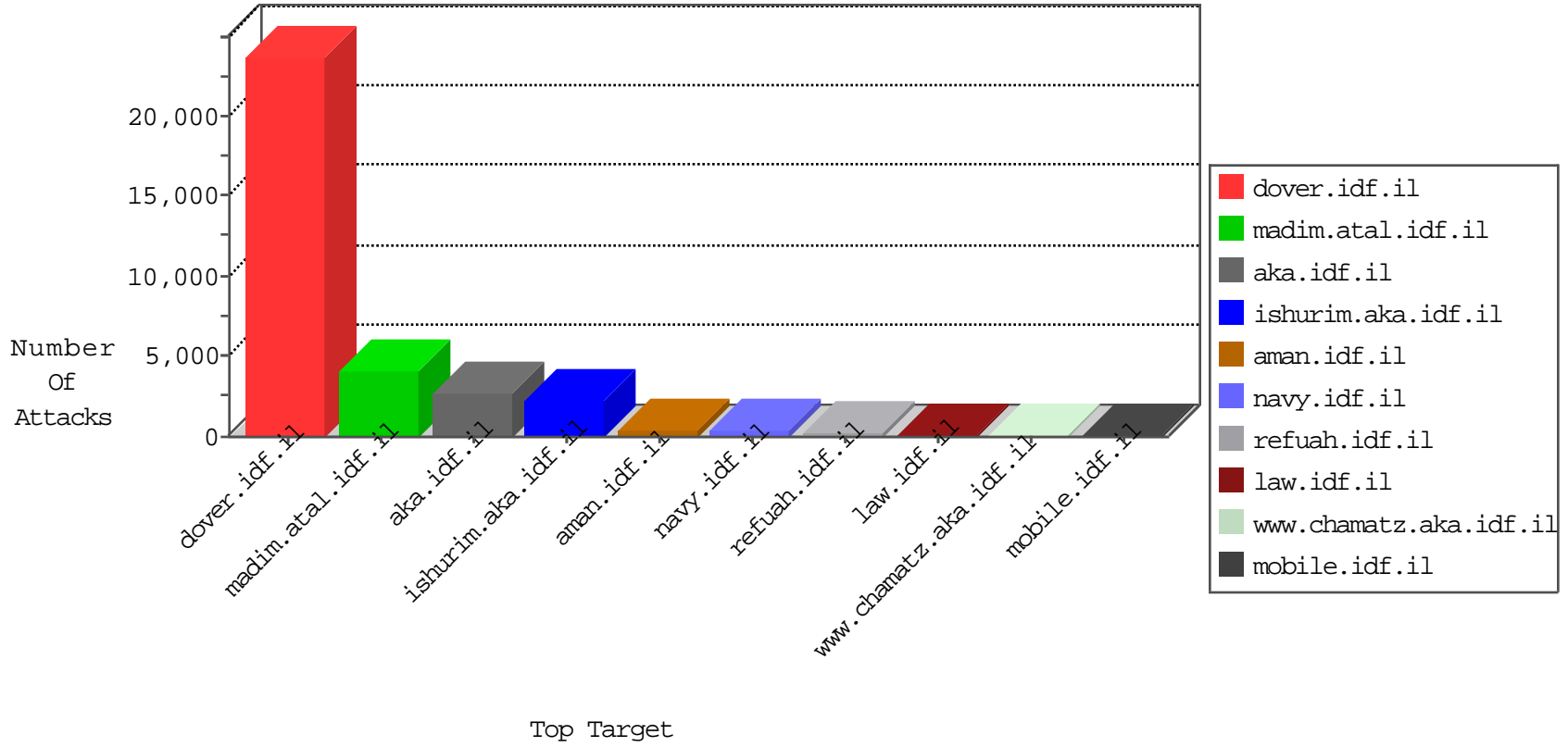


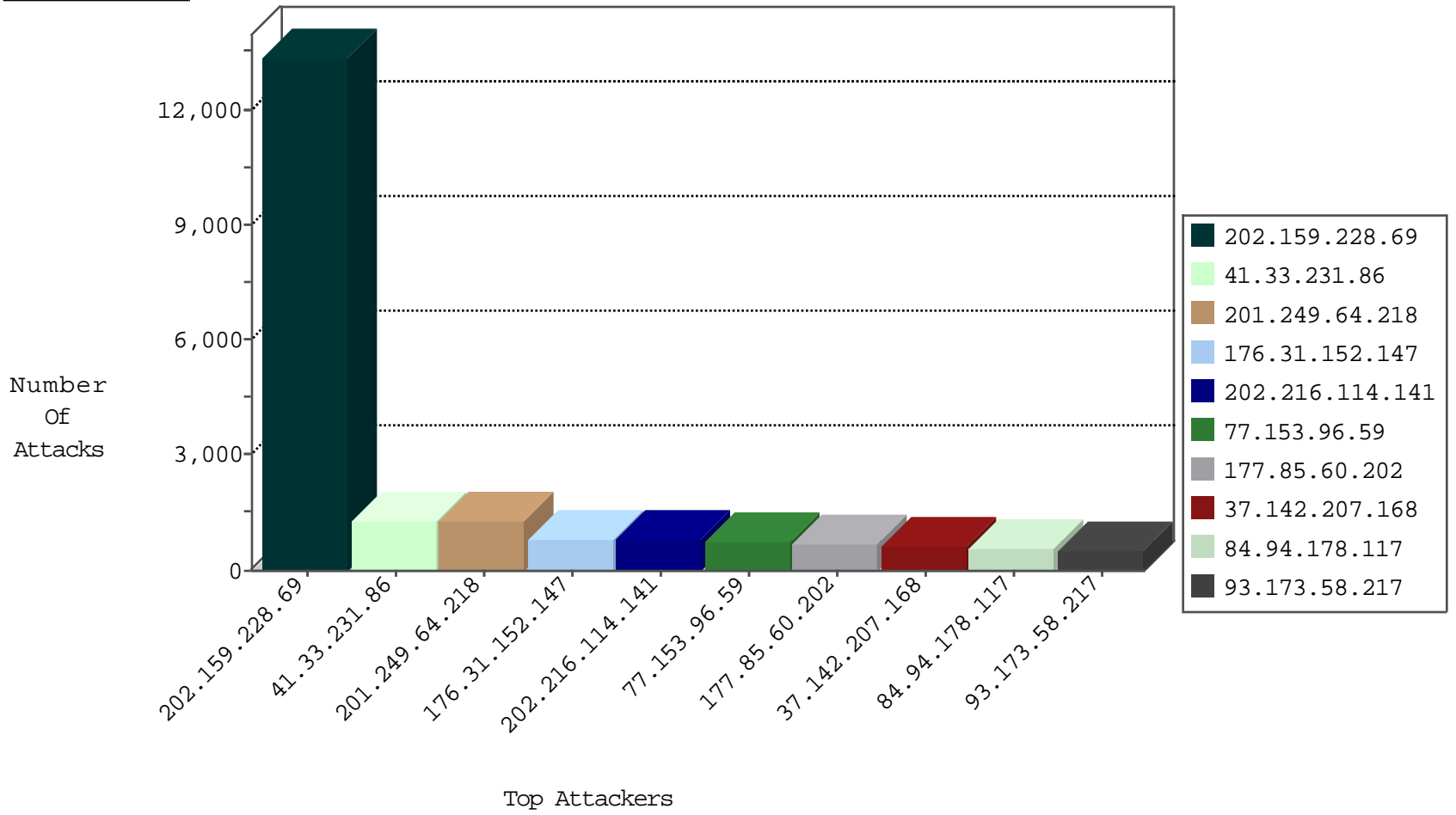
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
88.172.148.225	France	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	12556
180.253.77.180	Indonesia	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	2717
37.142.173.20	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	2609
202.159.228.69	India	147.237.77.216	dover.idf.il	Frk_Purple_Con_Limit_Http	drop	1995
202.159.228.69	India	147.237.77.216	dover.idf.il	Frk_Purple_Con_Limit_Tcp	drop	1357
37.236.224.43	Iraq	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	844
79.178.142.113	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	748
37.142.207.168	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-SSL-renegotiation-Cli	forward	715
84.111.158.229	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	556
5.102.197.218	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	334
37.142.207.168	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	193
149.78.209.164	United States	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	189
84.229.1.129	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	159
212.117.143.29	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	130
149.78.209.164	United States	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	forward	120
87.68.71.75	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	115
37.26.147.225	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-SSL-renegotiation-Cli	forward	113
37.26.147.225	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	112
149.78.254.138	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	111
80.246.141.27	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	109
80.246.141.27	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	forward	100
89.138.79.137	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	98
2.54.18.88	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	forward	98
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	94
84.229.237.134	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	92
87.69.173.238	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	89
46.19.85.195	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	87
85.65.52.121	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	84
84.228.177.166	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	79
85.64.9.203	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	79
46.19.85.246	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	79
37.26.148.204	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	78
81.218.205.165	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	77
2.54.18.88	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	74
2.54.190.112	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	73
46.121.244.2	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	72
2.54.147.99	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	72
109.66.158.86	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
84.229.174.34	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	69
79.176.18.8	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	69
213.57.182.179	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	65
109.64.196.102	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	63
2.54.147.99	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	forward	56
46.19.86.243	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	forward	52
109.65.131.170	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	forward	44
46.19.85.246	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-SSL-renegotiation-Cli	forward	32
46.19.85.90	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	forward	28
82.145.209.134	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	24
46.117.160.26	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	forward	22
109.253.147.7	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-SSL-renegotiation-Cli	forward	22

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.65.31.209	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
218.77.79.43	China	147.237.76.177	ncore.idf.il	Block_Level_70_100	Block	6
218.77.79.43	China	147.237.76.86	navy.idf.il	Block_Level_70_100	Block	6
208.92.211.54	United States	147.237.76.31	nakchal.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	6
218.77.79.43	China	147.237.76.201	e.atal.idf.il	Block_Level_70_100	Block	6
218.77.79.43	China	147.237.76.39	mobile.meitav.idf.il	Block_Level_70_100	Block	6
218.77.79.43	China	147.237.76.176	test.ncore.idf.il	Block_Level_70_100	Block	6
208.92.211.14	United States	147.237.72.166	aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	6
218.77.79.43	China	147.237.76.44	e.refuah.idf.il	Block_Level_70_100	Block	5
218.77.79.43	China	147.237.76.34	yochalan.idf.il	Block_Level_70_100	Block	5
218.77.79.43	China	147.237.76.200	eitan.aka.idf.il	Block_Level_70_100	Block	5
218.77.79.43	China	147.237.76.196	e.sviva.idf.il	Block_Level_70_100	Block	5
218.77.79.43	China	147.237.76.38	e.e.meitav.idf.il	Block_Level_70_100	Block	5
218.77.79.43	China	147.237.77.243	mobile.idf.il	Block_Level_70_100	Block	5
218.77.79.43	China	147.237.76.147	chinuch.aka.idf.il	Block_Level_70_100	Block	5
218.77.79.43	China	147.237.76.197	e.himush.idf.il	Block_Level_70_100	Block	5
71.6.135.131	United States	147.237.76.86	navy.idf.il	Block_Level_70_100	Block	5
218.77.79.43	China	147.237.76.198	e.yochalan.idf.il	Block_Level_70_100	Block	5
218.77.79.43	China	147.237.76.42	refuah.idf.il	Block_Level_70_100	Block	5
218.77.79.43	China	147.237.76.31	nakchal.idf.il	Block_Level_70_100	Block	5
218.77.79.43	China	147.237.0.19	madim.atal.idf.il	Block_Level_70_100	Block	4
218.77.79.43	China	147.237.76.199	e.nakchal.idf.il	Block_Level_70_100	Block	4
71.6.135.131	United States	147.237.72.167	ishurim.aka.idf.il	Block_Level_70_100	Block	4
208.92.211.98	United States	147.237.77.176	matpash.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
66.240.192.138	United States	147.237.76.44	e.refuah.idf.il	Block_Level_70_100	Block	4
198.20.69.98	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Level_70_100	Block	4
218.77.79.43	China	147.237.76.148	ggcenter.aka.idf.il	Block_Level_70_100	Block	4
218.77.79.43	China	147.237.76.30	himush.idf.il	Block_Level_70_100	Block	4
198.20.69.98	United States	147.237.76.201	e.atal.idf.il	Block_Level_70_100	Block	4
71.6.135.131	United States	147.237.0.16	my-kosher-kravi.idf.il	Block_Level_70_100	Block	4
208.92.211.98	United States	147.237.72.156	anan.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
218.77.79.43	China	147.237.77.19	law-forum.idf.il	Block_Level_70_100	Block	4
218.77.79.43	China	147.237.0.200	m4u.idf.il	Block_Level_70_100	Block	4
66.240.192.138	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Level_70_100	Block	4
218.77.79.43	China	147.237.77.234	halag.idf.il	Block_Level_70_100	Block	4
66.240.236.119	United States	147.237.8.14	e.orchot.idf.il	Block_Level_70_100	Block	3
71.6.135.131	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Level_70_100	Block	3
93.120.27.62	Romania	147.237.76.38	e.e.meitav.idf.il	Block_Level_70_100	Block	3
218.77.79.43	China	147.237.77.216	dover.idf.il	Block_Level_70_100	Block	3
71.6.135.131	United States	147.237.77.227	e.hamaz.idf.il	Block_Level_70_100	Block	3
66.240.236.119	United States	147.237.77.235	sviva.idf.il	Block_Level_70_100	Block	3
198.20.69.98	United States	147.237.72.14	dover.idf.il(old)	Block_Level_70_100	Block	3
46.117.0.206	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
71.6.167.142	United States	147.237.0.15	kosher-kravi.idf.il	Block_Level_70_100	Block	3
77.125.135.118	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
71.6.135.131	United States	147.237.0.200	m4u.idf.il	Block_Level_70_100	Block	3
218.77.79.43	China	147.237.0.34	tikshuv.idf.il	Block_Level_70_100	Block	3
66.240.236.119	United States	147.237.8.27	e.madim.atal.idf.il	Block_Level_70_100	Block	3
66.240.192.138	United States	147.237.77.227	e.hamaz.idf.il	Block_Level_70_100	Block	3
84.109.50.31	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3

## Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
201.249.64.218	Venezuela	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	423
202.159.228.69	India	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	195
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	142
162.213.25.67	United States	147.237.76.86	navy.idf.il	SERVER-WEBAPP Setup.php access	74
162.213.25.67	United States	147.237.76.86	navy.idf.il	Admin login page scan - Havij	51
212.38.181.110	United Kingdom	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential VNC Scan 5900-5920	12
212.38.181.110	United Kingdom	147.237.77.235	sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	11
212.38.181.110	United Kingdom	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	10
212.38.181.110	United Kingdom	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	8
66.249.75.121	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	7
212.38.181.110	United Kingdom	147.237.77.212	e.dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	7
212.38.181.110	United Kingdom	147.237.77.234	halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	7
212.38.181.110	United Kingdom	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5900-5920	7
180.253.77.180	Indonesia	147.237.77.216	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	7
212.38.181.110	United Kingdom	147.237.72.14	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	6
212.38.181.110	United Kingdom	147.237.0.19	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	6
77.153.96.59	France	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 2 Inbound	6
212.38.181.110	United Kingdom	147.237.76.30	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	6
212.38.181.110	United Kingdom	147.237.77.178	e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	6
212.38.181.110	United Kingdom	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5900-5920	6
212.38.181.110	United Kingdom	147.237.77.233	atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	6
212.38.181.110	United Kingdom	147.237.77.205	prisha.idf.il	ET SCAN Potential VNC Scan 5900-5920	6
180.253.77.180	Indonesia	147.237.77.216	dover.idf.il	ET SCAN Potential VNC Scan 5800-5820	5
212.38.181.110	United Kingdom	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
212.38.181.110	United Kingdom	147.237.77.170	maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
177.85.60.202	Brazil	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	5
212.38.181.110	United Kingdom	147.237.76.196	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
212.38.181.110	United Kingdom	147.237.77.176	matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
212.38.181.110	United Kingdom	147.237.76.176	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
37.26.146.160	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
87.238.162.59	Belgium	147.237.77.176	matpash.idf.il	Tehila - Perl LWP with fake user agent	4
79.183.153.229	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
212.38.181.110	United Kingdom	147.237.76.86	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
212.38.181.110	United Kingdom	147.237.76.202	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
212.38.181.110	United Kingdom	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
109.186.69.79	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
149.88.100.17	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
212.38.181.110	United Kingdom	147.237.72.166	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
212.38.181.110	United Kingdom	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
212.38.181.110	United Kingdom	147.237.76.42	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
212.38.181.110	United Kingdom	147.237.76.177	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
212.38.181.110	United Kingdom	147.237.72.156	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
212.38.181.110	United Kingdom	147.237.8.14	e.orchot.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
212.38.181.110	United Kingdom	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
212.38.181.110	United Kingdom	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
212.38.181.110	United Kingdom	147.237.77.179	e.mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
202.216.114.141	Japan	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 2 Inbound	2
222.186.15.202	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	2
212.38.181.110	United Kingdom	147.237.77.121	e.navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
212.38.181.110	United Kingdom	147.237.8.28	e.mobile-ks.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
202.159.228.69	India	147.237.77.216	dover.idf.il	SAM rule	drop	drop	7557
202.159.228.69	India	147.237.77.216	dover.idf.il		drop	drop	4041
41.33.231.86	Egypt	147.237.77.216	dover.idf.il		drop	drop	1307
201.249.64.218	Venezuela	147.237.77.216	dover.idf.il		drop	drop	862
202.159.228.69	India	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	847
202.216.114.141	Japan	147.237.77.216	dover.idf.il		drop	drop	750
77.153.96.59	France	147.237.77.216	dover.idf.il		drop	drop	743
177.85.60.202	Brazil	147.237.77.216	dover.idf.il		drop	drop	702
202.159.228.69	India	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	467
41.33.232.65	Egypt	147.237.77.216	dover.idf.il		drop	drop	433
201.236.98.35	Chile	147.237.77.216	dover.idf.il		drop	drop	280
66.249.75.153	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission		210
66.249.75.153	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	210
66.249.75.137	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	175
66.249.75.137	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission		175
66.249.75.121	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission		160
66.249.75.121	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	160
41.97.55.79	Algeria	147.237.77.216	dover.idf.il		drop	drop	115
204.13.200.8	United States	147.237.77.74	law.idf.il		drop	drop	85
202.159.228.69	India	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence		73
94.230.86.42	Israel	147.237.77.226	www.chamatz.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	50
201.219.174.165	Argentina	147.237.72.166	aka.idf.il		drop	drop	50
176.31.152.147	France	147.237.77.216	dover.idf.il	illegal header format detected: Invalid HTTP End Of Line in request	Block HTTP Non Compliant	monitor	47
176.31.152.147	France	147.237.77.216	dover.idf.il		drop	drop	42
176.31.152.147	France	147.237.77.216	dover.idf.il	illegal header format detected: Malformed HTTP format in request	Block HTTP Non Compliant	monitor	40
176.31.152.147	France	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	36
81.218.183.91	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	33
202.216.114.141	Japan	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	33
46.210.237.205	Israel	147.237.77.226	www.chamatz.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	27
79.178.66.113	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	27
207.241.226.140	United States	147.237.72.166	aka.idf.il	SAM rule	drop	drop	27
79.180.54.143	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
37.26.147.209	Israel	147.237.77.216	dover.idf.il		drop	drop	24
109.67.190.219	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	24
195.34.150.18	Austria	147.237.77.216	dover.idf.il		drop	drop	23
5.102.253.150	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	23
168.235.196.128		147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	21
79.180.194.239	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
31.168.115.185	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	20
77.125.97.205	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	19
46.19.85.92	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	19
188.120.148.46	Israel	147.237.72.167	ishurim.aka.idf.il		drop	drop	19
79.182.33.42	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	18
176.31.152.147	France	147.237.77.216	dover.idf.il	illegal header format detected: Illegal status line in request	Block HTTP Non Compliant	monitor	18
79.182.188.31	Israel	147.237.77.216	dover.idf.il		drop	drop	18
79.178.50.8	Israel	147.237.72.166	aka.idf.il		drop	drop	18
80.246.130.196	Israel	147.237.76.31	nakchal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	17
2.54.4.62	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
213.55.107.141	Ethiopia	147.237.77.216	dover.idf.il		drop	drop	15
82.102.141.251	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	15

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
84.94.178.117	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 84.94.178.117	Block	538
93.173.58.217	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	527
46.19.86.191	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	314
176.12.142.122	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	275
109.253.147.7	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	264
37.142.207.168	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 37.142.207.168	Block	257
176.12.148.25	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.12.148.25	Block	251
84.111.225.206	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	248
46.19.85.246	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	172
37.26.147.225	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	167
207.241.229.192	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	160
77.126.208.149	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/resources/styles/	Block	137
176.31.152.147	France	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Method from 176.31.152.147	Block	111
109.64.196.102	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	99
176.12.151.71	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	97
176.31.152.147	France	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 176.31.152.147	Block	86
77.125.109.24	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	84
46.19.86.71	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.71	Block	84
176.31.152.147	France	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 176.31.152.147	Block	78
176.31.152.147	France	147.237.77.216	dover.idf.il	Multiple Malformed URL from 176.31.152.147	Block	73
2.54.57.240	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	69
37.142.207.28	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	63
176.31.152.147	France	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Header Name from 176.31.152.147	Block	60
176.31.152.147	France	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in URL from 176.31.152.147	Block	51
82.102.141.200	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	48
164.138.120.149	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	40
176.31.152.147	France	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 176.31.152.147	Block	31
80.246.133.139	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	30
31.44.140.43	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	29
176.31.152.147	France	147.237.77.216	dover.idf.il	Multiple Abnormally Long Header Line from 176.31.152.147	Block	29
176.31.152.147	France	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Header Value from 176.31.152.147	Block	27
198.24.146.194	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/994-8613-he/navy.aspx.aspx	Block	26
5.22.129.178	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	23
149.88.109.208	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	22
66.249.75.137	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.75.137	Block	20
176.31.152.147	France	147.237.77.216	dover.idf.il	Multiple Malformed HTTP Header Line from 176.31.152.147	Block	20
85.65.109.128	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	19
66.249.75.153	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.75.153	Block	18
198.24.146.194	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on navy.idf.il//994-8613-he/navy.aspx.aspx	Block	18
217.194.207.80	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	17
66.249.78.104	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/gyius/gyius/general.aspx	Block	15
31.44.141.12	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/gyius/controls/atuda/Å	Block	15
85.65.10.127	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	14
66.249.75.121	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.75.121	Block	14
95.86.75.225	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	14
87.68.222.211	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	14
84.110.86.229	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	13
46.19.85.103	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	13
176.31.152.147	France	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Query String from 176.31.152.147	Block	13
213.151.48.142	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	12