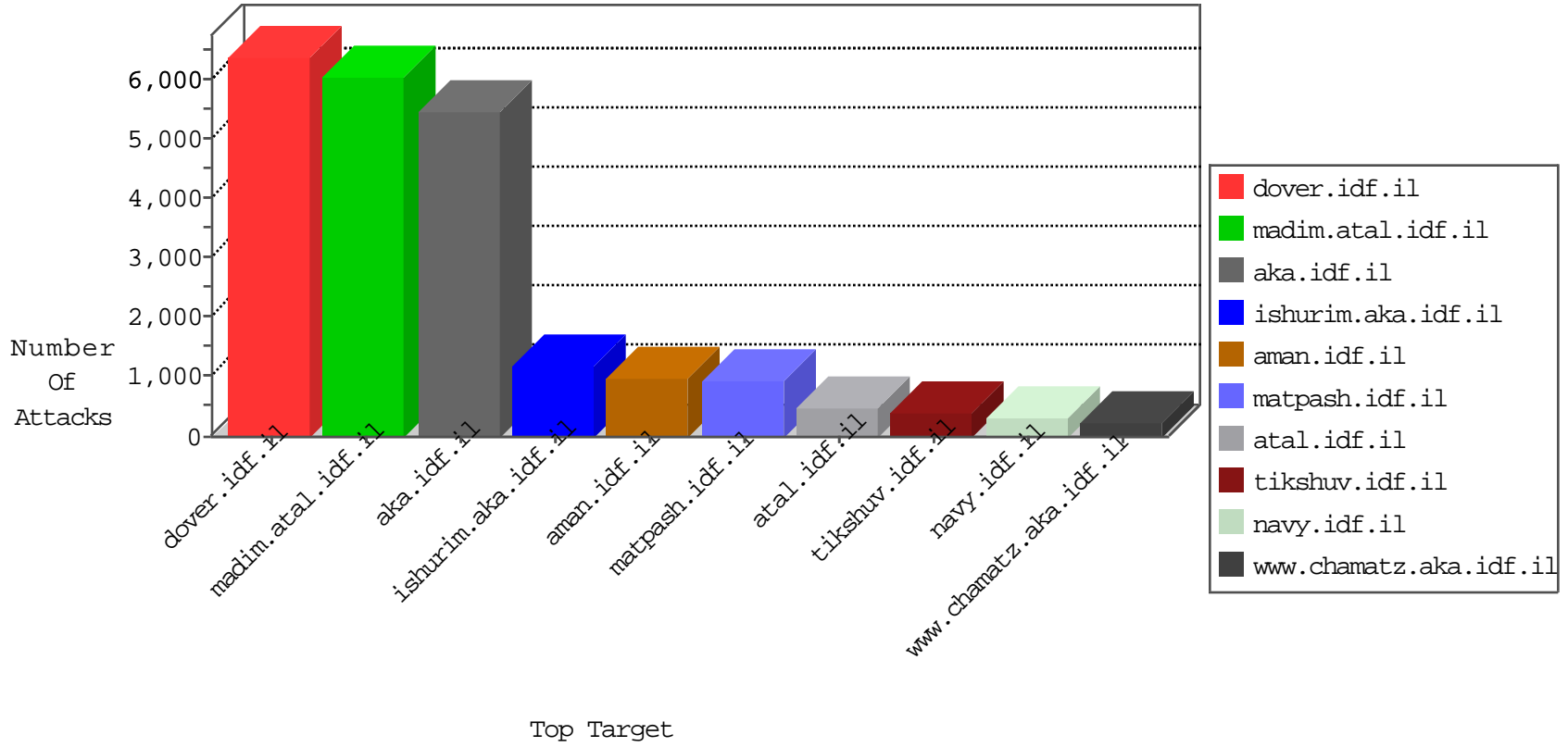


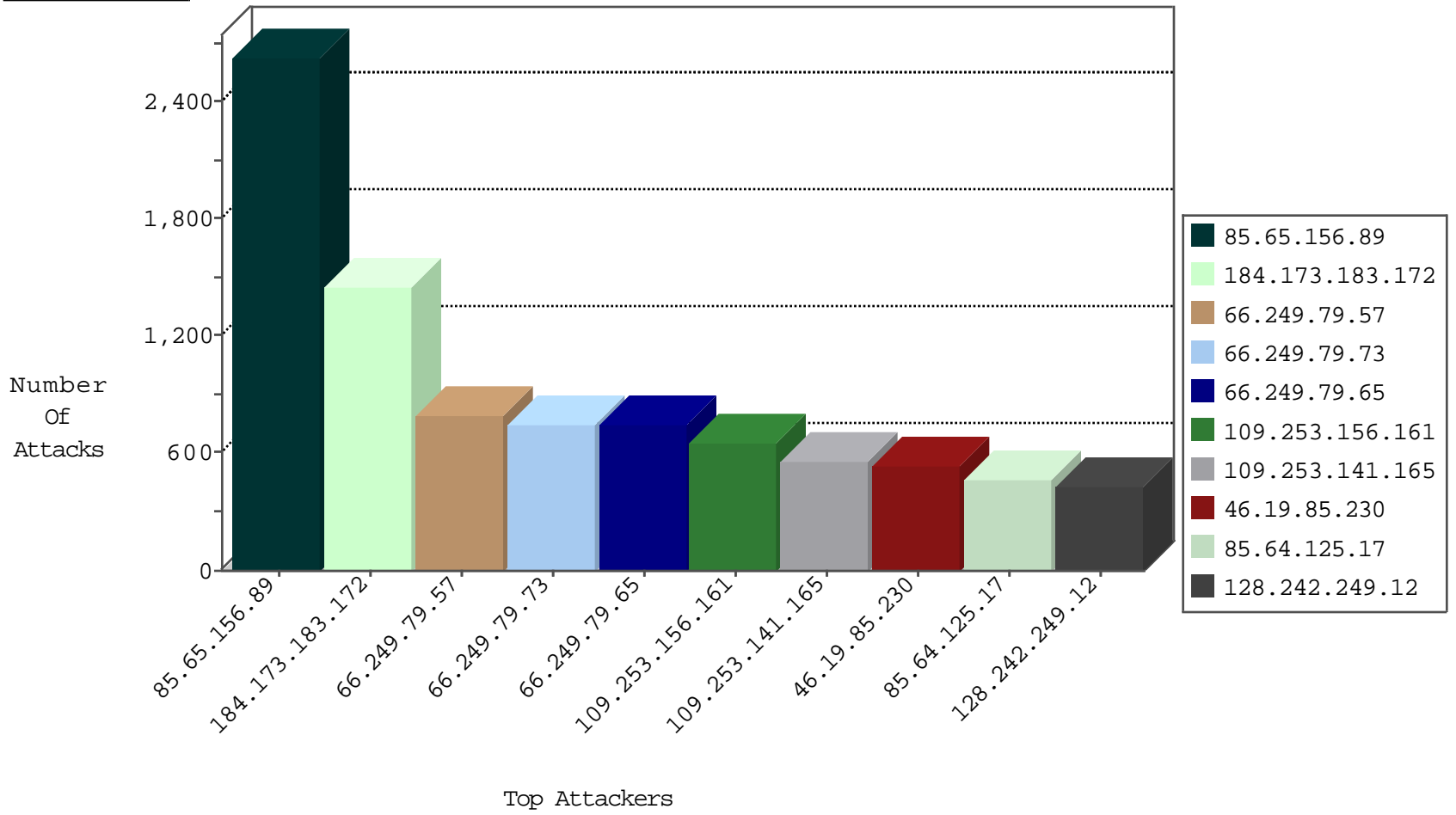
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
46.120.146.147	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	726
46.117.20.86	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	682
85.65.156.89	Israel	147.237.72.166	aka.idf.il	JLM_Purple_Con_Limit_Http	drop	603
46.121.74.138	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	511
93.172.57.21	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	457
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	456
109.65.48.24	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	447
83.130.103.109	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	334
85.65.156.89	Israel	147.237.72.166	aka.idf.il	JLM_Purple_Con_Limit_Tcp	drop	316
5.29.40.169	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	294
77.125.97.24	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	283
84.229.197.205	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	265
85.250.109.125	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	246
77.125.124.94	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	196
109.186.154.148	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	177
87.69.148.235	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	174
79.178.2.153	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	160
66.249.73.132	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	133
79.180.190.164	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	129
77.126.147.173	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	123
85.250.153.133	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	123
188.120.148.59	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	120
79.179.33.58	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	119
2.54.158.59	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	118
46.117.228.118	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	118
46.121.229.80	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	116
212.117.143.250	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	114
66.249.73.244	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	94
213.57.182.179	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	93
87.69.18.47	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90
2.54.18.37	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	86
2.54.145.76	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	85
93.172.57.21	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	forward	83
46.19.86.172	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	81
149.78.53.250	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	81
77.125.117.219	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	80
109.253.137.11	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	79
149.88.112.117	United States	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	79
87.69.7.2	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	78
46.19.86.184	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	77
85.250.158.218	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	77
176.12.136.128	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	75
79.178.102.192	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	75
79.177.110.5	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	74
89.138.78.145	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	73
109.253.140.117	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
109.253.156.125	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
2.54.175.21	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
46.19.85.111	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	69
79.177.0.127	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	68

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	657
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	526
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	425
87.69.36.147	Israel	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	311
184.173.183.172	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_P-N_40-59	Permit	140
184.173.183.172	United States	147.237.0.34	tikshuv.idf.il	DVRep_P-N_40-59	Permit	127
128.186.158.185	United States	147.237.72.166	aka.idf.il	1106: HTTP: IIS .%5c Encoded \ in URI	Permit	18
87.69.36.147	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	10
109.67.123.146	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	8
173.2.216.7	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
212.34.12.191	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
180.76.5.193	China	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	5
71.6.167.142	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	5
46.120.65.60	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
85.64.165.214	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
69.125.18.243	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
79.183.59.246	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
1.186.245.18	India	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.167.142	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	5
66.240.236.119	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	5
79.183.59.246	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
50.7.159.133	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	4
85.25.43.94	Germany	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	4
85.25.103.50	Germany	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	4
85.25.43.94	Germany	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	4
85.25.43.94	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	4
66.240.236.119	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	4
84.108.136.51	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
41.239.45.159	Egypt	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
204.73.55.131	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
85.25.43.94	Germany	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	4
93.197.244.178	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	4
82.211.223.3	Denmark	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	3
71.6.167.142	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	3
66.240.236.119	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	3
85.25.43.94	Germany	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	3
24.44.5.194	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
94.159.158.102	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
71.6.167.142	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	3
198.96.155.3	Canada	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	3
79.134.234.200	Iceland	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	3
71.6.165.200	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	3
179.99.200.39	Brazil	147.237.76.86	navy.idf.il	C1000098: Block - dns poisoning	Block	3
188.138.9.50	Germany	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	3
62.0.72.32	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
5.29.135.141	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
80.74.98.102	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	330
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	137
5.28.153.161	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	16
109.253.156.161	Israel	147.237.0.19	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	7
109.67.80.254	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	6
87.68.167.41	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
79.182.152.225	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
66.249.79.65	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	3
109.253.149.245	Israel	147.237.0.19	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	3
109.253.141.165	Israel	147.237.0.19	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	3
58.20.54.249	China	147.237.76.197	e.himush.idf.il	ET SCAN NMAP -sS window 1024	2
46.19.85.96	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
58.20.54.249	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
37.142.246.83	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
77.126.230.142	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
37.142.154.35	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.120.139.69	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
93.173.239.225	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.229.8.55	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
77.125.103.35	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
31.210.187.110	Israel	147.237.0.19	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
5.29.202.194	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.111.65.42	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.117.127.59	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
2.54.171.57	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.108.136.51	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.116.169.98	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.105.114.103	France	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
85.64.88.47	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.65	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	2
46.19.86.15	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
87.216.216.184	Spain	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
61.240.144.67	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	2
149.78.44.15	Israel	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
82.102.141.210	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
87.69.240.211	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
213.8.129.132	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
87.69.114.11	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.67	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	2
37.142.236.12	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
87.68.109.98	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.177.103.116	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.120.222.29	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
95.86.67.227	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.253.128.133	Israel	147.237.72.156	aman.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
84.229.33.250	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.66	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	2
77.126.213.140	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
188.41.253.139	Turkey	147.237.77.216	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
85.65.156.89	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	1198
66.249.79.57	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	608
66.249.79.73	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	580
66.249.79.65	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	568
82.145.210.162	Europe	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	360
136.173.162.144	Belgium	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	138
149.88.105.14	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	90
66.249.93.158	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	64
176.219.151.9	Turkey	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	60
66.249.93.155	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	58
66.249.73.244	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	56
93.172.176.161	Israel	147.237.72.156	aman.idf.il	SAM rule	drop	drop	54
93.172.176.161	Israel	147.237.72.166	aka.idf.il	SAM rule	drop	drop	53
85.64.111.102	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	48
78.108.161.226	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	45
109.66.160.188	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
109.64.152.133	Israel	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	42
203.132.214.155	India	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	38
66.249.78.51	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
66.249.93.152	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
66.249.78.44	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
84.108.14.90	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.160.156.83	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	29
66.249.81.200	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
149.78.196.165	United States	147.237.77.216	dover.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	27
85.65.156.89	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	27
82.102.141.215	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
66.249.78.37	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
84.229.5.206	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
31.210.186.76	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	23
188.120.148.117	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	monitor	23
158.169.150.10	Belgium	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	22
46.19.86.155	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	21
213.6.134.45	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	20
66.249.93.195	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
158.169.40.6	Luxembourg	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	20
109.66.137.214	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	19
109.253.128.133	Israel	147.237.72.156	aman.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	19
66.249.81.197	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
136.243.36.96	Germany	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
198.15.120.42	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
109.253.137.11	Israel	147.237.72.167	ishurim.aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	17
109.253.132.194	Israel	147.237.72.167	ishurim.aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	17
46.19.85.224	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	monitor	17
31.154.2.14	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	17
199.30.25.2	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
89.187.219.9	Lebanon	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
77.126.157.82	Israel	147.237.72.156	aman.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	16
190.92.78.46	Honduras	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
2.54.129.233	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.253.156.161	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	640
85.65.156.89	Israel	147.237.72.166	aka.idf.il	Automated Vulnerability Scanning	Block	572
109.253.141.165	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.141.165	Block	551
46.19.85.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	531
85.64.125.17	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	458
79.176.10.231	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 79.176.10.231	Block	414
84.228.80.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	399
31.210.187.110	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	310
176.12.148.88	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	310
46.19.85.48	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	310
82.80.163.88	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 82.80.163.88	Block	289
2.54.139.66	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	283
89.138.247.146	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	262
46.19.86.191	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	246
109.253.149.245	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.149.245	Block	238
87.68.30.68	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 87.68.30.68	Block	202
5.29.167.204	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	190
66.249.79.57	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.57	Block	173
66.249.79.65	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.65	Block	157
66.249.79.73	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.73	Block	156
176.12.137.39	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	106
176.12.150.28	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	86
149.78.136.214	United States	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 149.78.136.214	Block	77
91.242.33.8	Russian Federation	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 91.242.33.8	Block	61
91.242.33.8	Russian Federation	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 91.242.33.8	Block	61
213.57.217.29	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	34
79.182.116.156	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	27
54.172.21.120	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 54.172.21.120	Block	22
84.108.89.230	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	21
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	20
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	20
54.88.168.129	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 54.88.168.129	Block	16
84.228.114.103	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	13
85.250.59.166	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 85.250.59.166	Block	12
5.29.26.213	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	11
66.249.79.111	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.111	Block	10
66.249.79.103	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.103	Block	10
66.249.79.95	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.95	Block	10
178.137.84.200	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to ww.idf.il/1498-en/dover.aspx/	Block	9
37.115.186.0	Ukraine	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1498-en/dover.aspx/	Block	9
46.118.154.155	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1498-en/dover.aspx/	Block	9
79.179.28.227	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 79.179.28.227	Block	8
82.166.229.4	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
66.249.79.111	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1086-he/dover.aspx	Block	8
188.165.15.119	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.119	Block	6
157.55.39.1	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	6
87.68.30.68	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/mobile/shared/ajax/updatemakatgauntity.aspx	Block	6
157.55.39.1	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.1	Block	6
46.19.85.50	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	6
85.250.59.166	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/homepage/6_s3_	Block	6