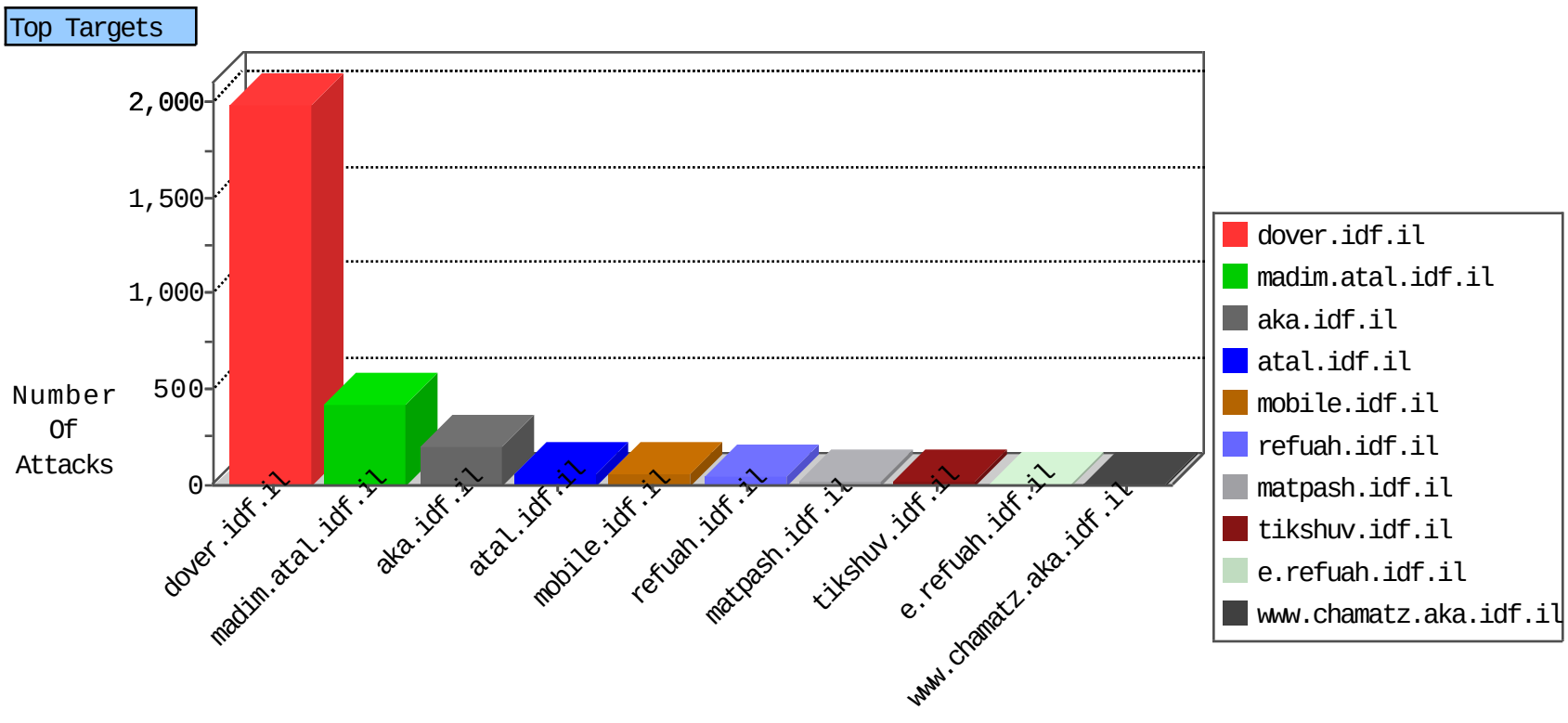
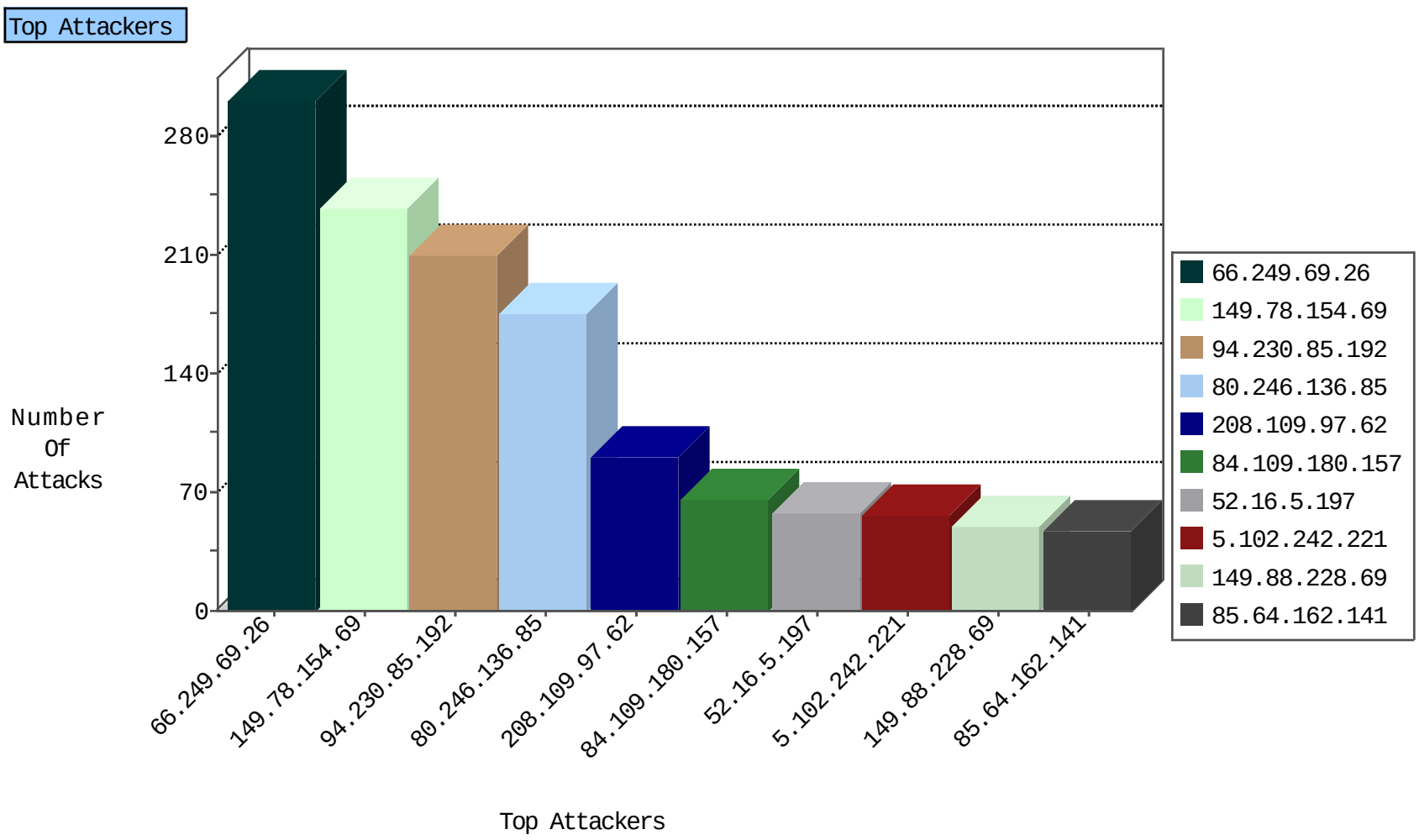
02-13-2016-17:04:00 to 02-13-2016-18:04:00

IDF Under Attack Daily Report





02-13-2016-17:04:00 to 02-13-2016-18:04:00

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	forward	2
222.186.51.180	China	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
92.222.135.148	France	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
151.80.109.153	Italy	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

02-13-2016-17:04:00 to 02-13-2016-18:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
155.94.254.143	United States	147.237.77.216	dover.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1
188.165.15.234	France	147.237.76.200	eitan.aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1

02-13-2016-17:04:00 to 02-13-2016-18:04:00

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	12
120.26.38.111	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
58.176.97.175	147.237.76.30	Hong Kong	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.45.137.67	147.237.77.170	Turkey	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
120.26.38.111	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
80.246.136.85	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	1
46.45.137.67	147.237.77.226	Turkey	www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.45.137.67	147.237.76.42	Turkey	refuah.idf.il	ET SCAN NMAP -sS window 1024	1

02-13-2016-17:04:00 to 02-13-2016-18:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
208.109.97.62	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	14
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	13
64.19.78.243	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	12
89.138.182.168	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
2.54.21.80	Israel	147.237.72.166	aka.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	12
37.26.147.207	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.67.13.226	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
41.254.8.96	Libyan Arab Jamahiriya	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	9
89.138.182.168	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
78.170.102.95	Turkey	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	7
78.170.102.95	Turkey	147.237.77.233	atal.idf.il	drop	SAM rule	drop	7
109.253.196.69	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
78.170.102.95	Turkey	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	7
109.253.196.69	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.66.169.46	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.255	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.106.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.137	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.137	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.114	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.246.136.85	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.114	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
94.230.85.192	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.163.119	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
212.29.220.238	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
86.161.182.7	United Kingdom	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	5
46.19.85.137	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
79.181.201.172	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
46.19.85.137	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.3.144.29	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
185.120.126.31		147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
2.52.162.30	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
178.255.215.87	France	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
37.46.41.28	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.64.70.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.186.44	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.55.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.130.95	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.41.197	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.181.65.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.27	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.133.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.155.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.42.52	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.174.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	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	300
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	235
80.246.136.85	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	114
94.230.85.192	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	111
94.230.85.192	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	86
208.109.97.62	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	76
84.109.180.157	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	66
52.16.5.197	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	58
5.102.242.221	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	51
149.88.228.69	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	50
80.246.136.85	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 80.246.136.85	Block	48
79.183.112.141	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	45
85.64.162.141	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	45
52.33.66.29	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	43
157.55.39.219	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	42
2.54.27.151	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	39
68.180.228.112	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	25
192.249.66.247	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
109.65.139.167	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	19
31.168.215.4	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
2.54.48.98	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
80.246.136.28	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
84.111.23.42	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
176.13.5.132	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
79.179.129.135	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
50.153.104.223	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
46.19.86.147	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
2.54.18.172	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
80.246.136.158	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	11
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	11
87.69.32.22	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
68.1.147.8	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
2.54.176.224	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
79.180.24.95	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	7
5.29.125.35	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	7
76.99.143.80	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	7
176.13.21.174	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
109.253.131.149	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
5.29.180.82	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
213.57.207.59	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
46.117.14.189	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
2.52.162.62	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
176.228.41.209	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
2.54.149.81	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
77.127.193.165	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
84.228.218.36	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
79.177.5.207	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6

02-13-2016-17:04:00 to 02-13-2016-18:04:00