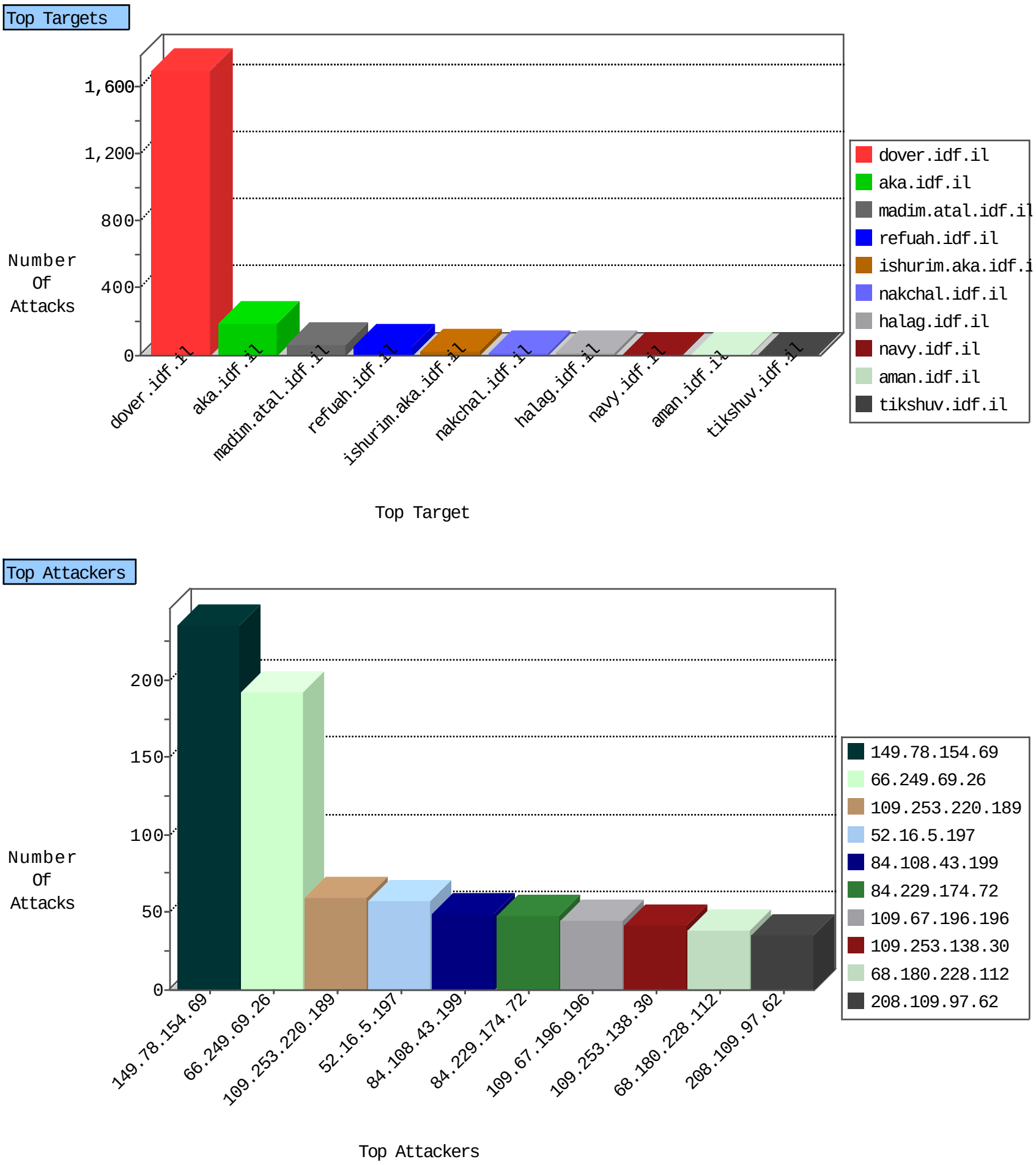
02-13-2016-14:04:03 to 02-13-2016-15:04:03

IDF Under Attack
Daily Report



02-13-2016-14:04:03 to 02-13-2016-15:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.177.149.88	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
185.94.111.1		147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
89.248.174.4	Netherlands	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
89.248.174.4	Netherlands	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
89.248.174.4	Netherlands	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1

02-13-2016-14:04:03 to 02-13-2016-15:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.15.110	France	147.237.77.216	dover.idf.il	C228: HTTP: AhrefBot crawler	Block	1

02-13-2016-14:04:03 to 02-13-2016-15:04:03

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	9
96.56.7.42	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
96.56.7.42	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.113	147.237.76.30	Ukraine	himush.idf.il	ET SCAN NMAP -sS window 1024	1
77.126.185.112	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
45.32.39.185	147.237.77.178		e.matpash.idf.il	ET SCAN NMAP -sS window 2048	1
218.246.0.97	147.237.76.30	China	himush.idf.il	ET SCAN NMAP -sS window 1024	1
96.56.7.42	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
96.56.7.42	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.193	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.79.104	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
45.32.39.185	147.237.77.178		e.matpash.idf.il	ET SCAN NMAP -sS window 4096	1
45.32.39.185	147.237.77.178		e.matpash.idf.il	ET SCAN NMAP -f -sS	1
218.246.0.97	147.237.76.34	China	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.72.217	China	e.idf.il	ET SCAN NMAP -sS window 1024	1

02-13-2016-14:04:03 to 02-13-2016-15:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
84.229.174.72	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	47
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
2.54.47.186	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
79.177.99.251	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
46.19.85.66	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.86.83	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	drop	SAM rule	drop	11
84.111.188.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	7
46.19.85.66	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.86.47	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
178.255.215.87	France	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
109.253.129.44	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
176.13.2.84	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.64.133	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.64.139	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
208.109.97.62	United States	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
2.54.181.244	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
178.255.215.87	France	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	4
197.167.0.79	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
185.32.179.19	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.86.249	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	4
2.54.47.186	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	3
77.127.220.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.68.43.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.172.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.16.77	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.110.184.84	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.68.79.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.249	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.66.48.250	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.126.74		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.9.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.8.204.27	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
2.54.8.133	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.66.112.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.4.157	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.57.123	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
46.19.86.249	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Block HTTP Non Compliant	illegal header format detected: Malformed HTTP format in request	monitor	2
66.249.64.250	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
157.55.2.132	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
109.67.57.123	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
84.94.20.189	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
68.180.229.94	United States	147.237.0.15	kosher-kravi.idf.i	drop	First packet isn't SYN	drop	2

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	235
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	191
109.253.220.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	60
52.16.5.197	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	57
84.108.43.199	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	49
109.67.196.196	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	45
109.253.138.30	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	42
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	38
46.19.86.15	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	32
208.109.97.62	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	31
66.102.8.238	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	30
157.55.39.209	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	30
82.205.113.88	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
176.13.23.156	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	24
50.87.144.145	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	23
109.67.22.236	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	22
77.126.185.112	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	20
46.19.86.143	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	20
176.13.2.55	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	18
85.65.26.236	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
109.65.183.45	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
46.121.137.150	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
157.55.39.31	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	12
89.139.150.68	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
79.182.58.231	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
37.142.68.95	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
213.57.178.214	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
109.67.57.123	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
109.65.176.156	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
80.246.130.48	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
109.65.2.224	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
109.253.209.165	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
176.13.2.103	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
79.180.155.254	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
109.253.210.20	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
46.19.86.77	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
79.183.234.226	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
149.78.119.148	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
2.54.173.247	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
46.121.245.104	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
109.66.36.83	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
89.138.119.108	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
109.253.207.95	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.28	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
80.246.137.179	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	5
205.203.135.1	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	5

02-13-2016-14:04:03 to 02-13-2016-15:04:03