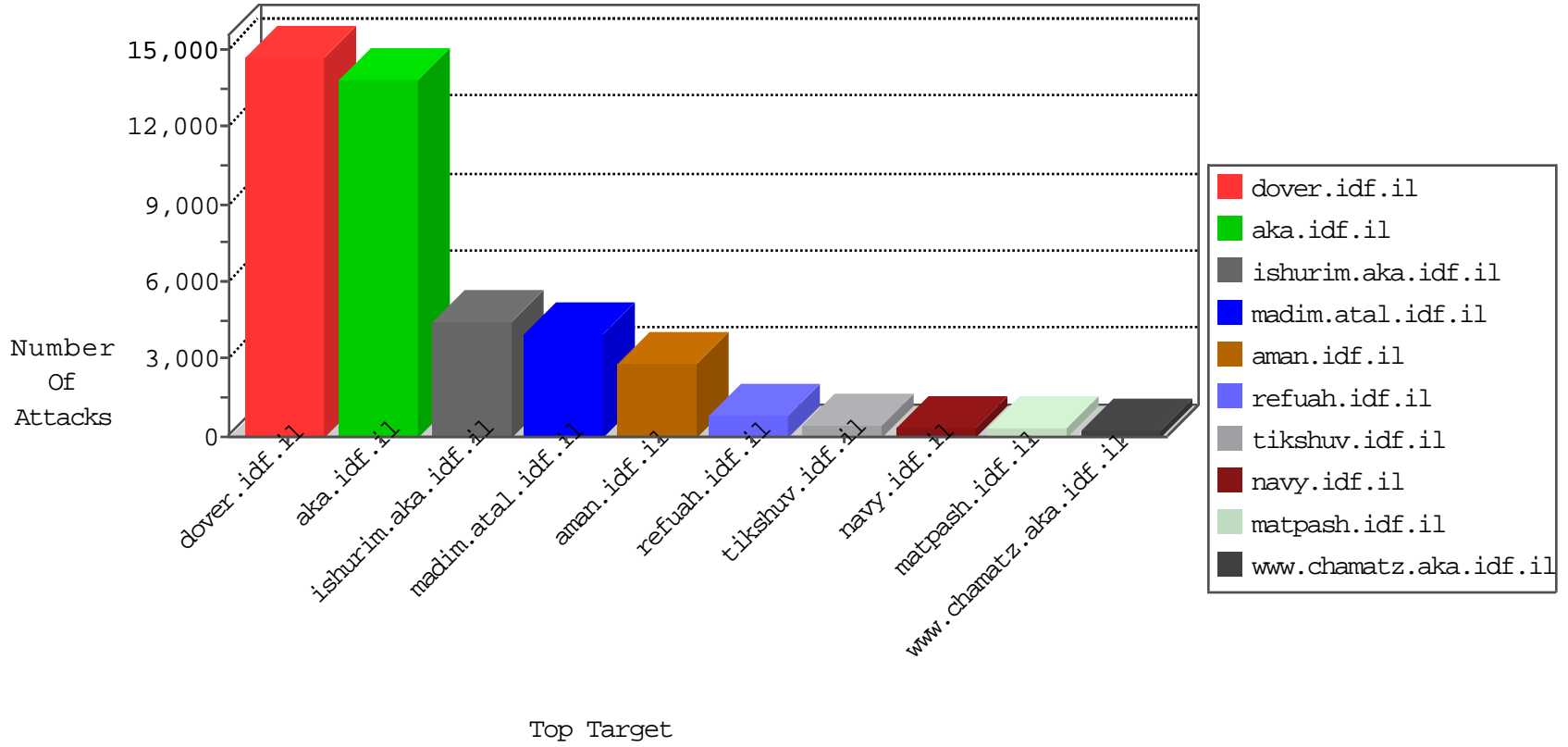


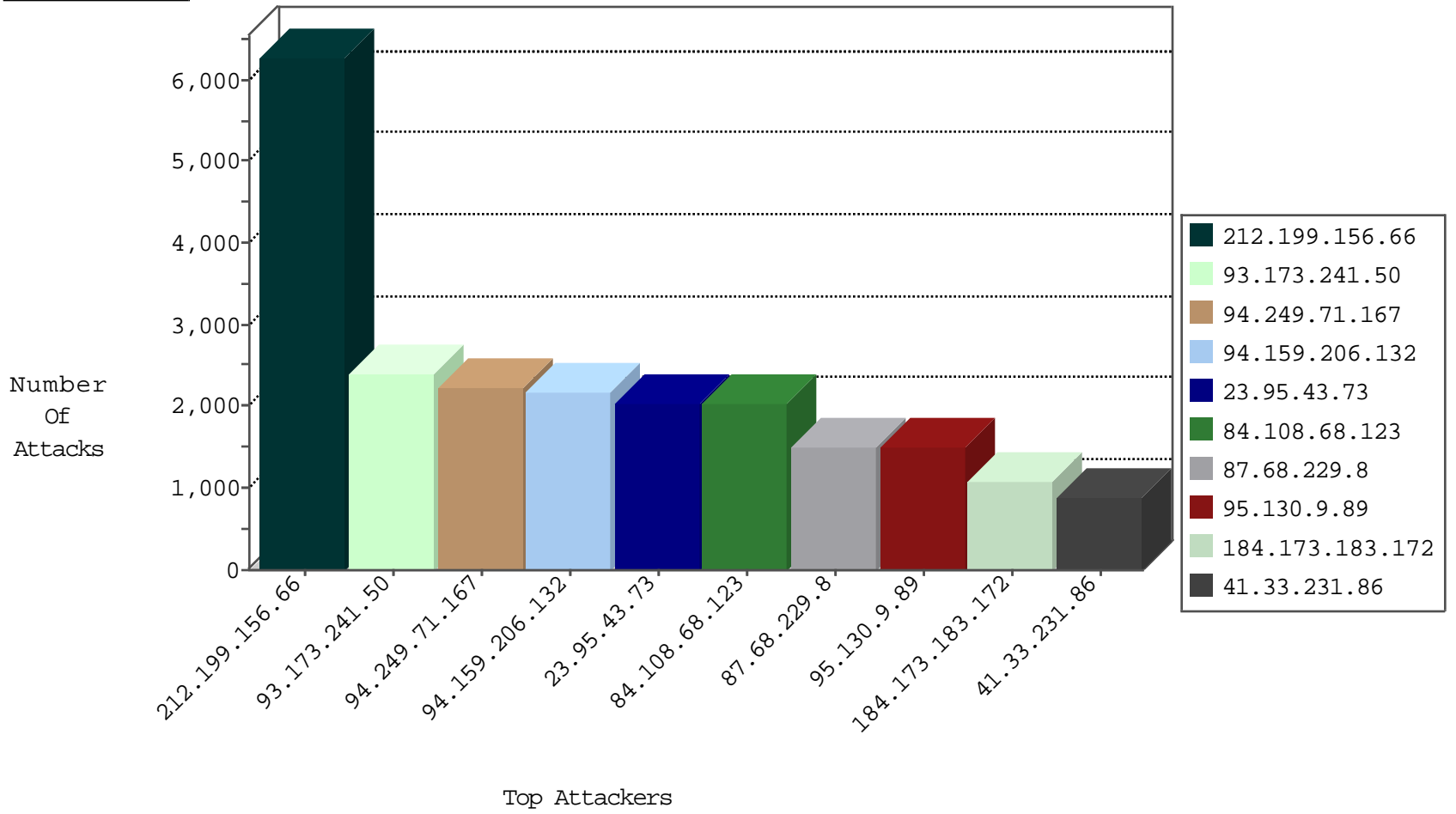
IDF Under Attack Daily Report



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	5680
46.120.146.147	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1307
109.253.134.40	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-SSL-renegotiation-Cli	forward	719
85.64.5.228	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	554
109.65.120.25	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	315
46.19.86.77	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	forward	310
37.26.148.207	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	282
66.249.78.96	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	276
109.160.204.170	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	257
84.228.156.76	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	231
79.182.103.183	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	209
213.57.44.166	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	forward	196
81.218.241.26	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	179
46.116.233.111	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	177
79.183.178.129	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	173
149.78.176.94	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	171
85.64.99.81	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	158
46.117.155.193	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	147
2.54.181.73	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	forward	146
91.231.192.149	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	145
46.19.85.154	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	forward	144
213.57.97.228	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	142
5.29.176.20	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	137
82.102.141.198	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	137
93.172.38.189	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	137
213.57.44.166	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	134
79.179.188.227	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	132
80.246.139.191	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	forward	132
46.120.31.40	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	131
87.68.67.61	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	127
79.183.165.242	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	123
94.249.71.167	Jordan	147.237.77.216	doover.idf.il	DOS-HTTP-fireflood	dest-reset	121
192.114.2.36	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	119
2.54.181.73	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	117
37.142.166.217	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	forward	117
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	117
149.78.209.164	United States	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	105
93.173.181.90	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	104
2.54.53.173	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	103
37.142.166.217	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	101
82.102.141.204	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	97
80.246.140.206	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	forward	96
2.54.2.12	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	93
2.54.59.177	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90
194.90.134.248	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	88
193.46.64.93	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	88
2.54.57.108	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	88
2.54.59.177	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	forward	88
46.120.146.147	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	forward	84
46.120.166.87	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	83

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
212.199.156.66	Israel	147.237.72.166	aka.idf.il	Rep_Notify_Only_Tehila	Permit	6283
93.173.241.50	Israel	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	2402
94.159.206.132	Israel	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	2178
23.95.43.73	United States	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	2037
84.108.68.123	Israel	147.237.72.156	aman.idf.il	Rep_Notify_Only_Tehila	Permit	2025
87.68.229.8	Israel	147.237.72.166	aka.idf.il	Rep_Notify_Only_Tehila	Permit	1506
95.130.9.89	France	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	1488
66.229.212.93	United States	147.237.72.166	aka.idf.il	Rep_Notify_Only_Tehila	Permit	730
184.173.183.172	United States	147.237.76.42	refuah.idf.il	Rep_Notify_Only_Tehila	Permit	548
162.247.72.27		147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	303
184.173.183.172	United States	147.237.77.176	matpash.idf.il	Rep_Notify_Only_Tehila	Permit	164
184.173.183.172	United States	147.237.76.86	navy.idf.il	Rep_Notify_Only_Tehila	Permit	140
184.173.183.172	United States	147.237.77.226	www.chamatz.aka.idf.il	Rep_Notify_Only_Tehila	Permit	138
176.10.99.207	Switzerland	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	129
184.173.183.172	United States	147.237.0.34	tikshuv.idf.il	Rep_Notify_Only_Tehila	Permit	95
84.229.91.5	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	68
27.159.235.46	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	33
79.176.52.18	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	15
212.34.12.153	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	12
37.205.9.131	Slovakia	147.237.72.156	aman.idf.il	Rep_Notify_Only_Tehila	Permit	10
37.205.9.131	Slovakia	147.237.72.166	aka.idf.il	Rep_Notify_Only_Tehila	Permit	10
66.85.131.91	United States	147.237.0.19	madim.atal.idf.il	Rep_Notify_Only_Tehila	Permit	8
192.114.23.18	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
218.77.79.43	China	147.237.76.38	e.e.meitav.idf.il	Block_Level_70_100	Block	6
71.6.135.131	United States	147.237.8.46	e.chinuch.idf.il	Block_Level_70_100	Block	6
212.29.202.206	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
84.229.91.5	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
37.142.49.53	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
87.69.148.24	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
218.77.79.43	China	147.237.76.202	e.halag.idf.il	Block_Level_70_100	Block	6
192.118.100.254	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
218.77.79.43	China	147.237.76.199	e.nakchal.idf.il	Block_Level_70_100	Block	5
218.77.79.43	China	147.237.76.44	e.refuah.idf.il	Block_Level_70_100	Block	5
71.6.135.131	United States	147.237.0.200	m4u.idf.il	Block_Level_70_100	Block	5
218.77.79.43	China	147.237.76.200	eitan.aka.idf.il	Block_Level_70_100	Block	5
79.177.181.114	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
218.77.79.43	China	147.237.76.196	e.sviva.idf.il	Block_Level_70_100	Block	5
218.77.79.43	China	147.237.76.201	e.atal.idf.il	Block_Level_70_100	Block	5
66.240.192.138	United States	147.237.77.243	mobile.idf.il	Block_Level_70_100	Block	5
218.77.79.43	China	147.237.76.147	chinuch.aka.idf.il	Block_Level_70_100	Block	5
71.6.165.200	United States	147.237.77.235	sviva.idf.il	Block_Level_70_100	Block	5
65.94.22.217	Canada	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
84.109.1.189	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
218.77.79.43	China	147.237.76.198	e.yochanan.idf.il	Block_Level_70_100	Block	5
218.77.79.43	China	147.237.76.42	refuah.idf.il	Block_Level_70_100	Block	5
46.19.85.104	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
218.77.79.43	China	147.237.76.31	nakchal.idf.il	Block_Level_70_100	Block	5
208.92.211.146	United States	147.237.72.166	aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
82.102.141.209	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.120.107.197	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	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	131
2.54.141.198	Israel	147.237.72.167	ishurim.aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	12
59.106.108.116	Japan	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
79.177.53.92	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
84.229.50.33	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
109.64.108.144	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	3
61.240.144.66	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	2
46.120.73.132	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
188.138.9.51	Germany	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 1024	2
62.90.176.91	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
2.54.47.173	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
94.159.189.172	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
212.38.181.177	United Kingdom	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	2
85.250.36.44	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
89.139.165.69	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.186.6.64	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
212.38.181.186	United Kingdom	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	2
85.250.15.255	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
212.38.181.194	United Kingdom	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
212.38.181.254	United Kingdom	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	2
212.38.181.173	United Kingdom	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	2
85.64.210.251	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
212.38.181.135	United Kingdom	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	2
93.172.19.103	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.177.7.34	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.67.16.217	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.140	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
80.246.130.33	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
212.38.181.197	United Kingdom	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	2
46.19.85.165	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
213.57.168.212	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.228.96.113	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
176.12.144.10	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
80.74.124.183	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.64.199.19	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
77.126.163.16	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
176.228.183.201	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.19.85.159	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
82.102.141.204	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.64.116.76	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
87.68.211.179	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.67	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
212.38.181.143	United Kingdom	147.237.76.148	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	2
95.86.90.115	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
132.66.223.67	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
87.68.52.230	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.180.62.134	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
62.0.231.1	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.19.85.17	Israel	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	871
41.33.232.65	Egypt	147.237.77.216	dover.idf.il		drop	drop	278
31.168.143.10	Israel	147.237.76.30	himush.idf.il		drop	drop	173
64.22.71.223	United States	147.237.72.166	aka.idf.il		drop	drop	67
2.54.141.103	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	63
213.8.96.180	Israel	147.237.77.216	dover.idf.il		drop	drop	45
82.166.65.243	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	43
195.110.40.7	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
80.178.206.210	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	39
2.54.23.251	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	37
46.19.85.72	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
62.219.237.218	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
212.150.71.177	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
2.54.141.103	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	29
80.179.6.134	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	28
46.19.86.56	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	26
85.65.117.142	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	25
46.19.85.80	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
192.115.248.2	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	24
31.44.143.192	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	24
82.80.161.185	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
212.143.57.115	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	22
194.90.147.229	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	21
212.25.102.63	Israel	147.237.77.216	dover.idf.il		drop	drop	21
46.19.86.63	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
185.32.179.118	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence		20
2.54.23.251	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	20
185.32.179.118	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	20
185.32.179.118	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	20
2.54.22.51	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	19
185.32.177.115	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence		19
185.32.177.115	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	19
46.19.85.51	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	19
185.32.177.115	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	19
2.54.22.51	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence		19
132.64.27.60	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	19
2.54.22.51	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	19
213.8.68.217	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	19
46.19.85.72	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	18
41.191.80.4	Egypt	147.237.77.216	dover.idf.il		drop	drop	18
5.28.132.42	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	18
199.190.45.67	Satellite Provider	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	18
192.116.165.35	Israel	147.237.77.226	www.chamatz.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	17
212.143.222.71	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	17
41.33.226.98	Egypt	147.237.77.216	dover.idf.il		drop	drop	17
82.166.65.243	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	17
84.108.105.151	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	16
31.168.202.63	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
109.160.235.27	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	monitor	16
31.186.228.65	United Kingdom	147.237.72.166	aka.idf.il		drop	drop	16

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.253.151.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	639
94.249.71.167	Jordan	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 94.249.71.167	Block	589
94.249.71.167	Jordan	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 94.249.71.167	Block	589
94.249.71.167	Jordan	147.237.77.216	dover.idf.il	Multiple Malformed URL from 94.249.71.167	Block	589
109.253.147.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	353
46.19.85.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	344
109.253.134.40	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.134.40	Block	321
46.19.86.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	303
2.54.129.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	251
176.12.138.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	236
193.41.209.2	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	173
94.249.71.167	Jordan	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 94.249.71.167	Block	171
94.249.71.167	Jordan	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	169
46.19.85.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	147
37.26.148.248	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.148.248	Block	146
46.19.85.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	146
37.26.147.235	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.147.235	Block	127
176.12.144.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	111
109.253.130.213	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.130.213	Block	100
207.241.229.184	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	72
109.253.136.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	69
100.42.60.215	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/994-8613-he/navy.aspx.aspx	Block	53
95.86.102.127	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	51
5.28.160.230	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	42
66.249.78.146	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.146	Block	41
79.176.52.18	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	36
87.68.111.5	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottonnavigaton.asp	Block	33
66.249.78.160	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.160	Block	33
46.19.85.46	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.46	Block	32
66.249.78.102	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.102	Block	28
176.12.142.66	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottonnavigaton.asp	Block	27
2.54.172.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	26
64.22.71.223	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 64.22.71.223	Block	25
2.54.134.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	25
213.8.52.149	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	24
66.249.78.95	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.95	Block	24
149.78.38.192	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	23
149.88.85.206	United States	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	None	22
5.102.203.193	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	22
84.228.156.114	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.228.156.114	Block	22
66.249.78.153	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.153	Block	21
192.114.91.228	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 192.114.91.228	Block	20
95.86.72.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il//main/rabanut/webresource.axd	Block	18
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	18
5.29.126.155	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	17
212.179.159.253	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	17
109.253.157.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
149.88.85.206	United States	147.237.72.167	ishurim.aka.idf.i	Too Many of the Same Response Code (404) in Session from 149.88.85.206	Block	16
109.253.147.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
66.249.78.236	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.236	Block	15