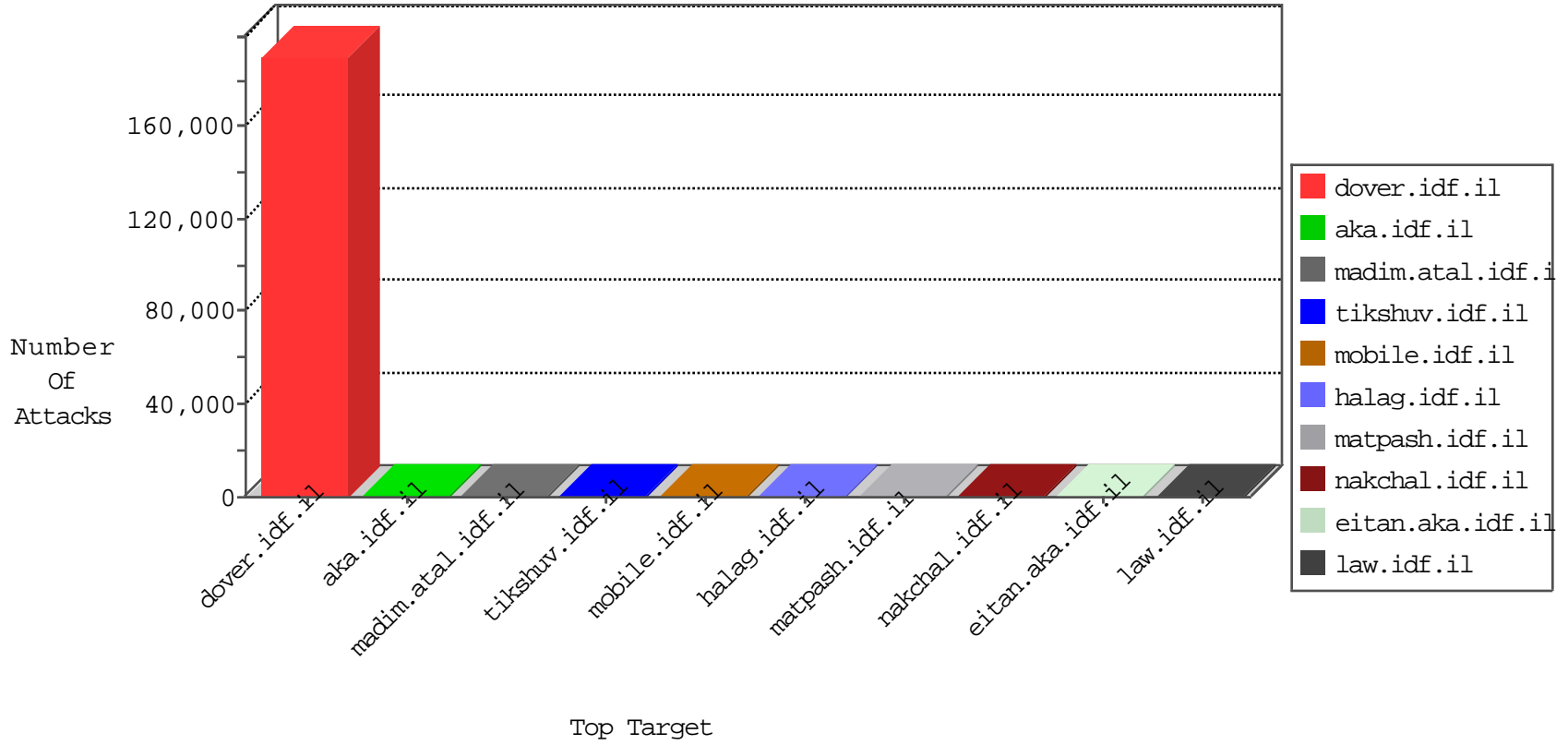


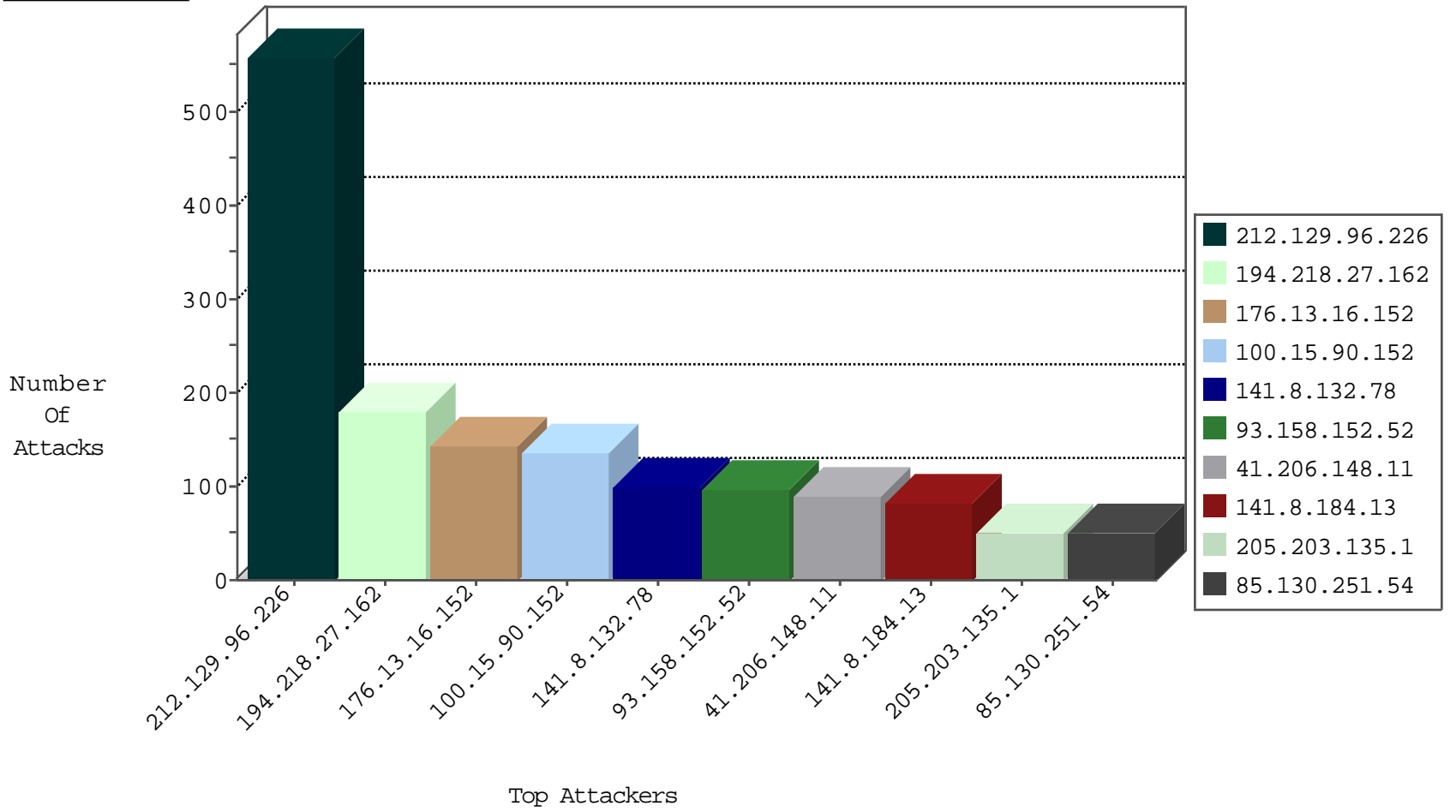
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
48.134.97.193	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	37713
62.196.20.133	Italy	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	36645
64.210.7.110	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	36535
225.70.227.37		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	36519
201.153.26.107	Mexico	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	36390
198.58.250.46	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	36382
48.131.196.189	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	36356
71.132.121.215	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	36309
144.128.156.111	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	36301
193.137.6.155	Portugal	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	36230
231.203.236.255		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	36140
232.158.119.149		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	36084
113.145.103.223	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	36055
18.175.203.248	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35894
49.69.212.179	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35844
62.26.93.122	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35815
99.246.148.127	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35810
216.206.154.150	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35798
160.208.183.23	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35672
1.58.211.200	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35663
101.195.118.204	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35661
160.20.38.113	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35642
73.151.81.143	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35546
36.18.120.202	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35527
223.67.27.185	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35477
149.252.208.255	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35417
191.48.136.46	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35389
228.245.255.101		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35310
219.102.86.8	Japan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35282
246.232.178.10		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35282
76.180.143.137	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35136
84.2.191.175	Hungary	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35041
105.115.172.150	Nigeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	35041
231.106.41.188		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34956
164.6.175.49	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34943
75.189.124.57	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34794
53.223.97.234	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34648
167.165.200.119	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34616
145.82.129.207	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34585
45.4.95.32		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34576
241.110.23.193		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34558
4.99.204.116	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34536
33.239.103.63	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34439
52.167.137.60	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34429
167.34.7.155	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34360
60.219.87.162	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34357
144.21.238.15	Portugal	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34296
253.111.82.211		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34260
158.227.252.203	Spain	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34249
102.243.86.248		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	34235

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.64.73.193	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	16
61.135.189.119	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	3
2.54.146.170	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
246.29.111.184		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	2
252.105.96.224		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
240.0.84.26		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.0.96.133		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.0.109.214		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.0.114.27		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.0.142.53		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.0.184.158		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.0.202.135		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.0.242.34		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.1.119.21		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.1.121.19		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.1.185.84		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.1.238.241		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.1.239.74		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.1.239.148		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.1.239.182		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.2.85.74		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.2.94.147		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.2.100.189		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.2.219.213		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.3.48.240		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.3.56.226		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.3.81.210		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.3.89.184		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.3.141.92		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.3.172.95		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.3.196.35		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.3.209.242		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.4.4.132		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.4.36.12		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.4.41.8		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.4.53.103		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.4.111.206		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.4.128.95		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.4.180.166		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.4.187.18		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.5.78.240		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.5.103.140		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.5.119.45		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.5.151.40		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.5.154.60		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.5.167.65		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.5.195.247		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1
240.5.218.253		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
85.64.2.84	147.237.76.30	Israel	himush.idf.il	ET SCAN NMAP -sA (2)	2
217.55.204.12	147.237.77.216	Egypt	dover.idf.il	portscan: TCP Distributed Portscan	1
138.43.240.230	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
61.240.144.67	147.237.0.19	China	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
213.8.204.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
137.226.113.7	147.237.72.156	Germany	aman.idf.il	ET SCAN Suspicious User-Agent Containing Web Scan/er, Likely Web Scanner	1
45.32.49.30	147.237.76.34		yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
112.72.184.211	147.237.0.17	Korea, Republic of	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
202.71.25.29	147.237.77.212	India	e.dover.idf.il	ET SCAN NMAP -sS window 3072	1
37.26.148.197	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.135.165	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.183.44.155	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
8.37.230.85	147.237.77.216	Anonymous Proxy	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.30.75	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.201.227.70	147.237.0.16	Ukraine	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
2.54.55.159	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
95.217.174.35	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
189.218.144.196	147.237.77.234	Mexico	halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
89.139.13.220	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.23.243	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.36.220	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
143.49.52.248	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
79.180.0.155	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.136.91.26	147.237.77.61	Germany	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
138.43.91.175	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
46.121.100.206	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.199.182.150	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
128.199.57.97	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
45.32.49.30	147.237.76.34		yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
209.148.91.8	147.237.77.216	United States	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
109.253.216.93	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
202.71.25.29	147.237.77.212	India	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
24.13.206.70	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.96.230	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
194.50.175.46	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.9.114	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.128.144.131	147.237.77.176	Canada	matpash.idf.il	ET SCAN NMAP -sS window 4096	1
192.219.172.228	147.237.77.216	Canada	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
93.172.26.80	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
177.238.147.122	147.237.76.34	Mexico	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
85.64.81.23	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
172.56.21.133	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
100.15.90.152	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	136
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	120
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	100
93.158.152.52	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	96
141.8.184.13	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	82
41.206.148.11	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	60
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
173.208.130.67	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
31.154.148.177	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	35
95.159.5.92	Syrian Arab Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
79.180.185.179	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
93.158.152.68	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
109.64.73.193	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
92.236.75.7	United Kingdom	147.237.77.216	dover.idf.il	drop	SAM rule	drop	20
85.130.251.54	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
85.130.251.54	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
94.11.30.69	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
213.57.172.234	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
198.58.103.92	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
139.162.216.112	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
107.170.142.158	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
149.88.109.135	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.85.60	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.29	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
5.22.131.29	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
5.22.131.29	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
41.206.148.11	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
85.130.251.54	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.206	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
37.46.39.6	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
217.31.55.69	Czech Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.66.202.238	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
141.8.132.95	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.179.161.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.139.17	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.77	Israel	147.237.76.200	eitan.aka.idf.il	drop	First packet isn't SYN	drop	6
41.206.148.11	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
50.108.23.219	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
70.198.202.255	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.16.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	142
89.138.101.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
66.249.64.190	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.190	Block	14
46.19.85.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
37.142.191.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.66.202.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.130.249	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
199.30.25.27	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.19.85.60	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
2.54.171.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	2
90.154.240.200	Bulgaria	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
79.178.102.73	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
208.49.213.4	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.102.9.91	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
109.66.202.238	Israel	147.237.77.243	mobile.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.146.209	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
87.69.121.223	Israel	147.237.76.39	mobile.meitav.idf.il	Parameter Type Violation ct100\$ContentPlaceholder1\$txtPassword in mobile.meitav.idf.il/templates/login.aspx	Block	1
66.249.66.72	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 66.249.66.72	Block	1
40.77.167.77	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
185.35.62.11	Switzerland	147.237.76.147	chinuch.aka.idf.il	Multiple Unauthorized URL Access from 185.35.62.11	Block	1
95.86.125.19	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/sachar/	Block	1
79.178.102.73	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.76.110.63	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ved in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
109.67.198.246	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct157 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
37.26.148.184	Israel	147.237.77.243	mobile.idf.il	Untraceable SSL Sessions: Open Mode	None	1
87.71.77.134	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.66.76	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	1
185.35.62.11	Switzerland	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
108.30.58.92	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.246.130.0	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
213.57.172.234	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter Do in www.aka.idf.il/giyus/general/default.asp	None	1
149.78.223.38	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct113 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
88.0.124.214	Spain	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
66.249.66.129	United States	147.237.76.200	eitan.aka.idf.il	Unknown Parameter PageNum in www.eitan.aka.idf.il/938-en/eitan.aspx	None	1
198.58.103.92	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
17.142.156.109	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/shalishut/site/faq.aspx	None	1
37.203.214.2	Sweden	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	1
157.55.39.148	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/imagevideogallerylobby/	Block	1
79.177.147.174	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/hgiyus	Block	1
46.120.134.152	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct102\$ct103\$txtField in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
109.66.202.238	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
31.154.148.177	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
86.162.10.209	United Kingdom	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/shalishut/site/list.aspx	None	1
37.203.214.2	Sweden	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/wp-login.php	Block	1