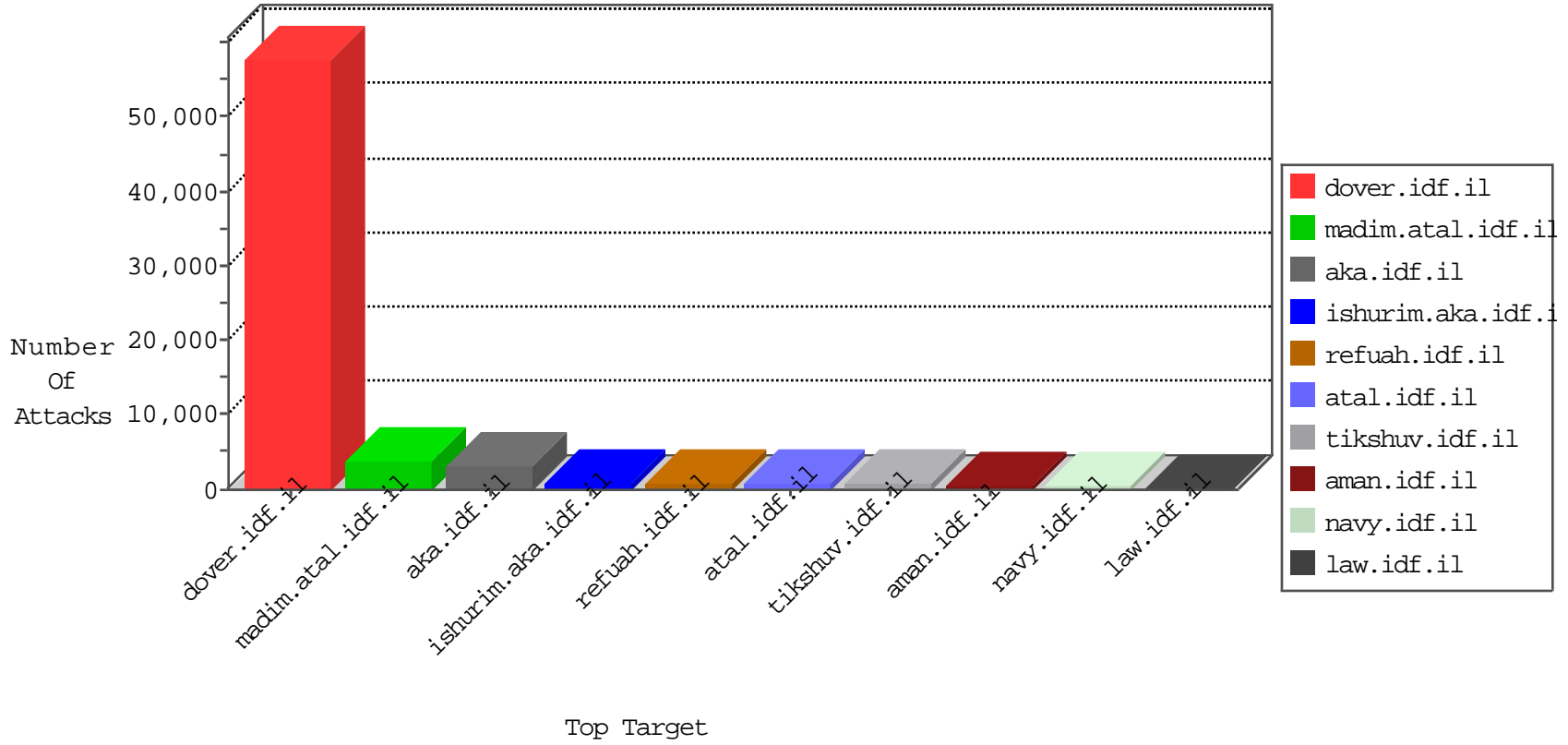


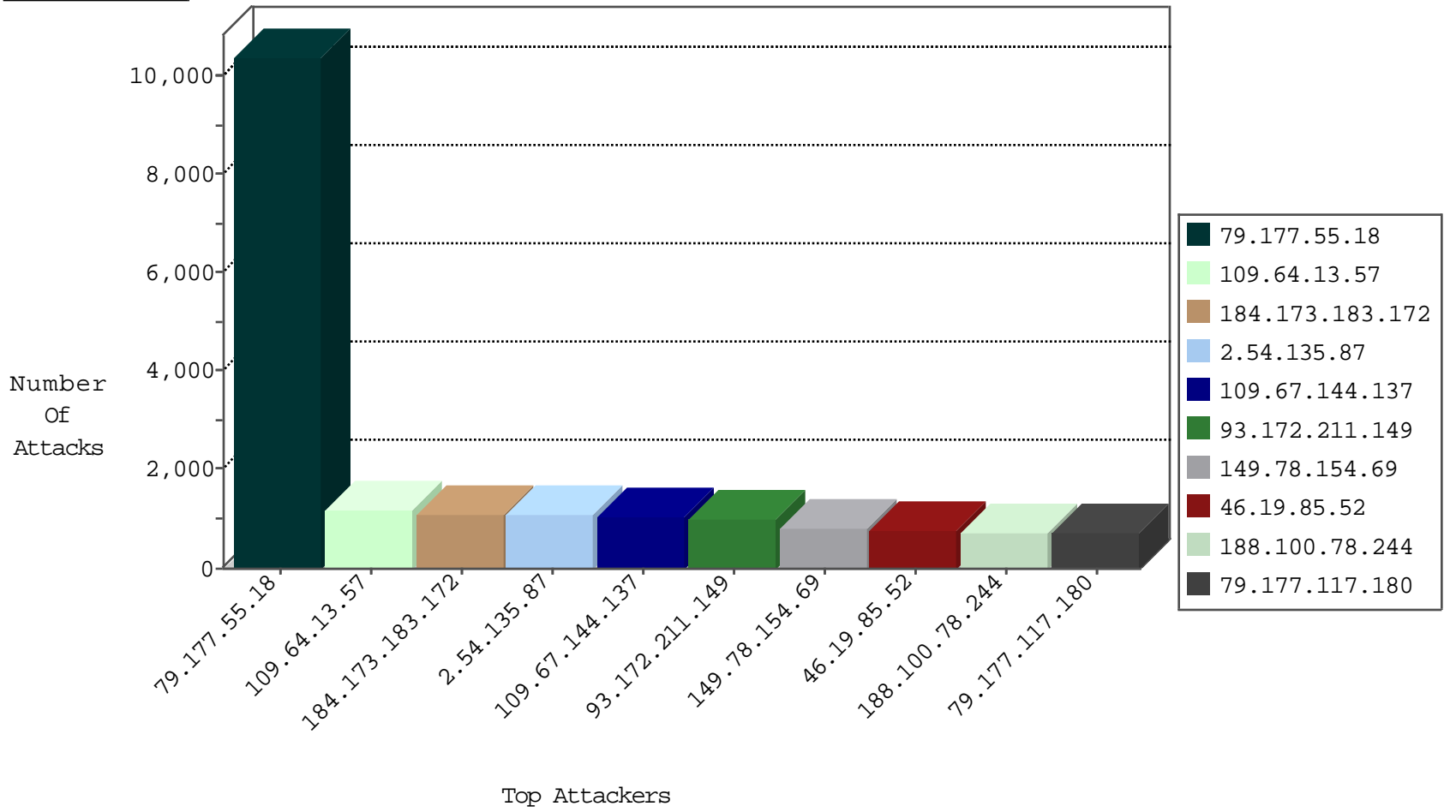
# IDF Under Attack Daily Report



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	10368
66.249.67.229	Israel	147.237.0.34	tikshuv.idf.il	TCP handshake violation, first packet not syn	drop	8930
66.249.78.173	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5105
149.78.154.69	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3186
46.4.123.172	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2566
79.182.173.17	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2560
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	948
100.8.141.122	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	779
5.29.18.179	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	739
66.249.78.190	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	609
192.115.116.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	548
220.181.108.163	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	542
46.19.85.115	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	478
212.179.21.194	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	454
77.126.244.87	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	362
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	314
5.22.130.201	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	254
31.168.90.18	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	253
79.181.161.184	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	245
85.65.82.10	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	240
37.142.213.241	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	240
109.65.5.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	237
79.180.231.231	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	203
79.176.54.98	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	191
193.43.244.102	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	169
5.29.156.248	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	168
37.60.46.143	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	168
220.181.108.175	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	167
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	165
94.159.237.9	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	165
84.94.47.94	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	164
66.249.78.166	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	157
168.235.198.194		147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	152
2.52.161.155	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	137
220.181.108.183	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	124
79.182.135.69	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	121
220.181.108.120	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	119
109.66.56.147	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	107
46.19.86.194	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	104
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	101
77.127.147.66	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	101
46.19.85.228	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	101
164.138.117.50	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	101
85.250.238.255	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	101
85.250.185.131	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	96
176.12.143.194	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	95
176.12.145.188	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	95
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	94
87.69.108.54	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	88
85.65.172.229	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	87

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	943
180.76.5.193	China	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	287
184.173.183.172	United States	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	128
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	124
180.76.5.193	China	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	101
185.4.253.18	Lebanon	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	36
192.115.116.25	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	35
79.181.189.133	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	22
62.219.165.48	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	22
84.110.208.9	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	21
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
79.176.110.207	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	17
85.64.255.47	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	16
212.143.49.22	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	16
79.177.203.3	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	16
46.117.24.17	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	16
89.138.83.176	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	15
81.218.241.26	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	15
85.64.200.198	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	12
79.182.57.215	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	12
85.65.106.120	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	12
209.88.173.130	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	11
66.249.67.229	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	11
77.127.94.46	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	10
132.72.224.221	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	10
84.108.130.25	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	10
149.88.28.188	United States	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	10
46.19.85.19	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	10
46.117.241.155	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
109.64.164.47	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
149.78.145.250	United States	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
93.173.229.35	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
79.178.169.189	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
46.117.221.59	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
84.109.9.199	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
37.26.146.223	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
71.6.165.200	United States	147.237.76.30	hinush.idf.il	DVRep_B-N_60_100	Block	7
157.55.39.222	United States	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	7
46.120.2.93	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	7
46.19.85.191	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
93.173.237.144	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	7
193.43.245.250	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
198.20.70.114	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	7
71.6.135.131	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	7
77.125.133.247	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	7
66.240.192.138	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	6
85.65.202.42	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6
77.127.149.206	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
66.240.192.138	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	6

## Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	91
66.249.65.22	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	24
66.249.73.203	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	14
66.249.73.219	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	11
66.249.73.211	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
66.249.65.48	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
221.235.189.245	China	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	2
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spanhaus DROP Listed Traffic Inbound	2
221.235.189.245	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.64	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	2
144.0.0.60	China	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	2
183.136.216.4	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	2
121.88.5.177	Korea, Republic of	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
176.12.147.168	Israel	147.237.0.19	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
193.189.117.26	Poland	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	2
59.106.108.116	Japan	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
218.24.171.223	China	147.237.76.34	yohalan.idf.il	GPL SCAN nmap TCP	2
221.235.189.245	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	2
104.149.17.166		147.237.77.216	dover.idf.il	SERVER-WEBAPP Manbo upload.php access	2
128.30.52.73	United States	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	2
61.240.144.66	China	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	2
91.238.134.92	Poland	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 1024	2
142.0.37.205	United States	147.237.76.42	refuah.idf.il	ET WEB_SERVER Muieblackcat scanner	2
221.235.189.245	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	2
66.249.65.80	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
183.136.216.4	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	2
193.189.117.26	Poland	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	2
109.253.158.125	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
61.240.144.65	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	2
221.235.189.245	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
91.238.134.92	Poland	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.189.244	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.130	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
144.0.0.60	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
37.123.96.71	Turkey	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 2048	1
101.226.2.99	China	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 2048	1
85.250.164.74	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
217.17.111.163		147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.66	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
176.123.28.24	Moldova, Republic of	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
58.20.54.251	China	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
118.97.204.69	Indonesia	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 3072	1
61.16.232.231	India	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
121.88.5.177	Korea, Republic of	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
2.54.182.48	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
95.187.104.161	Romania	147.237.77.216	dover.idf.il	GPL WEB_SERVER /etc/passwd	1
221.235.189.245	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
81.200.91.2	Russian Federation	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 2048	1
202.71.25.29	India	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.64	China	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 1024	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
79.177.55.18	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10401
109.64.13.57	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1183
2.54.135.87	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1070
109.67.144.137	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1046
93.172.211.149	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	994
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	830
46.19.85.52	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	762
188.100.78.244	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	734
79.177.117.180	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	733
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	689
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	549
2.54.27.51	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	442
46.121.81.194	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	432
192.115.248.2	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	425
132.66.40.116	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	412
82.145.220.181	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	373
212.179.21.196	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	326
37.142.87.84	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	319
213.8.96.180	Israel	147.237.72.167	ishurim.aka.idf.il	First packet isn't SYN	drop	drop	312
96.44.71.120	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	300
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	258
212.179.61.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	257
212.179.21.195	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	239
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	239
46.19.86.115	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	235
108.54.206.238	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	230
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	209
46.19.85.118	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	204
46.116.50.45	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	200
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	197
120.155.55.72	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	194
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	187
213.8.96.180	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	181
41.182.30.144	Namibia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	180
31.223.186.94	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	179
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	179
2.54.46.164	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	172
95.86.120.144	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	167
98.124.175.139	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	161
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	155
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	144
79.178.30.30	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	139
194.90.122.40	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	139
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	136
77.75.77.17	Czech Republic	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	134
2.52.141.182	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	127
194.90.83.233	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	127
46.116.210.130	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	124
95.172.68.145	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	124
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	123



## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
2.54.55.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	570
176.12.147.168	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.147.168	Block	570
213.57.111.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	392
46.19.85.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	331
79.181.167.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	293
2.54.154.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	255
46.19.85.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	195
46.19.86.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	187
2.54.42.6	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.42.6	Block	163
213.57.111.31	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 213.57.111.31	Block	158
46.19.85.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	144
109.253.144.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	127
46.19.85.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	115
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	98
37.26.147.178	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.147.178	Block	73
176.12.141.85	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.141.85	Block	71
109.253.139.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	69
2.54.189.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	58
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	39
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	39
46.19.85.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	37
207.232.28.184	Israel	147.237.77.216	dover.idf.il	Distributed Too Many of the Same Response Code (404)	Block	37
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	25
95.86.98.207	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	18
95.86.81.190	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	16
207.46.13.127	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
157.55.39.32	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
176.12.147.228	Israel	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	13
46.19.86.240	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	12
46.116.105.230	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	11
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	10
109.253.138.244	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 109.253.138.244	Block	10
207.46.13.99	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 207.46.13.99	Block	10
46.116.198.84	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	9
176.12.137.118	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.137.118	Block	9
213.57.182.23	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigat on.asp	Block	9
109.253.145.177	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	9
85.65.124.51	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
95.86.64.184	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	8
176.12.146.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	8
157.55.39.191	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 157.55.39.191	Block	8
213.57.206.167	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5n uhg	Block	8
5.28.146.125	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	8
188.120.148.237	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
207.46.13.40	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
46.19.86.117	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
84.108.147.68	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 84.108.147.68	None	7
212.76.109.46	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	7
37.26.147.162	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	6
109.64.13.57	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	6