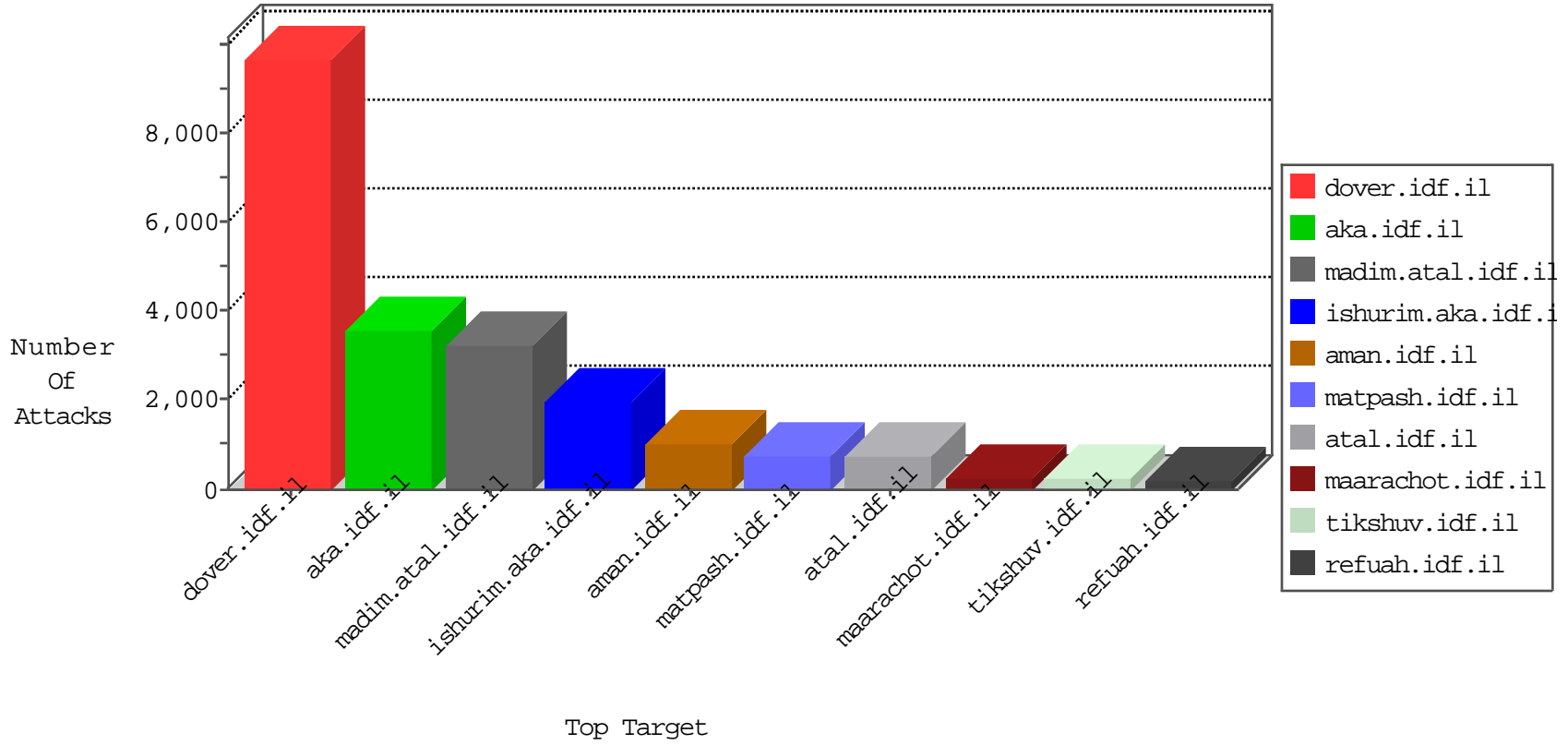


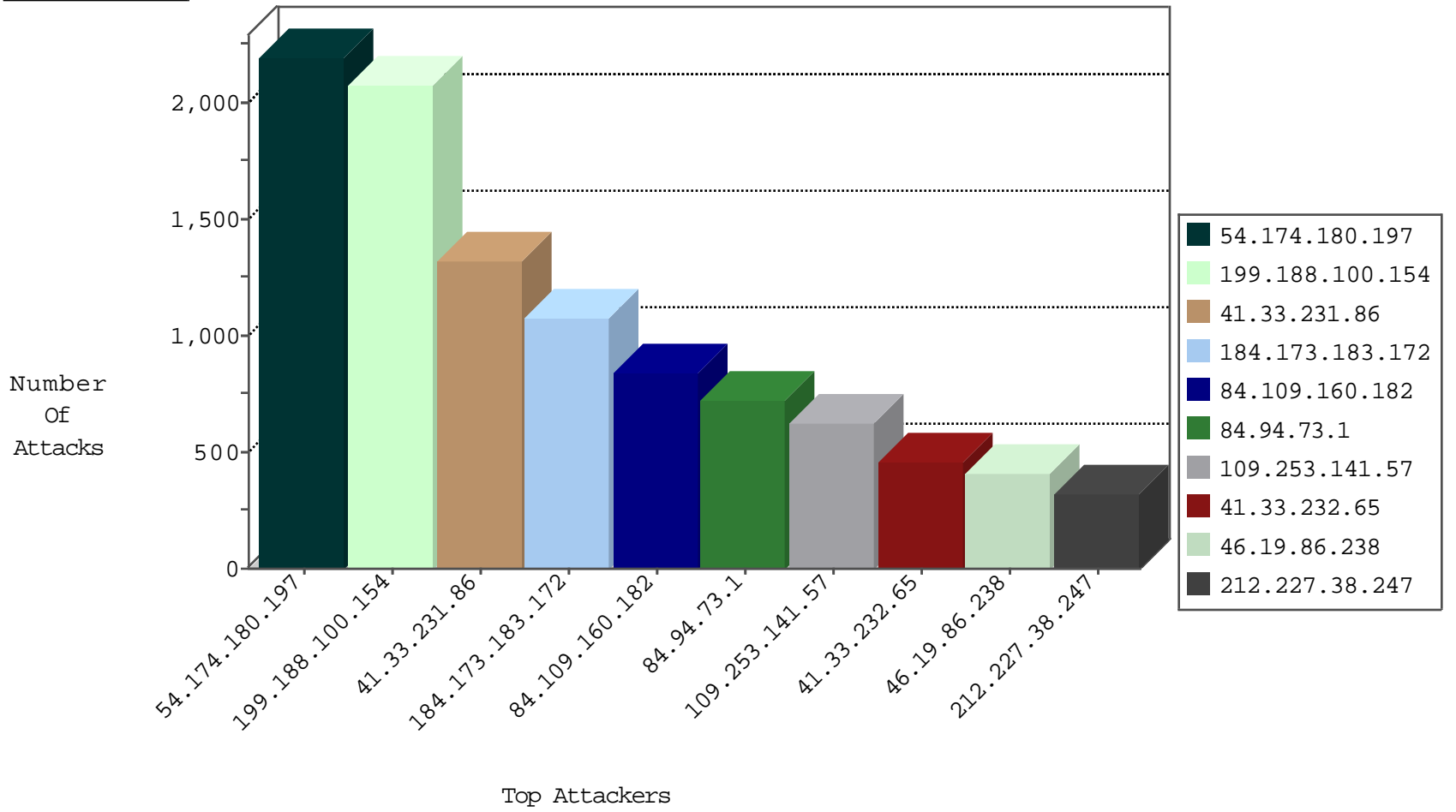
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	7199
66.249.67.31	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	4116
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3535
66.249.64.135	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3507
66.249.78.96	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2791
93.172.200.170	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	2206
82.80.156.245	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1387
66.249.78.89	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1188
66.249.78.82	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1158
66.249.78.127	United States	147.237.0.34	tikshuv.idf.il	TCP handshake violation, first packet not syn	drop	870
82.80.175.43	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	792
66.249.78.134	United States	147.237.0.34	tikshuv.idf.il	TCP handshake violation, first packet not syn	drop	742
66.249.64.195	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	722
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	697
66.249.67.23	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	628
66.249.64.131	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	583
66.249.78.2	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	409
66.249.78.29	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	362
149.88.108.96	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	278
79.179.67.124	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	277
66.249.93.224	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	267
66.249.78.160	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	258
79.183.56.172	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	230
79.176.174.242	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	217
197.200.127.252	Algeria	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-dun	dest-reset	213
46.120.31.40	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	201
84.95.199.113	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	191
217.132.218.108	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	173
93.173.44.125	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	155
79.181.28.10	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	144
109.160.250.150	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	136
109.66.113.133	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	118
66.249.81.191	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	118
81.199.120.207	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	112
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	102
84.228.153.83	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	forward	102
84.228.153.83	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	88
109.253.138.235	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	87
2.54.38.31	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	82
2.54.151.202	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	82
84.111.115.36	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	80
109.253.149.201	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	forward	80
2.54.33.31	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	78
46.19.86.193	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	78
93.173.241.76	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	77
93.173.186.121	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	76
85.65.144.201	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	76
213.57.47.90	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	75
213.57.197.50	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	74
5.22.129.241	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	74

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
54.174.180.197	United States	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	2196
199.188.100.154	United States	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	2075
184.173.183.172	United States	147.237.77.233	atal.idf.il	Rep_Notify_Only_Tehila	Permit	610
184.173.183.172	United States	147.237.77.176	matpash.idf.il	Rep_Notify_Only_Tehila	Permit	468
212.227.38.247	Germany	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	321
77.95.229.11	Netherlands	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	163
77.125.112.206	Israel	147.237.72.166	aka.idf.il	1633: HTTP: WebDAV Protocol PROPFIND Method	Block	117
178.175.131.194	Moldova, Republic of	147.237.72.156	aman.idf.il	Rep_Notify_Only_Tehila	Permit	73
93.115.84.124	Anonymous Proxy	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	34
79.183.38.190	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	32
176.9.25.72	Germany	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	19
62.212.89.116	Netherlands	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	19
64.87.19.244	United States	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	19
193.111.137.178	Germany	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	18
192.188.242.174	Hungary	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	15
37.205.9.131	Slovakia	147.237.72.166	aka.idf.il	Rep_Notify_Only_Tehila	Permit	10
5.9.230.65	Germany	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	10
193.11.137.201	Sweden	147.237.0.17	m.my-kosher-kravi.idf.il	Rep_Notify_Only_Tehila	Permit	10
37.205.9.131	Slovakia	147.237.72.156	aman.idf.il	Rep_Notify_Only_Tehila	Permit	10
37.142.68.47	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
71.6.165.200	United States	147.237.72.14	dover.idf.il(old)	Block_Level_70_100	Block	6
212.34.12.134	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
66.240.192.138	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Level_70_100	Block	6
213.140.59.158	Algeria	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
37.142.126.154	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
188.255.112.224	Russian Federation	147.237.0.19	madim.atal.idf.il	Rep_Notify_Only_Tehila	Permit	6
66.240.192.138	United States	147.237.72.156	aman.idf.il	Block_Level_70_100	Block	5
46.116.203.34	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
198.20.69.98	United States	147.237.76.177	ncore.idf.il	Block_Level_70_100	Block	5
66.240.192.138	United States	147.237.0.200	m4u.idf.il	Block_Level_70_100	Block	5
66.240.236.119	United States	147.237.77.178	e.matpash.idf.il	Block_Level_70_100	Block	5
66.240.236.119	United States	147.237.76.198	e.yohalan.idf.il	Block_Level_70_100	Block	5
66.240.236.119	United States	147.237.77.61	e.cogat.idf.il	Block_Level_70_100	Block	5
66.240.192.138	United States	147.237.76.201	e.atal.idf.il	Block_Level_70_100	Block	5
71.6.135.131	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Level_70_100	Block	5
79.181.160.20	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
5.29.199.135	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
66.240.236.119	United States	147.237.76.31	nakchal.idf.il	Block_Level_70_100	Block	4
66.240.192.138	United States	147.237.76.42	refuah.idf.il	Block_Level_70_100	Block	4
71.6.165.200	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Level_70_100	Block	4
71.6.135.131	United States	147.237.77.233	atal.idf.il	Block_Level_70_100	Block	4
71.6.167.142	United States	147.237.72.166	aka.idf.il	Block_Level_70_100	Block	4
66.240.236.119	United States	147.237.77.121	e.navy.idf.il	Block_Level_70_100	Block	4
77.125.3.71	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
84.108.101.27	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
109.64.106.132	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
84.110.0.53	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
66.240.192.138	United States	147.237.77.227	e.hamaz.idf.il	Block_Level_70_100	Block	4
71.6.135.131	United States	147.237.8.50	e.tikshuv.idf.il	Block_Level_70_100	Block	4
66.240.236.119	United States	147.237.76.148	ggcenter.aka.idf.il	Block_Level_70_100	Block	4

## 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	143
54.224.149.230	United States	147.237.77.176	matpash.idf.il	Tehila - Perl LWP with fake user agent	36
178.238.235.184	Germany	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	30
109.65.97.96	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	10
188.120.148.158	Israel	147.237.72.167	ishurim.aka.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	10
84.111.65.42	Israel	147.237.72.166	aka.idf.il	POLICY-OIHER TCP packet with urgent flag attempt	5
109.253.141.57	Israel	147.237.0.19	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	3
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	3
213.151.63.240	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
5.22.130.21	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
85.250.158.232	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
222.186.15.202	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	2
213.57.161.246	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
115.231.218.23	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	2
79.183.145.106	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
37.142.46.107	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
85.64.89.8	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
222.186.15.202	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	2
46.116.149.47	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.181.179.120	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
115.231.218.23	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	2
176.12.147.141	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.181.22.168	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.108.210.49	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.180.110.114	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
149.88.69.180	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.65	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
167.88.43.233		147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	2
84.94.20.153	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.177.144.203	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
149.78.50.209	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
115.231.218.23	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	2
80.246.133.12	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
222.186.15.202	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	2
213.57.171.7	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
2.54.60.225	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
115.231.218.23	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	2
85.250.142.12	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.182.182.147	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
115.231.218.23	China	147.237.76.34	yochalan.idf.il	ET SCAN Potential SSH Scan	2
176.12.149.47	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.228.227.86	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.181.146.40	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.67	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	2
149.88.70.77	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.180.124.32	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.66	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
84.95.223.164	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.179.180.214	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
149.78.186.189	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
41.33.231.86	Egypt	147.237.77.216	dover.idf.il		drop	drop	1322
41.33.232.65	Egypt	147.237.77.216	dover.idf.il		drop	drop	454
207.241.229.191	United States	147.237.72.166	aka.idf.il	SAM rule	drop	drop	136
188.120.148.158	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	117
168.235.195.24		147.237.77.176	matpash.idf.il		drop	drop	109
188.120.148.158	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid ACK number	Bad TCP sequence		56
111.67.21.185	Australia	147.237.77.216	dover.idf.il	SAM rule	drop	drop	48
5.102.254.132	Israel	147.237.0.19	madim.atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	48
207.241.229.191	United States	147.237.77.216	dover.idf.il	SAM rule	drop	drop	40
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission		33
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	33
5.28.186.149	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
192.117.105.8	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	32
168.235.195.24		147.237.77.176	matpash.idf.il	Invalid ACK number	Bad TCP sequence	monitor	29
84.228.186.140	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	27
2.54.12.154	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	26
2.54.12.154	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence		26
31.44.129.222	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	26
2.54.12.154	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	26
91.115.132.120	Austria	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	25
91.115.132.120	Austria	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission		25
77.125.84.193	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	24
37.76.193.192	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il		drop	drop	24
79.180.112.94	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	23
79.177.161.91	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	23
89.138.240.168	Israel	147.237.72.166	aka.idf.il		drop	drop	22
46.19.85.76	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
166.137.252.85	United States	147.237.77.226	www.chamatz.aka.idf.il		drop	drop	22
213.55.107.67	Ethiopia	147.237.77.216	dover.idf.il		drop	drop	21
79.182.11.62	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	21
94.159.162.129	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	21
8.37.225.140	Anonymous Proxy	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	20
65.255.37.232	Satellite Provider	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	20
70.39.187.130	Satellite Provider	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	20
46.116.171.131	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	20
23.236.125.224	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	20
79.178.199.58	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	19
46.19.85.76	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission		19
80.246.130.187	Israel	147.237.77.226	www.chamatz.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	19
81.218.104.6	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	18
84.111.164.124	Israel	147.237.77.170	maarachot.idf.il	Invalid ACK number	Bad TCP sequence	monitor	18
212.179.61.127	Israel	147.237.77.212	e.dover.idf.il	Geo-location inbound enforcement	Geo-location enforcement	monitor	18
107.188.0.18		147.237.77.216	dover.idf.il		drop	drop	17
46.117.249.186	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	17
94.159.155.206	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	17
5.28.186.149	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	17
83.19.96.114	Poland	147.237.77.216	dover.idf.il	SAM rule	drop	drop	16
31.210.185.153	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	16
2.54.133.221	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
197.200.127.252	Algeria	147.237.77.216	dover.idf.il		drop	drop	16

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
84.109.160.182	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 84.109.160.182	Block	834
84.94.73.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	720
109.253.141.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	619
109.253.149.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	293
46.19.86.238	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.238	Block	257
46.19.86.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	149
207.241.229.191	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	124
46.116.34.1	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	47
46.117.236.245	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.117.236.245	Block	46
66.249.78.153	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.153	Block	44
66.249.78.146	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.146	Block	41
46.210.92.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	37
46.19.85.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	32
94.159.159.218	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (404) in Session from 94.159.159.218	Block	29
66.249.78.160	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.160	Block	28
66.249.78.159	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	28
109.65.32.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	28
82.102.141.204	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 82.102.141.204	Block	22
46.19.85.202	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	21
66.249.78.236	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//giyus/forum/asp/showforum.asp	Block	20
184.74.50.54	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/hebrew/news/main.stm	Block	18
37.142.207.28	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	16
77.127.177.207	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	16
184.74.50.46	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/hebrew/news/main.stm	Block	16
184.74.50.46	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/newsite/hebrew/main.stm	Block	16
66.249.81.197	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	16
66.249.81.194	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	15
66.249.78.95	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.95	Block	14
5.29.62.179	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/70684.pdfwww.tamil2100.co.il/category.aspx	Block	14
213.151.62.249	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/haredim/webresource.axd	Block	13
66.249.78.102	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.102	Block	13
184.74.50.50	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/newsite/hebrew/main.stm	Block	12
66.249.78.243	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//giyus/forum/asp/showforum.asp	Block	12
95.86.118.1	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	12
184.74.50.42	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 184.74.50.42	Block	11
39.50.152.168	Pakistan	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	11
176.12.145.19	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	11
46.116.203.34	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	11
66.249.81.191	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	11
66.249.78.250	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//giyus/forum/asp/showforum.asp	Block	11
46.116.212.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/lobby.aspx	Block	11
95.86.118.1	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	11
184.74.50.54	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/newsite/hebrew/main.stm	Block	11
151.250.10.208	Turkey	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	11
109.65.71.150	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	10
184.74.50.50	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/news/main.stm	Block	10
94.159.169.169	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	10
77.125.3.71	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	10
79.177.4.24	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/gius	Block	10
79.179.137.66	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	10