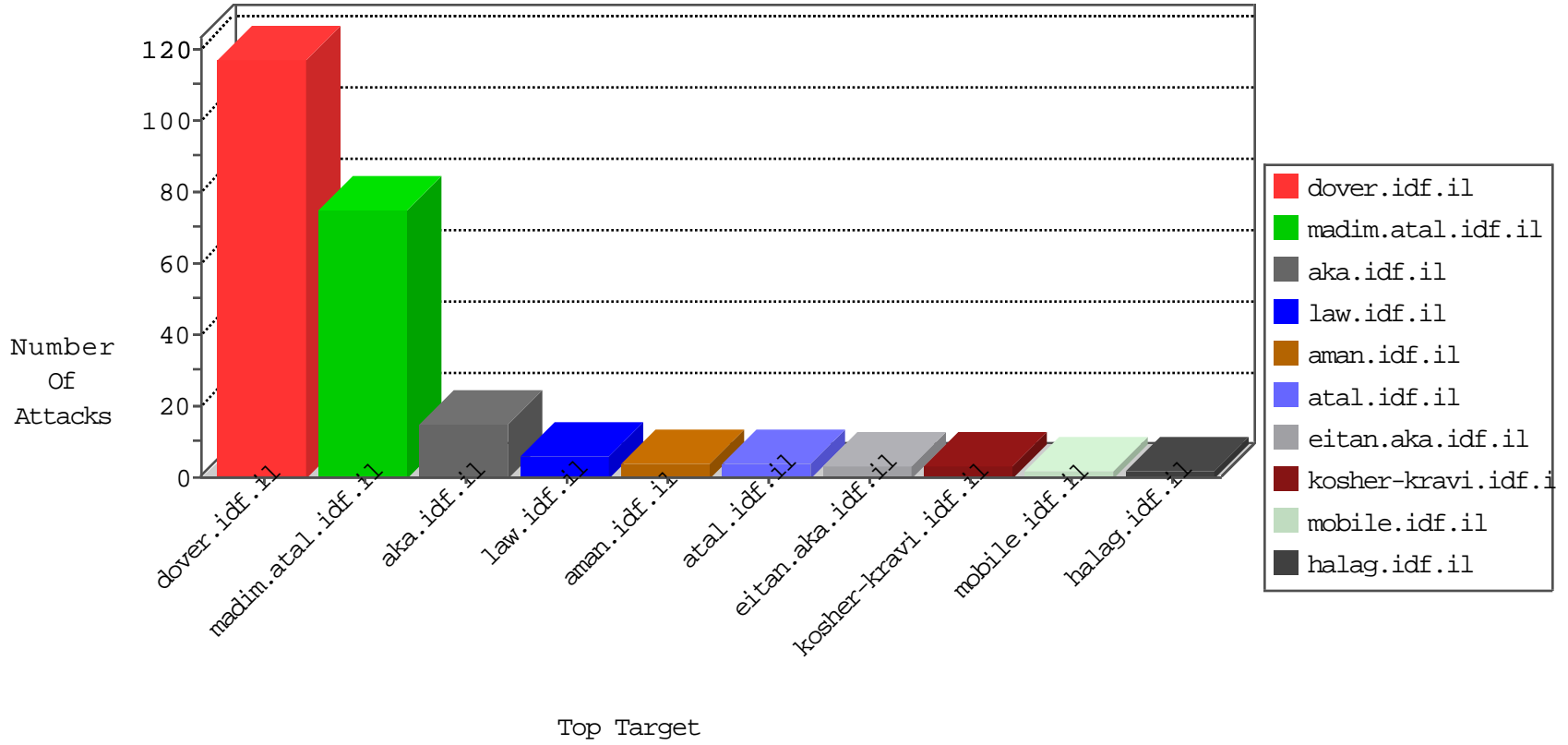


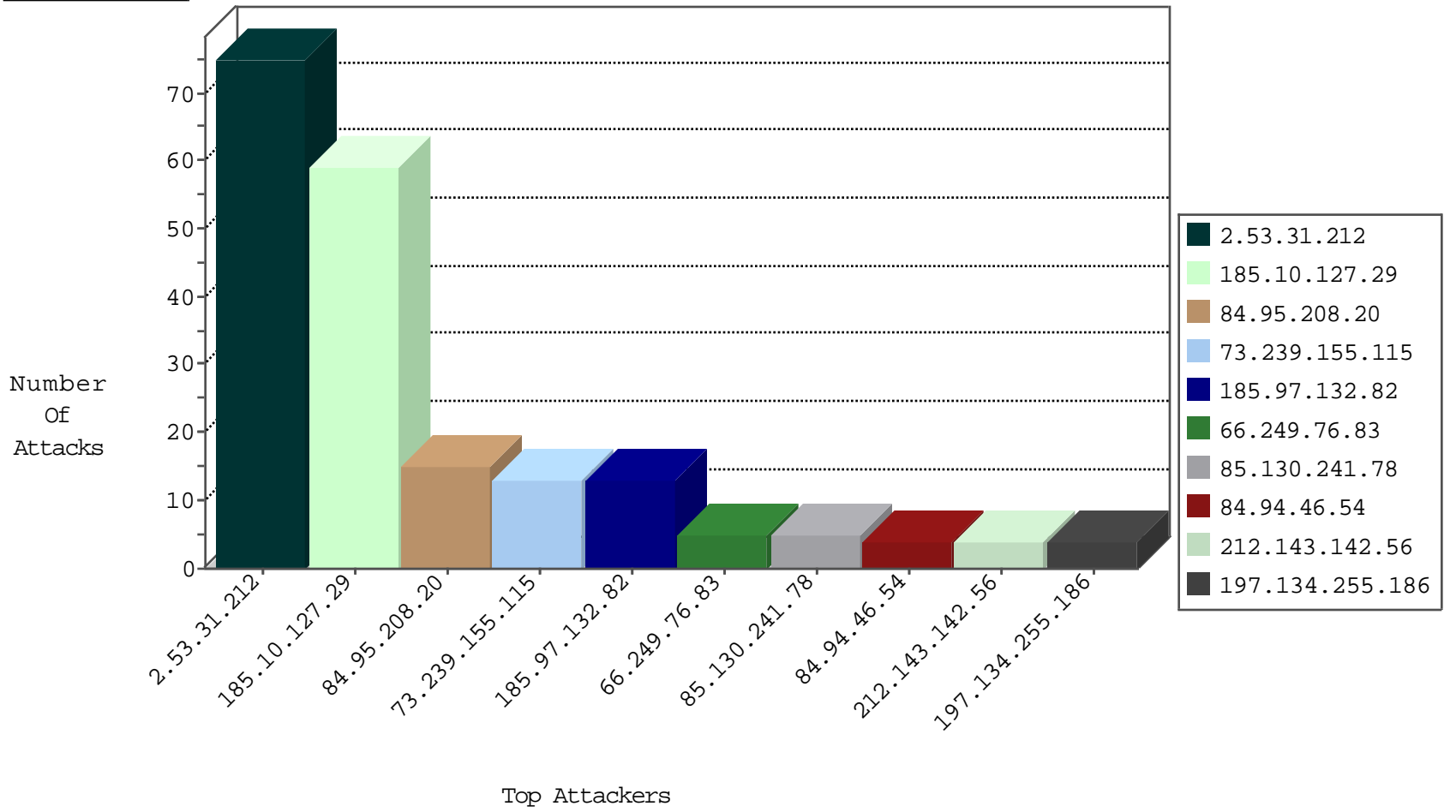
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.97.132.82	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	39

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.197.177.50	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
46.4.116.197	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	2
51.255.65.68	France	147.237.76.200	eitan.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.97	France	147.237.76.200	eitan.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
89.248.167.131	Netherlands	147.237.8.50	e.tikshuv.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
164.132.161.31	Italy	147.237.76.200	eitan.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
162.213.1.246	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	4

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.10.127.29	Hungary	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
73.239.155.115	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
197.134.255.186	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
85.130.241.78	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
109.253.136.199	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.13.238.213	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	2
85.130.241.78	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.13.226.15	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
212.143.142.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.0.200	m4u.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.76.34	yohalan.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.76.196	e.sviva.idf.il	drop	SAM rule	drop	1
40.77.167.64	United States	147.237.77.216	dover.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
2.53.31.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	75
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
84.94.46.54	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	2
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
77.138.255.202	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	2
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/default.aspx	Block	1
77.138.245.97	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	1
188.53.172.10	Saudi Arabia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
66.249.66.213	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
199.30.25.22	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
84.94.46.54	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/wp-login.php	Block	1
157.55.39.110	United States	147.237.77.216	dover.idf.il	Abnormally Long Request URL	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	PHP Attempt	Block	1
77.139.71.96	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1
207.46.13.20	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
84.94.61.63	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/giyus/login.aspx	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
157.55.39.138	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/62532.pdfq2=whvq9jgvov3igm-0flegda	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
77.237.138.202	Czech Republic	147.237.77.233	atal.idf.il	Unauthorized URL Access to /	Block	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/div.item	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
188.52.79.177	Saudi Arabia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
84.94.46.54	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 84.94.46.54	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1