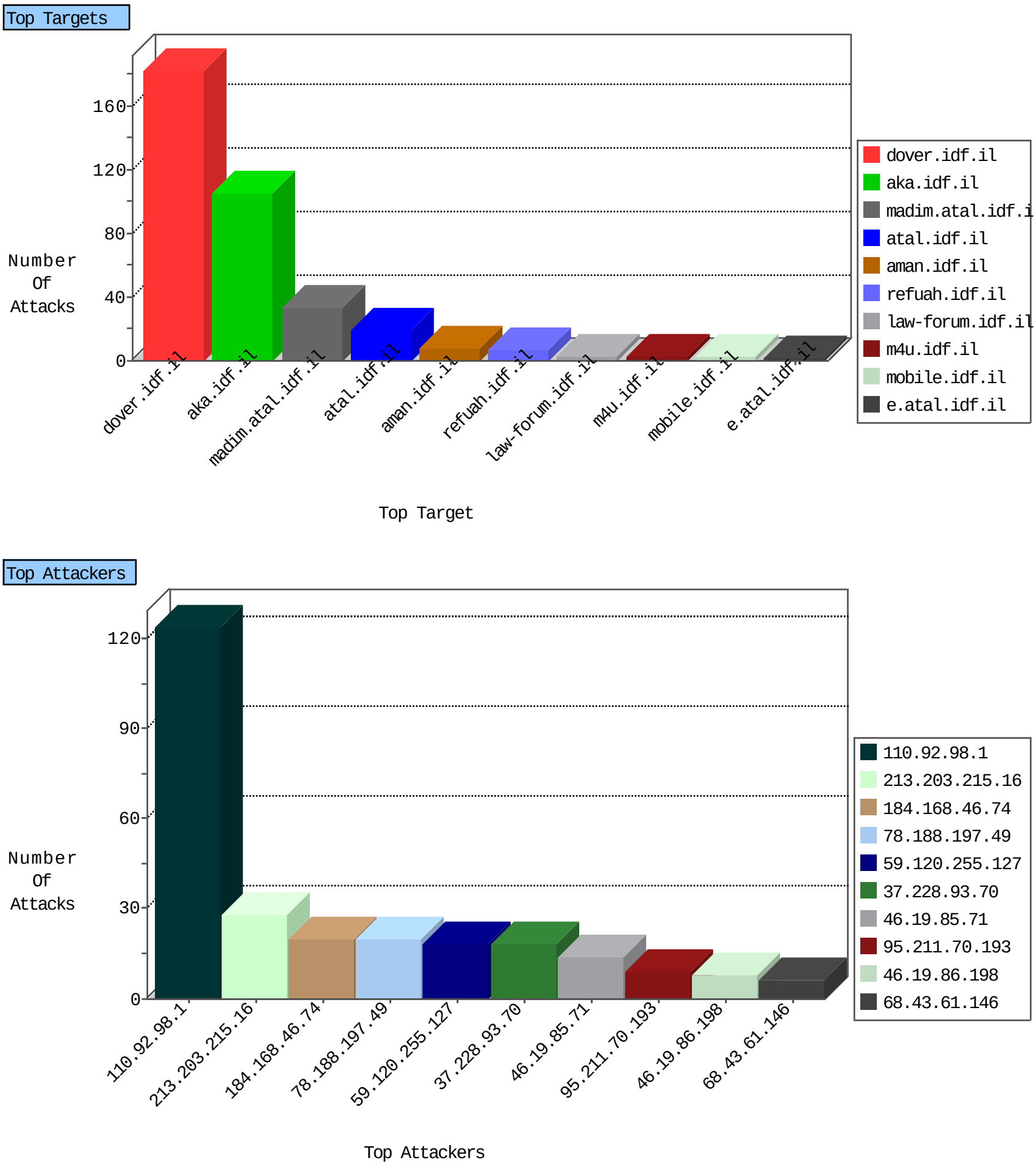
09-02-2016-14:04:09 to 09-02-2016-15:04:09

IDF Under Attack
Daily Report



09-02-2016-14:04:09 to 09-02-2016-15:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.156.128.101	Bulgaria	147.237.76.42	refuah.idf.il	Black List	drop	1
93.158.200.97	Netherlands	147.237.76.201	e.atal.idf.il	Black List	drop	1

09-02-2016-14:04:09 to 09-02-2016-15:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-02-2016-14:04:09 to 09-02-2016-15:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
213.203.215.16	147.237.72.166	Germany	aka.idf.il	SQL Injection - Select From	28
184.168.46.74	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	20
59.120.255.127	147.237.77.233	Taiwan	atal.idf.il	SQL Injection - Select From	18
37.228.93.70	147.237.72.166	Russian Federation	aka.idf.il	SQL Injection - Select From	18
95.211.70.193	147.237.72.166	Netherlands	aka.idf.il	SQL Injection - Select From	9
45.32.253.192	147.237.0.200	Japan	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
45.32.253.192	147.237.0.16	Japan	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.201.236.50	147.237.0.35	Ukraine	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
54.72.0.55	147.237.77.216	Ireland	dover.idf.il	portscan: TCP Distributed Portscan	1
47.89.177.157	147.237.77.19	Canada	law-forum.idf.il	ET SCAN NMAP -sS window 2048	1
45.32.253.192	147.237.76.201	Japan	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
45.32.253.192	147.237.76.30	Japan	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
193.201.225.138	147.237.77.226	Ukraine	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
45.32.253.192	147.237.0.19	Japan	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.128.144.131	147.237.8.45	Canada	e.eitan.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.50	147.237.0.35	Ukraine	akaws.idf.il	ET SCAN NMAP -sS window 3072	1
66.249.66.19	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	1
54.166.82.60	147.237.0.15	United States	kosher-kravi.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
47.89.177.157	147.237.77.19	Canada	law-forum.idf.il	ET SCAN NMAP -sS window 3072	1
47.89.177.157	147.237.77.19	Canada	law-forum.idf.il	ET SCAN NMAP -f -sS	1
45.32.253.192	147.237.76.39	Japan	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

09-02-2016-14:04:09 to 09-02-2016-15:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
110.92.98.1	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	124
78.188.197.49	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
93.169.147.145	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.117.182.13	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3
216.243.31.2	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
141.212.122.82	United States	147.237.0.200	m4u.idf.il	drop		drop	1
186.208.218.44	Brazil	147.237.76.34	yohalan.idf.il	drop		drop	1
109.253.156.19	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.83	United States	147.237.0.200	m4u.idf.il	drop		drop	1
61.150.12.33	China	147.237.0.33	idf.il	drop		drop	1
109.253.192.251	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
176.13.8.209	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
216.218.206.108	United States	147.237.0.33	idf.il	drop		drop	1
109.253.216.134	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
176.13.12.219	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
92.114.163.92	Moldova, Republic of	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	1
216.218.206.111	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
31.168.195.119	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
176.13.228.246	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

09-02-2016-14:04:09 to 09-02-2016-15:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
46.19.86.198	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
77.139.87.52	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar	Block	5
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
80.246.130.97	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
77.42.193.79	Lebanon	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
68.43.61.146	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 68.43.61.146	Block	3
87.68.40.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
68.43.61.146	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	3
94.187.23.238	Lebanon	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
193.186.163.3	Greece	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	2
178.36.14.12	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/dover.aspx/	Block	2
46.19.85.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.228.253.248	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
207.46.13.90	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
37.26.149.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
68.180.228.29	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/undefined/	Block	1
46.121.37.58	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl13 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
109.65.129.245	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
37.46.38.158	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
77.138.238.98	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
213.57.33.122	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 213.57.33.122	Block	1
46.19.86.229	Israel	147.237.76.42	refuah.idf.il	Malformed URL	Block	1
2.53.147.112	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
207.46.13.64	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.102.9.2	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
109.67.109.145	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/newsarchive.aspx	Block	1
77.138.245.180	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/popups/markivsachar.aspx	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
46.19.86.229	Israel	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method 468 in URL	Block	1
180.76.15.9	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
85.65.139.130	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
2.55.43.80	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
77.125.46.251	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	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
66.102.9.118	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
136.243.11.18	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
46.117.248.238	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
192.243.55.131	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/default.aspx	Block	1
77.127.0.156	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.240.236.119	United States	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to 147.237.76.147/robots.txt	Block	1
136.243.67.234	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/home/default.aspx	Block	1
2.53.12.141	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	1
79.181.191.140	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
192.243.55.134	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?docid=64966	Block	1
46.120.38.133	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
77.138.238.98	France	147.237.76.42	refuah.idf.il	Unauthorized Method POST for 147.237.76.42/894-he/refuah.aspx	Block	1
213.8.204.51	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	1

09-02-2016-14:04:09 to 09-02-2016-15:04:09