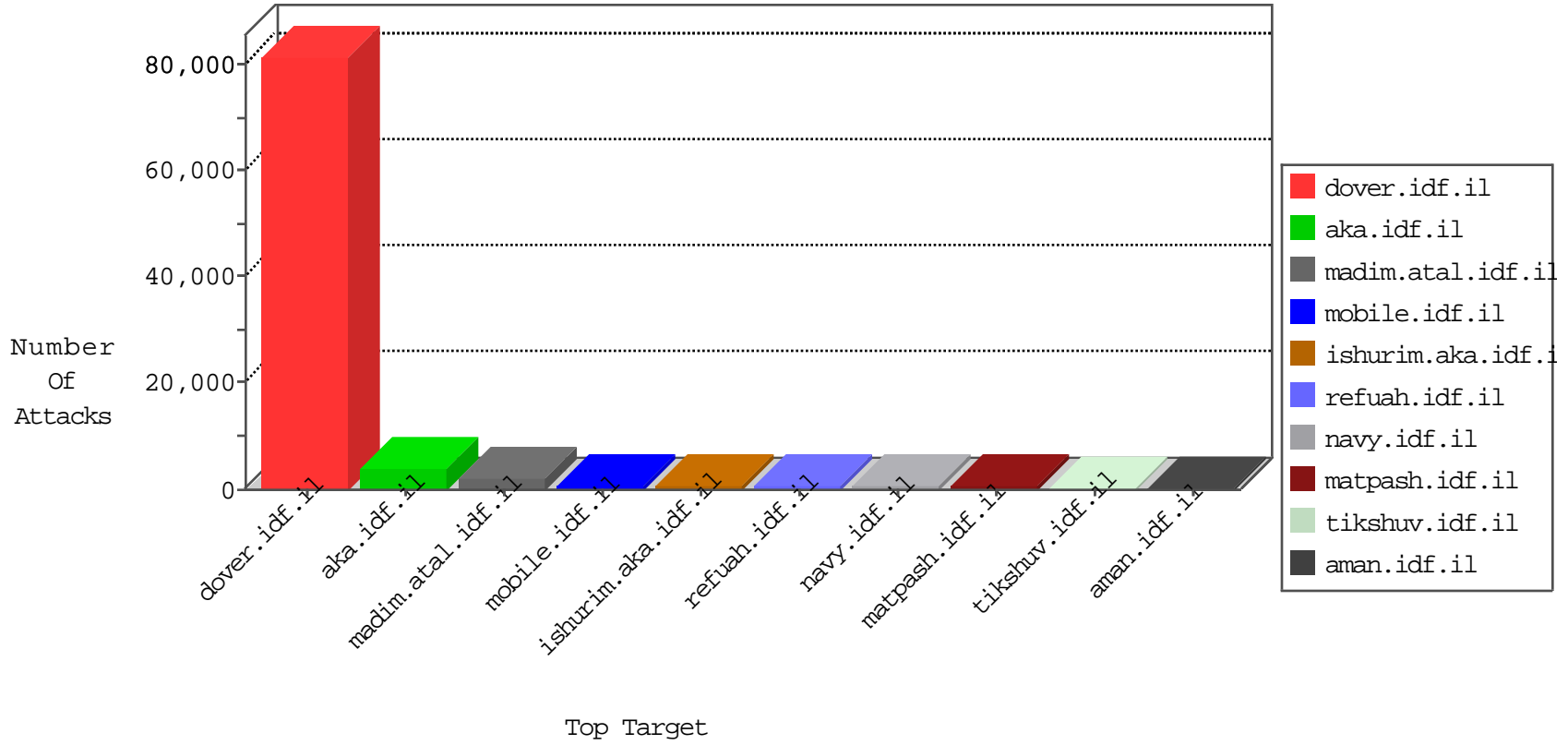


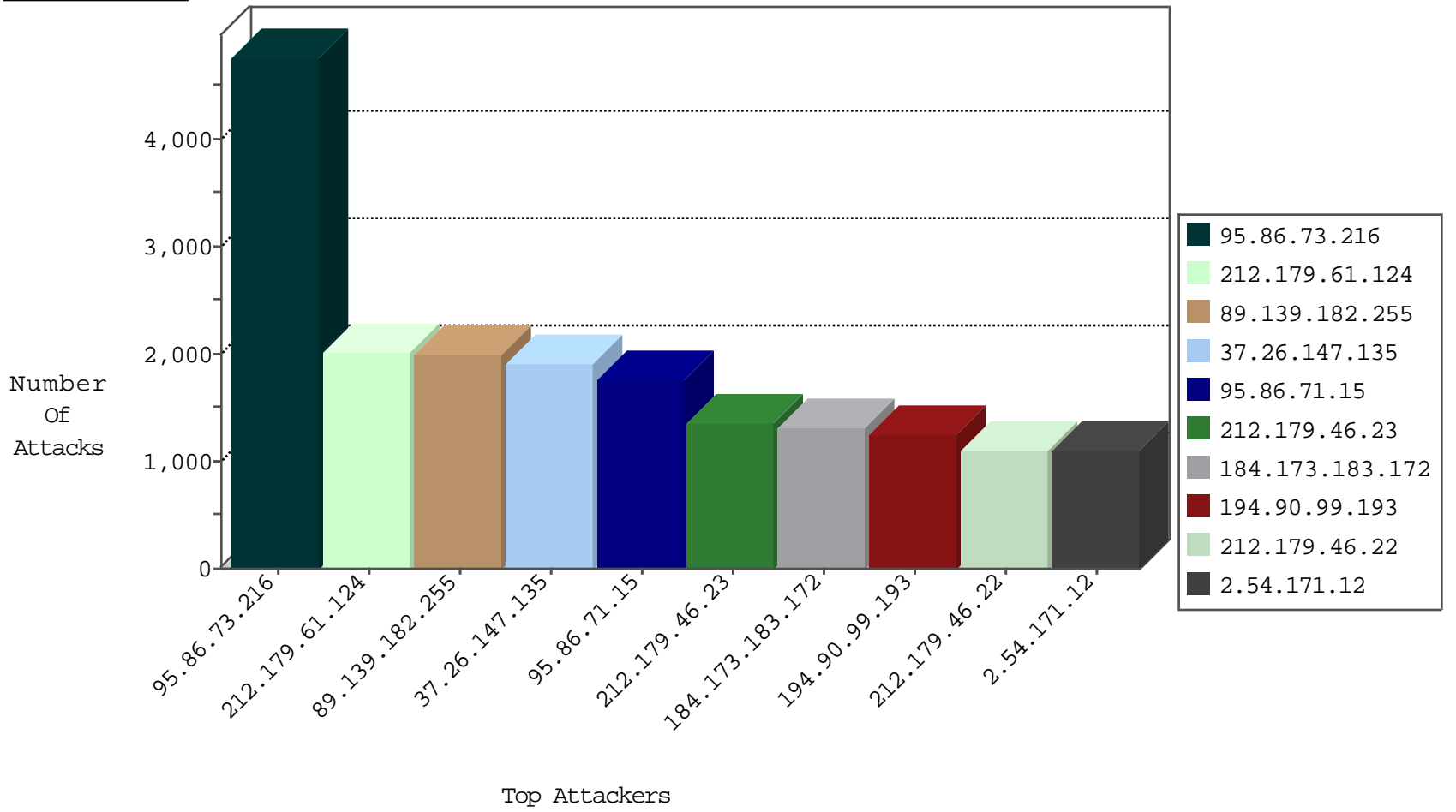
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	4543
66.249.78.15	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3496
220.181.108.101	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	3026
220.181.108.77	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	2695
192.115.116.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	708
212.143.110.33	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	469
220.181.108.81	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	460
109.64.128.69	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	443
5.28.190.27	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	416
84.228.138.164	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	404
5.28.181.20	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	390
149.78.252.193	United States	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	384
220.181.108.105	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	306
79.176.203.188	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	304
212.179.61.120	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	298
66.249.78.166	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	298
80.246.137.216	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	261
77.126.0.50	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	254
82.166.20.161	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	244
89.139.6.137	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	210
109.64.147.25	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	201
37.26.147.138	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	195
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	186
5.29.110.236	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	185
87.69.234.189	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	171
89.139.17.188	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	164
220.181.108.161	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	163
79.179.55.49	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	162
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	160
46.120.92.249	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	160
220.181.108.88	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	155
109.253.130.50	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	150
84.94.36.92	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	147
220.181.108.82	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	145
79.177.24.49	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	135
66.87.117.61	United States	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	forward	134
134.191.232.69	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	129
192.115.116.25	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	127
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	117
84.108.104.187	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	115
79.181.182.63	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	108
2.54.165.96	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	108
109.67.14.142	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	108
212.179.46.21	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	104
95.86.78.16	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	103
46.120.158.23	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	103
79.176.19.189	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	102
212.179.61.124	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	102
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	101
5.29.95.143	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	100

## 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	553
184.173.183.172	United States	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	325
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	187
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	167
184.173.183.172	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_P-N_40-59	Permit	129
184.173.183.172	United States	147.237.0.34	tikshuv.idf.il	DVRep_P-N_40-59	Permit	125
89.139.182.255	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	47
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	20
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	20
52.28.2.176	United States	147.237.72.166	aka.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	12
52.28.2.176	United States	147.237.72.166	aka.idf.il	13375: HTTP: Joomla Component JCE BOT for JCE	Block	12
58.59.235.176	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	9
46.116.140.48	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	9
79.180.123.75	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	9
5.29.29.83	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
185.33.168.150	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	EgovRep_B-N_70-99	Block	7
62.90.255.56	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
79.181.212.246	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	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	6
84.229.34.77	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
50.144.0.19	United States	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
71.6.135.131	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	6
66.240.192.138	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	6
79.179.22.203	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
71.6.165.200	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	6
37.26.148.153	Israel	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	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	5
81.218.144.203	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	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	5
93.172.140.77	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
66.240.192.138	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	5
109.186.162.78	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.135.131	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	5
77.127.205.84	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
109.186.162.78	Israel	147.237.77.234	halag.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
58.59.235.176	China	147.237.72.167	ishurim.aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
71.6.165.200	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	4
213.8.130.50	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
71.6.135.131	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	4
31.154.253.238	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
71.6.135.131	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	4
81.218.48.37	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	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	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	4

## Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	102
109.67.111.99	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	36
66.249.67.54	United States	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sA (2)	12
78.176.99.236	Turkey	147.237.77.216	dover.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	6
78.176.99.236	Turkey	147.237.76.42	refuah.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	6
78.176.99.236	Turkey	147.237.77.176	matpash.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	6
78.176.99.236	Turkey	147.237.72.166	aka.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	6
66.249.75.44	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	5
89.139.182.255	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	4
149.78.134.249	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
62.48.187.49	Portugal	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.79.190	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
109.66.102.101	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
79.177.113.185	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	3
77.127.134.224	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.66	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential VNC Scan 5800-5820	2
109.66.17.10	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.109.89.92	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.29	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.65	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	2
89.138.243.111	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.178.2.191	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.183.128.6	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	2
61.183.128.6	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential -sS window 1024	2
202.162.78.118	Thailand	147.237.77.235	sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
176.67.114.241	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	http_inspect: MULTIPLE HOST HEADERS DETECTED	2
183.136.216.4	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.64	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	2
221.235.189.244	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.135	Japan	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	2
85.65.176.254	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	ET SCAN NMAP -sA (2)	2
176.12.148.240	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
202.162.78.118	Thailand	147.237.0.19	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
61.240.144.66	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	2
46.19.85.11	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
85.64.6.85	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
94.159.189.11	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
85.250.93.5	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
183.136.216.3	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	2
221.235.189.244	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	2
66.249.79.139	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
61.149.161.186	China	147.237.0.200	m4u.idf.il	GPL SCAN nmap TCP	2
66.249.78.173	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.65	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	2
219.153.48.146	China	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	2
198.23.192.34	United States	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.135	Japan	147.237.76.176	test.noore.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.130	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
79.179.18.159	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
95.86.73.216	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4761
212.179.61.124	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1989
89.139.182.255	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1920
37.26.147.135	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1909
95.86.71.15	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1749
212.179.46.23	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1301
194.90.99.193	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1250
2.54.171.12	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1101
84.110.109.251	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1076
212.179.46.22	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1055
66.87.117.61	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	946
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	890
168.235.196.134		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	614
37.142.147.25	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	583
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	576
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	528
85.250.91.71	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	521
81.218.251.252	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	509
93.91.80.7	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	495
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	456
95.35.10.73	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	454
217.249.42.199	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	434
132.66.40.116	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	431
212.179.61.120	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	423
94.188.132.2	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	421
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	366
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	364
46.19.85.148	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	346
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	346
95.86.120.161	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	344
212.179.21.196	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	340
2.54.61.20	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	339
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	331
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	326
212.25.102.63	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	317
2.54.35.11	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	315
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	301
195.34.150.18	Austria	147.237.77.216	dover.idf.i	SAM rule	drop	drop	284
84.108.148.162	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	280
62.128.48.130	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	266
213.204.103.36	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	251
93.173.28.39	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	251
212.179.46.21	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	239
212.179.61.122	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	221
207.46.13.136	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	220
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	204
81.218.40.194	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	199
81.218.251.250	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	196
69.157.9.43	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	193
66.249.78.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	186

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
79.179.190.159	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 79.179.190.159	Block	794
109.253.144.212	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.144.212	Block	328
176.12.139.36	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.139.36	Block	208
46.19.86.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	176
2.54.129.181	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.129.181	Block	159
62.219.164.51	Israel	147.237.72.167	ishurim.aka.idf.il	Too Many of the Same Response Code (404) in Session from 62.219.164.51	Block	115
2.54.13.76	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.13.76	Block	104
46.19.86.211	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	83
5.102.199.103	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 5.102.199.103	Block	83
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	59
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	55
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	53
2.52.176.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	53
176.12.144.99	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	53
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	50
109.65.58.203	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	46
176.12.151.183	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	45
2.54.10.183	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.10.183	Block	42
46.19.86.175	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.175	Block	39
66.249.78.197	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.78.197	Block	37
46.121.17.127	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	34
2.54.32.238	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	32
37.26.147.217	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	30
46.19.85.217	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	28
66.249.78.190	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.78.190	Block	28
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.78.204	Block	26
176.12.139.74	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	26
195.160.240.11	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	25
95.86.71.238	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	25
5.29.83.134	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (404) in Session from 5.29.83.134	Block	23
176.12.146.130	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	22
212.179.61.124	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	21
2.52.175.91	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	19
95.86.109.136	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	19
46.19.85.155	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	19
46.121.197.112	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (404) in Session from 46.121.197.112	Block	18
176.12.150.176	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	17
199.203.111.183	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	17
46.19.86.18	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	16
46.19.85.213	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	16
176.12.139.102	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	16
109.253.147.38	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	15
109.253.157.155	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
176.12.144.204	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
80.246.136.139	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
183.60.243.190	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 183.60.243.190	Block	14
109.253.137.236	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
2.54.36.142	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	13
2.54.133.208	Israel	147.237.72.166	aka.idf.il	Distributed Unknown HTTP Request Method	Block	13
85.130.208.225	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	12