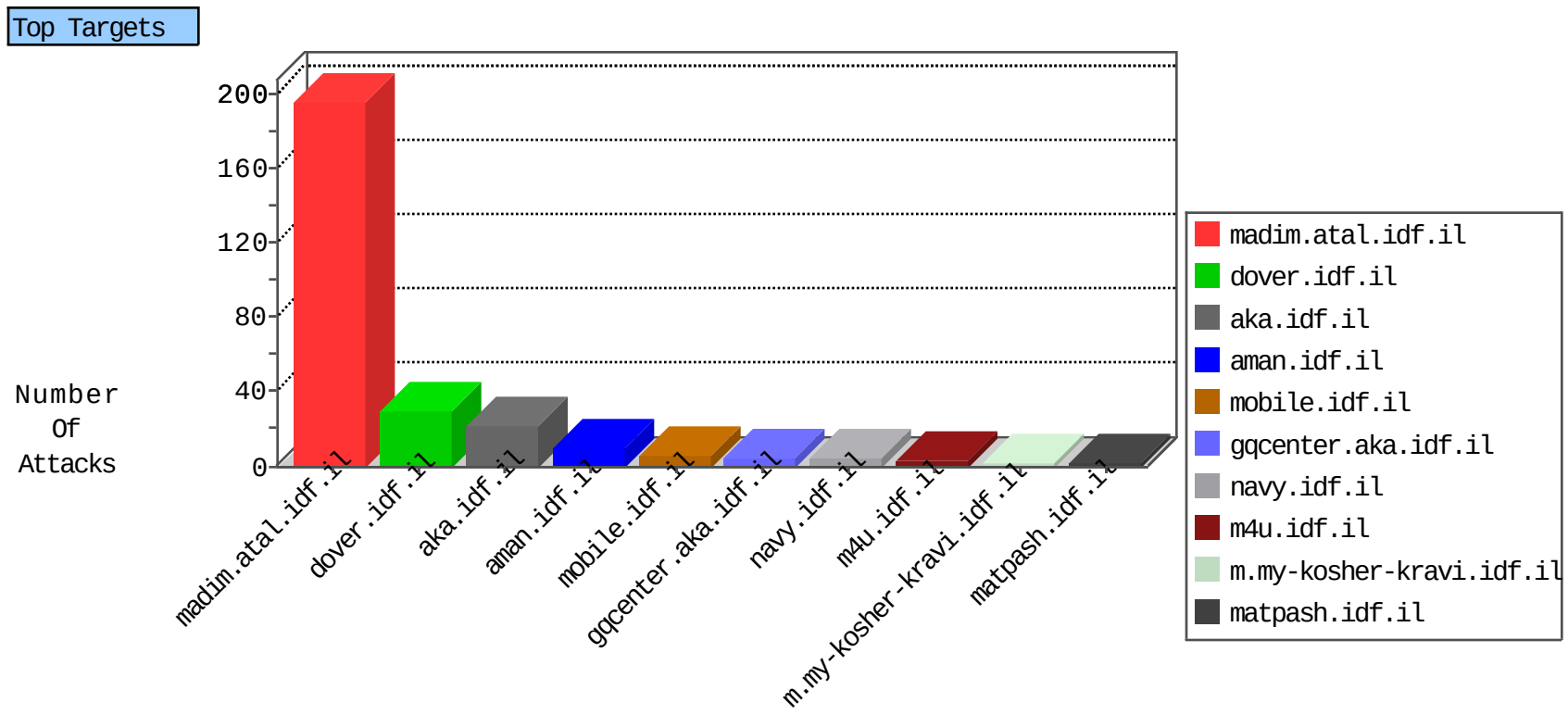
09-03-2016-14:04:00 to 09-03-2016-15:04:00

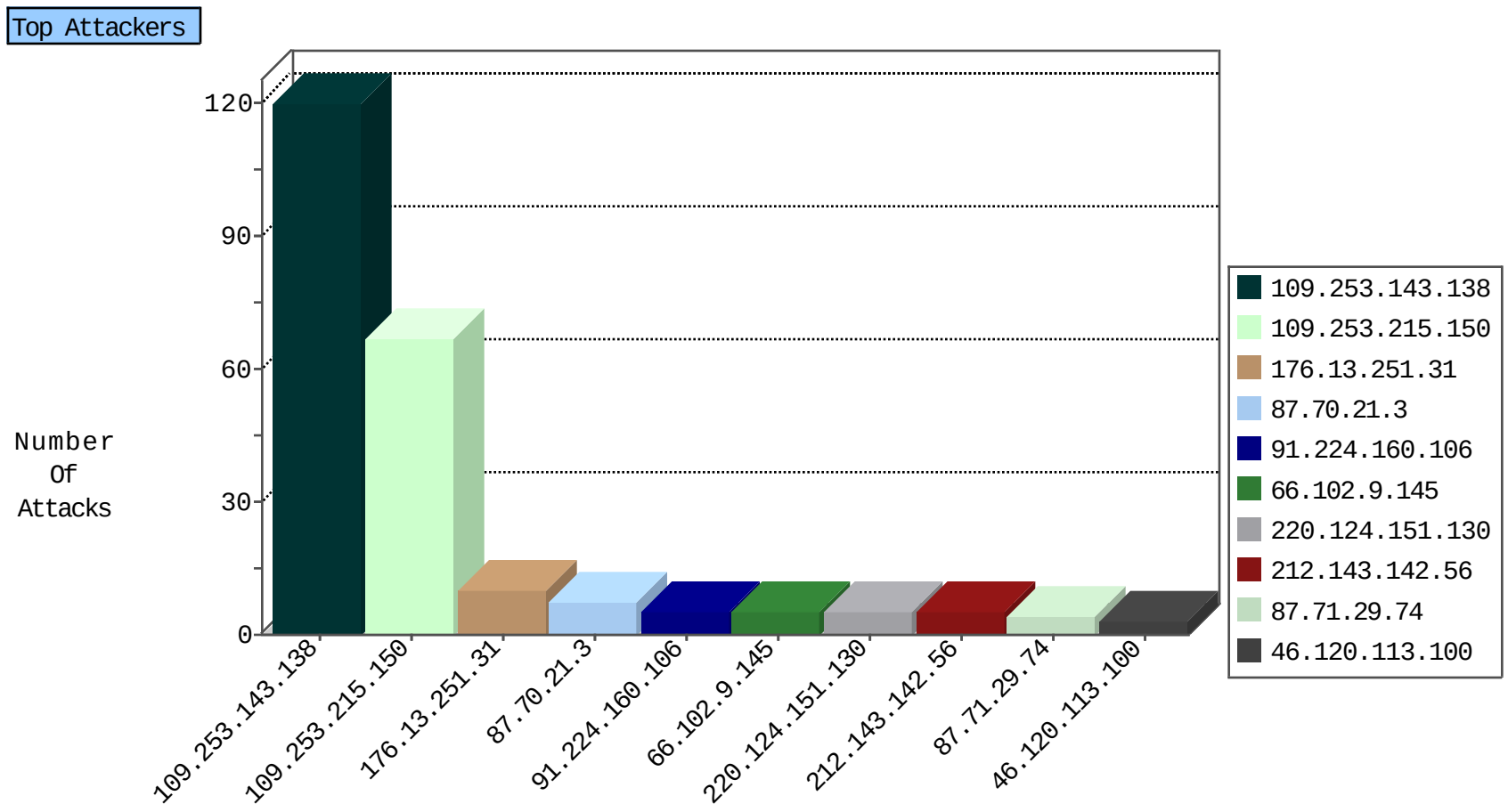
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

09-03-2016-14:04:00 to 09-03-2016-15:04:00

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	1
93.174.93.156	Netherlands	147.237.76.198	e.yohalan.idf.il	Black List	drop	1

09-03-2016-14:04:00 to 09-03-2016-15:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-03-2016-14:04:00 to 09-03-2016-15:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
45.56.74.212	147.237.77.212	United States	e.dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.238.37	147.237.76.197	United Kingdom	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
116.12.175.233	147.237.76.86	Singapore	navy.idf.il	ET SCAN NMAP -sS window 3072	1
109.60.153.178	147.237.76.148	Russian Federation	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.102.52.71	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
220.124.151.130	147.237.77.216	Korea, Republic of	dover.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
220.124.151.130	147.237.76.148	Korea, Republic of	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential SSH Scan	1
220.124.151.130	147.237.0.17	Korea, Republic of	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential SSH Scan	1
219.87.191.219	147.237.0.17	Taiwan	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
46.227.67.172	147.237.77.243	Sweden	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
177.200.192.50	147.237.77.170	Brazil	maarachot.idf.il	ET SCAN NMAP -sS window 4096	1
116.12.175.233	147.237.76.86	Singapore	navy.idf.il	ET SCAN NMAP -sS window 4096	1
109.60.153.178	147.237.76.200	Russian Federation	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
108.61.199.29	147.237.72.217	Netherlands	e.idf.il	ET SCAN Potential SSH Scan	1
94.102.52.71	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
220.124.151.130	147.237.76.200	Korea, Republic of	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
220.124.151.130	147.237.76.39	Korea, Republic of	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN Potential SSH Scan	1
219.87.191.219	147.237.76.199	Taiwan	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
198.58.110.199	147.237.77.178	United States	e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

09-03-2016-14:04:00 to 09-03-2016-15:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.13.251.31	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
87.70.21.3	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
66.102.9.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
176.13.245.201	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	2
82.205.33.34	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.48	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	2
107.170.125.121	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.226.40.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
79.178.6.114	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.217.227	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
31.154.81.35	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
128.232.110.28	United Kingdom	147.237.76.34	yohalan.idf.il	drop		drop	1
183.129.160.229	China	147.237.0.200	m4u.idf.il	drop	SAM rule	drop	1
141.212.122.162	United States	147.237.0.200	m4u.idf.il	drop		drop	1
141.212.122.163	United States	147.237.0.200	m4u.idf.il	drop		drop	1
66.102.9.149	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
216.243.31.2	United States	147.237.0.33	idf.il	drop		drop	1

09-03-2016-14:04:00 to 09-03-2016-15:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.143.138	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	120
109.253.215.150	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	67
87.71.29.74	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	4
84.109.124.192	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
85.250.197.215	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/pratim/pirteychayal/	Block	1
89.237.111.92	France	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
79.179.155.224	Israel	147.237.0.19	madim.atal.idf.i	SSL Untraceable Connection - Open Mode	None	1
68.180.228.169	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
46.19.85.251	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
207.46.13.57	United States	147.237.72.166	aka.idf.il	Unknown Parameter 136cd360 in www.aka.idf.il/main/home/default.aspx	None	1
77.139.6.178	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar	Block	1
66.249.76.2	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
80.246.130.151	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
68.180.229.49	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
212.29.222.162	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mas.aspx	None	1
46.120.113.100	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/robots.txt	Block	1
79.176.96.171	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/tmuna/	Block	1
80.246.137.20	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
77.138.46.85	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
217.69.133.29	Russian Federation	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
46.120.113.100	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 46.120.113.100	Block	1
87.70.20.242	Israel	147.237.77.170	maarachot.idf.il	URL is Above Root Directory maarachot.idf.il/../images/shared/maarachot_logo.png	Block	1
79.177.195.238	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	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
131.253.27.209	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
80.246.137.152	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
77.138.133.62	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
46.120.113.100	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
79.179.155.224	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
136.243.11.18	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
84.108.27.188	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
77.138.234.212	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1

09-03-2016-14:04:00 to 09-03-2016-15:04:00