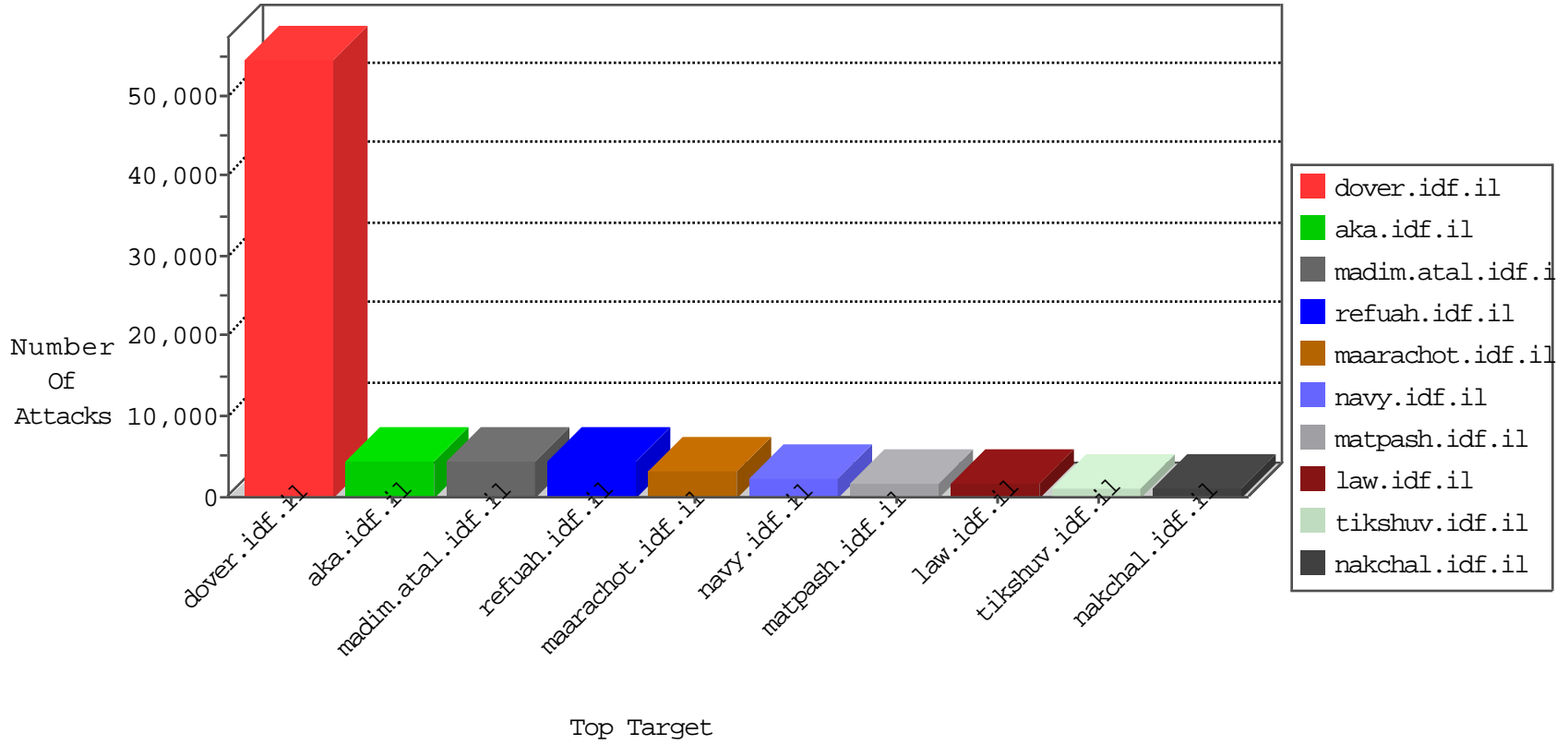


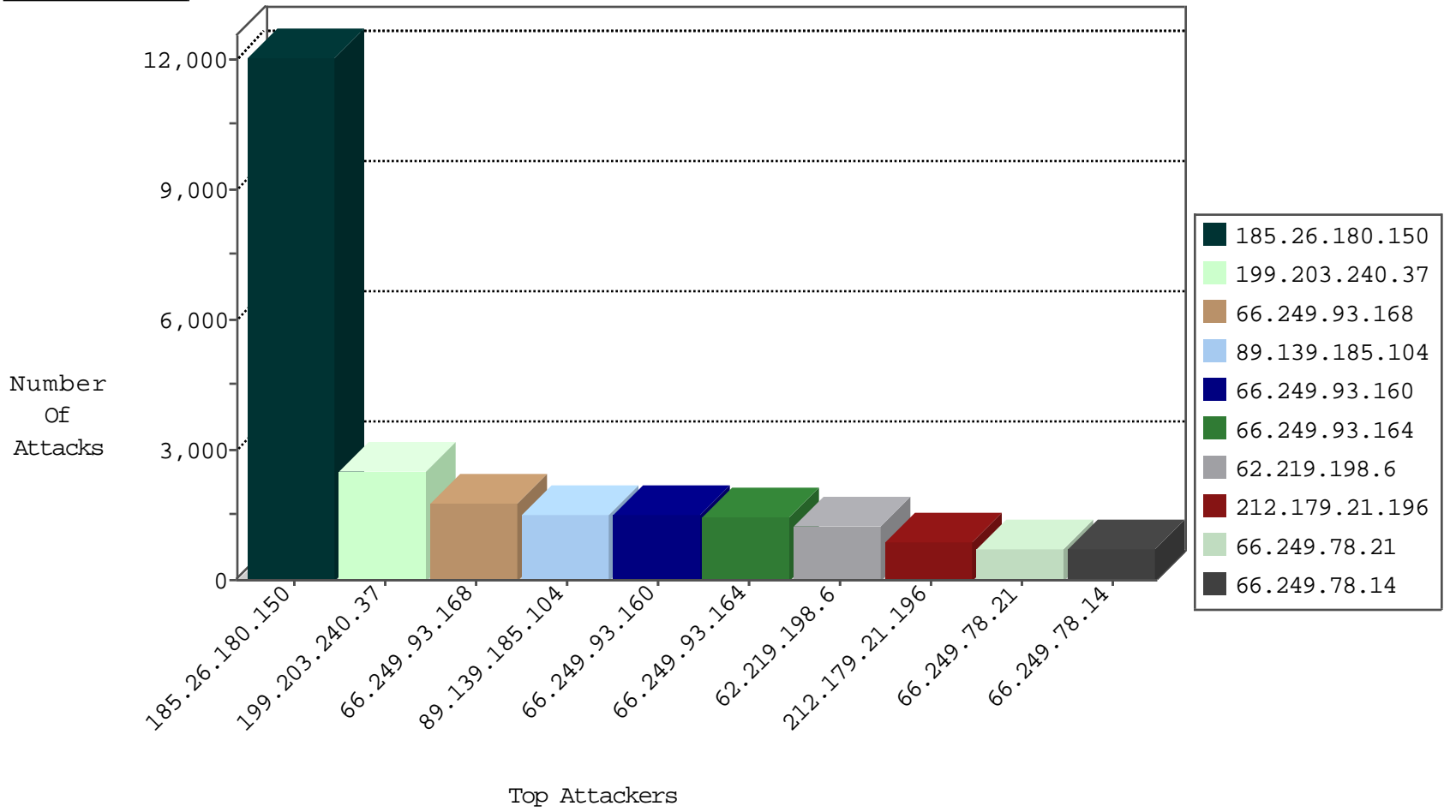
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
89.139.185.104	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7201
220.181.108.83	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	7131
220.181.108.172	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	6165
46.19.85.34	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1713
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	1480
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	1450
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	1423
5.41.84.241	Romania	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1365
46.120.42.56	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1080
84.108.153.105	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1017
81.249.187.57	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	962
195.154.233.184	France	147.237.72.14	dover.idf.il(old)	TCP handshake violation, first packet not syn	drop	892
84.110.60.143	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	784
109.66.129.224	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	745
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	738
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	707
206.45.162.159	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	678
109.253.144.87	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	667
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	637
192.114.182.2	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	591
79.178.99.109	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	586
84.108.240.254	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	558
84.228.222.138	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	542
37.238.20.109	Iraq	147.237.0.15	kosher-kravi.idf.il	TCP Scan (vertical)	drop	538
79.183.101.79	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	530
193.43.244.102	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	529
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	487
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	480
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	438
66.249.69.96	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	429
66.249.65.152	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	417
66.249.69.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	416
220.181.108.123	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	400
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	398
66.249.93.176	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	395
66.249.69.88	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	379
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	370
82.213.16.130	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	357
66.249.93.168	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	354
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	351
149.78.138.255	United States	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	348
204.93.154.220	United States	147.237.77.233	atal.idf.il	TCP Scan (vertical)	drop	338
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	336
66.249.93.172	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	334
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	332
66.249.78.190	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	320
66.249.65.156	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	316
149.78.6.214	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	314
66.249.65.148	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	313
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	309

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	185
184.173.183.172	United States	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	142
184.173.183.172	United States	147.237.77.216	dover.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	74
180.76.5.193	China	147.237.0.34	tikshuv.idf.il	DVRep_P-N_40-59	Permit	29
180.76.5.193	China	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	26
89.139.185.104	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	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
212.199.112.144	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	18
205.134.224.235	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	15
31.168.171.81	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	8
5.29.140.253	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
81.218.171.152	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
5.102.254.206	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
212.235.62.104	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
84.228.191.93	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
2.54.5.245	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
79.178.173.218	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
73.43.31.212	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
5.29.227.76	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
194.114.146.227	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
93.172.163.29	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
46.19.85.106	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
89.216.115.8		147.237.77.216	dover.idf.il	17272: HTTP: Suspicious User-Agent (WindowsNT) With No Separating Space	Block	4
82.166.232.164	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
67.180.158.88	United States	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
109.67.193.121	Israel	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	4
79.182.203.156	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
5.102.254.174	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
85.250.135.85	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
180.76.5.193	China	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	4
176.67.104.138	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
109.65.96.190	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
46.19.86.109	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.220	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
212.199.107.106	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
37.142.3.56	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
93.172.102.253	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.144	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
2.54.45.231	Israel	147.237.0.19	madim.atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
62.219.21.30	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
212.179.5.3	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
79.176.60.3	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
62.219.146.13	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
31.168.179.144	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
84.111.6.7	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
109.64.153.23	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.31.97.124	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
93.120.27.62	Romania	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	2

## 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
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	61
95.86.67.114	Israel	147.237.77.216	dover.idf.il	POLICY-OTHER script tag in URI - likely cross-site scripting attempt	9
37.238.20.109	Iraq	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
195.200.205.2	Israel	147.237.72.166	aka.idf.il	ET SCAN NMAP -sA (2)	4
37.16.72.139	France	147.237.72.167	ishurim.aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
132.68.245.243	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	3
88.198.58.233	Germany	147.237.77.74	law.idf.il	Tehila - Perl LWP with fake user agent	2
221.235.188.210	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	2
43.255.191.170	Japan	147.237.76.148	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	2
221.235.188.210	China	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	2
221.235.188.210	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.67	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
84.110.60.143	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
81.218.77.162	Israel	147.237.77.74	law.idf.il	GPL SCAN nmap TCP	2
87.69.78.237	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
221.235.188.210	China	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	2
221.235.188.210	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	2
109.65.16.89	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
85.250.135.85	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
61.240.144.64	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
2.54.21.242	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
221.235.188.212	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
79.178.198.212	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
221.235.188.212	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	2
207.166.127.153	Puerto Rico	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	2
207.166.127.153	Puerto Rico	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
221.235.188.212	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.65	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
79.183.15.63	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
221.235.188.212	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
79.176.206.113	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
2.54.188.139	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
79.181.196.66	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
221.235.188.210	China	147.237.77.179	e.mazi.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
159.220.74.6	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	2
84.109.190.157	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
93.172.34.126	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
46.121.106.19	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
221.235.188.210	China	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	2
221.235.188.210	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	2
109.65.6.99	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
193.43.245.250	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.66	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	2
221.235.188.210	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	2
58.20.54.249	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.191.170	Japan	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
43.255.191.170	Japan	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	2

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
185.26.180.150	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12037
199.203.240.37	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2505
89.139.185.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1439
62.219.198.6	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1233
212.179.21.196	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	860
79.183.27.176	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	666
95.86.112.134	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	648
212.179.61.127	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	514
46.117.179.149	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	508
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	421
94.188.132.2	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	350
46.19.86.164	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	329
85.250.135.85	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	315
109.67.153.167	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	272
82.145.223.49	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	266
2.54.172.186	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	265
84.228.43.230	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	251
194.114.146.227	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	251
149.78.186.96	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	246
213.151.37.12	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	201
79.177.15.147	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	194
208.99.238.226	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	188
109.186.186.83	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	187
212.179.61.125	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	186
5.108.14.7	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	186
5.108.15.182	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	179
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	178
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	166
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	165
176.228.29.132	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	162
37.216.18.83	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	157
85.65.52.53	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	156
164.138.118.28	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	150
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	149
46.19.85.46	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	148
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	147
157.55.39.6	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	141
46.19.85.31	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	137
81.249.187.57	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	130
157.55.39.42	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	125
162.243.222.48	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	121
77.127.149.224	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	121
207.46.13.89	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	121
213.151.49.47	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	120
193.169.70.108	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	117
46.19.86.236	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	117
69.203.68.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	115
207.46.13.82	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	111
84.228.94.152	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	108
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	105

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
176.12.148.238	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.12.148.238	Block	362
2.52.183.34	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.52.183.34	Block	291
2.54.167.86	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	240
46.19.85.138	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	235
46.19.86.103	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	230
46.19.85.48	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	230
46.19.86.137	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	186
2.54.140.167	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	185
46.19.86.186	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	168
2.54.43.109	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	154
46.19.85.103	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	141
46.19.86.255	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	129
93.173.137.111	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	128
109.253.135.119	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	123
2.54.62.187	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	117
62.219.118.151	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	116
109.253.156.7	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	115
37.26.148.189	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	106
109.253.128.165	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	95
109.253.144.140	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.144.140	Block	92
46.19.85.233	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	75
2.52.149.40	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	75
2.54.19.74	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	66
212.235.35.62	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 212.235.35.62	Block	53
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	48
46.19.86.48	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	48
79.180.106.90	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	45
176.12.137.167	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	44
31.168.71.189	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	37
176.12.146.184	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	32
87.68.145.10	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	26
2.54.150.227	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.150.227	Block	23
85.7.204.38	Switzerland	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 85.7.204.38	Block	21
207.46.13.79	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	20
157.55.39.172	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	17
84.228.144.238	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	16
77.127.232.44	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	16
212.76.102.103	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	16
46.19.86.26	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	15
84.109.14.117	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.109.14.117	Block	15
5.102.254.83	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	14
195.160.240.11	Israel	147.237.76.31	nakchal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	14
176.12.141.78	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	13
176.12.144.83	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	13
109.253.143.21	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	12
176.12.140.246	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	11
157.55.39.171	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
5.102.254.107	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	10
2.54.166.241	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
164.138.112.105	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	10