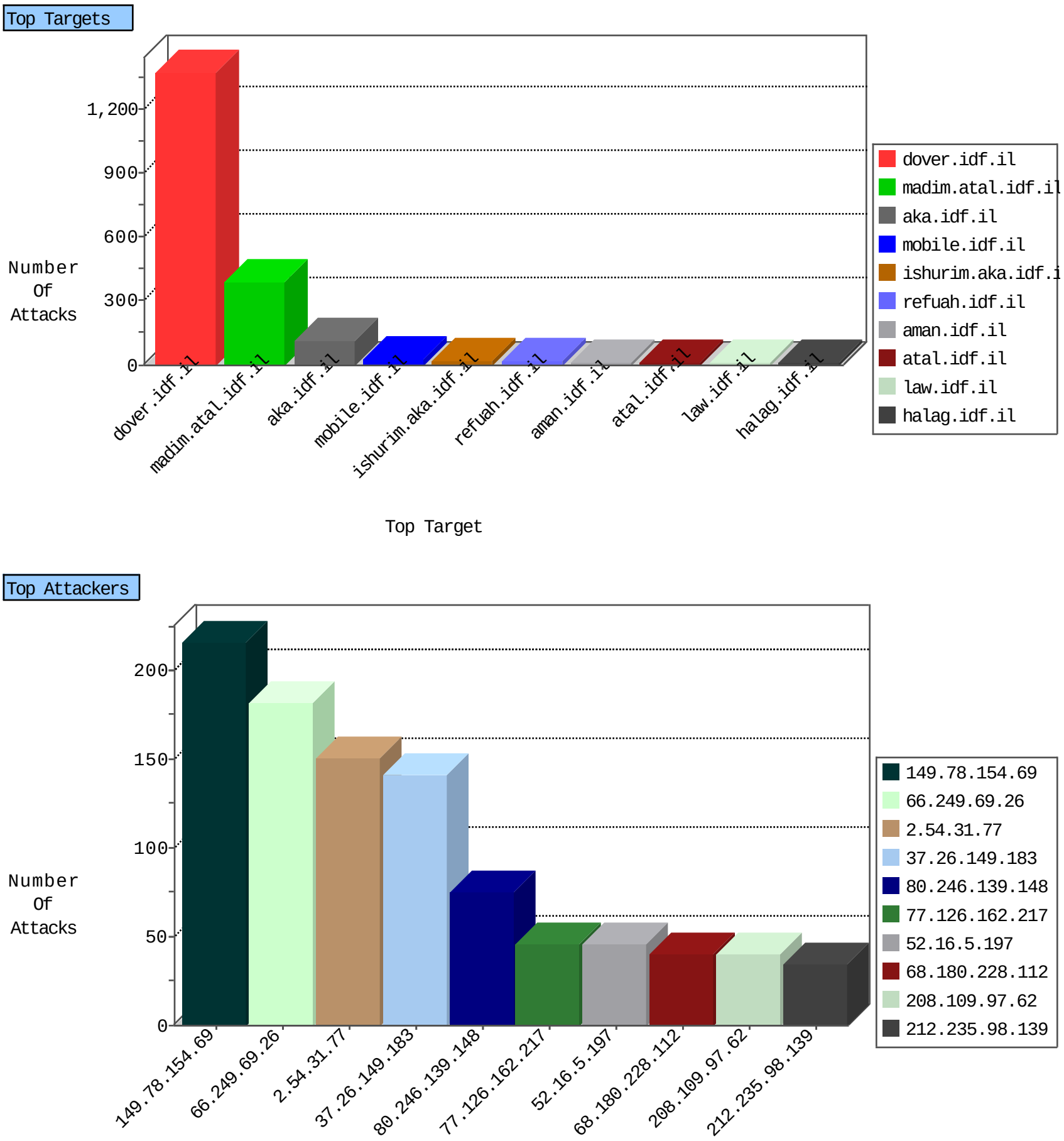
02-14-2016-07:04:06 to 02-14-2016-08:04:06

IDF Under Attack Daily Report



02-14-2016-07:04:06 to 02-14-2016-08:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
23.228.101.234	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
115.38.229.3	Japan	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1

02-14-2016-07:04:06 to 02-14-2016-08:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-14-2016-07:04:06 to 02-14-2016-08:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
59.45.79.117	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
50.204.188.142	147.237.0.33	United States	idf.il	ET SCAN NMAP -f -sS	1
218.246.0.97	147.237.77.74	China	law.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
50.204.188.142	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 2048	1
130.211.100.171	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1

02-14-2016-07:04:06 to 02-14-2016-08:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
213.57.143.236	Israel	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
2.54.58.242	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
37.26.149.237	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.19	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
2.54.59.46	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.246.130.166	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
79.181.23.31	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
79.176.224.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.13.23.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.156	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.156	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.229	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.183.33.95	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.229	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
208.109.97.62	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
212.76.127.10	Israel	147.237.77.234	halag.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
46.19.85.215	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.215	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.215	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
37.26.149.183	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence		alert	4
46.19.85.215	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
37.26.149.183	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence		monitor	4
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	3
2.54.155.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.6	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
82.80.157.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.195.27	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
80.178.206.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.163.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.235.98.139	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.26.147.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.230.86.76	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.26.148.185	Israel	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
46.19.86.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.205.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
37.26.148.188	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.144	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.19	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.26.149.133	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
176.13.9.138	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
212.235.98.139	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
203.133.168.41	Korea, Republic of	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
66.249.64.181	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.19	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
66.249.66.60	United States	147.237.76.86	navy.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	214
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	180
37.26.149.183	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	131
2.54.31.77	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	100
80.246.139.148	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	61
2.54.31.77	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	51
77.126.162.217	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	46
52.16.5.197	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	46
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	39
208.109.97.62	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	34
176.13.17.202	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	30
157.55.39.159	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	30
212.235.98.139	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
157.55.39.19	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	27
50.87.144.145	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
203.133.170.12	Korea, Republic of	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	21
40.77.167.100	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	21
192.249.66.247	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	21
5.29.87.14	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	20
109.253.205.235	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
131.253.25.157	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
176.13.18.137	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
2.54.134.152	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
80.246.139.148	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	14
2.54.58.242	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
79.176.211.34	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
2.54.30.110	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
212.179.21.194	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	11
46.19.85.144	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	9
82.81.52.131	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
109.253.209.175	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
84.95.212.141	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
45.35.64.142		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
46.19.86.61	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
185.120.125.44		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
176.13.12.199	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
37.26.148.185	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
176.13.7.160	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
148.177.129.212	Europe	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
176.13.16.213	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
109.64.179.210	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
109.253.139.69	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
79.180.214.11	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
81.218.251.250	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	5
46.19.86.49	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
85.113.98.234	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
2.54.25.203	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
31.168.30.69	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4

02-14-2016-07:04:06 to 02-14-2016-08:04:06