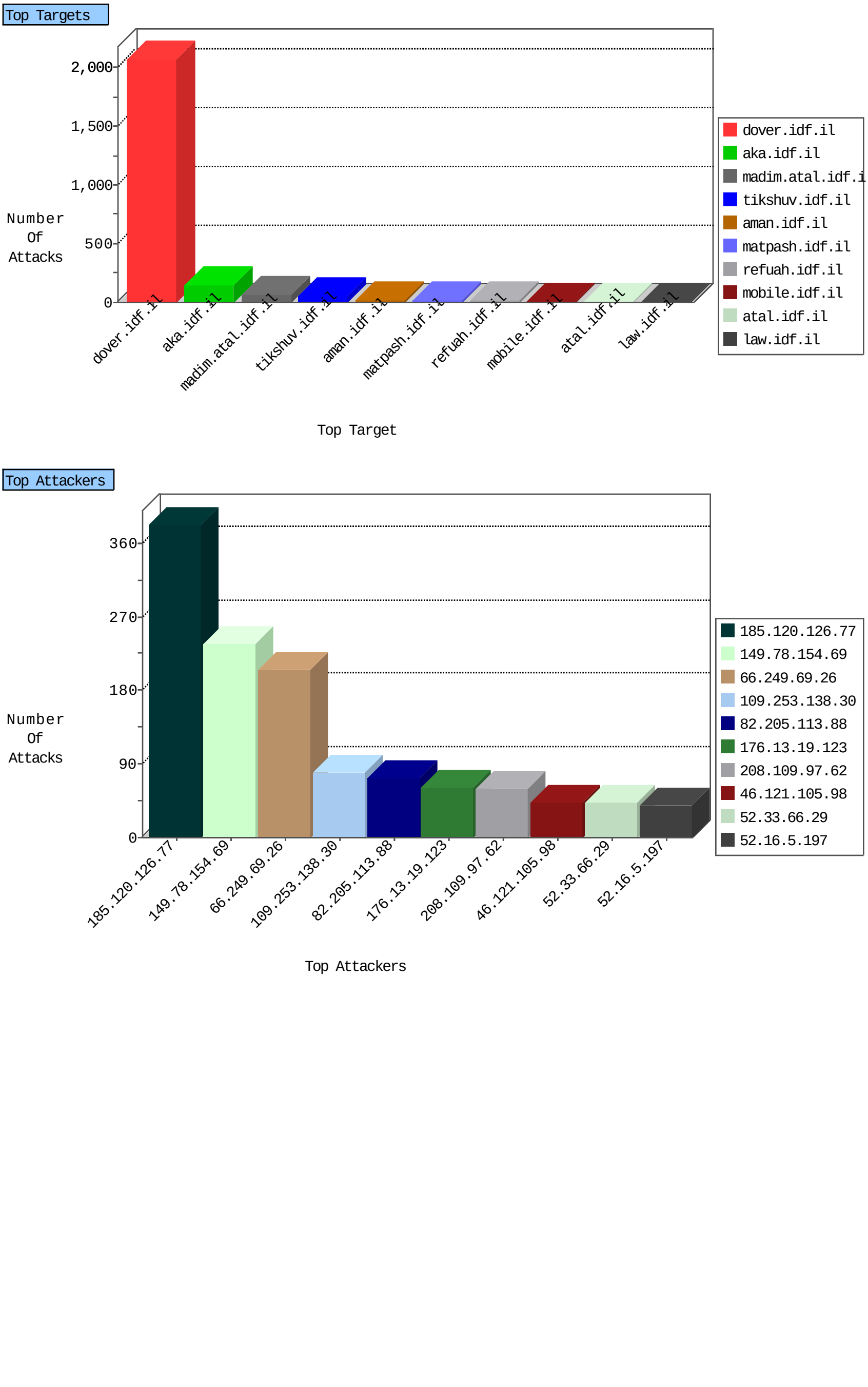
02-13-2016-12:04:04 to 02-13-2016-13:04:04

IDF Under Attack Daily Report



02-13-2016-12:04:04 to 02-13-2016-13:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
71.6.167.142	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
85.25.43.94	Germany	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
66.102.9.10	United States	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
185.94.111.1		147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
66.249.93.184	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1

02-13-2016-12:04:04 to 02-13-2016-13:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
162.210.196.98	United States	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1

02-13-2016-12:04:04 to 02-13-2016-13:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
162.244.31.3	147.237.0.200	Canada	m4u.idf.il	ET SCAN NMAP -sS window 3072	1
45.32.39.185	147.237.72.166		aka.idf.il	ET SCAN NMAP -sS window 3072	1
45.32.39.185	147.237.0.33		idf.il	ET SCAN NMAP -sS window 4096	1
31.184.195.114	147.237.77.233	Russian Federation	atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
162.244.31.3	147.237.0.200	Canada	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
45.32.39.185	147.237.72.166		aka.idf.il	ET SCAN NMAP -sS window 1024	1
45.32.39.185	147.237.0.33		idf.il	ET SCAN NMAP -sS window 3072	1

02-13-2016-12:04:04 to 02-13-2016-13:04:04

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
109.66.115.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
41.217.160.89	Egypt	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	17
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	14
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
31.210.186.138	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
41.217.160.89	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
208.109.97.62	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	7
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
41.217.160.89	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.22.135.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.138.30	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.54.225	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.135.156	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.22.135.101	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
185.120.126.31		147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
37.26.146.150	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.34.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.37.16	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.14.129	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.188.83	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.68.245.151	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.56.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
195.154.184.110	France	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
41.217.160.89	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.183.109.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
5.22.135.189	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
93.172.51.184	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
109.253.197.182	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
93.172.51.184	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.86.198	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.107.110	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.178.15.138	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.112.125	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.210.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
41.217.160.89	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.181.123.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.120.148.129	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.22.135.158	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.102.254.239	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
94.230.86.229	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.251	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
5.22.135.158	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
81.218.201.142	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
84.108.224.253	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
77.127.202.209	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
194.90.129.187	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
84.111.54.94	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2

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	382
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	235
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	204
109.253.138.30	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	73
82.205.113.88	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	71
176.13.19.123	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	62
208.109.97.62	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	52
52.33.66.29	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	43
46.121.105.98	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	43
52.16.5.197	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	39
157.55.39.209	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	30
157.55.39.31	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	30
50.87.144.145	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	25
85.64.214.156	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 85.64.214.156	Block	25
37.26.149.230	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	23
109.66.52.87	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	22
109.67.190.238	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	20
109.65.75.235	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	20
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
176.13.14.5	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
176.13.18.131	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
176.106.46.74	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
109.253.217.125	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
176.13.5.132	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
84.111.159.124	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	11
84.94.160.76	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
109.64.65.64	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
105.109.112.166	Algeria	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
212.179.243.12	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	9
79.180.167.118	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
5.22.135.158	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
79.180.214.11	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
93.173.253.173	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
109.253.220.20	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
85.64.125.82	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
176.13.3.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
149.88.231.234	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
109.65.175.157	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
46.19.86.47	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
109.253.218.92	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
37.26.148.131	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
77.126.167.244	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
5.29.154.74	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	5
149.78.216.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	5
184.72.145.109	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	5
37.142.64.115	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
79.183.63.59	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4

02-13-2016-12:04:04 to 02-13-2016-13:04:04