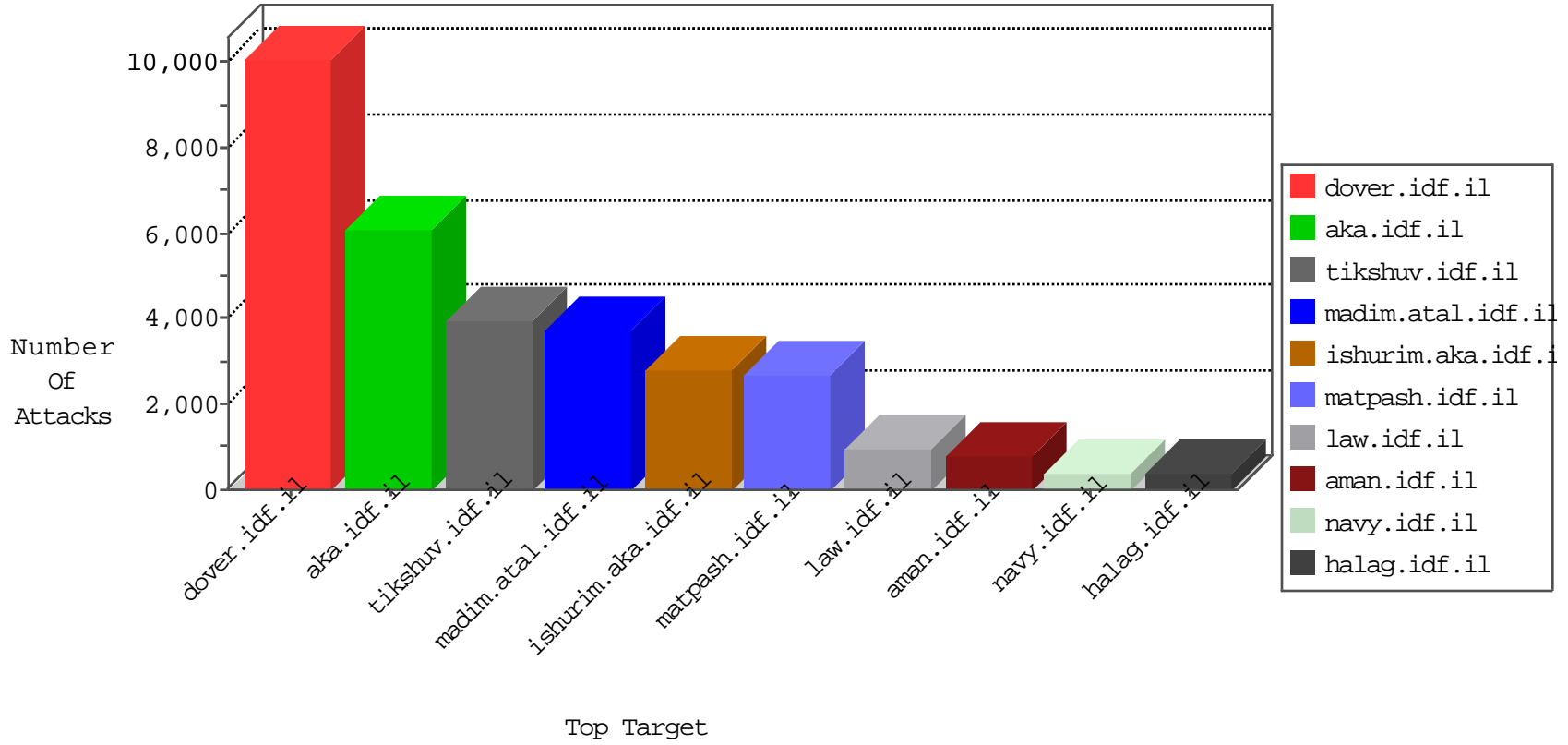


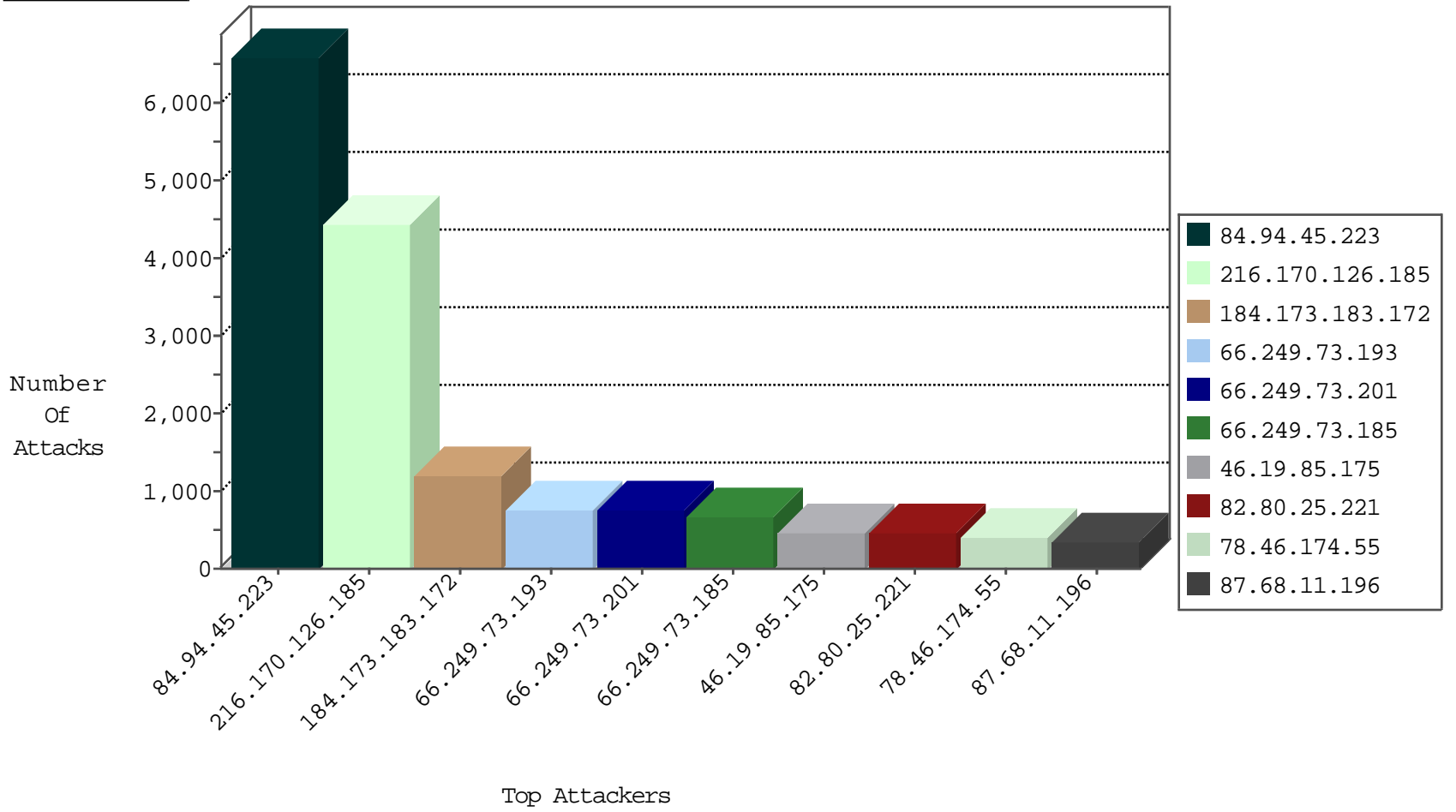
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
176.67.108.81	Palestinian Territory, Occupied	147.237.0.19	madim.atal.idf.il	TCP Scan (vertical)	drop	1078
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	819
192.116.94.67	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	571
87.69.222.23	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	509
5.28.170.97	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	496
109.66.120.46	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	436
79.180.111.7	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	402
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	256
46.121.142.226	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	230
85.64.109.73	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	224
5.29.155.104	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	207
109.64.131.209	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	205
79.180.194.58	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	191
109.160.254.196	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	183
212.76.114.240	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	182
2.54.56.219	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	174
79.180.160.106	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	172
79.177.191.10	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	169
84.108.119.106	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	168
84.228.170.99	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	158
79.183.106.170	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	154
79.178.201.248	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Client	dest-reset	153
212.117.143.250	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	128
212.25.67.206	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	123
194.90.233.61	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	117
194.90.151.18	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	114
77.127.60.197	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	113
5.29.38.219	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	112
5.28.181.150	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	107
213.57.182.179	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	107
213.8.71.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	105
79.177.24.43	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	102
77.126.3.76	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	102
84.111.5.7	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	100
109.66.142.116	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	96
80.179.78.115	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	93
84.228.34.91	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	87
46.19.85.108	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	86
5.29.97.58	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	82
2.54.1.39	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	82
82.80.25.221	Israel	147.237.77.216	doover.idf.il	Block_Udp_All_Nets	drop	81
91.231.192.149	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	80
85.64.64.28	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	80
46.19.85.192	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	78
84.111.54.107	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	78
109.160.241.207	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	77
46.19.86.170	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	76
109.67.10.64	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	75

02-25-2015-00:00:07 to 02-26-2015-00:00:07

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
80.246.136.171	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	74
109.253.152.254	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Client	dest-reset	73

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
84.94.45.223	Israel	147.237.0.34	tikshuv.idf.il	DVRep_P-N_40-59	Permit	3699
84.94.45.223	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	2904
216.170.126.185		147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	2221
216.170.126.185		147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	1486
216.170.126.185		147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	721
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	649
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	200
184.173.183.172	United States	147.237.76.30	himush.idf.il	DVRep_P-N_40-59	Permit	194
184.173.183.172	United States	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	183
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	174
37.59.19.32	France	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	120
85.250.116.231	Israel	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	55
180.76.5.193	China	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	47
46.116.205.31	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	32
212.235.62.200	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
194.50.175.183	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
91.227.164.5	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	11
84.108.174.41	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
71.6.135.131	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	6
198.211.110.195	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	6
198.20.70.114	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	6
198.20.70.114	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	5
79.176.48.37	Israel	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
46.19.85.56	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
198.20.69.98	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.72.156	aman.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
198.20.69.98	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	4
188.138.9.50	Germany	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	4
198.20.69.98	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	4
93.183.204.25	Ukraine	147.237.72.166	aka.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	4
46.121.202.210	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
198.20.69.98	United States	147.237.0.35	akaws.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	4
192.114.23.211	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
85.25.43.94	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	4
66.240.192.138	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	4
93.183.204.25	Ukraine	147.237.77.74	law.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	4
66.240.236.119	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	4
188.138.9.50	Germany	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	4
66.240.192.138	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	4
198.20.70.114	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	4
85.25.103.50	Germany	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	4
198.20.69.98	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	4
66.240.192.138	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	4

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	377
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	112
104.42.11.155		147.237.77.233	atal.idf.il	Tehila - Perl LWP with fake user agent	68
109.253.152.176	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	36
104.42.11.155		147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	33
176.67.108.81	Palestinian Territory, Occupied	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	11
93.183.204.25		147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	8
93.183.204.25	Ukraine	147.237.77.74	law.idf.il	Tehila - Perl LWP with fake user agent	8
46.19.86.17	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	5
109.66.9.154	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
87.69.241.127	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
104.42.18.238		147.237.77.233	atal.idf.il	Tehila - Perl LWP with fake user agent	4
199.38.85.16	United States	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
59.106.108.116	Japan	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
84.110.218.5	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.79.157	United States	147.237.72.166	aka.idf.il	ET SCAN NMAP -sA (2)	2
109.65.9.94	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.178.120.37	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.193	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	2
212.179.132.202	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.116.138.186	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
95.86.124.27	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
87.69.245.207	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.65	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	2
132.64.37.17	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
94.159.161.166	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
212.129.41.16	France	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	2
87.68.32.92	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.19.86.56	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
95.179.102.128	Russian Federation	147.237.76.86	navy.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
77.125.11.254	Israel	147.237.76.39	mobile.meitav.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	2
109.66.60.31	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
157.55.39.88	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
95.179.102.128	Russian Federation	147.237.72.166	aka.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
128.61.240.66	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	2
104.42.18.238		147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
213.57.242.107	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
109.65.126.129	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.193	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	2
2.52.133.201	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.65.25.23	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
149.88.113.57	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
81.218.66.107	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.64.129.80	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
212.150.214.90	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
176.12.150.193	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
5.102.254.95	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
77.127.60.88	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
128.61.240.66	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	2

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.73.201	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	466
66.249.73.193	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	449
66.249.73.185	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	382
82.145.219.74	Europe	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	210
67.246.115.103	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	160
137.135.176.71	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	104
41.63.181.54	Angola	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	75
192.116.220.67	Israel	147.237.72.166	aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	58
109.253.137.76	Israel	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	58
158.102.162.6	Italy	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	57
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	56
137.135.176.175	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	56
31.168.150.201	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	52
176.12.147.27	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	52
67.52.216.1	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	48
193.188.156.17	Sweden	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	48
190.153.249.194	Chile	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	45
193.43.244.102	Israel	147.237.72.167	ishurim.aka.idf.il	First packet isn't SYN	drop	drop	44
134.191.232.70	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
62.90.139.121	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	41
109.253.130.189	Israel	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	40
80.179.114.27	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	39
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
174.119.114.83	Canada	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
109.253.138.185	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
109.253.152.176	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	35
87.68.86.31	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	35
66.249.73.223	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
176.12.149.0	Israel	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
134.191.232.69	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
5.170.100.83	Italy	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
63.143.240.236	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
212.25.102.57	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	31
109.253.135.26	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.128.72	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.136.222	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.143.203	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.139.51	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.135.223	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
46.19.86.15	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
132.64.162.40	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	29
93.172.77.244	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	28
109.253.144.58	Israel	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
168.63.200.167	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
84.94.194.236	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
62.0.103.119	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
109.253.137.51	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
132.3.37.78	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
66.249.73.239	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
46.210.204.233	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.85.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	455
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 78.46.174.55	Block	341
87.68.11.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	338
66.249.73.193	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.193	Block	313
66.249.73.201	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.201	Block	277
66.249.73.185	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.185	Block	273
82.102.141.254	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 82.102.141.254	Block	222
82.80.131.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	209
46.19.86.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	199
176.12.151.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	183
80.246.136.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	178
176.12.138.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	173
109.253.153.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	143
80.246.137.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	140
109.253.145.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	122
109.253.133.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	120
213.57.137.121	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 213.57.137.121	Block	114
109.253.135.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	96
109.253.136.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	96
109.253.141.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	82
176.12.139.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	77
109.253.140.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	69
109.253.142.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	57
2.52.134.201	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.52.134.201	Block	50
46.19.86.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	50
109.253.156.205	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.156.205	Block	49
109.253.135.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	47
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	46
109.253.149.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	37
176.12.137.52	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.137.52	Block	32
80.179.5.71	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	30
176.12.140.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	27
2.54.58.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	21
95.86.90.12	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	21
109.253.145.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	20
62.219.142.146	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	None	18
66.249.73.185	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/view_imgtop.asp	Block	16
87.68.120.247	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 87.68.120.247	Block	15
176.12.151.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	15
109.253.135.188	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
2.52.33.22	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/console/core/doc_mgr/undefined	Block	13
84.94.205.212	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	None	13
46.229.164.113	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.229.164.113	Block	13
46.19.86.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	12
85.64.123.44	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	12
195.160.240.11	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/resources/styles/	Block	11
79.180.3.128	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
172.18.115.57		147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	11
178.255.215.87	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 178.255.215.87	Block	11
84.109.147.90	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/2042	Block	10