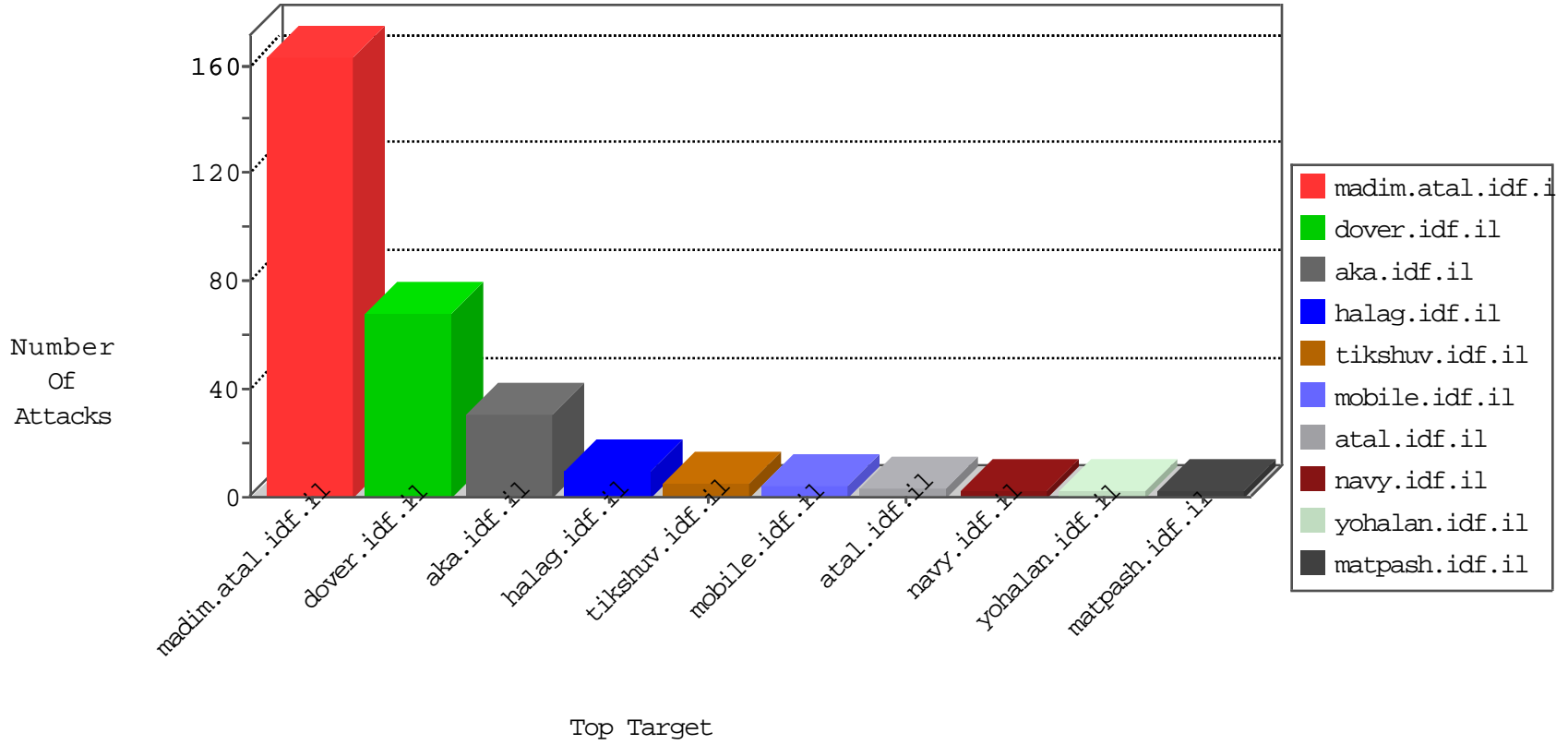


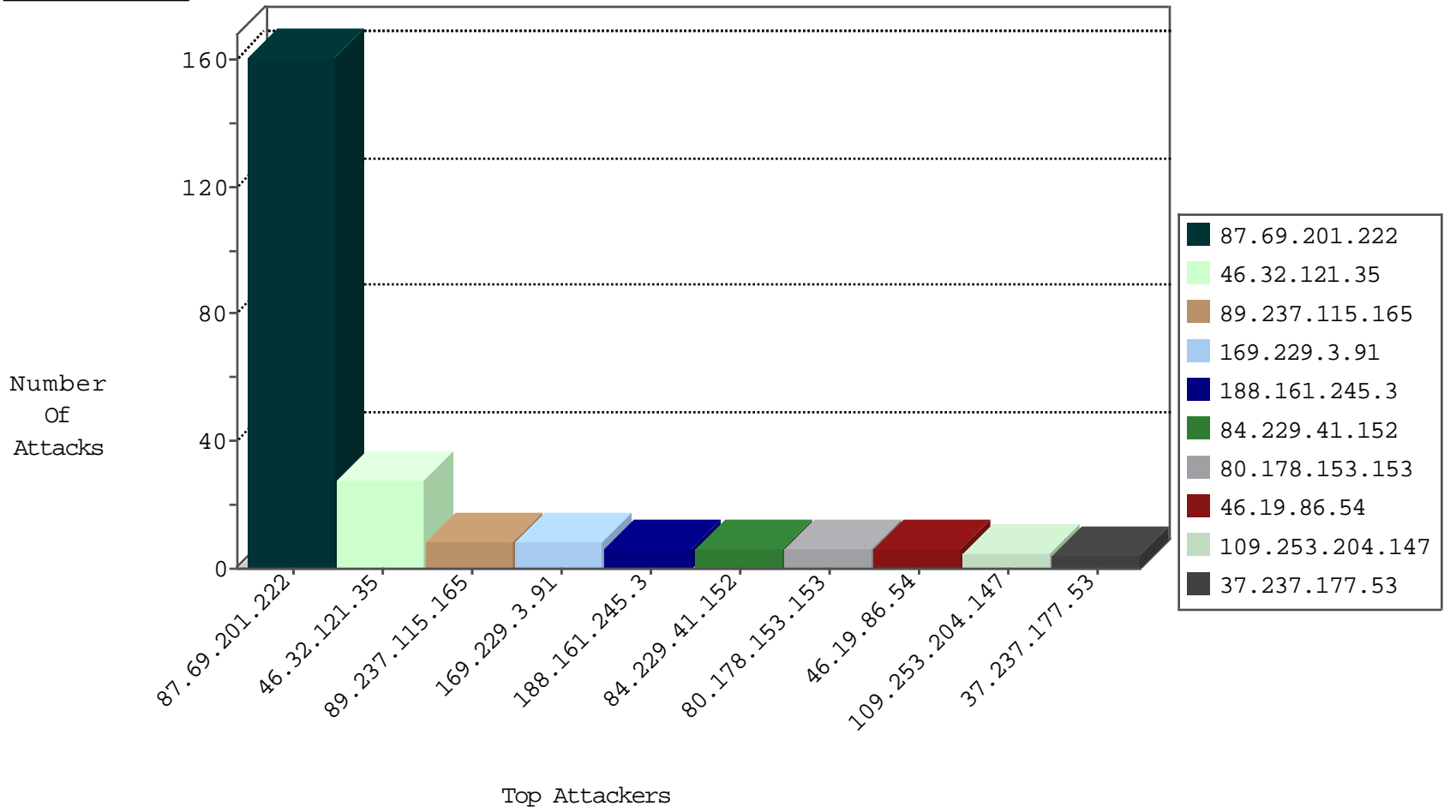
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
8.37.225.125	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
82.80.78.2	Israel	147.237.76.86	navy.idf.il	Black List	drop	2
185.94.111.1	Russian Federation	147.237.76.44	e.refuah.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
164.132.161.76	Italy	147.237.76.200	eitan.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.7	France	147.237.76.200	eitan.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
162.213.1.246	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	4
84.109.180.213	147.237.77.170	Israel	maarachot.idf.il	Xenu Link Sleuth User Agent	2

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.32.121.35	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
89.237.115.165	France	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.54	Israel	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	6
84.229.41.152	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
188.161.245.3	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
80.178.153.153	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	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	First packet isn't SYN	drop	3
178.137.160.45	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
109.67.164.158	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
37.237.177.53	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
144.76.12.75	Germany	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
141.212.122.29	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
176.13.16.226	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
157.55.39.38	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
141.212.122.30	United States	147.237.76.148	ggcenter.aka.idf.il	drop		drop	1
169.229.3.91	United States	147.237.8.28	e.mobile-ks.idf.il	drop	SAM rule	drop	1
109.226.40.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
141.212.122.31	United States	147.237.76.148	ggcenter.aka.idf.il	drop		drop	1
80.178.153.153	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
185.125.4.222	Poland	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.8.50	e.tikshuv.idf.il	drop	SAM rule	drop	1
109.253.207.185	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	1
141.212.122.28	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
77.44.149.114	Syrian Arab Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	drop	SAM rule	drop	1
156.211.35.54	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
31.154.81.44	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
199.30.24.58	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.69.201.222	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	161
109.253.204.147	Israel	147.237.77.234	halag.idf.il	Parameter Type Violation search in www.logistics.atal.idf.il/1213-he/halag.aspx	Block	4
77.139.17.65	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/	Block	2
77.139.104.140	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/giyus/	Block	2
69.159.49.55	Canada	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	2
213.151.35.220	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 213.151.35.220	Block	2
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	2
109.253.212.209	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.213	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
66.249.82.224	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
176.13.11.219	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
66.249.69.112	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/contactus/contactus.aspx	Block	1
109.253.204.147	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
81.218.66.211	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
77.138.255.202	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
213.151.35.220	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/	Block	1
84.108.71.101	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
77.139.17.65	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/smalim/smalim.aspx	Block	1
37.237.177.53	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/favicon.ico	Block	1
86.134.249.201	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
66.249.82.221	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
149.56.223.98	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/blog/	Block	1