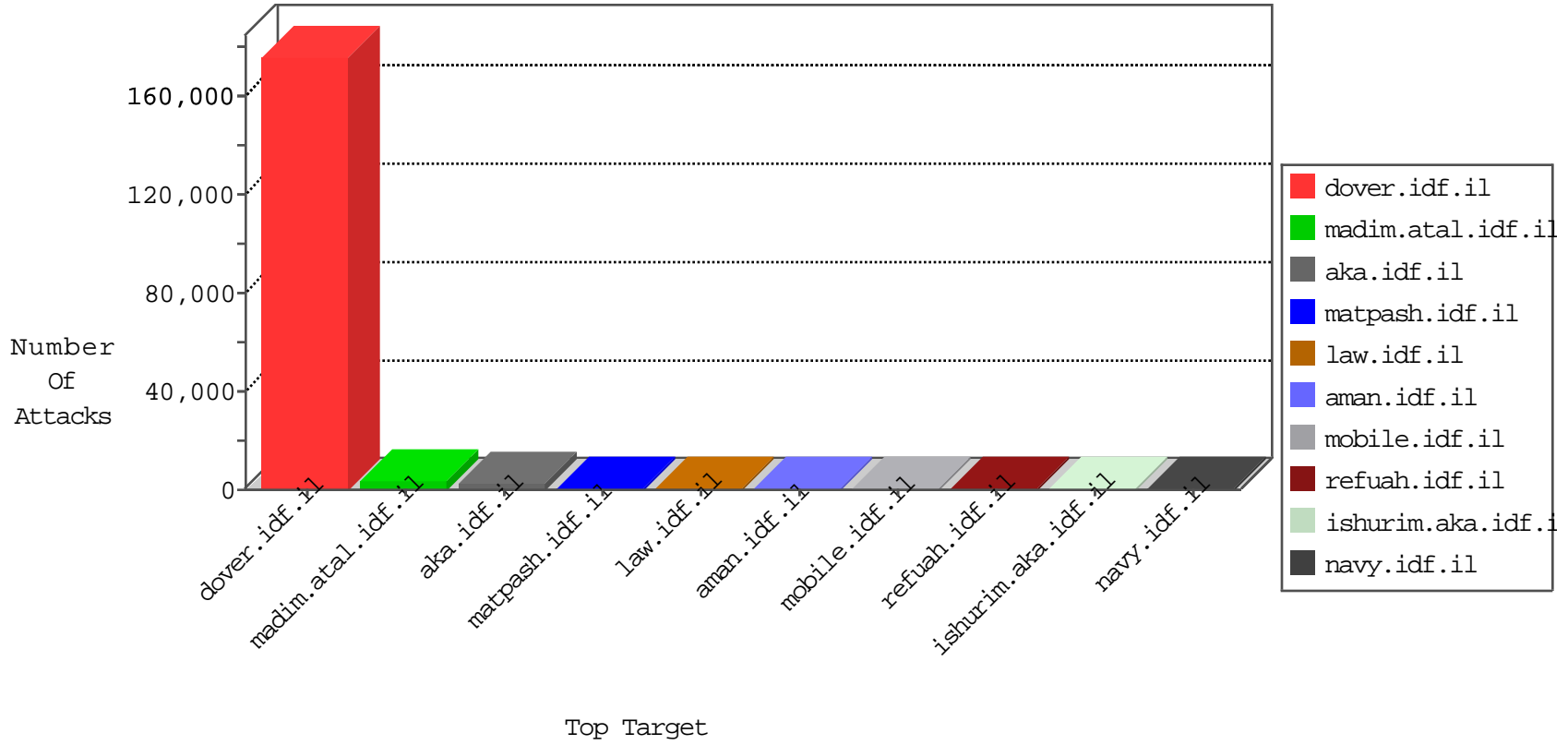


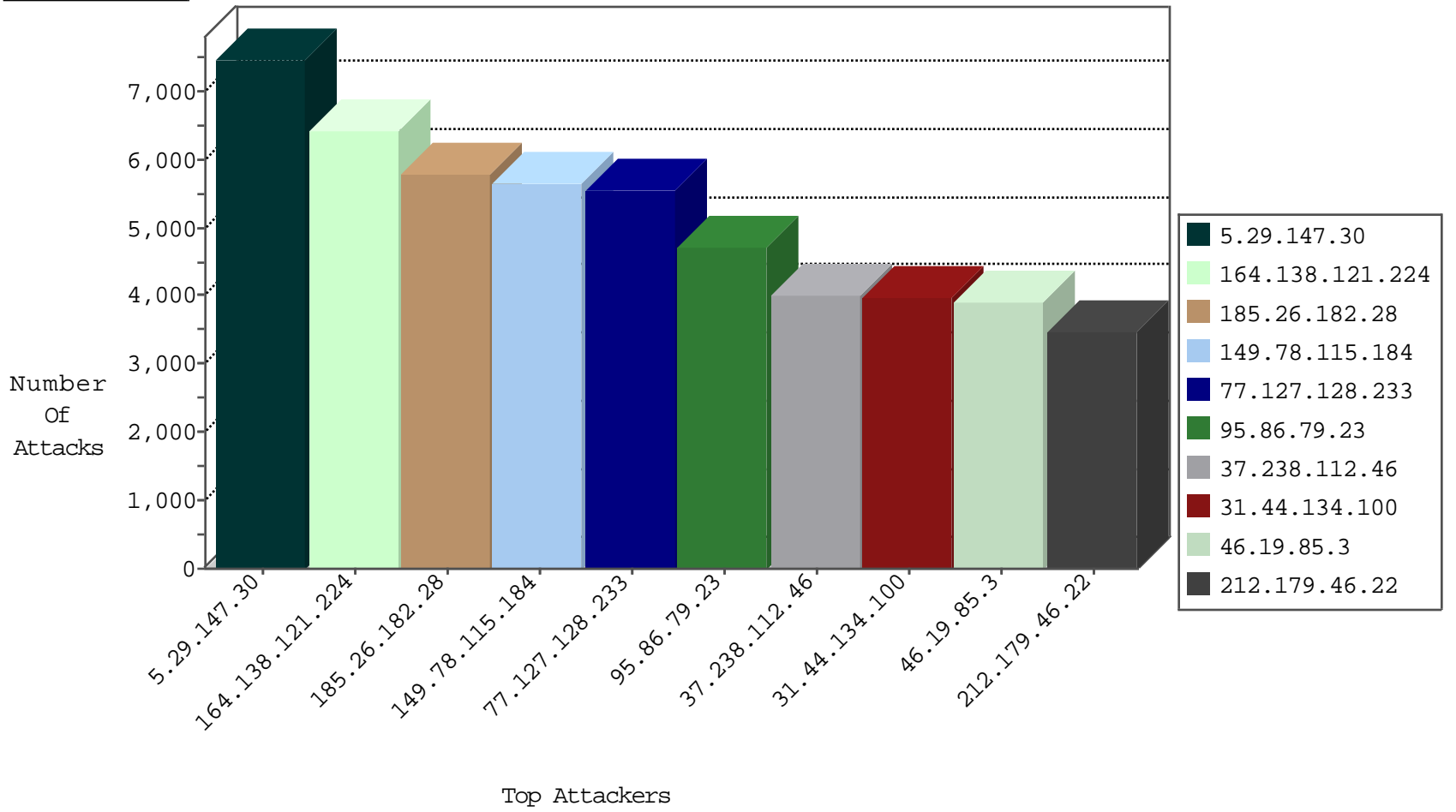
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
109.65.6.62	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6756
107.1.99.189	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6619
66.249.64.24	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	4952
66.249.64.21	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3768
66.249.64.29	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3029
79.180.9.114	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1521
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1428
66.249.78.89	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1142
66.249.64.156	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1031
87.68.43.224	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	842
84.228.223.80	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	747
109.64.165.32	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	704
220.181.108.110	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	679
220.181.108.90	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	642
79.176.12.242	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	632
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	617
96.250.86.58	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	608
84.228.87.182	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	527
79.178.176.137	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	490
79.177.177.207	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	484
77.127.147.66	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	464
46.19.86.245	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	388
220.181.108.143	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	374
220.181.108.175	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	347
79.177.208.79	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	326
79.181.13.235	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	255
84.228.170.195	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	246
84.94.167.123	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	221
212.199.218.50	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	221
212.126.101.178	Iraq	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	211
149.88.78.54	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	201
220.181.108.87	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	186
109.65.52.11	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	180
220.181.108.140	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	176
220.181.108.97	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	170
220.181.108.139	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	168
220.181.108.80	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	160
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	151
37.142.2.191	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	150
37.142.100.130	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	127
176.12.144.249	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	121
85.250.181.88	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	120
109.67.38.10	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	120
109.64.147.25	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	117
192.115.116.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	108
2.54.47.97	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	107
83.130.117.225	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	106
66.249.78.159	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	101
46.19.85.227	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	96
79.176.201.177	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	95

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	259
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	128
37.59.19.32	France	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	123
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	78
37.130.227.133	United Kingdom	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	35
50.63.138.53	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	30
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	20
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	20
89.139.182.255	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	12
105.51.213.101	Kenya	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	11
89.139.166.243	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	10
192.116.102.75	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	9
46.118.157.21	Ukraine	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	8
71.6.135.131	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	8
37.142.172.85	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
5.79.68.161	Netherlands	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	6
37.142.197.138	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
66.240.192.138	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	5
5.102.232.177	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
104.172.178.80		147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
46.116.118.217	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
96.44.189.102	United States	147.237.77.216	dover.idf.il	EgovRep_B-N_70-99	Block	5
66.240.192.138	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	5
46.117.178.197	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.167.142	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	5
46.120.101.210	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
79.180.121.39	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
46.19.85.91	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.135.131	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	5
71.6.167.142	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	5
82.166.20.109	Israel	147.237.77.216	dover.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	4
71.6.135.131	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	4
66.240.192.138	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	4
66.240.192.138	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	4
66.240.192.138	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	4
198.20.69.98	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	4
222.84.7.43	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
71.6.135.131	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	4
66.240.192.138	United States	147.237.77.212	e.dover.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
71.6.165.200	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	4
80.179.97.34	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
66.240.192.138	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	4
46.19.85.11	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4

Top Attackers In IDF

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	259
191.190.108.145	Brazil	147.237.77.74	law.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	12
191.190.108.145	Brazil	147.237.77.176	matpash.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	6
191.190.108.145	Brazil	147.237.76.42	refuah.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	6
79.181.162.85	Israel	147.237.76.30	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	6
191.190.108.145	Brazil	147.237.77.216	dover.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	6
66.249.64.161	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
105.158.149.5	Morocco	147.237.77.216	dover.idf.il	SERVER-WEBAPP Mambo upload.php access	4
66.249.64.34	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
66.249.78.159	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	4
66.249.78.137	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	4
66.249.78.96	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
183.136.216.4	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	3
61.240.144.65	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	3
183.136.216.4	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	3
183.136.216.4	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	3
46.117.26.50	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
212.179.42.242	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.22	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
149.88.109.250	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.65.115.202	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.66	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	2
79.178.54.178	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
221.235.189.245	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
62.32.27.225	Switzerland	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 1024	2
193.107.16.206	Russian Federation	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	2
149.78.115.19	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.116.75.245	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
77.127.23.28	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
192.117.173.247	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
132.70.66.10	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
221.235.189.244	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.133	Japan	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	2
5.29.28.165	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
50.63.138.53	United States	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
221.235.189.244	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2
2.54.151.138	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.64.26	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.67	China	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	2
93.172.216.2	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.93.238	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.64	China	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 1024	2
85.64.145.114	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.67	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	2
183.136.216.4	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	2
66.249.84.146	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
221.235.189.244	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	2
84.111.5.122	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
91.224.132.118	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.64	China	147.237.0.15	kosher-kravi.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
5.29.147.30	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7484
164.138.121.224	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6418
185.26.182.28	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5797
149.78.115.184	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5657
77.127.128.233	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5557
95.86.79.23	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4728
31.44.134.100	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3966
37.238.112.46	Iraq	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3956
46.19.85.3	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3930
212.179.46.22	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3476
109.160.199.235	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3262
31.168.73.15	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3257
84.228.137.98	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2882
212.126.101.178	Iraq	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2249
2.54.129.50	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2110
46.19.85.13	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1889
212.76.105.98	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1795
85.65.60.59	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1762
89.139.172.235	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1530
37.142.175.10	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1438
2.52.182.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1435
89.139.182.255	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1395
93.172.76.65	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1271
84.110.216.145	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1199
46.19.85.253	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1151
109.65.114.21	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1116
46.117.17.122	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1092
46.19.86.191	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1017
109.67.11.68	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1015
50.118.172.70	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	938
95.86.78.43	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	861
84.108.246.116	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	837
109.186.11.30	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	829
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	803
2.54.186.105	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	800
79.183.190.86	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	778
87.68.29.223	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	770
46.116.151.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	724
2.54.55.236	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	665
79.179.184.74	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	663
109.64.32.188	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	647
82.145.221.157	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	620
2.52.186.202	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	585
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	565
80.179.188.98	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	562
66.249.93.160	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	556
46.116.38.248	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	554
83.24.121.131	Poland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	553
79.182.175.240	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	552
213.151.63.109	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	538

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
85.65.57.61	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 85.65.57.61	Block	996
93.172.137.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	717
2.54.158.158	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.158.158	Block	396
79.181.120.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	189
109.67.161.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	177
217.132.251.22	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	166
176.12.150.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	151
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	105
2.54.54.24	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	95
46.121.45.7	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	69
109.67.161.9	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.67.161.9	Block	67
46.121.17.127	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	48
176.12.147.69	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	45
109.253.141.120	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	30
176.12.147.227	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	22
109.253.132.66	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	17
109.253.158.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	15
77.125.87.96	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 77.125.87.96	Block	14
176.12.151.179	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
109.186.55.67	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	13
43.249.81.65	Japan	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 43.249.81.65	Block	12
87.68.33.199	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	12
176.12.149.157	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	11
109.253.145.206	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	11
109.253.142.75	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	10
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	10
207.46.13.42	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
213.151.32.163	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	10
2.54.176.21	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	9
109.253.131.98	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	9
2.54.44.117	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	9
46.117.254.166	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	9
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	8
176.12.140.229	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	8
157.55.39.201	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
77.126.43.72	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 77.126.43.72	Block	8
176.12.149.246	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	8
46.116.47.172	Israel	147.237.0.16	my-kosher-kravi.idf.il	Multiple MSSQL Data Retrieval with Implicit Conversion Errors(+) from 46.116.47.172	None	8
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	7
84.228.136.135	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
46.116.47.172	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 46.116.47.172	None	7
84.108.155.24	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
54.174.57.181	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 54.174.57.181	Block	7
37.26.146.247	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	7
176.12.151.55	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	7
77.127.227.4	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
109.253.136.42	Israel	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	7
46.19.85.8	Israel	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	6
77.125.155.181	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	6