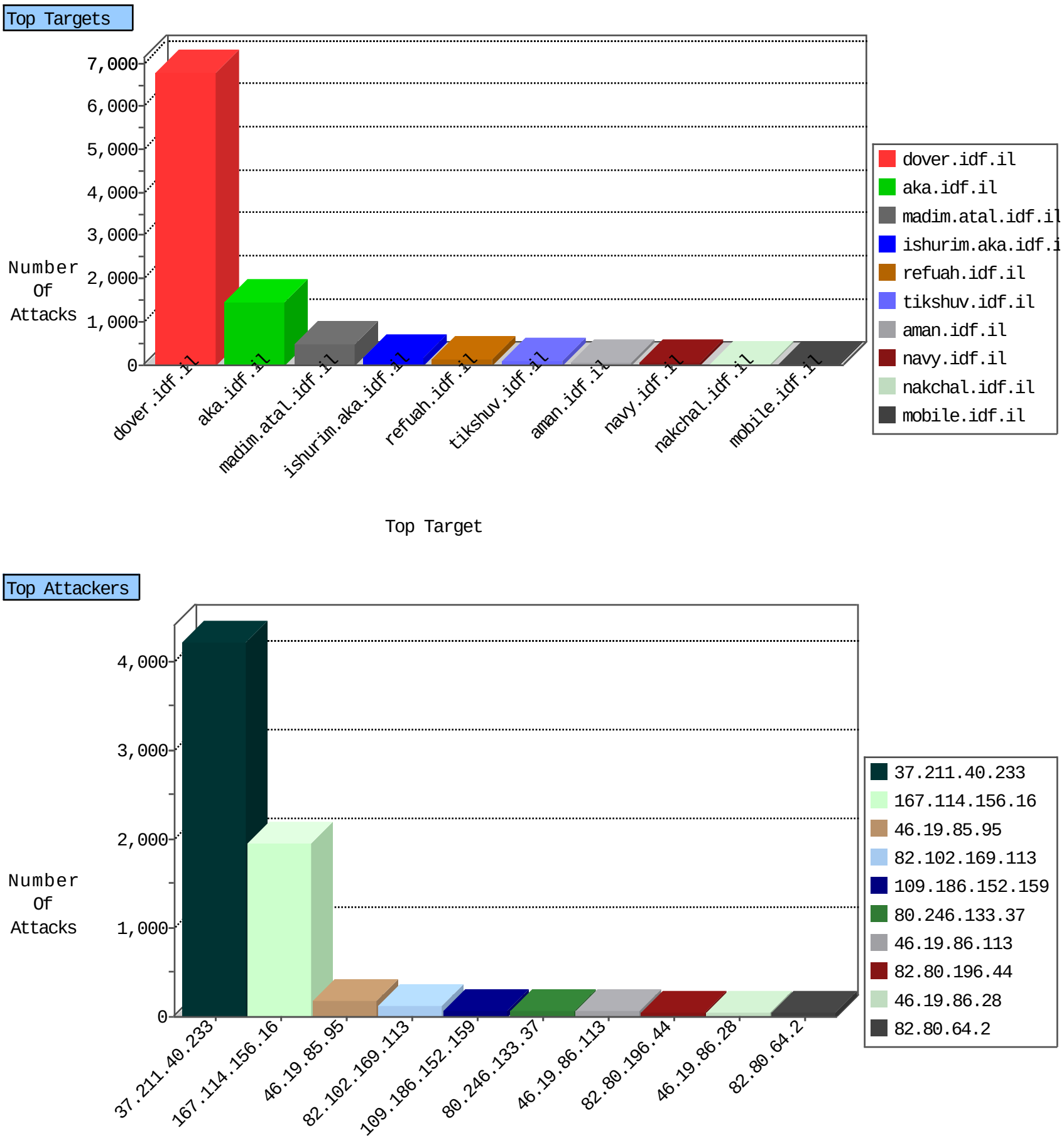
01-14-2016-12:04:07 to 01-14-2016-13:04:07

IDF Under Attack Daily Report



01-14-2016-12:04:07 to 01-14-2016-13:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3019
79.176.107.179	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	24
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
66.249.93.99	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
66.249.93.107	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

01-14-2016-12:04:07 to 01-14-2016-13:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
191.252.61.244	Brazil	147.237.76.86	navy.idf.il	C041: HTTP: Access to - index.php?option=com_jce	Block	1

01-14-2016-12:04:07 to 01-14-2016-13:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.130.39	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
212.199.10.173	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
109.251.56.171	147.237.77.212	Ukraine	e.dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.179.98.238	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.4.11	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.143.147.38	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.216	147.237.0.17		m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
24.121.225.29	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

01-14-2016-12:04:07 to 01-14-2016-13:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.211.40.233	Qatar	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1510
37.211.40.233	Qatar	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1397
37.211.40.233	Qatar	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	881
37.211.40.233	Qatar	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	169
80.246.133.37	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	67
37.211.40.233	Qatar	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	60
37.211.40.233	Qatar	147.237.77.216	dover.idf.il	SYN Attack		reject	53
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
46.19.86.28	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	41
82.80.64.2	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
37.211.40.233	Qatar	147.237.77.216	dover.idf.il	drop		drop	28
37.211.40.233	Qatar	147.237.77.216	dover.idf.il	Bad TCP sequence		alert	27
37.211.40.233	Qatar	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	27
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
176.13.20.255	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
46.19.86.94	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
176.13.20.255	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	18
37.211.40.233	Qatar	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
81.218.106.146	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
109.253.129.123	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
46.19.86.60	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
85.130.223.86	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
85.250.144.133	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
91.227.71.250	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
62.90.203.122	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	13
82.80.64.2	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	13
109.253.129.123	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.19.86.94	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
89.139.158.239	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
66.249.93.99	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.54.33.151	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
84.94.171.195	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
2.54.33.151	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
66.249.93.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
91.193.51.38	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
2.52.176.228	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
66.249.93.107	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
80.246.137.174	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
37.26.149.253	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
66.249.64.119	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
212.179.155.129	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
194.114.146.227	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
2.54.167.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.103.67.69	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
85.64.16.248	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
2.54.49.82	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.86.148	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	110
46.19.85.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	73
82.102.169.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	71
109.186.152.159	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 109.186.152.159	Block	69
46.19.86.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	63
82.102.169.113	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 82.102.169.113	Block	54
176.13.18.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
37.211.40.233	Qatar	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 37.211.40.233	Block	34
80.246.137.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
46.19.86.70	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	30
94.159.155.126	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	17
5.22.130.101	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	14
176.13.9.147	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	7
192.118.12.102	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	7
109.253.137.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.86.97	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	6
149.78.237.199	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 149.78.237.199	Block	6
46.19.86.28	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	5
213.57.56.205	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	5
5.29.67.49	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	5
46.19.85.95	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 46.19.85.95	Block	4
213.184.119.136	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 213.184.119.136	Block	4
89.138.186.196	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
109.65.62.81	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
46.19.85.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
2.54.177.52	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	4
2.54.38.99	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
89.138.116.251	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
2.54.180.95	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
46.19.86.60	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
2.54.14.224	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
77.125.6.83	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
37.26.149.227	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
212.179.241.235	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
87.69.118.87	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
2.54.168.169	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
2.54.142.241	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
79.180.204.48	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
46.121.102.190	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
46.19.86.177	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
109.253.156.0	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
46.19.85.103	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
77.125.12.22	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
2.52.156.73	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
217.194.198.94	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
46.19.85.221	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
176.13.19.26	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
37.26.147.173	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
79.179.199.80	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
46.19.86.147	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3

01-14-2016-12:04:07 to 01-14-2016-13:04:07