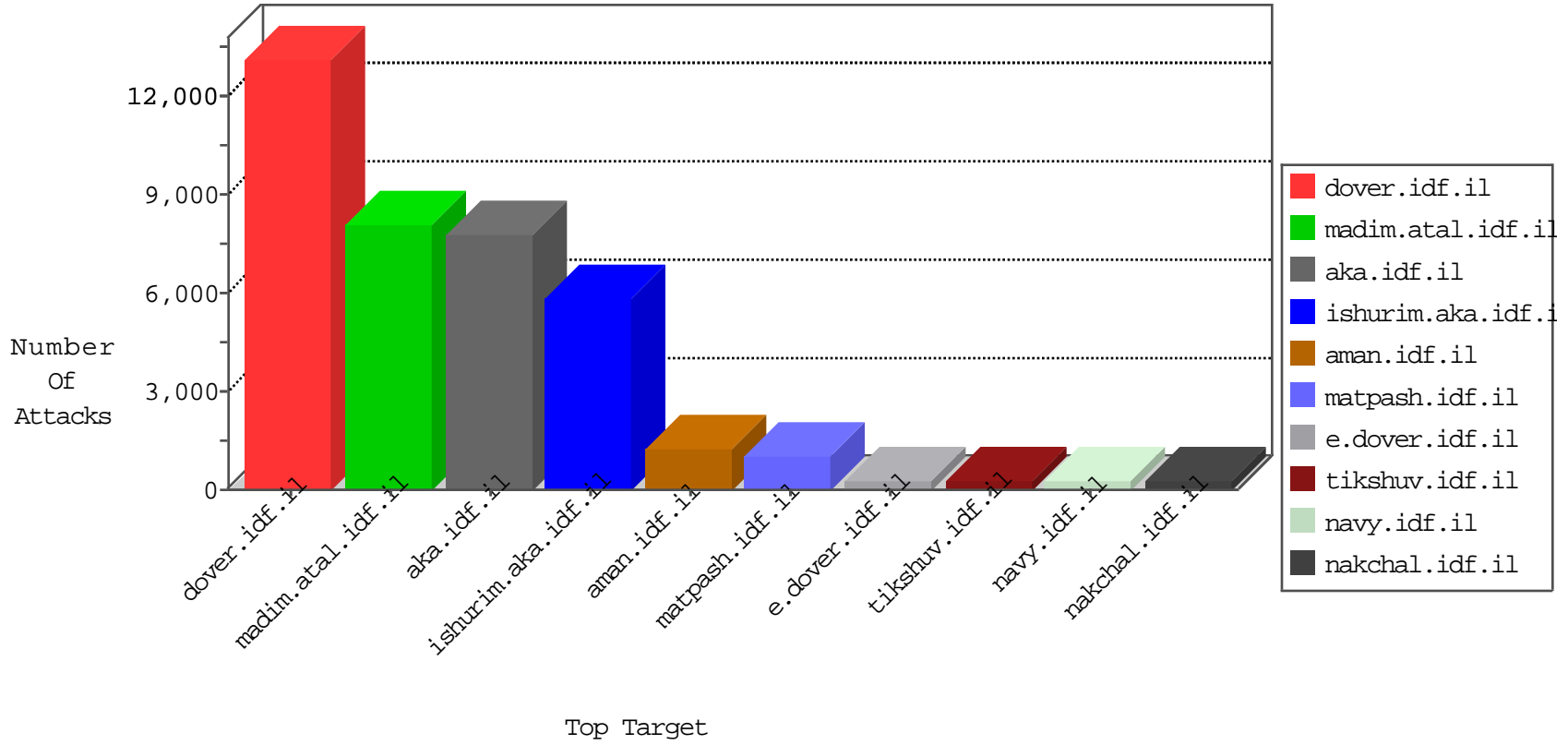


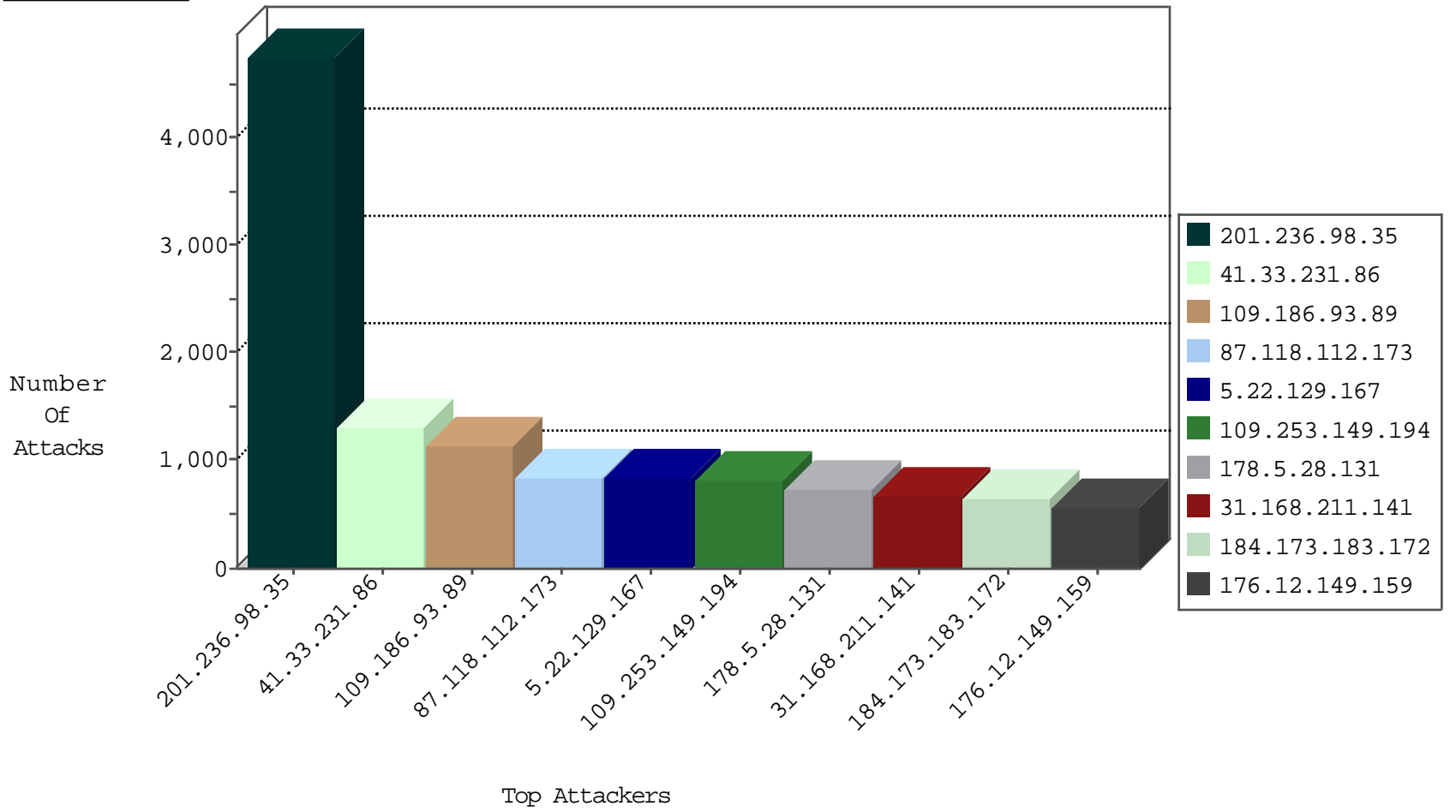
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
109.186.93.89	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-SSL-renegotiation-Cli	forward	1407
85.64.96.218	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	701
66.249.78.38	United States	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	637
79.177.60.103	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	464
46.121.74.138	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	445
149.88.108.96	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	441
66.249.78.153	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	398
66.249.78.31	United States	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	397
109.186.93.89	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	319
192.114.2.36	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	312
46.19.85.136	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	278
212.199.112.144	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	271
149.78.51.253	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	238
213.57.46.23	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	238
80.246.138.245	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-SSL-renegotiation-Cli	forward	238
46.117.75.152	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	235
79.178.134.59	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	232
109.160.171.12	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	230
77.125.76.55	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	230
79.182.102.160	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	225
213.57.155.222	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	216
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	210
213.57.153.144	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	202
66.249.78.9	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	183
82.102.141.222	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	175
5.29.107.250	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	166
37.142.138.118	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	165
79.178.33.225	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	161
85.64.94.24	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	157
46.19.85.114	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	forward	148
185.32.177.119	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	146
87.68.60.122	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	143
84.108.106.152	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	141
46.19.86.31	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	forward	138
2.54.21.153	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	forward	130
212.199.149.78	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	126
80.246.137.181	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	121
46.19.86.93	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	forward	120
79.182.132.134	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	118
212.143.44.5	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	117
212.199.66.195	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	117
185.32.177.119	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-SSL-renegotiation-Cli	forward	114
79.176.173.69	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	114
212.179.44.27	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	104
109.253.134.16	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	96
46.117.23.83	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	95
93.173.22.80	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	95
2.54.21.153	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	92
109.64.36.2	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	91
79.177.20.122	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	89

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
87.118.112.173	Germany	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	846
178.5.28.131	Germany	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	727
37.46.47.42	Israel	147.237.72.166	aka.idf.il	Rep_Notify_Only_Tehila	Permit	560
184.173.183.172	United States	147.237.77.176	matpash.idf.il	Rep_Notify_Only_Tehila	Permit	503
176.58.100.98	United Kingdom	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	163
94.242.255.236	Luxembourg	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	163
184.173.183.172	United States	147.237.76.86	navy.idf.il	Rep_Notify_Only_Tehila	Permit	139
198.96.155.3	Canada	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	82
212.199.156.66	Israel	147.237.77.233	atal.idf.il	Rep_Notify_Only_Tehila	Permit	49
86.98.50.52	United Arab Emirates	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	35
85.250.177.106	Israel	147.237.72.166	aka.idf.il	Block_Level_70_100	Block	29
82.211.201.188	Denmark	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	19
171.25.193.78	Sweden	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	19
31.31.76.50	Czech Republic	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	19
31.31.76.149	Czech Republic	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	19
37.157.195.83	Czech Republic	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	19
5.79.68.161	Netherlands	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	19
91.213.8.236	Ukraine	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	19
217.115.10.133	Germany	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	19
89.73.177.236	Poland	147.237.77.216	dover.idf.il	Rep_Notify_Only_Tehila	Permit	16
37.205.9.131	Slovakia	147.237.72.166	aka.idf.il	Rep_Notify_Only_Tehila	Permit	10
37.205.9.131	Slovakia	147.237.72.156	aman.idf.il	Rep_Notify_Only_Tehila	Permit	10
5.29.39.29	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	9
46.117.61.17	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	9
218.77.79.43	China	147.237.76.42	refuah.idf.il	Block_Level_70_100	Block	6
71.6.135.131	United States	147.237.76.201	e.atal.idf.il	Block_Level_70_100	Block	6
37.142.97.39	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
46.19.85.197	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
192.115.248.2	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
218.77.79.43	China	147.237.76.148	ggcenter.aka.idf.il	Block_Level_70_100	Block	5
218.77.79.43	China	147.237.76.198	e.yohalan.idf.il	Block_Level_70_100	Block	5
71.6.165.200	United States	147.237.77.74	law.idf.il	Block_Level_70_100	Block	5
218.77.79.43	China	147.237.76.176	test.ncore.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
198.20.69.98	United States	147.237.76.177	ncore.idf.il	Block_Level_70_100	Block	5
218.77.79.43	China	147.237.76.199	e.nakchal.idf.il	Block_Level_70_100	Block	5
66.240.236.119	United States	147.237.76.34	yohalan.idf.il	Block_Level_70_100	Block	5
71.6.135.131	United States	147.237.72.167	ishurim.aka.idf.il	Block_Level_70_100	Block	5
218.77.79.43	China	147.237.76.177	ncore.idf.il	Block_Level_70_100	Block	5
194.90.107.69	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
218.77.79.43	China	147.237.76.196	e.sviva.idf.il	Block_Level_70_100	Block	5
71.6.165.200	United States	147.237.76.147	chinuch.aka.idf.il	Block_Level_70_100	Block	5
71.6.135.131	United States	147.237.77.179	e.mazi.idf.il	Block_Level_70_100	Block	5
218.77.79.43	China	147.237.76.202	e.halag.idf.il	Block_Level_70_100	Block	5
85.25.43.94	Germany	147.237.77.233	atal.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
46.120.72.202	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
71.6.165.200	United States	147.237.77.233	atal.idf.il	Block_Level_70_100	Block	4
71.6.165.200	United States	147.237.76.176	test.ncore.idf.il	Block_Level_70_100	Block	4
89.139.50.154	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.78.204	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	154
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	132
201.236.98.35	Chile	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	66
82.102.141.197	Israel	147.237.77.216	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	35
2.54.144.71	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	23
82.102.141.197	Israel	147.237.72.167	ishurim.aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	23
59.106.108.116	Japan	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	4
177.85.60.202	Brazil	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	4
93.172.152.213	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	4
200.47.31.25	Venezuela	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
2.54.17.188	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.19.86.140	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.181.121.242	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
149.78.12.173	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
95.86.75.144	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.117.171.165	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
222.186.15.202	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.67	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	2
109.66.13.168	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	2
93.184.66.150	Slovakia	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	2
85.250.185.114	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
167.88.43.233		147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	2
84.229.242.123	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.190.87.102	France	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
5.22.130.59	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
93.184.66.150	Slovakia	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
213.57.216.12	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
177.85.60.202	Brazil	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
80.246.133.31	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
93.173.20.103	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
213.57.13.252	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.111.137.79	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.67	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	2
84.108.208.144	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
77.126.41.88	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.120.99.212	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.19.86.79	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.94.170.18	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.64.199.19	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.179.174.110	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
128.139.197.114	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.65	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	2
109.64.5.141	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
87.68.63.222	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
85.65.99.21	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
213.57.229.7	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
80.246.133.67	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.67	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	2
46.19.86.239	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
201.236.98.35	Chile	147.237.77.216	dover.idf.il	SAM rule	drop	drop	4627
41.33.231.86	Egypt	147.237.77.216	dover.idf.il		drop	drop	1306
41.33.232.65	Egypt	147.237.77.216	dover.idf.il		drop	drop	435
168.235.197.58		147.237.72.166	aka.idf.il		drop	drop	359
149.78.11.178	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	288
207.241.226.182	United States	147.237.77.216	dover.idf.il	Web Servers Slow HTTP Denial of Service	Web Server Enforcement Violation	reject	196
5.22.129.167	Israel	147.237.0.19	madim.atal.idf.il	Invalid ACK number	Bad TCP sequence		188
5.22.129.167	Israel	147.237.0.19	madim.atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	185
82.166.6.216	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	144
212.179.140.133	Israel	147.237.76.31	nakchal.idf.il	SAM rule	drop	drop	126
87.68.96.223	Israel	147.237.8.50	e.tikshuv.idf.il	Geo-location inbound enforcement	Geo-location enforcement	monitor	84
82.166.6.216	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	82
201.236.98.35	Chile	147.237.77.216	dover.idf.il		drop	drop	64
89.139.184.99	Israel	147.237.72.166	aka.idf.il		drop	drop	63
79.176.131.192	Israel	147.237.72.166	aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	61
41.254.9.144	Libyan Arab Jamahiriya	147.237.77.176	matpash.idf.il		drop	drop	59
81.218.183.91	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	57
94.230.86.195	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	57
212.179.21.195	Israel	147.237.77.212	e.dover.idf.il	Geo-location inbound enforcement	Geo-location enforcement	monitor	56
194.90.131.82	Israel	147.237.72.166	aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	54
5.22.129.198	Israel	147.237.72.167	ishurim.aka.idf.il		drop	drop	51
194.90.131.82	Israel	147.237.72.166	aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence		50
87.68.225.231	Israel	147.237.72.166	aka.idf.il		drop	drop	50
109.44.3.8	Germany	147.237.77.176	matpash.idf.il		drop	drop	48
193.37.128.8	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	48
193.37.128.8	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	46
84.110.168.174	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	44
212.179.61.122	Israel	147.237.77.212	e.dover.idf.il	Geo-location inbound enforcement	Geo-location enforcement	monitor	43
41.254.5.165	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il		drop	drop	41
82.80.198.164	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	41
62.219.238.215	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	41
31.44.142.27	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	40
84.94.76.215	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	monitor	39
84.94.193.23	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	36
192.115.248.2	Israel	147.237.72.156	aman.idf.il	Invalid sequence number	Bad TCP sequence	monitor	36
79.176.152.253	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	33
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission		32
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
46.19.86.80	Israel	147.237.72.166	aka.idf.il		drop	drop	32
212.179.61.124	Israel	147.237.77.212	e.dover.idf.il	Geo-location inbound enforcement	Geo-location enforcement	monitor	31
213.8.96.180	Israel	147.237.77.216	dover.idf.il		drop	drop	30
212.179.21.194	Israel	147.237.77.212	e.dover.idf.il	Geo-location inbound enforcement	Geo-location enforcement	monitor	30
62.219.160.159	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.64.63.58	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
213.244.81.60	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il		drop	drop	28
81.218.37.2	Israel	147.237.77.226	www.chamatz.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	27
84.94.193.23	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	27
62.219.238.141	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	27
95.35.11.185	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	27
212.179.61.122	Israel	147.237.8.27	e.madim.atal.idf.il	Geo-location inbound enforcement	Geo-location enforcement	monitor	26

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.253.149.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	814
31.168.211.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	664
176.12.149.159	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.149.159	Block	572
109.186.93.89	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.186.93.89	Block	450
5.22.129.167	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 5.22.129.167	Block	447
46.19.85.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	414
37.26.147.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	409
109.253.135.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	381
109.253.135.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	343
2.54.157.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	334
80.179.195.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	267
46.19.86.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	214
176.12.136.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	211
207.241.226.182	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	160
37.26.148.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	150
46.19.86.48	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.48	Block	133
2.54.60.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	133
46.19.85.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	99
82.102.141.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	90
46.19.86.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	83
185.32.177.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	77
213.151.60.253	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	74
109.253.128.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	67
80.246.138.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	62
37.26.147.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	54
37.26.146.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	54
66.249.78.102	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.102	Block	52
46.120.48.110	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.120.48.110	Block	50
66.249.78.109	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.109	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	48
93.172.167.239	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	46
66.249.78.159	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	43
79.180.127.25	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	38
66.249.78.236	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.236	Block	31
66.249.78.153	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.153	Block	26
84.228.125.124	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	24
31.168.132.131	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	24
79.176.100.237	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	24
66.249.78.160	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.160	Block	21
5.29.39.29	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	21
93.173.154.169	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	21
87.69.104.134	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	21
185.32.176.22	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	20
79.182.0.226	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/gyus/controls/atuda/Å	Block	20
84.111.100.150	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.111.100.150	Block	20
79.177.35.204	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
79.180.127.25	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/resources/controls/captcha.ashx	Block	19
82.166.247.195	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	19
84.111.164.157	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	18
193.193.229.35	Kazakstan	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 193.193.229.35	Block	16