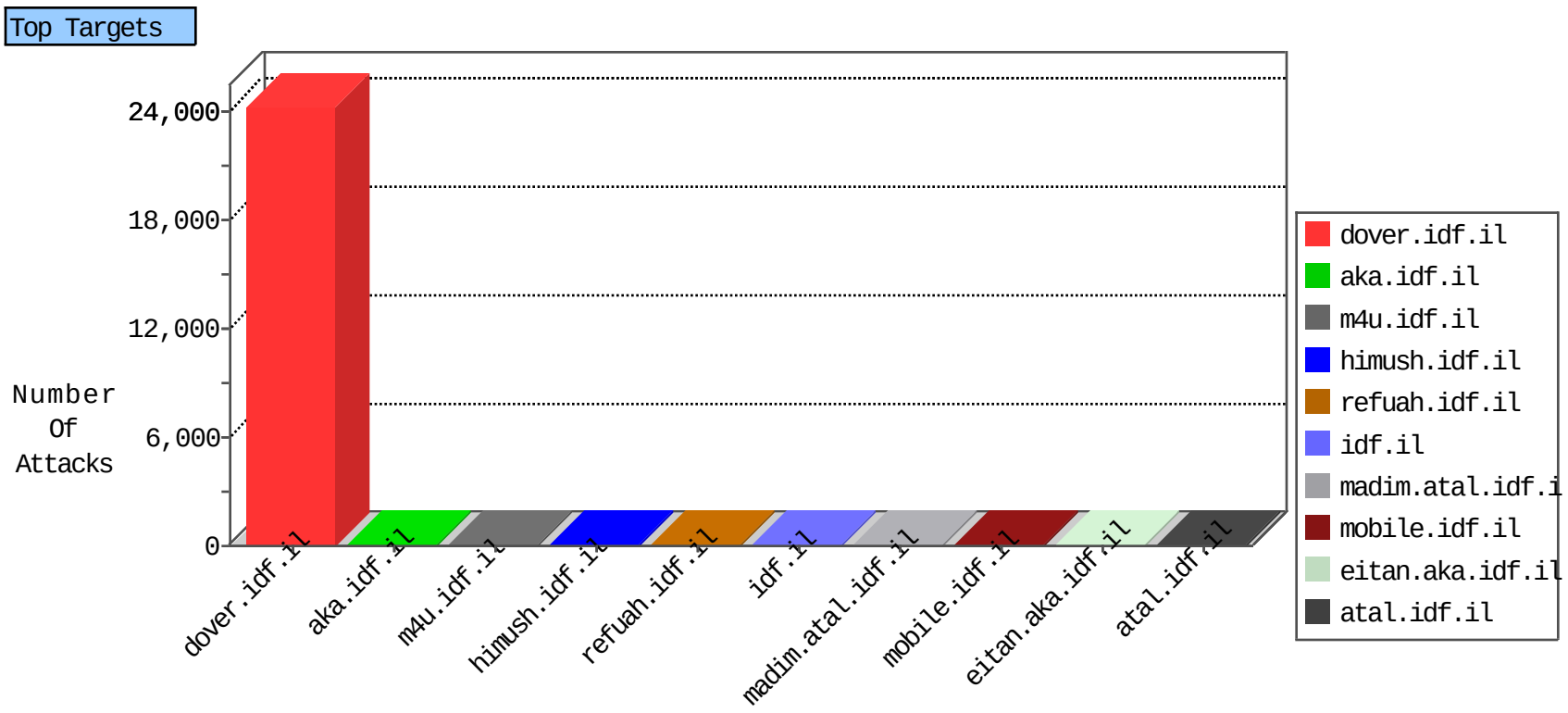
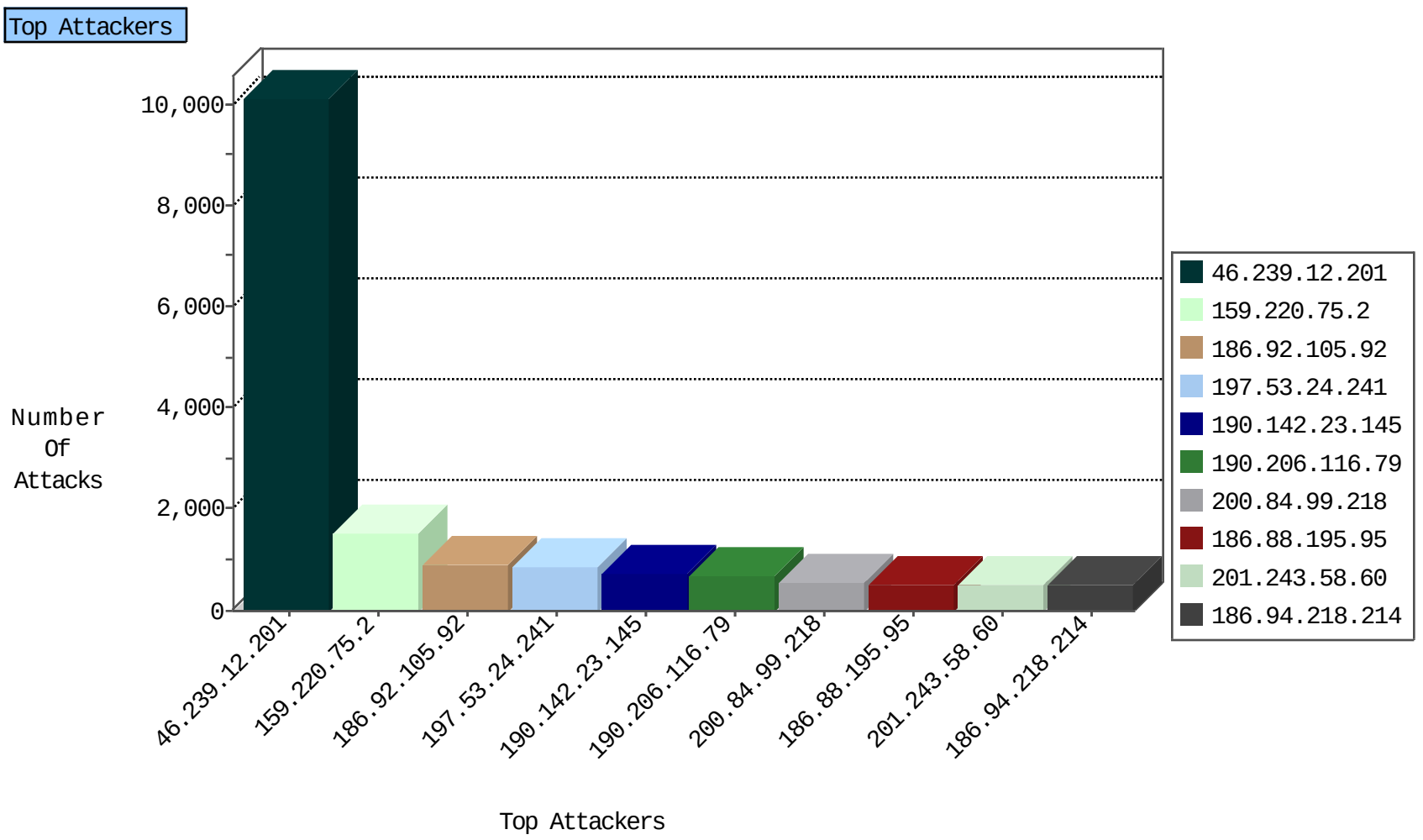
08-26-2016-01:07:19 to 08-26-2016-02:07:19

IDF Under Attack Daily Report





08-26-2016-01:07:19 to 08-26-2016-02:07:19

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	2627183
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	520700
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	342395
197.118.7.45	Algeria	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	4361
181.161.229.143	Chile	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	1384
159.220.75.2	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1082
197.53.24.241	Egypt	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	469
159.220.75.2	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	454
190.142.23.145	Venezuela	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	453
186.92.105.92	Venezuela	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	401
197.53.24.241	Egypt	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	346
200.84.99.218	Venezuela	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	330
186.94.218.214	Venezuela	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	325
190.206.116.79	Venezuela	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	323
186.88.195.95	Venezuela	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	298
186.92.105.92	Venezuela	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	297
190.206.116.79	Venezuela	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	258
201.243.58.60	Venezuela	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	247
109.226.40.40	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	216
190.142.23.145	Venezuela	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	207
186.88.195.95	Venezuela	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	203
201.211.30.212	Venezuela	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	203
200.84.99.218	Venezuela	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	197
186.94.218.214	Venezuela	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	193
186.92.105.92	Venezuela	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	192
186.185.255.50	Venezuela	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	188
201.243.58.60	Venezuela	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	171
190.39.24.177	Venezuela	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	167
190.205.185.112	Venezuela	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	166
186.153.180.10	Argentina	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	142
201.248.194.154	Venezuela	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	139
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	134
190.205.185.112	Venezuela	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	123
68.180.230.171	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	123
201.249.13.82	Venezuela	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	112
190.206.116.79	Venezuela	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	109
68.180.230.171	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	107
190.39.24.177	Venezuela	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	102
41.34.203.1	Egypt	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	99
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	96
66.249.69.14	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	94
201.248.194.154	Venezuela	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	93
190.37.114.78	Venezuela	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	89
190.142.23.145	Venezuela	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	89
201.243.58.60	Venezuela	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	80
156.205.199.204	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	75
190.162.251.103	Chile	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	71
197.48.254.38	Egypt	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	69
201.208.18.143	Venezuela	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	68
212.199.57.206	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	67

08-26-2016-01:07:19 to 08-26-2016-02:07:19

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

08-26-2016-01:07:19 to 08-26-2016-02:07:19

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
190.255.14.8	147.237.0.33	Colombia	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
180.97.81.71	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
133.242.4.52	147.237.72.167	Japan	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
133.208.21.66	147.237.76.38	Japan	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
123.206.85.139	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.8.46	Ukraine	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
50.116.123.135	147.237.77.243	United States	mobile.idf.il	ET SCAN Potential SSH Scan	1
50.116.123.135	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
201.238.202.219	147.237.76.30	Chile	himush.idf.il	ET SCAN NMAP -sS window 1024	1
190.69.225.211	147.237.0.35	Colombia	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
163.172.169.150	147.237.77.235	United Kingdom	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
133.242.4.52	147.237.0.16	Japan	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
123.206.85.139	147.237.76.42	China	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
103.207.38.14	147.237.77.74	Vietnam	law.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.76.117	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
50.116.123.135	147.237.77.212	United States	e.dover.idf.il	ET SCAN Potential SSH Scan	1

08-26-2016-01:07:19 to 08-26-2016-02:07:19

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.239.12.201	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9579
46.239.12.201	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop		drop	544
40.77.169.99	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	43
40.77.169.103	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
40.77.169.96	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	14
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
40.77.169.103	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	7
46.120.129.196	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.199.57.206	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.238.166.152	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
77.125.8.125	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
176.13.17.168	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
85.64.211.195	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
212.179.42.227	Israel	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	3
141.8.184.13	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
85.130.183.141	Israel	147.237.76.200	eitan.aka.idf.il	drop	First packet isn't SYN	drop	2
109.253.216.160	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
213.8.204.60	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
81.165.165.100	Belgium	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
141.8.183.17	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
45.33.42.9	United States	147.237.0.200	m4u.idf.il	drop		drop	2
169.229.3.91	United States	147.237.77.234	halag.idf.il	drop	SAM rule	drop	1
159.220.75.2	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	1
141.212.122.106	United States	147.237.0.200	m4u.idf.il	drop		drop	1
79.178.254.6	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
46.119.122.177	Ukraine	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.77.243	mobile.idf.il	drop	SAM rule	drop	1
159.220.75.3	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.76.201	e.atal.idf.il	drop	SAM rule	drop	1
141.212.122.107	United States	147.237.0.200	m4u.idf.il	drop		drop	1
165.50.129.191	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	1
141.212.122.163	United States	147.237.0.33	idf.il	drop		drop	1
84.94.106.178	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
46.121.254.156	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
187.191.63.31	Mexico	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	1
169.229.3.91	United States	147.237.8.27	e.madim.atal.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	1
141.212.122.164	United States	147.237.0.33	idf.il	drop		drop	1
169.229.3.91	United States	147.237.72.217	e.idf.il	drop	SAM rule	drop	1

08-26-2016-01:07:19 to 08-26-2016-02:07:19

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.243.203	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	3
40.77.169.98	United States	147.237.77.176	matpash.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
84.94.191.196	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/yuatl/templates/sendtofriend/sendtofriend.aspx	Block	1
66.249.76.117	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
5.165.252.239	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/haredim/general.aspx	Block	1
79.179.22.170	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/1119-he/atal.aspxvk	Block	1
46.120.129.246	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/zgowp/templates/navmenu/navmenu.css.aspx	Block	1
85.65.197.0	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
77.124.57.70	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/oprolescategory/oprolescategory.in.aspx	Block	1
31.154.81.77	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/bgunz/templates/navmenu/navmenu.css.aspx	Block	1
180.76.15.23	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8911-he/refuah.aspx	Block	1
79.183.47.228	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.229.164.99	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
91.135.102.171	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.139.116.48	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/lomdim/tochen/	Block	1
180.76.15.31	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
84.94.1.51	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/otari/templates/navmenu/navmenu.css.aspx	Block	1
66.249.75.174	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1
2.53.38.149	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
95.174.36.190	Poland	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.178.13.239	Israel	147.237.76.30	himush.idf.il	Unauthorized HTTP Method	Block	1
46.19.85.156	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/obmkf/templates/navmenu/navmenu.css.aspx	Block	1
212.199.57.206	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/gkopj/templates/navmenu/navmenu.css.aspx	Block	1
84.94.106.178	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/menle/shared/ajax/getemergencybanner.aspx	Block	1
66.249.76.98	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list.htm	Block	1
2.55.131.54	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xxrqb/shared/ajax/getemergencybanner.aspx	Block	1
148.251.2.180	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/iturim/asp/displayonesoldier.asp	Block	1
79.178.13.239	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.tech.atal.idf.il/1271-he/	Block	1
46.19.85.191	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/yihwi/	Block	1

08-26-2016-01:07:19 to 08-26-2016-02:07:19