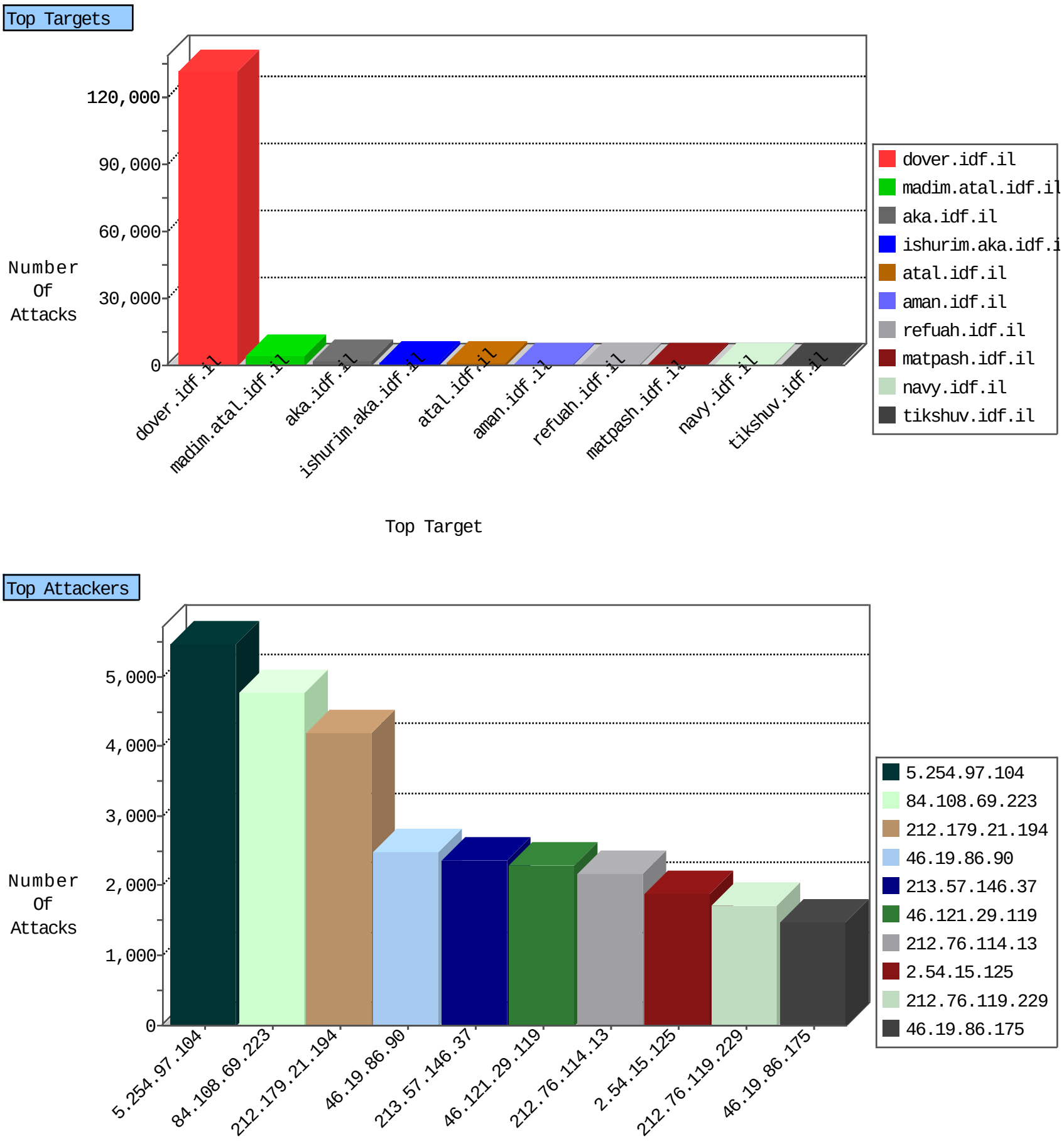
07-05-2015-00:00:07 to 07-06-2015-00:00:07

IDF Under Attack Daily Report



07-05-2015-00:00:07 to 07-06-2015-00:00:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
46.116.218.58	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3396
5.28.178.122	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2727
149.78.154.69	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2561
77.127.204.103	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	691
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	590
31.168.122.149	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	511
79.176.20.189	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	476
93.173.134.194	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	466
5.28.172.122	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	422
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	412
84.229.192.50	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	407
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	364
87.69.139.206	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	344
82.166.212.94	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	341
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	321
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	320
46.117.45.60	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	316
82.166.183.229	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	307
79.181.150.249	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	293
87.68.66.10	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	275
79.181.22.12	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	240
46.120.17.162	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	204
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	199
84.111.234.21	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	198
37.60.40.37	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	195
220.181.108.86	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	188
132.68.89.173	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	181
79.183.27.26	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	180
213.57.89.62	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	179
46.117.175.200	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	177
93.172.36.12	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	176
84.229.170.224	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	170
79.181.61.116	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	156
147.235.236.1	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	147
37.26.147.155	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	141
80.179.93.88	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	134
79.181.205.4	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	131
85.250.247.25	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	124
77.127.237.243	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	119
79.183.49.246	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	107
46.19.86.158	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	104
37.26.146.216	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	104
87.69.110.86	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	101
37.142.4.179	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	96
212.199.61.93	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	95
2.52.131.211	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	89
178.162.217.137	Germany	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	87
80.178.197.185	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	86
109.160.226.48	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	85
77.127.204.103	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	forward	84

07-05-2015-00:00:07 to 07-06-2015-00:00:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
77.127.204.103	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	48
80.179.223.31	Israel	147.237.77.176	matpash.idf.il	C1000004: HTTP: options method (Microsoft)	Block	18
87.69.139.206	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	16
79.183.116.96	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	13
82.102.169.113	Israel	147.237.72.167	ishurim.aka.idf.i	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	11
95.179.9.49	Russian Federation	147.237.77.176	matpash.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	9
79.183.151.146	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	9
84.108.82.58	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
37.142.198.45	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
46.19.85.230	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
84.94.26.133	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
84.94.181.145	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
132.70.66.14	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
192.117.105.148	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
46.19.85.137	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
46.19.85.128	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.106	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
79.180.218.43	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.187	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.29	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.254	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.115	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.70	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
109.67.170.69	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
84.108.130.89	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
5.29.176.148	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.48	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.147	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.13	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
212.179.222.212	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
46.19.85.91	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
79.180.119.163	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.28	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.45	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
83.244.5.151	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.107	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.245	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.31	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.116	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
119.159.113.44	Pakistan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
79.182.6.167	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
109.66.104.60	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
5.102.254.28	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
198.48.202.138	Canada	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.250	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.212	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.83	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
132.70.159.194	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.19.85.165	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.43	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2

07-05-2015-00:00:07 to 07-06-2015-00:00:07

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	32
182.50.130.105	Singapore	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	8
82.166.22.63	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	4
43.255.188.130	Japan	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	3
43.255.188.130	Japan	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	3
41.141.218.244	Morocco	147.237.77.216	dover.idf.il	SERVER-WEBAPP login.htm access	3
43.255.188.130	Japan	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	3
46.119.115.165	Ukraine	147.237.77.74	law.idf.il	http_inspect: MULTIPLE CONTENT LENGTH HEADER FIELDS	3
43.255.188.130	Japan	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	3
43.255.188.133	Japan	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	2
199.203.59.121	Israel	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.132	Japan	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.130	Japan	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
109.66.6.175	Israel	147.237.76.86	navy.idf.il	http_inspect: MULTIPLE HOST HEADERS DETECTED	2
43.255.188.130	Japan	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	2
79.176.9.9	Israel	147.237.77.216	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
93.184.2.74	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.79	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.130	Japan	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	2
176.58.123.82	United Kingdom	147.237.77.170	maarachot.idf.il	Tehila - Perl LWP with fake user agent	2
43.255.188.130	Japan	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.130	Japan	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	2
176.13.12.6	Israel	147.237.72.156	aman.idf.il	GPL SCAN myscan	2
199.203.59.121	Israel	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.130	Japan	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.132	Japan	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	2
66.249.81.168	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.130	Japan	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	2
212.179.21.194	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
43.255.188.130	Japan	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	2
66.249.67.79	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
61.183.128.6	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	2
41.141.218.244	Morocco	147.237.77.216	dover.idf.il	SERVER-WEBAPP admin.php access	2
43.255.188.130	Japan	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.135	Japan	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.135	Japan	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2
176.13.12.6	Israel	147.237.72.156	aman.idf.il	INDICATOR-SCAN myscan	2
43.255.188.130	Japan	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
85.64.76.56	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
2.52.128.0	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
62.219.83.119	Israel	147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
201.65.173.34	Brazil	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.188.135	Japan	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	1
130.185.74.152	Iran, Islamic Republic of	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
43.255.188.132	Japan	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
101.226.2.99	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -f -sS	1
37.220.14.122	United Kingdom	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
79.179.37.171	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
217.25.26.142	Azerbaijan	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 2048	1
60.18.162.244	China	147.237.76.86	navy.idf.il	ET SCAN NMAP -f -sS	1

07-05-2015-00:00:07 to 07-06-2015-00:00:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
5.254.97.104	Romania	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5365
84.108.69.223	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4783
212.179.21.194	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4127
46.19.86.90	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2487
213.57.146.37	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2371
46.121.29.119	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2292
212.76.114.13	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2177
2.54.15.125	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1901
212.76.119.229	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1731
46.19.86.175	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1400
79.183.129.71	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1327
95.86.98.18	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1325
85.65.0.129	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1306
79.182.39.238	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1195
82.166.22.63	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1121
2.54.170.145	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1047
77.125.141.171	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1030
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1020
79.179.207.250	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	864
82.166.243.162	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	810
46.117.212.244	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	793
149.88.77.187	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	770
79.182.164.249	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	751
46.121.211.156	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	743
192.116.160.248	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	729
192.116.48.203	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	721
2.54.142.105	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	678
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	629
192.249.64.249	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	614
95.86.118.172	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	611
46.210.133.223	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	538
79.181.152.198	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	536
2.52.25.109	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	525
164.138.117.95	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	511
46.19.86.224	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	504
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	485
2.52.159.79	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	476
109.186.0.186	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	466
46.19.86.152	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	460
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	456
84.228.100.192	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	451
192.116.164.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	451
46.19.85.86	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	446
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	444
46.19.86.113	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	428
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	428
69.118.118.123	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	421
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	405
132.71.141.22	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	402
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	398

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
37.26.147.199	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.147.199	Block	520
2.54.154.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	401
46.19.85.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	399
2.54.157.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	358
176.13.0.23	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.0.23	Block	345
46.19.86.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	251
46.19.86.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	231
46.19.86.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	205
176.12.138.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	95
176.13.23.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	86
176.13.20.111	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.20.111	Block	86
46.19.86.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	82
89.138.16.145	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 89.138.16.145	Block	81
79.177.24.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	79
2.54.38.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	77
80.246.136.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	73
46.19.86.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	71
46.120.48.135	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.120.48.135	Block	70
46.19.86.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	69
37.142.1.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	65
37.142.0.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	64
176.12.139.114	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.139.114	Block	57
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	54
176.13.1.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	53
46.19.86.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	46
2.52.163.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	25
176.12.138.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	20
46.116.148.221	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	19
176.12.140.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
80.246.136.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
46.19.85.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	15
157.55.39.62	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 157.55.39.62	Block	14
79.176.168.160	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/smalim/6_s3_	Block	13
212.179.21.194	Israel	147.237.76.147	chinuch.aka.idf.il	Multiple Unauthorized URL Access from 212.179.21.194	Block	13
79.178.206.254	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	12
109.18.44.13	France	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.18.44.13	Block	11
2.54.32.36	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	11
2.54.184.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	10
46.19.86.7	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.7	Block	10
5.255.253.33	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.33	Block	9
5.28.137.37	Israel	147.237.72.156	aman.idf.il	Too Many of the Same Response Code (400) in All Sources from 5.28.137.37	Block	8
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	7
157.55.39.17	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il//site/unselecatble.aspx	Block	7
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	7
176.13.4.156	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.13.4.156	None	7
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	7
185.6.59.58	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuhg	Block	7
176.12.151.131	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	7
198.100.144.55	Canada	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/default.aspx	Block	6
46.19.86.100	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6

07-05-2015-00:00:07 to 07-06-2015-00:00:07