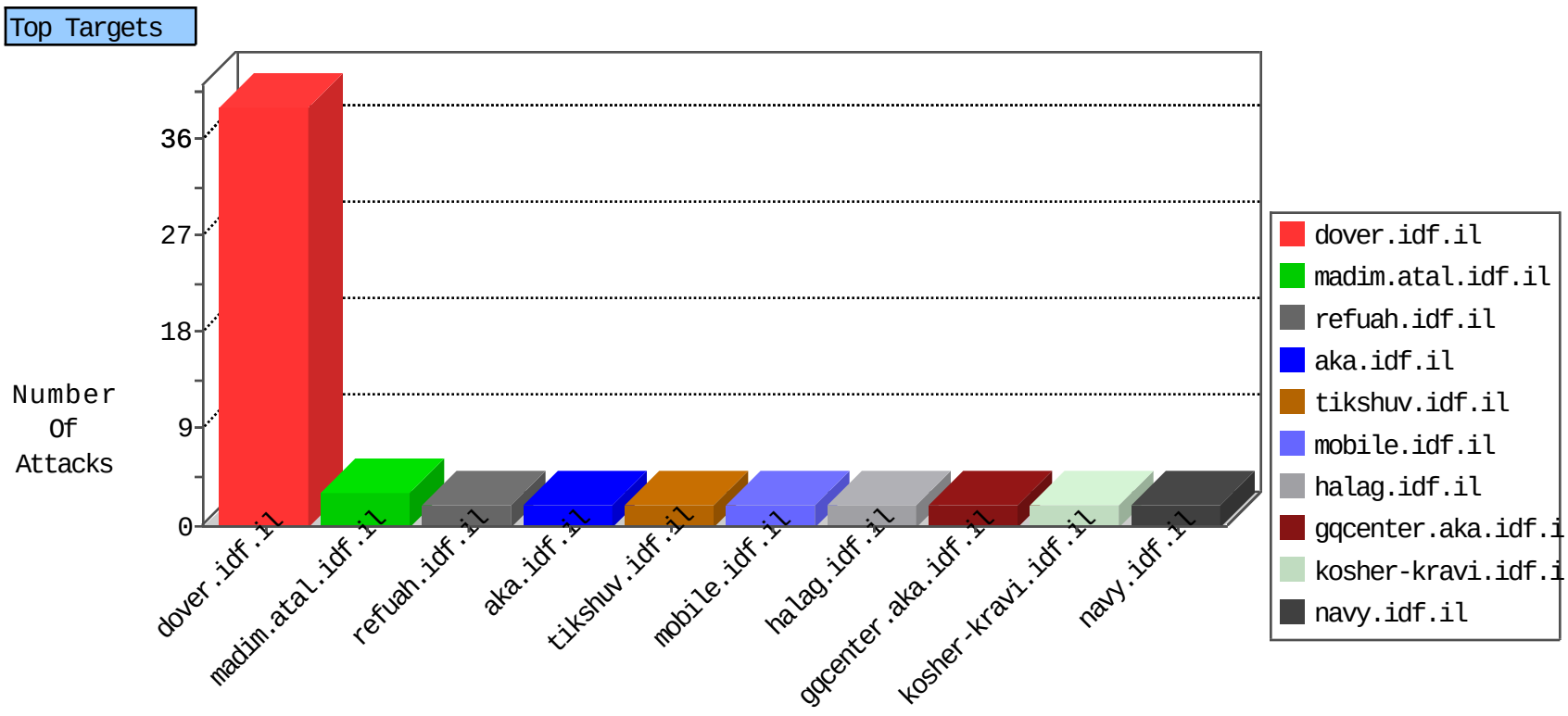
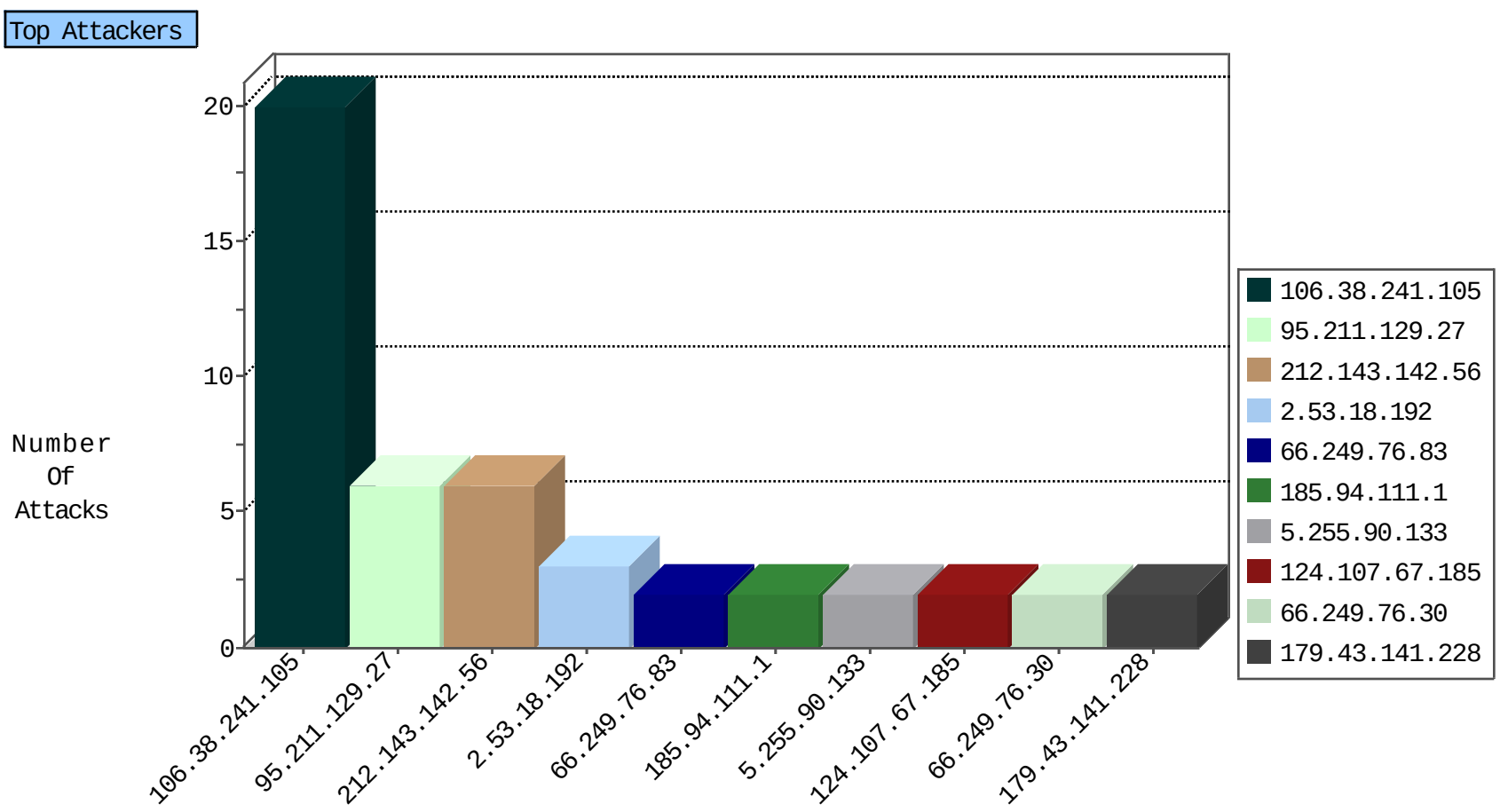
08-20-2016-04:04:00 to 08-20-2016-05:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-20-2016-04:04:00 to 08-20-2016-05:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
185.94.111.1	Russian Federation	147.237.76.176	test.ncore.idf.il	Black List	drop	1
66.240.219.146	United States	147.237.76.202	e.halag.idf.il	Black List	drop	1
204.42.253.132	United States	147.237.76.44	e.refuah.idf.il	Black List	drop	1
82.80.78.2	Israel	147.237.76.86	navy.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.42	refuah.idf.il	Black List	drop	1

08-20-2016-04:04:00 to 08-20-2016-05:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.105	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	20
86.186.225.159	United Kingdom	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1
72.5.72.225	United States	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

08-20-2016-04:04:00 to 08-20-2016-05:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
85.93.5.66	147.237.77.205	United Arab Emirates	prisha.idf.il	ET SCAN Potential SSH Scan	1
5.255.90.133	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.225.138	147.237.0.34	Ukraine	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
179.43.141.228	147.237.77.234	Switzerland	halag.idf.il	ET SCAN Potential SSH Scan	1
123.206.73.185	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
95.211.129.27	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN Potential SSH Scan	1
95.211.129.27	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
95.211.129.27	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
31.184.195.114	147.237.76.42	Russian Federation	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
5.255.90.133	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.6.34	147.237.0.17	Lithuania	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
179.43.141.228	147.237.77.226	Switzerland	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
95.211.129.27	147.237.77.234	Netherlands	halag.idf.il	ET SCAN Potential SSH Scan	1
95.211.129.27	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN Potential SSH Scan	1
95.211.129.27	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1

08-20-2016-04:04:00 to 08-20-2016-05:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
124.107.67.185	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
139.162.37.113	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1

08-20-2016-04:04:00 to 08-20-2016-05:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.18.192	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	2
192.99.147.201	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
66.249.66.187	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/templates/templatecontrols/news/לכתבה המלאה	Block	1
66.249.76.87	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
40.77.167.34	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1
204.79.180.209	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/home.asp	Block	1
66.249.76.30	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.76.30	Block	1
66.249.79.27	Israel	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.240.236.119	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/robots.txt	Block	1
66.249.76.30	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/.well-known/assetlinks.json	Block	1
79.179.9.210	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/6/68416.doc	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
66.249.64.142	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
66.249.76.85	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
38.104.195.70	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1

08-20-2016-04:04:00 to 08-20-2016-05:04:00