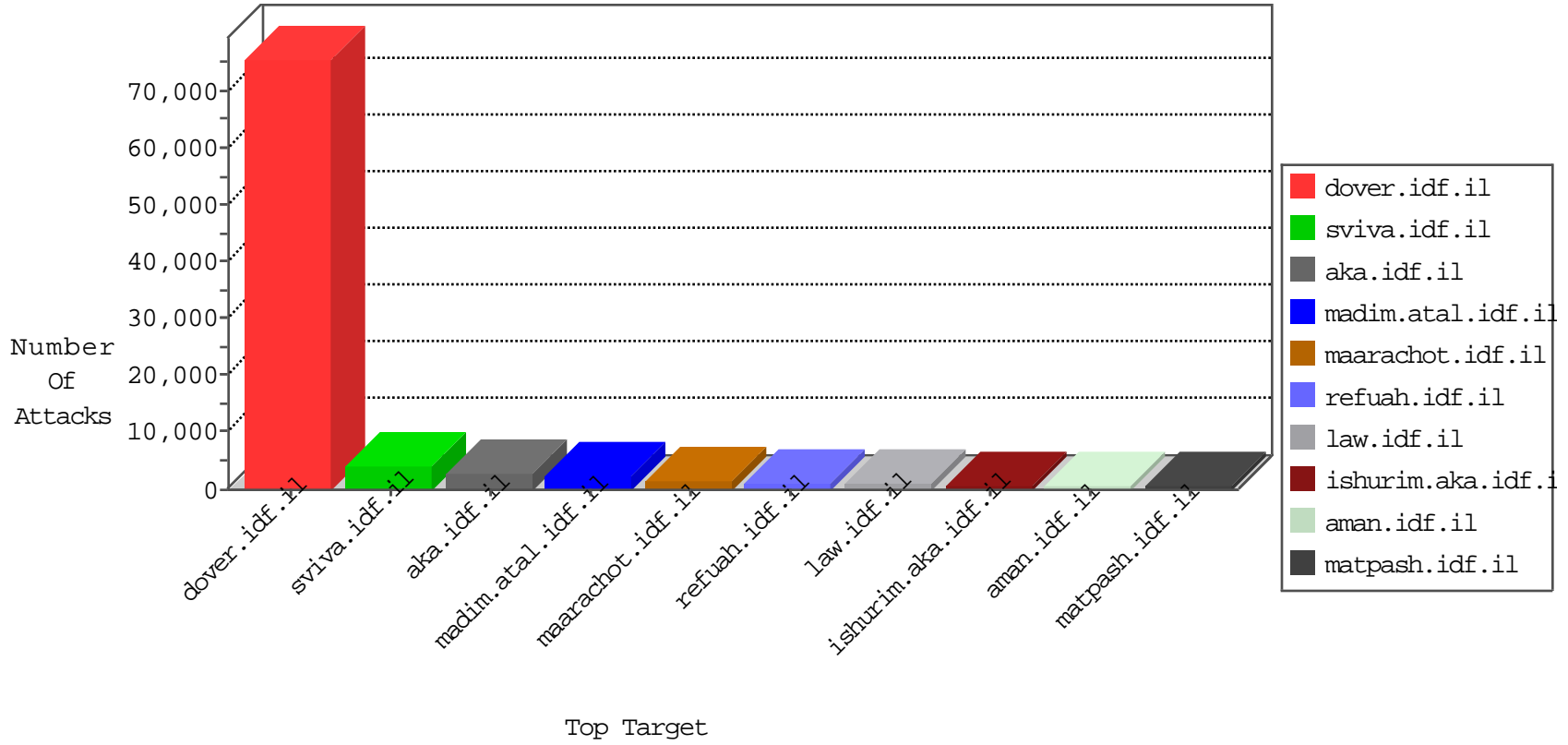


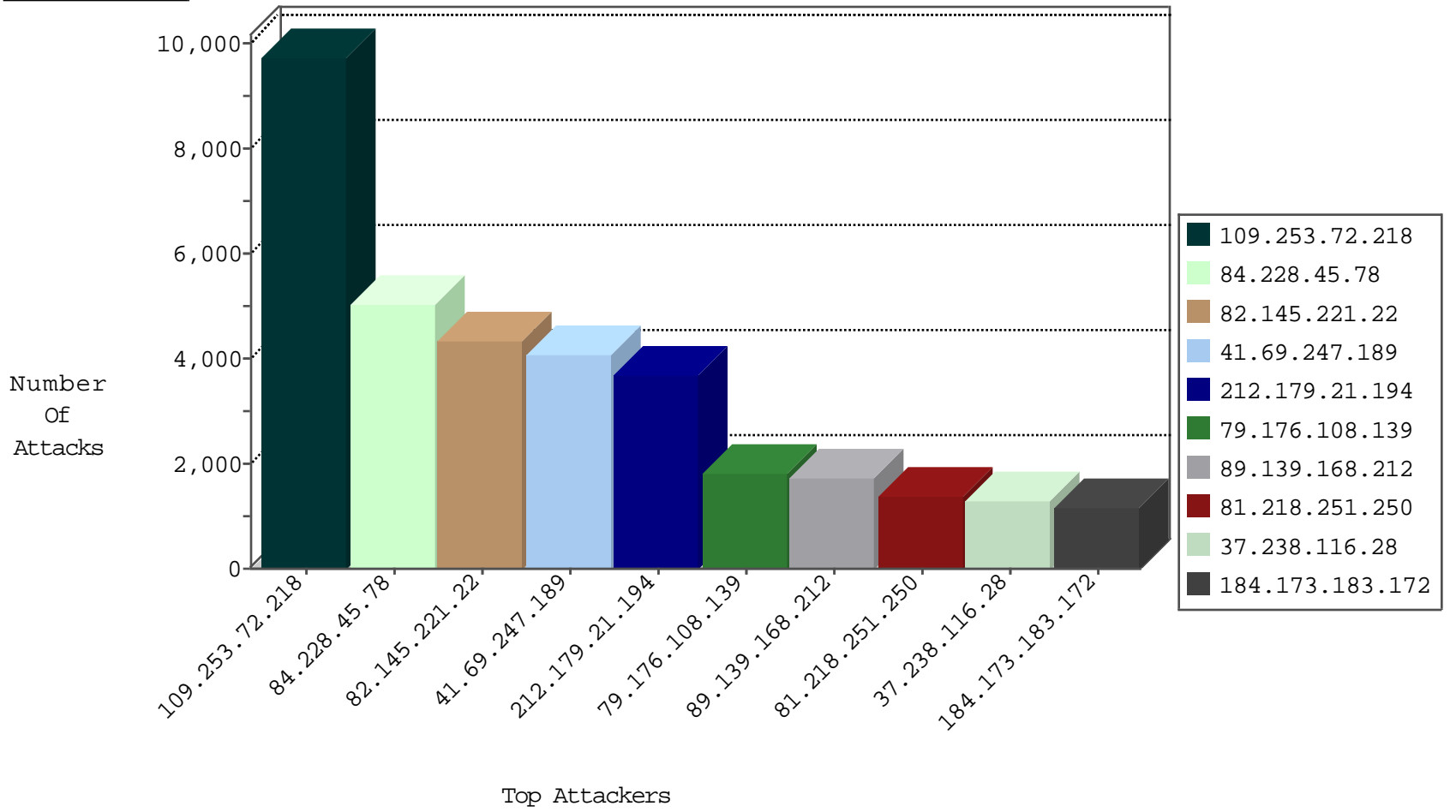
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1035
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	806
131.252.200.44	United States	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	745
109.67.124.31	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	663
46.120.52.140	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	627
149.88.85.190	United States	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	624
79.177.4.132	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	602
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	602
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	589
213.8.71.26	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	542
212.179.21.194	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	513
149.88.31.73	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	480
79.182.10.26	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	409
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	355
79.181.141.17	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	339
87.68.243.120	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	290
185.32.178.173	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	289
213.57.189.42	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	261
81.218.37.2	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	244
89.139.59.163	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	218
87.69.110.29	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	208
109.64.204.86	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	187
79.177.173.99	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	176
81.218.241.25	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	170
77.126.117.61	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	167
31.154.146.247	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	161
85.250.36.223	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	152
87.69.88.208	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	147
84.108.200.9	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	141
213.151.53.59	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	131
192.116.95.222	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	130
85.64.215.141	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	125
85.250.231.132	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	124
62.219.162.230	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	123
220.181.108.94	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	120
212.199.112.144	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	119
79.180.99.13	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	115
149.78.102.127	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	111
62.219.148.147	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	104
31.154.160.112	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	102
46.121.218.185	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	96
46.19.85.134	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	92
109.253.138.226	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	91
2.54.38.142	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90
109.253.156.89	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90
37.26.146.210	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	87
37.26.147.179	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	83
84.109.145.153	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	83
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	83
37.142.8.34	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	81

## 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	692
77.125.87.161	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	649
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	297
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	167
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	126
109.64.111.70	Israel	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	79
89.139.168.212	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	21
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	20
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	20
212.143.3.44	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	18
85.132.77.12	Azerbaijan	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	14
89.248.160.192	Netherlands	147.237.77.233	atal.idf.il	DVRep_P-N_40-59	Permit	12
77.127.126.190	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	10
36.248.167.241	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	10
188.165.250.158	France	147.237.77.170	maarachot.idf.il	19813: HTTP: WordPress Theme Divi Directory Traversal Vulnerability	Block	9
192.117.236.29	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	9
178.234.222.210	Russian Federation	147.237.77.176	matpash.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	9
132.66.178.194	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	9
31.168.171.81	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
84.94.82.186	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
192.115.248.2	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
37.142.162.233	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
71.6.135.131	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	6
198.20.69.98	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	6
71.6.135.131	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	6
10.0.0.8		147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
66.240.192.138	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	6
66.240.192.138	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	6
213.57.204.33	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
194.114.146.227	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
79.182.207.180	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
71.6.135.131	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	6
66.240.192.138	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	6
66.240.192.138	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	6
71.6.135.131	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	5
188.138.9.50	Germany	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	5
71.6.165.200	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	5
198.20.70.114	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	5
167.88.94.186		147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
77.127.137.5	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
66.240.192.138	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	5
198.20.69.98	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	5
198.20.70.114	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	5
188.138.9.50	Germany	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	5

## Top Attackers In IDF

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.78.22	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	289
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	92
2.52.17.54	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	58
89.139.168.212	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	11
66.249.78.89	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	6
66.249.78.29	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	6
61.240.144.66	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	4
61.183.128.6	China	147.237.76.34	yochanan.idf.il	ET SCAN NMAP -sS window 1024	2
212.179.21.194	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
59.49.25.66	China	147.237.76.197	e.himush.idf.il	GPL SCAN nmap TCP	2
61.240.144.64	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.79.42	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.96	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.64	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.78.82	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
217.66.228.201	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
61.183.128.6	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	2
213.204.103.36	Lebanon	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
197.135.255.237	Egypt	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
37.105.158.85	Saudi Arabia	147.237.77.216	dover.idf.il	SERVER-WEBAPP TRACE attempt	2
61.240.144.67	China	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.79.218	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.67	China	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.78.159	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
202.112.38.190	China	147.237.76.197	e.himush.idf.il	GPL SCAN nmap TCP	2
217.91.181.112	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.67	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.130	Japan	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	2
213.204.103.36	Lebanon	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.67	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	1
187.183.178.39		147.237.0.33	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
43.255.188.130	Japan	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
109.66.117.211	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.181.207	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.65	China	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	1
199.203.59.121	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
45.64.158.230		147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 3072	1
123.177.18.194	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
5.56.62.149	Spain	147.237.72.166	aka.idf.il	ET DOS SSL Bomb DoS Attempt	1
89.248.160.192	Netherlands	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
37.237.200.109	Iraq	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
104.128.144.130		147.237.76.198	e.yochanan.idf.il	ET SCAN NMAP -f -sS	1
66.249.64.60	United States	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
221.235.205.123	China	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 4096	1
61.183.128.6	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.74	United States	147.237.76.197	e.himush.idf.il	ET DROP Dshield Block Listed Source	1
43.255.188.133	Japan	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
116.204.8.58	China	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
109.253.72.218	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9738
84.228.45.78	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5016
82.145.221.22	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4318
41.69.247.189	Egypt	147.237.77.235	sviva.idf.il	First packet isn't SYN	drop	drop	4089
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3474
79.176.108.139	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1815
89.139.168.212	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1663
81.218.251.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1366
37.237.200.109	Iraq	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1135
37.238.116.28	Iraq	147.237.77.170	maarachot.idf.il	First packet isn't SYN	drop	drop	1117
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	981
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	975
46.19.86.45	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	935
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	787
79.182.139.39	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	529
131.252.200.44	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	482
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	432
77.127.84.69	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	430
2.54.144.122	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	424
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	386
197.41.133.186	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	381
66.87.135.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	353
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	332
168.235.197.16		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	311
82.102.136.65	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	299
46.19.86.6	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	291
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	284
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	273
37.142.162.233	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	268
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	260
77.126.253.45	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	257
85.250.140.105	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	246
109.66.138.140	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	240
64.20.186.2	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	238
93.173.152.113	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	233
84.94.32.197	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	229
82.145.209.91	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	227
79.177.108.184	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	226
82.117.196.218		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	204
155.56.68.218	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	202
46.116.141.17	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	198
47.19.130.146	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	192
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	186
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	165
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	160
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	160
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	159
37.247.93.251	Spain	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	153
70.210.4.169	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	153
213.244.82.139	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	146

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.116.127.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1086
46.19.86.247	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.247	Block	312
2.54.49.85	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.49.85	Block	275
46.19.86.0	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.0	Block	186
176.12.137.166	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.137.166	Block	152
46.19.86.114	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.114	Block	113
2.54.28.28	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.28.28	Block	99
2.54.55.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	55
176.12.145.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	39
109.253.145.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	35
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	28
2.54.44.30	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	25
66.249.78.159	Israel	147.237.77.216	doover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	23
212.143.3.162	Israel	147.237.77.216	doover.idf.il	Multiple Unauthorized URL Access from 212.143.3.162	Block	22
66.249.78.173	Israel	147.237.77.216	doover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	20
78.51.28.246	Germany	147.237.77.74	law.idf.il	PHP Attempt	Block	16
66.249.78.166	Israel	147.237.77.216	doover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	15
213.151.32.163	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	12
78.51.28.246	Germany	147.237.76.42	refuah.idf.il	PHP Attempt	Block	12
78.51.28.246	Germany	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 78.51.28.246	Block	12
85.64.17.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	12
78.51.28.246	Germany	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	12
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	11
78.51.28.246	Germany	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 78.51.28.246	Block	11
213.151.32.163	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	10
212.143.3.162	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 212.143.3.162	Block	10
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	9
78.51.28.246	Germany	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 78.51.28.246	Block	8
78.51.28.246	Germany	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 78.51.28.246	Block	8
93.172.25.59	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
78.51.28.246	Germany	147.237.77.234	halag.idf.il	PHP Attempt	Block	8
192.116.130.15	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	8
176.12.151.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	8
78.51.68.194	Germany	147.237.72.166	aka.idf.il	PHP Attempt	Block	8
5.144.57.214	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	8
5.29.26.39	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	8
78.51.28.246	Germany	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/register/	Block	8
109.66.167.216	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
79.177.5.68	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g5lei5nuhg	Block	7
183.60.237.70	China	147.237.77.216	doover.idf.il	Multiple Unauthorized URL Access from 183.60.237.70	Block	7
5.28.137.99	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	7
46.120.142.235	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 46.120.142.235	None	7
37.8.104.57	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g5lei5nuhg	Block	6
62.219.13.180	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
84.94.82.186	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	6
31.44.141.107	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	6
31.168.132.131	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	6
31.154.151.50	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	6
89.138.220.50	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
68.180.229.51	United States	147.237.77.216	doover.idf.il	Multiple Unauthorized URL Access from 68.180.229.51	Block	6