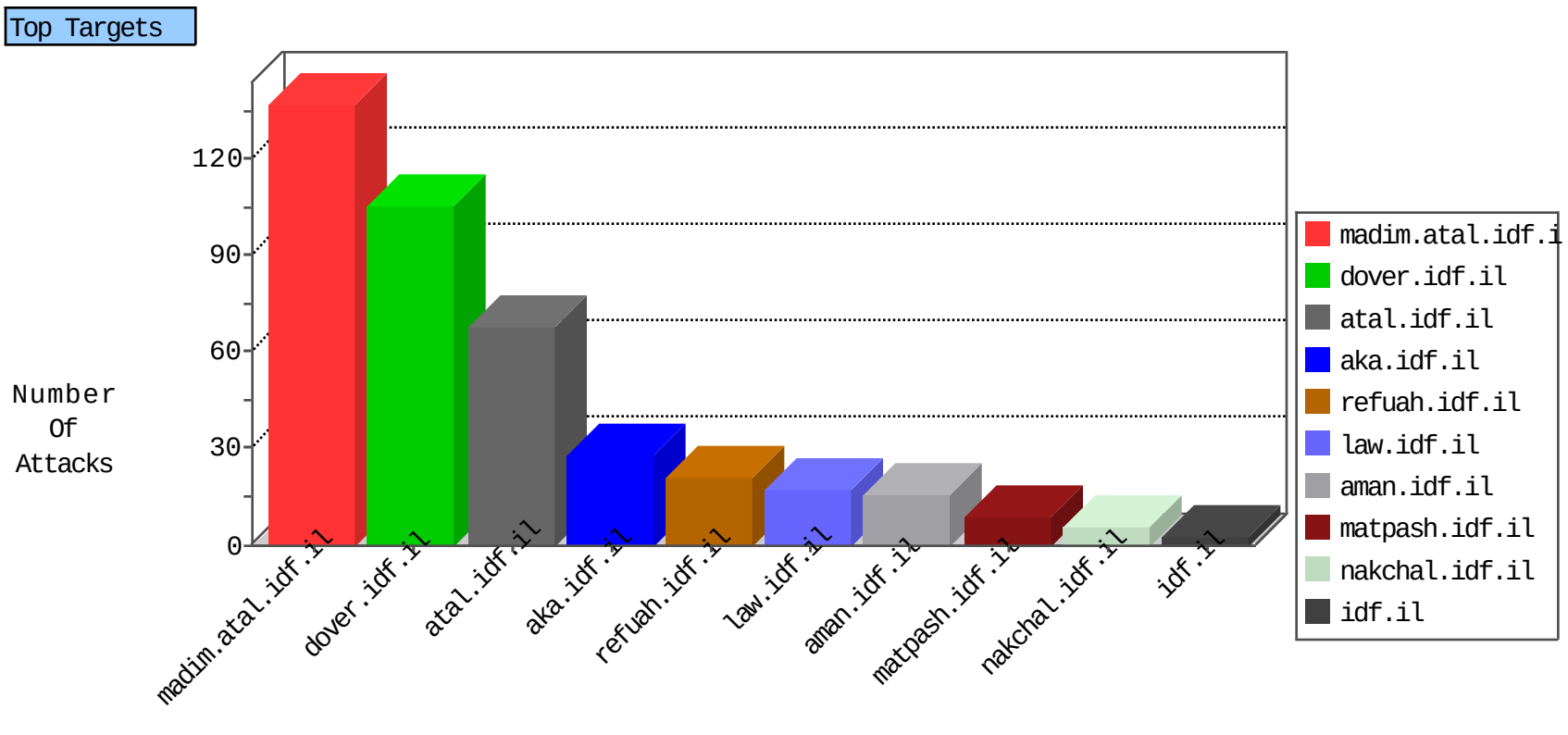
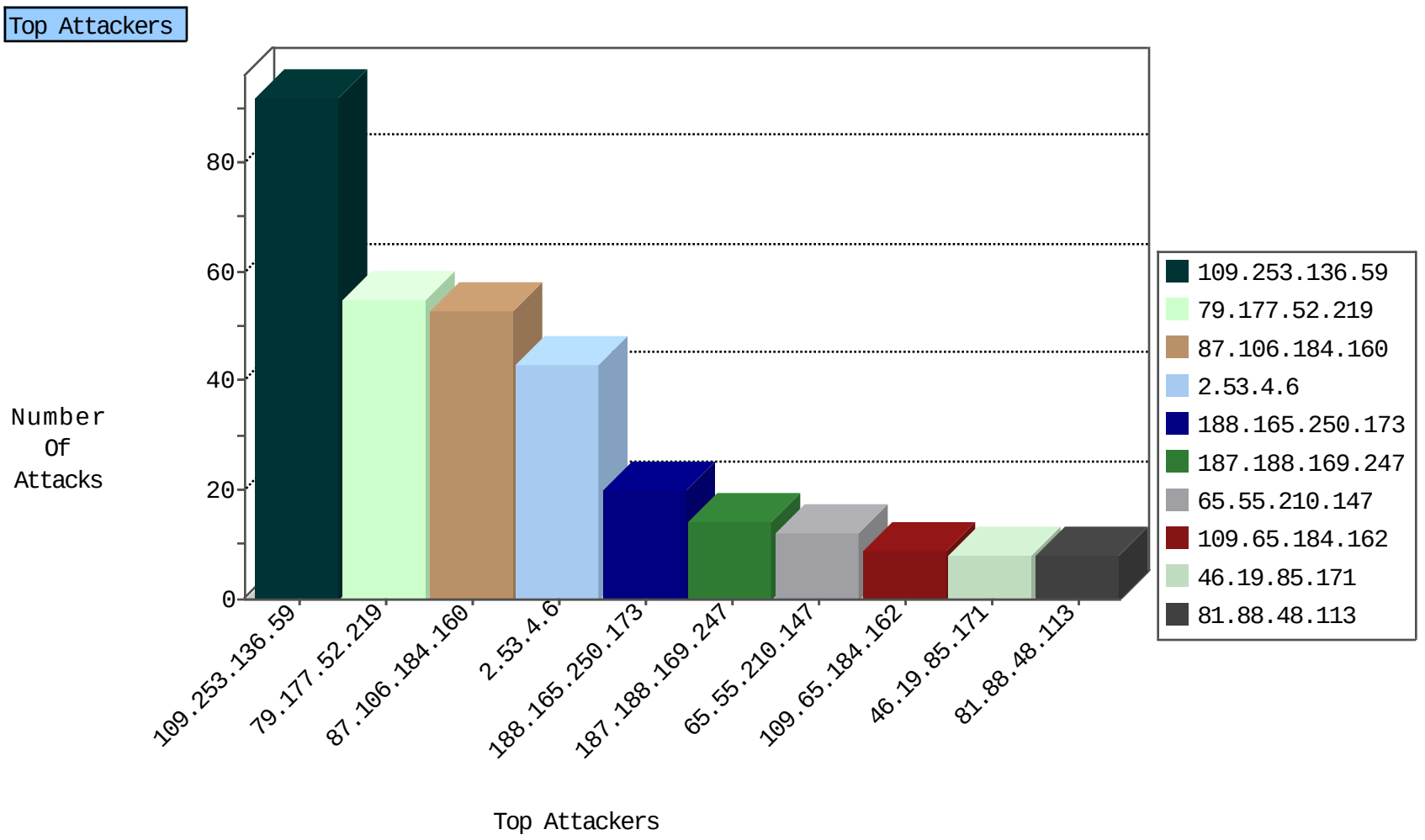
09-03-2016-12:04:01 to 09-03-2016-13:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-03-2016-12:04:01 to 09-03-2016-13:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.171	Israel	147.237.77.216	dover.idf.il	network flood IPv4 TCP-FIN-ACK	drop	34
5.102.104.36	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	9
109.236.84.10	Netherlands	147.237.76.196	e.sviva.idf.il	Black List	drop	1

09-03-2016-12:04:01 to 09-03-2016-13:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-03-2016-12:04:01 to 09-03-2016-13:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
87.106.184.160	147.237.77.233	Germany	atal.idf.il	SQL Injection - Select From	53
188.165.250.173	147.237.76.42	France	refuah.idf.il	SQL Injection - Select From	20
187.188.169.247	147.237.77.74	Mexico	law.idf.il	SQL Injection - Select From	14
81.88.48.113	147.237.77.233	Italy	atal.idf.il	SQL Injection - Select From	8
96.251.45.13	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	6
83.168.250.50	147.237.76.31	Sweden	nakchal.idf.il	SQL Injection - Select From	4
212.179.216.93	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	4
5.135.164.228	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	3
185.125.32.26	147.237.0.16	Turkey	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
116.12.175.233	147.237.77.235	Singapore	sviva.idf.il	ET SCAN NMAP -sS window 4096	1
108.61.199.29	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	147.237.76.200	Canada	eitan.aka.idf.il	ET SCAN NMAP -sS window 4096	1
208.100.26.228	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
42.116.29.68	147.237.8.24	Vietnam	e.lifestyle.idf.il	ET SCAN NMAP -sS window 3072	1
161.10.63.16	147.237.0.34	Colombia	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
132.255.155.186	147.237.72.156	Brazil	aman.idf.il	ET SCAN NMAP -sS window 1024	1
117.135.131.60	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
116.12.175.233	147.237.77.235	Singapore	sviva.idf.il	ET SCAN NMAP -sS window 3072	1
108.61.199.29	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	147.237.76.86	Canada	navy.idf.il	ET SCAN NMAP -sS window 4096	1
185.125.32.26	147.237.0.17	Turkey	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
185.93.185.10	147.237.77.179	Ukraine	e.mazi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
132.255.155.186	147.237.72.156	Brazil	aman.idf.il	ET SCAN NMAP -sS window 3072	1
117.135.131.60	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1

09-03-2016-12:04:01 to 09-03-2016-13:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.177.52.219	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.253.217.164	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
5.102.104.36	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.73	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
176.13.237.136	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
199.119.140.203	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
119.94.97.19	Philippines	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
183.129.160.229	China	147.237.72.14	dover.idf.il(old)	drop	SAM rule	drop	1
128.232.110.28	United Kingdom	147.237.0.33	idf.il	drop		drop	1
89.108.144.115	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
45.63.30.95	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
109.253.217.164	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.0.17	m.my-kosher-kravi.idf.il	drop	SAM rule	drop	1
216.243.31.2	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
183.129.160.229	China	147.237.0.33	idf.il	drop	SAM rule	drop	1
66.249.66.153	Israel	147.237.0.33	idf.il	drop		drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.136.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	92
2.53.4.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
65.55.210.147	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	12
109.65.184.162	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	9
79.179.21.160	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
46.117.67.42	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.120.46.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.116.79.183	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
79.178.203.39	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
46.117.67.42	Israel	147.237.72.166	aka.idf.il	Illegal Parameter Encoding text in www.aka.idf.il/main/giyus/pniothandler1.asmx/sendrequest	None	1
104.237.91.189	Hong Kong	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 104.237.91.189	Block	1
80.230.227.55	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
70.189.145.213	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
194.90.36.155	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1405-he/atal.aspx	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
82.166.20.137	Israel	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/pratim/pirteykatava/	Block	1
80.230.227.56	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
74.91.23.166	United States	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to 147.237.72.167/	Block	1
204.79.180.47	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
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
2.53.47.2	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
82.166.20.137	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/6/	Block	1
79.183.104.175	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	1
80.230.227.60	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
74.91.23.166	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.76.70	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.70	Block	1
5.22.135.174	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
89.138.154.215	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.230.226.64	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.76.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-22550-he/idfgdover.aspx	Block	1
109.253.214.245	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
80.230.227.61	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
77.138.57.16	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
66.249.76.70	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/.well-known/apple-app-site-association	Block	1
89.139.203.63	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
80.230.226.251	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
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	1
188.161.19.165	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
66.102.9.118	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
82.80.62.45	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/guyus	Block	1

09-03-2016-12:04:01 to 09-03-2016-13:04:01