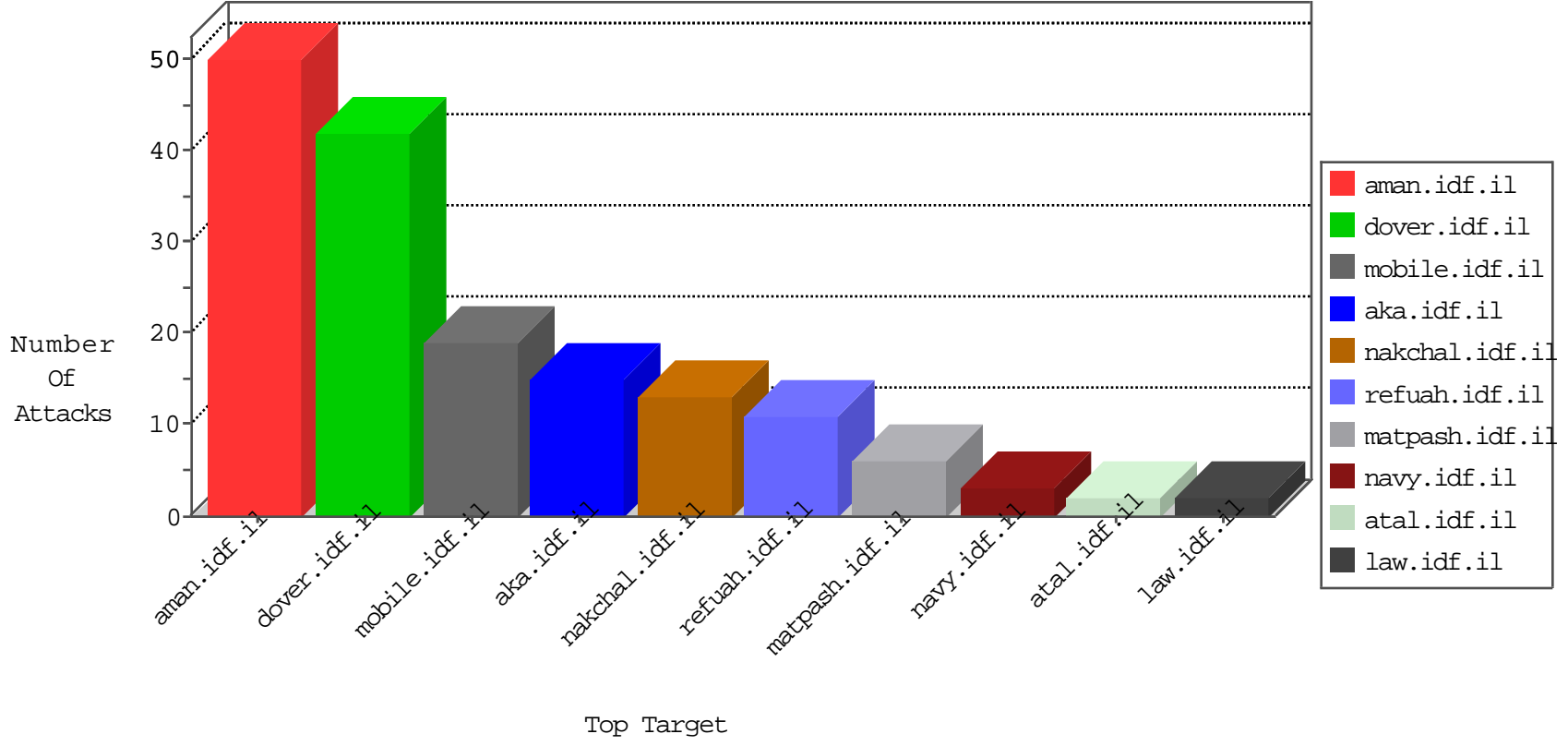


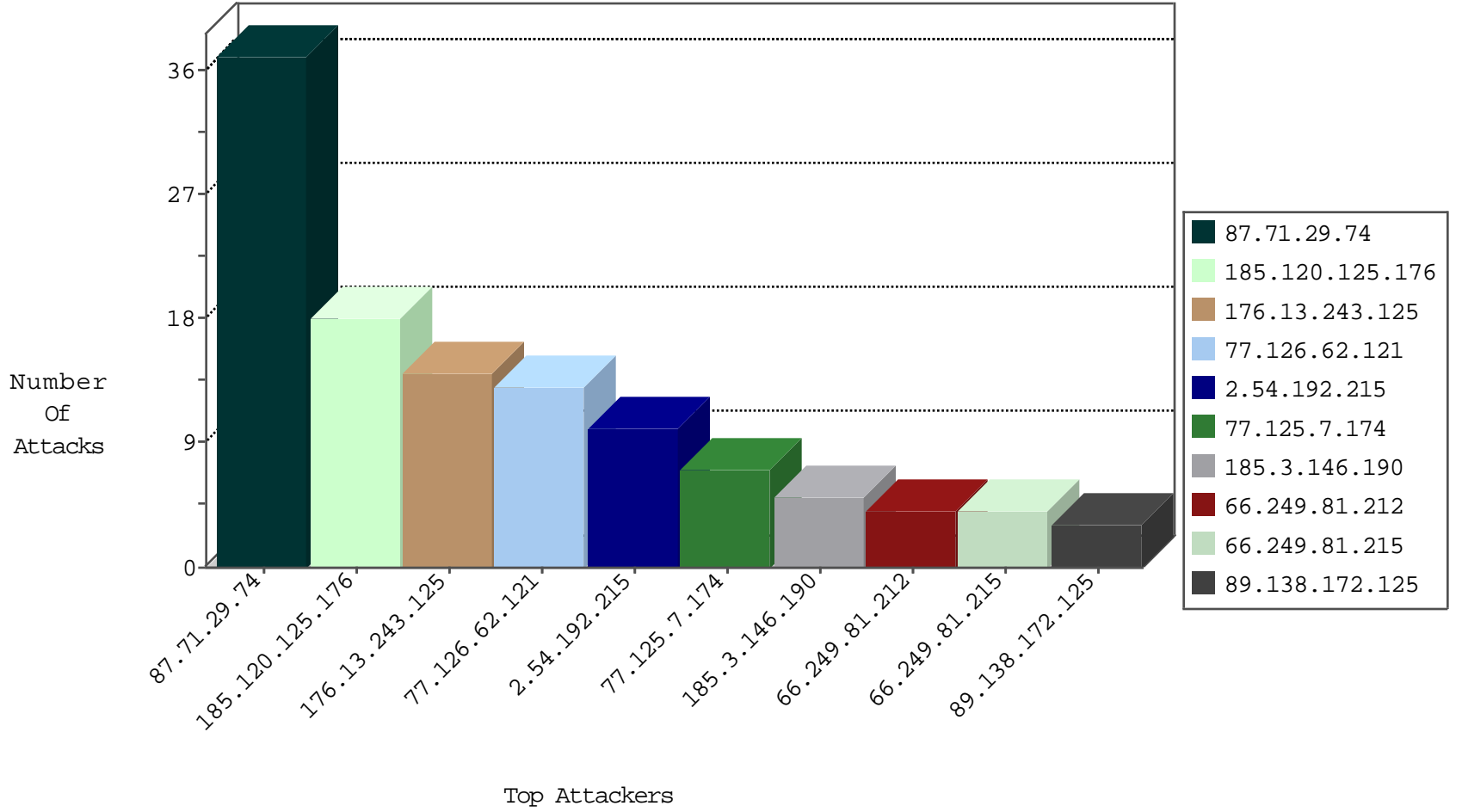
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.221.105.6	Iceland	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
158.69.244.42	United States	147.237.76.86	navy.idf.il	Black List	drop	1
179.99.200.39	Brazil	147.237.76.39	mobile.meitav.idf.il	block-sp-trafl	forward	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
91.121.106.226	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
162.213.1.246	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1
110.55.107.68	147.237.76.86	Philippines	navy.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
66.249.93.185	147.237.76.86	Europe	navy.idf.il	ET SCAN NMAP -sA (2)	1
191.109.210.200	147.237.0.34	Colombia	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
113.190.3.30	147.237.77.176	Vietnam	matpash.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
93.174.93.99	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
80.117.21.75	147.237.8.46	Italy	e.chinuch.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.227.67.172	147.237.76.202	Sweden	e.halag.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
185.120.125.176	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
2.54.192.215	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	7
2.54.192.215	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.176.30.13	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
109.64.9.11	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
178.240.166.180	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.66.197.210	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
87.71.29.74	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	37
176.13.243.125	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	14
77.126.62.121	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	7
77.125.7.174	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	7
185.3.146.190	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/resource/userfollowresource/create/	Block	5
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
77.126.62.121	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakchal.idf.il/sip_storage/files/2/	Block	4
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
89.138.172.125	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
77.126.62.121	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 77.126.62.121	Block	2
213.57.158.186	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
37.142.184.29	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus	Block	2
109.65.95.49	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/kiosk/kiosk.aspx	Block	2
66.249.69.67	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	1
207.46.13.191	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
148.251.2.180	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
79.177.41.220	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
31.154.81.57	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.aspx/getauthuser	Block	1
109.64.109.7	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.64.109.7	Block	1
66.249.69.72	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/3058.jpg	Block	1
157.55.39.8	United States	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
85.250.159.51	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1437-he/atal.aspx	Block	1
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
203.127.58.234	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.64.109.7	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/9/	Block	1
219.75.81.197	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.69.127	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/3296.jpg	Block	1
176.13.240.127	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
68.180.228.99	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
46.117.14.189	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
203.127.96.244	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.65.35.186	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
77.139.218.35	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
220.255.183.170	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
46.117.124.97	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
203.127.96.252	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
78.46.23.198	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/yohalan/	Block	1
5.102.242.155	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/homepage/homepage.aspx	Block	1
176.106.47.211	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
89.138.184.111	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1