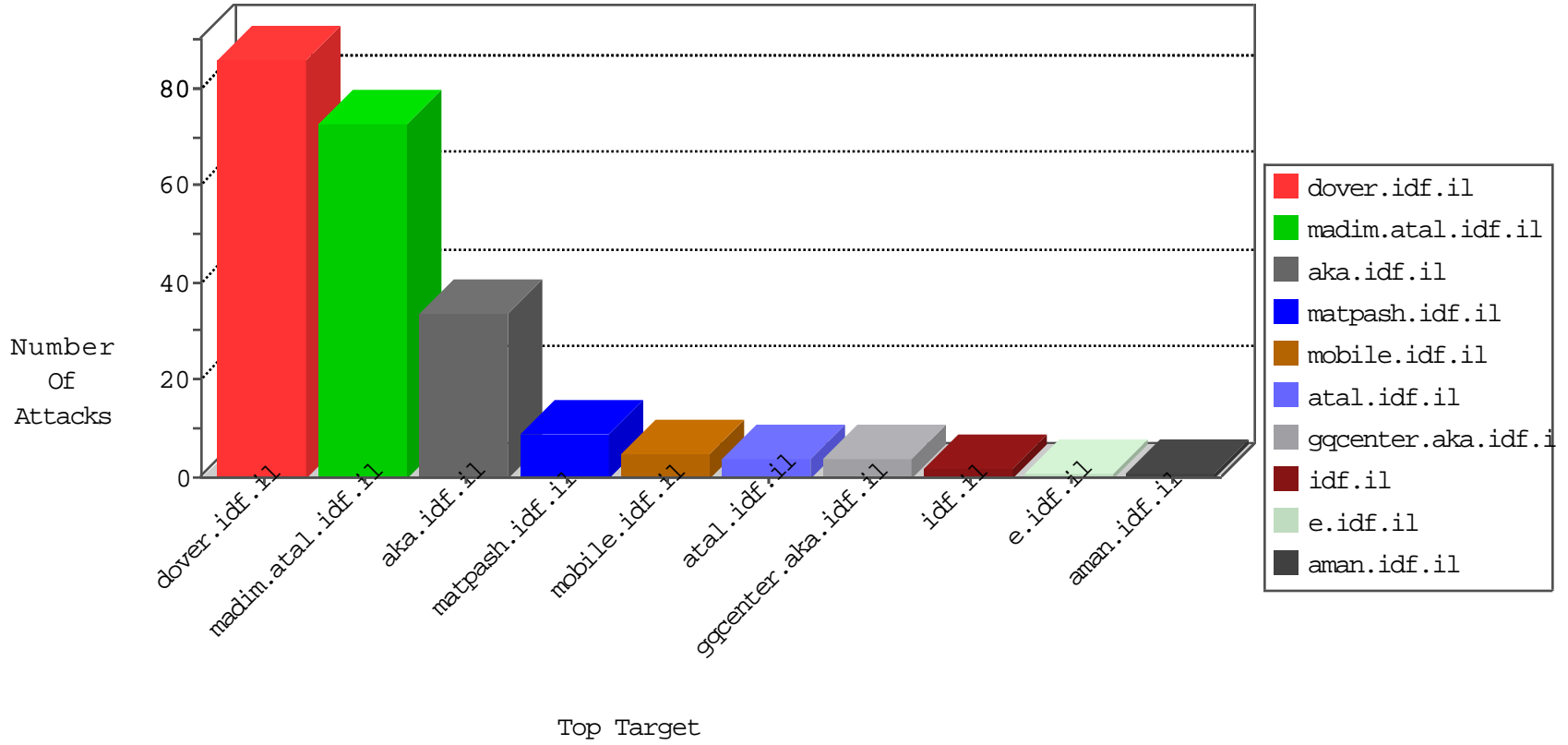


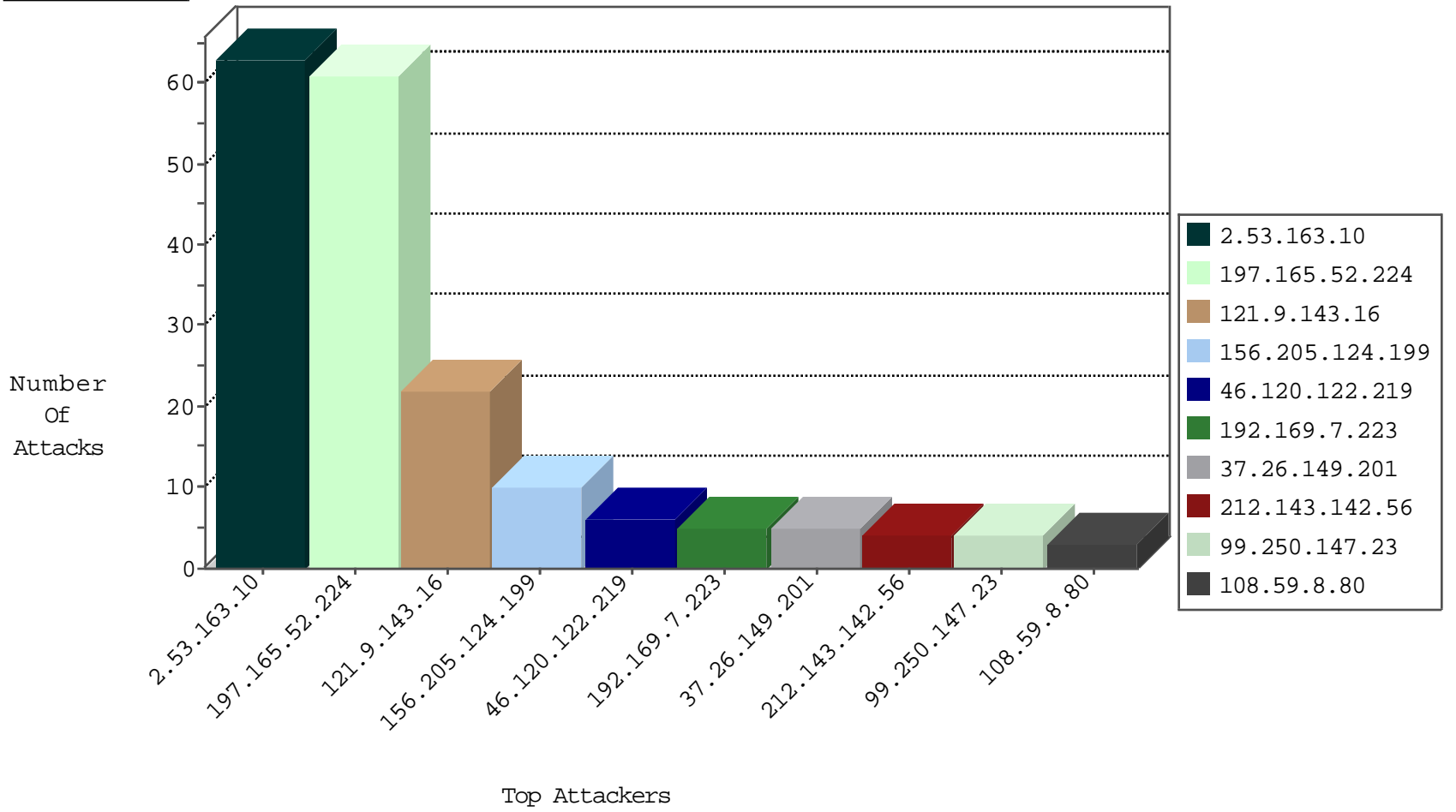
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
156.205.124.199	Egypt	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	9
197.165.52.224	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
185.94.111.1	Russian Federation	147.237.76.30	himush.idf.il	Black List	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.165.197.142	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
108.59.8.80	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.77.176	Israel	matpash.idf.il	Xenu Link Sleuth User Agent	6
87.115.230.45	147.237.77.176	United Kingdom	matpash.idf.il	Tehila - Perl LWP with fake user agent	2
94.102.48.195	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.91.29	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
198.167.223.33	147.237.72.217	Saint Kitts and Nevis	e.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
197.165.52.224	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
192.169.7.223	United States	147.237.76.148	ggcenter.aka.idf.il	drop		drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.253.137.182	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
120.76.24.17	China	147.237.0.33	idf.il	drop		drop	1
207.46.13.64	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
65.242.97.127	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.12.143	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
66.249.69.10	Israel	147.237.0.33	idf.il	drop		drop	1
177.131.48.59	Brazil	147.237.76.34	yohalan.idf.il	drop		drop	1
79.177.25.32	Israel	147.237.72.156	aman.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
2.53.163.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	63
121.9.143.16	China	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 121.9.143.16	Block	15
121.9.143.16	China	147.237.72.166	aka.idf.il	PHP Attempt	Block	6
37.26.149.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
37.26.147.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
99.250.147.23	Canada	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 99.250.147.23	Block	3
80.246.137.95	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
77.126.28.208	Israel	147.237.77.233	atal.idf.il	Suspicious Response Code	Block	2
2.53.31.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.55.29.44	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
207.46.13.93	United States	147.237.77.233	atal.idf.il	Abnormally Long Request URL	Block	1
99.250.147.23	Canada	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
66.249.79.60	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/apple-app-site-association	Block	1
156.205.124.199	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1141-ar/	Block	1
82.66.92.107	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 82.66.92.107	Block	1
157.55.39.97	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
82.66.92.107	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/french	Block	1
77.126.28.208	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
185.24.76.139	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
89.237.111.92	France	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
46.19.85.20	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
121.9.143.16	China	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
79.177.37.222	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.173.5	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/894-ar	Block	1
192.169.7.223	United States	147.237.76.42	refuah.idf.il	Unauthorized Method HEAD for 147.237.76.42/	Block	1
46.116.172.133	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	1
148.251.2.180	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/iturim/asp/displayonesoldier.asp	Block	1