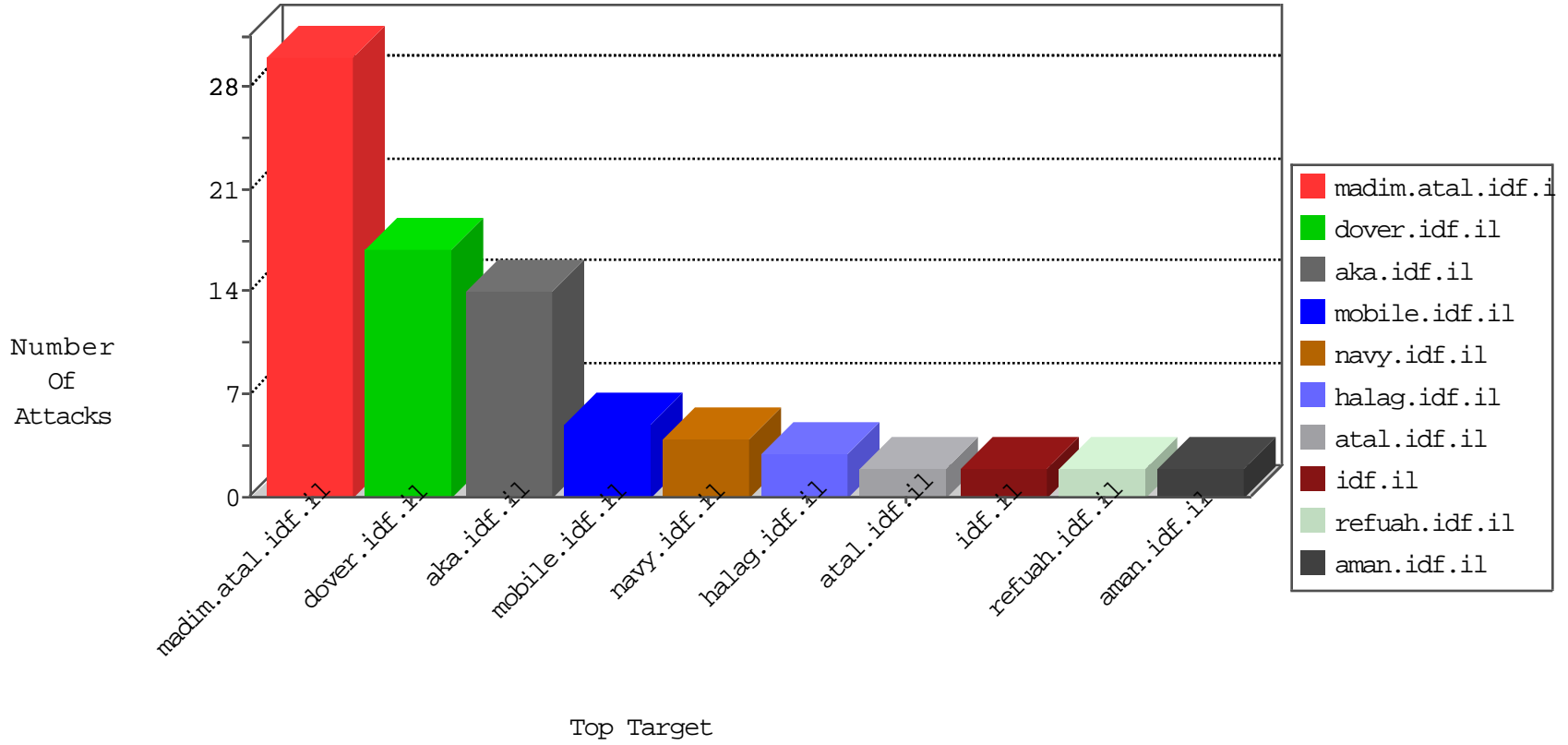


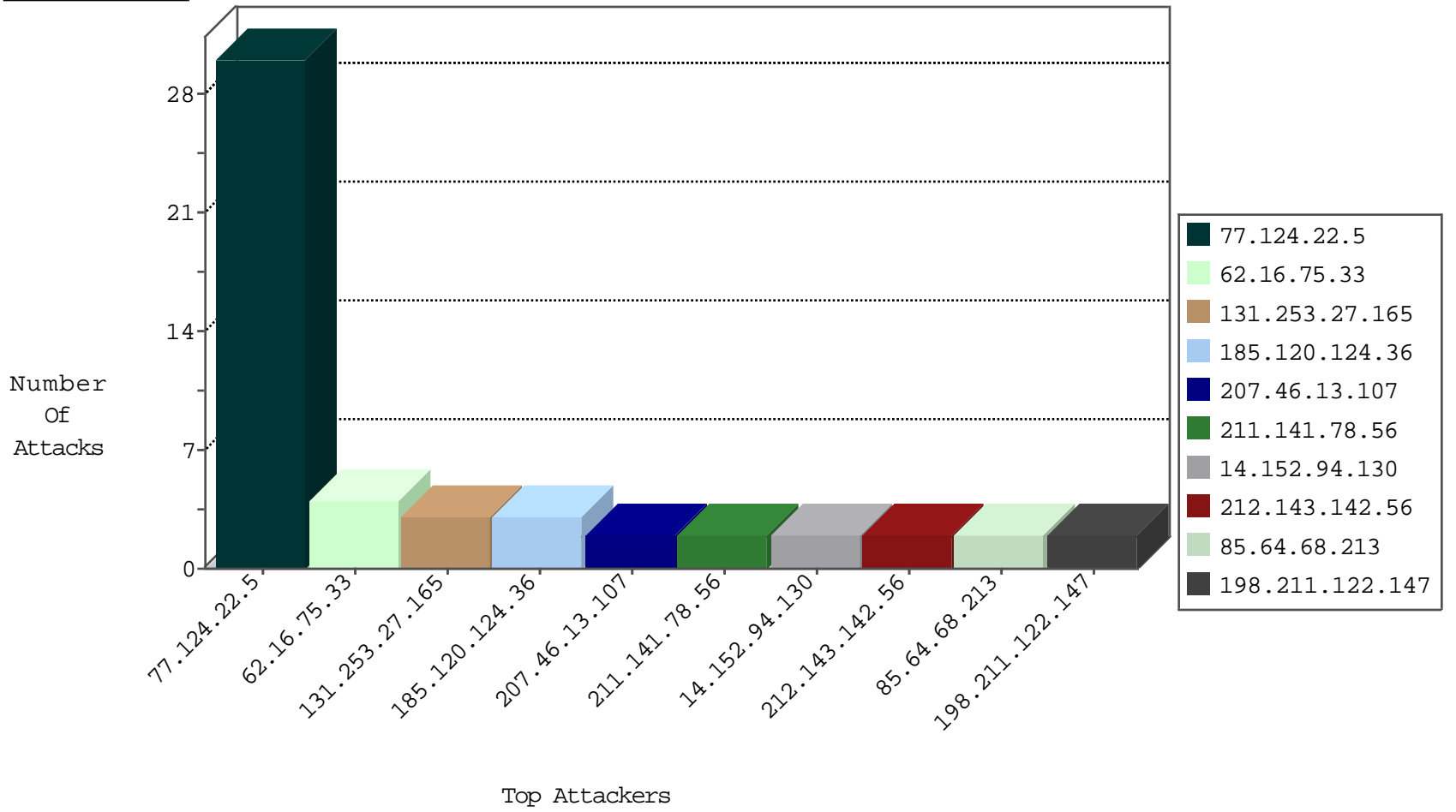
# IDF Under Attack Daily Report



## Top Targets



## Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
142.0.39.182	United States	147.237.77.243	mobile.idf.il	JLM_Purple_Con_Limit_Tcp	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
211.141.78.56	147.237.0.35	China	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
198.211.122.147	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
176.47.110.20	147.237.77.176	Saudi Arabia	matpash.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
161.18.113.42	147.237.77.216	Colombia	dover.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
61.240.144.66	147.237.0.200	China	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
14.152.94.130	147.237.76.86	China	navy.idf.il	ET SCAN NMAP -f -sS	1
220.242.82.131	147.237.76.86	China	navy.idf.il	ET SCAN NMAP -f -sS	1
211.141.78.56	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 1024	1
198.211.122.147	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.238.40	147.237.0.16	United Kingdom	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.76.69	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	1
14.152.94.130	147.237.76.86	China	navy.idf.il	ET SCAN NMAP -sS window 2048	1
220.242.82.131	147.237.76.86	China	navy.idf.il	ET SCAN NMAP -sS window 2048	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
62.16.75.33	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
178.162.205.25	Germany	147.237.76.148	ggcenter.aka.idf.il	drop		drop	1
216.243.31.2	United States	147.237.0.33	idf.il	drop		drop	1
79.177.178.200	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.124.22.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
185.120.124.36	Israel	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	3
131.253.27.165	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
91.4.151.238	Germany	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
207.46.13.107	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
85.64.68.213	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 85.64.68.213	Block	1
66.249.76.79	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/gyus/forum/asp/showforum.asp	Block	1
37.142.184.236	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1400-he/atal.aspx	Block	1
77.138.79.114	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
66.102.9.13	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
85.64.68.213	Israel	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/atal1/izkor/view_imgtop.asp	Block	1
46.19.86.50	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
194.242.168.227	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/gyus/sitemap.aspx	Block	1
79.176.125.229	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.102.9.21	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/faq.asp	Block	1
2.53.1.26	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/redirects/ssl-redirect.html	Block	1
46.19.86.138	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
207.46.13.90	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	1
79.179.197.215	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.69.67	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1305-he/refuah.aspx	Block	1
2.53.176.33	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
46.20.83.217	Italy	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
82.166.228.10	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
5.29.54.7	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mas.aspx	None	1
176.13.250.53	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
77.138.8.255	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/gyus/kadatz/	Block	1
65.55.210.177	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1