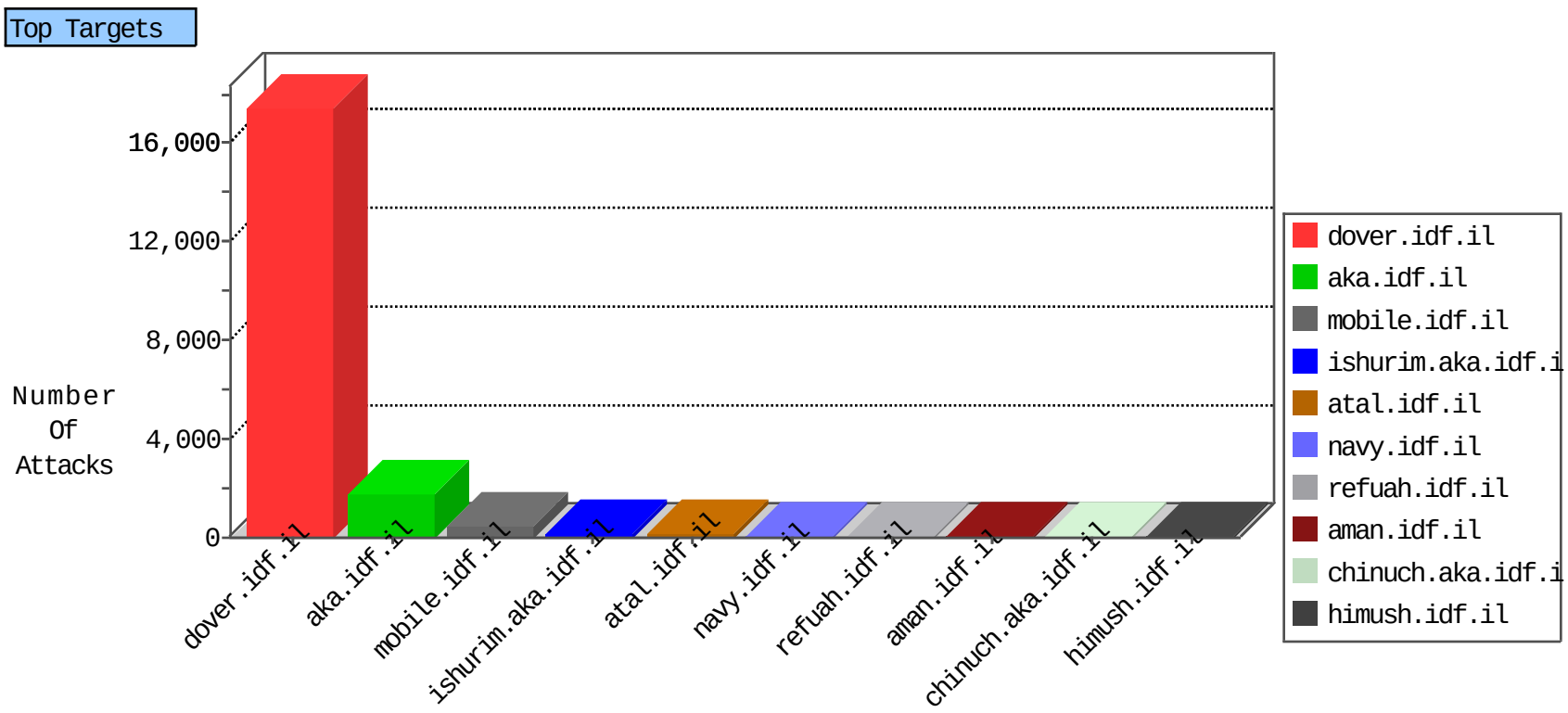
11-01-2015-11:04:09 to 11-01-2015-12:04:09

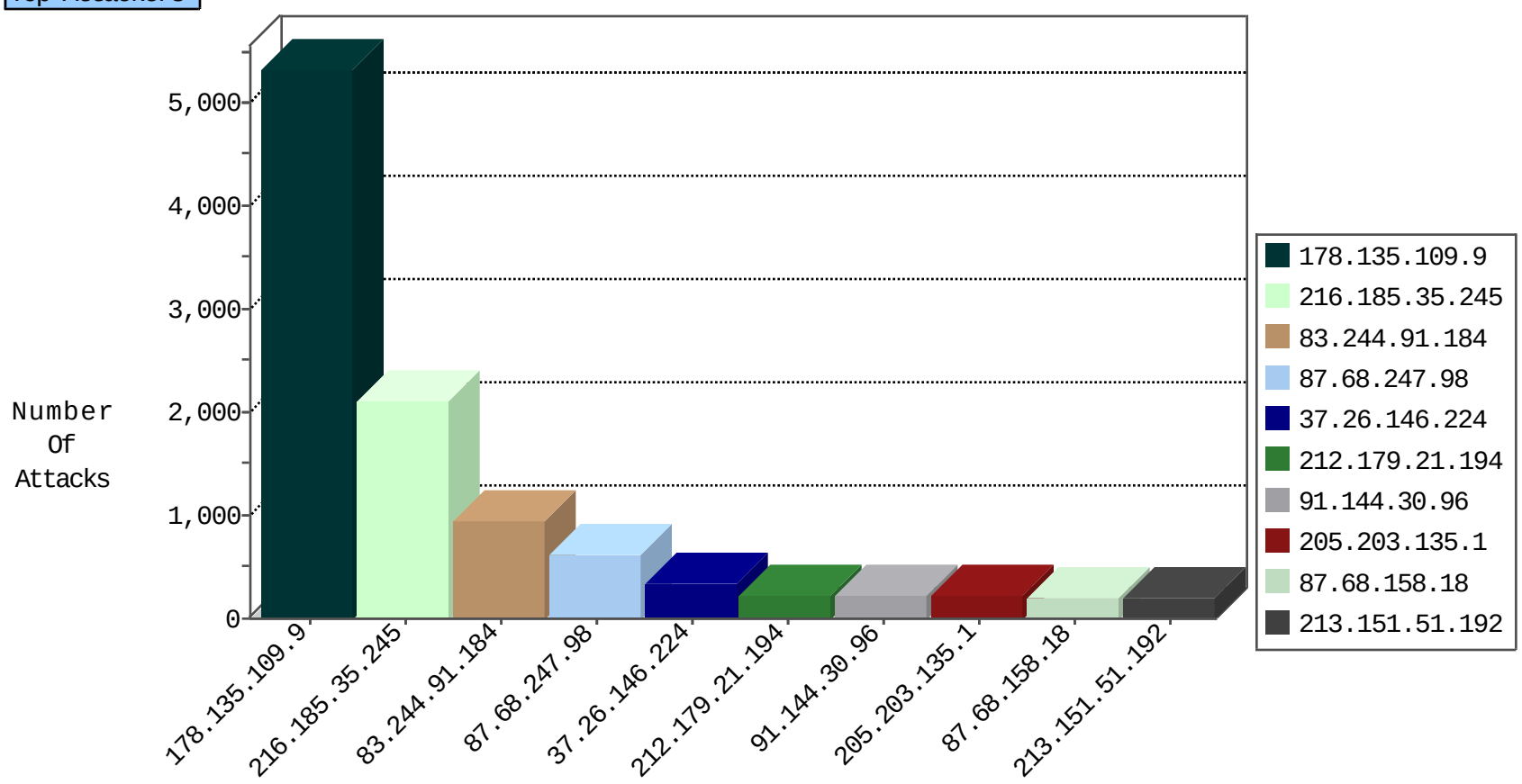
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

11-01-2015-11:04:09 to 11-01-2015-12:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
216.185.35.245	United States	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	4189
91.144.30.96	Syrian Arab Republic	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	3137
83.244.91.184	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	2694
37.26.146.128	Israel	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	1507
66.249.78.159	United States	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	689
0.0.0.0		147.237.77.216	dover.idf.i	SYN Flood full table	drop	645
41.109.57.127	Algeria	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	530
132.66.23.138	Israel	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	473
5.29.53.238	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	36
132.70.66.10	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	26
205.203.135.1	United States	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	26
84.228.162.114	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	23
212.143.3.44	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	22
79.183.12.53	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	21
84.228.162.114	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	18
212.179.21.194	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	13
31.168.213.204	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	11
83.244.53.153	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	SYN Flood full table	drop	11
82.80.69.90	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	11
46.121.247.68	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	10
46.116.103.98	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	10
2.54.42.145	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	10
10.60.0.210		147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	10
2.54.56.140	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	10
2.54.42.145	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	10
213.8.57.205	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	9
213.151.32.163	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	9
132.70.66.11	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	9
46.116.73.10	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	8
41.109.57.127	Algeria	147.237.77.216	dover.idf.i	DOS-HTTP-fireflood	dest-reset	8
79.181.122.145	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	8
93.172.3.101	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	8
81.218.48.37	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	7
188.161.150.178	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	7
93.173.30.173	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	7
79.179.60.182	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	6
84.228.218.22	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	6
46.19.86.191	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	6
81.218.48.37	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	6
178.135.109.9	Lebanon	147.237.77.216	dover.idf.i	TCP handshake violation, first packet not syn	drop	6
176.13.18.56	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	5
195.95.183.254	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	5
176.106.226.240	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	5
213.151.51.192	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	5
195.95.183.254	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	5
46.210.159.70	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	5
46.120.92.202	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	5
46.19.85.206	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	5
176.13.18.56	Israel	147.237.77.216	dover.idf.i	SYN Flood full table	drop	5
46.19.85.21	Israel	147.237.77.216	dover.idf.i	SYN Flood unverified cookie	drop	5

11-01-2015-11:04:09 to 11-01-2015-12:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.109.57.127	Algeria	147.237.77.216	dover.idf.il	12026: HTTP: LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	2
106.38.241.106	China	147.237.76.42	refuah.idf.i	C103: HTTP: User Agent Sogou+web+spider	Block	1
198.20.69.74	United States	147.237.77.179	e.mazi.idf.i	13840: TLS: OpenSSL Heartbeat Packet	Block	1

11-01-2015-11:04:09 to 11-01-2015-12:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.75.44	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	1
46.19.86.5	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
31.25.173.15	147.237.8.50	Turkey	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.59.206	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.98	147.237.77.205	United States	prisha.idf.il	ET DROP Dshield Block Listed Source	1
194.114.146.227	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.4.186	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.125.127.208	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.26	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.173	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.140.188.112	147.237.72.166	Russian Federation	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.240.212	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
176.13.22.202	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.192.0.20	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 1024	1

11-01-2015-11:04:09 to 11-01-2015-12:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
178.135.109.9	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5238
216.185.35.245	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2076
83.244.91.184	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	936
37.26.146.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	339
91.144.30.96	Syrian Arab Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	221
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	210
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	206
87.68.158.18	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	200
213.151.51.192	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	192
87.68.247.98	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	156
37.26.149.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	127
37.26.146.205	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	123
70.48.160.55	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	119
46.19.85.223	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	98
81.249.56.47	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	98
81.218.101.3	Israel	147.237.77.243	mobile.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	96
79.180.0.43	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	95
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	91
212.179.131.93	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	90
67.205.200.219	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	75
194.90.254.244	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	70
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	67
37.26.146.181	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	64
46.19.85.47	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
46.19.85.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
37.140.188.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
81.218.48.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
66.249.81.212	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
66.249.81.218	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
31.168.213.204	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
120.148.227.148	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
2.54.56.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
79.179.162.131	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
46.19.86.121	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
5.29.129.212	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
37.26.148.251	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
79.177.115.201	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
46.184.68.180	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
212.179.140.133	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
66.249.78.159	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39

11-01-2015-11:04:09 to 11-01-2015-12:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.12.142.44	Israel	147.237.72.166	aka.idf.il	Distributed Unknown HTTP Request Method	Block	98
176.13.16.14	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	45
78.154.170.6	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/iturim/resources/images/body/images/main.jpg	Block	45
2.52.164.158	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	45
87.68.247.98	Israel	147.237.72.166	aka.idf.il	Distributed Unknown HTTP Request Method	Block	40
176.13.19.174	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1440-he/atal.aspx	Block	30
176.12.149.174	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	30
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	30
37.26.146.149	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	30
95.86.109.128	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/iturim/resources/images/body/images/main.jpg	Block	30
46.19.85.57	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/sachar/.aspx	Block	30
176.13.5.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	30
87.68.247.98	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	30
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	30
79.178.99.99	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	30
80.246.137.145	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	30
213.151.36.20	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	30
176.12.145.102	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	30
2.54.189.136	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	30
85.65.193.69	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	30
87.68.247.98	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 87.68.247.98	Block	29
87.68.247.98	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 87.68.247.98	Block	26
87.68.247.98	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 87.68.247.98	Block	26
87.68.247.98	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 87.68.247.98	Block	25
87.68.247.98	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 87.68.247.98	Block	25
46.19.86.31	Israel	147.237.77.243	mobile.idf.il	Untraceable SSL Sessions: Open Mode	None	15
91.227.165.5	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	15
81.218.206.48	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	15
217.194.198.104	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	15
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	15
37.142.68.135	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
87.68.247.98	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 87.68.247.98	Block	15
66.249.67.216	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	15
5.22.129.142	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	15
87.68.247.98	Israel	147.237.72.166	aka.idf.il	Malformed URL Â¥×³×˜Â»â€“â€¢Ö¸ â€œÖ¼Ãš[[#0]][[#15]]mÃŠ Â¾lÃ¼Â¸ Ã—ÂŠ[[#24]]g/	Block	15
87.68.247.98	Israel	147.237.72.166	aka.idf.il	Abnormally Long Header Line request header name	Block	15
46.19.86.196	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	15
109.186.167.68	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
198.20.69.74	United States	147.237.72.167	ishurim.aka.idf.i	Distributed Unauthorized URL Access on 147.237.72.167/	Block	15
46.19.85.196	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	15
87.68.247.98	Israel	147.237.72.166	aka.idf.il	Too Many Headers per Request - 36 Headers	Block	15
37.26.146.149	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	15
66.249.78.52	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	15
176.13.14.84	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	15
66.249.65.132	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/links.aspx	Block	15
157.55.39.185	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
2.54.147.102	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
87.68.247.98	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Value	Block	15
46.19.86.60	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	15
93.172.3.101	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	15

11-01-2015-11:04:09 to 11-01-2015-12:04:09