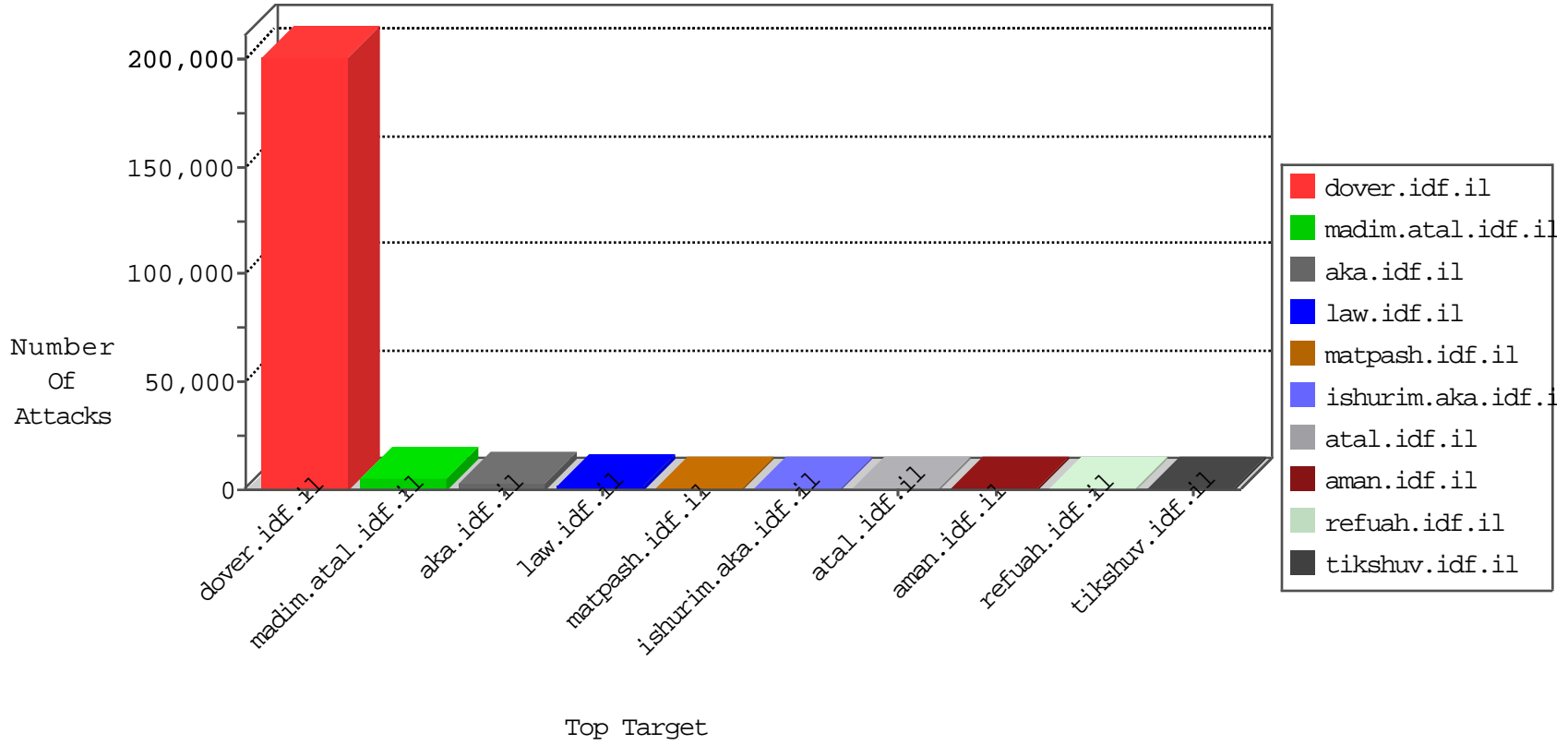


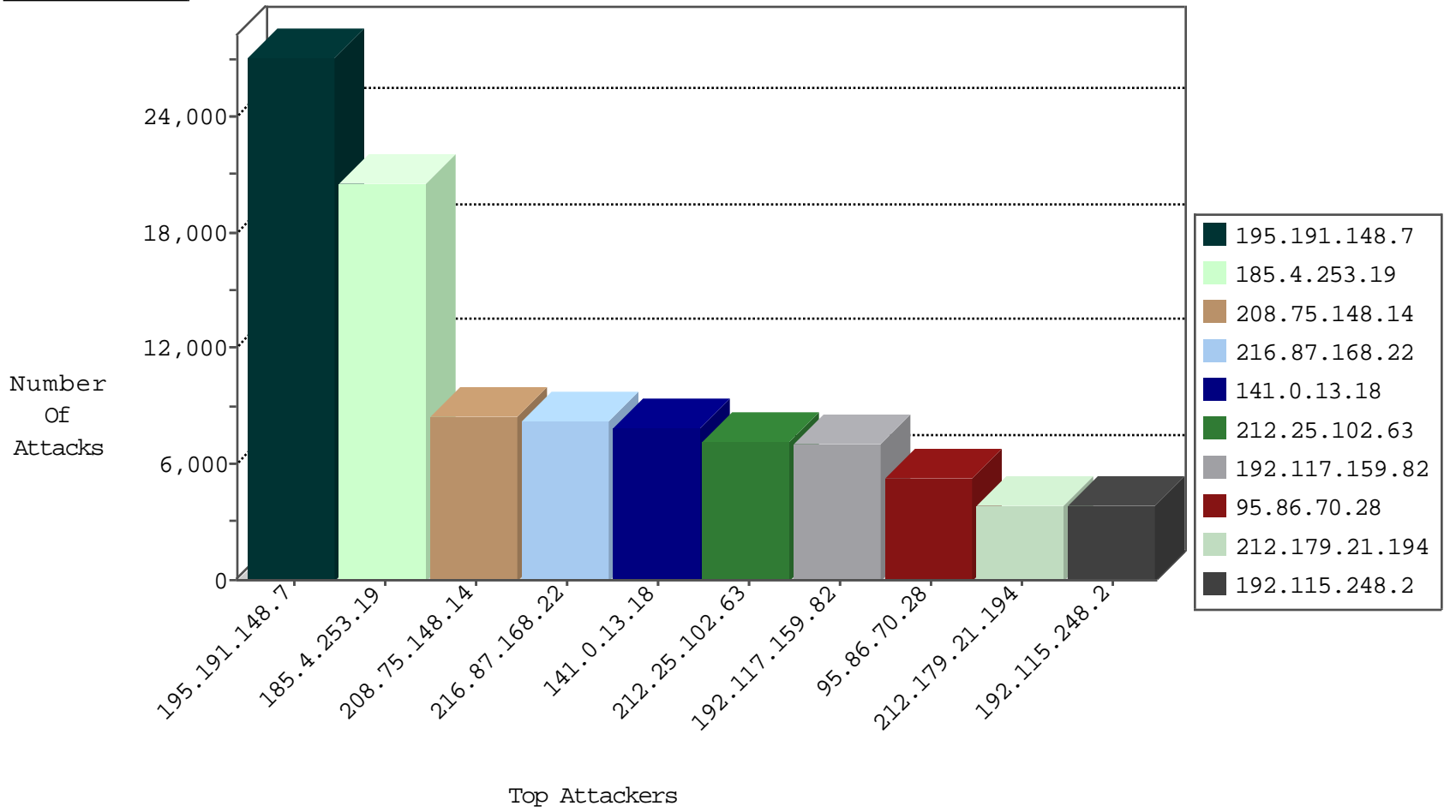
# IDF Under Attack Daily Report



## Top Targets



## Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
195.191.148.7	Bulgaria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	208340
66.249.73.211	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	164818
208.75.148.14	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	142421
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	124005
216.87.168.22	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	71457
185.4.253.19	Lebanon	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	67128
66.249.79.65	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	58424
37.76.216.9	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	34080
41.38.63.163	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	24086
66.249.65.48	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	23750
185.26.182.32	Europe	147.237.0.34	tikshuv.idf.il	TCP handshake violation, first packet not syn	drop	18392
66.249.73.219	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	18195
66.249.67.38	Israel	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	17207
66.249.73.203	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	15850
216.87.168.22	United States	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	12278
217.118.95.120	Russian Federation	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	10908
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	10339
5.255.253.152	Russian Federation	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	9572
66.249.79.2	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	8197
66.249.65.51	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	7177
213.251.182.114	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6841
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5370
200.53.156.138	Mexico	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4792
157.150.193.1	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4670
216.87.168.22	United States	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	4422
66.249.78.104	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3639
66.249.64.16	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3575
82.80.54.195	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3372
208.75.148.14	United States	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	3338
81.98.199.169	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3164
192.114.7.2	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3138
141.0.13.18	Norway	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3030
66.249.64.29	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2903
80.246.130.241	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2885
66.249.78.159	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2824
46.19.86.254	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2772
84.228.19.116	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2749
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	2730
82.109.66.145	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2623
208.75.148.14	United States	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	2489
66.249.65.45	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2140
76.164.214.86	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2127
66.249.64.151	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	1575
220.181.108.104	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	742
220.181.108.160	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	709
12.184.167.11	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	623
87.69.20.217	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	540
176.12.142.65	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	517
66.249.64.151	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	497
66.249.64.26	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	437

## 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	316
184.173.183.172	United States	147.237.77.233	atal.idf.il	7610: IP Reputation	Permit	205
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	119
184.173.183.172	United States	147.237.0.34	tikshuv.idf.il	DVRep_P-N_40-59	Permit	100
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	57
213.251.182.114	France	147.237.77.216	dover.idf.il	8262: HTTP: Slowloris DoS Tool	Block	36
87.240.182.185	Russian Federation	147.237.77.176	matpash.idf.il	2273: HTTP: ../ Directory Traversal Beyond WebRoot (level 1)	Permit	30
194.114.146.227	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	24
5.45.134.57	Jordan	147.237.77.216	dover.idf.il	C017: HTTP: Malicious UserAgent FOCA	Block	16
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	10
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	10
212.29.223.130	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
37.49.55.39	Germany	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
217.118.79.23	Russian Federation	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	6
95.86.127.10	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
46.19.85.212	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
213.57.167.152	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
85.64.128.110	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
218.77.79.43	China	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	5
37.26.147.230	Israel	147.237.77.176	matpash.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	5
218.77.79.43	China	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	4
218.77.79.43	China	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	4
85.130.130.44	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
73.200.121.113	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
71.6.165.200	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	4
108.220.160.235	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
218.77.79.43	China	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	3
218.77.79.43	China	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	3
66.240.192.138	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	3
198.20.69.98	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	3
218.77.79.43	China	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	3
37.26.147.138	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
66.240.192.138	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	3
218.77.79.43	China	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	3
218.77.79.43	China	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	3
50.56.74.143	United States	147.237.77.74	law.idf.il	19863: HTTP: WordPress Revslider/Showbiz PHP File Upload	Block	3
85.25.103.50	Germany	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	3
71.6.165.200	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	3
66.240.192.138	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	3
218.77.79.43	China	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	3
71.6.135.131	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	3
218.77.79.43	China	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	3
218.77.79.43	China	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	3
218.77.79.43	China	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	3
66.240.192.138	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	3
71.6.135.131	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	3
188.138.9.50	Germany	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	3
71.6.167.142	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	3
218.77.79.43	China	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	3
66.240.192.138	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	3

## Top Attackers In ID

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	88
85.250.140.105	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	9
66.249.64.34	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	4
66.249.64.21	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
193.107.17.72	Russian Federation	147.237.76.38	e.e.meitav.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	3
61.183.128.6	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	3
176.12.150.238	Israel	147.237.76.30	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDoS attack	3
81.218.77.162	Israel	147.237.76.31	nakchal.idf.il	GPL SCAN nmap TCP	3
43.255.188.134	Japan	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	3
66.249.73.219	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.64	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	2
199.203.59.121	Israel	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	2
66.249.73.211	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.133	Japan	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	2
199.203.59.121	Israel	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	2
46.19.85.231	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
66.249.64.24	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.16	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.133	Japan	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.130	Japan	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
58.20.54.249	China	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.134	Japan	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.133	Japan	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.67	China	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.66	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.134	Japan	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	2
61.240.144.67	China	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 1024	2
61.183.128.6	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.134	Japan	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	2
216.87.168.22	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
54.90.152.65	United States	147.237.77.176	matpash.idf.il	Tehila - Perl LWP with fake user agent	2
193.107.17.72	Russian Federation	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	2
109.234.38.226	Russian Federation	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.66	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	2
109.234.38.226	Russian Federation	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.65.51	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.130	Japan	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.65	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.64.29	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.66	China	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.134	Japan	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	2
218.77.79.43	China	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	2
178.89.191.77	Kazakhstan	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.134	Japan	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	2
66.249.85.204	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.134	Japan	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.132	Japan	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
84.109.91.127	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
195.191.148.7	Bulgaria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26590
185.4.253.19	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16362
141.0.13.18	Norway	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7894
212.25.102.63	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7152
192.117.159.82	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6992
208.75.148.14	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6176
95.86.70.28	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5230
192.115.248.2	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3860
212.179.21.194	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3713
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2215
2.54.147.120	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2053
95.86.120.28	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2049
85.250.140.105	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1662
213.251.182.114	France	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1597
82.80.54.195	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1539
216.87.168.22	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1480
46.210.135.82	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1312
199.190.46.119	Satellite Provider	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1068
77.125.159.221	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	939
41.33.231.86	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	904
212.76.123.154	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	904
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	899
5.45.134.57	Jordan	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	875
79.181.203.128	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	817
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	809
79.176.155.172	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	714
46.19.85.168	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	710
200.53.156.138	Mexico	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	706
46.19.85.193	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	689
167.205.23.15	Indonesia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	687
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	635
82.166.22.29	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	624
192.249.64.249	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	623
205.203.135.1	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	601
95.86.124.115	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	600
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	587
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	582
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	573
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	570
212.199.51.125	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	563
103.247.50.188	Sri Lanka	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	562
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	556
84.109.5.107	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	553
46.19.86.82	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	551
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	536
66.249.78.159	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	534
66.249.78.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	507
200.53.156.138	Mexico	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	503
66.249.78.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	503
68.180.229.51	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	502



## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
185.4.253.19	Lebanon	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/undefined	Block	4024
2.52.189.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	736
46.19.85.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	657
2.54.26.14	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.26.14	Block	573
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	487
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	479
176.12.145.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	444
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	388
95.175.35.73	Israel	147.237.77.74	law.idf.il	Distributed Suspicious Response Code	Block	290
109.253.159.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	271
2.54.179.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	269
176.12.149.75	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.149.75	Block	268
109.253.156.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	166
46.19.85.204	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.204	Block	159
84.229.161.16	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 84.229.161.16	Block	146
41.129.90.99	Egypt	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/news/undefined	Block	104
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atall/izkor/view_img.asp	Block	103
109.253.141.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	100
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atall/izkor/view_img.asp	Block	85
37.26.146.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	83
109.253.132.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	80
2.52.29.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	78
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atall/izkor/view_img.asp	Block	75
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atall/izkor/view_imgtop.asp	Block	67
176.12.151.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	66
46.19.85.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	64
46.19.85.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	58
5.29.83.134	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 5.29.83.134	Block	58
46.19.85.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	51
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 212.179.21.194	Block	49
109.253.136.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	45
2.54.25.66	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.25.66	Block	43
200.53.156.138	Mexico	147.237.76.147	chimuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	42
2.54.0.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	42
192.118.11.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	33
2.52.3.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	29
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/gyus/forum/asp/showforum.asp	Block	27
176.12.149.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	26
109.226.15.199	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	21
212.143.186.38	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.143.186.38	Block	18
5.9.45.155	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 5.9.45.155	Block	18
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atall/izkor/view_imgtop.asp	Block	17
85.250.169.170	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.250.169.170	Block	16
109.253.149.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
46.19.85.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atall/izkor/view_imgtop.asp	Block	16
37.26.147.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	15
109.253.138.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	15
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atall/izkor/view_imgtop.asp	Block	14
46.19.86.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	13