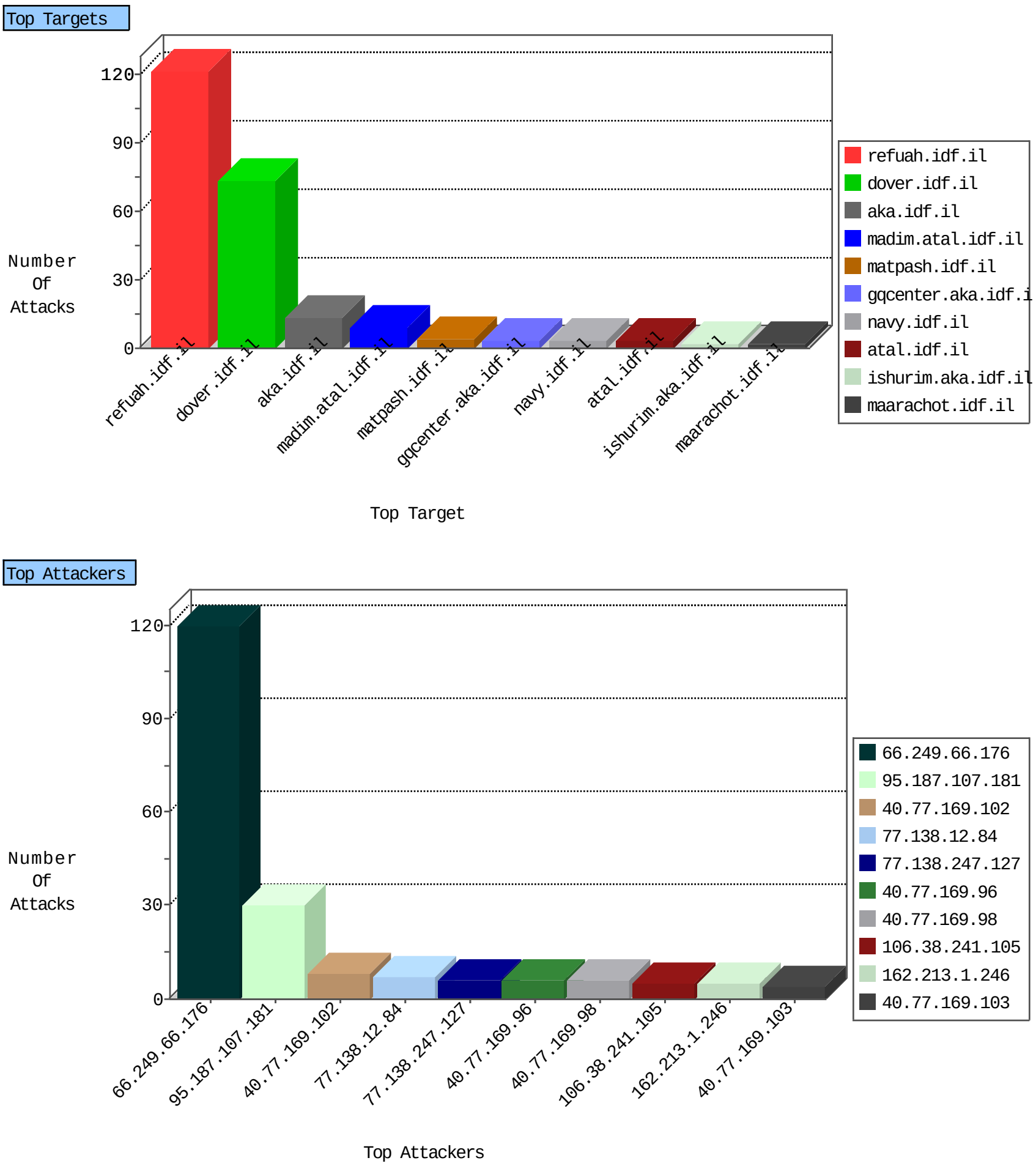
08-23-2016-05:04:02 to 08-23-2016-06:04:02

IDF Under Attack Daily Report



08-23-2016-05:04:02 to 08-23-2016-06:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
63.135.128.2	United States	147.237.76.86	navy.idf.il	Black List	drop	1
206.40.102.223	United States	147.237.76.86	navy.idf.il	Black List	drop	1
61.136.195.22	China	147.237.76.199	e.nakchal.idf.il	JLM_Under_Attack_Con_Http	drop	1

08-23-2016-05:04:02 to 08-23-2016-06:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

08-23-2016-05:04:02 to 08-23-2016-06:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.176	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	120
162.213.1.246	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	5
217.165.67.151	147.237.72.167	United Arab Emirates	ishurim.aka.idf.il	ET SCAN NMAP -sS window 3072	1
195.88.208.193	147.237.76.86	Russian Federation	navy.idf.il	ET SCAN NMAP -sS window 1024	1
190.196.178.78	147.237.76.177	Chile	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.53.196	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.53.196	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.130.56	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
5.255.90.133	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
217.165.67.151	147.237.72.167	United Arab Emirates	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
190.196.178.78	147.237.76.177	Chile	ncore.idf.il	ET SCAN NMAP -sS window 4096	1
163.172.169.150	147.237.0.17	United Kingdom	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
109.226.40.40	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.53.196	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1

08-23-2016-05:04:02 to 08-23-2016-06:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
95.187.107.181	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
106.38.241.105	China	147.237.72.166	aka.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
106.38.241.105	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
141.212.122.94	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
141.212.122.95	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
109.253.216.243	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
74.82.47.40	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
128.232.110.28	United Kingdom	147.237.0.35	akaws.idf.il	drop		drop	1

08-23-2016-05:04:02 to 08-23-2016-06:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.138.12.84	France	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	6
40.77.169.96	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	5
40.77.169.102	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	5
40.77.169.98	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
40.77.169.99	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
40.77.169.101	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
40.77.169.103	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
77.138.247.127	France	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 77.138.247.127	Block	3
77.138.247.127	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.138.247.127	Block	3
37.26.146.190	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
40.77.169.97	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
40.77.169.102	United States	147.237.77.176	matpash.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
40.77.169.100	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
167.220.232.104	Japan	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
66.249.76.79	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
77.138.12.84	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1
207.46.13.126	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/kamlar/klali/default.asp	None	1
66.249.79.37	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.37	Block	1
40.77.169.102	United States	147.237.77.74	law.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
50.200.240.2	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
68.180.230.171	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1393-en/dover.aspx	Block	1
40.77.169.97	United States	147.237.77.234	halag.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.249.66.203	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/m/	Block	1
40.77.169.100	United States	147.237.77.74	law.idf.il	Illegal Byte Code Character in URL /351-en/patzar.aspx#011404	Block	1
75.82.117.252	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
40.77.169.98	United States	147.237.77.176	matpash.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
66.249.76.31	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1683	Block	1
40.77.169.96	United States	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
40.77.169.103	United States	147.237.77.170	maarachot.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
40.77.169.98	United States	147.237.77.176	matpash.idf.il	Illegal Byte Code Character in URL /sip_storage/files/4/3274.pdf#011200	Block	1

08-23-2016-05:04:02 to 08-23-2016-06:04:02