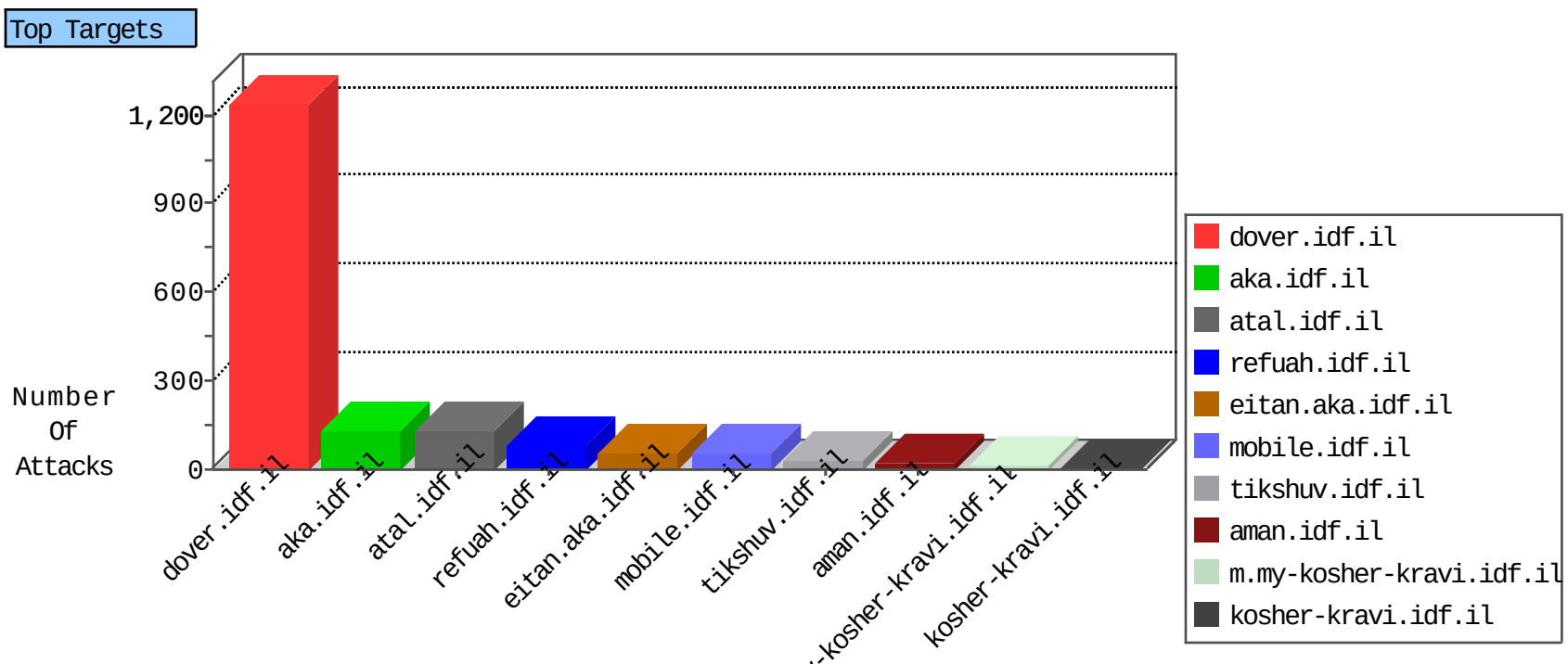
02-13-2016-22:04:03 to 02-13-2016-23:04:03

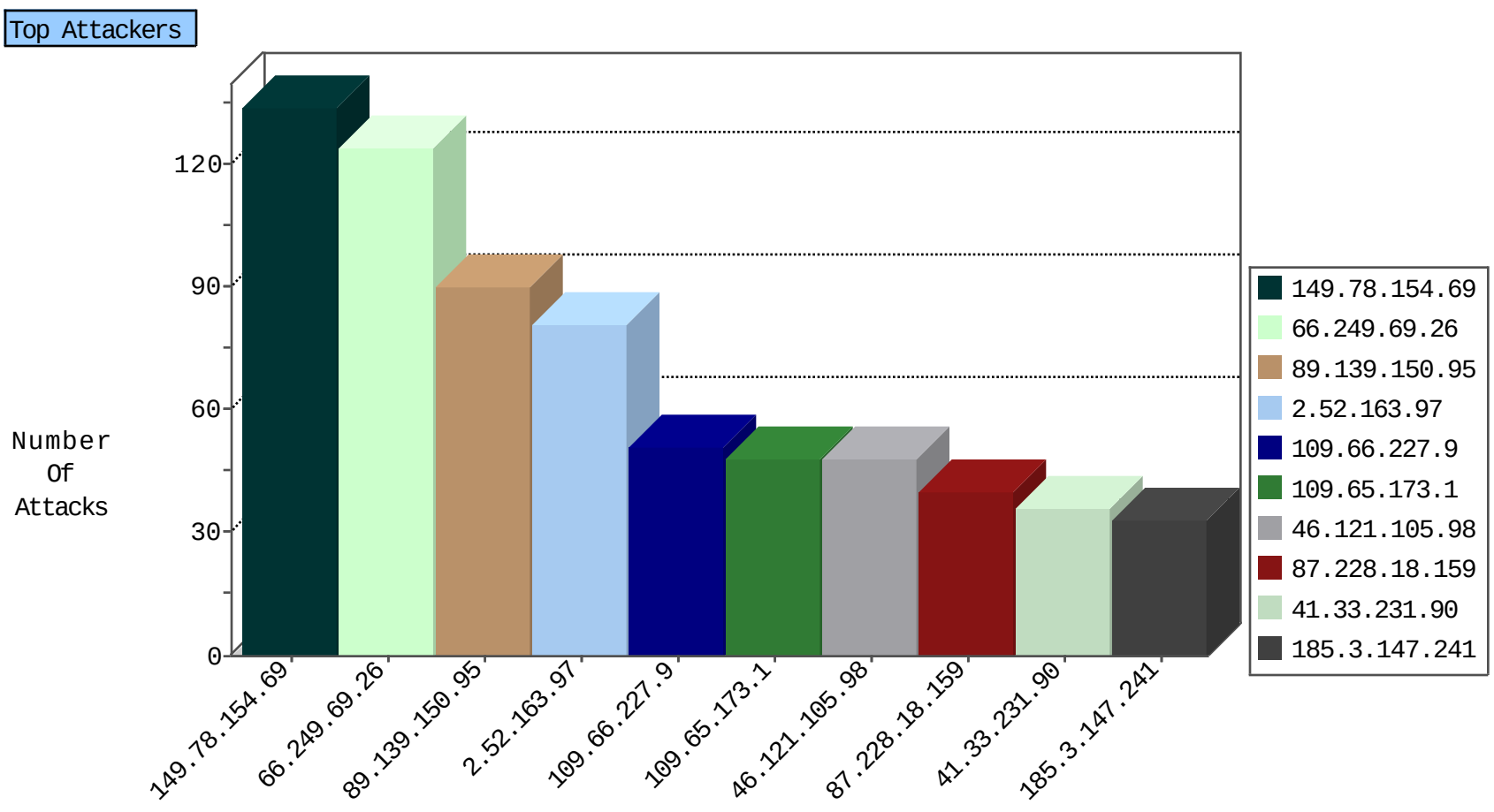
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

02-13-2016-22:04:03 to 02-13-2016-23:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.94.111.1		147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
64.74.133.83	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
71.6.158.166	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
193.242.218.6	Switzerland	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
85.25.43.94	Germany	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1

02-13-2016-22:04:03 to 02-13-2016-23:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-13-2016-22:04:03 to 02-13-2016-23:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
69.197.145.242	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
221.226.31.210	147.237.0.34	China	tikshuv.idf.il	ET SCAN NMAP -f -sS	1
221.6.32.82	147.237.0.34	China	tikshuv.idf.il	ET SCAN NMAP -f -sS	1
114.112.90.54	147.237.77.74	China	law.idf.il	ET SCAN NMAP -sS window 1024	1
98.119.105.221	147.237.0.15	United States	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
91.201.236.113	147.237.76.198	Ukraine	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
85.250.136.169	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
79.182.196.31	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
221.226.31.210	147.237.0.34	China	tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
221.6.32.82	147.237.0.34	China	tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
198.20.69.98	147.237.76.200	United States	eitan.aka.idf.il	ET DROP Dshield Block Listed Source	1
98.119.105.221	147.237.0.15	United States	kosher-kravi.idf.i	ET SCAN NMAP -sS window 4096	1
94.102.48.193	147.237.72.217	Netherlands	e.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.113	147.237.76.198	Ukraine	e.yohalan.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
80.82.79.104	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN NMAP -sS window 1024	1

02-13-2016-22:04:03 to 02-13-2016-23:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
89.139.150.95	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	89
109.66.227.9	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
87.228.18.159	Russian Federation	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	40
109.65.173.1	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
37.26.149.208	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
109.253.204.220	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
79.183.172.13	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
109.253.204.220	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
89.138.177.21	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
176.2.137.250	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.86.128	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
85.250.136.169	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
185.32.179.172	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
109.253.208.205	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
80.230.79.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.3.176	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
79.183.39.117	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.47	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
37.26.146.208	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.31	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.147.216	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
64.19.78.242	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
105.105.97.208	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.121.134.214	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
87.68.46.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.217	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.72	Israel	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
149.78.250.27	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.12.181	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.63.95	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.154.167	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.108.219.183	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.0.14.181	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.182.21.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
95.172.233.91	United Kingdom	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
5.28.175.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.98	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.49.149	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.30	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
212.199.0.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.151.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.101.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-13-2016-22:04:03 to 02-13-2016-23:04:03

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
185.3.147.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	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

02-13-2016-22:04:03 to 02-13-2016-23:04:03

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	134
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	121
2.52.163.97	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	81
46.121.105.98	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	48
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
149.78.45.222	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
52.16.5.197	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	23
79.181.221.73	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	21
184.153.75.12	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	21
157.55.39.19	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
185.3.147.241	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 185.3.147.241	Block	15
50.87.144.145	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
37.26.146.223	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
149.88.81.12	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
185.3.147.241	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
192.249.66.247	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
84.108.16.88	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
2.54.13.27	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
89.138.197.226	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
37.8.81.128	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
40.77.167.100	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	11
176.13.4.195	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
79.177.104.60	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
208.109.97.62	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	10
84.228.254.204	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	9
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	9
89.139.234.12	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
109.65.173.1	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
2.54.47.115	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
109.67.148.219	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.67.148.219	Block	8
2.54.5.15	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
109.65.5.57	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
109.65.165.135	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
46.19.86.43	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	7
109.186.183.134	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
87.70.4.13	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
176.13.2.130	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	6
85.64.115.162	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
109.64.148.41	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
5.28.129.66	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
45.35.64.142		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
89.139.29.55	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
5.22.131.114	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
212.179.21.194	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
95.172.233.91	United Kingdom	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
109.64.59.224	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
2.54.8.0	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	5
37.26.148.217	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	5
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	5
210.172.183.48	Japan	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 210.172.183.48	Block	5

02-13-2016-22:04:03 to 02-13-2016-23:04:03