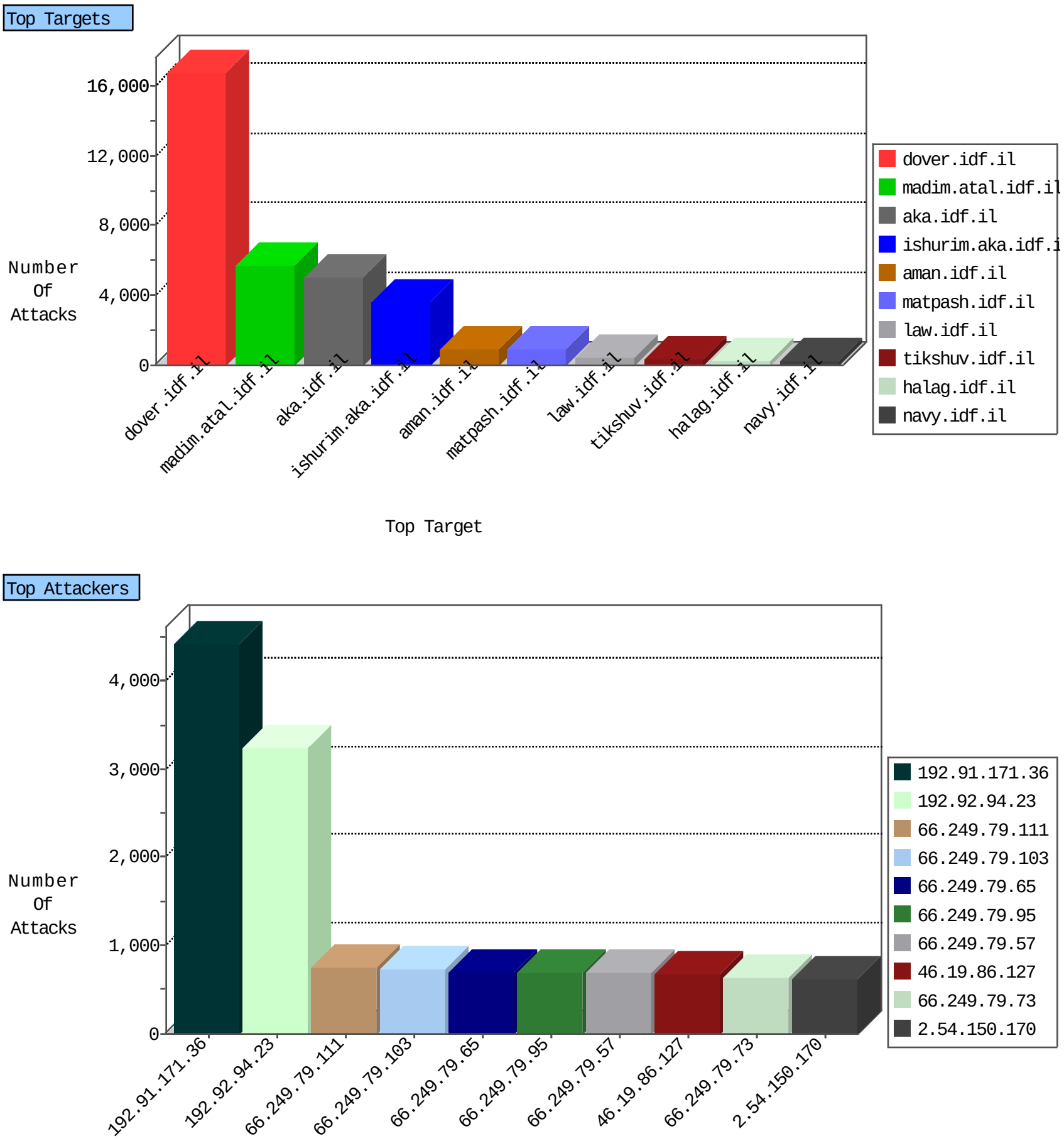
01-29-2015-00:00:05 to 01-30-2015-00:00:05

IDF Under Attack Daily Report



01-29-2015-00:00:05 to 01-30-2015-00:00:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
213.57.47.172	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	918
192.116.94.67	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	916
212.116.162.6	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	767
109.65.184.13	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	660
132.74.208.174	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	630
31.168.103.115	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	391
149.88.11.131	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	309
5.102.216.200	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	279
77.126.165.236	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	267
46.19.85.64	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	258
109.67.132.213	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	252
46.19.85.98	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	242
46.19.86.135	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	228
46.121.244.2	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	186
84.229.144.108	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	182
87.68.24.64	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	177
149.78.154.40	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	172
46.121.110.244	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	170
192.116.52.79	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	169
79.177.123.154	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	158
46.116.135.188	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	143
79.181.128.107	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	136
84.108.207.192	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	133
109.64.61.157	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	123
79.177.120.83	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	121
85.65.48.139	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	120
79.178.2.153	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	111
85.64.129.113	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	106
193.46.64.93	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	98
5.102.253.154	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	92
80.246.136.74	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	90
37.26.148.239	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	89
5.29.51.41	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	87
85.65.53.98	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	79
62.90.235.246	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	79
2.54.144.85	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	76
185.32.177.169	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	74
109.253.143.250	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	73
46.19.85.104	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	72
93.173.5.120	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
46.117.22.97	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	71
82.102.141.198	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	63
46.116.135.188	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	forward	61
80.246.140.51	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	61
80.246.141.17	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	59
46.19.86.17	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	52
185.32.178.159	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	51
82.102.141.217	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	43
82.102.141.205	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	38
82.145.208.156	Europe	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	37

01-29-2015-00:00:05 to 01-30-2015-00:00:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
192.91.171.36	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	4427
192.92.94.23	Europe	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	3240
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	437
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	280
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	113
180.76.5.193	China	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	54
180.76.5.193	China	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	48
95.185.50.22	Romania	147.237.77.216	dover.idf.il	C091: HTTP: Access to - admin.asp	Block	38
180.76.5.193	China	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	33
180.76.5.193	China	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	28
194.114.146.227	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
192.115.88.194	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
85.250.46.140	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
54.172.196.207	United States	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	5
77.126.224.211	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
82.102.169.113	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
192.114.23.18	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
85.25.43.94	Germany	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	5
157.166.167.129	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
87.98.159.231	France	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	5
81.218.134.186	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
46.120.146.233	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
147.236.238.22	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
71.6.165.200	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	4
66.240.236.119	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	4
84.111.227.100	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
95.130.15.97	France	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	4
212.179.21.126	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
71.6.167.142	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	4
106.138.56.200	Japan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
93.120.27.62	Romania	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	3
85.25.43.94	Germany	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	3
185.32.177.219	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
82.211.223.3	Denmark	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	3
176.126.252.12	Romania	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	3
124.240.221.17	Papua New Guinea	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.184	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
171.25.193.20	Sweden	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	3
71.6.165.200	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	3
76.110.163.61	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
147.236.238.97	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
85.25.43.94	Germany	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	3
66.240.236.119	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	3
85.25.43.94	Germany	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	3
93.120.27.62	Romania	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	3
85.25.43.94	Germany	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	3
85.25.43.94	Germany	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	3
66.240.236.119	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	3
71.6.167.142	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	3
199.203.84.218	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3

01-29-2015-00:00:05 to 01-30-2015-00:00:05

Top Attackers In IDS

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	331
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	135
95.185.50.22	Romania	147.237.77.216	dover.idf.il	Admin login page scan - Havij	28
85.65.35.82	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	14
46.19.85.70	Israel	147.237.77.216	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	12
155.254.238.13		147.237.72.166	aka.idf.il	SERVER-WEBAPP cat%20 access	8
109.66.50.68	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	8
95.185.50.22	Romania	147.237.77.216	dover.idf.il	SERVER-WEBAPP adminlogin access	7
95.185.50.22	Romania	147.237.77.216	dover.idf.il	SERVER-WEBAPP admin.php access	7
95.185.50.22	Romania	147.237.77.216	dover.idf.il	SERVER-WEBAPP login.htm access	4
59.106.108.116	Japan	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
121.42.54.18	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	3
107.167.110.60	United States	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	3
168.63.139.43	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.66.166.81	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
213.57.37.180	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
80.91.80.57	Spain	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
2.54.158.49	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.66.122.221	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
212.199.218.246	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.19.86.149	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
85.65.220.225	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
85.65.157.215	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.183.136.172	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
121.42.54.18	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	2
109.253.144.212	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
59.45.73.134	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
79.181.113.83	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.64	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	2
87.69.93.176	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
5.144.61.9	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
121.42.54.18	China	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sS window 1024	2
84.111.77.124	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
64.79.75.194	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.67	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	2
79.179.29.139	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.65	China	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.64	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	2
46.117.120.97	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.94.41.20	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
5.29.51.47	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.160.236.23	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
213.57.43.124	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.116.218.47	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
2.54.161.228	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.66.144.212	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
85.65.223.220	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
80.91.80.57	Spain	147.237.77.216	dover.idf.il	SERVER-WEBAPP phpThumb fltr[] parameter remote command execution attempt	2
82.166.102.236	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.65	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	2

01-29-2015-00:00:05 to 01-30-2015-00:00:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.79.57	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	602
66.249.79.65	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	596
66.249.79.73	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	556
189.40.89.135	Brazil	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	246
136.173.162.144	Belgium	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	168
112.198.77.105	Philippines	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	120
158.169.40.6	Luxembourg	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	106
66.249.81.197	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	80
217.20.178.209	Ukraine	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	76
82.145.211.172	Europe	147.237.77.226	www.chamatz.aka.idf.il	First packet isn't SYN	drop	drop	74
132.79.13.16	United States	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	73
76.174.18.243	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	72
136.173.162.129	Belgium	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	72
66.249.78.44	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	70
109.64.152.133	Israel	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	66
193.188.156.17	Sweden	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	65
66.249.78.51	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	60
109.253.149.148	Israel	147.237.72.156	aman.idf.il	First packet isn't SYN	drop	drop	57
132.76.50.5	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	56
66.249.81.200	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	54
176.102.73.6	Czech Republic	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	52
147.236.238.10	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	52
193.178.209.225	Belgium	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	52
82.145.211.172	Europe	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	50
192.114.23.211	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	48
66.249.78.37	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	48
158.169.150.10	Belgium	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	47
83.244.111.98	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	47
212.14.228.162	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	44
212.150.178.252	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
198.7.238.40	United States	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	42
109.65.60.8	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	41
66.249.93.152	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	40
66.249.81.203	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
157.166.167.129	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
83.76.188.233	Switzerland	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
82.102.169.113	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	35
87.69.137.17	Israel	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	35
84.229.66.69	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
46.19.86.135	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	34
149.78.35.179	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
138.162.128.54	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
5.28.181.56	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	31
46.19.86.202	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
66.249.93.155	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
199.30.25.92	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
41.131.117.128	Egypt	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
2.54.171.145	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
37.145.65.145	Russian Federation	147.237.77.74	law.idf.il	First packet isn't SYN	drop	drop	28
41.196.79.106	Egypt	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	27

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.86.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	665
66.249.79.111	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.111	Block	640
2.54.150.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	627
66.249.79.103	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.103	Block	597
66.249.79.95	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.95	Block	575
46.117.237.120	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	440
37.26.147.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	430
95.185.50.22	Romania	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 95.185.50.22	Block	373
176.12.137.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	367
85.64.255.252	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 85.64.255.252	Block	361
46.19.86.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	353
176.12.136.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	317
95.86.121.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	277
176.12.136.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	250
82.102.141.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	244
46.19.86.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	229
176.12.136.103	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	223
84.108.139.199	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 84.108.139.199	Block	215
87.69.157.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	138
66.249.79.103	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//1133-he/dover.aspx	Block	125
66.249.79.95	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//1133-he/dover.aspx	Block	113
66.249.79.111	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//1133-he/dover.aspx	Block	108
94.159.190.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	105
66.249.79.65	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.65	Block	88
66.249.79.57	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.57	Block	83
66.249.79.73	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.73	Block	76
46.19.85.175	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.175	Block	74
46.19.86.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	73
37.26.146.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	46
2.54.155.211	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.155.211	Block	43
80.246.137.119	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 80.246.137.119	Block	42
86.157.39.68	United Kingdom	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 86.157.39.68	Block	41
81.218.118.126	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	29
46.19.85.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	28
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	27
213.57.217.29	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	27
79.181.12.244	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	21
202.55.2.117	Hong Kong	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	16
80.230.16.249	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	None	15
84.228.173.109	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	None	15
85.250.154.238	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	15
176.12.140.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	15
209.95.38.180	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 209.95.38.180	Block	15
46.117.185.68	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 46.117.185.68	Block	15
5.28.187.90	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 5.28.187.90	Block	14
79.178.141.13	Israel	147.237.0.15	kosher-kravi.idf.i	Multiple Unauthorized URL Access from 79.178.141.13	Block	14
95.86.70.219	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	13
212.235.98.139	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	13
72.229.236.13	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 72.229.236.13	Block	13
62.90.210.124	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	None	12