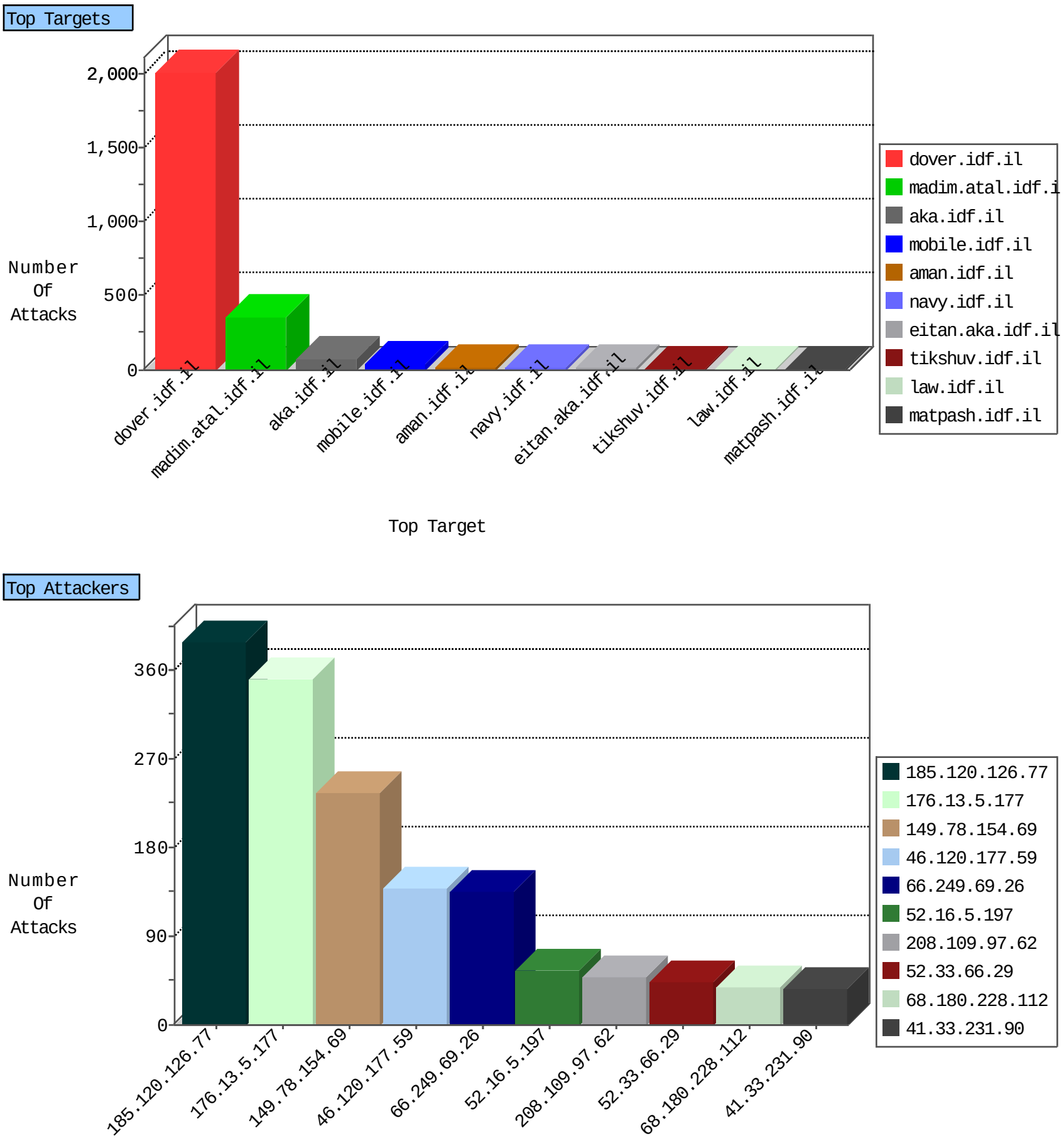
02-13-2016-10:04:08 to 02-13-2016-11:04:08

IDF Under Attack Daily Report



02-13-2016-10:04:08 to 02-13-2016-11:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.130.5.224		147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1

02-13-2016-10:04:08 to 02-13-2016-11:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-13-2016-10:04:08 to 02-13-2016-11:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
117.34.70.143	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
115.28.218.77	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
84.0.124.54	147.237.77.226	Hungary	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
84.0.124.54	147.237.77.178	Hungary	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
45.32.39.185	147.237.72.14		dover.idf.il(old)	ET SCAN NMAP -sS window 4096	1
45.32.39.185	147.237.72.14		dover.idf.il(old)	ET SCAN NMAP -f -sS	1
218.246.0.97	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
176.13.5.177	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	1
117.34.70.143	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
93.23.130.198	147.237.72.167	France	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
84.0.124.54	147.237.77.216	Hungary	dover.idf.il	ET SCAN NMAP -sS window 1024	1
84.0.124.54	147.237.77.74	Hungary	law.idf.il	ET SCAN NMAP -sS window 1024	1
62.90.49.25	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
45.32.39.185	147.237.72.14		dover.idf.il(old)	ET SCAN NMAP -sS window 2048	1
196.207.132.126	147.237.8.27		e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

02-13-2016-10:04:08 to 02-13-2016-11:04:08

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
66.249.78.216	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
77.125.125.37	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	13
66.249.64.193	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
66.249.66.90	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
109.64.211.85	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
46.19.85.147	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.64.206.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.17.20	Israel	147.237.76.147	chinuch.aka.idf.il	drop	First packet isn't SYN	drop	5
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
87.69.55.159	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.181.188.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.126.144.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.108.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.61.197	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.50.89	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.225.161	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.126.89		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.147	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.66.150.166	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.48.129	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.120.154.78	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.143.244	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.124.149	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
132.74.145.98	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.26.149.151	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
66.249.66.93	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
5.22.131.31	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
176.13.5.177	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid sequence number	alert	2
209.141.58.114	United States	147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
61.135.190.200	China	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
176.13.5.177	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid sequence number	monitor	2
46.19.86.126	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.46.41.99	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
109.64.20.160	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
36.77.100.24	Indonesia	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
199.255.138.45	United States	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	2
141.212.122.200	United States	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
213.8.204.77	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
5.22.131.13	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
64.125.239.99	United States	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
85.64.224.39	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.139.75	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	drop	SAM rule	drop	1
84.0.124.54	Hungary	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.120.126.77		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	389
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	236
176.13.5.177	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.13.5.177	Block	188
46.120.177.59	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	138
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	133
176.13.5.177	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
52.16.5.197	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	55
176.13.5.177	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 176.13.5.177	Block	54
208.109.97.62	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	48
52.33.66.29	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	43
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	37
157.55.39.31	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	35
157.55.39.209	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	33
85.64.154.3	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
50.87.144.145	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	26
192.249.66.247	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
46.121.105.98	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
109.65.96.178	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
2.52.129.63	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
2.54.39.139	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	23
46.19.86.161	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	19
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
37.142.64.3	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
46.19.86.127	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
79.181.144.202	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
176.13.4.147	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
79.177.11.135	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
87.68.35.234	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
46.19.85.160	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
89.138.180.141	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
185.120.126.89		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
109.253.208.226	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
46.120.95.29	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
46.121.130.71	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
66.249.69.34	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	8
62.90.49.25	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
2.52.188.54	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	7
46.19.85.152	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
2.54.38.30	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
46.19.86.221	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
5.102.195.116	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
79.180.16.71	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
37.142.131.184	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
2.54.23.161	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
79.180.50.121	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
93.173.46.108	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
176.13.0.35	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
185.120.125.22		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6

02-13-2016-10:04:08 to 02-13-2016-11:04:08