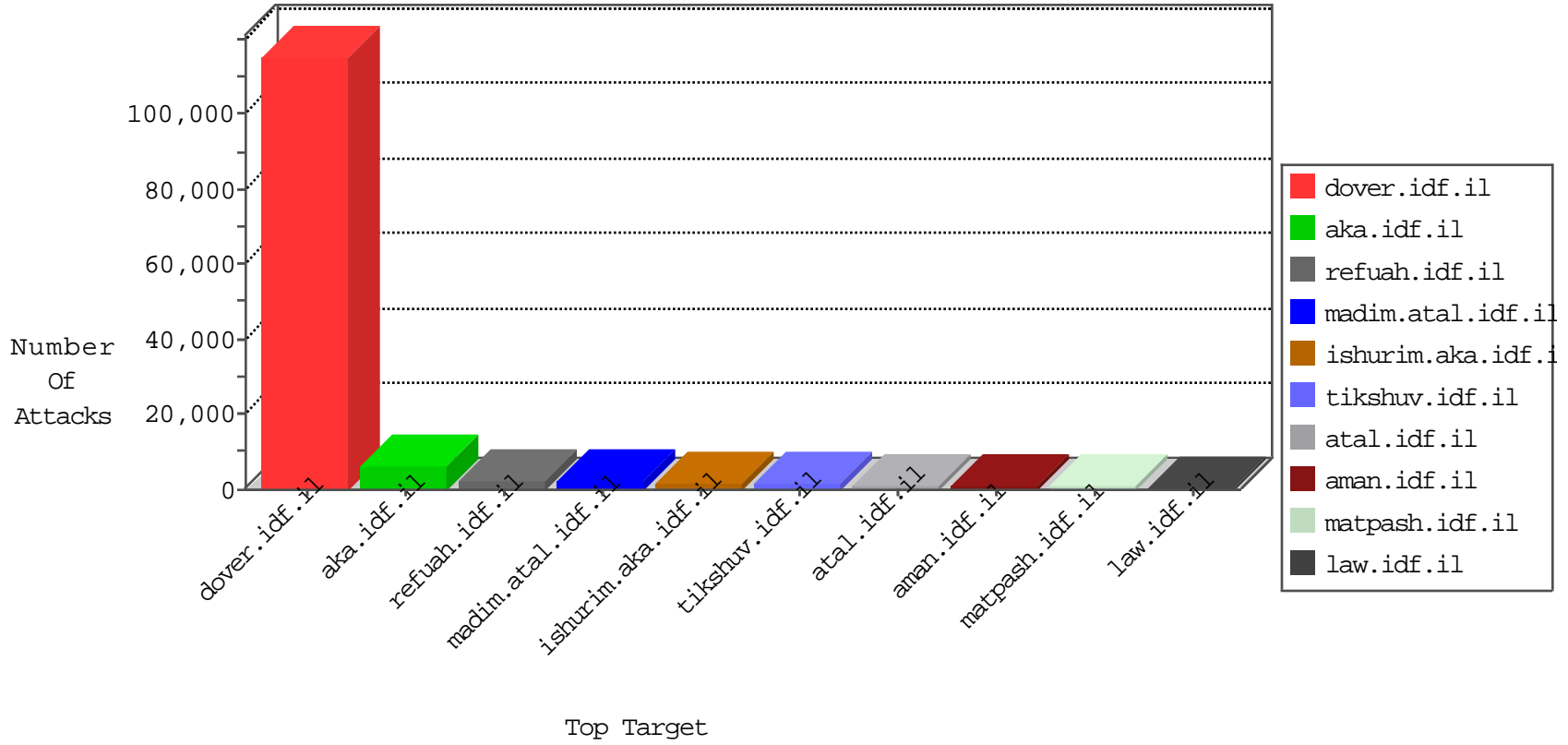


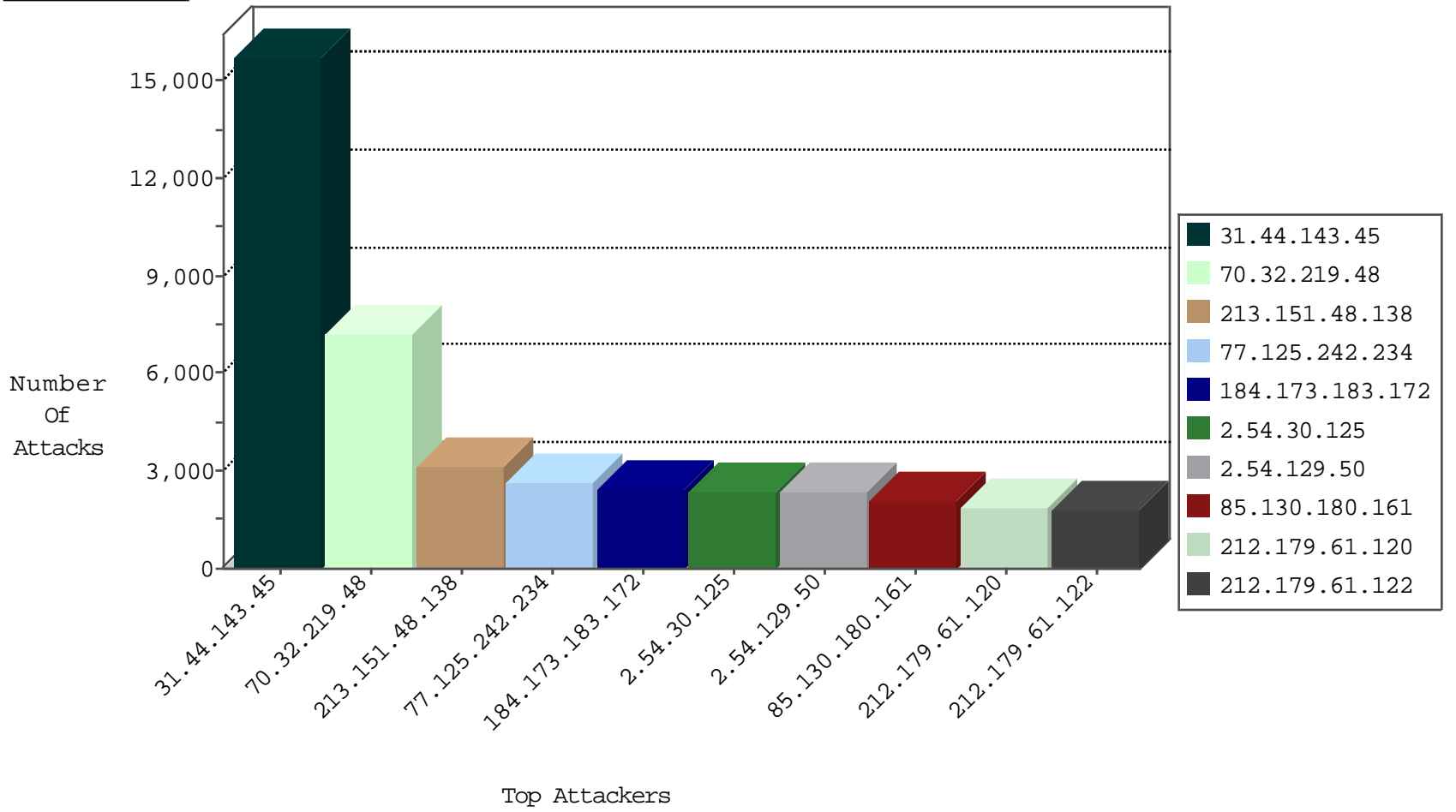
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.78.159	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4793
66.249.78.173	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4786
66.249.78.96	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	4052
79.182.175.81	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cl	dest-reset	822
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	605
212.179.61.125	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	499
46.121.121.44	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cl	dest-reset	487
84.108.112.20	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cl	dest-reset	485
82.166.20.23	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cl	dest-reset	479
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cl	forward	366
79.178.166.189	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cl	dest-reset	343
220.181.108.144	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	328
95.86.113.2	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cl	dest-reset	311
212.199.154.194	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cl	dest-reset	301
98.193.57.41	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	275
46.121.203.241	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cl	dest-reset	264
66.249.78.22	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	264
85.65.17.196	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cl	dest-reset	257
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cl	dest-reset	249
79.183.196.165	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cl	dest-reset	183
213.57.99.34	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cl	dest-reset	173
213.57.21.62	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cl	dest-reset	167
94.230.87.7	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cl	dest-reset	167
176.12.141.52	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cl	dest-reset	164
220.181.108.120	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	164
220.181.108.86	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	161
81.218.163.154	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cl	dest-reset	160
149.88.108.23	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cl	dest-reset	160
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	156
79.182.169.151	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cl	dest-reset	156
84.108.9.212	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cl	dest-reset	148
109.67.55.4	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cl	dest-reset	146
212.179.61.122	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cl	dest-reset	145
79.177.56.105	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cl	dest-reset	143
149.78.195.132	United States	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cl	dest-reset	142
212.179.61.125	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cl	dest-reset	140
84.109.216.190	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cl	dest-reset	136
220.181.108.163	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	131
220.181.108.92	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	115
2.54.158.210	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cl	dest-reset	114
220.181.108.75	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	109
79.181.140.193	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cl	dest-reset	104
85.64.127.117	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cl	dest-reset	101
2.52.32.212	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cl	dest-reset	101
5.29.117.206	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cl	dest-reset	97
176.12.145.71	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cl	dest-reset	91
185.32.178.120	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cl	dest-reset	88
5.29.120.137	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cl	dest-reset	88
220.181.108.111	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	85
46.19.85.106	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cl	dest-reset	83

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
77.125.87.109	Israel	147.237.72.167	ishurim.aka.idf.il	DVRep_P-N_40-59	Permit	1261
84.94.163.167	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	715
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	670
184.173.183.172	United States	147.237.77.233	atal.idf.il	DVRep_P-N_40-59	Permit	650
84.111.24.80	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	445
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	330
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	324
184.173.183.172	United States	147.237.76.31	nakchal.idf.il	DVRep_P-N_40-59	Permit	313
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	145
184.173.183.172	United States	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	128
77.125.87.158	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	119
109.66.164.198	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	27
80.178.13.219	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	25
62.219.143.26	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	20
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	20
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	20
212.25.102.57	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	18
183.60.217.62	China	147.237.76.31	nakchal.idf.il	DVRep_P-N_40-59	Permit	18
81.218.48.37	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	17
5.102.254.184	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	17
213.57.20.226	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	17
46.118.157.21	Ukraine	147.237.77.176	matpash.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	15
46.116.150.130	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	14
93.172.174.78	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	13
89.139.171.79	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	13
212.29.231.212	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	12
109.253.145.133	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	12
146.0.42.58	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	12
82.80.56.15	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	12
77.127.47.27	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	12
95.179.112.2	Russian Federation	147.237.77.170	maarachot.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	11
95.179.112.2	Russian Federation	147.237.77.176	matpash.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	11
89.139.188.134	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	11
79.177.3.19	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	10
149.78.137.30	United States	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	10
93.173.19.11	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	9
192.114.23.208	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	9
149.78.119.211	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	9
109.186.156.78	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	9
31.154.25.102	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	9
109.66.52.7	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
84.228.211.66	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
87.69.71.237	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
2.54.153.91	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
77.127.182.153	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
85.65.106.120	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
46.116.58.151	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
193.43.245.250	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
79.178.2.220	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
85.250.155.145	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8

Top Attackers In ID

Attacker Address	Attacker Country	Target Address	Site	Name	Count
70.32.219.48	United States	147.237.77.216	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	7135
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	179
46.19.86.157	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	41
107.6.154.228	Netherlands	147.237.77.216	dover.idf.il	SERVER-WEBAPP WEB-INF access	13
66.249.78.96	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	8
66.249.64.116	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	6
66.249.78.89	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	5
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	4
84.21.142.230	United Kingdom	147.237.77.170	maarachot.idf.il	Tehila - Perl LWP with fake user agent	4
107.6.154.228	Netherlands	147.237.77.216	dover.idf.il	ET SCAN DEBUG Method Request with Command	4
183.136.216.4	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	3
66.249.78.82	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	3
107.6.154.228	Netherlands	147.237.77.216	dover.idf.il	SERVER-WEBAPP TRACE attempt	3
91.224.132.118	Russian Federation	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.81.204	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
84.21.142.230	United Kingdom	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
221.235.189.245	China	147.237.77.227	e.haraz.idf.il	ET SCAN Potential SSH Scan	2
95.110.183.83	Italy	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
185.32.178.118	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
94.159.238.63	Israel	147.237.77.233	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 Ddos attack	2
107.6.154.228	Netherlands	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
91.224.132.118	Russian Federation	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	2
107.6.154.228	Netherlands	147.237.77.216	dover.idf.il	SERVER-WEBAPP client negative Content-Length attempt	2
188.165.129.51	Spain	147.237.77.176	matpash.idf.il	Tehila - Perl LWP with fake user agent	2
61.240.144.64	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	2
61.183.128.6	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	2
128.199.241.231	Singapore	147.237.72.166	aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	2
89.139.171.79	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
81.218.77.162	Israel	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	2
61.240.144.66	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	2
91.224.132.118	Russian Federation	147.237.77.226	www.chanatz.aka.idf.il	ET SCAN NMAP -sS window 1024	2
80.246.137.124	Israel	147.237.0.19	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
183.247.165.129	China	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	2
61.183.128.6	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.131	Japan	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	2
218.24.171.223	China	147.237.8.27	e.madim.atal.idf.il	GPL SCAN nmap TCP	2
66.249.78.222	United States	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sA (2)	2
192.95.33.188	Canada	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
183.136.216.4	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	2
91.224.132.118	Russian Federation	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	2
205.254.147.8	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
185.32.176.96	Israel	147.237.0.19	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
66.249.78.15	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.130	Japan	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.66	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.64	China	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.131	Japan	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
66.249.69.84	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.130	Japan	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.131	Japan	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	2

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
31.44.143.45	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15752
213.151.48.138	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3149
77.125.242.234	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2655
2.54.30.125	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2365
2.54.129.50	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2350
85.130.180.161	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2092
212.179.61.122	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1746
212.179.61.120	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1742
164.138.124.146	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1583
87.68.75.20	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1477
212.179.132.202	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1473
212.179.61.125	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1469
81.218.251.252	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1332
8.37.224.60	Anonymous Proxy	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1138
194.50.175.183	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1126
213.57.29.126	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	1088
82.145.216.29	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1044
89.139.188.134	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	989
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	886
93.172.154.44	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	845
212.116.173.226	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	811
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	805
89.139.171.79	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	783
81.218.251.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	673
46.121.233.152	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	621
87.68.59.143	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	549
212.179.21.197	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	494
2.54.145.162	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	478
212.179.61.124	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	472
2.54.191.164	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	432
79.182.129.79	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	416
46.19.85.92	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	396
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	390
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	372
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	365
63.217.168.125	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	329
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	326
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	321
212.143.120.158	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	317
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	314
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	308
213.57.241.19	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	289
107.6.154.228	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	288
91.227.71.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	285
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	276
46.19.85.96	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	256
81.218.126.226	Israel	147.237.76.42	refuah.idf.il	Windows System Files Information Disclosure	Web Server Enforcement Violation	reject	254
37.26.148.230	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	252
149.78.200.119	United States	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	250
174.95.106.217	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	234

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
89.139.1.154	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 89.139.1.154	Block	498
185.32.178.41	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 185.32.178.41	Block	324
84.110.53.109	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 84.110.53.109	Block	279
46.19.86.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	269
80.246.137.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	246
185.32.176.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	129
46.19.85.206	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.206	Block	100
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	90
109.253.137.6	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.137.6	Block	86
185.32.176.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	63
80.246.133.209	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	57
157.55.39.201	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	45
192.114.5.10	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	40
207.46.13.138	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	37
212.179.132.203	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 212.179.132.203	Block	37
85.64.86.174	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	36
207.46.13.42	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	31
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	26
66.249.93.245	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	25
37.26.147.216	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.147.216	Block	24
31.44.129.83	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	22
46.116.5.192	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	22
89.139.17.153	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	20
66.249.93.242	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	19
199.168.173.138	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	18
82.80.198.164	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 82.80.198.164	Block	18
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	17
109.64.128.70	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	17
109.64.227.202	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	17
176.12.149.246	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	16
80.246.138.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	15
95.86.66.25	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	14
66.249.93.239	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
95.86.69.47	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	14
213.151.35.218	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	13
94.230.86.159	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	13
37.26.148.134	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 37.26.148.134	Block	13
212.179.61.120	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
185.32.178.147	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	13
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	12
37.8.88.149	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 37.8.88.149	Block	12
85.65.196.205	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	11
109.160.173.95	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	11
212.179.132.204	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 212.179.132.204	Block	11
109.67.107.183	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
157.55.39.153	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	10
212.76.115.233	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.76.115.233	Block	10
79.180.173.201	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	9
46.117.120.36	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	9