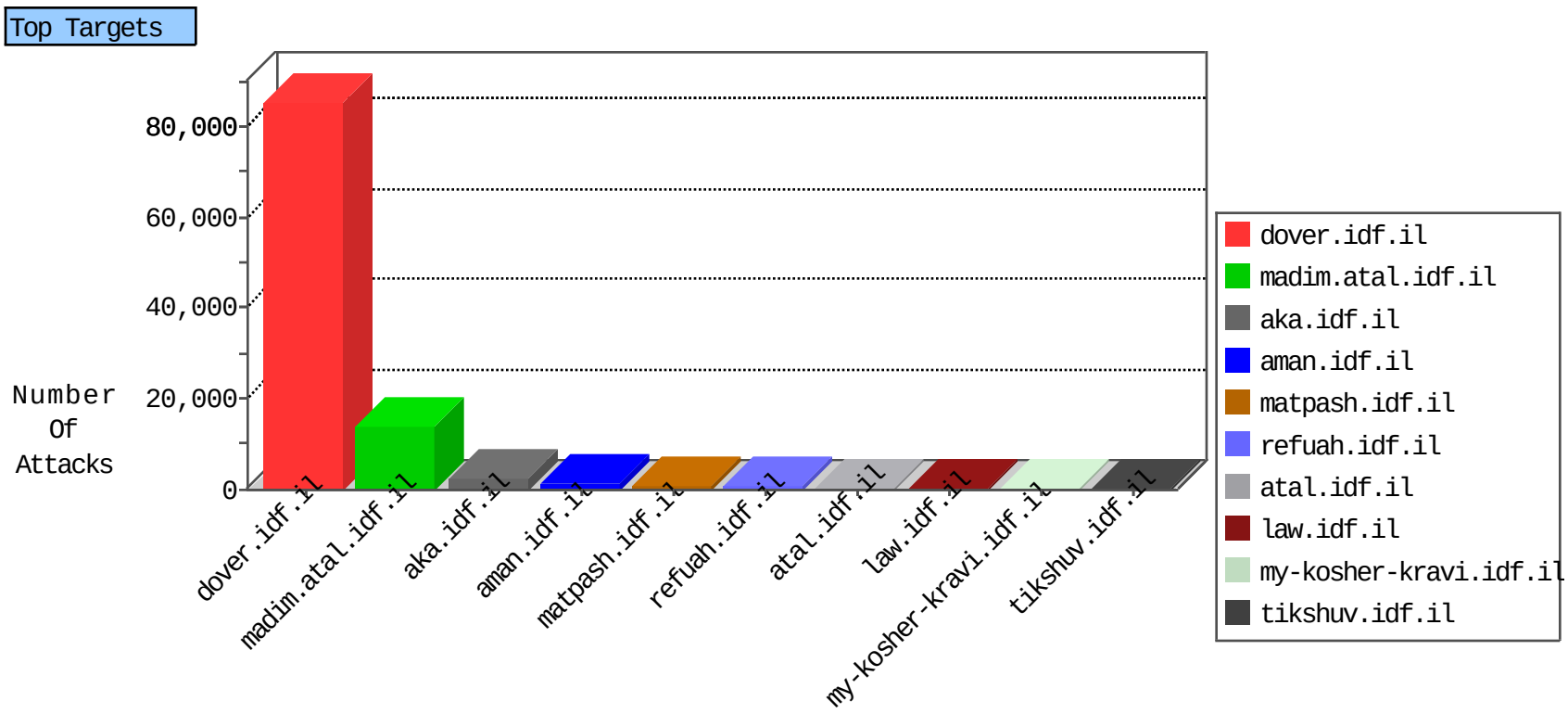
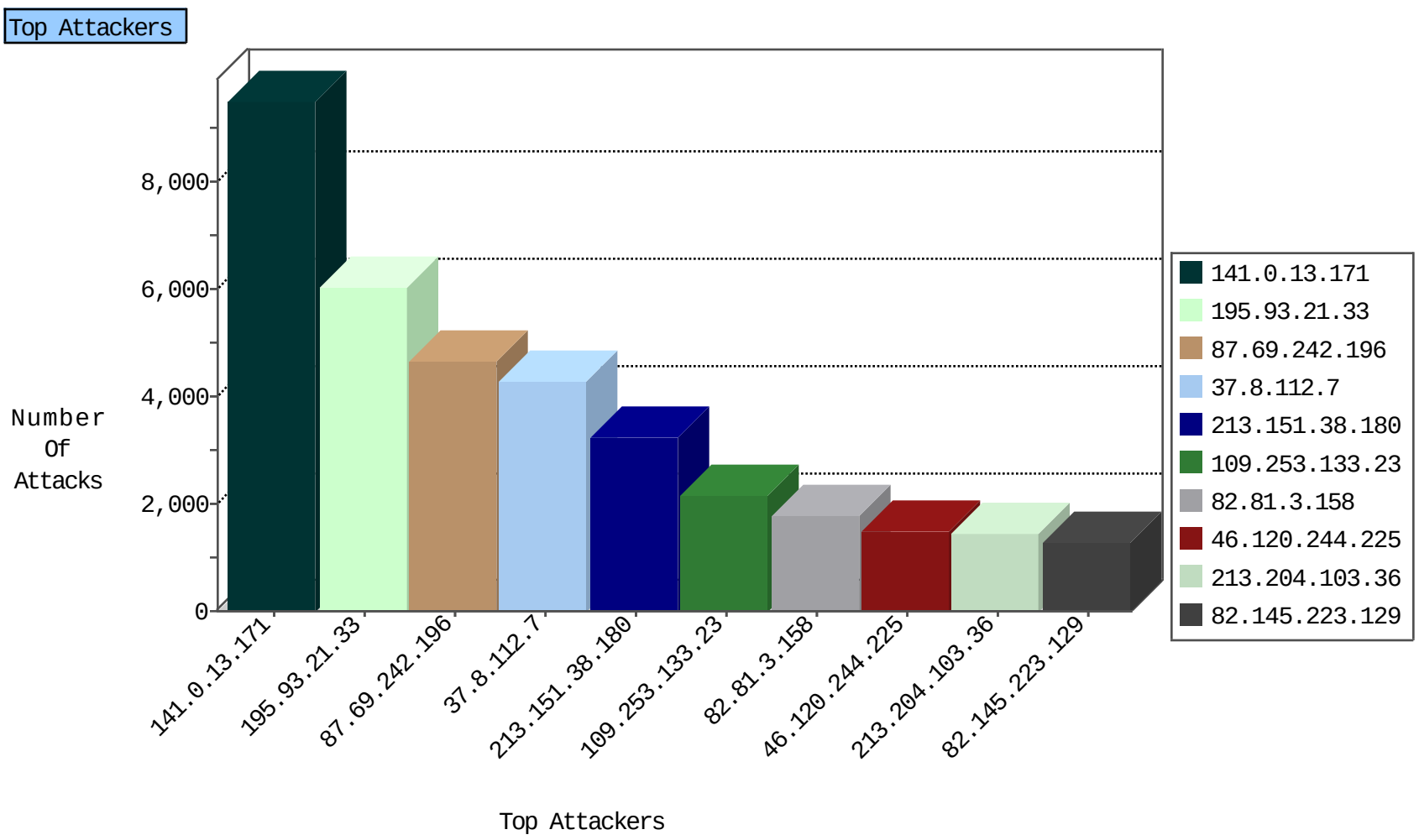
08-28-2015-00:00:08 to 08-29-2015-00:00:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-28-2015-00:00:08 to 08-29-2015-00:00:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
54.72.0.55	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10186
66.249.78.166	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9682
41.46.219.133	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7223
141.0.13.171	Norway	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3488
85.250.81.14	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	597
37.142.143.239	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	519
79.177.58.52	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	486
52.16.5.197	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	449
84.228.162.21	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	422
31.154.91.111	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	340
84.228.78.20	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	306
213.57.160.27	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	275
84.228.200.109	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	257
200.219.249.89	Brazil	147.237.77.216	dover.idf.il	SQL-Inj-Pang-GMSSQLInt1	dest-reset	240
87.68.81.179	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	205
84.229.34.210	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	191
89.138.58.82	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	190
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	182
79.182.54.58	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	180
46.117.214.151	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	176
79.183.51.198	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	176
94.230.86.199	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	174
79.179.10.97	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	172
84.111.65.71	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	171
109.160.137.81	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	162
2.52.154.62	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	158
149.88.41.245	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	157
220.181.108.108	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	156
85.250.113.159	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	154
85.64.204.208	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	145
82.166.23.32	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	140
46.120.84.148	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	140
109.64.173.242	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	127
37.142.64.82	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	123
220.181.108.115	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	122
87.69.23.1	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	119
84.228.88.187	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	112
82.166.23.16	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	111
176.228.176.37	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	110
85.64.191.231	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	109
194.90.167.120	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	108
109.64.3.35	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	97
94.159.160.20	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	96
109.67.35.2	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	92
87.69.63.132	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	91
31.154.91.205	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	89
213.57.62.231	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	86
84.228.161.48	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	84
37.142.234.18	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	82
109.67.177.37	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	81

08-28-2015-00:00:08 to 08-29-2015-00:00:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
84.228.162.21	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	41
194.90.66.9	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	23
110.85.94.228	China	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	12
213.139.53.180	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	11
197.211.52.18	Nigeria	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	10
46.19.85.97	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	10
46.19.85.16	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	9
46.19.85.111	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	7
82.222.127.38	Turkey	147.237.72.166	aka.idf.il	12373: HTTP: WordPress admin Login	Block	7
194.114.146.227	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
109.66.133.13	Israel	147.237.72.167	ishurim.aka.idf.i	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	6
79.178.206.61	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	6
46.19.85.17	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	6
46.19.85.23	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	6
176.106.226.5	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	6
46.19.85.166	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	5
46.19.85.46	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	4
82.166.23.32	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	4
24.120.54.60	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	4
46.19.85.251	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	4
5.29.77.201	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
46.117.133.210	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
46.19.85.77	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
194.90.66.9	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
46.19.85.217	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	3
31.13.163.20	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
108.83.18.103	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
2.52.56.238	Israel	147.237.77.243	mobile.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
85.64.154.3	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
95.86.73.232	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.116.152.115	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
46.121.15.122	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
110.85.94.228	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	2
5.29.77.201	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
93.172.180.39	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
46.117.22.209	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
84.109.71.174	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
108.16.207.105	United States	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
46.19.85.106	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	2
94.159.129.208	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	1
200.219.249.89	Brazil	147.237.77.216	dover.idf.il	3630: HTTP: SQL Injection (Boolean Identity)	Block	1
46.19.85.159	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	1
84.109.209.143	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	1
79.177.132.107	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	1
149.78.21.213	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	1
52.1.90.117	United States	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
46.19.86.41	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	1
189.238.20.215	Mexico	147.237.77.74	law.idf.il	12580: HTTP: SQL Injection (Cookie Header)	Block	1
76.189.201.111	United States	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	1
201.255.184.202	Argentina	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Permit	1

08-28-2015-00:00:08 to 08-29-2015-00:00:08

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	64
197.32.72.114	Egypt	147.237.77.216	dover.idf.il	SERVER-WEBAPP TRACE attempt	4
66.249.64.153	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
200.219.249.89	Brazil	147.237.77.216	dover.idf.il	SQL union select - possible sql injection attempt - GET parameter	4
66.249.78.173	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	4
93.174.93.100	Netherlands	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	4
66.249.93.247	United States	147.237.76.30	himush.idf.il	ET SCAN NMAP -sA (2)	4
200.219.249.89	Brazil	147.237.77.216	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT	4
66.249.67.27	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	4
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	3
93.174.93.100	Netherlands	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	3
66.249.78.158	United States	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
93.174.93.100	Netherlands	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	3
83.71.247.34	Ireland	147.237.72.167	ishurim.aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
93.174.93.100	Netherlands	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	3
93.174.93.100	Netherlands	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	3
200.219.249.89	Brazil	147.237.77.216	dover.idf.il	SQL url ending in comment characters - possible sql injection attempt	3
93.174.93.100	Netherlands	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	3
93.174.93.100	Netherlands	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	3
66.249.78.172	United States	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
93.174.93.100	Netherlands	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	3
93.174.93.100	Netherlands	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	3
66.249.64.178	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
23.234.51.12	United States	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
93.174.93.100	Netherlands	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
94.242.239.208	Luxembourg	147.237.77.216	dover.idf.il	ET DOS SSL Bomb DoS Attempt	2
93.174.93.100	Netherlands	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	2
128.199.171.41	Singapore	147.237.77.176	matpash.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	2
200.219.249.89	Brazil	147.237.77.216	dover.idf.il	INDICATOR-OBFUSCATION large number of calls to char function - possible sql injection obfuscation	2
115.196.25.224	China	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	2
93.174.93.100	Netherlands	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	2
213.204.103.26	Lebanon	147.237.76.30	himush.idf.il	ET SCAN NMAP -sA (2)	2
198.52.97.84	United States	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
80.246.136.113	Israel	147.237.0.19	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
197.32.72.114	Egypt	147.237.77.216	dover.idf.il	SQL Injection - Select From	2
66.249.64.244	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
93.174.93.100	Netherlands	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
66.249.64.156	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
138.186.94.157		147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
113.236.12.103	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	2
93.174.93.100	Netherlands	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	2
93.174.93.100	Netherlands	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	2
66.249.64.143	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
113.236.12.103	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	2
200.219.249.89	Brazil	147.237.77.216	dover.idf.il	SQL 1 = 1 - possible sql injection attempt	2
197.32.72.114	Egypt	147.237.77.216	dover.idf.il	ET SCAN w3af Scan In Progress ARGENTINA Req Method	2
37.236.200.7	Iraq	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	2
93.174.93.100	Netherlands	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	2
203.115.93.156	India	147.237.8.27	e.madim.atal.idf.i	ET SCAN Potential SSH Scan	2
93.174.93.100	Netherlands	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	2

08-28-2015-00:00:08 to 08-29-2015-00:00:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
141.0.13.171	Norway	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9491
195.93.21.33	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6029
213.151.38.180	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3217
82.81.3.158	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1759
213.204.103.36	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1406
82.145.223.129	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1268
37.26.148.252	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1233
82.166.23.108	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1124
79.176.5.11	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	897
84.229.146.175	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	867
77.127.217.157	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	801
155.140.133.214	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	729
81.218.143.81	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	721
5.255.253.19	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	702
46.117.195.124	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	637
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	610
98.124.175.5	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	592
79.177.109.95	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	570
208.109.97.62	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	546
5.245.162.11	Saudi Arabia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	536
192.249.64.249	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	509
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	478
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	474
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	457
109.160.237.58	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	452
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	442
68.180.228.112	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	417
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	406
176.224.20.21	Saudi Arabia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	405
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	396
185.4.252.171	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	394
208.109.97.62	United States	147.237.77.216	dover.idf.i	SAM rule	drop	drop	388
179.190.17.138	Brazil	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	377
37.26.149.137	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	320
46.19.85.123	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	305
37.231.50.93	Kuwait	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	293
85.65.150.182	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	288
95.175.78.117	Kuwait	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	288
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	286
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	286
54.187.55.213	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	280
46.19.86.145	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	276
2.54.147.0	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	275
41.33.231.86	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	266
2.54.14.175	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	260
46.19.86.98	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	259
109.67.140.7	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	250
217.169.229.157	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	242
98.124.175.142	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	227
197.32.72.114	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	208

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
87.69.242.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4644
37.8.112.7	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/undefined	Block	4262
109.253.133.23	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.133.23	Block	2163
46.120.244.225	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.120.244.225	Block	1498
80.246.136.62	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 80.246.136.62	Block	996
80.246.136.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	804
2.52.55.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	696
85.64.156.198	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 85.64.156.198	Block	690
85.250.208.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	606
46.19.86.28	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.28	Block	392
46.19.85.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	372
93.173.156.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	348
82.102.237.187	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/undefined	Block	342
77.127.224.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	294
149.88.192.12	United States	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	168
95.86.112.114	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 95.86.112.114	Block	108
109.64.39.183	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.64.39.183	Block	102
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.173	Block	96
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	96
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	96
46.19.86.101	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.101	Block	84
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.178	Block	78
193.201.224.126	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 193.201.224.126	Block	72
89.138.216.247	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	72
66.249.64.154	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	66
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	60
167.114.172.229	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	60
66.249.78.27	Israel	147.237.0.16	my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	54
91.200.12.49	Ukraine	147.237.77.216	dover.idf.il	PHP Attempt	Block	48
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.168	Block	48
66.249.78.13	Israel	147.237.0.16	my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	48
91.200.12.49	Ukraine	147.237.77.176	matpash.idf.il	PHP Attempt	Block	48
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	48
157.55.39.93	United States	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on tikshuv.idf.il/main/giyus/giyus/general.aspx	Block	48
66.249.64.212	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	48
66.249.78.20	Israel	147.237.0.16	my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	48
91.200.12.49	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 91.200.12.49	Block	42
91.200.12.49	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 91.200.12.49	Block	42
213.204.103.36	Lebanon	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/901-8504/tikshuv.aspx	Block	36
87.98.217.58	France	147.237.77.170	maarachot.idf.il	Distributed Suspicious Response Code	Block	36
176.13.5.85	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	36
85.64.168.195	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/homepage/homepage.aspx	Block	30
85.10.220.65	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.10.220.65	Block	30
88.208.252.224	United Kingdom	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 88.208.252.224	Block	30
37.142.68.119	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	30
192.116.102.74	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	30
85.64.168.195	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 85.64.168.195	Block	30
89.139.177.124	Israel	147.237.0.16	my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	24
41.238.216.37	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	24
82.166.23.99	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	24

08-28-2015-00:00:08 to 08-29-2015-00:00:08