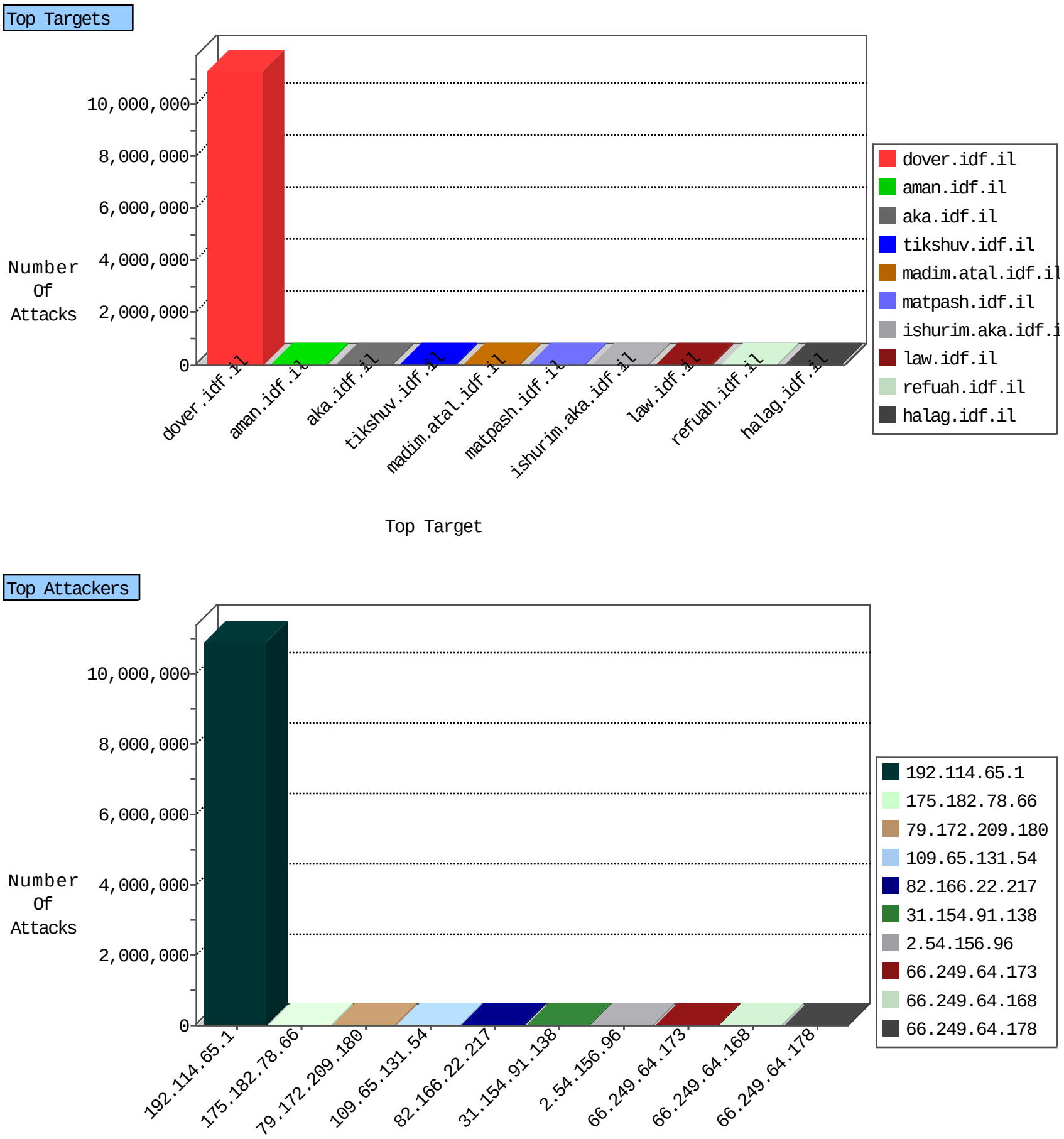
07-25-2015-00:00:05 to 07-26-2015-00:00:05

IDF Under Attack Daily Report



07-25-2015-00:00:05 to 07-26-2015-00:00:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
192.114.65.1	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	3124202
0.0.0.0		147.237.77.216	dover.idf.il	network flood IPv4 TCP-SYN	drop	1077059
0.0.0.0		147.237.77.216	dover.idf.il	DOSS-tcp-ack-zero-ack-num	drop	906368
66.249.78.254	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	291150
66.249.78.2	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	257927
192.114.65.1	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	190074
14.25.160.15	China	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	184712
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	149905
66.249.78.153	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	82186
37.182.180.61	Italy	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	44773
66.249.78.160	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	37607
182.58.53.81	India	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	31873
175.182.78.66	Taiwan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	28663
110.33.14.234	Australia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	15237
175.180.130.98	Taiwan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	14969
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	13378
109.187.157.116	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9949
137.166.76.24	Australia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8661
178.128.229.28	Greece	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8111
41.36.212.101	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8015
201.240.15.36	Peru	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6848
190.86.30.97	El Salvador	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	5596
79.172.209.180	Hungary	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	4979
204.93.154.216	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	1801
185.3.145.191	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	718
188.120.133.194	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	forward	512
85.64.214.156	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	435
77.125.5.12	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	333
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	328
188.120.148.141	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	297
84.228.59.245	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	280
109.64.185.163	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	250
188.120.133.57	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	248
192.114.65.1	Israel	147.237.77.216	dover.idf.il	DOSS-tcp-ack-zero-ack-num	drop	224
149.78.95.161	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	218
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	211
2.52.59.100	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	205
109.65.43.211	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	193
149.78.21.224	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	178
5.29.207.212	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	176
89.138.217.165	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	174
204.93.154.211	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	173
84.228.33.38	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	168
87.68.242.204	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	165
85.65.126.115	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	157
93.172.0.27	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	145
79.176.6.78	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	135
212.25.121.195	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	132
66.249.64.178	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	130
93.172.23.76	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	129

07-25-2015-00:00:05 to 07-26-2015-00:00:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
84.109.50.71	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
213.139.52.16	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
74.214.56.205	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
79.179.213.112	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
149.78.21.224	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
87.68.37.94	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
149.78.87.14	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
46.19.85.41	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
77.127.224.167	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
85.250.227.1	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
85.250.36.26	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
85.250.94.44	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
85.65.64.163	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
79.180.135.69	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
196.207.98.4		147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
84.229.173.27	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
79.177.36.9	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
87.69.232.38	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
85.64.247.232	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
109.64.198.213	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
84.108.62.118	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.191	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
96.51.136.164	Canada	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
80.246.136.235	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
82.22.27.19	United Kingdom	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.172	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
79.177.209.1	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
85.132.77.12	Azerbaijan	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
79.181.160.147	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
62.210.251.69	France	147.237.77.176	matpash.idf.il	17031: HTTP: GetSimple CMS File Upload	Block	2
46.121.74.13	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
149.78.86.11	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.19.85.135	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
109.64.64.111	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
31.154.92.228	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
185.19.223.42	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.151	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
80.178.210.146	Israel	147.237.77.226	www.chamatz.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
79.177.123.143	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.74	United States	147.237.77.227	e.hamaz.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
37.142.153.37	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
89.139.164.102	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.65.26.224	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
62.210.251.69	France	147.237.77.176	matpash.idf.il	19661: HTTP: Wordpress InBoundio Marketing PHP Upload Vulnerability	Block	1
165.215.209.15	United States	147.237.77.216	dover.idf.il	14511: HTTP: Win32/Oliga Fake User Agent	Block	1
109.253.137.52	Israel	147.237.77.216	dover.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	1
185.32.179.197	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
37.26.147.139	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.250.221.8	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.121.206.183	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

07-25-2015-00:00:05 to 07-26-2015-00:00:05

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
192.114.65.1	Israel	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	6214158
175.182.78.66	Taiwan	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	13502
79.172.209.180	Hungary	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	8586
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	120
192.114.65.1	Israel	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	118
1.139.42.178	Australia	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
2.110.161.226	Denmark	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
2.232.202.174	Italy	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
2.238.228.77	Italy	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
4.47.48.64	United States	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
4.154.36.154	United States	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
4.161.48.223	United States	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
4.169.228.98	United States	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
5.98.186.155	Italy	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
5.107.69.19	Romania	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
8.86.19.218	United States	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
8.185.17.195	United States	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
8.191.197.9	United States	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
8.204.67.3	United States	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
12.36.148.217	United States	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
12.252.210.50	United States	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
14.202.170.191	Australia	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
15.127.147.193	United States	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
15.138.139.162	United States	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
15.226.108.135	United States	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
15.245.76.248	United States	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
17.71.227.232	United States	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
17.209.110.22	United States	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
17.216.242.16	United States	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
17.217.208.236	United States	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
17.248.199.102	United States	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
18.105.43.76	United States	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
18.165.12.96	United States	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
18.254.121.210	United States	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
23.254.237.153	United States	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
27.176.140.38	Korea, Republic of	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
27.185.71.58	China	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
31.18.31.173	Germany	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
31.249.188.47	Germany	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
35.2.242.243	United States	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
35.44.93.229	United States	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
35.58.26.186	United States	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
35.119.134.200	United States	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
35.130.216.54	United States	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
35.136.45.45	United States	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
36.209.89.254	China	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
37.18.118.150	Russian Federation	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
37.84.151.161	Germany	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
37.239.103.142	Iraq	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
38.3.217.210	United States	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4

07-25-2015-00:00:05 to 07-26-2015-00:00:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
192.114.65.1	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4415609
175.182.78.66	Taiwan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8764
79.172.209.180	Hungary	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6329
109.65.131.54	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3560
82.166.22.217	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1887
31.154.91.138	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1040
2.54.156.96	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1009
185.26.182.27	Europe	147.237.0.34	tikshuv.idf.i	First packet isn't SYN	drop	drop	792
2.54.171.52	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	773
2.54.47.75	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	708
77.127.69.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	671
66.249.64.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	644
84.110.108.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	644
87.69.229.164	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	609
66.249.64.168	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	603
46.19.86.198	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	596
109.67.136.205	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	584
66.249.64.178	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	574
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	544
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	541
87.68.16.132	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	537
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	489
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	486
2.54.167.92	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	478
8.37.224.167	Anonymous Proxy	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	447
46.116.201.115	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	432
79.181.177.170	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	416
85.250.247.37	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	411
2.52.57.237	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	393
92.250.172.147	Luxembourg	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	392
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	380
37.237.204.29	Iraq	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	380
8.37.225.125	Anonymous Proxy	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	345
46.19.86.196	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	343
2.54.174.98	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	305
98.114.219.67	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	296
109.160.235.136	Israel	147.237.72.156	aman.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	287
87.69.88.144	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	284
89.139.162.241	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	249
5.29.135.3	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	248
46.19.85.242	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	233
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	230
46.117.251.44	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	228
37.26.146.141	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	227
85.214.216.18	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	220
2.54.157.108	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	219
188.120.133.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	213
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	200
166.137.242.89	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	194
46.19.86.254	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	189

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.116.186.74	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.116.186.74	Block	272
79.180.50.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	201
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.173	Block	87
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.178	Block	82
77.125.129.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	74
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.168	Block	64
2.52.59.100	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.52.59.100	Block	36
176.13.3.96	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.13.3.96	None	14
100.34.115.16	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
85.65.98.171	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	10
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	9
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	8
74.6.254.122	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	7
79.176.4.93	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
62.90.126.10	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 62.90.126.10	Block	6
216.177.132.157	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	6
69.89.31.199	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	6
66.249.65.83	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	6
109.65.191.249	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
192.99.148.94	Canada	147.237.77.74	law.idf.il	PHP Attempt	Block	6
82.80.176.62	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 82.80.176.62	Block	6
142.54.165.154	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 142.54.165.154	Block	6
50.57.48.124	United States	147.237.72.166	aka.idf.il	PHP Attempt	Block	6
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	6
109.67.6.76	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	6
79.180.50.140	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtMobile in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	5
188.40.38.76	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 188.40.38.76	Block	5
188.165.15.98	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.98	Block	5
66.249.65.86	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	5
27.149.238.53	China	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	5
74.63.254.218	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 74.63.254.218	Block	5
79.178.171.147	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/smalim/6_s3_	Block	5
23.29.122.198	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
112.74.75.173	China	147.237.77.74	law.idf.il	Distributed Admin Blocking	Block	4
89.139.19.211	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
213.57.160.177	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
216.177.132.157	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 216.177.132.157	Block	4
77.125.255.101	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	4
78.87.14.26	Greece	147.237.76.31	nakchal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucFaqControl$txtSearch in www.nakhal.idf.il/1119-he/nakhal.aspx	Block	4
176.13.22.137	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	4
198.46.149.165	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 198.46.149.165	Block	4
69.89.31.199	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 69.89.31.199	Block	4
50.57.48.124	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 50.57.48.124	Block	4
31.154.91.96	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
46.120.230.39	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	4
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	4
66.249.65.80	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	4
85.250.36.26	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	4
66.249.65.86	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	4

07-25-2015-00:00:05 to 07-26-2015-00:00:05