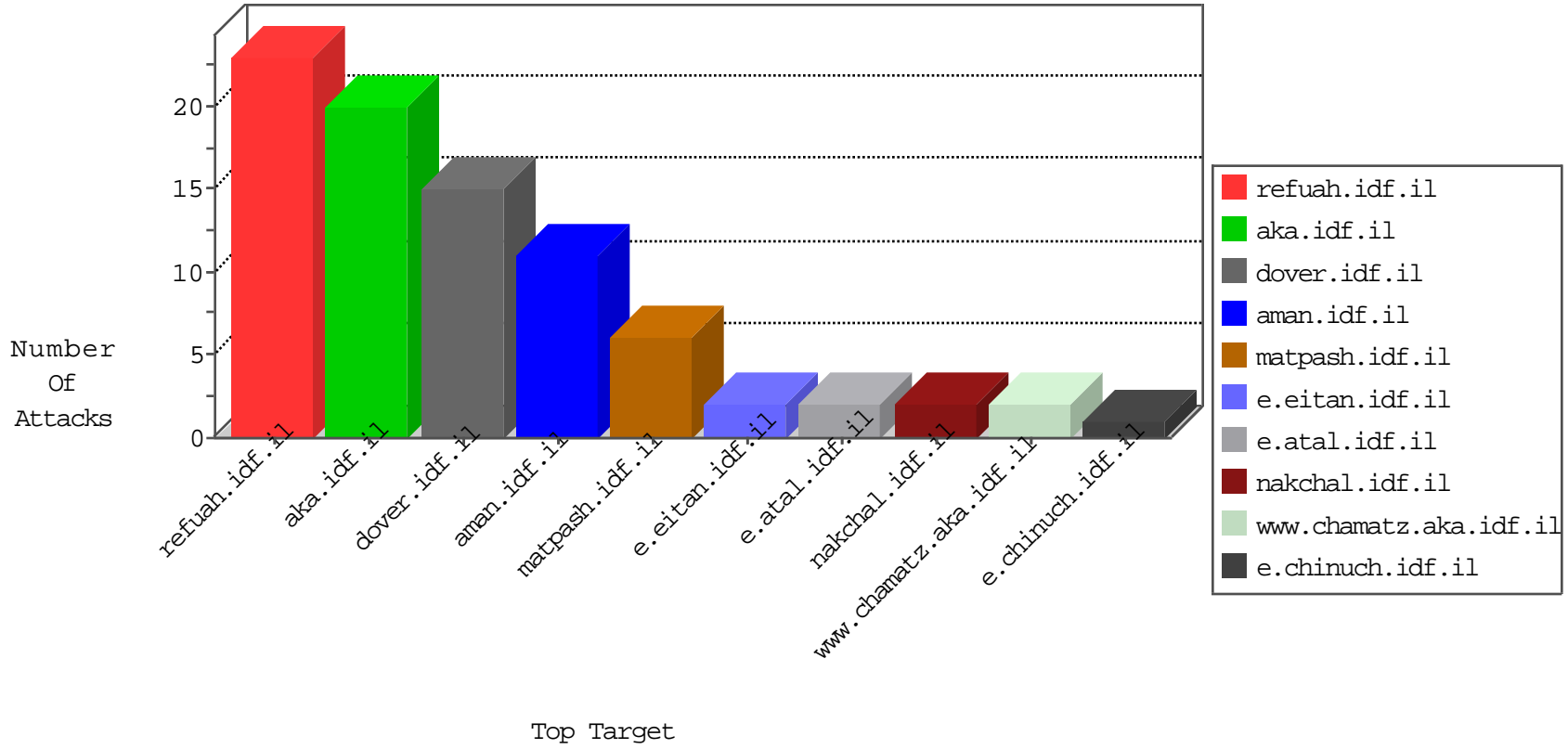


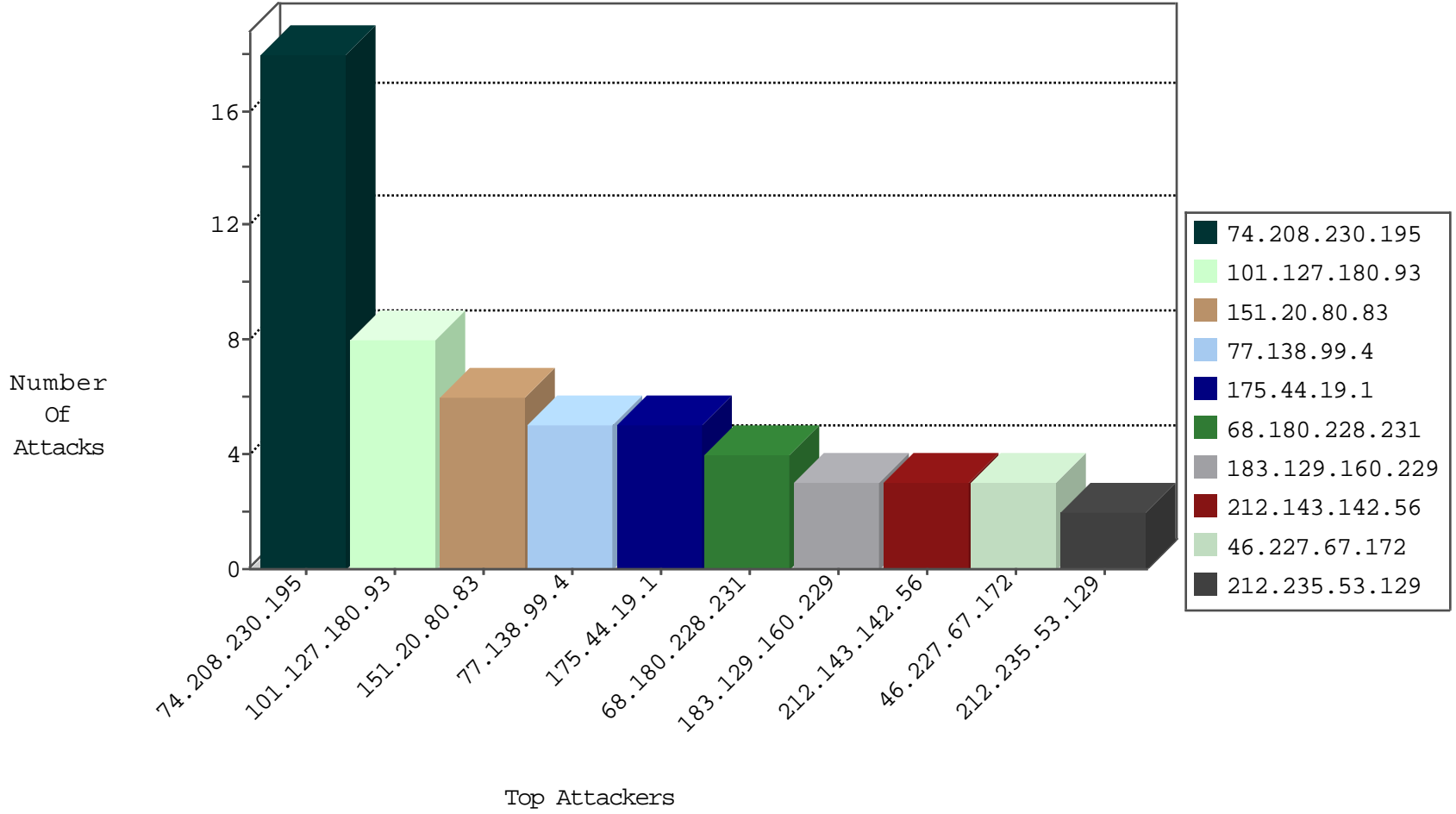
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.42.253.132	United States	147.237.76.201	e.atal.idf.il	Black List	drop	1
71.6.158.166	United States	147.237.76.31	nakchal.idf.il	Black List	drop	1
91.230.107.174	Russian Federation	147.237.76.176	test.ncore.idf.il	Black List	drop	1

09-03-2016-09:04:07 to 09-03-2016-10:04:07

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
208.100.26.228	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 1024	1
117.135.131.60	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
66.249.76.112	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
46.227.67.172	147.237.8.46	Sweden	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
45.63.30.95	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
219.87.191.219	147.237.76.201	Taiwan	e.atal.idf.il	ET SCAN Potential SSH Scan	1
122.224.250.234	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 1024	1
87.236.194.161	147.237.72.217	Czech Republic	e.idf.il	ET SCAN NMAP -sS window 1024	1
46.227.67.172	147.237.8.50	Sweden	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
46.227.67.172	147.237.8.45	Sweden	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
219.87.191.219	147.237.76.202	Taiwan	e.halag.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
74.208.230.195	United States	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	18
101.127.180.93	Singapore	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	8
151.20.80.83	Italy	147.237.77.216	dover.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
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
203.219.208.156	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
183.129.160.229	China	147.237.8.28	e.mobile-ks.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	1
176.13.15.21	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
89.139.215.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.8.24	e.lifestyle.idf.il	drop	SAM rule	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
68.180.228.231	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-ar/cogat.aspx	Block	4
175.44.19.1	China	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 175.44.19.1	Block	4
77.138.99.4	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/ishurim/main/	Block	2
77.138.99.4	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.138.99.4	Block	2
46.120.38.133	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
212.235.53.129	Israel	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
79.181.113.163	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.75.115	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
212.235.53.129	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-login.php	Block	1
84.229.3.29	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.76.72	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/default.	Block	1
2.53.149.155	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
175.44.19.1	China	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.41	Block	1
216.244.66.233	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/miluiml/	Block	1
148.251.2.180	Germany	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	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
5.29.73.104	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	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
77.138.99.4	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	1
66.249.64.47	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/sip_storage/files/0/1920.doc	Block	1
157.55.39.71	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
46.117.251.80	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
204.79.180.47	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
79.181.105.241	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.64.49	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/robots.txt	Block	1
157.55.39.160	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1