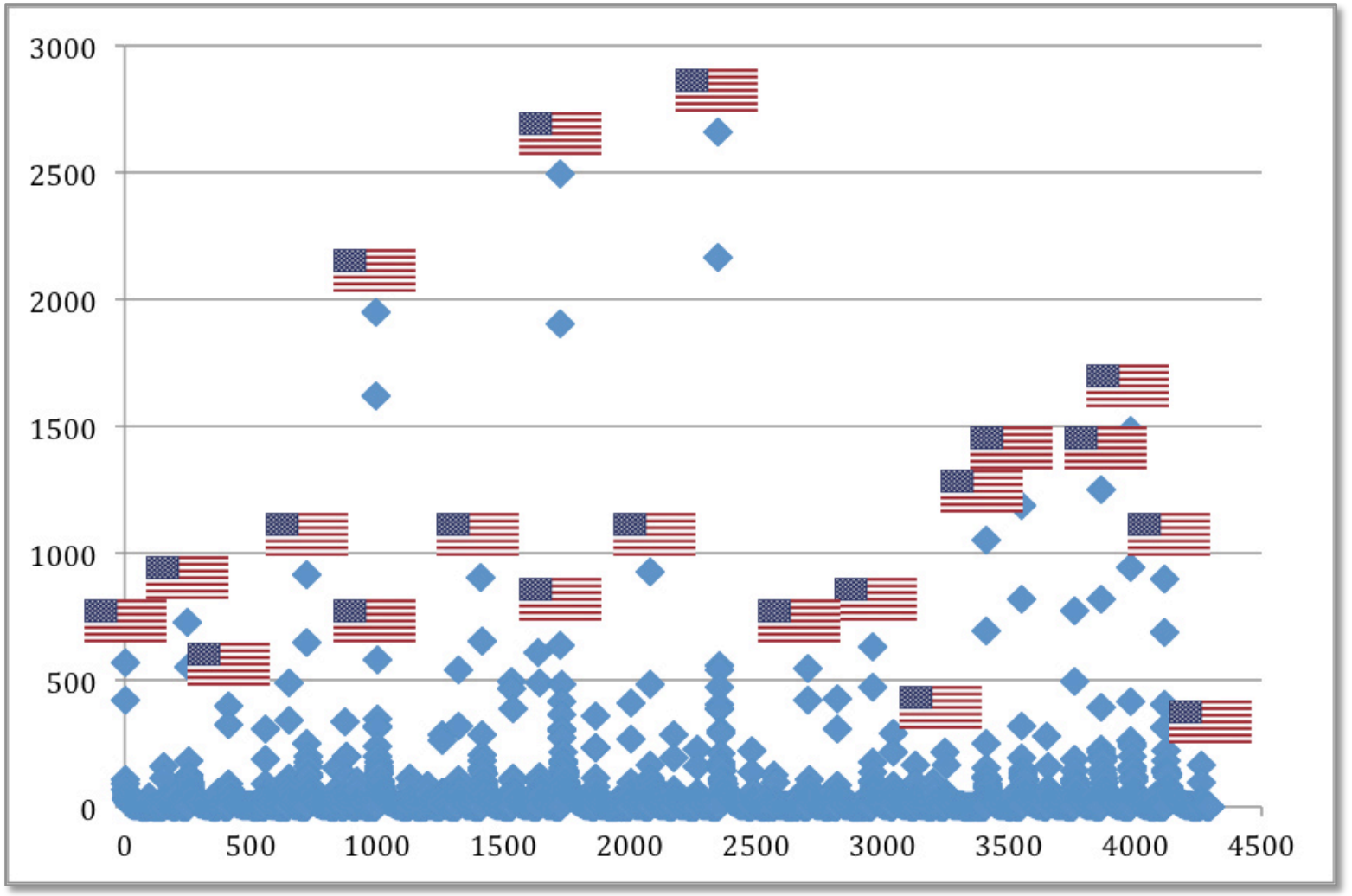
Callbacks by vertical / country



The king of malware

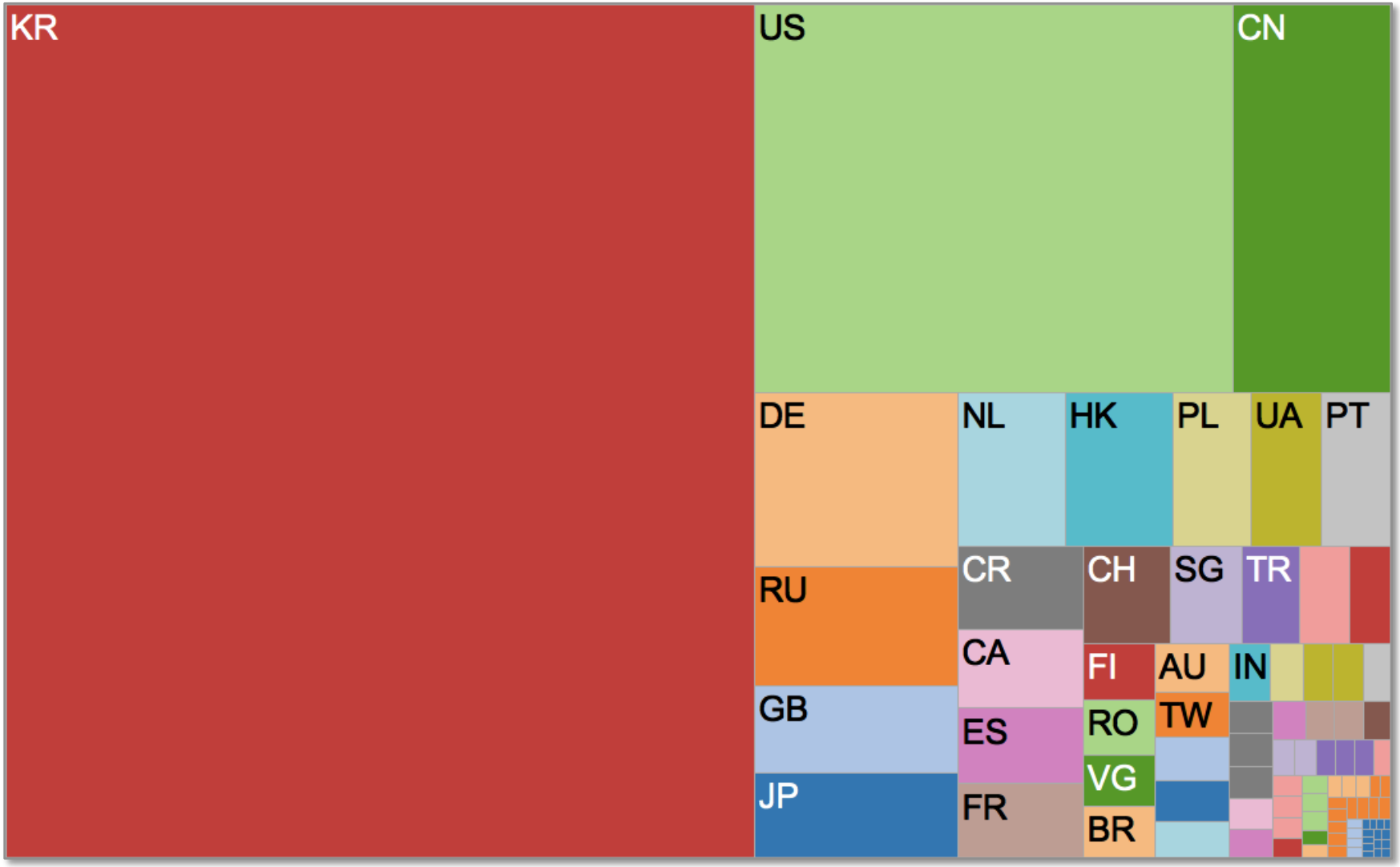
FireEye

USA: the top callback destination

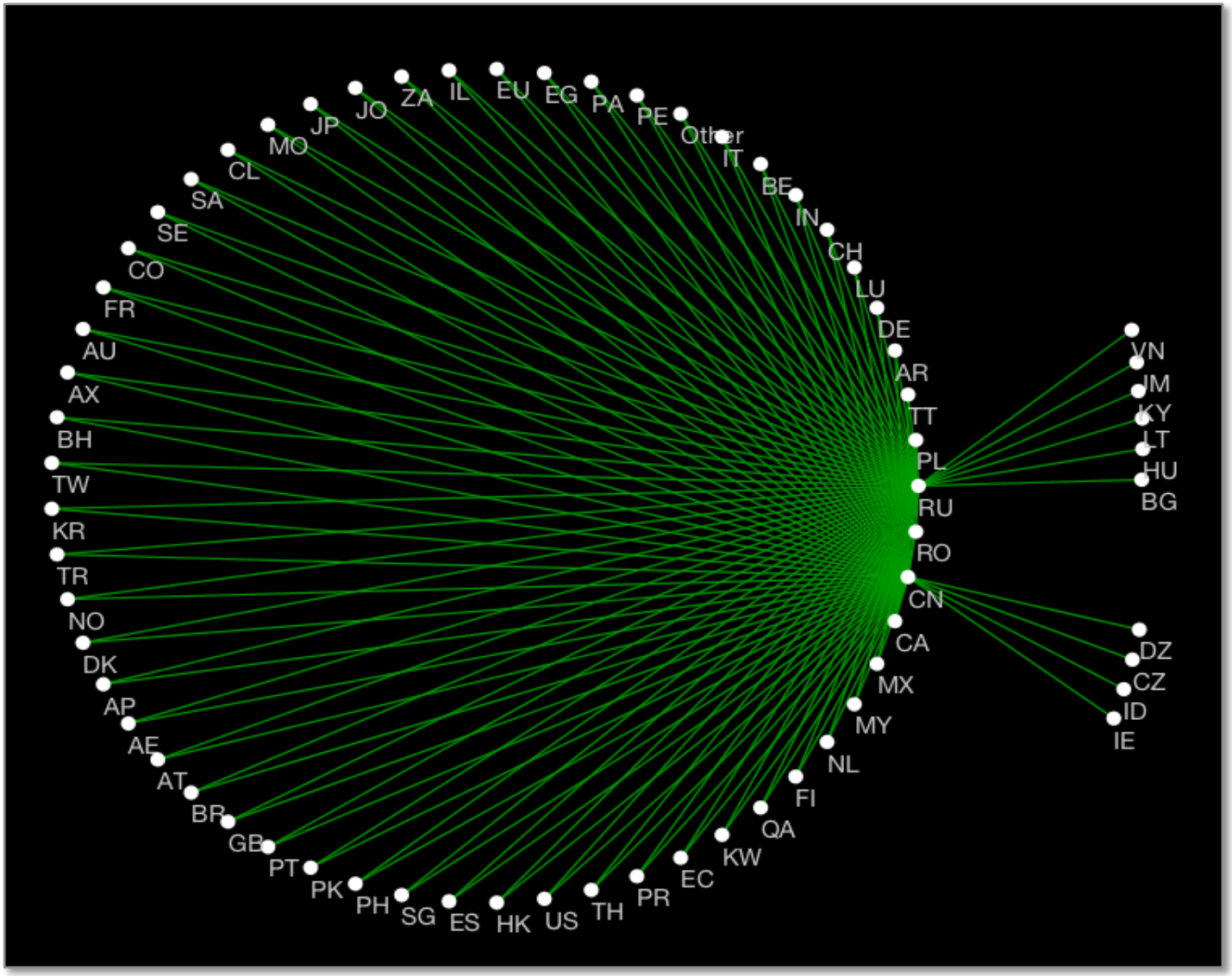


FireEye

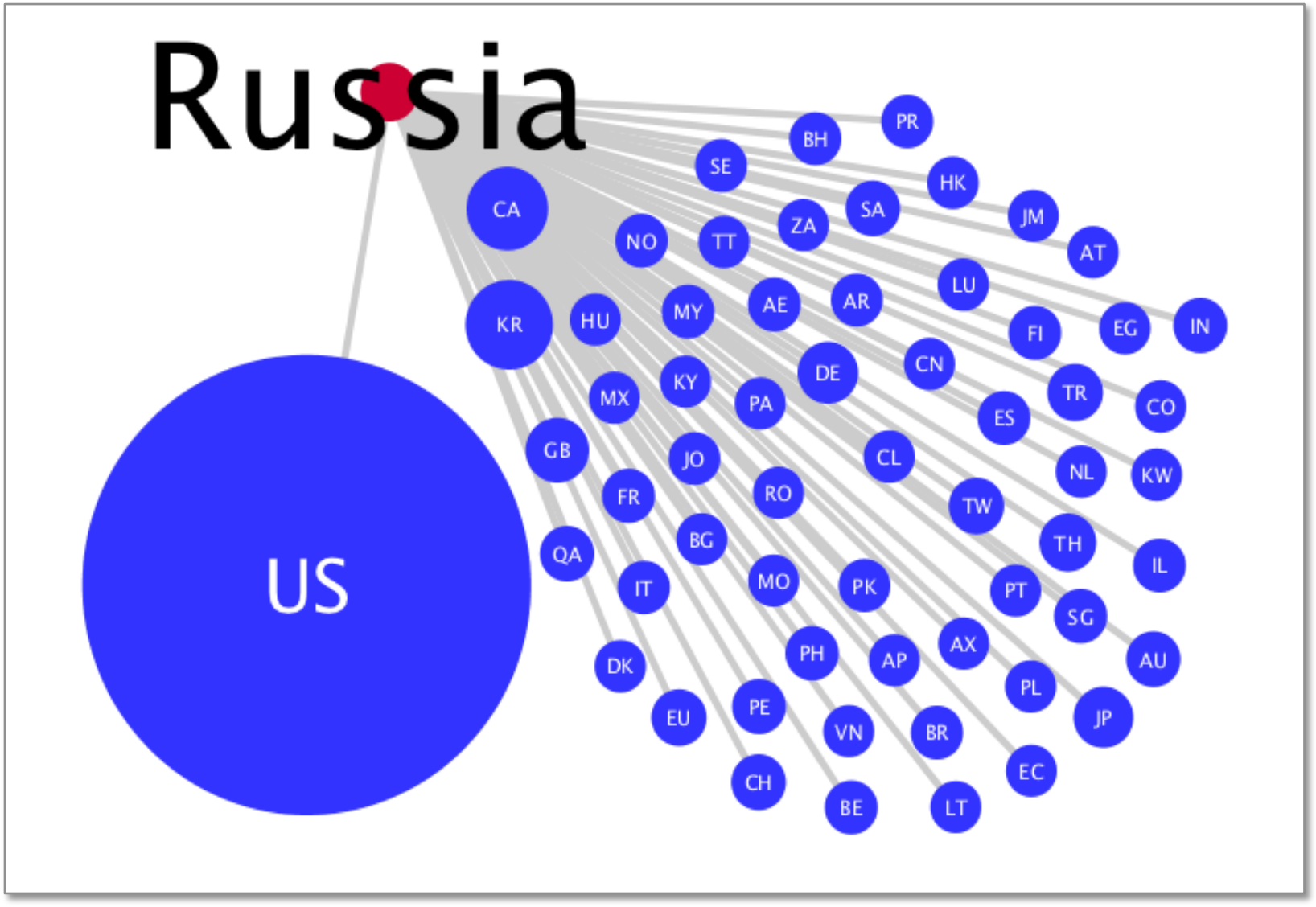
Callback destinations from South Korea



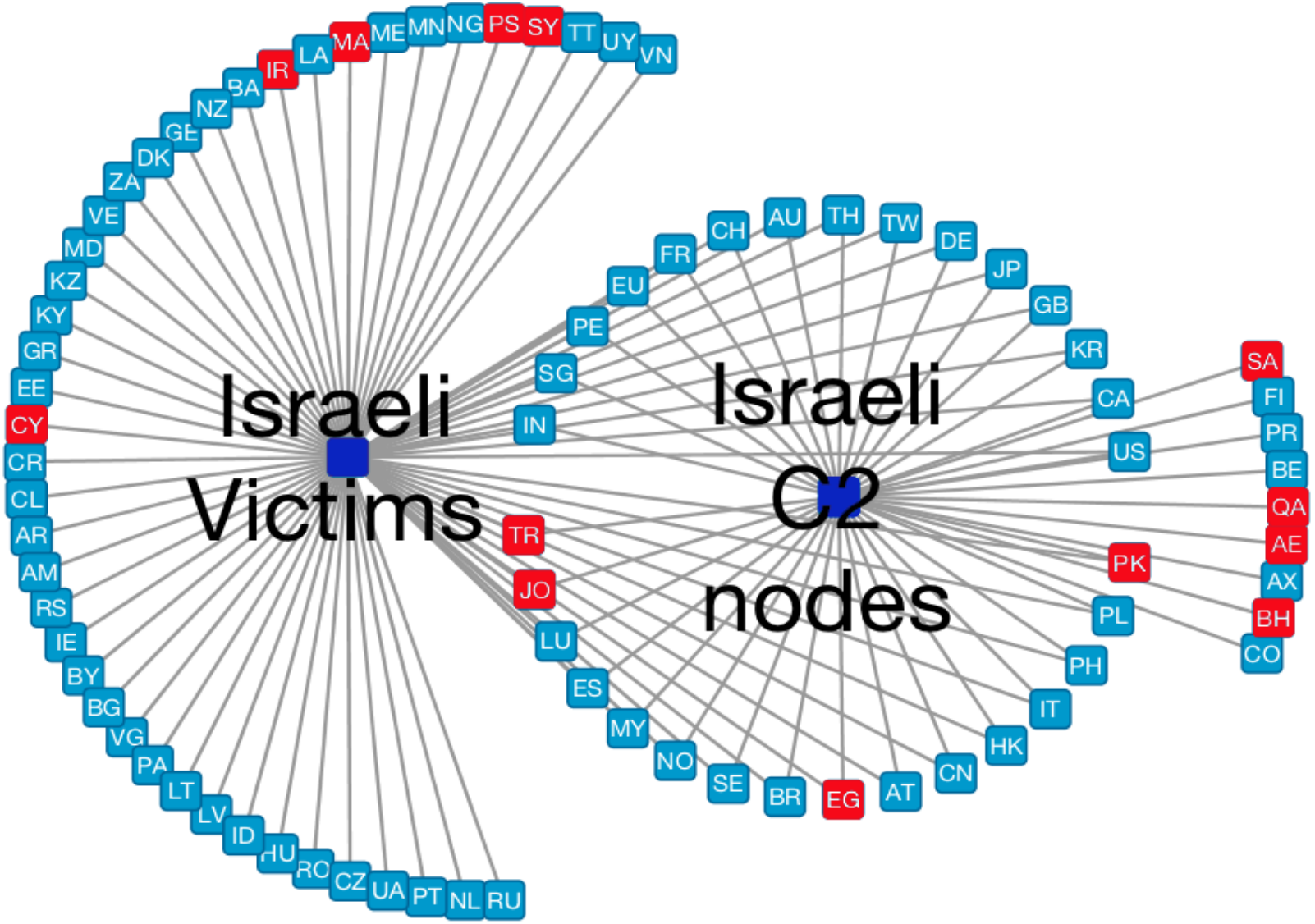
Overlap: investigative headache



USA: also a favorite target



Israel: traffic analysis

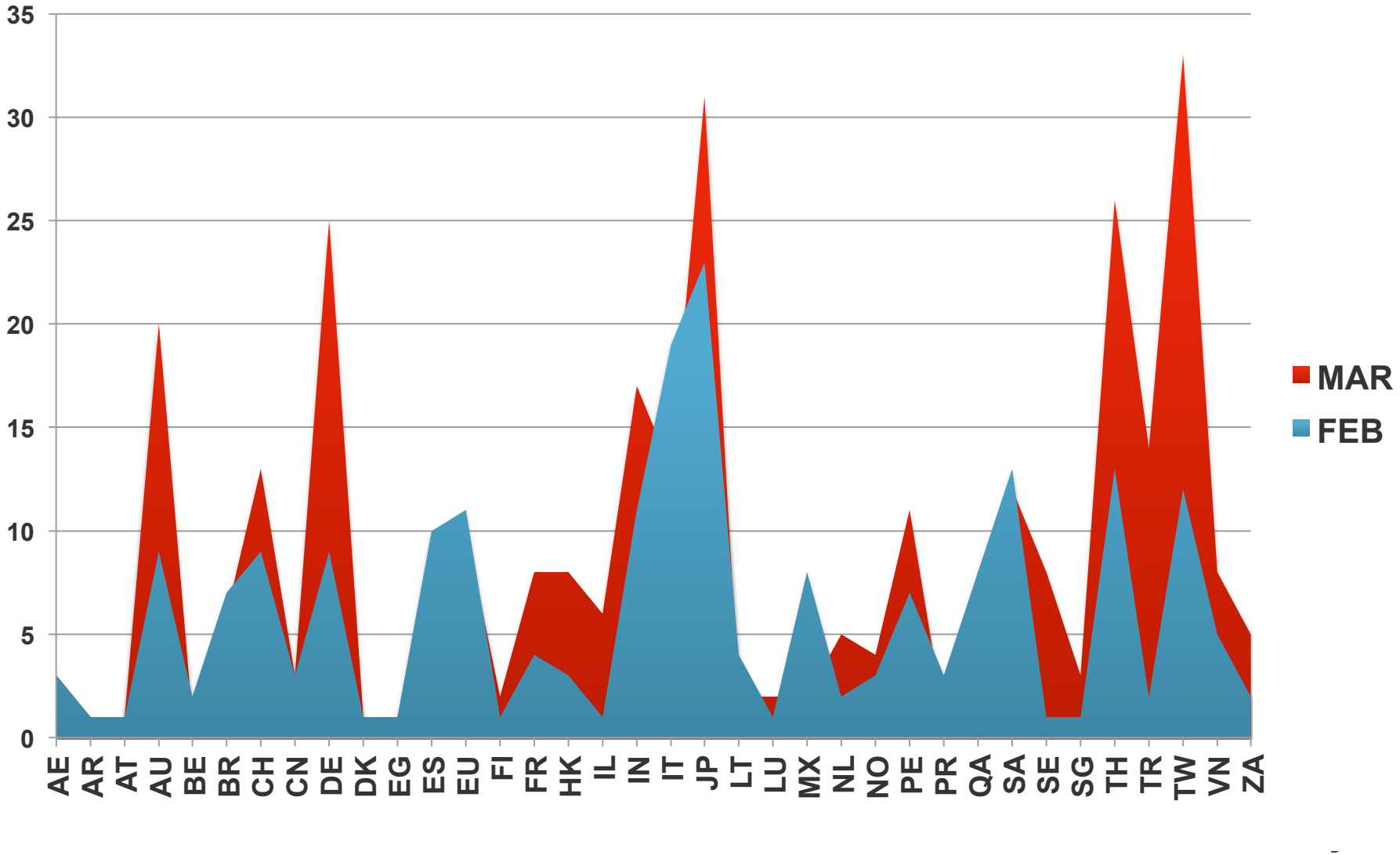


Geopolitical reflection: Ukraine crisis

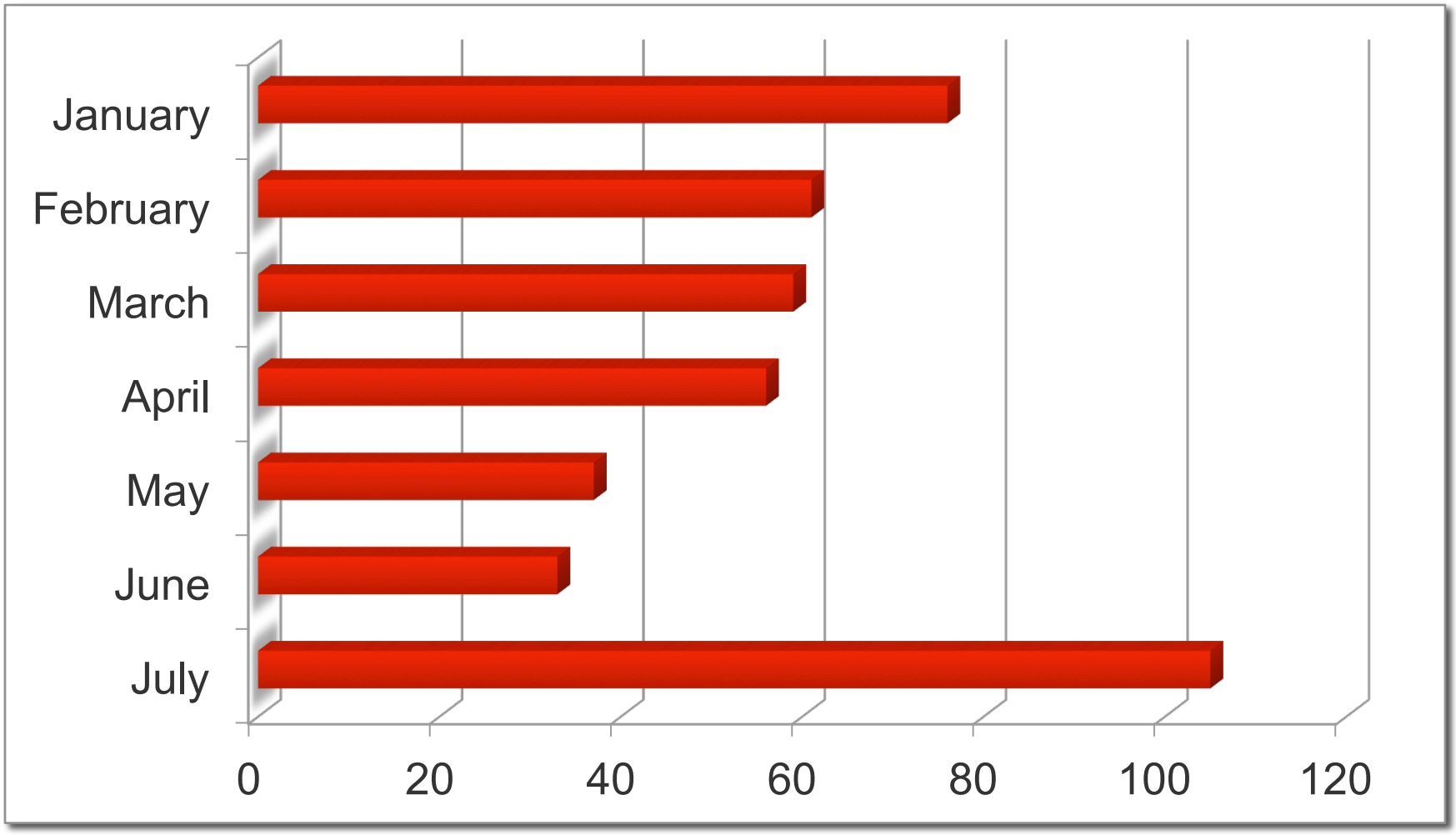
	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr
1	US	US	US	US	US	US	US	US	US	US	US	US	US	US	US	US
2	DE	KR	DE	DE	DE	KR	KR	KR	DE	DE	KR	KR	KR	KR	KR	KR
3	KR	DE	KR	KR	KR	DE	DE	DE	KR	KR	DE	CN	CN	DE	RU	DE
4	CN	CN	CN	CN	NL	NL	GB	CN	CN	CN	CN	NL	DE	CN	DE	RU
5	RU	RU	HK	HK	RU	GB	NL	GB	GB	NL	NL	DE	FR	FR	CN	GB
6	FR	FR	FR	RU	GB	CN	CN	NL	CA	GB	GB	GB	RU	NL	GB	CN
7	NL	GB	NL	NL	CN	RU	CA	CA	NL	RU	CA	FR	NL	RU	NL	NL
8	GB	TR	RU	GB	CA	CA	RU	RU	RU	CA	RU	RU	GB	GB	FR	UA
9	JP	NL	CA	FR	FR	FR	JP	FR	TR	JP	FR	CA	CA	UA	UA	FR
10	PL	CA	TH	CA	HK	HK	PL	JP	FR	UA	UA	UA	UA	CA	CA	CA
11	CA	ID	GB	IT	IN	TR	FR	PL	UA	TR	JP	RO	PT	PT	HK	PL
12	IN	JP	BG	JP	UA	JP	HK	HK	JP	RO	TR	PL	RO	PL	PT	PT
13	RO	HK	TR	PL	PL	IT	UA	UA	PT	CZ	PT	PT	TR	JP	RO	JP
14	IT	UA	UA	UA	JP	PL	PT	CZ	IT	IE	AU	TR	PL	RO	TR	TR
15	UA	PL	JP	BG	TR	AR	IT	BR	CZ	FR	GE	IN	JP	TR	PL	RO
16	ID	RO	IT	TR	PT	UA	TR	IT	PL	PT	HK	JP	BR	CZ	JP	HK
17	HK	IN	PL	IN	BG	RO	VN	TR	HK	PL	PL	ES	CZ	BR	CZ	CZ
18	TW	PA	ID	TH	IT	IN	RO	PT	ES	IT	RO	AU	IT	IT	ES	IT
19	TR	IT	LT	TW	TH	AU	IN	AU	BR	SE	ES	EU	ES	ES	BR	BR
20	HU	TH	IN	CH	RO	BG	SD	TW	IN	HK	IN	HK	HK	HK	IT	TH
	2013	2013	2013	2013	2013	2013	2013	2013	2013	2013	2013	2013	2014	2014	2014	2014

FireEye

RU-UA unique callbacks by country

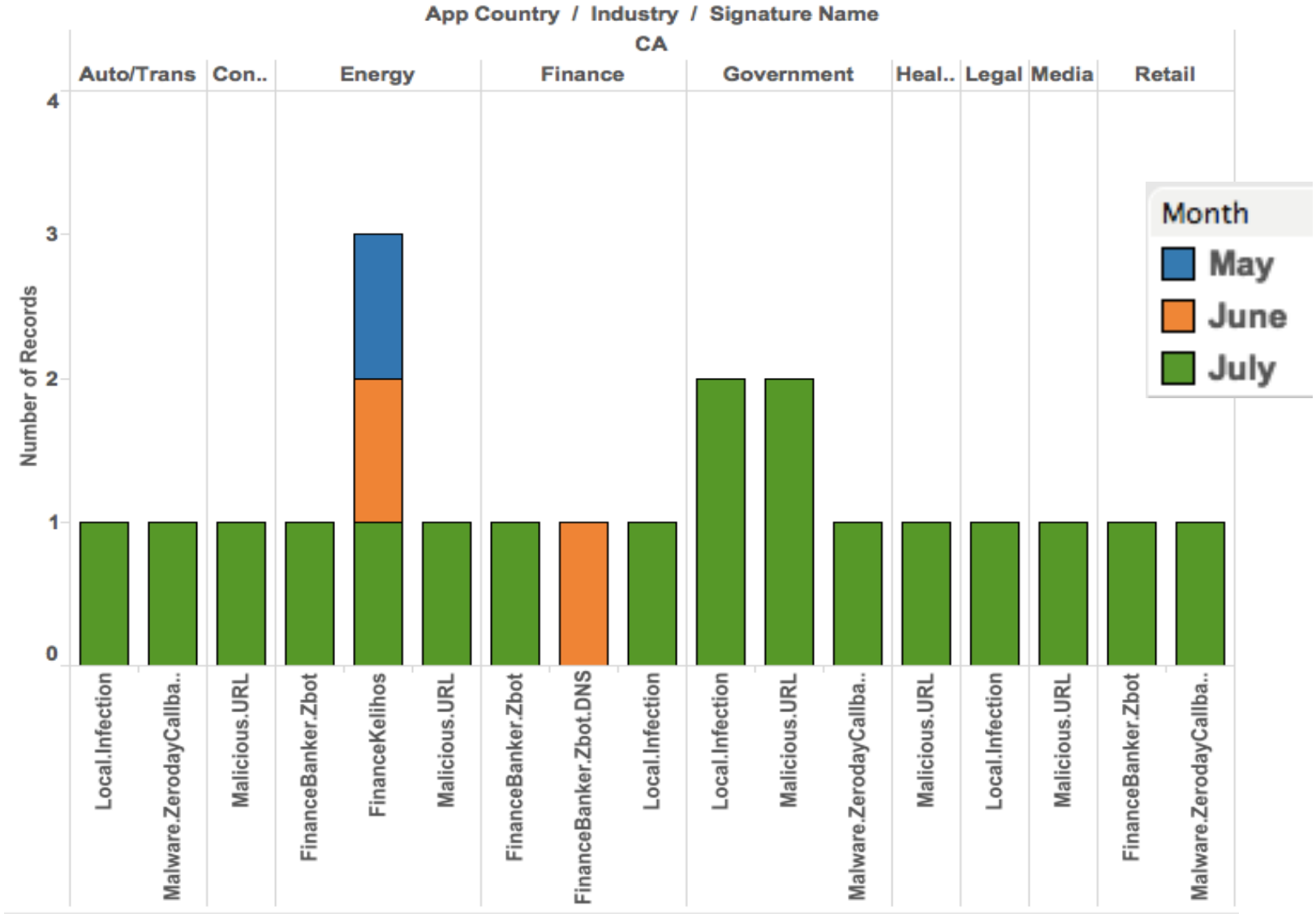


Geopolitical reflection: Israel-Gaza crisis



FireEye

Unique callbacks: CA to IL (2014)



FireEye

Leviathan: Command and Control Communications on Planet Earth

Dr. Kenneth Geers
2501
Kevin Thompson
FireEye