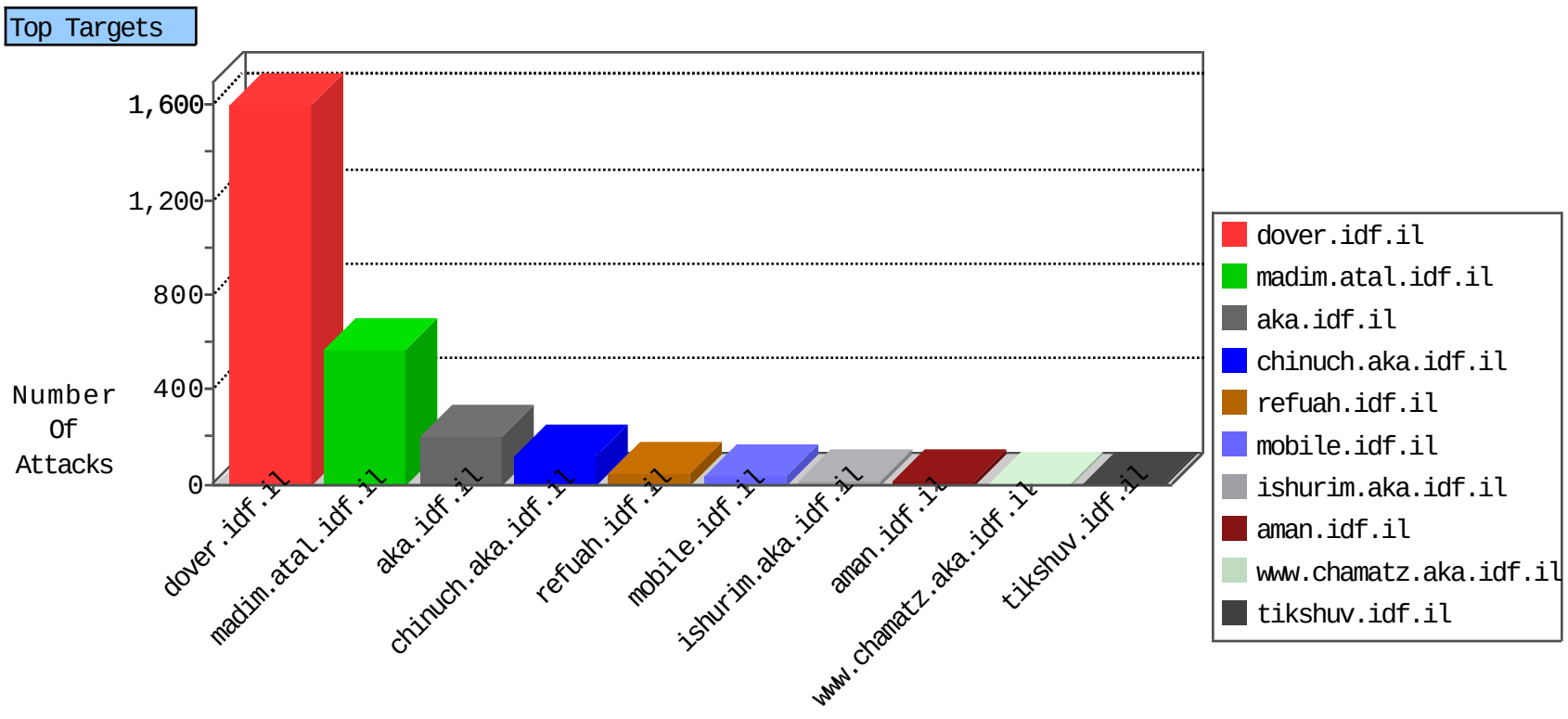
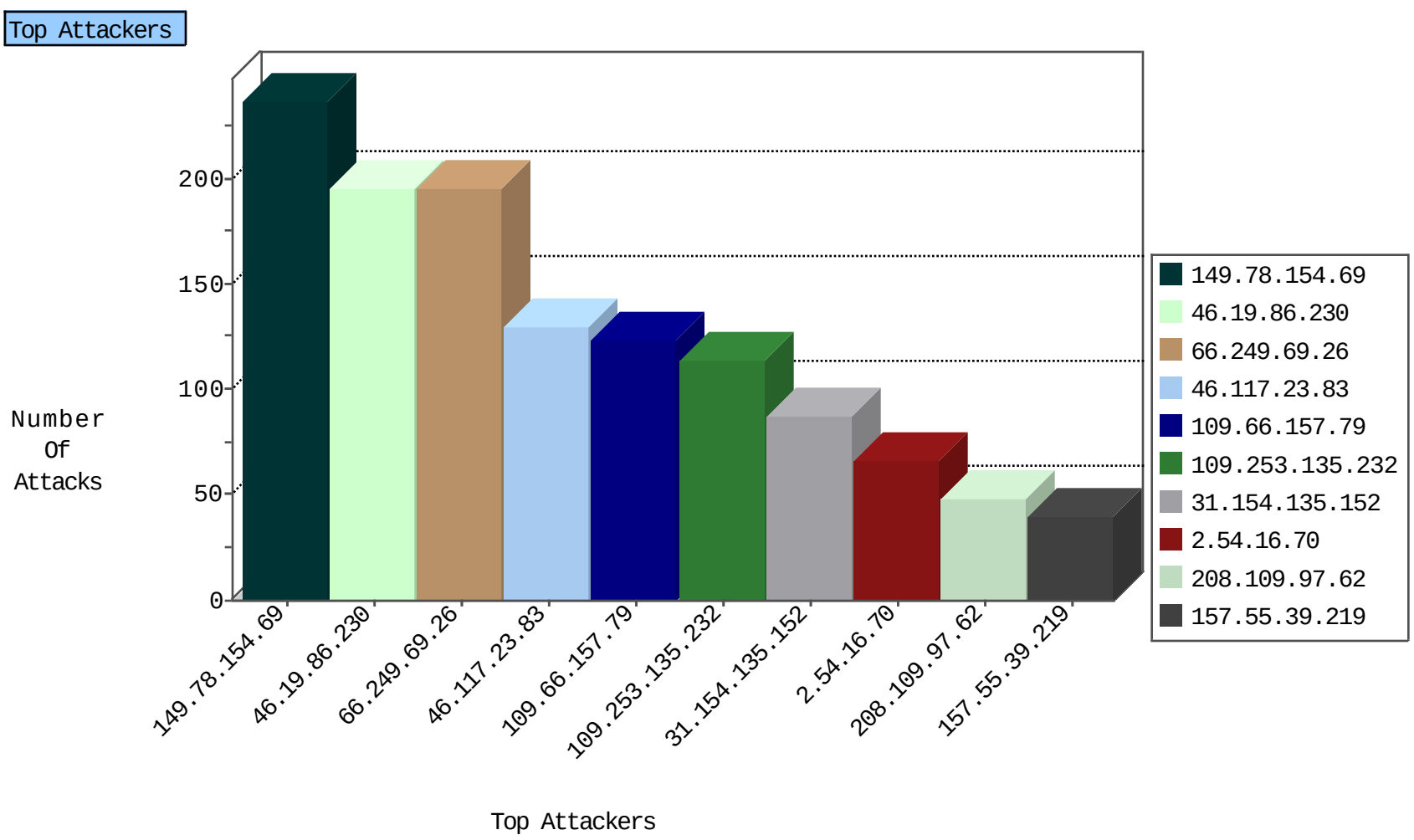
02-13-2016-15:04:03 to 02-13-2016-16:04:03

IDF Under Attack Daily Report





02-13-2016-15:04:03 to 02-13-2016-16:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
1.93.51.221	China	147.237.76.34	yohalan.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1

02-13-2016-15:04:03 to 02-13-2016-16:04:03

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

02-13-2016-15:04:03 to 02-13-2016-16:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	10
113.59.33.61	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -f -sS	1
111.207.243.73	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
40.76.83.120	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
1.93.51.221	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
120.24.54.239	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
113.59.33.61	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
111.207.243.73	147.237.8.45	China	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
40.76.83.120	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
128.199.62.41	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
113.59.33.61	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -sS window 2048	1

02-13-2016-15:04:03 to 02-13-2016-16:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
109.66.157.79	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	123
84.229.174.72	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	40
46.19.86.183	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	35
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
109.66.213.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	13
46.121.107.219	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	11
46.19.86.59	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
31.210.187.184	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
208.109.97.62	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
5.22.129.89	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.181.149.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
132.66.237.70	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
217.132.37.237	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.141.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.46.41.80	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.120.126.31		147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
213.57.146.214	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
91.200.12.7	Ukraine	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	4
91.200.12.7	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
46.19.85.167	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.181.4.169	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.188.13	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.126.203.47	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.222.198	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.69.122.113	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
185.3.147.121	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.194	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.178.101.20	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.69.122.113	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.221	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.64.8.123	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.130.68	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.158	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.144.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.12.99	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.148.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.137.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.142.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.147.178	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.99.162	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.191.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.184.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-13-2016-15:04:03 to 02-13-2016-16:04:03

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
109.66.58.41	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.189	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
62.219.132.230	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
5.29.52.169	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	236
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	195
46.117.23.83	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	114
46.19.86.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
109.253.135.232	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	84
31.154.135.152	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	78
2.54.16.70	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	66
46.19.86.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	63
208.109.97.62	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	42
157.55.39.219	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	40
52.16.5.197	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	37
2.54.136.100	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	37
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	35
109.253.135.232	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.135.232	Block	30
66.102.8.238	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
132.66.231.153	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	27
2.54.191.235	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	26
50.87.144.145	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
185.32.179.54	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
176.13.13.72	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	20
84.108.138.192	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	20
109.186.26.103	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	20
213.57.50.164	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	17
87.68.155.196	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	17
46.117.23.83	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	16
46.121.74.73	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
85.250.224.65	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
185.32.179.66	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
79.183.197.17	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
37.26.149.178	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
78.84.166.222	Latvia	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
46.19.86.230	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 46.19.86.230	Block	12
77.126.9.162	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
46.19.85.182	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
31.210.187.184	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
2.54.178.246	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
192.249.66.247	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
2.54.149.143	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
109.186.185.226	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	9
45.35.64.142		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	9
2.54.28.172	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	9
31.154.135.152	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	9
89.138.34.59	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
79.179.104.86	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
46.19.86.39	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
176.13.22.149	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
46.121.96.117	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
5.29.236.142	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6

02-13-2016-15:04:03 to 02-13-2016-16:04:03