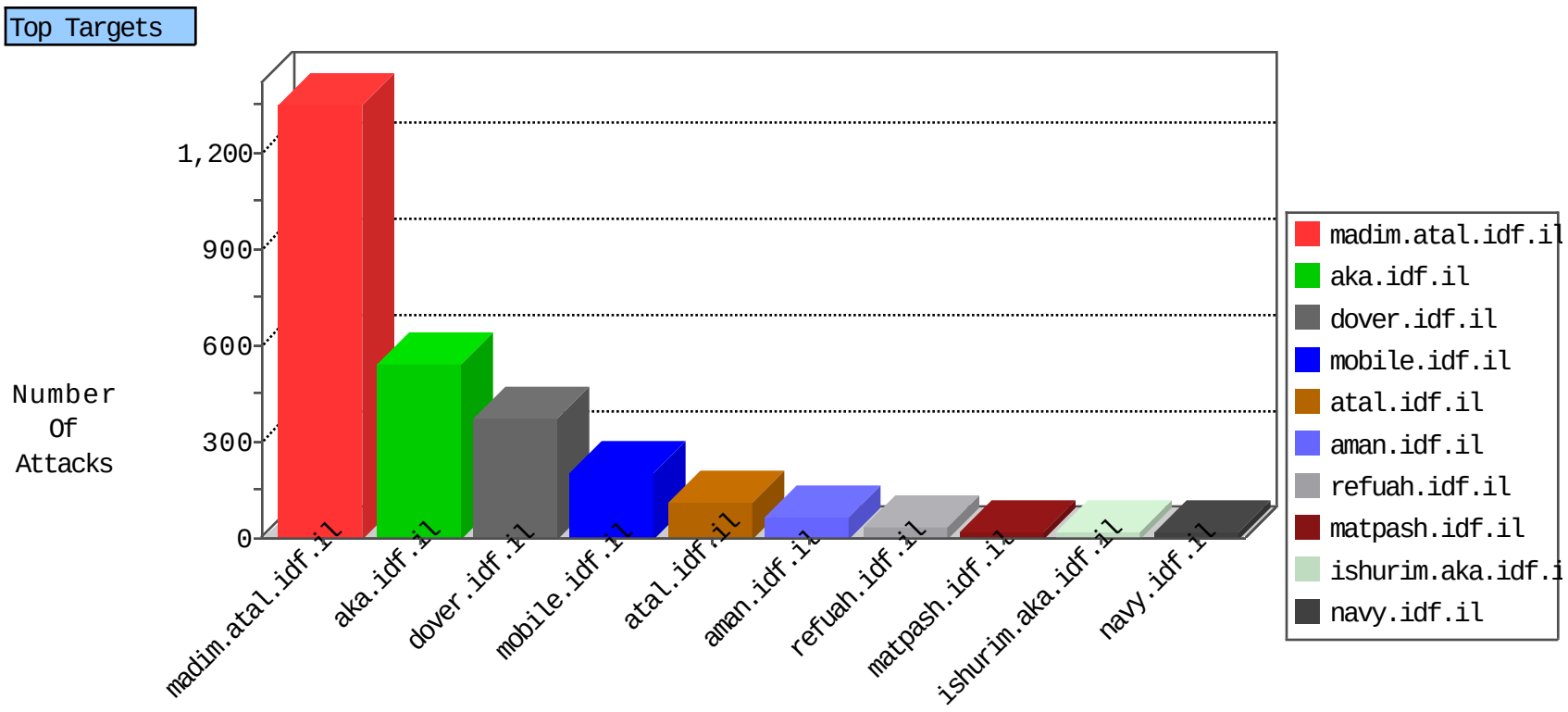
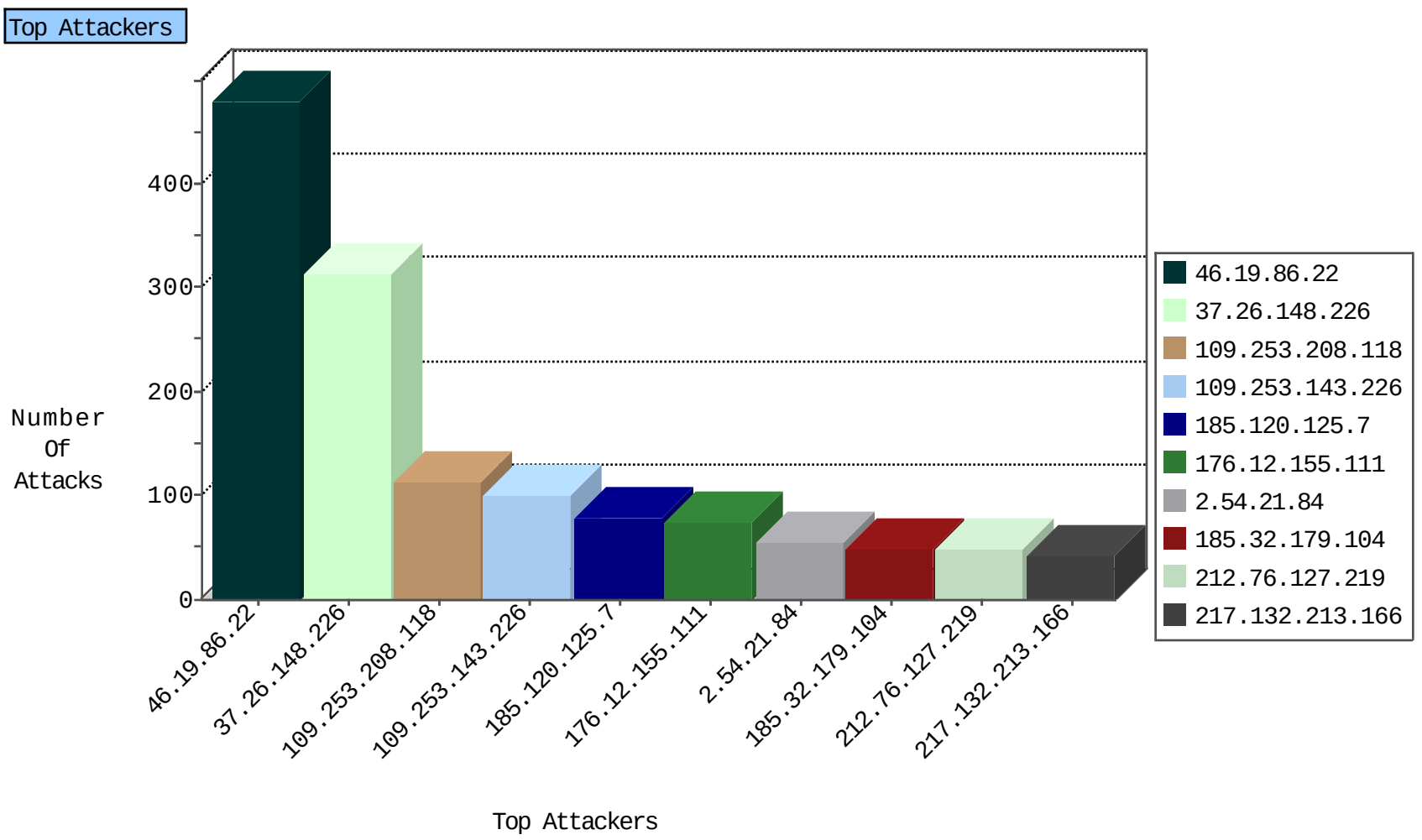
02-01-2016-14:04:04 to 02-01-2016-15:04:04

IDF Under Attack Daily Report





02-01-2016-14:04:04 to 02-01-2016-15:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.208.118	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	184
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
115.28.88.157	China	147.237.76.202	e.halag.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
74.91.28.58	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1
202.110.64.103	China	147.237.76.199	e.nakchal.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
142.54.169.166	United States	147.237.77.233	atal.idf.il	block-sp-traf1	drop	1

02-01-2016-14:04:04 to 02-01-2016-15:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-01-2016-14:04:04 to 02-01-2016-15:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
174.37.194.144	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
2.54.27.176	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
168.62.238.153	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
109.253.150.219	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.65.29.49	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.68.251.158	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.90.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.229.132.230	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
82.80.219.164	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.160.242.40	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.80.174	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.107	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.117.194.43	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
174.37.194.144	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sA (2)	1
2.54.21.84	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
132.72.15.208	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.66.24.134	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.230.86.103	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.0.34	China	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
85.64.207.163	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
84.117.113.152	147.237.77.121	Romania	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
208.109.97.62	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.196.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.118.78.57	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.121.158.222	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

02-01-2016-14:04:04 to 02-01-2016-15:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.120.125.7		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	52
212.76.127.219	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	48
213.55.104.210	Ethiopia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
31.168.123.247	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
185.120.125.7		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	26
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
46.19.85.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
109.253.215.202	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
5.29.185.114	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
2.54.162.35	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
2.54.21.84	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
91.231.193.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
79.180.119.6	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
83.130.99.229	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
217.132.213.166	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
217.132.213.166	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
79.176.236.65	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.253.220.59	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.31	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	9
217.132.213.166	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
80.246.136.195	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
46.19.85.133	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.253.194.22	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
185.32.179.142	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.21.84	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
2.52.45.2	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
2.54.21.84	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
2.54.21.84	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
84.108.184.198	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
2.54.21.84	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
2.54.27.176	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	7
2.52.137.252	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.86.3	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.181.26.171	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.45.2	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
87.68.153.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.157.69	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.134.149	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.219.128	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.94.76.213	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.45.2	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
2.54.198.162	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
84.228.130.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.116.220.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.21.84	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.151	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.228	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.146.198	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.151	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

02-01-2016-14:04:04 to 02-01-2016-15:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.22	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	279
37.26.148.226	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	138
46.19.86.22	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	113
37.26.148.226	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
109.253.208.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	98
46.19.86.22	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 46.19.86.22	Block	85
109.253.143.226	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	78
176.12.155.111	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	74
37.26.148.226	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	71
185.32.179.104	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	49
37.26.149.192	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	39
176.12.155.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	38
176.12.154.94	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	30
109.253.143.226	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.143.226	Block	22
176.12.154.66	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
109.253.140.156	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
109.253.192.246	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
109.253.210.153	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
5.29.185.114	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
109.253.215.202	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
109.253.192.117	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
2.54.162.35	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
46.19.85.21	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
176.12.154.62	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
95.86.75.243	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 95.86.75.243	Block	3
46.19.86.43	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.194.22	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
84.108.184.198	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.142	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
109.253.215.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.12.155.45	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
149.50.92.68	United States	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.179.63.150	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	3
2.54.23.36	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
212.179.42.226	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/×’×™××•×¡	Block	2
109.253.209.0	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.220.59	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
84.94.76.213	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
46.19.85.133	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
62.128.35.91	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
109.253.194.22	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.145	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
82.205.74.171	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	2
31.168.116.1	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
66.249.93.241	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/894-ar	Block	1
184.105.139.67	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
52.88.232.26	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wp-login.php	Block	1
46.19.85.162	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1

02-01-2016-14:04:04 to 02-01-2016-15:04:04