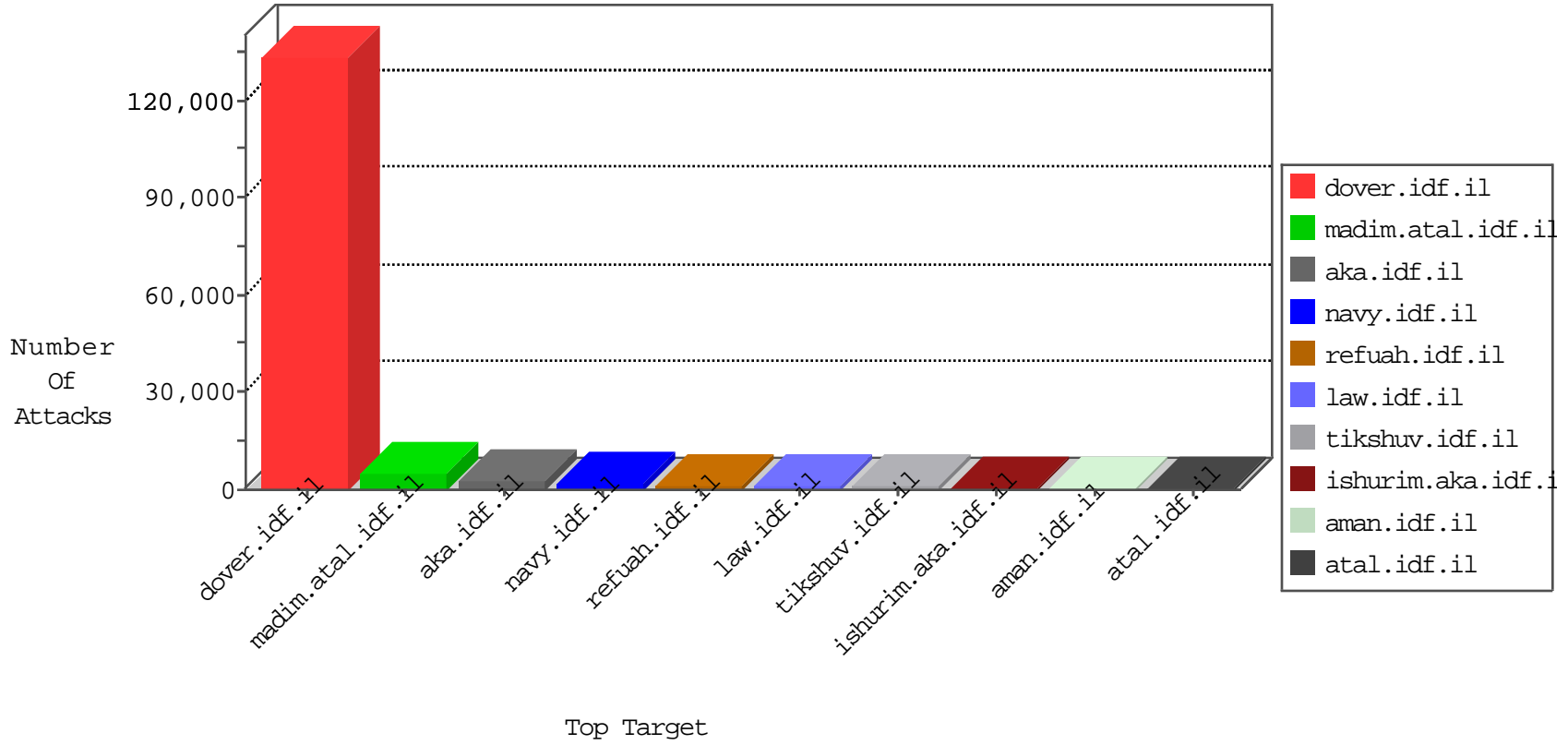


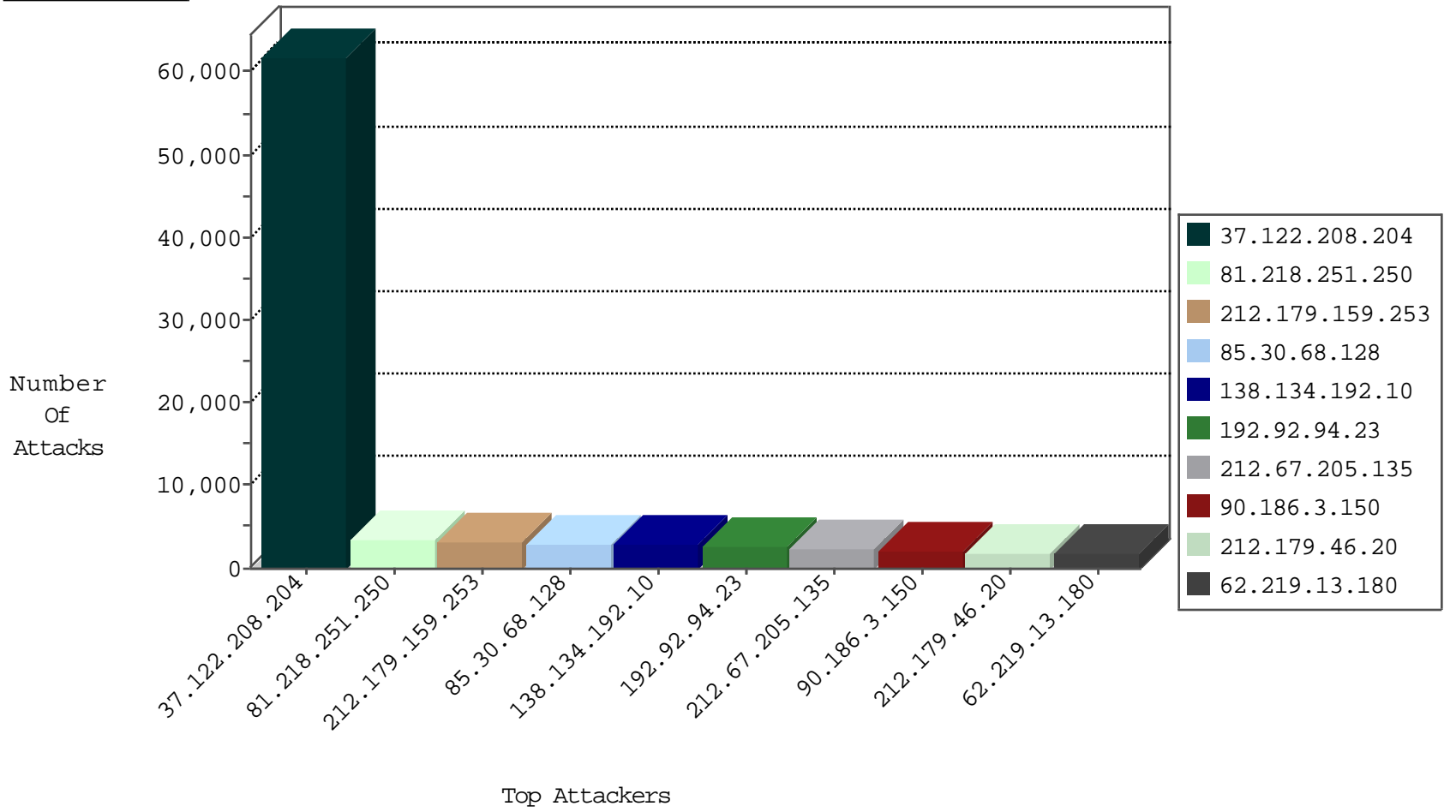
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
212.67.205.135	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	111684
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	72080
66.249.78.190	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	23100
212.67.205.135	United Kingdom	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	13259
85.250.1.6	Israel	147.237.0.15	kosher-kravi.idf.il	TCP Scan (vertical)	drop	9031
220.181.108.123	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	8514
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6715
104.131.228.99		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6240
66.249.67.152	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	5941
66.249.64.153	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	4408
66.249.78.89	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3667
176.12.147.99	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2961
220.181.108.157	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	2763
78.46.174.197	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2667
37.122.208.204	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1356
212.67.205.135	United Kingdom	147.237.77.216	dover.idf.il	block-sp-trafl	drop	1290
37.122.208.204	United Kingdom	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1152
85.30.68.128	Macedonia, the Former Yugoslav Republic of	147.237.76.86	navy.idf.il	DOS-HTTP-torshammer	forward	1036
128.90.94.205	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	750
212.67.205.135	United Kingdom	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	617
85.30.68.128	Macedonia, the Former Yugoslav Republic of	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Http	drop	539
77.127.219.185	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	533
84.229.31.191	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	504
85.30.68.128	Macedonia, the Former Yugoslav Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	483
109.160.234.59	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	455
85.30.68.128	Macedonia, the Former Yugoslav Republic of	147.237.76.86	navy.idf.il	JLM_Purple_Con_Limit_Tcp	drop	454
137.95.1.11	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	452
149.78.154.69	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	443
5.29.18.179	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	409
93.173.163.221	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	366
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	352
109.64.182.15	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	333
46.116.186.107	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	277
46.117.234.233	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	263
46.19.86.239	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	259
109.67.111.10	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	237
79.177.119.210	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	228
77.127.147.66	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	227
212.117.143.250	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	220
66.249.78.29	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	214
37.122.208.204	United Kingdom	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	195
46.121.242.244	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	164
81.218.97.114	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	157
220.181.108.155	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	137
132.72.225.98	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	137
94.230.86.232	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	137
79.183.120.21	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	123
84.109.200.204	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	121
31.210.186.153	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	121
85.65.139.150	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	115

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
192.92.94.23	Europe	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	2598
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	391
180.76.5.193	China	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	304
184.173.183.172	United States	147.237.76.42	refuah.idf.il	DVRep_P-N_40-59	Permit	297
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	271
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	193
180.76.5.193	China	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	156
184.173.183.172	United States	147.237.77.233	atal.idf.il	DVRep_P-N_40-59	Permit	146
180.76.5.193	China	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	119
180.76.5.193	China	147.237.77.170	maarachot.idf.il	DVRep_P-N_40-59	Permit	105
104.148.71.126		147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	36
212.67.205.135	United Kingdom	147.237.77.216	dover.idf.il	8262: HTTP: Slowloris DoS Tool	Block	35
212.199.251.235	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	28
46.117.221.59	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	27
212.199.251.235	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	24
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
198.188.210.45	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	18
66.249.79.229	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	17
87.69.211.184	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	17
84.108.174.212	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	16
80.178.138.115	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	14
5.29.234.14	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	13
79.177.4.166	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	13
109.247.160.149	Norway	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	12
46.120.2.93	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	12
212.143.3.44	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	12
84.111.37.22	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	12
138.134.102.16	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
212.199.251.227	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	12
82.80.89.41	Israel	147.237.77.226	ww.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
149.78.239.250	United States	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	12
138.134.102.15	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	11
66.249.79.241	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	10
5.29.237.241	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	10
212.150.189.2	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	10
213.57.172.147	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	10
84.108.193.192	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	9
178.238.238.44	Germany	147.237.77.216	dover.idf.il	19813: HTTP: WordPress Theme Divi Directory Traversal Vulnerability	Permit	9
79.177.37.94	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	9
79.180.150.126	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
109.67.144.128	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
93.172.201.72	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
84.94.176.24	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
37.26.148.169	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
149.78.119.211	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
109.65.143.180	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
93.172.19.104	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	8
77.127.72.29	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	7
93.172.40.147	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	7

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	89
2.52.21.193	Israel	147.237.76.86	navy.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	78
66.249.64.153	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	16
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	12
85.250.1.6	Israel	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	8
65.49.68.172	United States	147.237.76.30	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDoS attack	6
5.101.157.38	Russian Federation	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
5.9.136.67	Germany	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
5.9.136.67	Germany	147.237.77.216	dover.idf.il	SERVER-WEBAPP phpThumb fltr[] parameter remote command execution attempt	5
66.249.64.161	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
66.249.64.156	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
66.249.78.190	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	4
66.249.78.15	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	3
66.249.67.25	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.66	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.64.156	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
221.235.189.245	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	2
128.199.167.194	Singapore	147.237.72.166	aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	2
5.29.147.226	Israel	147.237.0.34	tikshuv.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDoS attack	2
61.240.144.66	China	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	2
180.210.234.87	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	2
121.88.5.177	Korea, Republic of	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	2
66.249.79.31	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	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	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.89	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
178.238.238.44	Germany	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
61.240.144.66	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	2
91.238.134.92	Poland	147.237.77.234	halag.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
66.249.64.148	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
183.136.216.3	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.67	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.79.32	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.66	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.78.96	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
81.218.77.162	Israel	147.237.72.156	aman.idf.il	GPL SCAN nmap TCP	2
91.238.134.92	Poland	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.64	China	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	2
73.160.112.218	United States	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 2048	1
196.12.153.45	Rwanda	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
171.107.83.229	China	147.237.76.147	chimuch.aka.idf.il	ET SCAN NMAP -sS window 4096	1
37.26.147.232	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
110.173.177.37	India	147.237.72.166	aka.idf.il	ET SCAN NMAP -f -sS	1
84.108.237.25	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.142.54	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.67	China	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 1024	1
182.71.32.254	India	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
61.160.224.130	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential VNC Scan 5800-5820	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
37.122.208.204	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	61560
81.218.251.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3450
212.179.159.253	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3111
138.134.192.10	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2771
90.186.3.150	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2000
212.179.46.20	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1719
62.219.13.180	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1684
85.30.68.128	Macedonia, the Former Yugoslav Republic of	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1481
2.52.138.111	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1254
85.30.68.128	Macedonia, the Former Yugoslav Republic of	147.237.76.86	navy.idf.il	First packet isn't SYN	drop	drop	1176
31.168.132.131	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1133
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	865
212.179.61.122	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	845
2.54.162.143	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	812
81.218.97.114	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	710
212.67.205.135	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	665
212.179.61.124	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	653
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	565
212.179.61.127	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	545
95.86.123.25	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	542
169.159.127.130		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	509
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	398
108.54.206.238	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	384
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	358
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	332
46.116.210.130	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	301
85.30.68.128	Macedonia, the Former Yugoslav Republic of	147.237.76.86	navy.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	297
71.205.57.133	United States	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	281
84.228.203.52	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	280
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	276
82.145.223.38	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	275
212.179.46.21	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	264
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	249
106.39.189.190	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	243
132.66.40.116	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	242
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	236
79.181.27.84	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	223
2.54.156.74	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	218
38.111.147.86	United States	147.237.77.74	law.idf.il		drop	drop	216
5.108.12.237	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	207
193.43.245.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	201
212.179.57.178	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	192
193.43.246.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	189
41.59.5.110	Tanzania, United Republic of	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	174
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	171
72.37.171.76	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	168
2.54.50.17	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	168
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	158
66.249.81.218	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	157
66.249.81.212	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	154

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.86.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1031
37.26.148.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	649
37.26.146.246	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.146.246	Block	446
109.253.79.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	415
2.54.139.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	399
176.12.140.23	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.140.23	Block	351
109.253.142.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	294
109.253.157.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	290
46.19.86.149	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.149	Block	239
185.32.176.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	162
37.26.147.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	114
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	88
185.32.176.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	71
46.19.85.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	70
2.54.26.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	68
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	57
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	47
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	39
66.249.78.216	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.78.216	Block	34
149.78.20.73	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	31
66.249.78.230	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.78.230	Block	30
37.142.234.131	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	27
66.249.78.223	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.78.223	Block	26
109.253.138.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	25
85.65.46.211	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	24
89.138.244.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 89.138.244.20	Block	22
157.55.39.182	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/captcha.ashx	Block	18
118.123.8.135	China	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 118.123.8.135	Block	18
149.78.35.33	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 149.78.35.33	Block	16
79.178.2.159	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
109.253.144.95	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.144.95	Block	13
207.46.13.57	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/captcha.ashx	Block	13
207.46.13.57	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 207.46.13.57	Block	12
157.55.39.191	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il/captcha.ashx	Block	12
189.149.92.114	Mexico	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	12
157.55.39.182	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 157.55.39.182	Block	12
62.219.198.6	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	12
207.46.13.121	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 207.46.13.121	Block	11
176.12.144.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	11
2.52.175.202	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.52.175.202	Block	11
109.186.140.56	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	10
212.199.57.66	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/4/	Block	10
93.173.190.158	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/0/	Block	10
207.46.13.121	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/captcha.ashx	Block	9
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	9
95.86.75.199	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	9
37.142.191.197	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
77.125.113.226	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
212.179.213.89	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	7
77.127.245.250	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	7