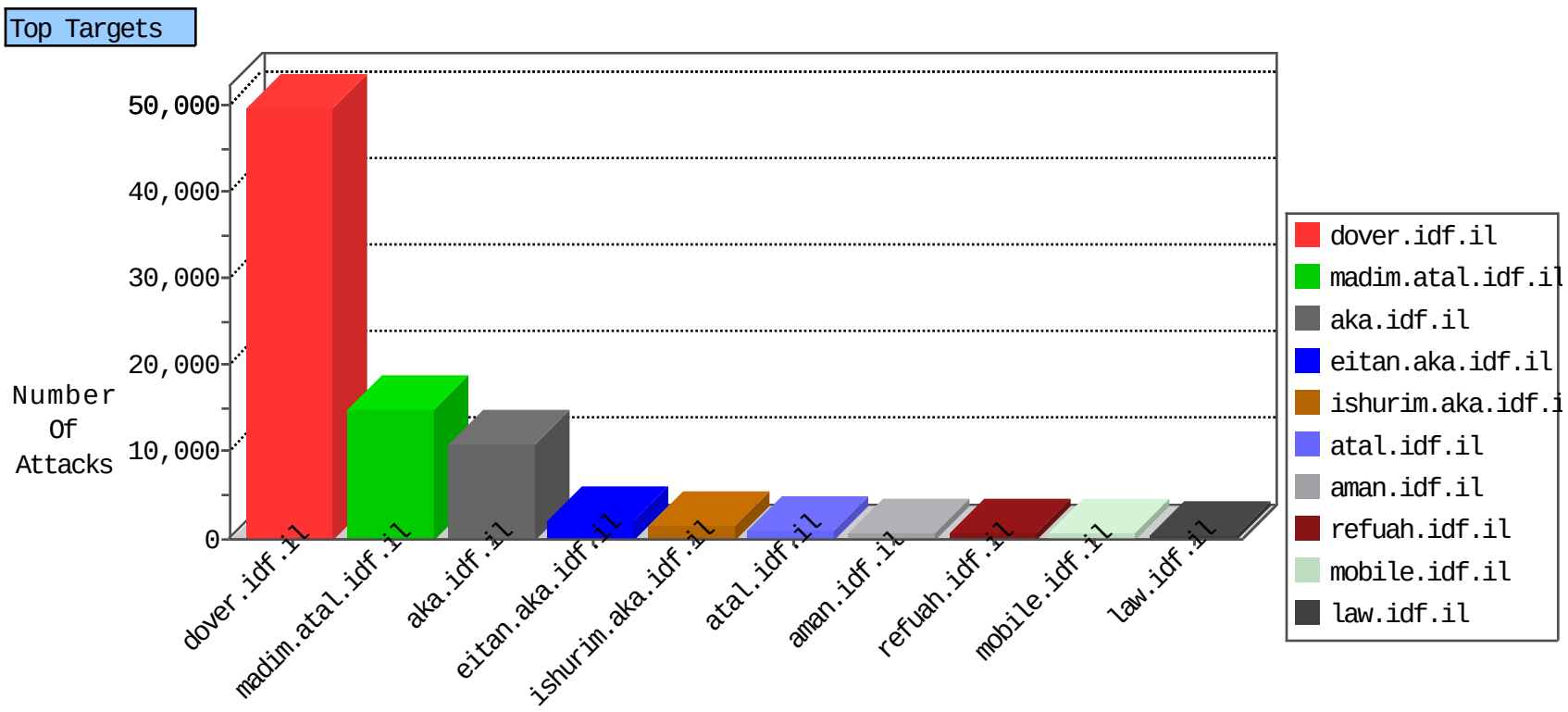
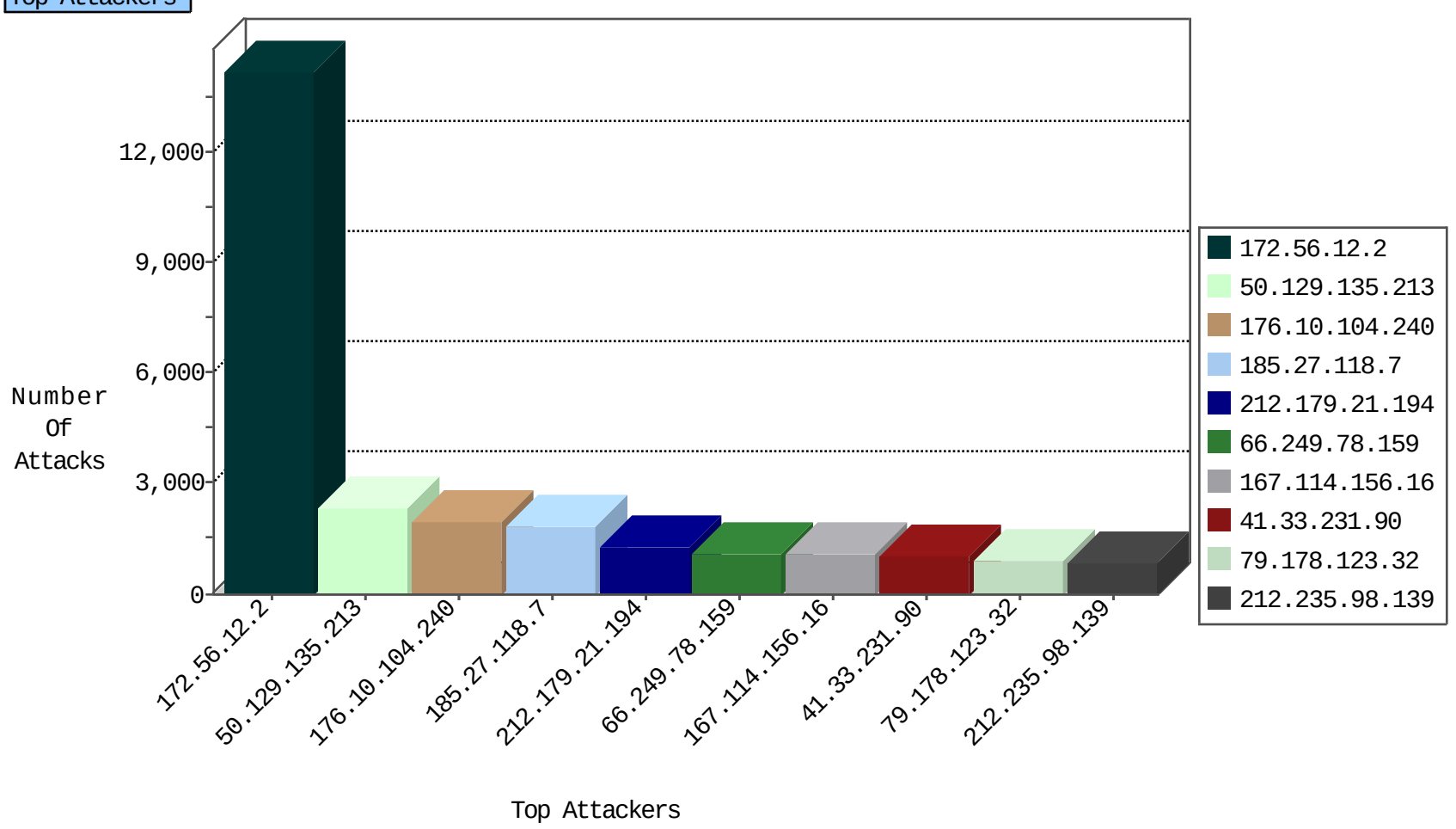
11-22-2015 to 11-23-2015

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-22-2015 to 11-23-2015

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	62509
0.0.0.0		147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	40072
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	21128
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	10225
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4685
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4078
66.249.64.190	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1889
66.249.78.159	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1772
81.218.37.2	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	412
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	403
71.230.34.237	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	269
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	245
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	201
185.27.118.7	Egypt	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	195
149.78.228.245	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	166
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	155
80.179.18.228	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	154
66.249.66.125	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	118
66.249.64.195	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	118
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	115
204.93.154.201	United States	147.237.77.216	dover.idf.il	JLM_Dover_Con_Limit_Https	drop	86
176.13.9.120	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	77
2.54.57.169	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	69
212.71.238.108	United Kingdom	147.237.77.216	dover.idf.il	JLM_Dover_Con_Limit_Https	drop	58
66.249.93.200	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	55
193.109.199.207	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	48
36.82.44.29	Indonesia	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	35
5.236.81.103	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	32
36.76.216.73	Indonesia	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	31
104.172.207.143	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	30
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	30
81.218.5.130	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	29
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	28
151.238.202.236	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	28
112.209.208.119	Philippines	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	24
84.95.86.215	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	22
190.31.135.167	Argentina	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	22
73.130.185.245	United States	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	22
46.19.85.242	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	21
112.209.208.119	Philippines	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	21
212.143.3.44	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	20
5.238.181.44	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	19
46.225.83.0	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	18
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	18
151.238.202.236	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
5.236.81.103	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	17
192.118.30.102	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	16
82.166.219.240	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	14
197.162.21.79	Egypt	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	13
5.235.219.178	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	13

11-22-2015 to 11-23-2015

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
104.47.147.196	United States	147.237.0.15	kosher-kravi.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	15
212.179.132.204	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
85.65.22.165	Israel	147.237.72.156	aman.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	8
194.114.146.227	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
183.171.21.74	Malaysia	147.237.77.216	dover.idf.il	12634: HTTP: JS LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	6
104.47.147.196	United States	147.237.0.19	madim.atal.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
209.88.198.1	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
91.193.51.30	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
81.218.57.242	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
79.181.107.65	Israel	147.237.77.176	matpash.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	4
104.47.147.196	United States	147.237.0.15	kosher-kravi.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	3
109.67.138.10	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
79.179.176.46	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
79.182.166.103	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
94.188.161.145	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
105.155.75.73	Morocco	147.237.77.216	dover.idf.il	12026: HTTP: LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	2
195.160.240.11	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
37.26.148.236	Israel	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	2
149.78.2.151	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.116.133.36	Israel	147.237.72.166	aka.idf.il	C1000098: Block - dns poisoning	Block	2
209.88.198.1	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
46.120.54.18	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
212.143.169.74	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
5.29.126.78	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
147.236.31.111	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
52.1.90.117	United States	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
167.114.242.197	Canada	147.237.77.235	sviva.idf.il	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	1
79.179.114.184	Israel	147.237.76.42	refuah.idf.il	20170: HTTP: Suspicious Range Header Field	Block	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
167.114.242.198	Canada	147.237.76.38	e.e.meitav.idf.il	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	1
149.78.76.170	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
111.206.116.217	China	147.237.0.17	m.my-kosher-kravi.idf.il	13076: HTTP: Apache Struts 2 OGNL Command Injection Vulnerability	Block	1
87.68.165.134	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
46.120.35.171	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
159.203.4.142	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
104.47.147.196	United States	147.237.0.19	madim.atal.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
187.40.110.206	Brazil	147.237.77.216	dover.idf.il	C041: HTTP: Access to - index.php?option=com_jce	Block	1
111.206.116.217	China	147.237.0.19	madim.atal.idf.il	13076: HTTP: Apache Struts 2 OGNL Command Injection Vulnerability	Block	1
167.114.229.247	Canada	147.237.0.16	my-kosher-kravi.idf.il	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	1

11-22-2015 to 11-23-2015

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	76
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	25
212.83.144.162	147.237.77.216	France	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	22
144.76.7.89	147.237.77.216	Germany	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	15
95.218.1.103	147.237.77.216	Romania	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	15
105.157.181.112	147.237.77.216	Morocco	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	14
37.27.204.133	147.237.77.216	Germany	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	11
89.144.141.123	147.237.77.216	Iran, Islamic Republic of	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	11
46.62.245.162	147.237.77.216	Iran, Islamic Republic of	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	11
101.50.81.3	147.237.77.216	Pakistan	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	10
46.225.28.181	147.237.77.216	Iran, Islamic Republic of	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	9
73.130.185.245	147.237.77.216	United States	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	9
37.239.120.13	147.237.77.216	Iraq	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	9
37.236.160.66	147.237.77.216	Iraq	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	9
46.225.83.0	147.237.77.216	Iran, Islamic Republic of	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	9
104.237.227.35	147.237.77.216		dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	9
37.238.180.5	147.237.77.216	Iraq	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	9
2.176.248.252	147.237.77.216	Iran, Islamic Republic of	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	9
5.233.216.138	147.237.77.216	Iran, Islamic Republic of	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	8
5.220.169.18	147.237.77.216	Iran, Islamic Republic of	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	8
2.190.135.218	147.237.77.216	Iran, Islamic Republic of	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	8
37.77.54.205	147.237.77.216	Iraq	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	8
193.32.81.5	147.237.77.216	Iran, Islamic Republic of	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	7
185.27.118.7	147.237.77.216	Egypt	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	7
179.233.241.201	147.237.77.216	Brazil	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	7
175.139.133.153	147.237.77.216	Malaysia	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	7
93.71.23.128	147.237.77.216	Italy	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	7
191.183.74.67	147.237.77.216	Brazil	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	7
37.237.161.190	147.237.77.216	Iraq	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	7
2.89.153.235	147.237.77.216	Saudi Arabia	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	6
5.200.185.108	147.237.77.216	Iran, Islamic Republic of	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	6
132.255.158.227	147.237.77.216		dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	6
5.250.43.67	147.237.77.216	Iran, Islamic Republic of	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	6
66.249.64.190	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	6
180.253.93.151	147.237.77.216	Indonesia	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	6
103.15.141.158	147.237.77.216	Bangladesh	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	6
181.74.60.146	147.237.77.216	Chile	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	5
180.250.36.4	147.237.77.216	Indonesia	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	5
37.237.173.6	147.237.77.216	Iraq	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	5
189.237.216.113	147.237.77.216	Mexico	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	5
151.242.119.96	147.237.77.216	Iran, Islamic Republic of	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	5
2.178.82.209	147.237.77.216	Iran, Islamic Republic of	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	5
151.233.175.27	147.237.77.216	Iran, Islamic Republic of	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	5
5.221.12.146	147.237.77.216	Iran, Islamic Republic of	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	5
5.219.92.224	147.237.77.216	Iran, Islamic Republic of	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	5
49.147.190.4	147.237.77.216	Philippines	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	5
89.144.164.75	147.237.77.216	Iran, Islamic Republic of	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	4
46.143.68.86	147.237.77.216	Iran, Islamic Republic of	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	4
2.191.249.232	147.237.77.216	Iran, Islamic Republic of	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	4
31.59.228.92	147.237.77.216	Iran, Islamic Republic of	dover.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	4

11-22-2015 to 11-23-2015

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
172.56.12.2	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14171
50.129.135.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2240
176.10.104.240	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1948
185.27.118.7	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1657
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	958
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	820
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	698
190.31.135.167	Argentina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	623
79.178.123.32	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	600
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	596
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	552
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	466
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	422
47.54.26.66	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	416
197.162.21.79	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	371
188.120.148.192	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	356
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	314
188.225.185.137	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	306
167.114.156.198	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	306
107.167.108.55	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	298
37.236.160.66	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	298
70.39.187.176	Satellite Provider	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	273
94.228.34.248	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	266
109.67.3.195	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	244
38.111.147.88	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	241
179.191.15.61	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	236
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	236
204.12.251.37	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	211
212.179.212.100	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	210
183.171.21.74	Malaysia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	190
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	154
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	147
151.238.202.236	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	137
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	137
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	136
85.128.142.60	Poland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	135
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	135
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	133
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	126
144.76.7.89	Germany	147.237.77.216	dover.idf.il	Streaming Engine: TCP SYN Modified Retransmission	Data received before SYN was acknowledged. Stripping all packet data.	drop	123
37.112.33.45	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	121
109.63.158.79	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	121
176.77.80.99	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	121
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	117
70.39.185.112	Satellite Provider	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	115
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	114
180.253.93.151	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	111
46.19.85.218	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	109
37.26.148.217	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	101
100.100.30.175		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	95

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	442
176.13.19.145	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.13.19.145	Block	365
176.13.1.170	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.13.1.170	Block	317
79.178.123.32	Israel	147.237.72.166	aka.idf.il	Automated Vulnerability Scanning	Block	307
46.19.86.100	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.100	Block	305
2.54.12.5	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	300
176.12.147.26	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	294
176.13.3.237	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	268
2.52.56.44	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	255
176.13.19.145	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	249
46.19.85.188	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	245
46.19.85.38	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.38	Block	239
109.67.100.245	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	237
46.19.86.17	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	231
2.54.17.186	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	225
2.52.56.44	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	219
147.235.8.51	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	181
46.19.85.188	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	175
144.76.7.89	Germany	147.237.77.216	dover.idf.il	Distributed Automated Vulnerability Scanning	Block	175
2.52.33.184	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	174
73.130.185.245	United States	147.237.77.216	dover.idf.il	Distributed Automated Vulnerability Scanning	Block	170
176.106.226.22	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	166
46.19.85.218	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	163
176.13.1.137	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	162
109.67.48.207	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	161
147.235.8.51	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	159
46.19.86.17	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	158
2.54.54.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	156
109.67.48.207	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	153
2.54.12.5	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	153
176.106.226.22	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	147
46.225.83.0	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Distributed Automated Vulnerability Scanning	Block	142
213.57.61.61	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	142
95.35.66.50	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	140
176.13.21.6	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	139
188.120.148.192	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 188.120.148.192	Block	138
89.138.176.12	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 89.138.176.12	Block	137
2.54.17.186	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	133
176.13.1.170	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 176.13.1.170	Block	132
212.83.144.162	France	147.237.77.216	dover.idf.il	Distributed Automated Vulnerability Scanning	Block	127
188.120.148.192	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	126
89.138.176.12	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	126
46.19.86.100	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	125
176.12.137.63	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	123
95.35.66.50	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	115
147.235.8.51	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 147.235.8.51	Block	114
109.67.100.245	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	110
212.25.102.57	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	109
46.19.86.100	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 46.19.86.100	Block	108
176.13.2.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107