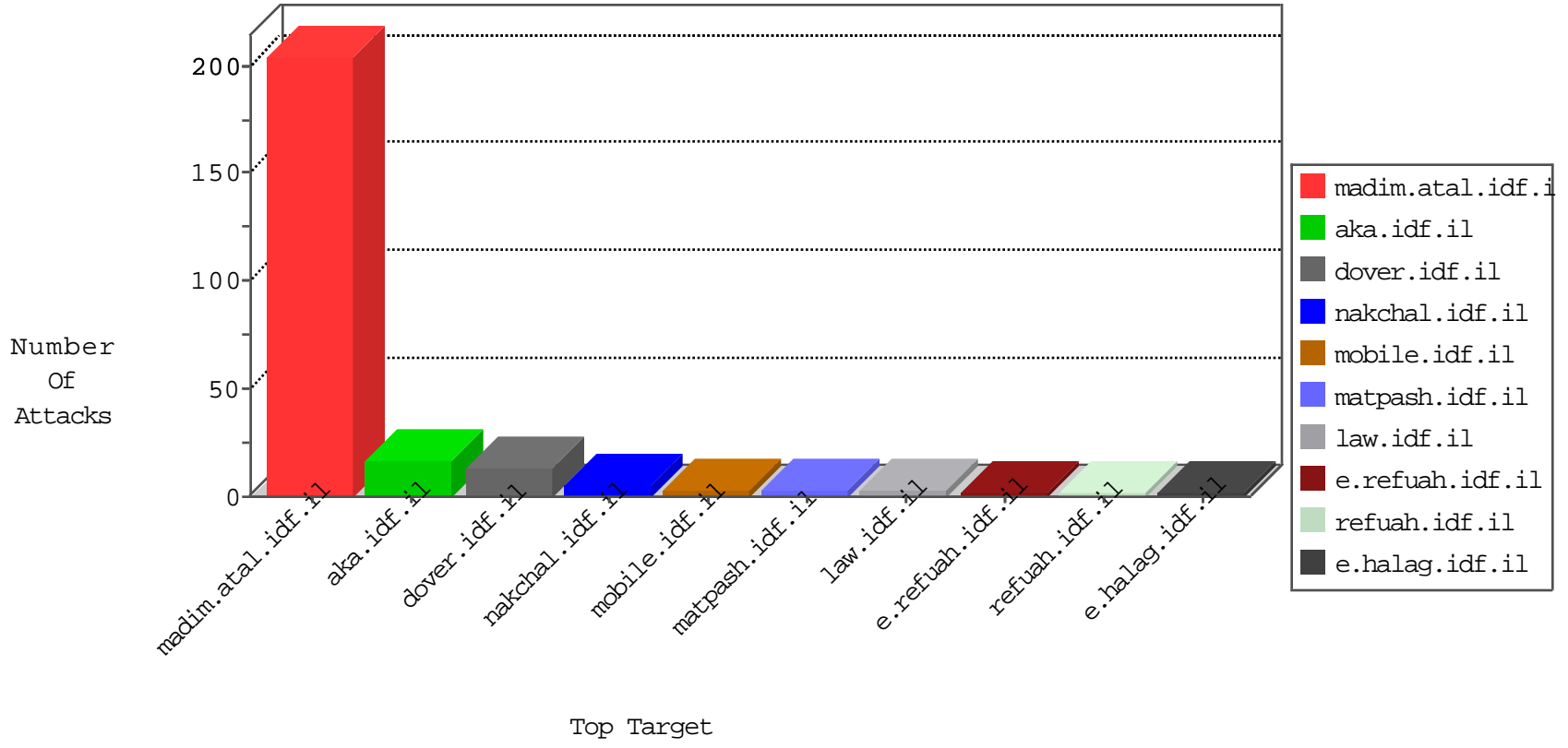


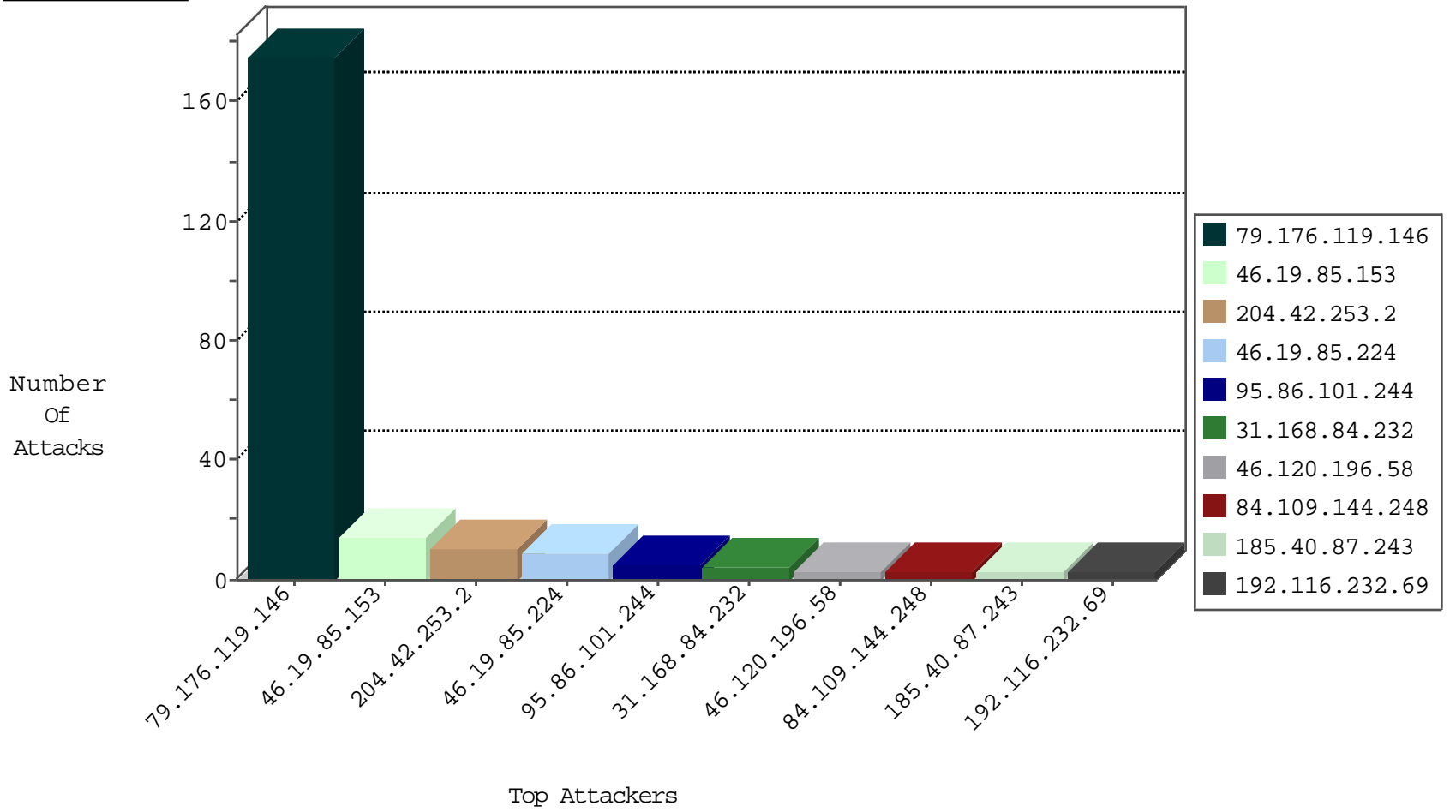
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.42.253.2	United States	147.237.76.201	e.atal.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.196	e.sviva.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.202	e.halag.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.198	e.yohalan.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.200	eitan.aka.idf.il	Black List	drop	2
183.60.48.25	China	147.237.0.17	m.my-kosher-kravi.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
71.6.165.200	United States	147.237.76.44	e.refuah.idf.il	Black List	drop	1
185.40.87.243	Turkey	147.237.0.35	akaws.idf.il	I4 Source or Dest Port Zero	drop	1
79.181.170.74	Israel	147.237.77.243	mobile.idf.il	Invalid TCP Flags	drop	1
185.40.87.243	Turkey	147.237.8.28	e.mobile-ks.idf.il	I4 Source or Dest Port Zero	drop	1
82.80.78.2	Israel	147.237.77.216	dover.idf.il	Black List	drop	1
185.40.87.243	Turkey	147.237.76.44	e.refuah.idf.il	I4 Source or Dest Port Zero	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.255.65.31	France	147.237.76.86	navy.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
80.169.91.26	United Kingdom	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
84.109.180.213	147.237.77.74	Israel	law.idf.il	Xenu Link Sleuth User Agent	2
151.80.40.87	147.237.77.176	France	matpash.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
66.249.66.187	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.120.196.58	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
79.178.254.224	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
136.243.152.18	Germany	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
141.212.122.59	United States	147.237.0.200	m4u.idf.il	drop		drop	1
141.212.122.60	United States	147.237.0.200	m4u.idf.il	drop		drop	1
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
85.130.129.120	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	1
213.57.136.111	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
216.243.31.2	United States	147.237.76.148	ggcenter.aka.idf.il	drop		drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.176.119.146	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	175
46.19.85.153	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
46.19.85.224	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
95.86.101.244	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/7/	Block	5
84.109.144.248	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
31.168.84.232	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	2
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	2
85.250.172.173	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
143.160.27.189	South Africa	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/sites/home/default.asp	Block	2
66.249.64.174	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.tech.atal.idf.il/mobile/	Block	1
31.154.49.161	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
157.55.39.176	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to ww.idf.il/aman	Block	1
199.30.16.179	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to ww.idf.il/error.htm	Block	1
109.253.143.33	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.187	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
31.168.84.232	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 31.168.84.232	Block	1
180.76.15.32	China	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/robots.txt	Block	1
66.102.9.85	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
207.46.13.39	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/home/default.aspx	Block	1
109.253.220.202	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchildsubcategories/1423	Block	1
66.249.76.51	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
66.249.64.135	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
217.132.240.226	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
139.59.132.56	Singapore	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/ishurim/main/	Block	1
68.180.228.185	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to ww.idf.il/1294-he/www.idf.il	Block	1
31.168.84.232	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakchal.idf.il/sip_storage/files/2/	Block	1
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to ww.idf.il/images/1.he/titlecap.png	Block	1
89.139.131.247	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.64.161	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
68.180.228.231	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1927-he/cogat.aspx	Block	1
192.198.151.36	Europe	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1