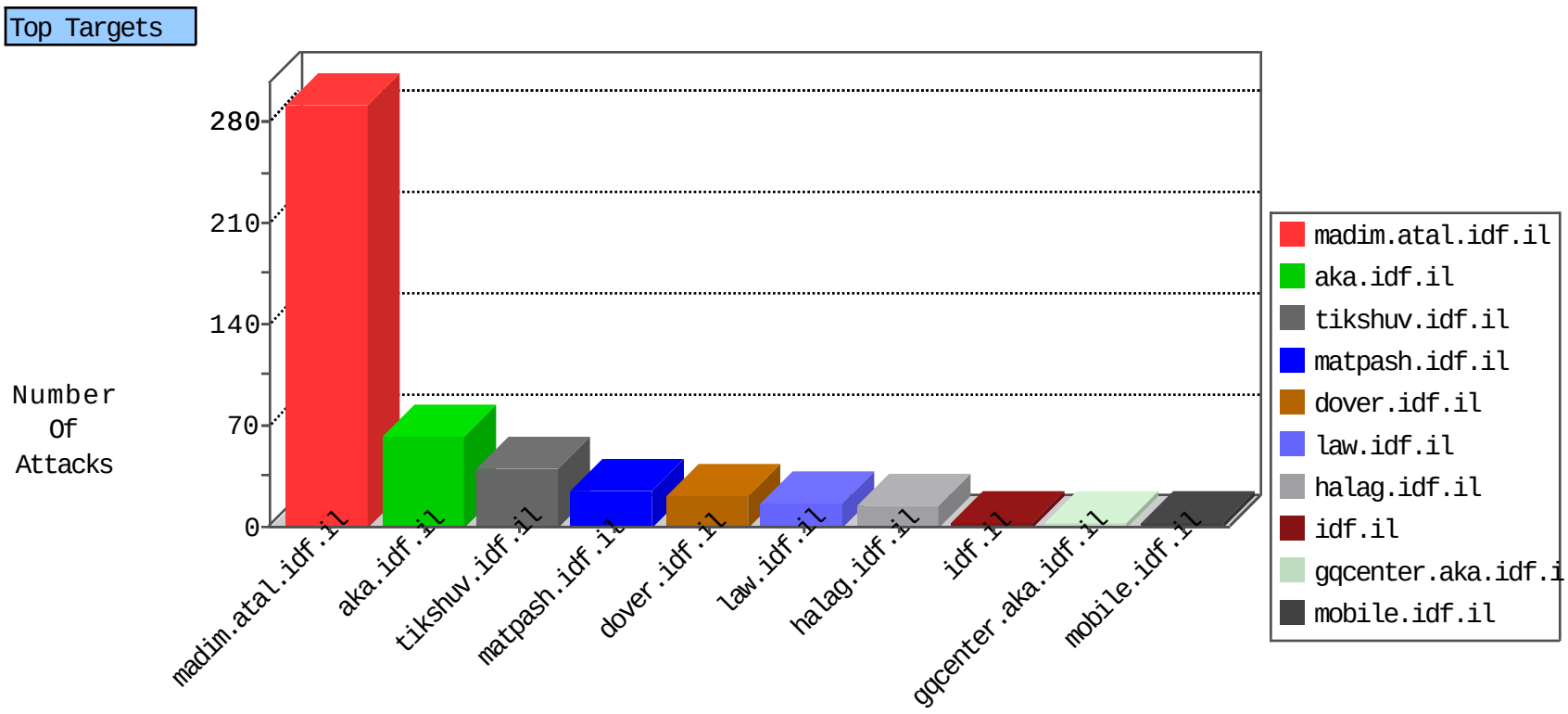
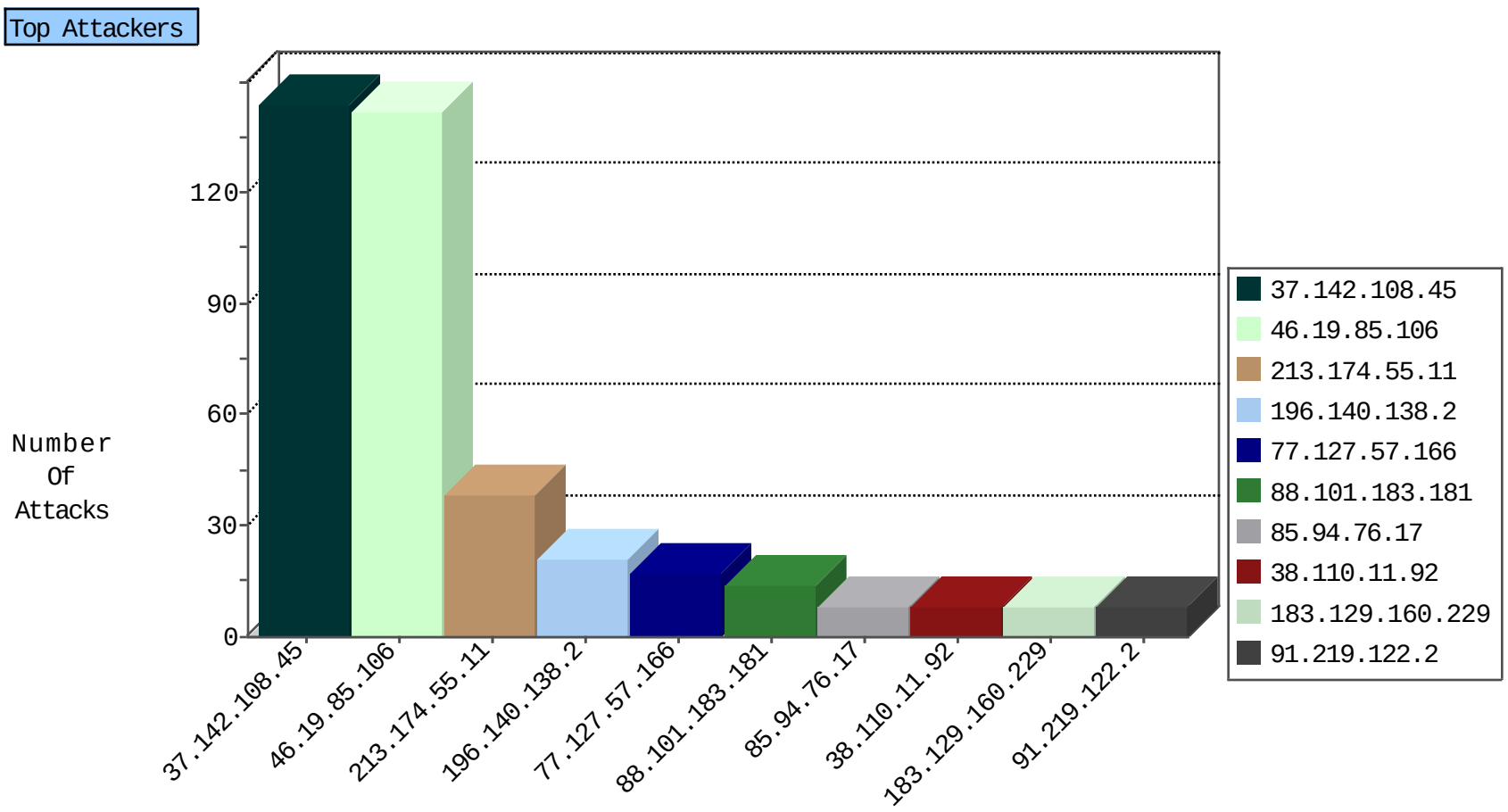
09-03-2016-10:04:07 to 09-03-2016-11:04:07

IDF Under Attack Daily Report



Top Target



Top Attackers

09-03-2016-10:04:07 to 09-03-2016-11:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-03-2016-10:04:07 to 09-03-2016-11:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-03-2016-10:04:07 to 09-03-2016-11:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
213.174.55.11	147.237.0.34	Germany	tikshuv.idf.il	SQL Injection - Select From	38
91.219.122.2	147.237.72.166	Poland	aka.idf.il	SQL Injection - Select From	8
81.88.48.113	147.237.77.74	Italy	law.idf.il	SQL Injection - Select From	8
38.110.11.92	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	8
85.94.76.17	147.237.77.74	Croatia	law.idf.il	SQL Injection - Select From	8
50.77.136.81	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	8
184.168.46.74	147.237.72.166	United States	aka.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
175.142.129.124	147.237.77.176	Malaysia	matpash.idf.il	Xenu Link Sleuth User Agent	2
122.224.250.234	147.237.0.19	China	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
185.110.132.201	147.237.72.167	Ukraine	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
185.110.132.201	147.237.0.33	Ukraine	idf.il	ET SCAN Potential SSH Scan	1
185.110.132.201	147.237.0.17	Ukraine	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
122.224.250.234	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 1024	1
109.253.228.110	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
218.67.69.15	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.110.132.201	147.237.76.31	Ukraine	nakchal.idf.il	ET SCAN Potential SSH Scan	1
185.110.132.201	147.237.0.35	Ukraine	akaws.idf.il	ET SCAN Potential SSH Scan	1
185.110.132.201	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN Potential SSH Scan	1

09-03-2016-10:04:07 to 09-03-2016-11:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
196.140.138.2	Egypt	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	21
77.127.57.166	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	17
88.101.183.181	Czech Republic	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	14
62.84.77.34	Lebanon	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	4
176.58.79.88	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.211	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.64.114.168	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
183.129.160.229	China	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	1
61.136.195.22	China	147.237.0.200	m4u.idf.il	drop		drop	1
183.129.160.229	China	147.237.76.202	e.halag.idf.il	drop	SAM rule	drop	1
176.13.15.21	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.76.86	navy.idf.il	drop	SAM rule	drop	1
185.120.125.101	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.76.147	chinuch.aka.idf.il	drop	SAM rule	drop	1
192.169.7.223	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
183.129.160.229	China	147.237.0.19	madim.atal.idf.il	drop	SAM rule	drop	1
61.136.195.22	China	147.237.0.33	idf.il	drop		drop	1
183.129.160.229	China	147.237.76.148	gqcenter.aka.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.0.33	idf.il	drop	SAM rule	drop	1
61.136.195.22	China	147.237.0.35	akaws.idf.il	drop		drop	1
183.129.160.229	China	147.237.76.201	e.atal.idf.il	drop	SAM rule	drop	1

09-03-2016-10:04:07 to 09-03-2016-11:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.142.108.45	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	144
46.19.85.106	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	142
109.65.4.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
77.69.27.3	Greece	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/default.aspx	Block	3
207.46.13.162	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/901-10992-he/cogat.aspx	Block	1
79.179.127.47	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
121.42.54.54	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/wp-login.php	Block	1
66.147.244.101	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
213.7.196.62	Cyprus	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.180.8.32	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __EVENTTARGET in aka.idf.il/main/giyus/	None	1
2.55.13.34	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
157.55.39.164	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim/templates/www.behazdaa.org.il	Block	1
66.240.236.119	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
85.65.48.238	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	1
37.26.146.215	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
194.242.168.227	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/sitemap.aspx	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	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_text.asp	Block	1
121.42.54.54	China	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	1

09-03-2016-10:04:07 to 09-03-2016-11:04:07