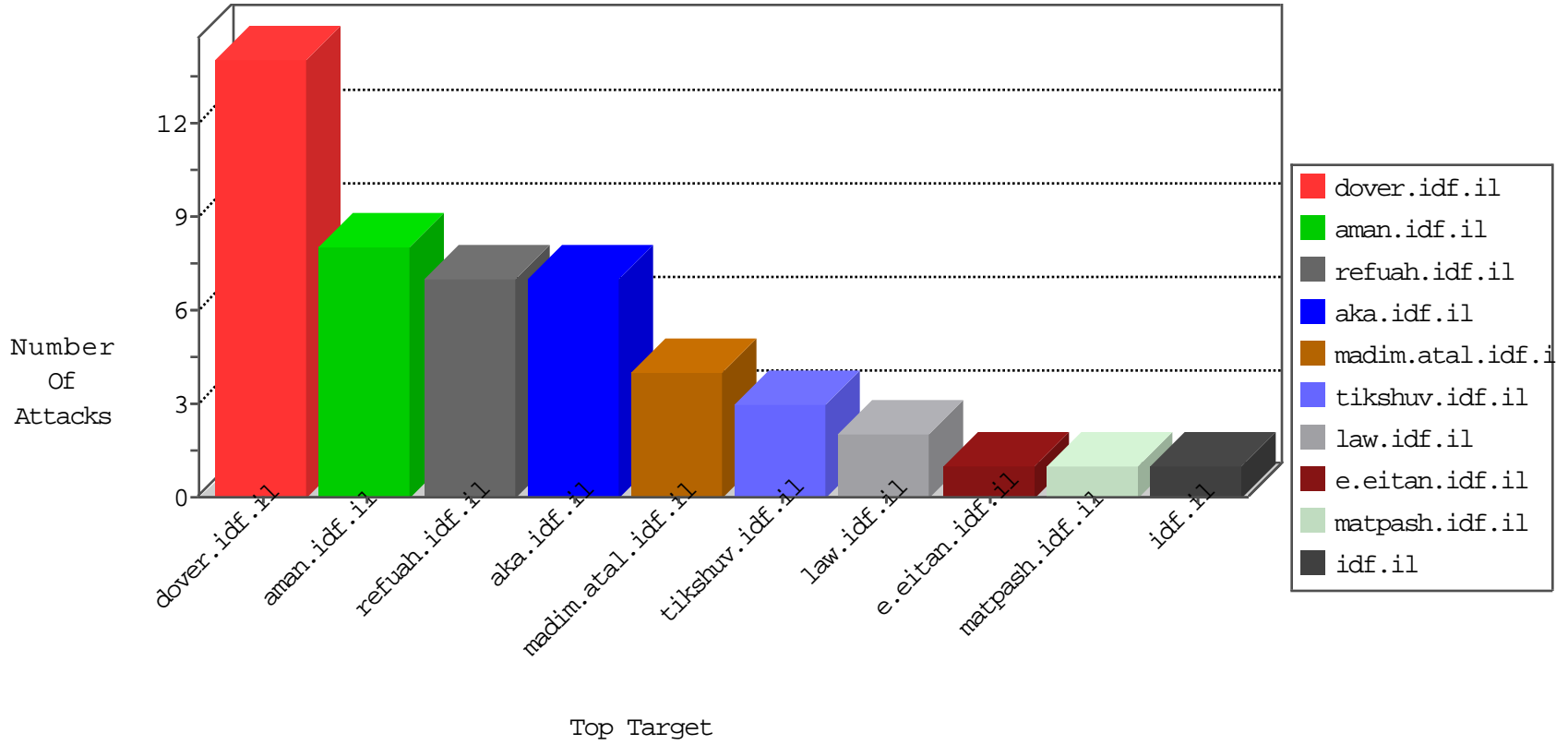


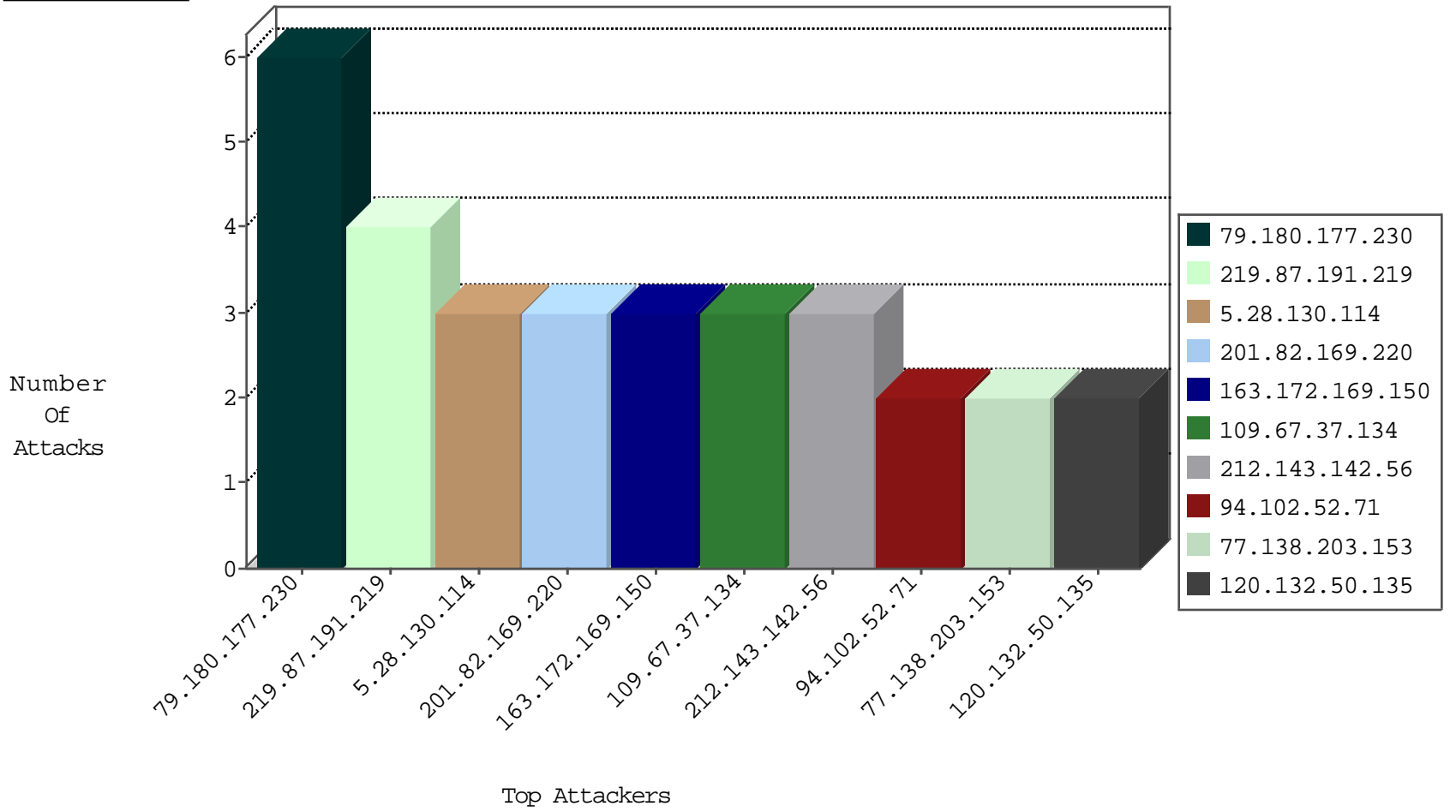
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
120.132.50.135	China	147.237.77.74	law.idf.il	block-sp-trafl	forward	2
89.248.167.131	Netherlands	147.237.76.44	e.refuah.idf.il	Black List	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
176.47.34.179	147.237.77.216	Saudi Arabia	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
163.172.169.150	147.237.76.39	United Kingdom	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
120.50.122.198	147.237.0.19	Korea, Republic of	madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.102.52.71	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
83.84.137.88	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
219.87.191.219	147.237.76.38	Taiwan	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
219.87.191.219	147.237.0.33	Taiwan	idf.il	ET SCAN Potential SSH Scan	1
179.32.110.250	147.237.0.34	Colombia	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
163.172.169.150	147.237.76.42	United Kingdom	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.76.30	United Kingdom	himush.idf.il	ET SCAN NMAP -sS window 1024	1
103.207.39.11	147.237.77.176	Vietnam	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.52.71	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
219.87.191.219	147.237.76.176	Taiwan	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
219.87.191.219	147.237.0.34	Taiwan	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
190.252.168.195	147.237.0.34	Colombia	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.180.177.230	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
201.82.169.220	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
91.240.80.24	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.67.37.134	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/1325-he/refuah.aspx)	Block	3
5.28.130.114	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	2
77.138.203.153	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/haredim/general.aspx	Block	2
109.64.56.239	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1
66.102.9.2	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/0/70980.pdf	Block	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/brothers/news/default.asp	Block	1
131.253.27.189	United States	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	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
5.226.86.2	Poland	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
207.46.13.107	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/view_moreinfo.asp	Block	1
66.249.66.197	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-22193-he/idfgdover.aspx	Block	1
107.3.29.210	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
40.77.167.8	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
207.46.13.191	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/faq.aspx	Block	1
66.249.69.67	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1410-he/refuah.aspx	Block	1