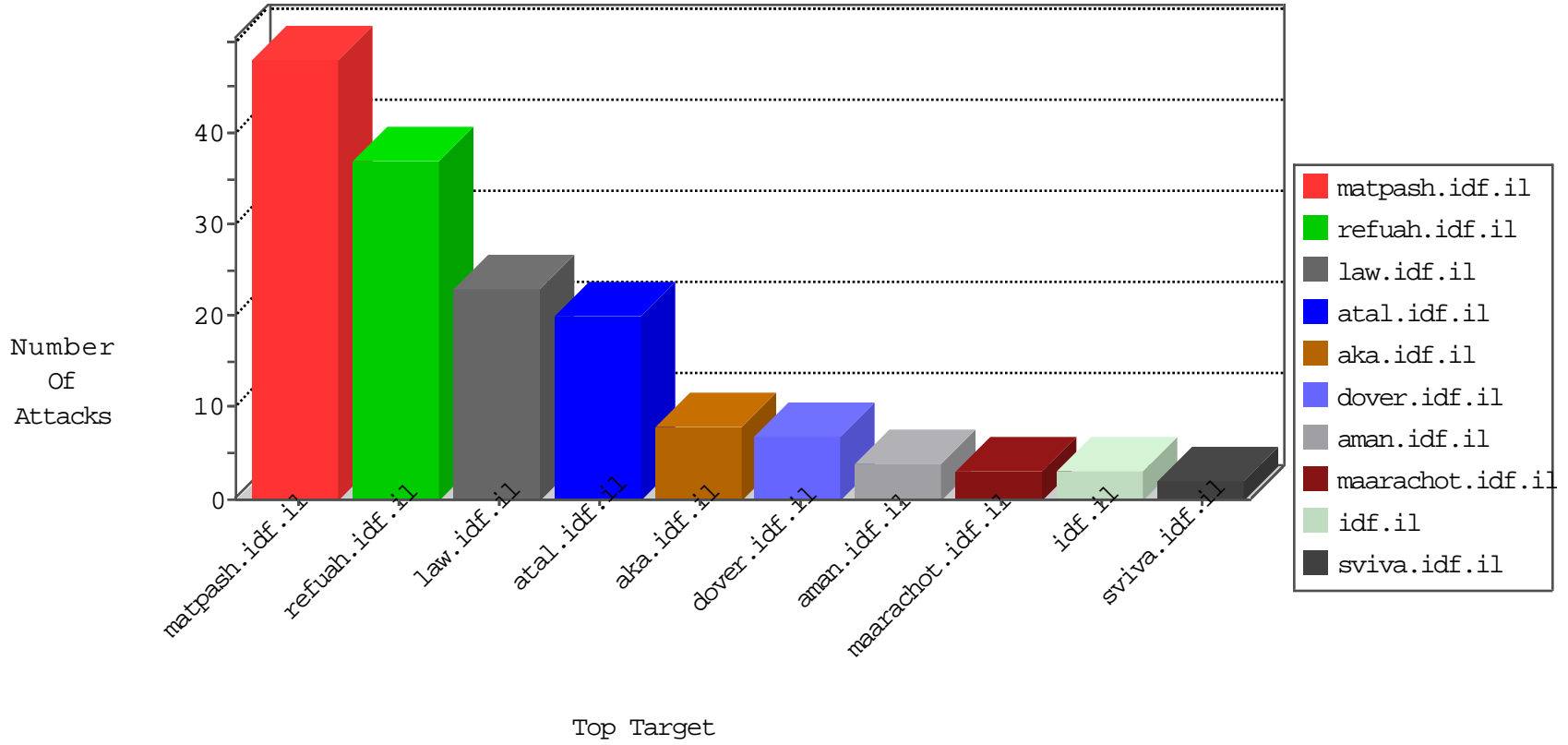


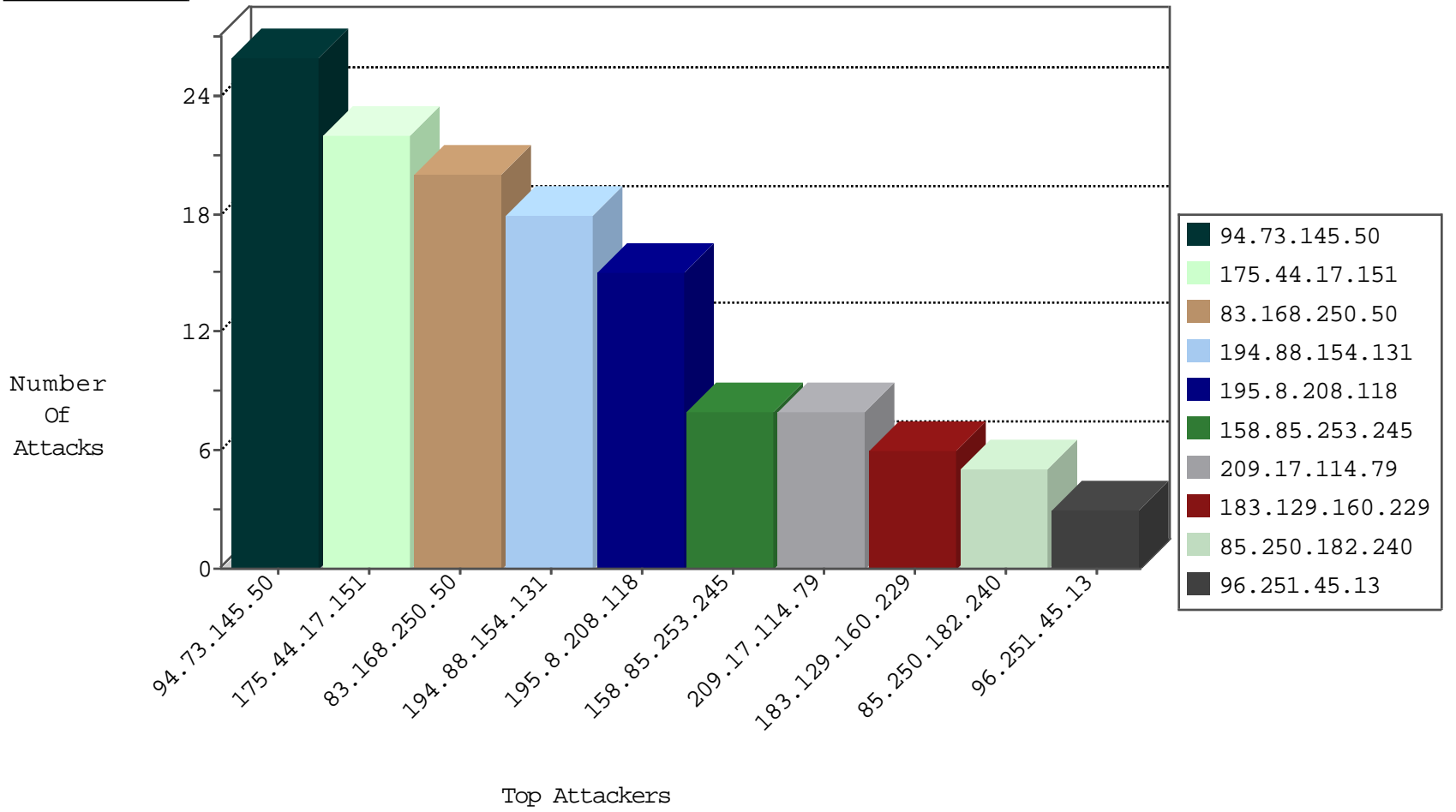
# IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.42.253.132	United States	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1

09-03-2016-07:04:07 to 09-03-2016-08:04:07

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
94.73.145.50	147.237.77.176	Turkey	matpash.idf.il	SQL Injection - Select From	26
83.168.250.50	147.237.77.233	Sweden	atal.idf.il	SQL Injection - Select From	20
194.88.154.131	147.237.76.42	Poland	refuah.idf.il	SQL Injection - Select From	18
195.8.208.118	147.237.76.42	Netherlands	refuah.idf.il	SQL Injection - Select From	15
209.17.114.79	147.237.77.74	United States	law.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
85.250.182.240	147.237.77.170	Israel	maarachot.idf.il	Xenu Link Sleuth User Agent	3
85.250.182.240	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	2
96.251.45.13	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	2
104.197.206.193	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
116.12.175.233	147.237.77.179	Singapore	e.mazi.idf.il	ET SCAN NMAP -sS window 2048	1
104.197.206.193	147.237.77.235	United States	sviva.idf.il	ET SCAN Potential SSH Scan	1
90.10.162.32	147.237.0.33	Reunion	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.227.67.172	147.237.8.14	Sweden	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
167.0.254.108	147.237.0.33	Colombia	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
123.176.80.201	147.237.77.74	China	law.idf.il	ET SCAN NMAP -sS window 1024	1
116.12.175.233	147.237.77.179	Singapore	e.mazi.idf.il	ET SCAN NMAP -f -sS	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
87.115.137.146	United Kingdom	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.13.242.153	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
183.129.160.229	China	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	1
202.28.10.20	Thailand	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
120.132.68.87	China	147.237.76.148	ggcenter.aka.idf.il	drop		drop	1
183.129.160.229	China	147.237.76.34	yohalan.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.8.14	e.orchot.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.76.44	e.refuah.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.8.24	e.lifestyle.idf.il	drop	SAM rule	drop	1
184.105.139.83	United States	147.237.0.33	idf.il	drop		drop	1

09-03-2016-07:04:07 to 09-03-2016-08:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
175.44.17.151	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 175.44.17.151	Block	15
175.44.17.151	China	147.237.77.176	matpash.idf.il	PHP Attempt	Block	6
79.180.35.1	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	2
104.200.154.63	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/ishurim/exampcert/	Block	1
207.46.13.77	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.76.100	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
66.249.69.67	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
68.180.230.47	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1153-he/dover.aspx	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
72.13.86.188	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
175.44.17.151	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.asp	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/yoman.asp	Block	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
204.79.180.238	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluum/templates/home.asp	Block	1
66.249.76.98	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list7.htm	Block	1

09-03-2016-07:04:07 to 09-03-2016-08:04:07