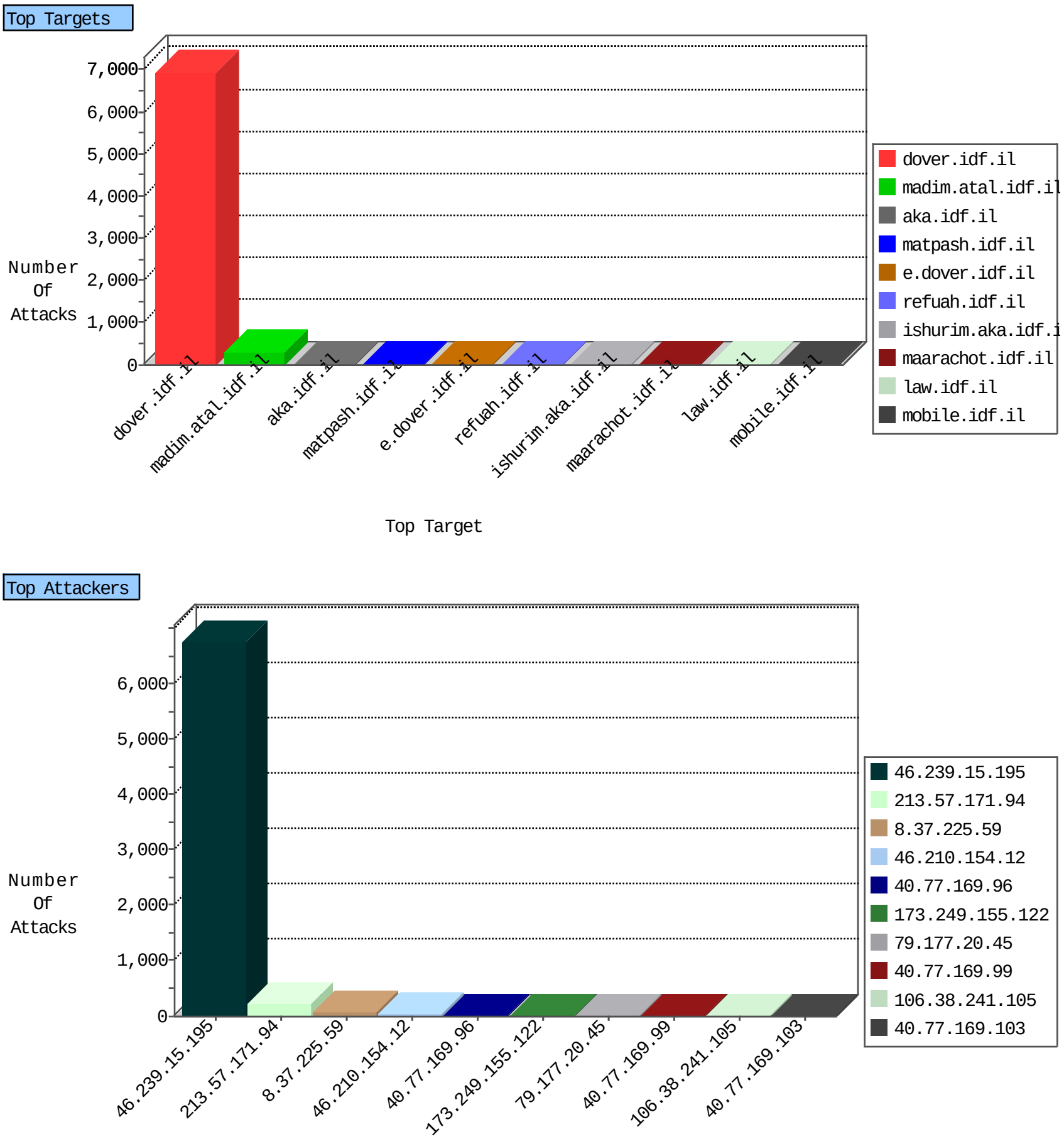
08-27-2016-13:04:03 to 08-27-2016-14:04:03

IDF Under Attack Daily Report



08-27-2016-13:04:03 to 08-27-2016-14:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
8.37.225.59	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	5
46.239.15.195	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	2
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	2
109.226.40.40	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
185.94.111.1	Russian Federation	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1

08-27-2016-13:04:03 to 08-27-2016-14:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

08-27-2016-13:04:03 to 08-27-2016-14:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
173.249.155.122	147.237.77.179	United Kingdom	e.mazi.idf.il	GPL SCAN superscan echo	1
173.249.155.122	147.237.77.176	United Kingdom	matpash.idf.il	GPL SCAN superscan echo	1
173.249.155.122	147.237.77.74	United Kingdom	law.idf.il	GPL SCAN superscan echo	1
94.102.48.195	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
63.221.141.195	147.237.76.176	United States	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
46.239.15.195	147.237.77.216	Bosnia and Herzegovina	dover.idf.il	portscan: TCP Distributed Portscan	1
5.39.222.253	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
173.249.155.122	147.237.77.216	United Kingdom	dover.idf.il	GPL SCAN superscan echo	1
173.249.155.122	147.237.77.205	United Kingdom	prisha.idf.il	GPL SCAN superscan echo	1
173.249.155.122	147.237.77.178	United Kingdom	e.matpash.idf.il	GPL SCAN superscan echo	1
173.249.155.122	147.237.77.170	United Kingdom	maarachot.idf.il	GPL SCAN superscan echo	1
120.50.122.168	147.237.0.34	Korea, Republic of	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
63.221.141.195	147.237.76.202	United States	e.halag.idf.il	ET SCAN Potential SSH Scan	1
63.221.141.195	147.237.76.148	United States	gqcenter.aka.idf.i	ET SCAN Potential SSH Scan	1
46.172.71.251	147.237.77.234	Ukraine	halag.idf.il	ET SCAN NMAP -sS window 1024	1
188.0.236.165	147.237.77.212	Moldova, Republic of	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
5.39.222.253	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
173.249.155.122	147.237.77.212	United Kingdom	e.dover.idf.il	GPL SCAN superscan echo	1

08-27-2016-13:04:03 to 08-27-2016-14:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.239.15.195	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6517
46.239.15.195	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop		drop	248
8.37.225.59	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	70
40.77.169.96	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	22
40.77.169.99	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
79.177.20.45	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
40.77.169.103	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
40.77.169.96	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
79.182.111.48	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
40.77.169.104	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
106.38.241.105	China	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	1
66.240.236.119	United States	147.237.0.35	akaws.idf.il	drop		drop	1
109.226.40.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
79.182.143.226	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	1
46.19.86.7	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
106.38.241.105	China	147.237.76.86	navy.idf.il	drop	SAM rule	drop	1
109.253.217.188	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
85.64.59.244	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
31.13.113.79	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
106.38.241.105	China	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	1
40.77.169.101	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
115.230.125.146	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
106.38.241.105	China	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	1
31.13.113.82	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
106.38.241.105	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
79.178.134.83	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	1
176.13.6.165	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
106.38.241.105	China	147.237.72.156	aman.idf.il	drop	SAM rule	drop	1
106.38.241.105	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1

08-27-2016-13:04:03 to 08-27-2016-14:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.57.171.94	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	232
46.210.154.12	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	58
40.77.169.97	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
40.77.169.102	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
176.13.6.165	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
40.77.169.100	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
77.138.245.28	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	2
40.77.169.103	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
207.46.13.43	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
77.126.58.164	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.64.41	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/1093-7963-he/מאיר שחמון.aspx	Block	1
112.196.166.223	India	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/new/jump-2.eng-300900	Block	1
40.77.169.101	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
77.138.245.28	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.138.245.28	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
40.77.169.98	United States	147.237.77.176	matpash.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
112.196.166.223	India	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
217.132.50.182	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 217.132.50.182	Block	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/960.css	Block	1
40.77.169.98	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
157.55.39.191	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
87.70.14.209	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.76.2	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1769	Block	1
40.77.169.100	United States	147.237.77.176	matpash.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.64.135.29	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1

08-27-2016-13:04:03 to 08-27-2016-14:04:03