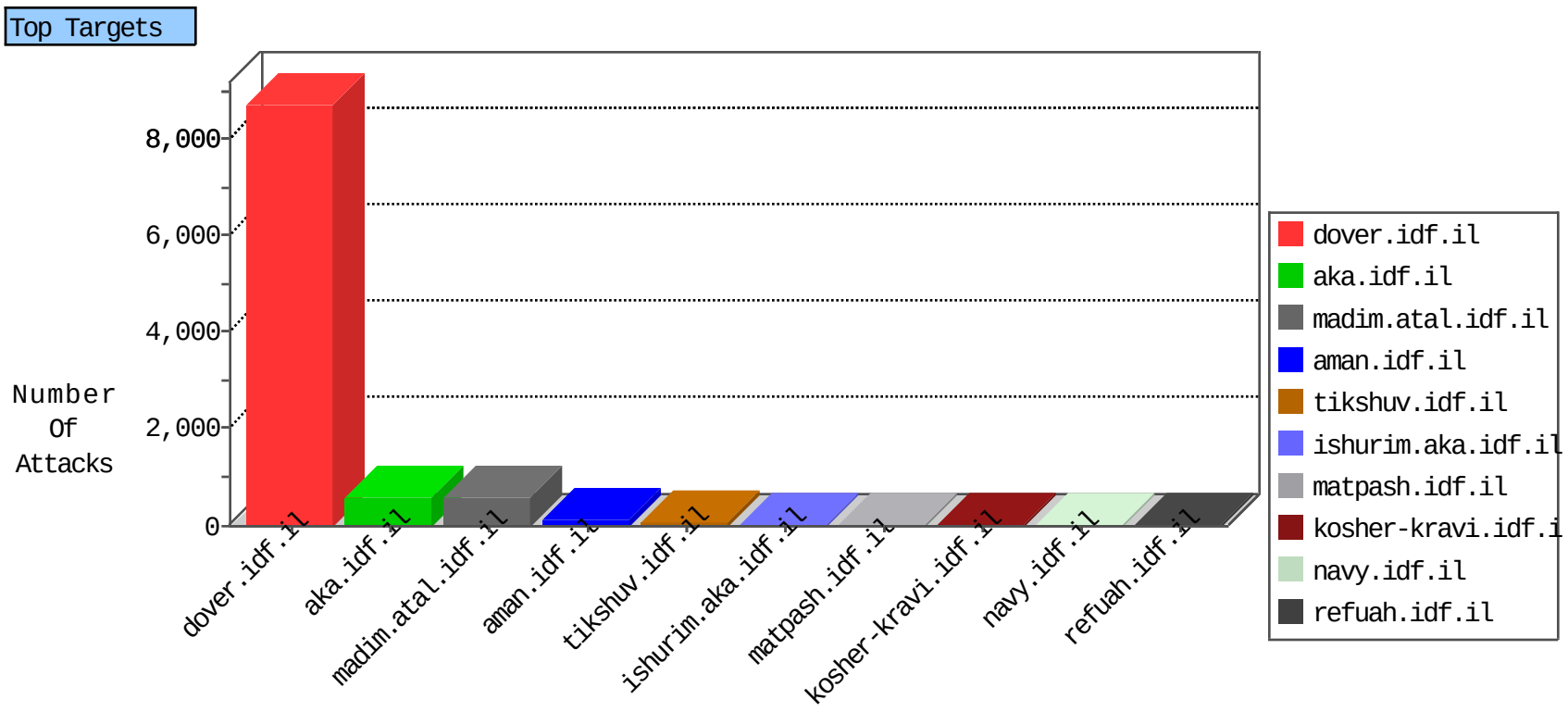
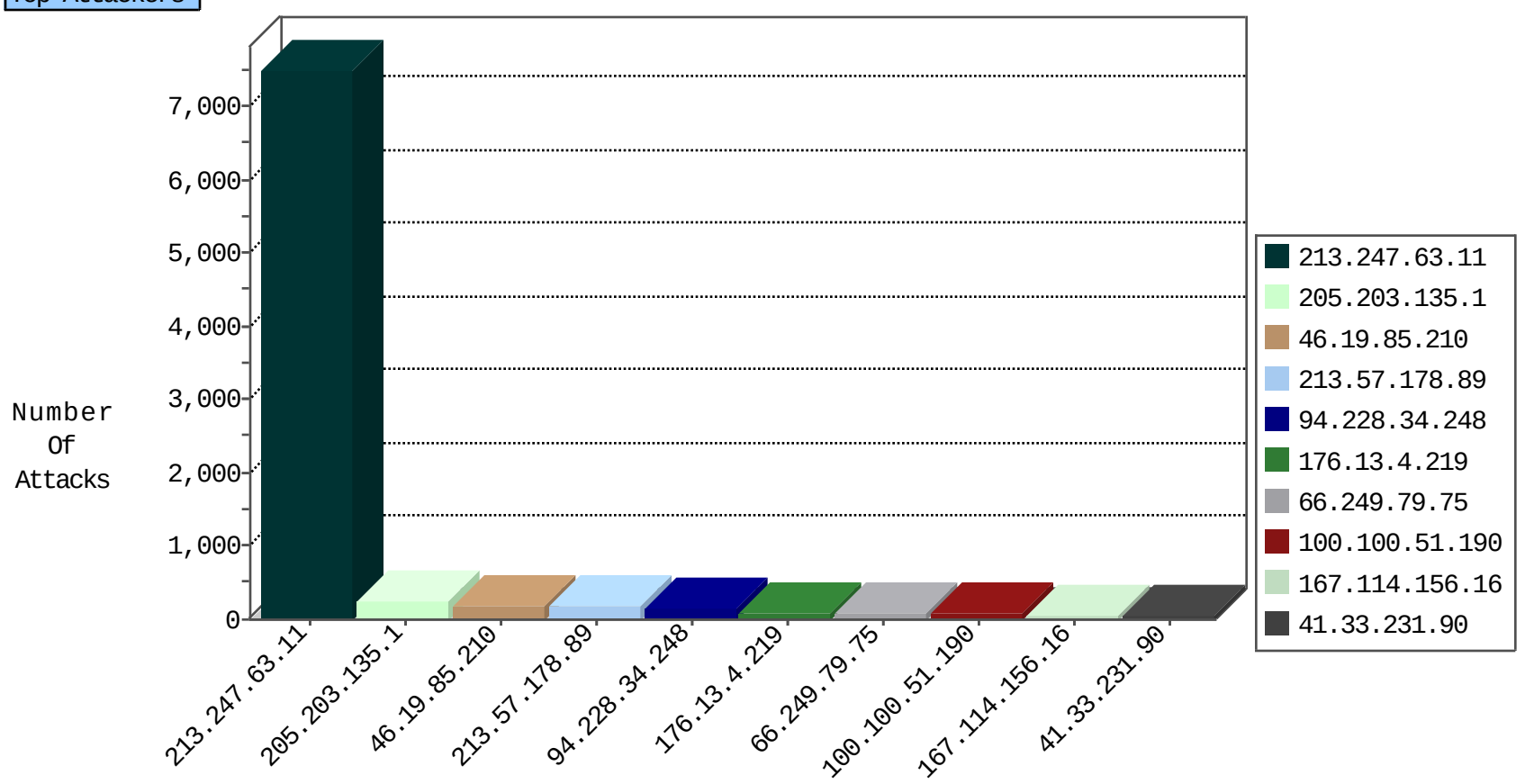
11-24-2015-15:04:01 to 11-24-2015-16:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-24-2015-15:04:01 to 11-24-2015-16:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2289
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1038
220.181.108.150	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	299
81.218.37.2	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	117
66.249.78.15	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	5
116.234.97.175	China	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	4
146.185.57.7	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	3
183.206.202.151	China	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	3
113.65.55.3	China	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
82.118.233.104	Bulgaria	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	1

11-24-2015-15:04:01 to 11-24-2015-16:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-24-2015-15:04:01 to 11-24-2015-16:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
213.247.63.11	147.237.77.216	Netherlands	dover.idf.il	SQL Injection - Select From	5791
37.205.0.60	147.237.77.74	Turkey	law.idf.il	SQL Injection - Select From	9
189.38.80.189	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	5
109.67.1.232	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.193.51.38	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.126.213.189	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.155.5	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.104.77.4	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
182.254.149.138	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.137.239	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.47.74	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

11-24-2015-15:04:01 to 11-24-2015-16:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
213.247.63.11	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1715
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	255
94.228.34.248	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	132
100.100.51.190		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	63
66.249.79.75	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	62
108.200.40.255	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
68.180.229.94	United States	147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	38
83.217.159.134	Luxembourg	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
100.100.18.137		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	28
176.106.226.63	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
79.176.114.167	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	26
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
50.97.138.113	United States	147.237.76.86	navy.idf.il	drop	SAM rule	drop	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	23
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
100.100.81.173		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
203.6.176.20	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
100.100.8.157		147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	19
92.253.95.47	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
100.100.8.157		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
100.100.72.138		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	18
46.19.85.42	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
213.57.143.226	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
203.6.176.20	Australia	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	15
80.178.202.238	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
91.135.102.190	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
78.108.169.25	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
2.54.150.140	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
96.255.43.138	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	13
109.65.206.94	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
100.100.32.249		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
91.135.102.190	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
139.162.216.112	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
100.100.72.138		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.14.127	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
198.58.103.158	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
52.33.66.29	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
37.231.102.163	Kuwait	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
37.26.148.225	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
37.26.146.239	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
100.100.89.97		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	10
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
79.180.201.31	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.47	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
100.100.72.184		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8

11-24-2015-15:04:01 to 11-24-2015-16:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	88
213.57.178.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	87
213.57.178.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	81
176.13.4.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	74
46.19.85.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	66
46.19.85.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
46.19.86.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
80.246.136.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
2.54.177.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
176.13.4.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
2.54.165.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
84.109.232.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
46.19.85.210	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.210	Block	7
2.54.57.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.13.1.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/$$$&?&?$$$	Block	4
79.183.130.215	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.183.130.215	Block	4
212.179.21.194	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/ufi/reaction/	Block	4
37.26.146.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
192.116.95.133	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/valtam	Block	3
66.249.66.96	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
176.12.151.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.183.130.215	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	3
84.229.55.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
93.173.14.63	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/×'×™××¡	Block	3
212.199.224.24	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 212.199.224.24	Block	3
81.218.76.12	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
2.54.166.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
95.86.113.11	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
77.125.83.253	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.125.83.253	Block	2
46.19.86.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.120.145.102	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
52.34.184.17	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
31.168.221.35	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.181.110.45	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.119	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
87.69.105.83	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
221.231.6.246	China	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized HTTP Method	Block	1
77.125.139.167	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
174.37.20.38	United States	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
66.249.69.89	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
149.78.253.255	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.85.186	Israel	147.237.77.216	dover.idf.il	Malformed URL sdch	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.65.112	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/scriptresource.axd	Block	1
109.66.133.102	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 109.66.133.102 (Unknown SSL Session)	None	1
40.114.47.247	United States	147.237.72.156	aman.idf.il	PHP Attempt	Block	1

11-24-2015-15:04:01 to 11-24-2015-16:04:01