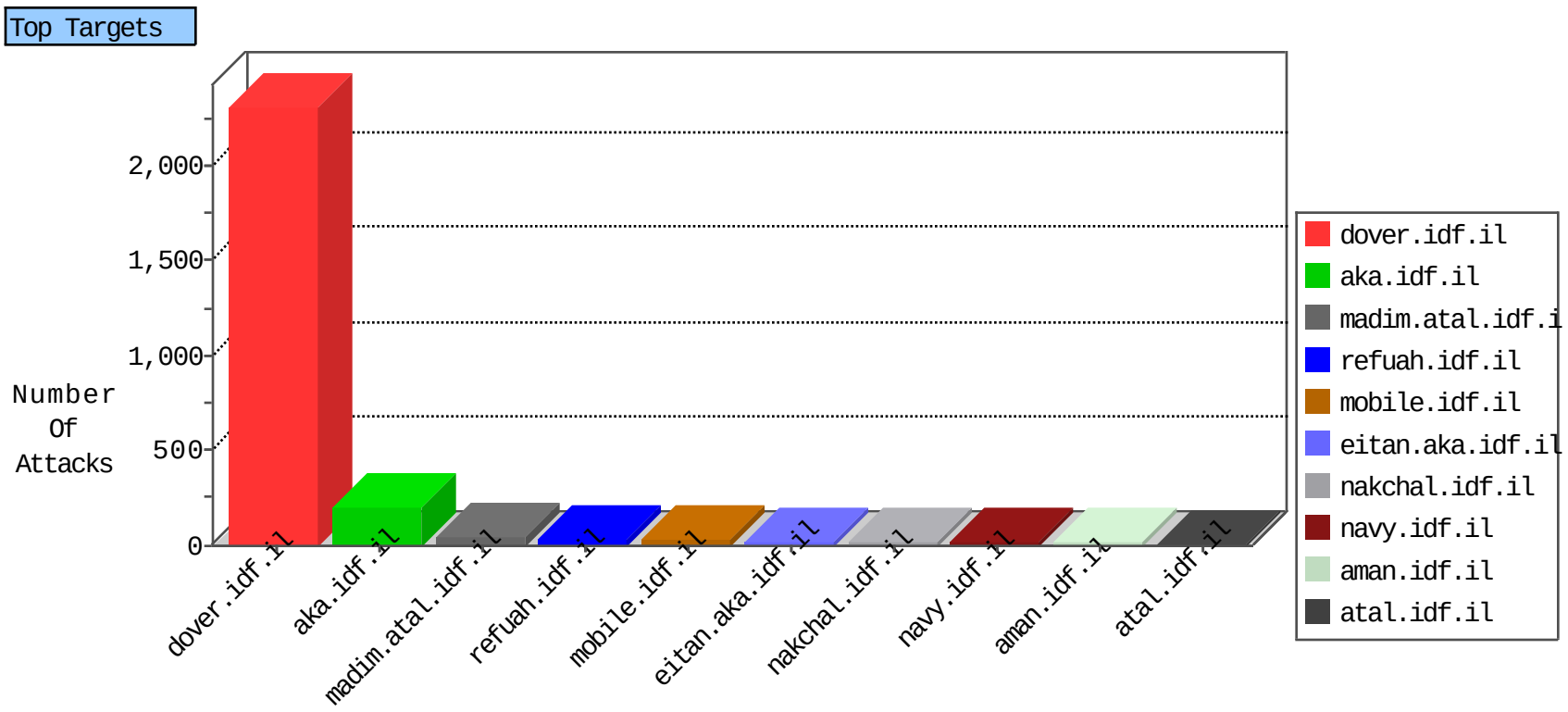
02-13-2016-21:04:00 to 02-13-2016-22:04:00

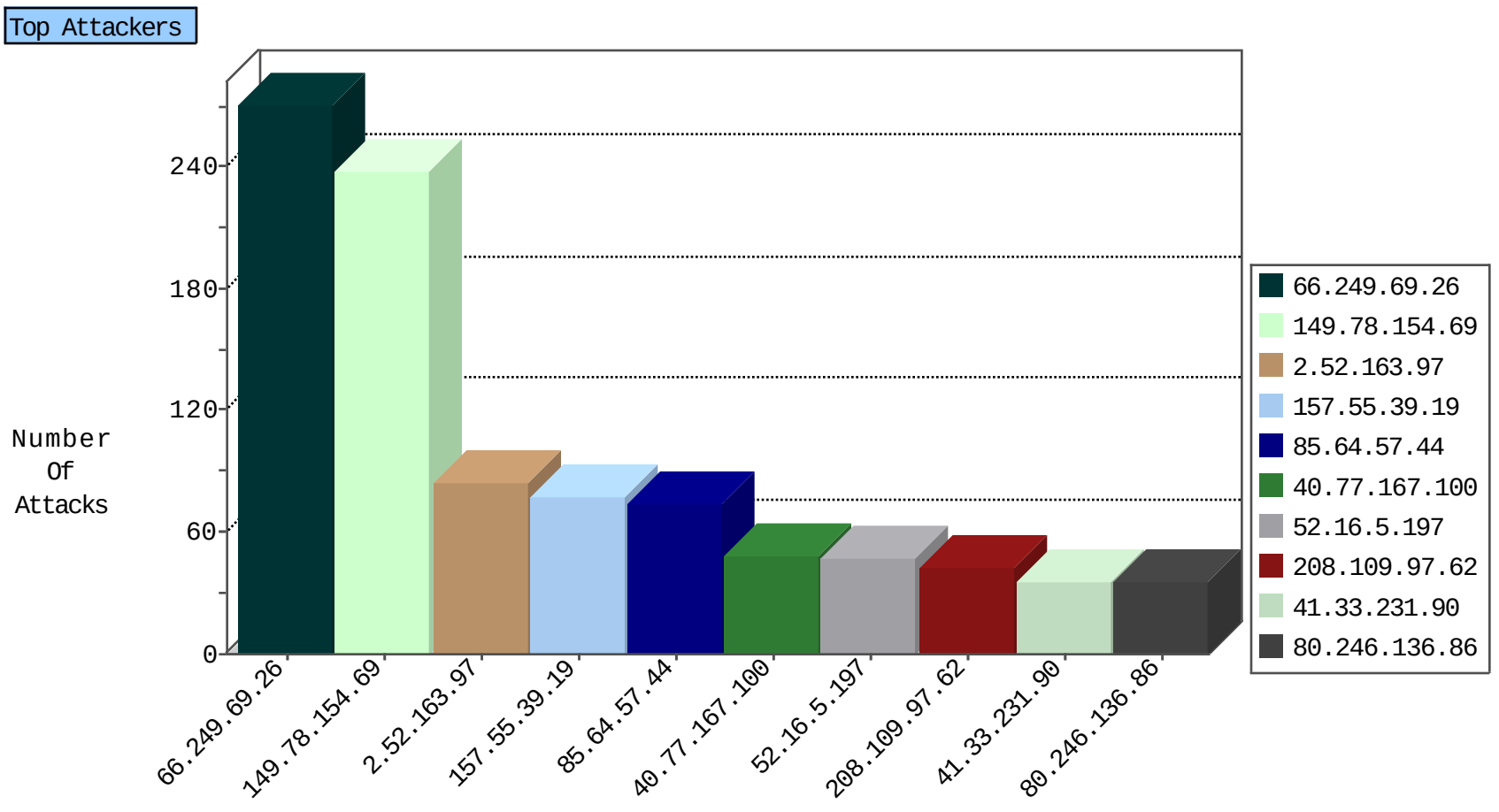
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

02-13-2016-21:04:00 to 02-13-2016-22:04:00

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	4
109.64.104.196	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
185.130.5.224		147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
89.248.174.4	Netherlands	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
198.55.103.19	United States	147.237.0.200	m4u.idf.il	JLM_Purple_Con_Limit_Http	drop	1
89.248.174.4	Netherlands	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1

02-13-2016-21:04:00 to 02-13-2016-22:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
155.94.254.143	United States	147.237.76.30	himush.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1

02-13-2016-21:04:00 to 02-13-2016-22:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
193.109.69.219	147.237.77.216	Russian Federation	dover.idf.il	Tehila - Perl LWP with fake user agent	4
176.13.14.57	147.237.72.166	Israel	aka.idf.il	INDICATOR-SCAN myscan	2
176.13.14.57	147.237.72.166	Israel	aka.idf.il	GPL SCAN myscan	2
121.201.27.61	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
112.196.49.101	147.237.77.176	India	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
93.113.125.11	147.237.77.212	Romania	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
112.196.49.101	147.237.77.176	India	matpash.idf.il	ET SCAN NMAP -sS window 4096	1
93.113.125.11	147.237.77.227	Romania	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.79.104	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

02-13-2016-21:04:00 to 02-13-2016-22:04:00

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	36
185.120.126.31		147.237.77.216	dover.idf.il	drop	SAM rule	drop	33
79.176.188.216	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
109.66.227.9	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
37.26.149.208	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
46.19.86.130	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
84.228.54.107	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
46.19.86.39	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
77.126.15.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
185.3.147.250	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.86.47	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.130	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.64.223.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.66.90	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.11.252	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.184.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.71.22.38	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence		monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
5.102.254.239	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
208.109.97.62	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
46.19.86.220	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
188.120.148.229	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.46.39.145	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
31.210.187.112	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
87.71.22.38	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	3
79.182.201.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.216.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
157.55.39.155	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.205.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.16.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
93.158.152.78	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.38.179	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
87.71.22.38	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
80.178.2.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.209	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.176.197.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.4.145	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.20.190	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.182.55	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.63.74	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
93.173.189.74	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
87.71.22.38	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.65.224.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.69.248.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.20.224	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.131.172	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
109.253.138.251	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-13-2016-21:04:00 to 02-13-2016-22:04:00

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
87.71.22.38	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	268
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	236
2.52.163.97	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	81
157.55.39.19	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	76
85.64.57.44	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	74
40.77.167.100	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	48
52.16.5.197	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	47
208.109.97.62	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	38
80.246.136.86	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	36
46.120.233.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
46.117.63.4	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	26
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
5.29.6.130	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
46.121.144.149	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	23
192.249.66.247	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	23
5.144.55.180	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	23
50.87.144.145	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	22
79.179.139.89	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	20
176.13.18.245	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
213.57.141.107	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
46.117.152.171	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	16
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
84.228.80.100	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
5.29.156.240	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
79.178.33.30	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
84.109.230.157	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
46.117.5.104	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
79.182.223.196	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
109.65.5.57	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
109.253.210.22	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
95.86.99.180	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
149.88.213.130	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	11
109.67.48.244	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
188.120.154.160	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
46.121.77.234	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
176.13.14.211	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	9
213.57.239.183	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	9
89.138.101.174	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
109.186.183.134	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
37.26.146.223	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
149.78.8.201	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
37.142.64.115	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
5.22.130.91	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
95.86.126.95	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
217.132.69.108	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
79.180.197.224	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
184.153.75.12	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	7
37.26.146.199	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6

02-13-2016-21:04:00 to 02-13-2016-22:04:00