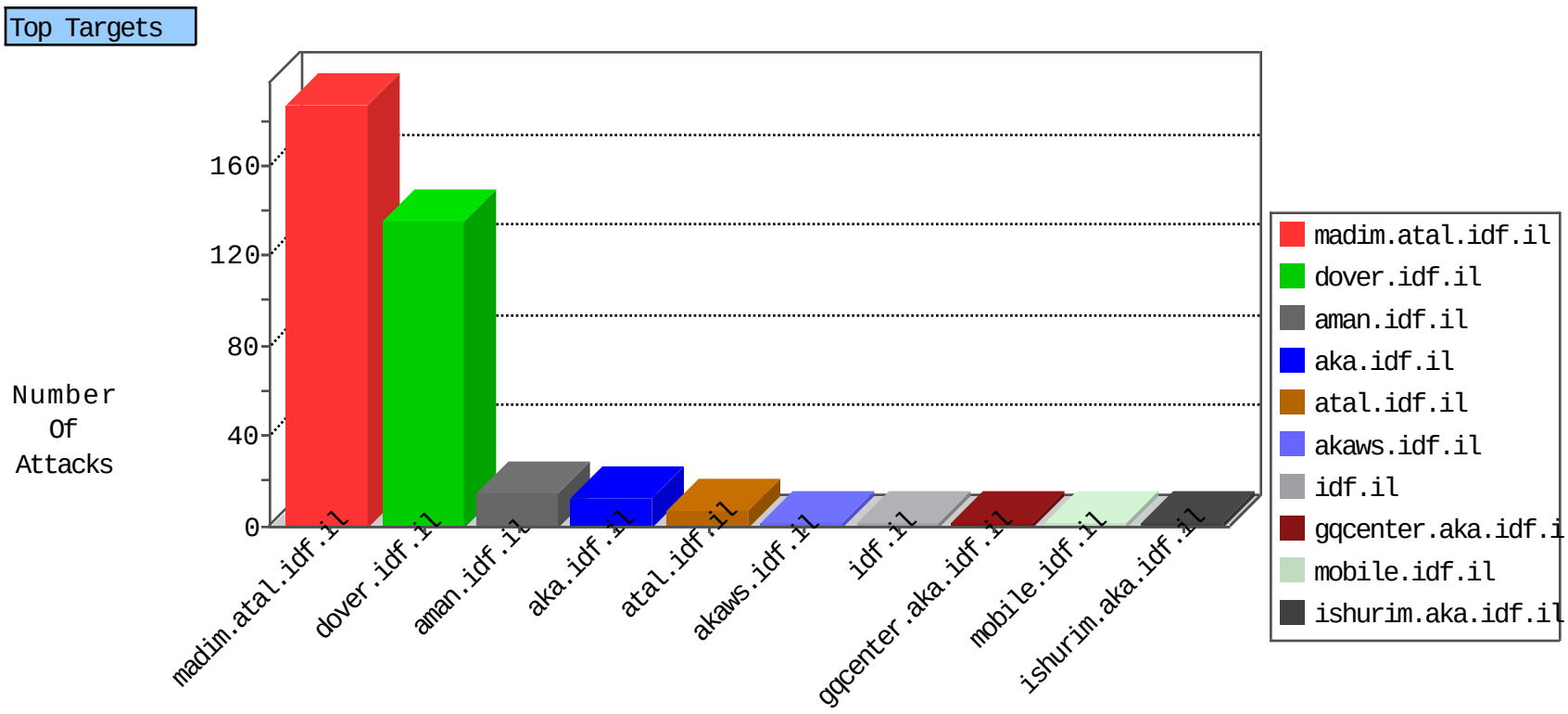
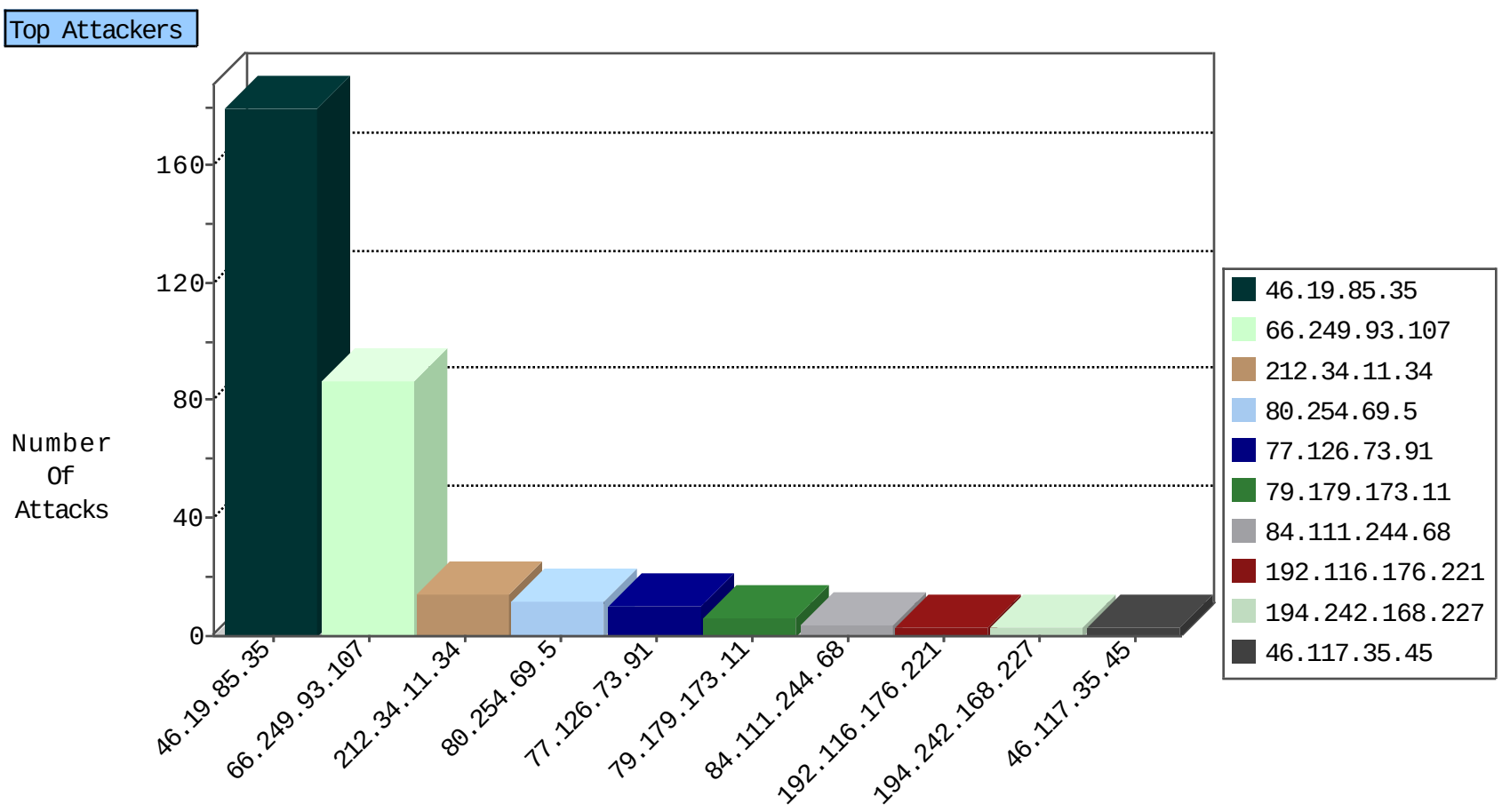
08-20-2016-11:04:02 to 08-20-2016-12:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-20-2016-11:04:02 to 08-20-2016-12:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
200.60.16.102	Peru	147.237.77.233	atal.idf.il	L4 Source or Dest Port Zero	drop	3
120.132.50.135	China	147.237.72.156	aman.idf.il	block-sp-traf1	forward	2
82.80.78.2	Israel	147.237.77.216	dover.idf.il	Black List	drop	2
93.174.95.106	Netherlands	147.237.76.196	e.sviva.idf.il	Black List	drop	1
66.240.236.119	United States	147.237.76.34	yohalan.idf.il	Black List	drop	1
198.20.70.114	United States	147.237.76.44	e.refuah.idf.il	Black List	drop	1

08-20-2016-11:04:02 to 08-20-2016-12:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

08-20-2016-11:04:02 to 08-20-2016-12:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.130.155	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
123.123.119.180	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
50.84.213.146	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
15.203.227.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 3072	1
15.203.227.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -f -sS	1
183.82.106.200	147.237.76.30	India	himush.idf.il	ET SCAN NMAP -sS window 4096	1
123.206.85.139	147.237.77.227	China	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
46.172.71.251	147.237.76.202	Ukraine	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
15.203.227.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 2048	1
191.190.204.212	147.237.8.28	Brazil	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
123.206.85.139	147.237.77.243	China	mobile.idf.il	ET SCAN NMAP -sS window 1024	1

08-20-2016-11:04:02 to 08-20-2016-12:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.93.107	Europe	147.237.77.216	dover.idf.il	drop	SAM rule	drop	79
80.254.69.5	Switzerland	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
77.126.73.91	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.249.93.107	Europe	147.237.77.216	dover.idf.il	drop		drop	6
79.179.173.11	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.93.107	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
176.13.231.210	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	2
122.167.157.102	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
141.212.122.145	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
216.218.206.76	United States	147.237.0.35	akaws.idf.il	drop		drop	1
157.55.39.110	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
216.218.206.118	United States	147.237.0.35	akaws.idf.il	drop		drop	1
109.186.77.41	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
66.249.79.62	Israel	147.237.0.33	idf.il	drop		drop	1
184.105.139.75	United States	147.237.0.33	idf.il	drop		drop	1
141.212.122.144	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

08-20-2016-11:04:02 to 08-20-2016-12:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.35	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	180
212.34.11.34	Jordan	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 212.34.11.34	Block	4
212.34.11.34	Jordan	147.237.77.216	dover.idf.il	Multiple Malformed URL from 212.34.11.34	Block	4
192.116.176.221	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
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	3
84.111.244.68	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
46.117.35.45	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
31.154.9.46	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
212.34.11.34	Jordan	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 212.34.11.34	Block	2
37.26.149.158	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	2
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arafat/terrorism2/	Block	1
212.34.11.34	Jordan	147.237.77.216	dover.idf.il	Illegal HTTP Version Android 4.2.2; GT-S7582 Build/JDQ39) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.98 Mobile Safari/537.36	Block	1
84.111.244.68	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
212.34.11.34	Jordan	147.237.77.216	dover.idf.il	Unknown HTTP Request Method 8cb1:0" in URL	Block	1
66.249.76.115	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
2.55.187.202	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
212.34.11.34	Jordan	147.237.77.216	dover.idf.il	Malformed URL	Block	1
131.253.25.188	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
46.117.35.45	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
207.46.13.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
68.180.228.231	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-ar/cogat.aspx	Block	1
176.106.43.59	Palestinian Territory, Occupied	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1065-he/dover.aspx	Block	1
79.176.91.9	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
180.76.15.28	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/main/stm	Block	1
212.34.11.34	Jordan	147.237.77.216	dover.idf.il	Abnormally Long Request request version	Block	1

08-20-2016-11:04:02 to 08-20-2016-12:04:02