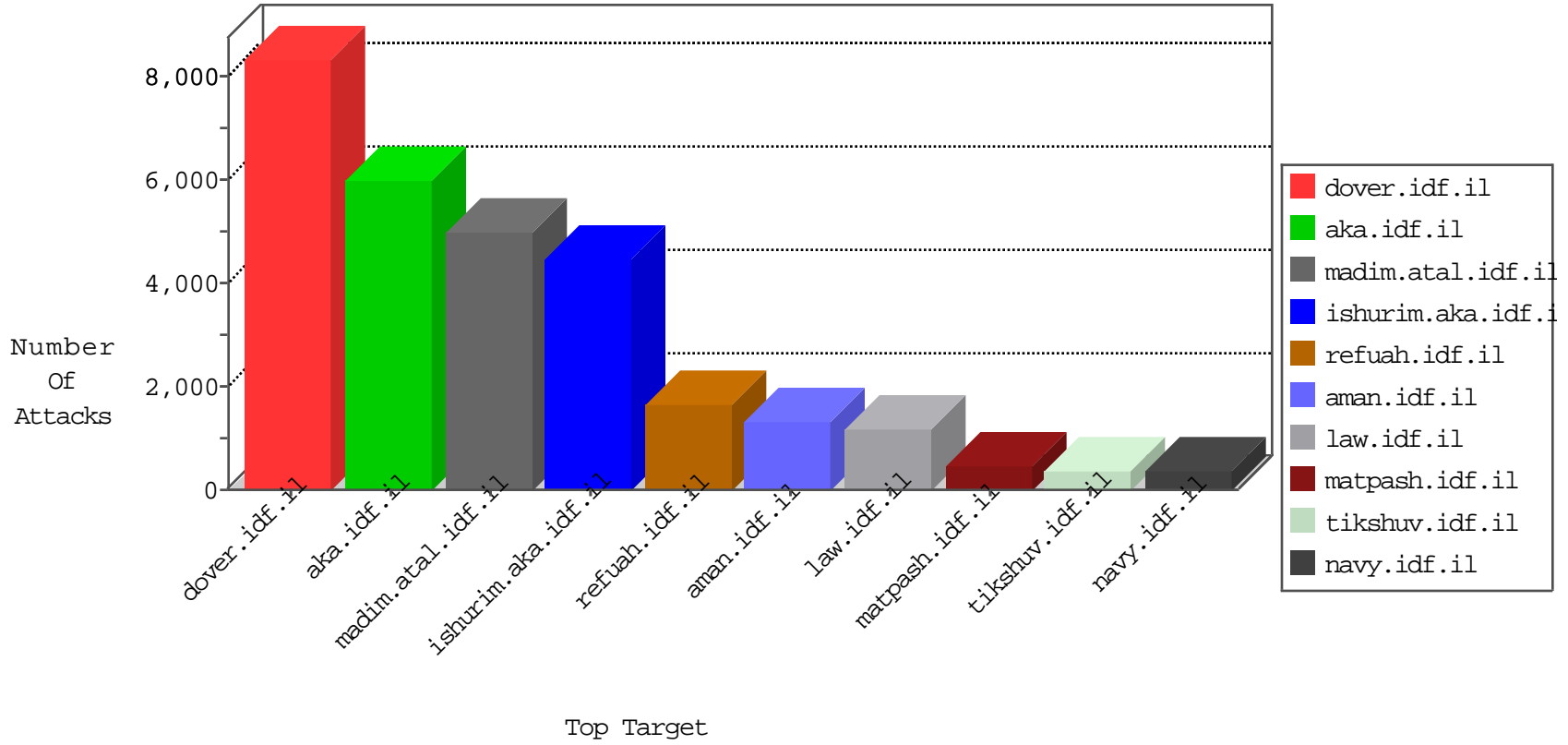


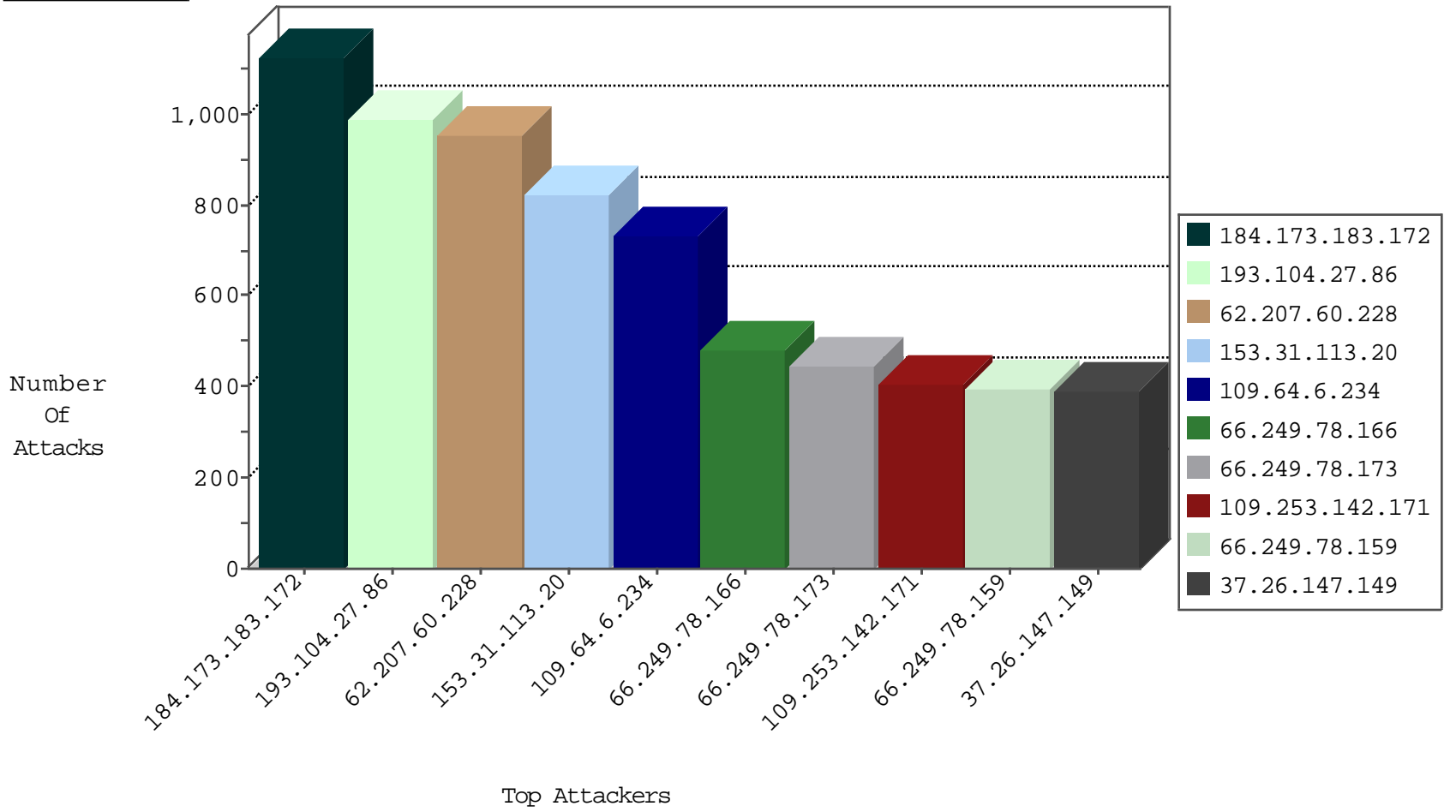
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
213.57.180.175	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	618
84.109.89.124	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	602
185.32.176.75	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	476
207.232.36.210	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	444
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	434
79.181.51.121	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	395
85.250.82.90	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	371
87.69.211.56	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	343
212.235.79.123	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	296
85.64.129.153	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	288
84.228.16.88	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	267
212.143.173.198	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	264
109.64.61.157	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	255
79.180.145.162	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	233
46.19.86.50	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	220
109.67.110.217	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	205
204.93.154.212	United States	147.237.77.233	atal.idf.il	TCP Scan (vertical)	drop	201
46.117.228.118	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	192
46.19.85.14	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	186
164.138.125.217	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	183
93.173.237.43	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	180
2.54.9.110	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	175
109.66.114.18	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	172
109.253.142.171	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	170
46.19.85.64	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	170
109.160.136.113	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	168
2.54.132.156	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	161
79.178.2.153	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	149
85.64.220.33	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	149
46.19.85.68	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	147
93.172.38.21	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	146
185.32.177.68	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	144
82.80.20.98	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	142
46.19.86.223	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	139
185.32.178.25	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	135
192.116.232.69	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	130
46.19.85.20	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	129
46.19.85.60	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	117
176.12.141.169	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	114
46.19.86.107	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	102
79.180.133.133	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	101
5.29.7.197	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	101
176.228.64.101	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	101
84.111.228.245	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	99
109.253.142.171	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	forward	98
46.19.86.50	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	95
2.54.140.129	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	93
46.19.85.186	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	90
84.109.127.254	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	89
46.117.231.159	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
193.104.27.86	Russian Federation	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	989
184.173.183.172	United States	147.237.76.42	refuah.idf.il	DVRep_P-N_40-59	Permit	548
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	523
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	376
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	57
180.76.5.193	China	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	41
104.148.44.150		147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	36
80.178.148.81	Israel	147.237.72.166	aka.idf.il	12371: TCP: Hulk DDoS Tool	Block	25
213.8.118.92	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	20
205.155.65.226	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	13
109.253.157.112	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	12
105.109.32.184	Algeria	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	9
66.42.249.229	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
84.109.139.246	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
84.108.236.233	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
80.74.104.71	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
37.26.147.167	Israel	147.237.72.156	aman.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	6
89.187.142.208	Czech Republic	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	6
85.25.43.94	Germany	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	5
77.247.181.163	Netherlands	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	5
71.6.165.200	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	5
66.240.236.119	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	5
71.6.165.200	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	5
85.25.43.94	Germany	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	5
79.181.177.218	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
71.6.167.142	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	5
66.175.218.156	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
46.121.142.118	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
92.40.54.124	United Kingdom	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
85.25.43.94	Germany	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	4
81.218.33.77	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
85.25.43.94	Germany	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	4
82.102.141.199	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
80.246.136.209	Israel	147.237.0.19	madim.atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
109.186.131.37	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	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	4
132.66.26.130	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
71.6.165.200	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	4
46.19.85.195	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
71.6.167.142	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	4
46.19.85.172	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
71.6.165.200	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	3
71.6.165.200	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	3
66.240.236.119	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	3
85.25.43.94	Germany	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	3
71.6.165.200	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	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	297
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	125
132.147.8.63	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	5
84.94.180.171	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
31.210.187.69	Israel	147.237.72.156	aman.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	3
213.57.37.180	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	3
132.74.95.59	Israel	147.237.77.170	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
79.183.114.212	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
85.64.216.38	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
159.220.76.2	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
65.175.104.99	United States	147.237.77.176	matpash.idf.il	Tehila - Perl LWP with fake user agent	2
82.102.141.193	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.66	China	147.237.76.197	e.himush.idf.il	ET SCAN NMAP -sS window 1024	2
46.19.86.155	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.176.39.137	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
185.22.34.126	Lebanon	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
109.253.144.70	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.66	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	2
109.65.147.152	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
149.88.112.199	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
113.200.251.8	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.67	China	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 1024	2
109.253.136.162	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
81.218.118.124	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
84.109.39.14	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
50.18.225.195	United States	147.237.77.216	dover.idf.il	ET WEB_SERVER PyCurl Suspicious User Agent Inbound	2
79.180.99.57	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.64.80.207	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.179.139.225	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.190.87.102	France	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
109.64.6.100	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
37.142.201.228	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.177.190.78	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
80.74.117.138	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
85.65.44.59	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.19.86.165	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.182.59.221	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.228.69.97	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.65.201.197	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
5.29.16.221	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
91.82.220.18	Hungary	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
46.19.86.146	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
89.248.162.228	Netherlands	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
109.253.143.248	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.109.185.165	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
62.90.110.105	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.253.141.232	Israel	147.237.0.19	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
84.109.165.124	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
149.78.164.113	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
89.248.162.228	Netherlands	147.237.76.42	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	2

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
62.207.60.228	Netherlands	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	955
153.31.113.20	United States	147.237.76.42	refuah.idf.il	First packet isn't SYN	drop	drop	817
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	422
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	366
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	324
66.249.79.57	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	218
66.249.79.65	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	184
66.249.79.73	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	162
77.126.157.82	Israel	147.237.72.156	aman.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	104
146.185.56.110	Israel	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	93
31.168.197.215	Israel	147.237.72.156	aman.idf.il	Invalid sequence number	Bad TCP sequence	monitor	88
82.81.163.138	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	78
38.111.147.86	United States	147.237.77.216	dover.idf.il		drop	drop	74
212.143.186.38	Israel	147.237.76.86	navy.idf.il	'Proxy-Authorization' header length exceeded maximum allowed length	HTTP Format Sizes	monitor	72
31.210.187.69	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	monitor	72
193.43.246.250	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	72
134.191.232.70	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	70
5.29.174.28	Israel	147.237.72.166	aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	62
90.164.55.32	Spain	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	58
66.249.93.152	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	58
212.143.23.84	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	58
213.8.96.180	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	54
81.218.77.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	54
158.169.150.10	Belgium	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	50
31.46.245.252	Hungary	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	50
66.249.81.200	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	50
80.179.18.228	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	49
132.76.50.5	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	48
85.159.214.117	United Kingdom	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	44
66.249.93.155	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	44
64.22.71.223	United States	147.237.77.216	dover.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	43
66.249.64.141	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	40
212.179.140.133	Israel	147.237.76.86	navy.idf.il	'Proxy-Authorization' header length exceeded maximum allowed length	HTTP Format Sizes	monitor	40
62.219.118.16	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
157.55.39.1	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
188.120.148.124	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	37
89.122.43.66	Romania	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	37
46.19.85.130	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
82.56.181.245	Italy	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
172.16.25.193		147.237.72.167	ishurim.aka.idf.il	First packet isn't SYN	drop	drop	36
185.37.160.65	Iraq	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
5.28.184.163	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
66.249.64.149	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
31.168.126.163	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	33
46.19.85.60	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	33
212.143.120.175	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
31.210.187.69	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	alert	32
70.60.126.82	United States	147.237.77.176	matpash.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	30
5.22.129.193	Israel	147.237.72.156	aman.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	30
168.235.195.102		147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	30

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.64.6.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	676
37.26.147.149	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.147.149	Block	392
109.253.142.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	358
87.68.129.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	322
2.54.140.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	299
46.19.86.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	279
109.253.147.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	252
109.253.141.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	237
80.246.140.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	230
79.178.141.13	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 79.178.141.13	Block	196
2.54.165.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	189
176.12.136.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	180
109.253.139.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	164
185.32.178.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	150
46.19.86.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	141
46.19.86.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	126
109.253.158.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	122
79.176.22.155	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/priv.dog.settings/getstatistics	Block	110
46.19.86.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	96
213.57.232.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	95
109.253.157.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	88
37.26.147.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	86
64.22.71.223	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 64.22.71.223	Block	85
212.25.102.57	Israel	147.237.77.226	www.chamatz.aka.idf.il	Too Many of the Same Response Code (404) in Session from 212.25.102.57	Block	82
66.249.78.173	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	72
66.249.78.159	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	67
109.64.6.234	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.64.6.234	Block	58
185.32.178.154	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 185.32.178.154	Block	55
66.249.78.166	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	52
37.26.147.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	46
109.65.66.222	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.65.66.222	Block	45
217.12.204.117	Ukraine	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 217.12.204.117	Block	45
79.178.141.13	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Abnormally Long Request from 79.178.141.13	Block	44
217.12.204.117	Ukraine	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 217.12.204.117	Block	40
217.12.204.117	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 217.12.204.117	Block	40
217.12.204.117	Ukraine	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 217.12.204.117	Block	36
217.12.204.117	Ukraine	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 217.12.204.117	Block	35
109.253.156.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	35
95.86.109.110	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	34
91.214.98.33	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	34
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	27
62.90.117.133	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 62.90.117.133	Block	27
217.12.204.117	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 217.12.204.117	Block	24
79.176.179.242	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigato n.asp	Block	23
46.19.86.239	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.239	Block	23
82.102.141.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	22
77.126.135.237	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 77.126.135.237	Block	16
31.168.187.203	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	16
217.12.204.117	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 217.12.204.117	Block	15
2.54.190.189	Israel	147.237.76.39	mobile.meitav.idf.il	Distributed Cookie Tampering on token: .ASPNETAUTH	None	15