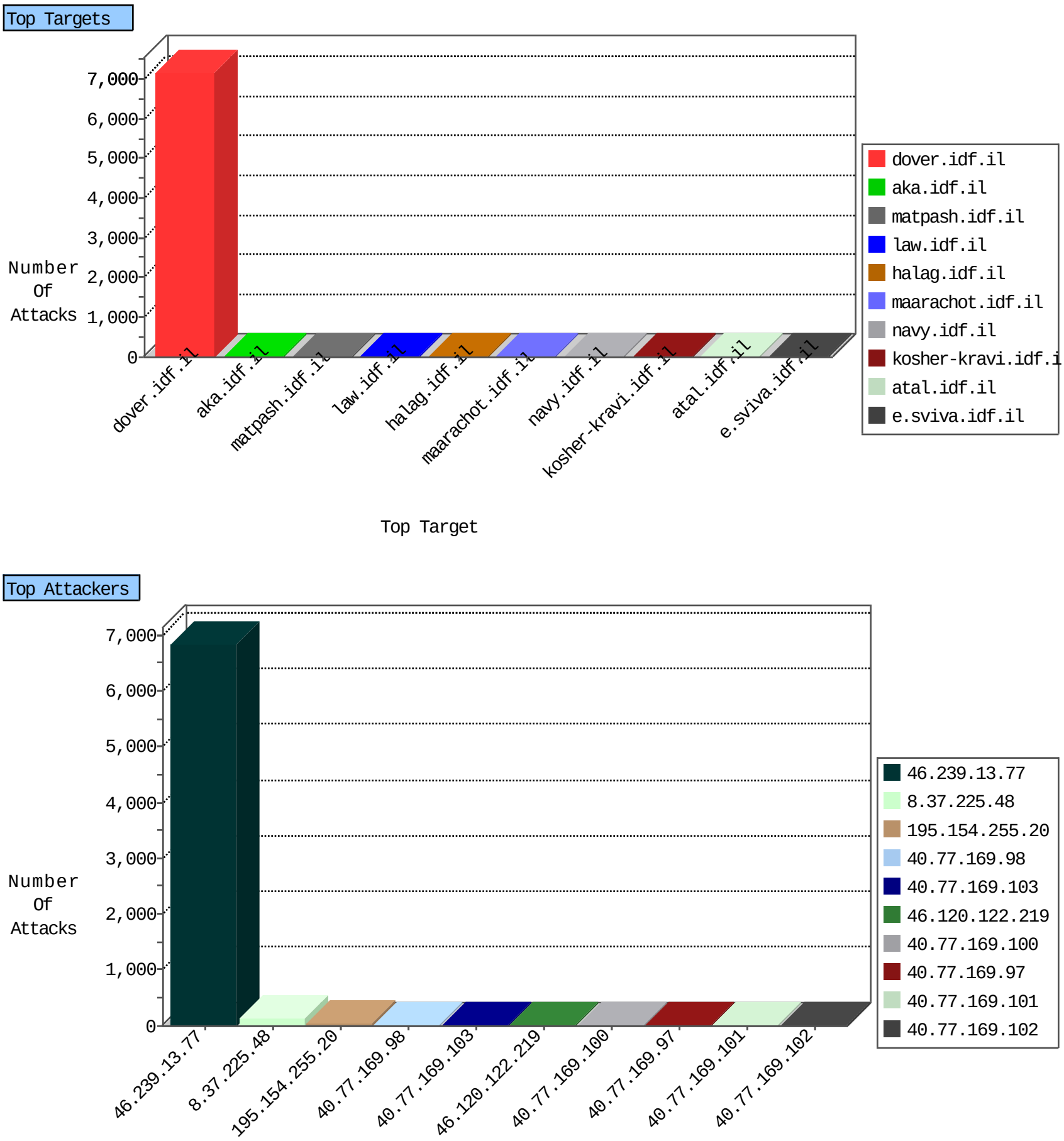
08-27-2016-04:04:01 to 08-27-2016-05:04:01

IDF Under Attack Daily Report



08-27-2016-04:04:01 to 08-27-2016-05:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
8.37.225.48	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
134.147.203.115	Germany	147.237.76.196	e.sviva.idf.il	Black List	drop	2
66.240.236.119	United States	147.237.76.42	refuah.idf.il	Black List	drop	1
123.59.59.52	China	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	1

08-27-2016-04:04:01 to 08-27-2016-05:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
195.154.255.20	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	37
80.169.91.26	United Kingdom	147.237.72.167	ishurim.aka.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

08-27-2016-04:04:01 to 08-27-2016-05:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	14
46.120.122.219	147.237.77.74	Israel	law.idf.il	Xenu Link Sleuth User Agent	6
46.120.122.219	147.237.76.86	Israel	navy.idf.il	Xenu Link Sleuth User Agent	4
46.120.122.219	147.237.77.170	Israel	maarachot.idf.il	Xenu Link Sleuth User Agent	2
183.60.48.25	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
163.172.169.150	147.237.72.166	United Kingdom	aka.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.245	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
18.85.22.228	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1
183.60.48.25	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
5.39.222.253	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1

08-27-2016-04:04:01 to 08-27-2016-05:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.239.13.77	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6599
46.239.13.77	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop		drop	250
8.37.225.48	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	124
40.77.169.103	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	26
40.77.169.98	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	19
40.77.169.101	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	14
40.77.169.100	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	12
40.77.169.102	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
40.77.169.104	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	10
76.68.37.61	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
40.77.169.97	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	9
167.220.232.104	Japan	147.237.72.166	aka.idf.il	drop	SAM rule	drop	8
40.77.169.98	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	7
40.77.169.100	United States	147.237.77.234	halag.idf.il	drop	SAM rule	drop	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
40.77.169.97	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	6
203.133.171.21	Korea, Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
40.77.169.99	United States	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	5
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
77.138.52.97	France	147.237.77.216	dover.idf.il	drop		drop	3
40.77.169.98	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	3
40.77.169.99	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
183.129.160.229	China	147.237.77.233	atal.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.77.212	e.dover.idf.il	drop	SAM rule	drop	1
79.179.186.199	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.77.234	halag.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
40.77.169.99	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.77.243	mobile.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.77.178	e.matpash.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.77.227	e.hamaz.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.0.19	madim.atal.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.77.205	prisha.idf.il	drop	SAM rule	drop	1
40.77.169.102	United States	147.237.77.234	halag.idf.il	drop	SAM rule	drop	1

08-27-2016-04:04:01 to 08-27-2016-05:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
40.77.169.96	United States	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in URL from 40.77.169.96	Block	2
65.55.210.179	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
131.253.27.54	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
37.59.62.43	France	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	1
66.249.66.233	Israel	147.237.76.31	nakchal.idf.i	Unauthorized URL Access to nakhal.idf.il/default.asp	Block	1
144.76.236.183	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
66.249.76.87	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-12533-en	Block	1
199.30.24.35	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.108.133.64	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
199.30.25.163	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.219	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1274-he/atal.aspx	Block	1
87.69.210.26	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.66.59	Israel	147.237.0.34	tikshuv.idf.i	Unauthorized URL Access to www.tikshuv.idf.il/modules/forums.frm/frmuserdetails.aspx	Block	1

08-27-2016-04:04:01 to 08-27-2016-05:04:01