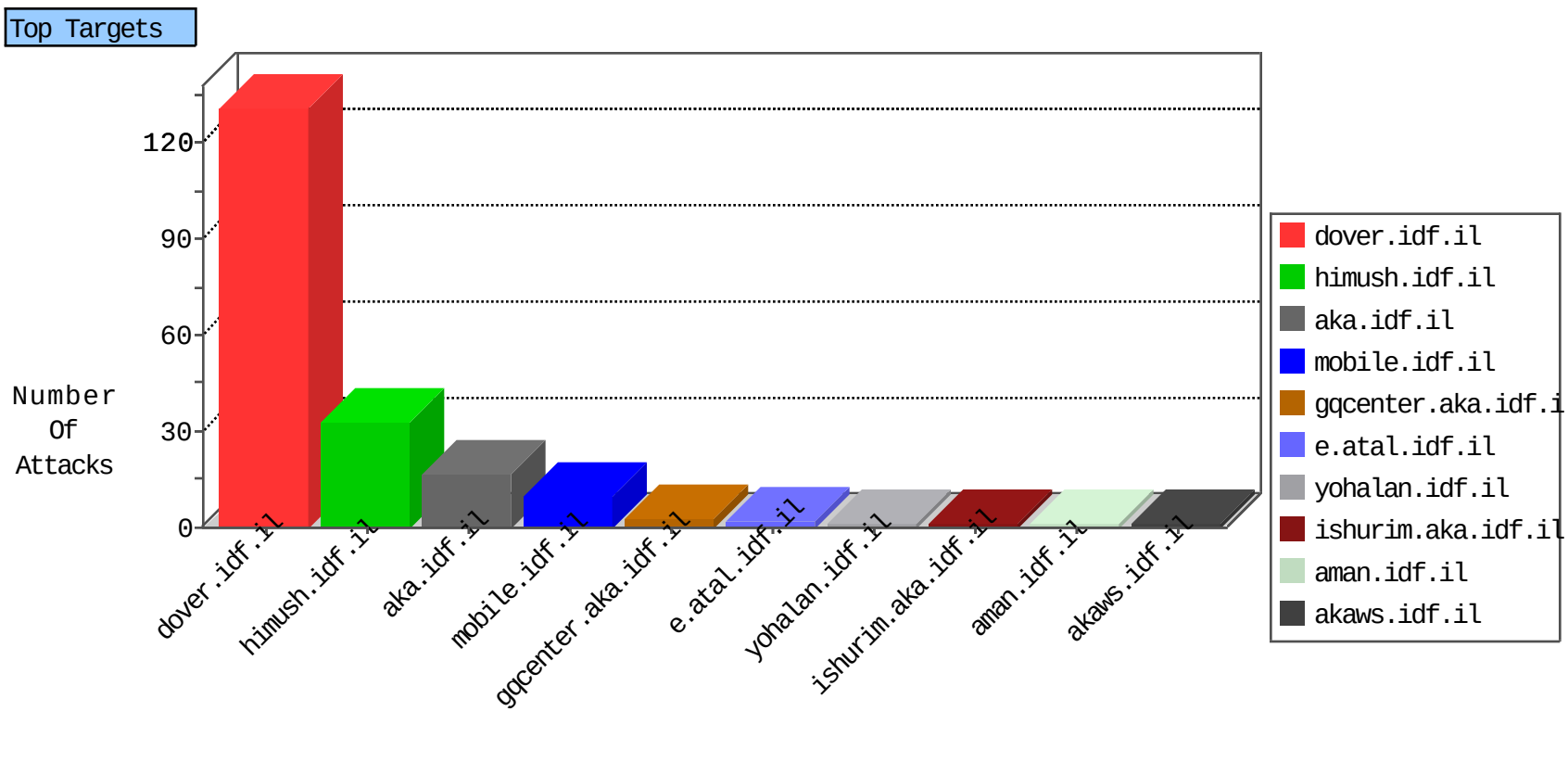
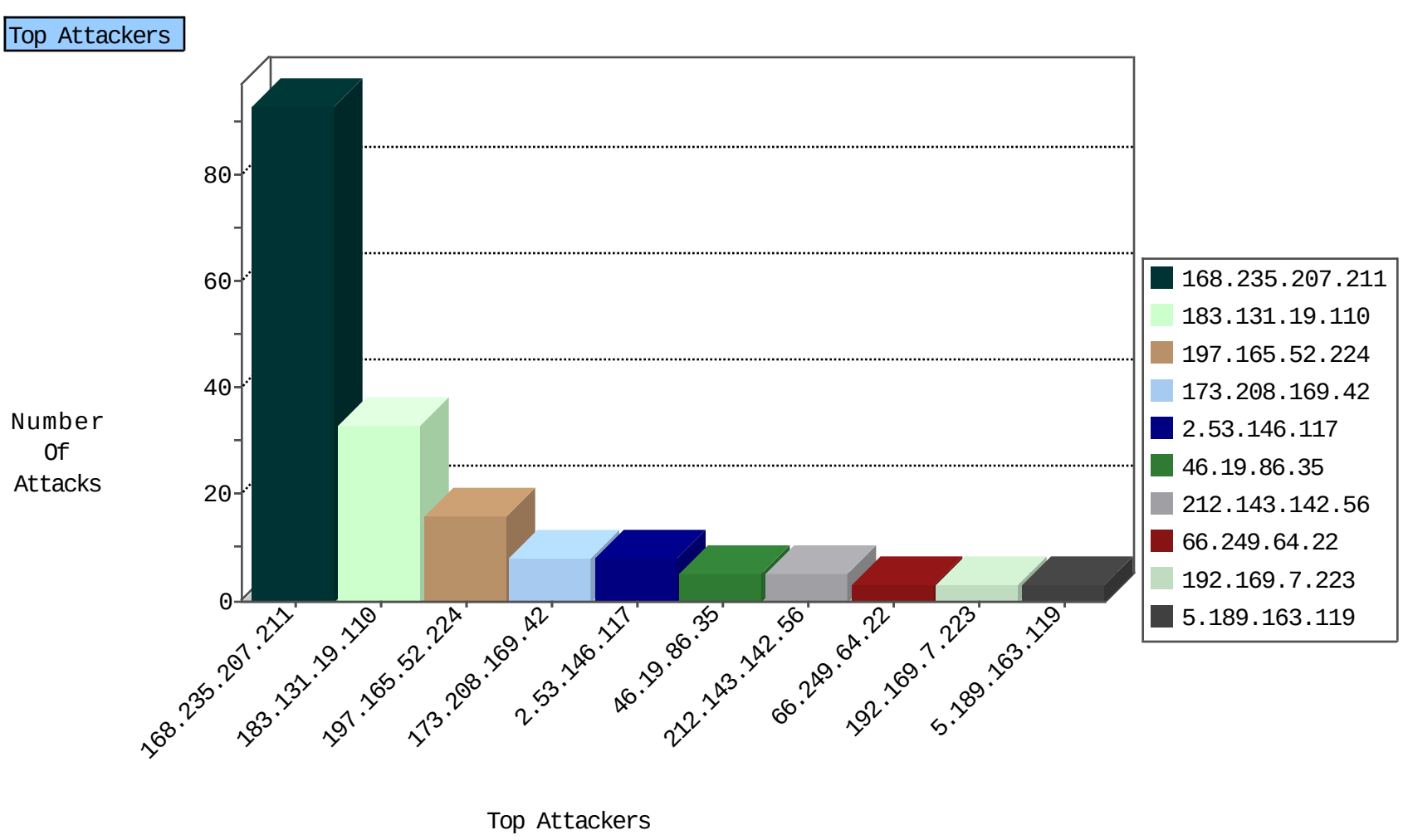
08-31-2016-02:04:01 to 08-31-2016-03:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-31-2016-02:04:01 to 08-31-2016-03:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
183.131.19.110	China	147.237.76.30	himush.idf.il	TCP Scan (vertical)	drop	171
183.131.19.110	China	147.237.76.30	himush.idf.il	block-sp-traf1	forward	5
168.235.207.211	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3

08-31-2016-02:04:01 to 08-31-2016-03:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
173.208.169.42	United States	147.237.72.166	aka.idf.il	C1000125: HTTP: Block admin login to gov.il sites ?q=user	Permit	8

08-31-2016-02:04:01 to 08-31-2016-03:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	2
5.189.163.119	147.237.76.202	Germany	e.halag.idf.il	ET SCAN Potential SSH Scan	1
185.141.27.44	147.237.76.201		e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.77.243	Ukraine	mobile.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
46.227.67.172	147.237.72.166	Sweden	aka.idf.il	ET SCAN NMAP -sS window 1024	1
5.189.163.119	147.237.77.19	Germany	law-forum.idf.il	ET SCAN Potential SSH Scan	1
5.189.163.119	147.237.76.201	Germany	e.atal.idf.il	ET SCAN Potential SSH Scan	1
94.103.150.195	147.237.72.166	Netherlands	aka.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.77.243	Ukraine	mobile.idf.il	ET SCAN NMAP -sS window 4096	1
66.249.79.99	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1

08-31-2016-02:04:01 to 08-31-2016-03:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
168.235.207.211	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	90
197.165.52.224	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.35	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.169.7.223	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	3
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.221.174	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
38.111.147.86	United States	147.237.77.216	dover.idf.il	drop		drop	2
212.143.165.117	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
180.97.106.162	China	147.237.0.35	akaws.idf.il	drop		drop	1
79.177.25.32	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
120.76.24.17	China	147.237.0.33	idf.il	drop		drop	1

08-31-2016-02:04:01 to 08-31-2016-03:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.146.117	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	8
66.249.64.22	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	2
183.131.19.110	China	147.237.76.30	himush.idf.il	NULL Character in Method	Block	1
66.102.9.13	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
178.154.149.7	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 178.154.149.7	Block	1
183.131.19.110	China	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.qq.com/404/search_children.js	Block	1
66.249.64.22	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.22	Block	1
178.154.149.7	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/chamatz/klali/default.	Block	1
207.46.13.64	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
178.255.87.242	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
66.249.66.180	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
183.131.19.110	China	147.237.76.30	himush.idf.il	Illegal Byte Code Character in Method	Block	1
46.19.86.63	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
94.103.150.195	Netherlands	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to /	Block	1

08-31-2016-02:04:01 to 08-31-2016-03:04:01