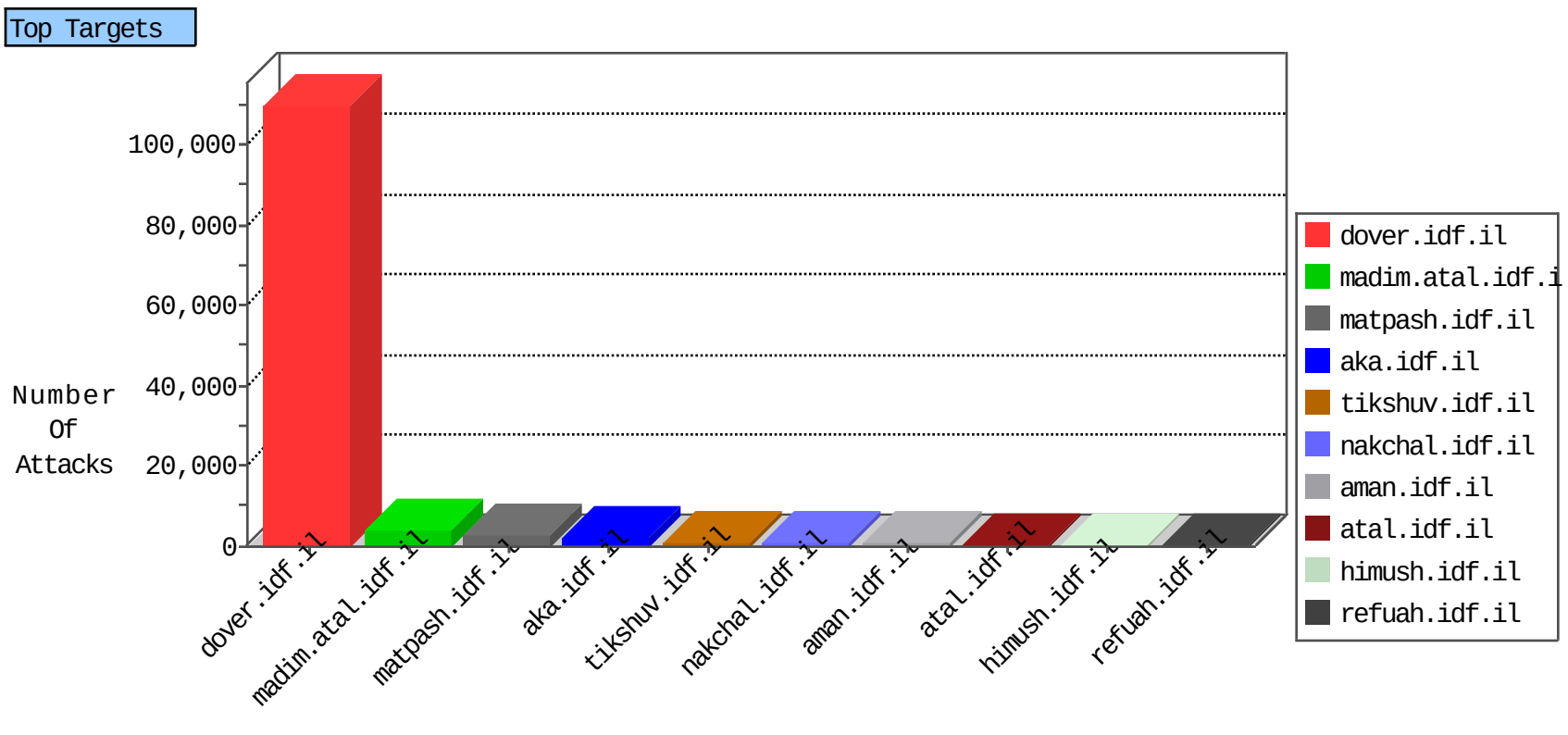
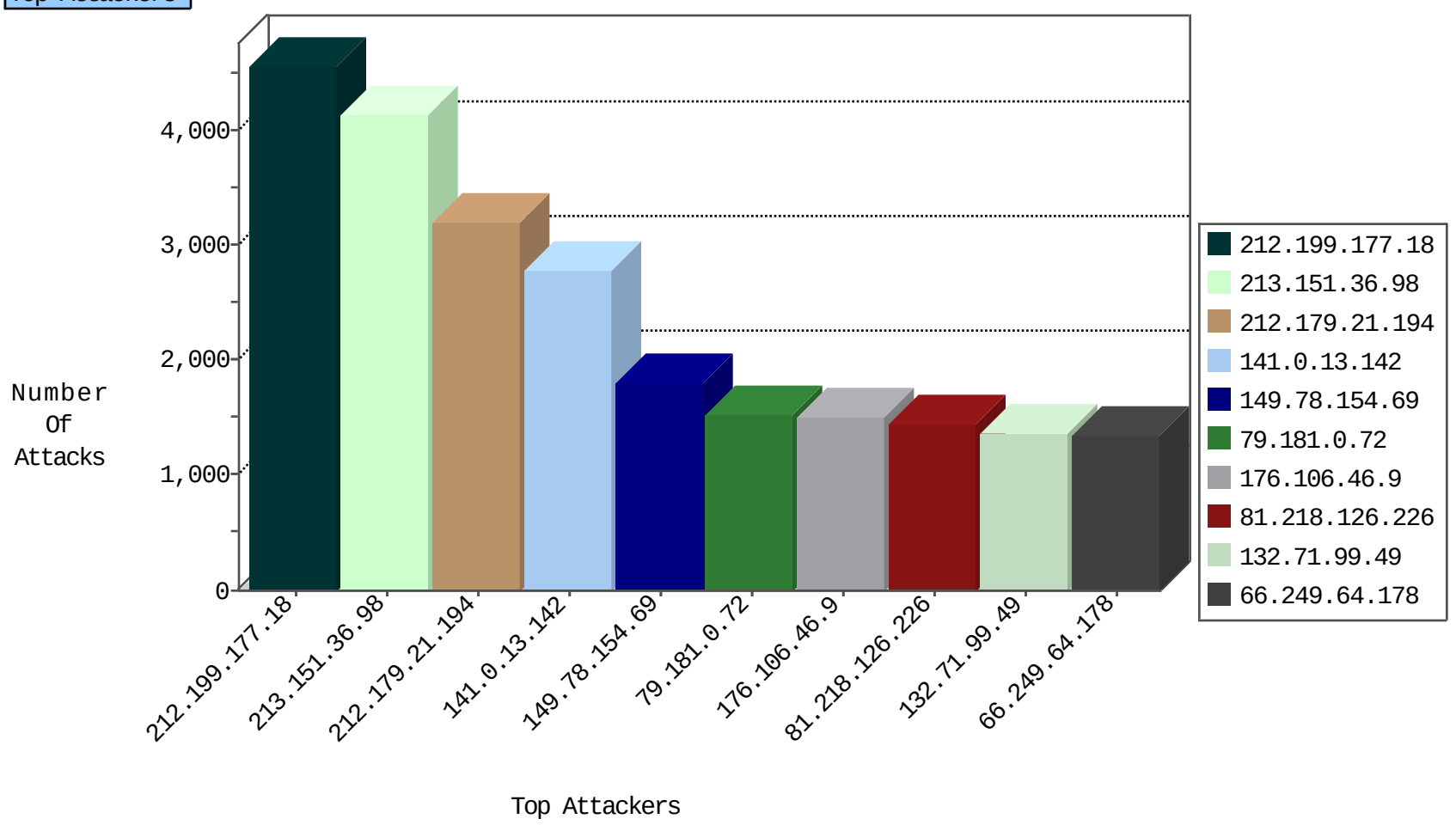
07-08-2015-00:00:00 to 07-09-2015-00:00:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



07-08-2015-00:00:00 to 07-09-2015-00:00:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
149.78.154.69	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5521
109.66.5.233	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	5198
81.218.126.226	Israel	147.237.76.31	nakchal.idf.il	TCP Scan (vertical)	drop	3584
95.211.211.182	Netherlands	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2783
192.117.173.158	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2651
132.71.99.49	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2602
66.249.78.2	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2562
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1396
81.218.126.226	Israel	147.237.76.31	nakchal.idf.il	JLM_Purple_Con_Limit_Tcp	drop	618
213.8.71.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	513
77.127.127.20	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	317
87.68.89.65	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	310
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	307
82.166.137.19	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	301
79.182.15.177	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	286
213.57.154.35	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	279
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	269
188.120.148.222	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	226
87.69.228.193	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	224
46.120.17.162	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	219
79.181.1.16	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	207
94.159.209.161	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	201
37.60.40.6	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	195
84.109.179.179	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	193
79.176.35.36	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	189
82.80.165.174	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	174
79.177.29.212	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	172
77.125.214.79	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	170
149.78.47.155	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	169
87.69.231.160	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	167
31.168.26.232	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	167
46.116.185.146	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	162
204.13.200.28	United States	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	forward	160
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	156
84.111.36.76	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	149
212.143.173.198	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	146
2.54.149.106	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	142
84.228.193.62	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	142
212.25.102.57	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	125
66.249.93.219	Israel	147.237.77.234	halag.idf.il	TCP handshake violation, first packet not syn	drop	114
80.246.136.197	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	110
80.230.80.93	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	106
85.64.100.128	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	102
185.32.178.127	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	98
46.121.116.17	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	97
46.121.102.202	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90
87.69.169.108	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90
46.19.86.170	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	88
2.52.28.206	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	87
2.54.13.70	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	86

07-08-2015-00:00:00 to 07-09-2015-00:00:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
192.118.30.102	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	26
109.226.20.135	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	19
45.79.214.25		147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	11
80.178.146.128	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
5.29.241.217	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
173.85.193.130	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
173.228.91.207	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
84.228.33.67	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
84.109.125.163	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
46.19.85.187	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
109.66.5.233	Israel	147.237.77.216	dover.idf.il	8262: HTTP: Slowloris DoS Tool	Block	5
87.68.97.93	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
89.19.29.90	Turkey	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
46.19.85.194	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.135	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
79.177.160.173	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
87.68.93.23	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.156	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
77.127.171.12	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
184.74.177.94	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.109	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
94.159.151.22	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
5.11.40.99	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
212.179.55.126	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
37.26.148.196	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
84.94.17.201	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
87.69.219.33	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
103.228.1.242		147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
23.253.20.54	United States	147.237.77.216	dover.idf.il	C104: HTTP: Access to - pageinfo.php	Block	3
89.19.29.90	Turkey	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	3
37.142.8.140	Israel	147.237.0.15	kosher-kravi.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
79.180.119.140	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
31.168.171.81	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
212.25.67.206	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.19.85.94	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.38	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
37.142.8.140	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.63	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.165	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
89.138.242.1	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
62.90.131.110	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
37.142.159.55	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.19.85.201	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
80.179.223.31	Israel	147.237.77.176	matpash.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.19.85.66	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.177	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
109.65.135.234	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
91.240.235.225	Israel	147.237.0.34	tikshuv.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
62.128.41.103	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	2

07-08-2015-00:00:00 to 07-09-2015-00:00:00

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	131
66.249.67.53	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	3
221.203.3.117	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	3
221.203.3.117	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	2
59.106.108.116	Japan	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.64.247	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.102.6.171	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
89.248.172.154	Netherlands	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	2
193.107.16.206	Russian Federation	147.237.72.166	aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	2
113.240.250.156	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	2
176.13.19.202	Israel	147.237.77.233	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
218.65.30.107	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
221.203.3.117	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2
176.13.16.37	Israel	147.237.76.30	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
218.65.30.107	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	2
221.203.3.117	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	2
79.179.206.101	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
199.203.59.121	Israel	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	2
221.203.3.117	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	2
221.203.3.117	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	2
218.87.111.107	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	2
66.249.64.156	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
218.87.111.107	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	2
221.203.3.117	China	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	2
193.107.16.206	Russian Federation	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 1024	2
221.203.3.117	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	2
218.65.30.107	China	147.237.76.39	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	2
66.249.93.247	United States	147.237.76.30	himush.idf.il	ET SCAN NMAP -sA (2)	2
54.209.60.63	United States	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
66.249.78.153	United States	147.237.72.166	aka.idf.il	ET SCAN NMAP -sA (2)	2
212.179.21.194	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
218.65.30.107	China	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	2
61.183.128.6	China	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.67.65	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
41.189.87.43	South Africa	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
124.29.219.218	Pakistan	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 4096	1
103.232.35.234		147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 3072	1
81.200.91.2	Russian Federation	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 3072	1
217.74.47.7	Russian Federation	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
177.22.79.1	Brazil	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 4096	1
2.54.20.173	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
110.153.8.116	China	147.237.76.31	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.121.242.209	France	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.111.107	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.74	United States	147.237.77.216	dover.idf.il	ET DROP Dshield Block Listed Source	1
79.176.128.24	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
210.61.150.154	Taiwan	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 3072	1
46.130.112.242	Armenia	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 3072	1
167.88.43.110		147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
107.179.95.29	United States	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1

07-08-2015-00:00:00 to 07-09-2015-00:00:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.199.177.18	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4567
213.151.36.98	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4138
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3138
141.0.13.142	Norway	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2794
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1805
79.181.0.72	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1521
176.106.46.9	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	1498
132.71.99.49	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1356
46.19.85.108	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1324
79.180.199.127	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1302
141.0.14.244	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1298
2.54.49.158	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1131
190.229.72.124	Argentina	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1022
79.182.167.247	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	996
2.52.179.14	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	965
95.86.99.246	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	934
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	852
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	835
95.86.114.217	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	816
194.114.146.227	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	725
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	697
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	680
67.6.171.212	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	675
60.229.48.54	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	675
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	660
79.180.162.35	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	630
2.54.30.44	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	604
68.180.229.51	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	604
72.9.148.10	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	596
95.211.211.182	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	569
54.187.55.213	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	566
109.186.0.186	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	553
66.249.64.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	548
37.238.164.83	Iraq	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	543
66.249.64.178	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	532
66.249.64.168	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	530
46.19.86.36	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	530
89.138.254.183	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	510
84.109.146.129	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	492
192.157.10.100	Sweden	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	456
81.218.126.226	Israel	147.237.0.34	tikshuv.idf.il	illegal header format detected: Malformed HTTP format in request	Block HTTP Non Compliant	monitor	444
115.188.131.254	New Zealand	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	426
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	422
46.19.86.238	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	407
149.101.1.117	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	407
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	383
66.249.64.178	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	379
66.249.64.173	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	372
46.19.85.30	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	356
66.249.64.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	354

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
37.26.147.241	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.147.241	Block	453
176.13.0.114	Israel	147.237.76.30	himush.idf.il	Distributed Suspicious Response Code	Block	450
185.32.178.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	353
46.19.86.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	302
176.12.136.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	262
2.54.38.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	255
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.178	Block	251
176.13.15.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	244
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.168	Block	230
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.173	Block	210
37.26.147.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	192
46.19.85.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	188
46.19.85.244	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.244	Block	181
2.54.13.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	165
84.94.49.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	151
2.54.19.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	139
176.13.11.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	131
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	128
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	128
46.19.85.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	118
37.26.147.142	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.147.142	Block	117
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.59	Block	110
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	108
213.151.32.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	105
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.53	Block	101
192.117.155.134	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	100
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.65	Block	93
185.32.178.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	73
213.151.38.144	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (404) in Session from 213.151.38.144	Block	70
2.54.149.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	69
46.19.85.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	62
2.54.18.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	47
2.54.42.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	46
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	46
37.26.146.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	44
176.13.13.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	41
2.52.176.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	32
194.90.66.15	Israel	147.237.76.31	nakchal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	27
2.54.181.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	22
176.12.137.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	21
109.253.140.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	20
2.52.145.227	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.52.145.227	Block	18
109.64.144.83	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.64.144.83	Block	16
23.239.208.33	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 23.239.208.33	Block	16
37.26.147.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	14
81.17.16.247	Switzerland	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	12
46.120.106.57	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	10
116.212.127.209	Hong Kong	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	10
27.126.188.85	Hong Kong	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	10
176.232.209.158	Turkey	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	9