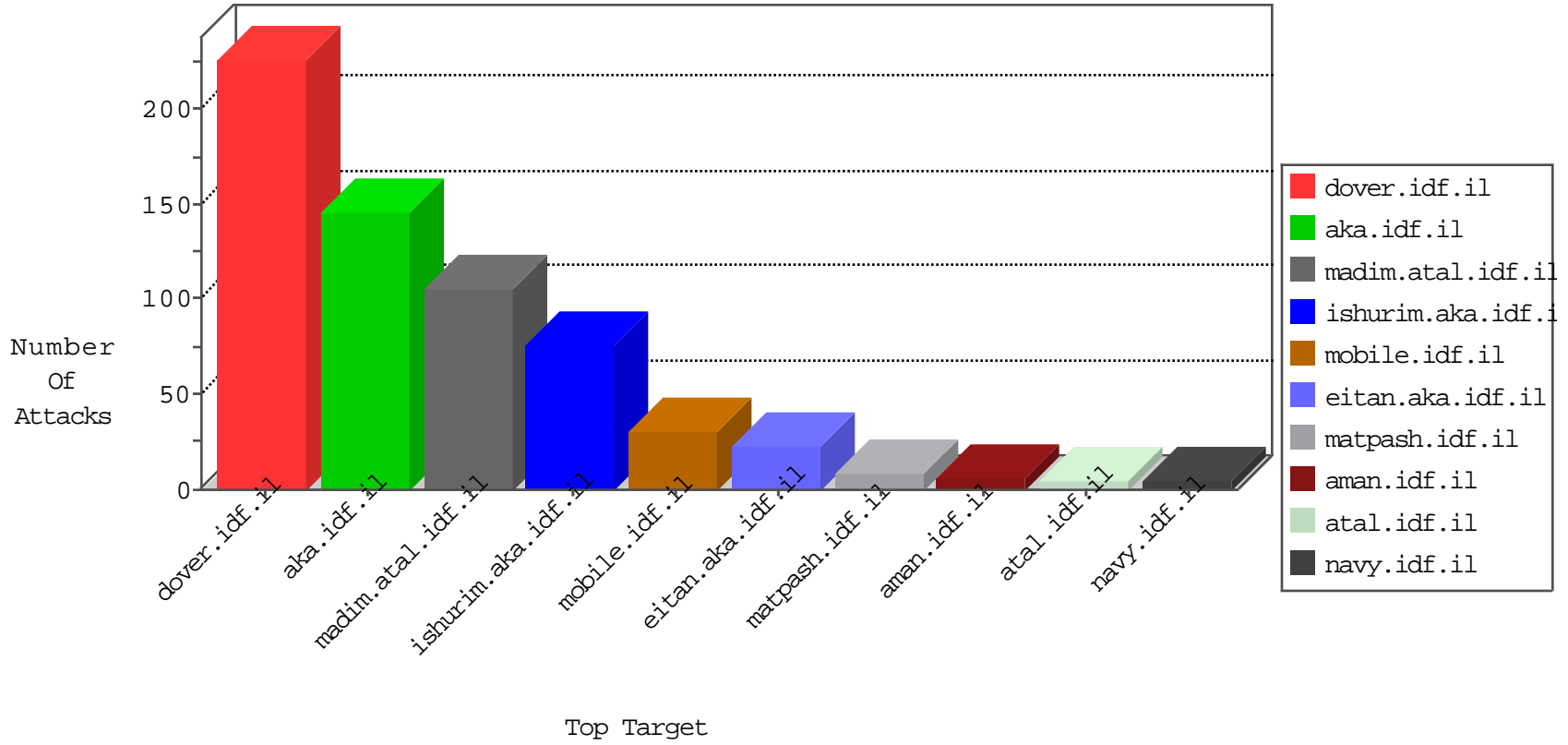


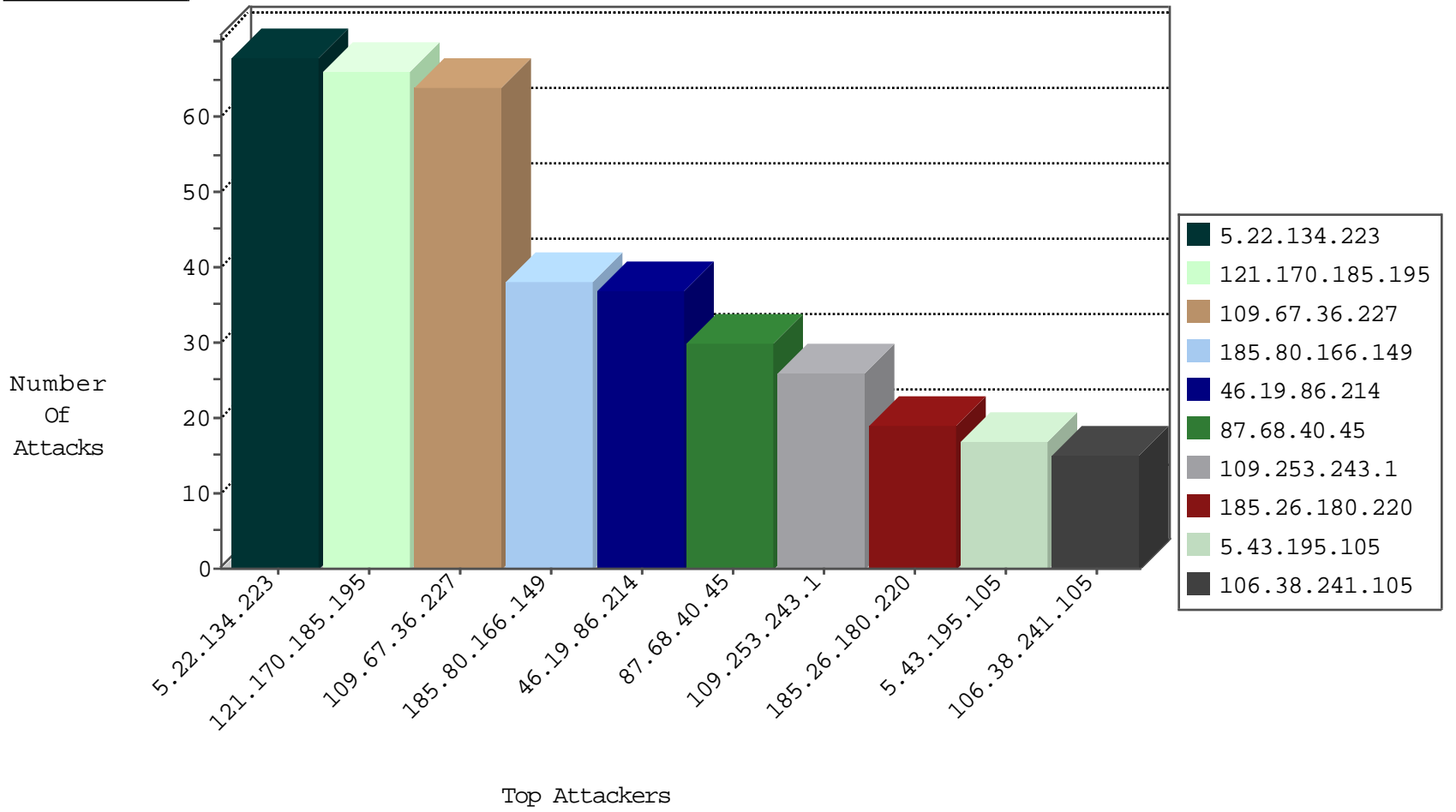
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
130.217.77.2	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
204.85.191.11	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
0.0.0.0		147.237.72.216	dover.idf.il	HTTP Page Flood Attack	forward	2
193.1.13.14	Ireland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
164.107.127.12	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
165.242.90.128	Japan	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
134.197.113.3	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
129.93.229.138	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
216.48.80.14	Canada	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
156.56.250.227	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
130.206.158.138	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.208.4.198	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
139.78.141.243	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.8.126.111	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
194.254.215.12	France	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
147.83.29.234	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
121.170.185.195	Korea, Republic of	147.237.77.216	dover.idf.il	C1000011: HTTP: Fuck in url	Permit	54
185.80.166.149	Macedonia, the Former Yugoslav Republic of	147.237.72.166	aka.idf.il	C1000076: HTTP: Trying to locate existing FCKeditor	Permit	28
86.132.208.154	United Kingdom	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
84.93.84.77	147.237.77.74	United Kingdom	law.idf.il	Tehila - Perl LWP with fake user agent	2
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	2
41.180.9.40	147.237.76.147	South Africa	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.98	147.237.77.234	United States	halag.idf.il	ET DROP Dshield Block Listed Source	1
162.243.218.193	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
133.208.21.66	147.237.76.201	Japan	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
103.207.39.82	147.237.8.50	Vietnam	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
93.158.203.168	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
185.120.125.131	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
133.242.4.52	147.237.8.46	Japan	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
133.208.21.66	147.237.76.197	Japan	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
93.158.203.168	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
92.29.69.152	147.237.76.31	United Kingdom	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	147.237.76.199	China	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.67.36.227	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
87.68.40.45	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.19.86.214	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	25
185.26.180.220	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
109.75.78.69	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
46.19.86.214	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
5.43.195.105	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.175	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
94.99.84.187	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.210	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
5.22.134.223	Israel	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	6
84.111.132.56	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
85.144.127.246	Netherlands	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.86.56	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
131.253.27.67	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
199.30.24.94	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.253	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
5.43.195.105	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
212.179.241.1	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
24.84.192.225	Canada	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	3
109.253.131.0	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
121.170.185.195	Korea, Republic of	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
2.53.175.228	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.55.36.60	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
121.170.185.195	Korea, Republic of	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
176.13.229.94	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.55.20.252	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
213.57.157.210	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
40.85.132.92	Ireland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
2.53.47.21	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
176.13.229.94	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
84.111.184.158	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
46.19.86.228	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
93.104.215.125	Germany	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
79.178.162.116	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
109.253.213.110	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
65.55.210.6	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
106.38.241.105	China	147.237.76.86	navy.idf.il	drop	SAM rule	drop	2
46.19.86.131	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
106.38.241.105	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
176.13.9.241	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
84.109.162.252	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
106.38.241.105	China	147.237.77.234	halag.idf.il	drop	SAM rule	drop	1
216.243.31.2	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
106.38.241.105	China	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	1
195.62.53.168	Russian Federation	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.22.134.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	62
109.253.243.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
79.178.222.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
121.170.185.195	Korea, Republic of	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 121.170.185.195	Block	4
185.80.166.149	Macedonia, the Former Yugoslav Republic of	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 185.80.166.149	Block	4
46.117.38.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
50.141.216.141	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/ishurim/main/	Block	3
185.80.166.149	Macedonia, the Former Yugoslav Republic of	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	3
31.168.72.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.238	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
180.76.15.144	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
185.80.166.149	Macedonia, the Former Yugoslav Republic of	147.237.72.166	aka.idf.il	Unauthorized Method PROPFIND for aka.idf.il/	Block	1
121.170.185.195	Korea, Republic of	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
66.249.65.52	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
46.19.85.210	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
185.30.90.22	Azerbaijan	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
84.111.233.36	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
185.80.166.149	Macedonia, the Former Yugoslav Republic of	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/index.php	Block	1
31.14.248.97	Egypt	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
121.170.185.195	Korea, Republic of	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 121.170.185.195	Block	1
68.180.229.223	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman/	Block	1
46.19.85.210	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version deflate	Block	1
185.80.166.149	Macedonia, the Former Yugoslav Republic of	147.237.72.166	aka.idf.il	Admin Blocking	Block	1
95.220.132.100	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
66.249.64.12	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
204.79.180.65	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
31.14.248.97	Egypt	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/wp-login.php	Block	1
77.139.16.47	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunlobby.aspx	Block	1
46.19.85.210	Israel	147.237.77.216	dover.idf.il	Malformed URL gzip,	Block	1
109.226.26.126	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
212.179.241.1	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
121.170.185.195	Korea, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/admin/fckeditor/t0phackteam/webfuck.shell	Block	1
77.139.242.229	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
46.19.85.210	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method Accept-Encoding: in URL gzip,	Block	1
66.249.64.45	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1