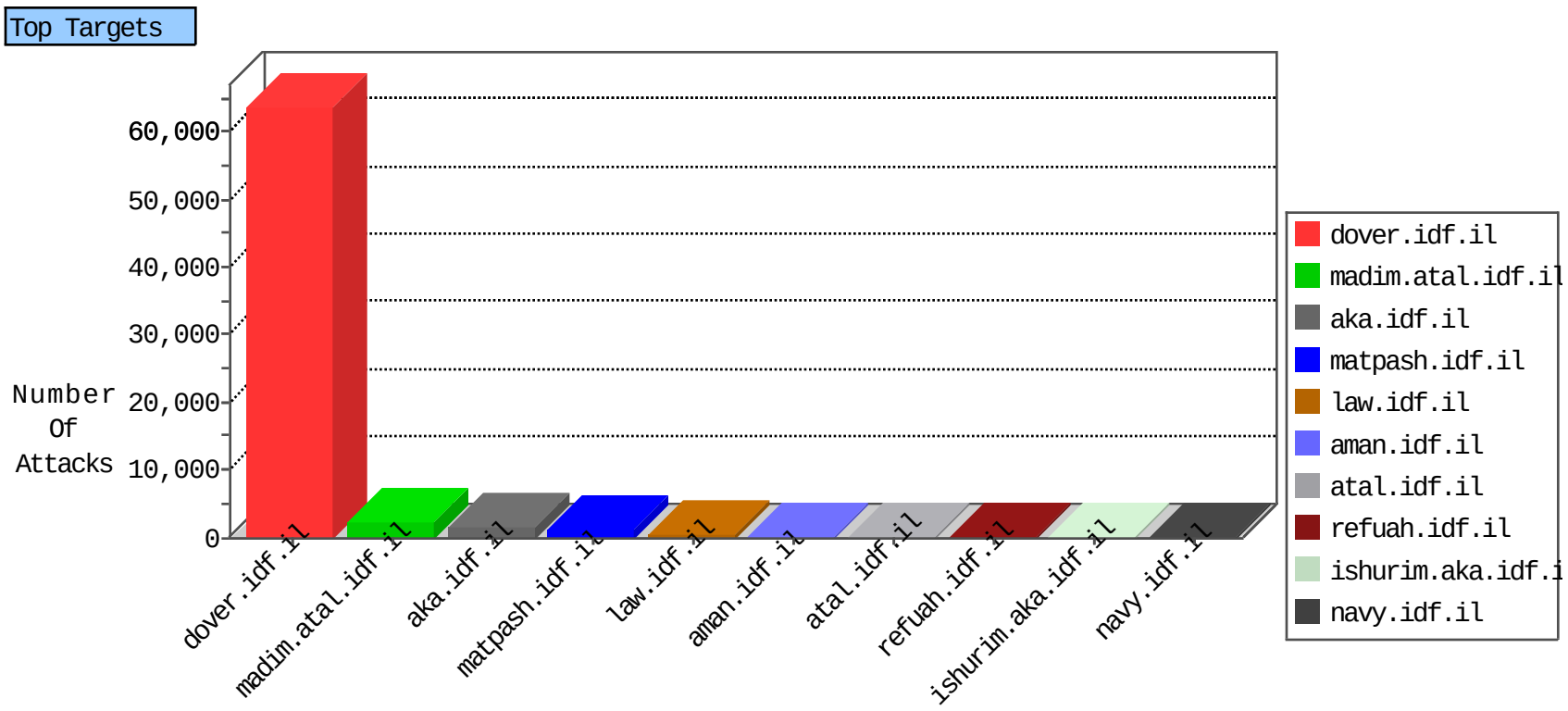
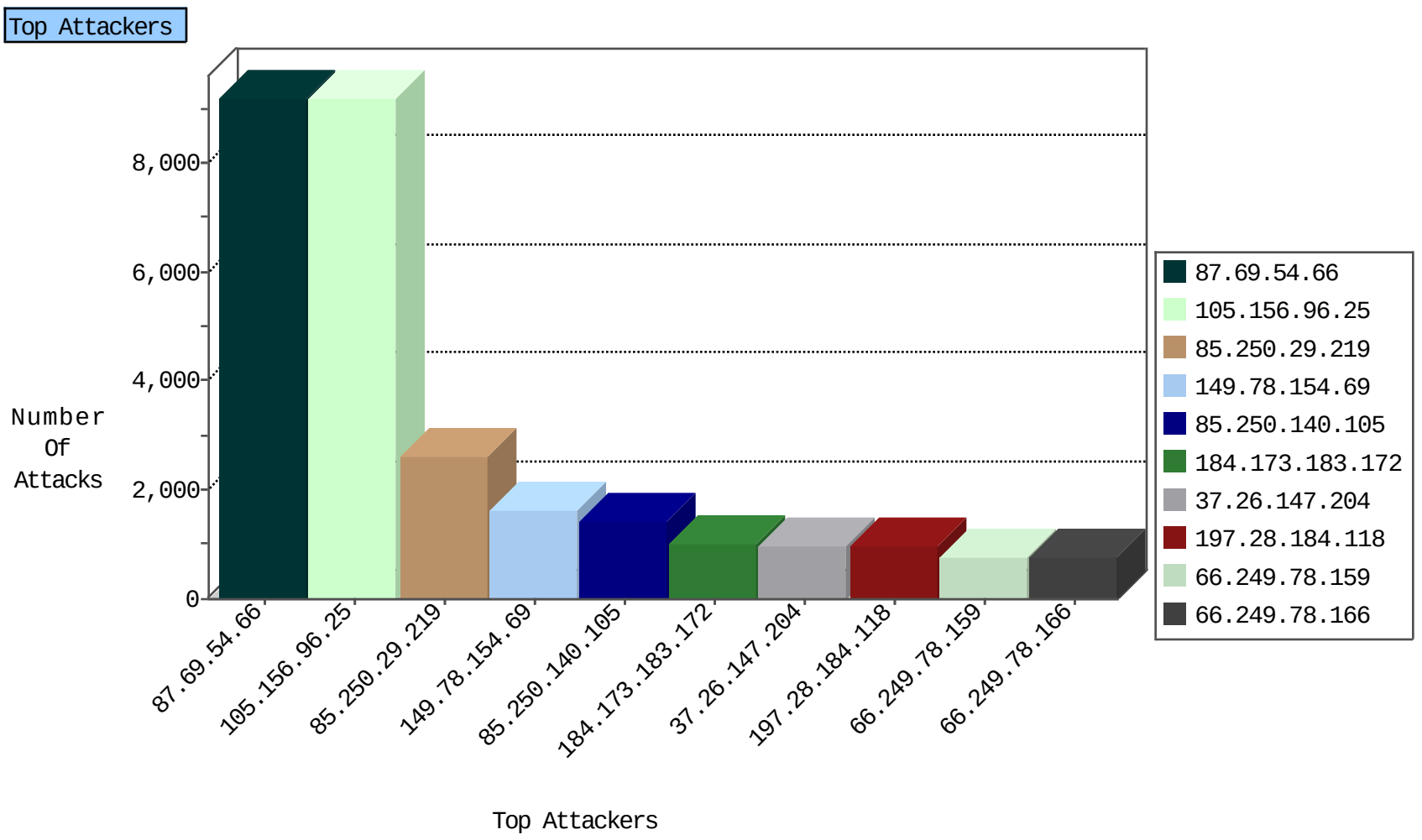
06-20-2015-00:00:08 to 06-21-2015-00:00:08

IDF Under Attack Daily Report





06-20-2015-00:00:08 to 06-21-2015-00:00:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
78.181.104.14	Turkey	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-cat	dest-reset	1784
220.181.108.90	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	1136
79.179.141.141	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	958
105.156.96.25	Morocco	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	824
46.120.229.31	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	455
5.29.219.246	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	375
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	329
204.13.200.28	United States	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	286
66.249.64.26	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	247
84.229.34.186	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	240
46.121.102.202	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	151
212.179.21.194	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	144
109.64.119.177	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	136
46.120.32.153	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	131
109.64.151.97	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	125
212.235.112.108	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	114
2.52.144.93	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	114
109.253.144.209	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	110
84.110.86.51	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	106
81.218.89.26	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	104
84.95.199.113	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	101
89.139.38.69	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	100
109.253.141.4	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	95
46.19.86.95	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	94
81.218.136.68	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	94
31.154.92.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	92
80.246.136.216	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	89
46.19.86.6	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	89
79.182.143.88	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	87
213.57.172.65	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	85
46.19.85.54	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	83
2.54.175.24	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	82
79.178.203.211	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	77
2.54.139.207	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	76
93.172.123.99	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	65
46.117.183.189	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	65
2.54.138.167	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	61
66.249.65.71	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	39
176.12.149.229	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	20
46.19.85.40	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
87.68.165.193	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	17
85.64.116.89	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	14
200.53.156.138	Mexico	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
75.70.21.209	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10
78.181.104.14	Turkey	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	10
79.178.177.170	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	9
109.65.126.65	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	9
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	8
213.8.125.165	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
79.177.136.13	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7

06-20-2015-00:00:08 to 06-21-2015-00:00:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	612
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	399
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	220
78.55.222.125	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	48
115.219.31.244	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	36
198.254.231.191	Canada	147.237.77.74	law.idf.il	1633: HTTP: WebDAV Protocol PROPFIND Method	Block	23
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	20
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	20
187.45.195.127	Brazil	147.237.72.166	aka.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	14
187.45.195.127	Brazil	147.237.72.166	aka.idf.il	13375: HTTP: Joomla Component JCE BOT for JCE	Block	12
187.45.195.127	Brazil	147.237.77.74	law.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	12
187.45.195.127	Brazil	147.237.77.74	law.idf.il	13375: HTTP: Joomla Component JCE BOT for JCE	Block	12
213.139.52.30	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	10
159.253.145.150	United States	147.237.77.216	dover.idf.il	C095: Suspicious Addresses MFA	Permit	8
91.230.121.131	Ukraine	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	8
178.214.86.200	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	7
66.240.192.138	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	6
66.240.192.138	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	6
216.155.131.70	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	6
71.6.167.142	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	6
71.6.167.142	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	6
198.20.69.98	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	5
79.182.202.229	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.135.131	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	5
71.6.165.200	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	5
188.138.9.50	Germany	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	5
71.6.135.131	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	5
188.138.9.50	Germany	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	5
188.138.9.50	Germany	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	5
66.240.192.138	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	5
188.138.9.50	Germany	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	5
85.25.103.50	Germany	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	5
79.179.227.149	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
46.19.85.180	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
71.6.135.131	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	4
95.215.227.115	United Kingdom	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
71.6.135.131	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	4
5.102.226.234	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
188.138.9.50	Germany	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	4
85.25.103.50	Germany	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	4
71.6.135.131	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	4
46.244.73.10	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
95.215.227.115	United Kingdom	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
66.240.192.138	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	4

06-20-2015-00:00:08 to 06-21-2015-00:00:08

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	140
89.187.101.77	United Kingdom	147.237.72.166	aka.idf.il	SQL Injection - Select From	63
105.157.129.214	Morocco	147.237.77.216	dover.idf.il	Admin login page scan - Havij	10
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	6
66.249.75.76	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	6
96.31.33.55	United States	147.237.72.166	aka.idf.il	SQL Injection - Select From	6
105.156.96.25	Morocco	147.237.77.216	dover.idf.il	ET WEB_SERVER Poison Null Byte	5
105.157.129.214	Morocco	147.237.77.216	dover.idf.il	SERVER-WEBAPP login.htm access	4
187.45.195.127	Brazil	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	4
43.255.188.130	Japan	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	3
43.255.188.130	Japan	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	3
61.183.128.6	China	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	3
43.255.188.135	Japan	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	3
43.255.188.133	Japan	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	2
61.183.128.6	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.134	Japan	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.130	Japan	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	2
66.249.64.16	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.132	Japan	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.133	Japan	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	2
109.253.145.1	Israel	147.237.72.166	aka.idf.il	GPL SCAN myscan	2
43.255.188.130	Japan	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.131	Japan	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.132	Japan	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	2
213.204.103.36	Lebanon	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
198.204.230.130	United States	147.237.77.216	dover.idf.il	SERVER-WEBAPP backup access	2
105.157.129.214	Morocco	147.237.77.216	dover.idf.il	SERVER-WEBAPP admin.php access	2
212.106.83.200	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.133	Japan	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.132	Japan	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	2
210.72.21.186	China	147.237.76.44	e.refuah.idf.il	GPL SCAN nmap TCP	2
61.240.144.66	China	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.93.172	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.135	Japan	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	2
84.228.16.147	Israel	147.237.76.86	navy.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
82.205.81.154	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.134	Japan	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.132	Japan	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	2
109.253.145.1	Israel	147.237.72.166	aka.idf.il	INDICATOR-SCAN myscan	2
61.240.144.66	China	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	2
61.240.144.64	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	2
43.255.188.133	Japan	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.67	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	2
43.255.188.132	Japan	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.66	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	2
105.157.129.214	Morocco	147.237.77.216	dover.idf.il	SERVER-WEBAPP adminlogin access	2
43.255.188.135	Japan	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	2
61.183.128.6	China	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	2
197.231.236.6	N/A	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
43.255.188.135	Japan	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	2

06-20-2015-00:00:08 to 06-21-2015-00:00:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
87.69.54.66	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9210
105.156.96.25	Morocco	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8859
85.250.29.219	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2617
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1614
85.250.140.105	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1355
37.26.147.204	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	981
197.28.184.118	Tunisia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	977
105.188.115.36		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	703
95.86.116.84	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	654
89.138.217.133	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	593
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	572
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	567
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	564
87.69.122.73	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	503
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	500
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	434
89.187.101.77	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	408
72.80.53.240	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	388
104.175.163.33		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	362
212.76.98.211	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	308
107.167.108.49	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	305
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	284
104.61.230.52		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	278
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	266
66.87.66.231	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	264
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	249
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	247
109.163.234.2	Romania	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	247
200.53.156.138	Mexico	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	246
66.102.6.163	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	239
68.180.229.51	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	236
79.183.227.37	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	234
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	223
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	216
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	214
66.102.6.167	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	207
91.213.8.235	Ukraine	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	202
149.255.204.104	Iraq	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	201
66.102.6.171	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	199
77.109.139.27	Switzerland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	192
105.157.129.214	Morocco	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	188
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	184
78.138.217.79	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	184
5.255.253.33	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	179
78.181.104.14	Turkey	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	172
157.55.39.60	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	168
205.203.135.1	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	162
217.66.228.71	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	158
166.137.139.75	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	156
50.154.141.52	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	156

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
213.57.172.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	502
85.65.55.134	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 85.65.55.134	Block	416
46.19.86.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	340
109.253.149.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	302
46.19.86.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	127
109.64.203.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	109
77.125.133.190	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 77.125.133.190	Block	106
77.125.12.229	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 77.125.12.229	Block	73
2.54.185.35	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.185.35	Block	49
109.66.148.16	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	33
79.178.177.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	30
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	29
105.156.96.25	Morocco	147.237.77.216	dover.idf.il	Multiple NULL Character in Header Name from 105.156.96.25	Block	26
105.156.96.25	Morocco	147.237.77.216	dover.idf.il	Multiple NULL Character in Method from 105.156.96.25	Block	26
105.156.96.25	Morocco	147.237.77.216	dover.idf.il	Multiple Abnormally Long Header Line from 105.156.96.25	Block	26
105.156.96.25	Morocco	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 105.156.96.25	Block	26
105.156.96.25	Morocco	147.237.77.216	dover.idf.il	Multiple Malformed HTTP Header Line from 105.156.96.25	Block	26
105.156.96.25	Morocco	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 105.156.96.25	Block	26
105.156.96.25	Morocco	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Header Name from 105.156.96.25	Block	26
105.156.96.25	Morocco	147.237.77.216	dover.idf.il	Multiple Malformed URL from 105.156.96.25	Block	26
105.156.96.25	Morocco	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Method from 105.156.96.25	Block	26
105.156.96.25	Morocco	147.237.77.216	dover.idf.il	Multiple Malformed URL from 105.156.96.25	Block	26
105.156.96.25	Morocco	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Method from 105.156.96.25	Block	26
200.53.156.138	Mexico	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	25
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	23
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	22
198.254.231.191	Canada	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	22
46.19.85.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	20
5.9.45.155	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 5.9.45.155	Block	18
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	16
105.157.129.214	Morocco	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	14
213.57.172.65	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 213.57.172.65	Block	13
94.153.9.220	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-15081-he/	Block	11
109.64.155.49	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 109.64.155.49	None	11
109.65.202.63	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	10
208.115.111.72	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	9
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	9
157.55.39.238	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	9
109.65.202.63	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	9
79.176.25.171	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
46.19.85.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	8
5.102.254.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	8
176.12.151.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	8
149.78.28.63	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized HTTP Method	Block	8
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	7
68.180.229.51	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.229.51	Block	7
207.46.13.99	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
69.160.54.33	United States	147.237.77.170	maarachot.idf.il	Distributed Suspicious Response Code	Block	6
207.241.226.75	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	6
69.160.54.33	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
37.57.231.137	Ukraine	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	6
105.157.129.214	Morocco	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	5