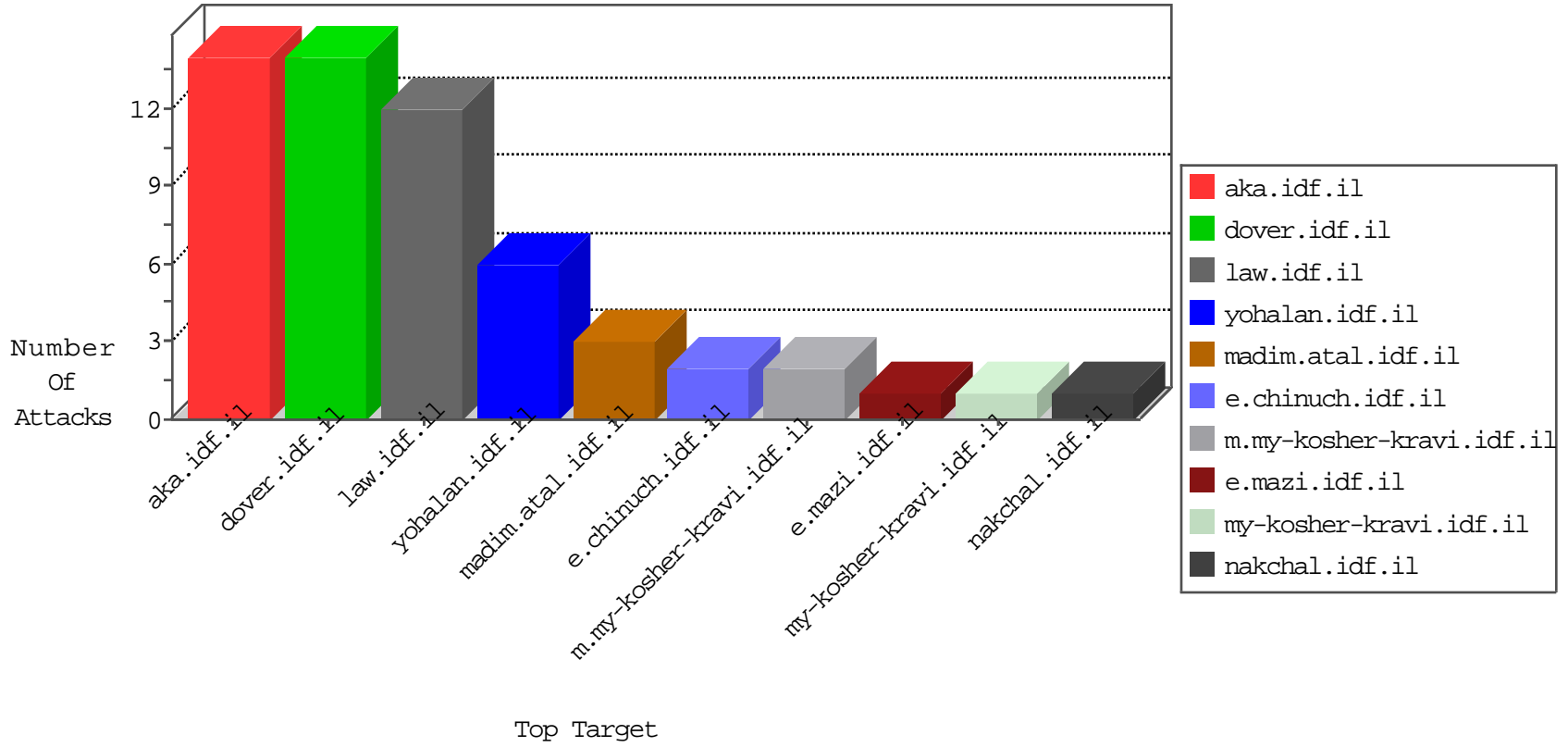


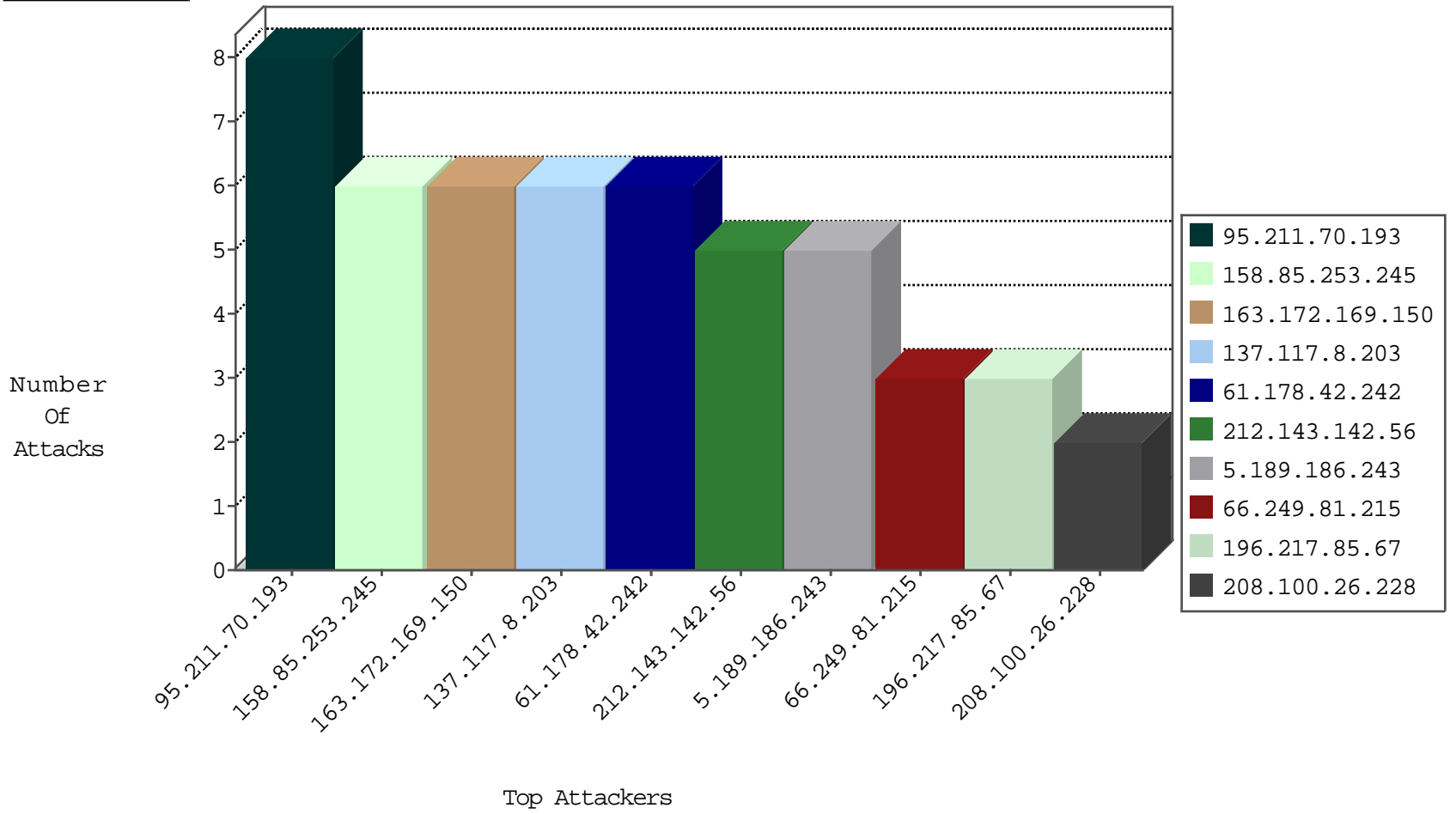
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.189.186.243	Germany	147.237.76.44	e.refuah.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.31	nakchal.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.86	navy.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.34	yohalan.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.42	refuah.idf.il	Black List	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
95.211.70.193	147.237.72.166	Netherlands	aka.idf.il	SQL Injection - Select From	8
137.117.8.203	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
163.172.169.150	147.237.8.27	United Kingdom	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
104.197.206.193	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.155	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
61.178.42.242	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
61.178.42.242	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
163.172.169.150	147.237.76.198	United Kingdom	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.178.42.242	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
163.172.169.150	147.237.76.34	United Kingdom	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.169.150	147.237.8.45	United Kingdom	e.eitan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.197.206.193	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
61.178.42.242	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
61.178.42.242	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.178.42.242	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
163.172.169.150	147.237.76.176	United Kingdom	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.227.67.172	147.237.77.19	Sweden	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.76.34	United Kingdom	yohalan.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
158.85.253.245	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
196.217.85.67	Morocco	147.237.77.216	dover.idf.il	drop		drop	3
141.212.122.153	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
141.212.122.154	United States	147.237.76.34	yohalan.idf.il	drop		drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
68.180.230.47	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	1
37.76.52.163	Hungary	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 37.76.52.163	Block	1
192.243.55.133	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=59390&docid=30485	Block	1
70.173.157.243	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
37.76.52.163	Hungary	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/	Block	1
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
71.6.165.200	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/robots.txt	Block	1
66.249.64.137	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding mrd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	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
128.232.110.28	United Kingdom	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
66.249.79.68	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/robots.txt	Block	1
68.180.228.29	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	1
192.243.55.132	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=59391&docid=65475	Block	1
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1