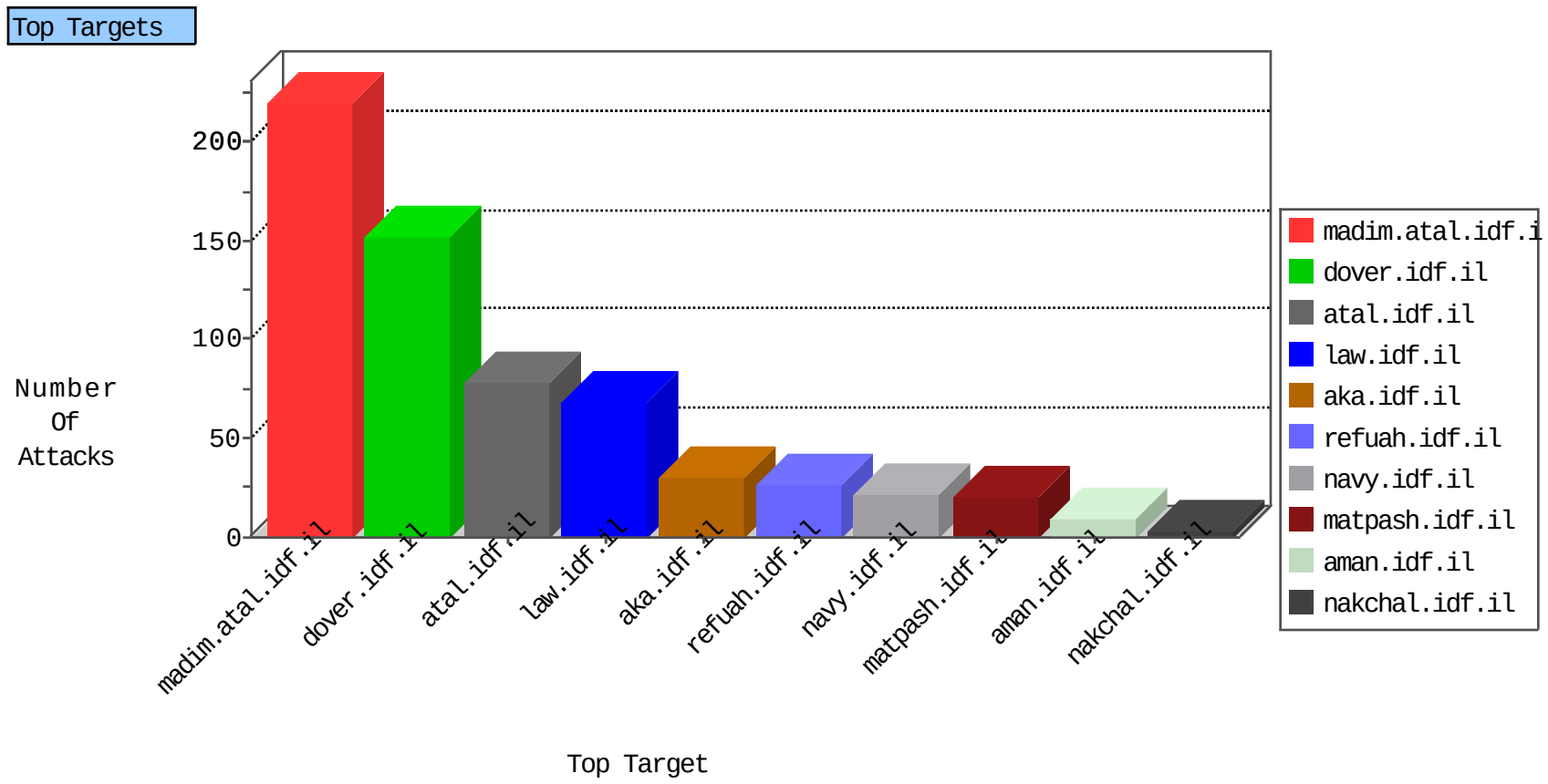
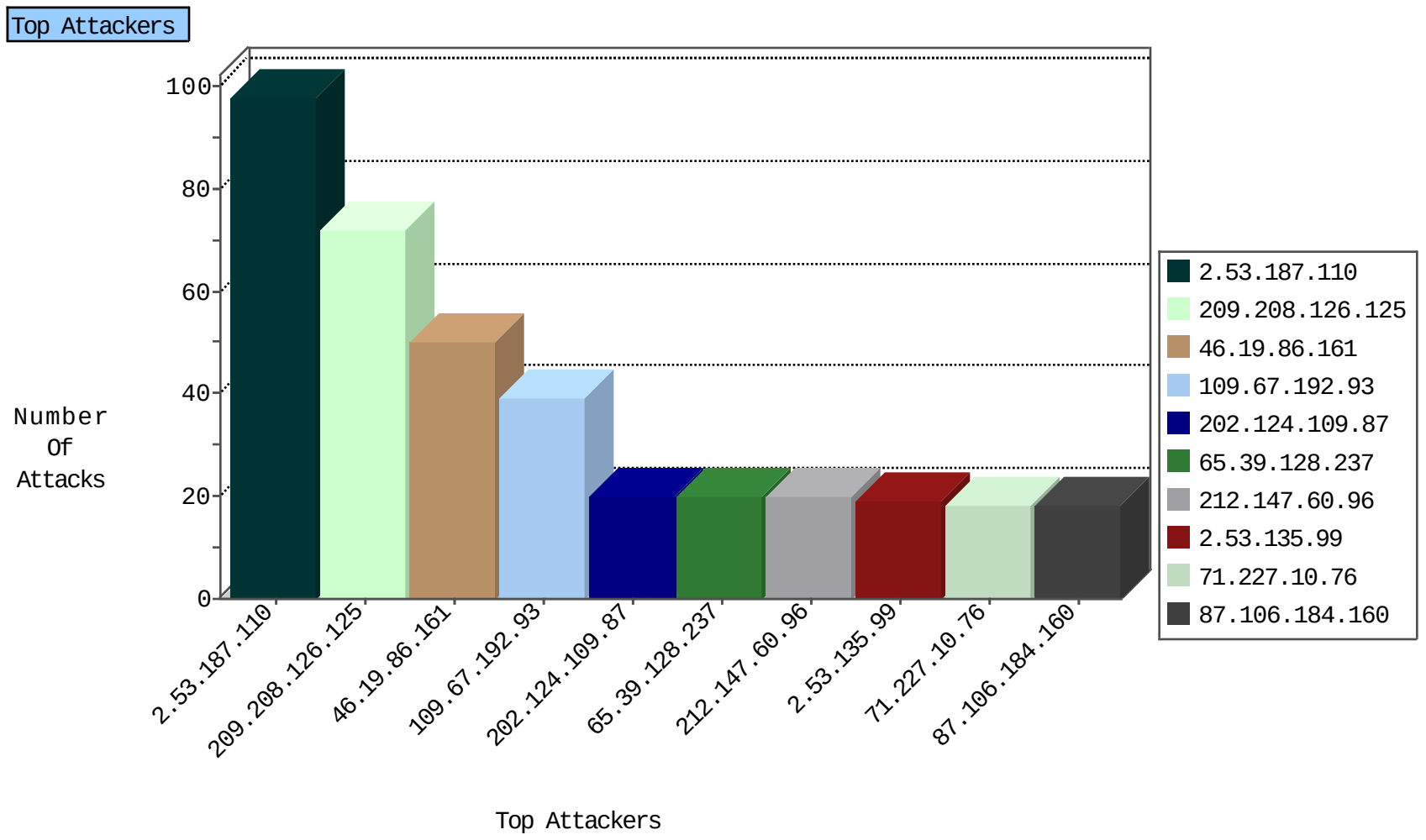
09-03-2016-13:04:02 to 09-03-2016-14:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-03-2016-13:04:02 to 09-03-2016-14:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.250.136.18	Israel	147.237.72.166	aka.idf.il	L4 Source or Dest Port Zero	drop	14
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	4
120.132.50.135	China	147.237.77.233	atal.idf.il	block-sp-traf1	forward	1

09-03-2016-13:04:02 to 09-03-2016-14:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-03-2016-13:04:02 to 09-03-2016-14:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
209.208.126.125	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	54
212.147.60.96	147.237.76.86	Switzerland	navy.idf.il	SQL Injection - Select From	20
65.39.128.237	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	20
202.124.109.87	147.237.76.42	New Zealand	refuah.idf.il	SQL Injection - Select From	20
177.185.192.85	147.237.77.233	Brazil	atal.idf.il	SQL Injection - Select From	18
71.227.10.76	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	18
173.0.129.149	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	14
50.63.197.9	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	12
96.251.45.13	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	9
85.136.227.77	147.237.77.74	Spain	law.idf.il	SQL Injection - Select From	8
204.93.196.218	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
184.168.192.31	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
158.85.253.245	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
175.142.129.124	147.237.77.216	Malaysia	dover.idf.il	Xenu Link Sleuth User Agent	2
83.168.250.50	147.237.76.31	Sweden	nakchal.idf.il	SQL Injection - Select From	2
45.56.74.212	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
108.61.199.29	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
65.183.101.8	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
66.249.93.181	147.237.77.170	Europe	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
65.183.101.8	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
62.219.14.189	147.237.77.19	Israel	law-forum.idf.il	ET SCAN Potential SSH Scan	1

09-03-2016-13:04:02 to 09-03-2016-14:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
87.106.184.160	Germany	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	18
209.208.126.125	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
37.231.24.182	Kuwait	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
176.65.29.130	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	9
46.43.107.3	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.63	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.212	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	5
2.53.184.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.43.107.3	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
105.157.51.184	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.253.192.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
5.102.104.36	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	3
66.249.81.179	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	2
37.8.120.156	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
141.212.122.18	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.136.59	Israel	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	1
79.183.53.161	Israel	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	1
45.63.30.95	United States	147.237.0.33	idf.il	drop		drop	1
216.243.31.2	United States	147.237.0.35	akaws.idf.il	drop		drop	1
2.139.151.41	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
184.105.247.238	United States	147.237.0.200	m4u.idf.il	drop		drop	1
45.63.30.95	United States	147.237.0.35	akaws.idf.il	drop		drop	1
120.59.247.95	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
62.219.14.189	Israel	147.237.77.19	law-forum.idf.il	drop	SAM rule	drop	1
141.212.122.17	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
66.249.81.175	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	1
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.128.246	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	1

09-03-2016-13:04:02 to 09-03-2016-14:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.187.110	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	98
46.19.86.161	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	50
109.67.192.93	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	39
2.53.135.99	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	19
199.30.24.95	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	10
199.30.24.210	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	10
31.168.240.21	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	5
65.55.210.142	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
65.55.210.147	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
109.253.146.217	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
2.53.128.53	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
217.132.124.110	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.209	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.146.86.243	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
109.253.147.114	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
207.46.13.134	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.253.223.5	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
212.76.97.15	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
131.253.27.212	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
207.46.13.90	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	1
185.27.105.73	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/site/templates/homepage.asp	Block	1
85.64.255.23	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/console/core/doc_mgr/doc_mgr.asp	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
207.46.13.90	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_moreinfo.asp	Block	1
46.19.85.138	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
77.138.200.77	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
87.70.19.187	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation SearchText in www.refua.atal.idf.il/938-he/refuah.aspx	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
79.177.247.180	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/about.aspx	Block	1
66.102.9.24	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
89.138.189.244	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	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
46.19.86.164	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
131.253.27.37	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
81.218.155.177	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/tizmoret/gallery/showpicture.asp	Block	1
207.46.13.68	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/1132-8613-he/navy.aspx.aspx	Block	1
82.81.97.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	1

09-03-2016-13:04:02 to 09-03-2016-14:04:02