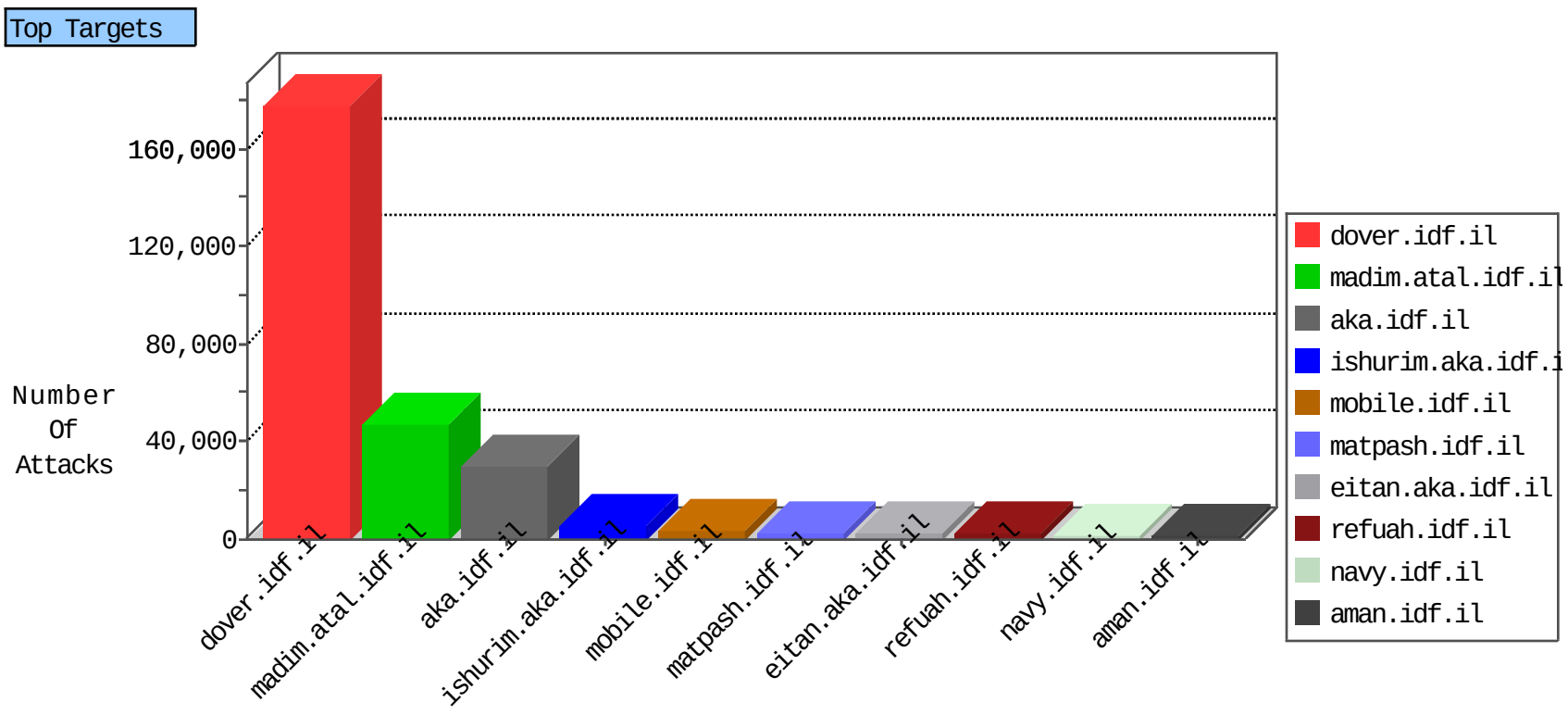
10-06-2015-00:00:04 to 10-07-2015-00:00:04

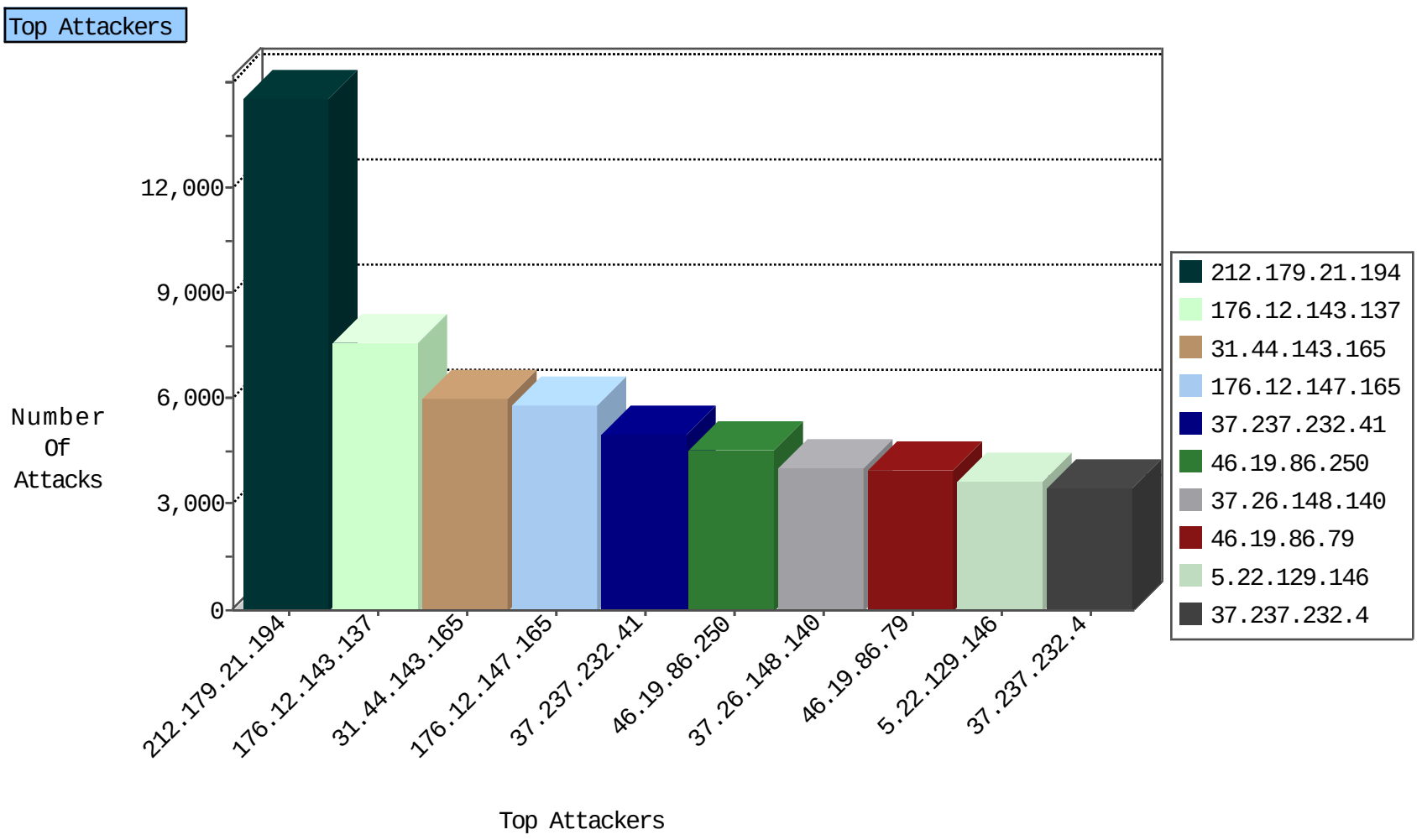
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

10-06-2015-00:00:04 to 10-07-2015-00:00:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.229.164.101	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3645
5.57.6.26	Lebanon	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3149
66.249.67.93	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2705
66.249.67.45	United States	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	2525
138.106.57.131	Sweden	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1165
41.249.5.96	Morocco	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	886
37.237.232.17	Iraq	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	807
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	791
37.237.232.4	Iraq	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	717
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	679
37.237.232.15	Iraq	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	576
66.249.67.122	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	489
66.249.67.143	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	419
66.249.67.251	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	311
66.249.67.6	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	252
41.68.179.104	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	185
168.235.200.56	United States	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	164
46.19.86.11	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	159
168.235.194.95	United States	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	152
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	148
2.54.154.237	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	145
79.177.154.120	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	138
185.32.179.111	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	123
68.180.228.112	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	122
2.54.31.124	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	116
46.19.86.150	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	116
93.173.16.15	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	113
2.52.164.206	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	113
84.228.10.120	Israel	147.237.77.243	mobile.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	111
2.54.39.106	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	107
2.52.61.55	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	97
46.19.85.40	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	95
46.19.85.2	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	91
109.66.128.107	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	83
109.160.217.252	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	83
87.68.20.233	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	72
46.19.85.132	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	71
37.26.149.247	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	71
195.160.240.11	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	71
37.237.232.12	Iraq	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	69
2.54.143.7	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	63
109.186.16.29	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	61
2.54.147.182	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	59
87.68.16.84	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	59
185.13.195.138	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	59
81.218.195.167	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	58
80.246.137.179	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	58
2.54.129.18	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	58
79.180.98.179	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	57
185.32.179.165	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	57

10-06-2015-00:00:04 to 10-07-2015-00:00:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.237.232.39	Iraq	147.237.77.216	dover.idf.il	C091: HTTP: Access to - admin.asp	Block	52
212.199.244.112	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	9
212.199.224.24	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
82.80.26.75	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
194.90.140.29	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
216.185.43.135	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
212.150.66.161	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
79.181.123.8	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
204.93.156.141	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
37.237.232.37	Iraq	147.237.77.216	dover.idf.il	C091: HTTP: Access to - admin.asp	Block	4
212.199.205.68	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
77.242.124.2	Netherlands	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
64.186.146.196	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
8.8.246.60	United States	147.237.0.34	tikshuv.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	3
46.121.132.155	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
178.210.160.50	Turkey	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	3
77.125.97.125	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
79.180.33.85	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
157.150.193.5	United States	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
37.237.232.40	Iraq	147.237.77.216	dover.idf.il	C091: HTTP: Access to - admin.asp	Block	2
79.181.210.37	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
62.219.114.170	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
109.66.142.87	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
31.168.1.54	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
64.87.23.55	United States	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	2
37.237.232.128	Iraq	147.237.77.216	dover.idf.il	C091: HTTP: Access to - admin.asp	Block	2
85.64.58.16	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
50.97.138.113	United States	147.237.76.86	navy.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	2
94.188.161.145	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
87.68.145.47	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.117.250.161	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
87.69.0.7	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
78.68.122.91	Sweden	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
62.210.152.89	France	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
94.245.88.231	United Kingdom	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	1
216.185.43.135	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
69.30.221.250	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
198.20.70.114	United States	147.237.77.179	e.mazi.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
106.38.241.118	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
46.118.155.216	Ukraine	147.237.77.74	law.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
87.106.179.116	Germany	147.237.77.216	dover.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	1
31.154.161.188	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
79.133.113.177	Russian Federation	147.237.77.216	dover.idf.il	12580: HTTP: SQL Injection (Cookie Header)	Block	1
176.12.141.159	Israel	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
37.237.232.46	Iraq	147.237.77.216	dover.idf.il	C091: HTTP: Access to - admin.asp	Block	1
94.245.88.231	United Kingdom	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
69.197.177.26	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
94.23.252.53	France	147.237.77.176	matpash.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	1
213.8.145.99	Israel	147.237.76.31	nakchal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	1
79.179.110.33	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

10-06-2015-00:00:04 to 10-07-2015-00:00:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	82
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	65
205.214.237.90	147.237.72.166	United States	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	22
2.91.164.61	147.237.77.216	Saudi Arabia	dover.idf.il	Admin login page scan - Havij	18
87.106.179.116	147.237.77.216	Germany	dover.idf.il	SQL Injection - Select From	14
46.19.85.229	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	11
216.185.43.135	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	9
178.210.160.50	147.237.72.166	Turkey	aka.idf.il	SQL Injection - Select From	8
64.186.146.196	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
66.249.67.13	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	6
66.249.64.146	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	6
64.87.23.55	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	6
213.8.145.99	147.237.76.31	Israel	nakchal.idf.il	SQL Injection - Select From	6
204.93.156.141	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
94.245.88.231	147.237.77.74	United Kingdom	law.idf.il	SQL Injection - Select From	5
50.97.138.113	147.237.76.86	United States	navy.idf.il	SQL Injection - Select From	5
204.12.168.26	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	5
8.8.246.60	147.237.0.34	United States	tikshuv.idf.il	SQL Injection - Select From	5
2.91.164.61	147.237.77.216	Saudi Arabia	dover.idf.il	SERVER-WEBAPP adminlogin access	5
77.242.124.2	147.237.77.74	Netherlands	law.idf.il	SQL Injection - Select From	4
2.91.164.61	147.237.77.216	Saudi Arabia	dover.idf.il	SERVER-WEBAPP login.htm access	4
92.44.171.58	147.237.77.216	Turkey	dover.idf.il	INDICATOR-OBFUSCATION script tag in POST parameters - likely cross-site scripting	4
176.13.10.173	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
87.106.179.116	147.237.77.216	Germany	dover.idf.il	ET WEB_SERVER SQLi - SELECT and sysobject	4
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	3
218.87.111.117	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	3
66.249.67.122	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	3
2.91.164.61	147.237.77.216	Saudi Arabia	dover.idf.il	SERVER-WEBAPP admin.php access	3
218.65.30.23	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	3
31.184.242.17	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	3
218.87.111.117	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	2
188.138.9.51	147.237.8.24	Germany	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	2
218.87.111.117	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	2
66.249.78.161	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
82.166.22.82	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
66.249.67.251	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
218.87.111.117	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	2
218.87.111.117	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
146.0.36.43	147.237.0.34	Germany	tikshuv.idf.il	ET SCAN Potential SSH Scan	2
218.87.111.117	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	2
66.249.67.67	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
218.65.30.23	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	2
218.87.111.117	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	2
188.138.9.51	147.237.77.226	Germany	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	2
218.65.30.23	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	2
218.87.111.117	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	2
218.65.30.23	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	2
218.87.111.117	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	2
218.87.111.117	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	2
176.13.21.66	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2

10-06-2015-00:00:04 to 10-07-2015-00:00:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14264
31.44.143.165	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6021
37.237.232.41	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4986
37.237.232.4	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3450
46.120.101.164	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2862
37.237.232.39	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2670
79.181.9.146	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2415
37.237.232.15	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2396
37.237.232.47	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2390
37.237.232.48	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2337
37.237.232.49	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2336
185.58.201.28	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2258
95.86.120.214	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1968
109.67.36.151	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1703
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1665
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1543
37.237.232.51	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1336
37.237.232.40	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1305
37.237.232.7	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1249
37.237.232.145	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1235
2.54.22.54	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1227
37.237.232.82	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1195
37.237.232.128	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1169
37.237.232.10	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1168
37.237.232.50	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1145
37.237.232.56	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1145
37.237.232.28	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1139
37.237.232.44	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1136
37.237.232.54	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1132
37.237.232.61	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1116
37.237.232.45	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1112
37.237.232.17	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1110
192.115.248.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1098
37.237.232.112	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1081
37.237.232.30	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1074
2.54.133.73	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	992
37.237.232.115	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	982
87.68.29.143	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	978
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	970
212.76.98.240	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	963
82.145.223.120	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	875
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	838
2.54.32.154	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	835
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	833
37.237.232.97	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	789
37.237.232.132	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	788
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	782
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	763
37.237.232.12	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	756
37.237.232.123	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	730

10-06-2015-00:00:04 to 10-07-2015-00:00:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.12.143.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	7608
176.12.147.165	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.147.165	Block	5800
46.19.86.250	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4587
37.26.148.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	4073
46.19.86.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3976
5.22.129.146	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 5.22.129.146	Block	3637
37.26.148.174	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 37.26.148.174	Block	3374
46.121.107.15	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (404) in Session from 46.121.107.15	Block	3088
2.54.156.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3087
176.12.140.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2808
176.13.10.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2577
46.19.85.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1220
37.26.148.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1165
176.12.144.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	942
75.126.122.176	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	792
46.19.86.77	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.77	Block	748
62.219.164.51	Israel	147.237.76.31	nakchal.idf.il	Too Many of the Same Response Code (404) in Session from 62.219.164.51	Block	715
2.54.180.165	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.180.165	Block	671
89.138.30.150	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 89.138.30.150	Block	605
72.9.148.10	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	550
46.19.85.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	417
79.180.140.8	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (404) in Session from 79.180.140.8	Block	304
85.250.48.197	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (404) in Session from 85.250.48.197	Block	297
212.143.137.187	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	220
80.246.139.43	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 80.246.139.43	Block	220
212.25.102.57	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 212.25.102.57	Block	209
37.26.148.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	198
46.19.85.209	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	198
95.35.37.153	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	176
185.32.179.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	165
176.13.7.239	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	143
79.176.162.26	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	143
188.76.156.172	Spain	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 188.76.156.172	Block	132
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	129
188.120.133.185	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1302	Block	121
212.143.3.44	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	121
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.173	Block	120
79.178.28.216	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 79.178.28.216	None	117
157.55.39.40	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	110
71.230.86.61	United States	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	110
66.249.67.224	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	110
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	110
79.178.23.221	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	110
193.43.244.72	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	99
207.46.13.65	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	99
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	99
46.229.164.101	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.229.164.101	Block	99
66.249.67.216	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	99
212.150.126.190	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	88
212.150.126.190	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.150.126.190	Block	88

10-06-2015-00:00:04 to 10-07-2015-00:00:04