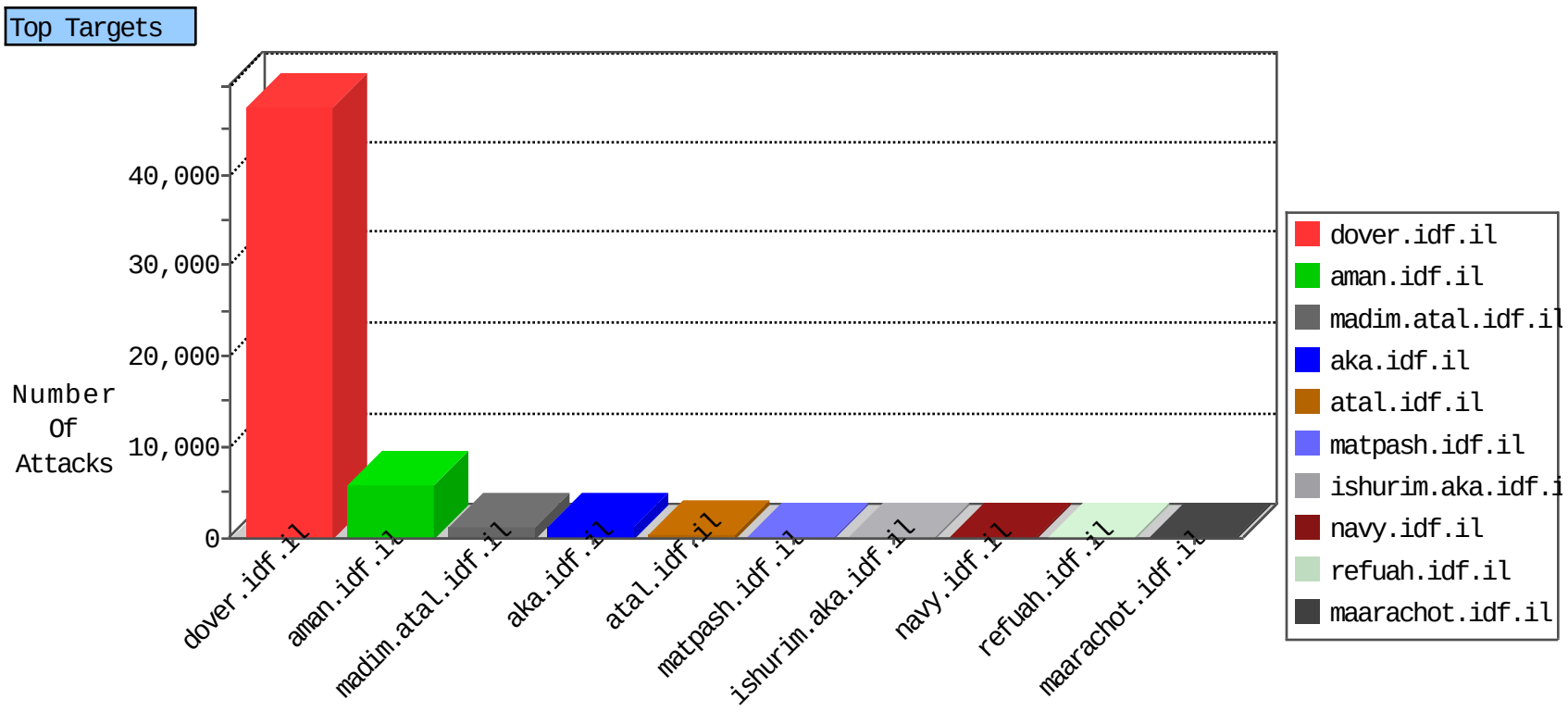
07-18-2015-00:00:09 to 07-19-2015-00:00:09

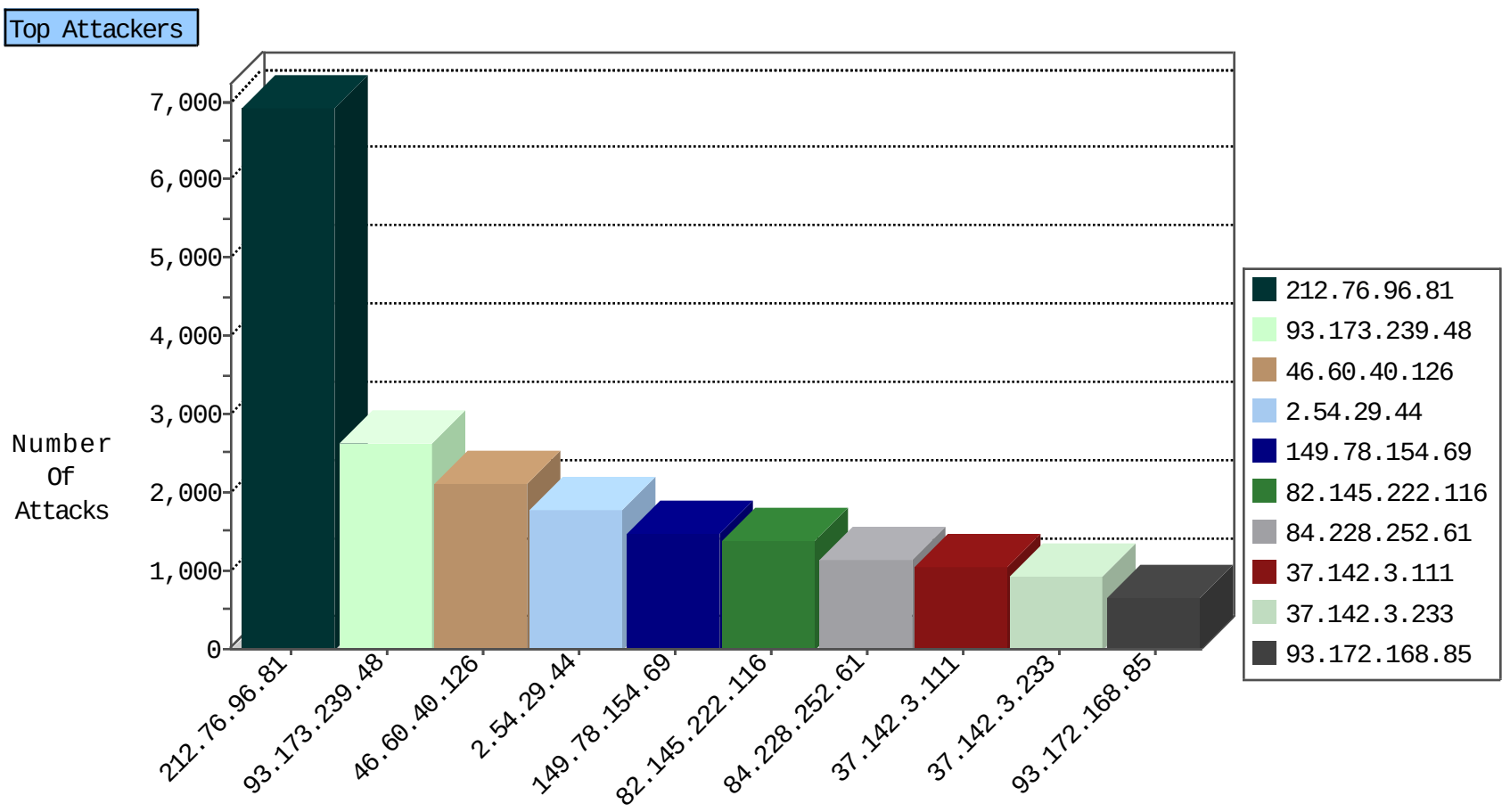
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

07-18-2015-00:00:09 to 07-19-2015-00:00:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.64.151	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	12159
104.236.162.87		147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	9426
192.249.64.249	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9388
66.249.81.215	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5994
66.249.81.212	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5882
54.72.0.55	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5769
66.249.93.166	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3398
66.249.78.153	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1476
84.108.105.50	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	875
79.177.130.41	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	676
66.249.64.143	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	627
66.249.78.95	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	485
89.138.218.146	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	418
84.109.243.107	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	390
79.181.108.174	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	352
79.179.189.154	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	318
80.178.251.210	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	318
213.57.160.97	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	292
31.154.154.50	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	291
79.178.169.187	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	268
5.29.112.141	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	267
84.228.203.52	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	256
87.68.68.190	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	231
79.182.5.185	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	217
109.65.99.186	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	216
5.28.187.73	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	211
87.68.16.132	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	198
109.64.200.242	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	197
213.57.37.250	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	186
109.64.177.177	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	171
31.210.179.153	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	164
5.22.130.245	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	154
149.88.69.214	United States	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	153
79.183.25.184	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	152
149.78.58.86	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	144
37.142.115.72	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	143
46.121.102.202	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	138
84.111.234.21	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	135
46.121.111.163	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	121
93.172.170.158	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	118
79.179.142.122	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	117
5.29.34.163	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	114
79.182.23.38	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	108
79.181.176.189	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	107
85.64.85.32	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	106
84.109.17.205	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	101
84.110.60.131	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	100
89.139.55.0	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	85
176.13.7.11	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	79
213.57.172.65	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	79

07-18-2015-00:00:09 to 07-19-2015-00:00:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.120.4.235	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	38
194.114.146.227	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	18
174.36.80.49	United States	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	16
174.36.80.49	United States	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
119.187.133.82	China	147.237.72.166	aka.idf.il	8479: HTTP: Suspicious HTTP Request	Permit	8
87.68.41.65	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
192.116.94.74	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
79.177.180.2	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
89.139.184.254	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
149.88.82.2	United States	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
37.142.115.72	Israel	147.237.72.167	ishurim.aka.idf.i	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
202.129.228.226	Fiji	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
212.97.133.238	Denmark	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
188.165.246.177	France	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
109.67.55.155	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
195.70.122.50	Austria	147.237.77.170	maarachot.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	4
212.97.133.238	Denmark	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
188.165.246.177	France	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
189.38.90.144	Brazil	147.237.77.216	dover.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	4
179.66.237.147	Brazil	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
81.196.244.23	Romania	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
37.76.204.82	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
38.124.248.66	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.117.237.74	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
167.57.110.11		147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
188.161.184.86	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
79.181.51.164	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
79.176.9.76	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.117	Israel	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
37.76.204.82	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
85.65.19.45	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
66.96.128.60	United States	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	2
87.69.88.122	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
109.67.137.81	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
93.172.17.59	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
81.196.244.23	Romania	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
84.109.235.122	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
62.128.41.103	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
165.215.209.15	United States	147.237.77.216	dover.idf.il	14511: HTTP: Win32/Oliga Fake User Agent	Block	1
79.183.14.158	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.19.85.231	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
109.186.63.226	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
94.127.33.68	Sweden	147.237.77.74	law.idf.il	3809: HTTP: SQL Injection Evasion SQL Comment Terminator	Block	1
198.100.144.83	Canada	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
5.22.130.27	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
66.188.84.181	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
130.235.252.1	Sweden	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
79.180.189.151	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
216.249.102.195	United States	147.237.77.74	law.idf.il	3809: HTTP: SQL Injection Evasion SQL Comment Terminator	Block	1
46.19.85.71	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

07-18-2015-00:00:09 to 07-19-2015-00:00:09

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
46.60.40.126	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2112
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	108
77.126.255.235	Israel	147.237.72.166	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	12
195.70.122.50	Austria	147.237.77.170	maarachot.idf.il	Tehila - Perl LWP with fake user agent	8
189.38.90.144	Brazil	147.237.77.216	dover.idf.il	SQL Injection - Select From	8
176.31.250.110	France	147.237.77.176	matpash.idf.il	Tehila - Perl LWP with fake user agent	5
176.31.250.110	France	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
176.31.250.110	France	147.237.77.74	law.idf.il	Tehila - Perl LWP with fake user agent	4
54.163.196.59	United States	147.237.76.30	himush.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	4
189.38.90.144	Brazil	147.237.77.216	dover.idf.il	ET WEB_SERVER SQLi - SELECT and sysobject	4
66.249.65.132	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	4
176.13.12.179	Israel	147.237.77.170	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
189.38.90.144	Brazil	147.237.77.216	dover.idf.il	ET WEB_SERVER ATTACKER SQLi - SELECT and Schema Columns	4
218.87.111.107	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	4
50.17.33.67	United States	147.237.77.234	halag.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	3
94.23.78.16	Portugal	147.237.77.176	matpash.idf.il	Tehila - Perl LWP with fake user agent	3
119.187.133.82	China	147.237.72.166	aka.idf.il	ET WEB_SERVER HTTP POST Generic eval of base64_decode	3
104.236.162.87		147.237.77.216	dover.idf.il	SERVER-WEBAPP login.htm access	3
94.23.78.16	Portugal	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
91.218.114.189	Russian Federation	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.64.161	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
78.157.207.29	United Kingdom	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
93.189.25.174	Austria	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 1024	2
61.183.128.6	China	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 1024	2
218.87.111.107	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	2
221.203.3.117	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	2
85.113.122.209	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
218.87.111.107	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	2
5.39.216.121	Netherlands	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 1024	2
203.158.230.124	Thailand	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 2048	2
203.158.230.124	Thailand	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -f -sS	2
218.65.30.107	China	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	2
61.149.161.186	China	147.237.8.28	e.mobile-ks.idf.il	GPL SCAN nmap TCP	2
218.87.111.107	China	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	2
221.203.3.117	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	2
66.249.81.201	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	2
218.87.111.107	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	2
62.219.83.119	Israel	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 4096	2
89.248.174.100	Netherlands	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 1024	2
218.87.111.107	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	2
218.65.30.107	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	2
218.87.111.107	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
109.237.26.139	United Kingdom	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	2
218.65.30.107	China	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	2
203.158.230.124	Thailand	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	2
62.210.251.69	France	147.237.77.216	dover.idf.il	SERVER-WEBAPP Mambo upload.php access	2
199.203.59.121	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
162.253.67.218	United States	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	2
218.87.111.107	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	2

07-18-2015-00:00:09 to 07-19-2015-00:00:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.76.96.81	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6933
93.173.239.48	Israel	147.237.72.156	aman.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	2633
2.54.29.44	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1758
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1462
82.145.222.116	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1367
84.228.252.61	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1137
37.142.3.111	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1036
37.142.3.233	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	942
93.172.168.85	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	664
82.145.221.15	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	628
82.166.22.13	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	492
170.218.219.21	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	478
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	449
192.249.64.249	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	351
66.249.69.26	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	339
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	332
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	329
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	321
92.40.249.138	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	301
66.249.69.34	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	290
85.250.247.37	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	268
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	259
69.41.14.215	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	258
66.249.69.42	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	250
66.87.79.205	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	247
195.34.150.18	Austria	147.237.77.216	dover.idf.i	SAM rule	drop	drop	238
46.19.85.83	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	225
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	222
37.142.1.108	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	219
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	210
69.41.14.159	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	207
2.54.2.6	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	199
5.108.129.44	Saudi Arabia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	196
188.165.15.193	France	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	189
41.33.231.86	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	183
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	178
66.249.81.215	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	177
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	170
41.68.41.232	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	168
66.249.81.212	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	165
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	162
66.249.81.218	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	159
46.19.86.152	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	156
203.135.187.11	Australia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	150
212.199.182.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	146
207.46.13.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	136
157.55.39.180	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	136
77.126.73.83	Israel	147.237.72.156	aman.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	135
157.55.39.86	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	134
87.68.64.193	Israel	147.237.72.156	aman.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	133

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
5.29.73.125	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 5.29.73.125	Block	434
213.57.243.152	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 213.57.243.152	Block	401
109.65.167.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	144
66.249.69.42	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.42	Block	107
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	105
66.249.69.34	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.34	Block	103
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	44
149.88.63.209	United States	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	42
115.78.235.170	Vietnam	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	41
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	30
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	27
176.12.144.22	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.144.22	Block	24
79.180.200.65	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	21
79.176.198.248	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.176.198.248	Block	20
79.183.136.214	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/kamlar/styles/import/bottomnavigaton.asp	Block	12
31.186.228.94	United Kingdom	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	11
183.79.221.129	Japan	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 183.79.221.129	Block	11
31.186.228.58	United Kingdom	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	11
188.165.15.193	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.193	Block	10
31.186.228.32	United Kingdom	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	9
119.187.133.82	China	147.237.72.166	aka.idf.il	PHP Attempt	Block	8
208.115.111.73	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 208.115.111.73	Block	8
204.12.251.37	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/default.aspx	Block	8
31.186.228.31	United Kingdom	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	8
80.178.6.46	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
84.228.80.192	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	6
31.186.228.29	United Kingdom	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	6
46.43.125.149	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	6
31.186.228.95	United Kingdom	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	6
31.186.228.30	United Kingdom	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	6
216.69.245.101	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	6
31.186.228.96	United Kingdom	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	6
46.119.112.178	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17155-en/	Block	6
89.139.7.107	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 89.139.7.107	Block	6
108.178.202.110	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	6
31.186.228.93	United Kingdom	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	6
109.64.222.100	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	6
37.142.152.207	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 37.142.152.207	Block	5
79.170.44.126	United Kingdom	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 79.170.44.126	Block	5
123.126.113.80	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	5
176.13.20.207	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	5
84.228.250.44	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
31.186.228.57	United Kingdom	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4
109.67.101.171	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
216.244.82.234	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/yohalan/main/main.asp/trackback/	Block	4
5.29.96.128	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
37.26.148.230	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	4
46.116.77.60	Israel	147.237.0.16	my-kosher-kravi.idf.il	Parameter Type Violation Master$ContentPlaceHolder1$password in my-kosher-kravi.idf.il/templates/login/login.aspx	Block	4
46.19.86.112	Israel	147.237.76.39	mobile.meitav.idf.il	Cookie Tampering on cookie .ASPNETAUTH: Expected 0102F27C09AAAE8FD208FEF2F44A75B18FD20800093300310035003300310035003000320038000012F00FF, Observed 01026C2EDF452586D208FE6CA620112886D20800093300310035003300310035003000320038000012F00FF	None	4
5.29.96.216	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	4