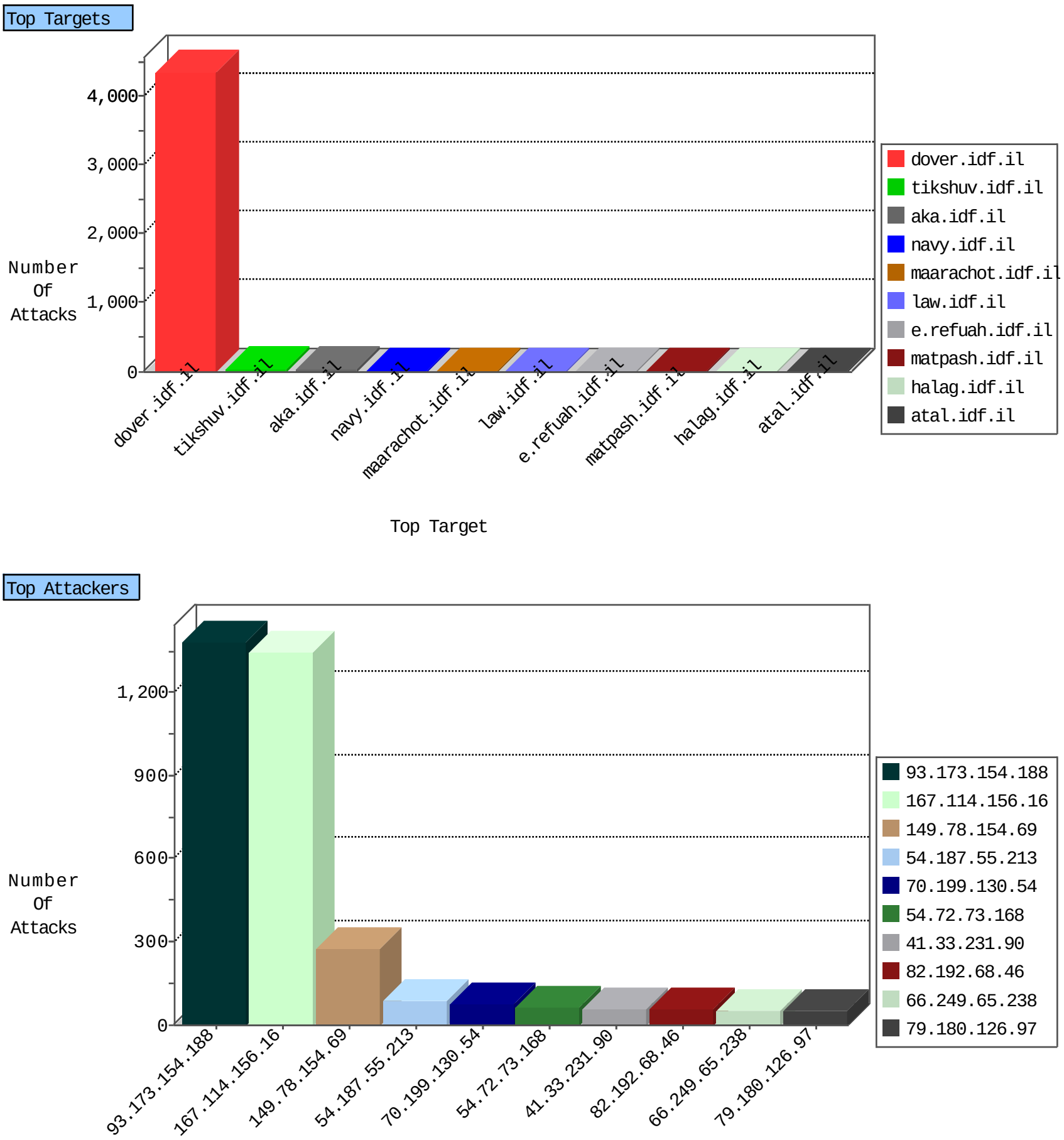
11-07-2015-03:04:06 to 11-07-2015-04:04:06

IDF Under Attack Daily Report



11-07-2015-03:04:06 to 11-07-2015-04:04:06

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	DOS-Tool-SwitchbladG	dest-reset	2280
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	431
66.249.64.191	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	182
66.249.64.181	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	54
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
222.186.34.48	China	147.237.76.44	e.refuah.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
204.42.253.132	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
204.42.253.132	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
5.8.66.78	Russian Federation	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
5.8.66.78	Russian Federation	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1

11-07-2015-03:04:06 to 11-07-2015-04:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-07-2015-03:04:06 to 11-07-2015-04:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.75.198	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	12
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.73.220	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	2
89.248.174.106	147.237.72.217	Netherlands	e.idf.il	ET SCAN NMAP -sS window 1024	1
46.151.52.8	147.237.8.45	Ukraine	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.98	147.237.77.227	United States	e.hamaz.idf.il	ET DROP Dshield Block Listed Source	1
188.138.9.51	147.237.77.74	Germany	law.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243	147.237.8.14		e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1

11-07-2015-03:04:06 to 11-07-2015-04:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
93.173.154.188	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	1385
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	270
54.187.55.213	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	85
70.199.130.54	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	74
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	64
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	55
79.180.126.97	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	53
212.199.182.150	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	48
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	44
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	43
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34
212.179.90.106	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	32
66.249.65.238	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
82.80.25.221	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
66.249.65.231	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
66.249.65.238	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
207.46.13.184	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
113.159.159.59	Japan	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
134.196.163.223	Thailand	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
207.46.13.11	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
157.55.39.181	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
195.34.150.18	Austria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
203.215.117.166	Philippines	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
189.157.167.28	Mexico	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
157.55.39.63	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
66.102.8.238	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.65.224	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
75.119.245.231	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
66.102.8.233	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
73.136.136.103	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
46.210.83.215	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
79.177.147.22	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
65.19.138.34	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
40.77.167.35	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
66.249.81.212	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
37.26.149.148	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
172.91.129.112		147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
46.19.85.38	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
188.165.15.14	France	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
46.19.86.34	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
108.63.102.29	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
40.77.167.39	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
79.183.107.103	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
66.249.65.224	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
157.55.2.150	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7

11-07-2015-03:04:06 to 11-07-2015-04:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
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	8
208.115.111.72	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.111.72	Block	2
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	2
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
157.55.39.0	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
62.210.88.201	France	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.google.pl/search	Block	1
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
157.55.39.61	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/haredim/general.aspx	None	1
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/3397.jpg	Block	1
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.240	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
66.249.65.237	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
157.55.39.243	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/robots.txt	Block	1
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
85.93.91.84	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
180.117.93.106	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/license.txt	Block	1

11-07-2015-03:04:06 to 11-07-2015-04:04:06