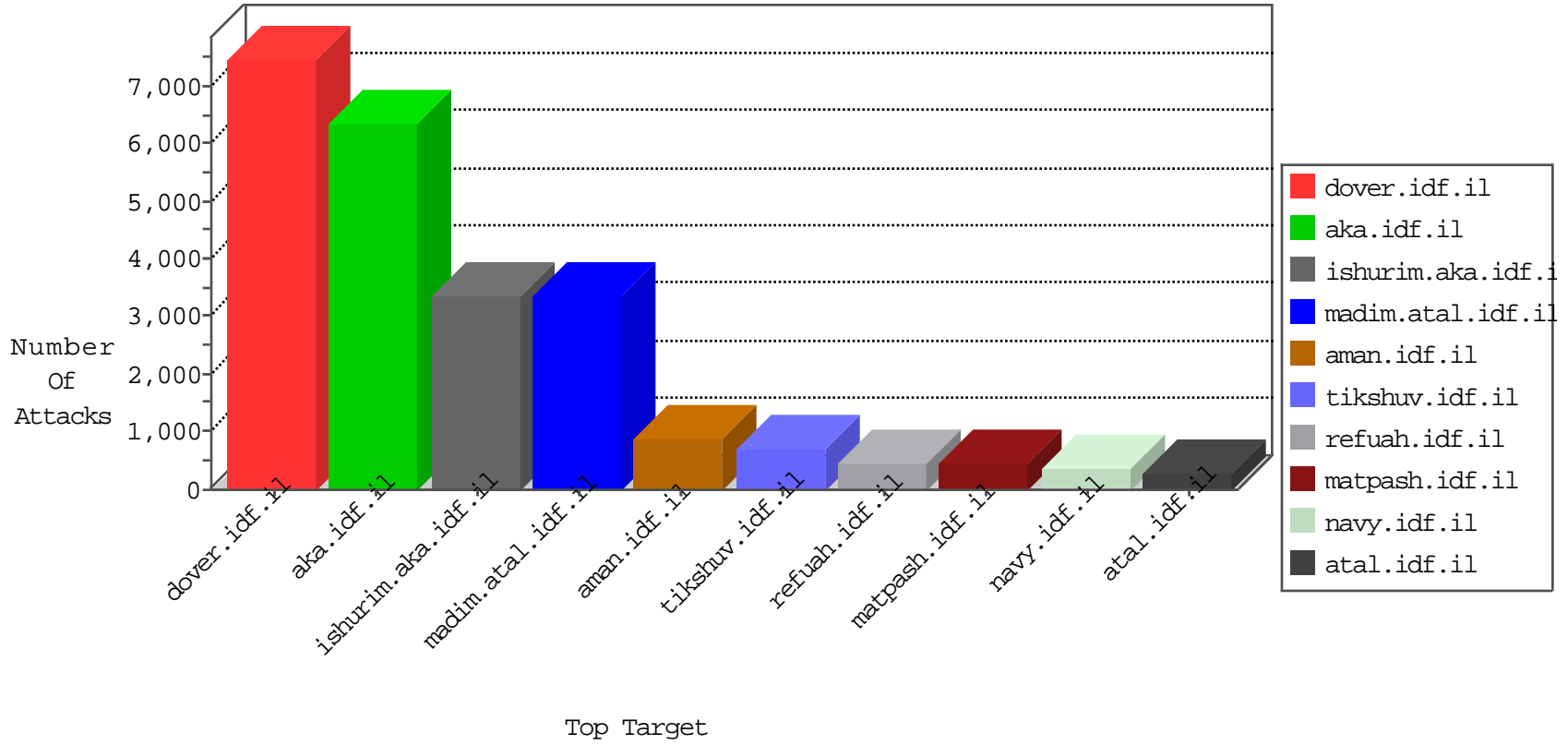


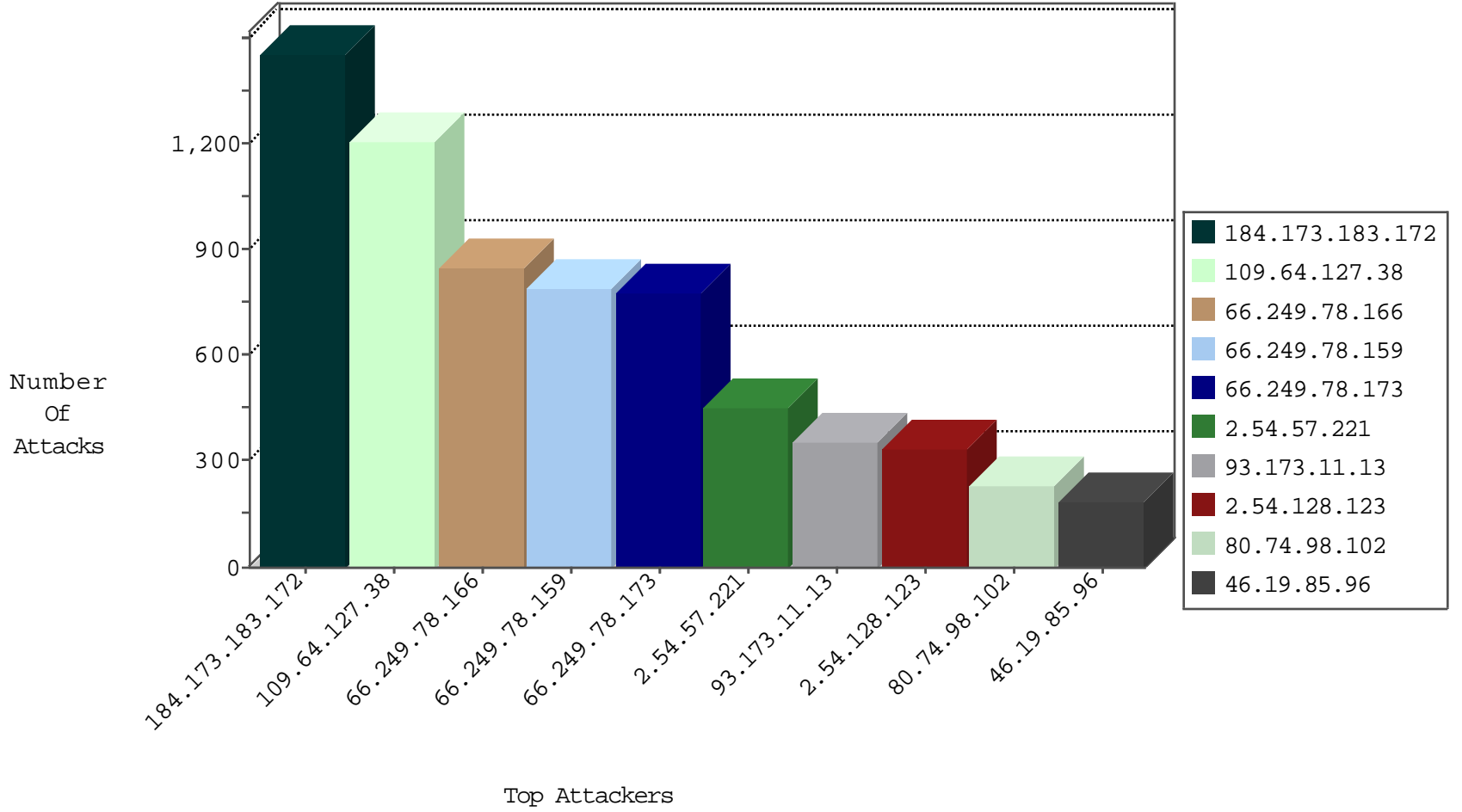
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
93.172.147.61	Israel	147.237.72.156	anan.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1349
109.186.52.176	Israel	147.237.72.156	anan.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	666
132.75.166.234	Israel	147.237.72.156	anan.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	287
37.142.55.184	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	229
46.121.94.95	Israel	147.237.72.166	aka.idf.il	HTTP-POST-Segmented-DoS	dest-reset	221
77.126.165.236	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	207
84.94.23.17	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	199
84.229.43.53	Israel	147.237.72.156	anan.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	179
81.218.188.76	Israel	147.237.72.156	anan.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	163
46.116.125.24	Israel	147.237.72.156	anan.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	153
79.180.35.9	Israel	147.237.72.156	anan.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	133
89.139.175.52	Israel	147.237.72.156	anan.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	129
89.138.205.35	Israel	147.237.72.156	anan.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	126
84.109.45.15	Israel	147.237.72.156	anan.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	78
2.54.59.135	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	76
2.54.171.172	Israel	147.237.72.156	anan.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	76
80.246.136.7	Israel	147.237.72.156	anan.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	74
89.138.252.196	Israel	147.237.72.156	anan.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	69
46.19.85.193	Israel	147.237.72.156	anan.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	68
93.172.147.61	Israel	147.237.72.156	anan.idf.il	Anomaly-TLS-renegotiation-Cli	forward	63
176.12.139.38	Israel	147.237.72.156	anan.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	61
2.54.59.135	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	43
82.102.141.210	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	38
82.102.141.200	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	36
82.102.141.220	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	22
82.102.141.223	Israel	147.237.0.34	tikshuv.idf.il	Invalid TCP Flags	drop	20
82.102.141.201	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	8
82.102.141.203	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	6
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	6
46.19.85.254	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	source-dest-reset	5
82.102.141.254	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	5
46.19.85.142	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	source-dest-reset	5
82.102.141.223	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
82.102.141.208	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
1.31.20.103	China	147.237.72.167	ishurim.aka.idf.il	Frk_Purple_Con_Limit_Http	drop	3
1.31.20.103	China	147.237.72.167	ishurim.aka.idf.il	Frk_Under_Attack_Con_Http	drop	2
222.186.34.202	China	147.237.76.202	e.halag.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
82.102.141.207	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	2
212.118.253.20	United Kingdom	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	2
221.87.170.102	Japan	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
104.192.0.20		147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
82.102.141.197	Israel	147.237.77.233	atal.idf.il	Invalid TCP Flags	drop	1
71.6.216.60	United States	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
104.192.0.20		147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
85.254.250.81	Latvia	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
82.102.141.205	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
66.240.236.119	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
82.102.141.219	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
104.192.0.20		147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
85.254.250.81	Latvia	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1

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	881
184.173.183.172	United States	147.237.0.34	tikshuv.idf.il	DVRep_P-N_40-59	Permit	229
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	180
184.173.183.172	United States	147.237.76.42	refuah.idf.il	DVRep_P-N_40-59	Permit	168
180.76.5.193	China	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	115
213.8.118.92	Israel	147.237.72.167	ishurim.aka.idf.il	DVRep_P-N_40-59	Permit	94
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	79
194.90.99.193	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	36
80.179.114.19	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	18
81.218.118.126	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	18
31.210.187.50	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
82.211.223.3	Denmark	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	10
213.8.245.58	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	8
82.166.233.182	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	8
121.54.112.182	Philippines	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
212.179.61.126	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
87.98.159.231	France	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	7
199.19.95.188	Canada	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	7
119.235.87.128	Fiji	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
190.188.15.138	Argentina	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
66.240.192.138	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	6
190.191.96.140	Argentina	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
109.201.154.178	Netherlands	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	6
109.64.109.80	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.165.200	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	5
84.94.98.111	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
178.217.187.39	Poland	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	5
212.200.34.219		147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
66.240.192.138	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	4
66.240.236.119	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	4
92.96.166.203	United Arab Emirates	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
199.203.142.65	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
82.80.196.44	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
82.102.141.216	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.228	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
213.8.245.50	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
85.25.43.94	Germany	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	4
149.78.214.12	United States	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
71.6.167.142	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	4
66.240.192.138	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	4
93.173.231.192	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
71.6.167.142	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	4
66.240.236.119	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	4
66.240.192.138	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	4

Top Attackers In IDF

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	229
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	121
213.57.56.173	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	6
109.169.45.231	United Kingdom	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
109.169.45.231	United Kingdom	147.237.76.197	e.hinush.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
109.169.45.231	United Kingdom	147.237.76.86	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
109.169.45.231	United Kingdom	147.237.77.176	matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
217.71.115.229	France	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	4
109.160.135.102	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
109.169.45.231	United Kingdom	147.237.8.14	e.orchot.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
109.169.45.231	United Kingdom	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
61.240.144.67	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	3
109.169.45.231	United Kingdom	147.237.77.178	e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
109.169.45.231	United Kingdom	147.237.77.170	maarachot.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
109.169.45.231	United Kingdom	147.237.77.243	mobile.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
109.169.45.231	United Kingdom	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
109.169.45.231	United Kingdom	147.237.76.34	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
109.169.45.231	United Kingdom	147.237.77.234	halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
109.169.45.231	United Kingdom	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
66.249.78.159	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	3
109.169.45.231	United Kingdom	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
109.169.45.231	United Kingdom	147.237.77.121	e.navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
109.169.45.231	United Kingdom	147.237.0.35	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
109.169.45.231	United Kingdom	147.237.77.61	e.cogat.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
109.169.45.231	United Kingdom	147.237.77.233	atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
2.54.181.106	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.65	China	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 1024	2
109.65.35.51	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
176.9.127.182	Germany	147.237.77.233	atal.idf.il	Tehila - Perl LWP with fake user agent	2
70.193.32.16	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
109.64.188.115	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.182.166.181	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.169.45.231	United Kingdom	147.237.76.196	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
109.169.45.231	United Kingdom	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
59.46.193.114	China	147.237.76.199	e.nakchal.idf.il	GPL SCAN nmap TCP	2
82.102.141.198	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.65	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	2
109.64.160.85	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
77.126.80.227	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.169.45.231	United Kingdom	147.237.72.156	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
109.169.45.231	United Kingdom	147.237.76.148	ggcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
84.228.158.72	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.160.185.8	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.67	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	2
109.64.101.157	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
91.227.164.5	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
93.173.30.224	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.111.163.89	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.81.168	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
5.29.176.34	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
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	770
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	710
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	686
46.210.254.32	Israel	147.237.77.176	matpash.idf.il	Invalid ACK number	Bad TCP sequence	monitor	135
156.34.191.113	Canada	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	126
188.139.237.91	Syrian Arab Republic	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	92
80.246.137.125	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	91
66.249.64.145	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	80
188.139.237.91	Syrian Arab Republic	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	76
66.249.93.152	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	76
66.249.64.141	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	74
194.98.114.103	France	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	63
132.76.50.5	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	60
66.249.64.149	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	56
82.80.198.164	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	54
81.218.170.220	Israel	147.237.72.166	aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	51
46.19.85.101	Israel	147.237.72.166	aka.idf.il	SAM rule	drop	drop	50
78.108.161.226	Lebanon	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	48
66.249.81.200	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	48
212.179.71.70	Israel	147.237.72.167	ishurim.aka.idf.i	First packet isn't SYN	drop	drop	47
157.55.39.234	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	46
79.176.124.153	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	45
155.41.109.97	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	44
66.249.93.158	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
82.145.217.212	Europe	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	39
212.179.230.180	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	39
31.210.187.4	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid ACK number	Bad TCP sequence	monitor	38
109.67.81.51	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
46.19.85.101	Israel	147.237.72.156	aman.idf.il	SAM rule	drop	drop	37
66.249.81.197	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
46.19.86.71	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	35
192.114.105.254	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
66.249.93.155	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
80.179.195.120	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
77.171.50.176	Netherlands	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
212.143.186.38	Israel	147.237.77.233	atal.idf.il	'Proxy-Authorization' header length exceeded maximum allowed length	HTTP Format Sizes	monitor	32
193.43.246.250	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
212.143.118.251	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	31
66.249.81.203	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
5.22.135.212	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
212.29.249.212	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
188.120.148.107	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	monitor	30
79.182.11.34	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
132.66.213.85	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
8.7.228.252	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	29
85.130.187.196	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	29
192.114.105.254	Israel	147.237.76.86	navy.idf.il	First packet isn't SYN	drop	drop	28
199.30.17.51	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
66.102.6.208	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.64.127.38	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.64.127.38	Block	1205
2.54.57.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	450
93.173.11.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	354
2.54.128.123	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.128.123	Block	327
46.19.85.96	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.96	Block	178
46.19.86.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	151
176.12.137.134	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.137.134	Block	137
202.55.10.106	Hong Kong	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	110
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	93
176.12.142.194	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.142.194	Block	87
66.249.78.173	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	82
109.253.146.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	76
37.26.148.239	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.148.239	Block	73
66.249.78.166	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	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	65
176.12.143.238	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.143.238	Block	52
66.249.78.109	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.109	Block	50
176.12.151.193	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.151.193	Block	50
66.249.78.95	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.95	Block	50
66.249.78.102	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.102	Block	48
91.207.7.77	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 91.207.7.77	Block	47
46.19.86.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	44
46.19.86.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	42
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	39
80.178.154.32	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	27
209.222.8.51	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 209.222.8.51	Block	23
79.182.145.182	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	22
188.161.5.1	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 188.161.5.1	Block	18
85.65.90.214	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 85.65.90.214	Block	15
188.161.5.1	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.161.5.1	Block	14
176.228.214.155	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	13
66.249.64.171	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/giyus/general.aspx	Block	13
109.160.191.73	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	11
188.161.5.1	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	11
85.250.87.93	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	10
84.228.56.94	Israel	147.237.72.166	aka.idf.il	Multiple Double URL Encoding from 84.228.56.94	Block	10
87.68.238.161	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	10
95.86.66.151	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	10
62.219.98.206	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	10
87.69.20.197	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatesmakatqantity.aspx	Block	10
46.121.224.211	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	9
37.115.186.0	Ukraine	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1498-en/dover.aspx/	Block	9
95.86.123.14	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	9
91.207.7.77	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/trackback/	Block	9
46.19.85.197	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	9
209.222.8.51	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	9
82.102.136.69	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	8
132.66.82.82	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	8
147.236.76.4	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	None	8
2.54.7.114	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	8