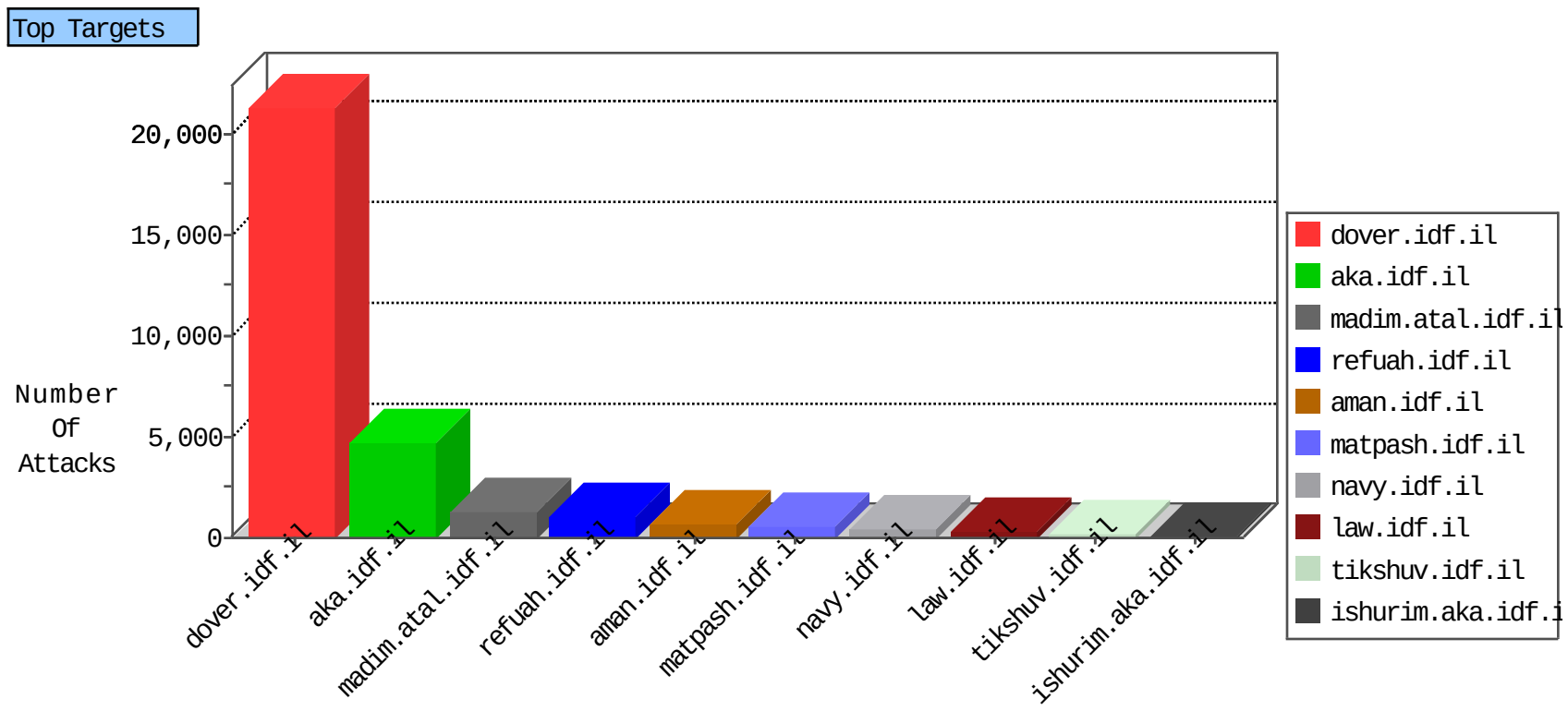
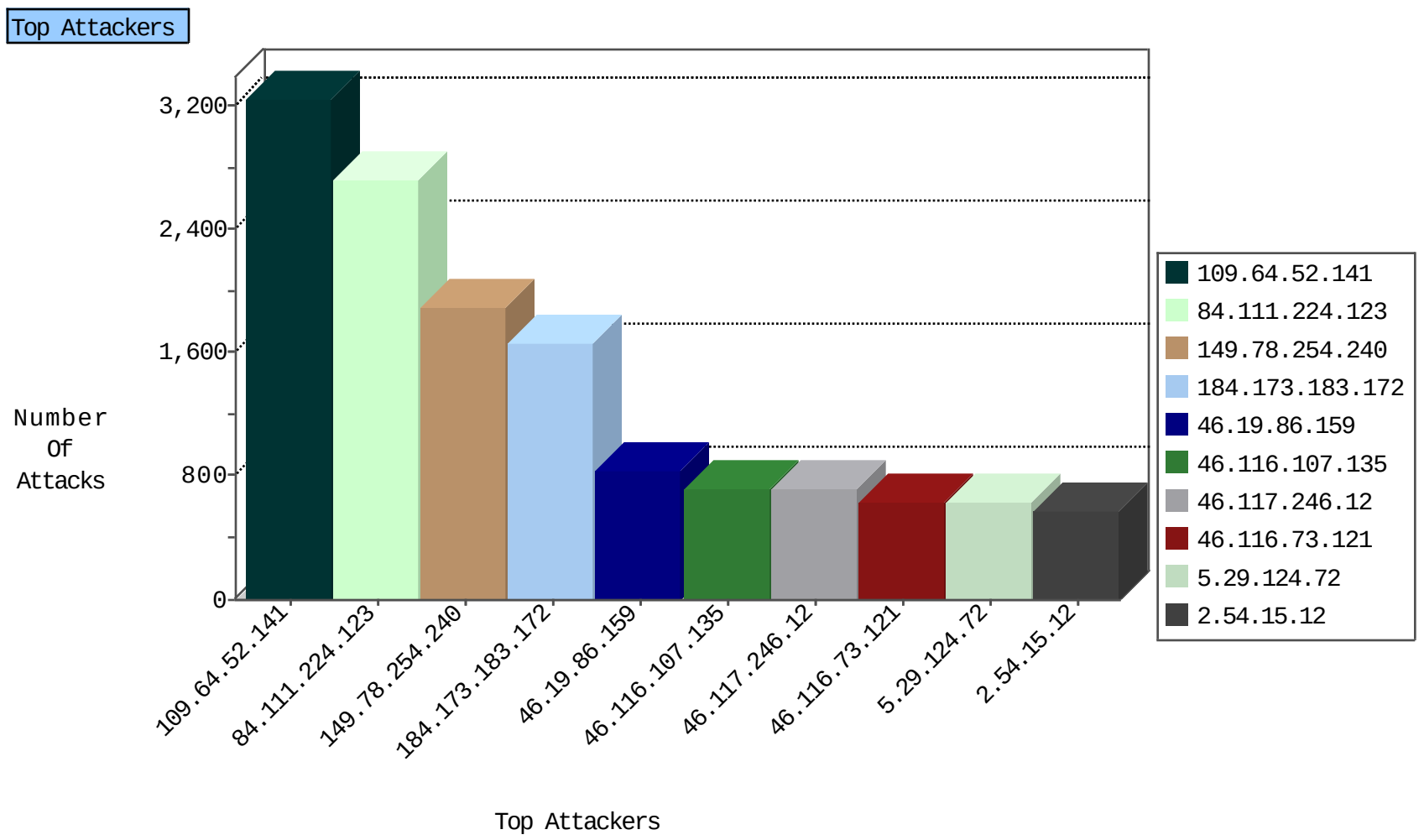
04-24-2015-00:00:04 to 04-25-2015-00:00:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-24-2015-00:00:04 to 04-25-2015-00:00:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
136.243.5.219	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	32501
66.249.78.190	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	19091
66.249.73.209	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	18911
66.249.65.185	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	11761
66.249.65.39	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	10581
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	9808
207.35.33.164	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9381
41.135.155.42	South Africa	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9207
100.33.79.215	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8234
176.12.148.33	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7978
66.249.73.217	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	6966
70.72.152.159	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6945
109.64.42.16	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6549
66.249.65.43	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	6460
68.207.115.112	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6186
77.127.96.149	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5664
47.19.118.253	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5406
82.145.222.142	Europe	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5382
10.0.0.10		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5056
214.38.145.227	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4915
66.249.93.239	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	4793
66.249.93.245	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	4366
66.249.65.41	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	4040
207.46.13.1	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3986
220.181.108.154	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	3435
220.181.108.83	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	3279
195.34.150.18	Austria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2861
220.181.108.177	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	2782
207.46.13.52	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2732
178.80.85.50	Saudi Arabia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2722
109.186.33.116	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2618
84.110.192.46	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2492
54.72.73.168	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2455
79.182.127.58	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2398
66.249.73.230	Israel	147.237.72.156	aman.idf.il	TCP handshake violation, first packet not syn	drop	2326
108.54.226.109	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2246
31.154.0.70	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2189
72.219.191.21	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2017
93.172.34.126	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2005
77.125.125.40	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1952
109.253.146.220	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1879
109.65.58.245	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1875
173.162.34.45	United States	147.237.72.156	aman.idf.il	TCP Scan (vertical)	drop	1864
5.29.172.182	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1731
5.29.17.22	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1443
41.42.188.215	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1411
79.182.18.232	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1399
77.125.138.65	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1340

04-24-2015-00:00:04 to 04-25-2015-00:00:04

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
84.109.184.143	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1228
220.181.108.145	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	1199

04-24-2015-00:00:04 to 04-25-2015-00:00:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.64.52.141	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	3251
184.173.183.172	United States	147.237.76.42	refuah.idf.il	DVRep_P-N_40-59	Permit	890
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	521
184.173.183.172	United States	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	256
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	63
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	20
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	20
104.199.136.202		147.237.77.74	law.idf.il	13375: HTTP: Joomla Component JCE BOT for JCE	Block	12
130.211.251.163		147.237.77.74	law.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	12
104.199.136.202		147.237.77.74	law.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	12
130.211.251.163		147.237.77.74	law.idf.il	13375: HTTP: Joomla Component JCE BOT for JCE	Block	12
217.115.10.131	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	8
79.183.170.184	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
107.10.240.187	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
212.34.12.177	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
46.116.211.238	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
2.52.55.59	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
46.120.128.121	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
71.6.167.142	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	5
71.6.165.200	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	5
71.6.165.200	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	5
198.20.69.98	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	5
198.20.70.114	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	5
85.25.103.50	Germany	147.237.77.234	halag.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
71.6.167.142	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	5
176.65.6.14	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	5
198.20.69.98	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	5
199.203.170.141	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
84.109.9.69	Israel	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
71.6.167.142	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	4
71.6.167.142	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	4
41.185.12.165	South Africa	147.237.76.86	navy.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
198.20.70.114	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.8.27	e.madim.atal.idf.i	DVRep_B-N_60_100	Block	4
110.164.184.11	Thailand	147.237.76.86	navy.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
89.216.115.8		147.237.77.216	dover.idf.il	17272: HTTP: Suspicious User-Agent (WindowsNT) With No Separating Space	Block	4
5.186.228.35	Germany	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
79.176.175.97	Israel	147.237.77.234	halag.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
71.6.167.142	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	4
198.20.69.98	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	4
71.6.165.200	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	4
80.178.15.170	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
110.164.184.11	Thailand	147.237.77.176	matpash.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
41.46.77.158	Egypt	147.237.76.86	navy.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
71.6.167.142	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	3
85.25.103.50	Germany	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	3
198.20.70.114	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	3
71.6.165.200	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	3
119.110.70.205	Indonesia	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3

04-24-2015-00:00:04 to 04-25-2015-00:00:04

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.78.204	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	306
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	273
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	135
66.249.65.28	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	72
66.249.65.152	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	32
66.249.73.203	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	10
66.249.65.148	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	10
66.249.78.190	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	8
66.249.73.219	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	8
66.249.65.30	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	6
66.249.65.26	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	6
66.249.65.156	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	6
173.162.34.45	United States	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 1024	5
105.98.10.127	Algeria	147.237.77.216	dover.idf.il	ET WEB_SERVER LOIC Javascript DDoS Inbound	5
66.249.79.74	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	4
66.249.65.34	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	4
91.224.132.118	Russian Federation	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	4
66.249.65.46	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	4
89.234.68.85	Ireland	147.237.77.216	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	4
79.179.37.226	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
84.111.155.234	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
79.176.37.81	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
66.249.93.179	United States	147.237.76.30	himush.idf.il	ET SCAN NMAP -sA (2)	4
66.249.73.217	United States	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
85.104.233.220	Turkey	147.237.77.216	dover.idf.il	INDICATOR-OBFUSCATION script tag in POST parameters - likely cross-site scripting	3
109.67.177.217	Israel	147.237.0.34	tikshuv.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
43.255.191.161	Japan	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	3
173.162.34.45	United States	147.237.72.156	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
85.250.17.165	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.19.86.149	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.191.161	Japan	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	2
61.240.144.66	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	2
37.8.4.131	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
66.249.65.41	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
46.19.85.225	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.65.37	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
43.255.191.161	Japan	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	2
43.255.191.162	Japan	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	2
109.67.168.146	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
89.138.95.240	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.191.161	Japan	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	2
2.54.130.187	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.75.110	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
109.65.55.86	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
54.147.46.79	United States	147.237.77.176	matpash.idf.il	Tehila - Perl LWP with fake user agent	2
213.57.178.33	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
180.169.108.158	China	147.237.8.14	e.orchot.idf.il	GPL SCAN nmap TCP	2
2.54.23.189	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.65.10	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.64	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	2

04-24-2015-00:00:04 to 04-25-2015-00:00:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
84.111.224.123	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2718
149.78.254.240	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1903
46.19.86.159	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	832
46.116.107.135	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	716
46.117.246.12	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	712
46.116.73.121	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	634
5.29.124.72	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	630
2.54.15.12	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	572
95.86.82.132	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	402
85.64.184.43	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	388
5.29.86.157	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	322
212.179.159.253	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	306
212.76.115.99	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	252
80.178.169.168	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	211
46.19.86.106	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	174
70.39.184.132	Satellite Provide	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	167
2.54.31.52	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	157
93.173.27.143	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	132
99.237.176.203	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	126
212.179.61.124	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	124
79.181.200.199	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	122
213.8.115.121	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	110
46.19.85.25	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	110
2.54.20.93	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	100
2.54.0.229	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	100
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	92
81.218.251.250	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	88
93.172.156.115	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	69
212.179.46.21	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	68
2.54.43.200	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	67
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	66
93.172.172.63	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	64
79.182.206.49	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	63
2.52.5.225	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	62
46.19.85.160	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	61
2.54.19.63	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	61
66.249.79.66	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	61
79.181.224.70	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	59
173.61.96.42	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	58
212.179.46.20	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	58
46.19.86.111	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	58
95.210.249.254	Italy	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	55
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	54
80.178.149.225	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	53
66.249.65.43	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	52
66.249.65.41	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	50
79.183.175.8	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	50
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	50
46.121.253.80	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	50
84.111.80.78	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	50

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 78.46.174.55	Block	394
109.160.183.10	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.160.183.10	Block	278
109.253.130.86	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	205
46.19.85.56	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	148
109.253.131.137	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.131.137	Block	138
109.253.141.191	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.141.191	Block	116
2.54.29.124	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.29.124	Block	108
46.19.86.57	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.86.57	Block	95
66.249.79.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.74	Block	84
176.12.138.146	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.12.138.146	Block	81
66.249.79.58	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.58	Block	69
66.249.79.66	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.66	Block	69
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 78.46.174.55	Block	54
78.46.174.55	Germany	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 78.46.174.55	Block	54
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	48
109.253.133.60	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	32
79.182.136.126	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 79.182.136.126	Block	26
104.32.162.117		147.237.77.74	law.idf.il	PHP Attempt	Block	25
104.32.162.117		147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 104.32.162.117	Block	22
5.102.198.105	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/kamlar/styles/import/bottomnavigaton.asp	Block	20
125.65.46.140	China	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 125.65.46.140	Block	20
176.12.141.128	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	15
5.29.184.33	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	14
109.253.138.38	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	12
173.162.34.45	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized HTTP Method	Block	12
162.243.89.33	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 162.243.89.33	Block	11
173.162.34.45	United States	147.237.72.156	aman.idf.il	Multiple Unknown HTTP Request Method from 173.162.34.45	Block	11
173.162.34.45	United States	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Header Name from 173.162.34.45	Block	11
173.162.34.45	United States	147.237.72.156	aman.idf.il	Multiple Malformed URL from 173.162.34.45	Block	11
79.177.13.83	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	11
173.162.34.45	United States	147.237.72.156	aman.idf.il	Multiple NULL Character in Header Name from 173.162.34.45	Block	11
173.162.34.45	United States	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Method from 173.162.34.45	Block	11
173.162.34.45	United States	147.237.72.156	aman.idf.il	Multiple NULL Character in Method from 173.162.34.45	Block	11
173.162.34.45	United States	147.237.72.156	aman.idf.il	Multiple Abnormally Long Header Line from 173.162.34.45	Block	11
173.162.34.45	United States	147.237.72.156	aman.idf.il	Multiple Abnormally Long Request from 173.162.34.45	Block	11
173.162.34.45	United States	147.237.72.156	aman.idf.il	Multiple Malformed HTTP Header Line from 173.162.34.45	Block	11
173.162.34.45	United States	147.237.72.156	aman.idf.il	Distributed Illegal HTTP Version	Block	9
93.173.190.231	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
192.151.151.202	United States	147.237.77.74	law.idf.il	Multiple Admin Blocking from 192.151.151.202	Block	7
109.253.139.120	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	7
66.249.73.136	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	7
188.165.15.13	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.13	Block	7
162.243.198.188	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 162.243.198.188	Block	7
173.162.34.45	United States	147.237.72.156	aman.idf.il	Multiple NULL Character in Url from 173.162.34.45	Block	7
134.249.53.8	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/	Block	6
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	6
95.86.113.239	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	6
46.251.64.235	Russian Federation	147.237.77.74	law.idf.il	PHP Attempt	Block	6
79.179.102.178	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	6
213.151.32.163	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	6

04-24-2015-00:00:04 to 04-25-2015-00:00:04