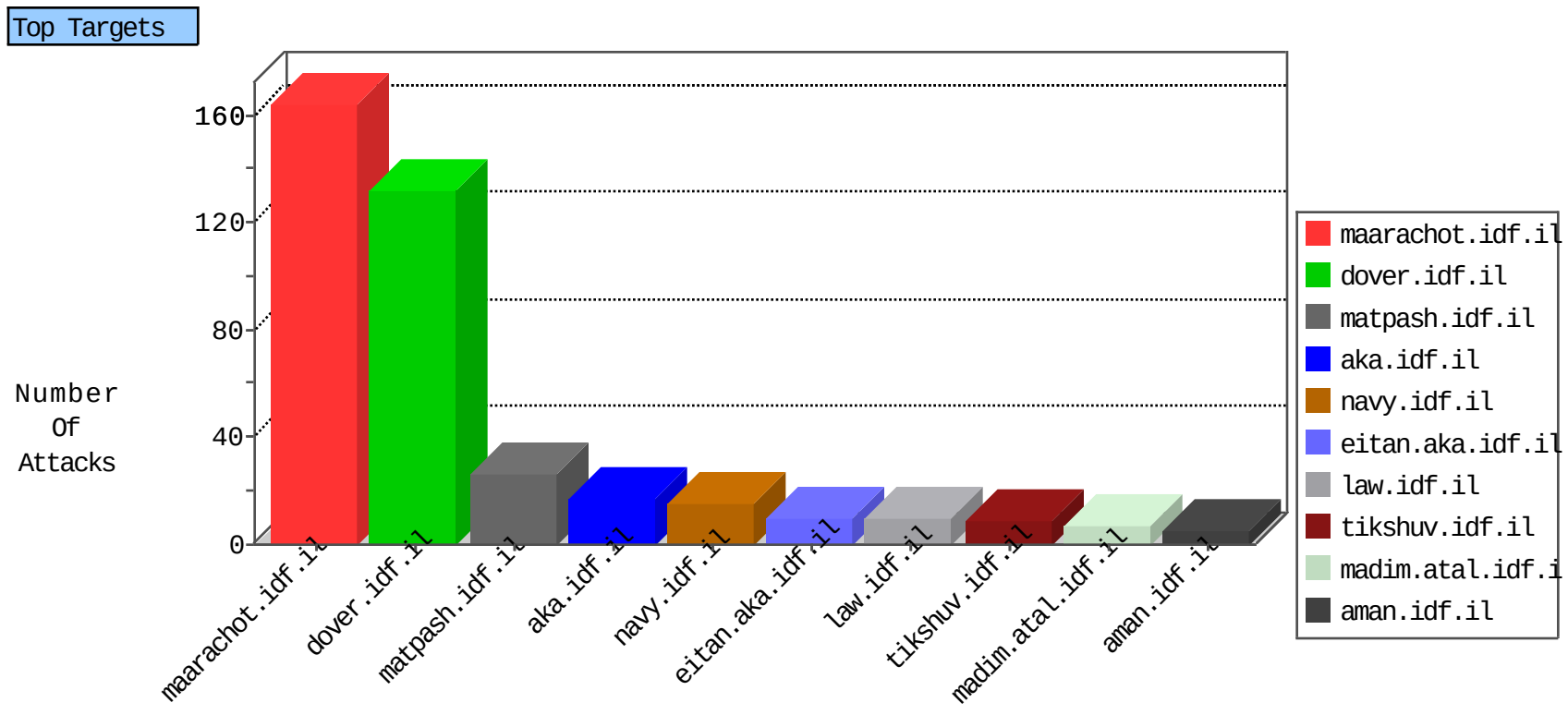
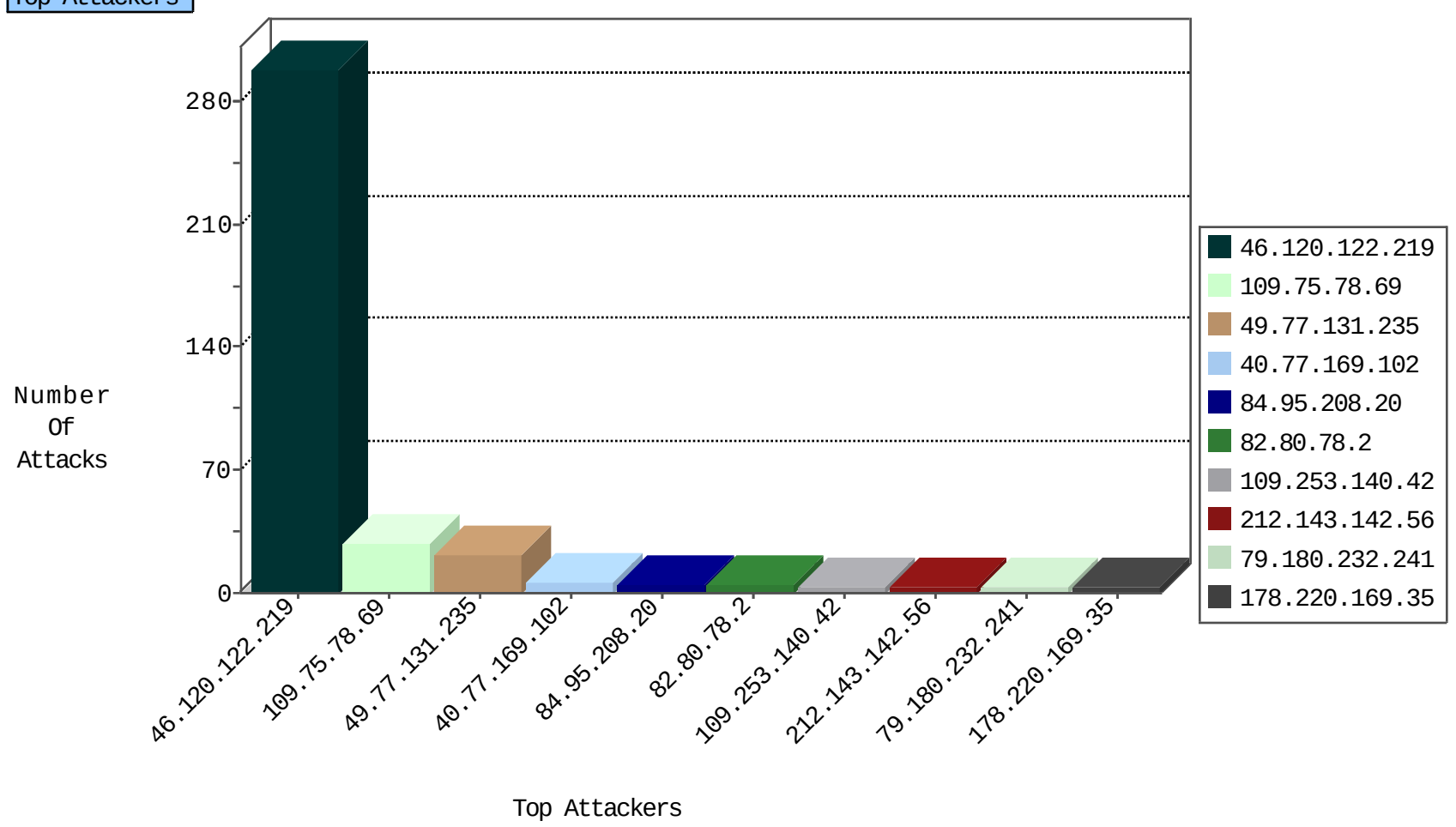
08-24-2016-05:04:03 to 08-24-2016-06:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-24-2016-05:04:03 to 08-24-2016-06:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.156.100	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
82.80.78.2	Israel	147.237.77.176	matpash.idf.il	Black List	drop	2
183.60.48.25	China	147.237.76.42	refuah.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
82.80.78.2	Israel	147.237.76.86	navy.idf.il	Black List	drop	2
94.177.160.214	Romania	147.237.76.86	navy.idf.il	Black List	drop	1
192.162.101.50	Russian Federation	147.237.76.197	e.himush.idf.il	Black List	drop	1
23.82.46.210	United States	147.237.76.202	e.halag.idf.il	Black List	drop	1
94.177.160.214	Romania	147.237.76.196	e.sviva.idf.il	Black List	drop	1
200.126.209.32	Argentina	147.237.77.243	mobile.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1

08-24-2016-05:04:03 to 08-24-2016-06:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
162.210.196.98	United States	147.237.77.234	halag.idf.il	C1000074: HTTP: majestic bot	Permit	2
5.189.188.111	Germany	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

08-24-2016-05:04:03 to 08-24-2016-06:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.77.170	Israel	maarachot.idf.il	Xenu Link Sleuth User Agent	164
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	88
46.120.122.219	147.237.76.86	Israel	navy.idf.il	Xenu Link Sleuth User Agent	10
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	9
46.120.122.219	147.237.76.200	Israel	eitan.aka.idf.il	Xenu Link Sleuth User Agent	8
46.120.122.219	147.237.77.74	Israel	law.idf.il	Xenu Link Sleuth User Agent	6
46.120.122.219	147.237.0.34	Israel	tikshuv.idf.il	Xenu Link Sleuth User Agent	6
46.120.122.219	147.237.77.176	Israel	matpash.idf.il	Xenu Link Sleuth User Agent	2
195.88.208.193	147.237.76.86	Russian Federation	navy.idf.il	ET SCAN NMAP -sS window 1024	2
178.220.169.35	147.237.0.34		tikshuv.idf.il	ET SCAN NMAP -f -sS	1
94.102.48.195	147.237.8.27	Netherlands	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
46.172.71.251	147.237.72.14	Ukraine	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
202.155.58.28	147.237.77.121	Indonesia	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
178.220.169.35	147.237.0.34		tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
133.208.21.66	147.237.72.217	Japan	e.idf.il	ET SCAN NMAP -sS window 1024	1
46.172.71.251	147.237.72.156	Ukraine	aman.idf.il	ET SCAN NMAP -sS window 1024	1
195.88.208.193	147.237.77.243	Russian Federation	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
178.220.169.35	147.237.0.34		tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1

08-24-2016-05:04:03 to 08-24-2016-06:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.75.78.69	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
40.77.169.102	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
74.82.47.35	United States	147.237.0.35	akaws.idf.il	drop		drop	1
184.105.139.83	United States	147.237.0.33	idf.il	drop		drop	1
89.151.191.4	Russian Federation	147.237.76.34	yohalan.idf.il	drop		drop	1
185.125.4.222	Poland	147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	1
185.125.4.222	Poland	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
137.116.71.170	United States	147.237.0.35	akaws.idf.il	drop		drop	1
66.249.65.161	Israel	147.237.0.33	idf.il	drop		drop	1
137.116.71.170	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1

08-24-2016-05:04:03 to 08-24-2016-06:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
49.77.131.235	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 49.77.131.235	Block	15
49.77.131.235	China	147.237.77.176	matpash.idf.il	PHP Attempt	Block	6
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.120.122.219	Block	4
46.19.86.132	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.140.42	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.180.232.241	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
84.95.208.20	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	2
109.253.159.1	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	1
49.77.131.235	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.asp	Block	1
83.24.68.182	Poland	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
46.120.122.219	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.120.122.219	Block	1
119.224.35.156	New Zealand	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
50.205.250.182	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	1
46.120.222.245	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
157.55.39.194	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/&q=للاسرائيلي &sa=x&ei=owytupr8joas0qxzyyc4cg&ved=0cdcqfjak	Block	1
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
183.160.115.80	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim/trackback/	Block	1
66.249.76.100	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
46.120.122.219	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized Method for Known URL from 46.120.122.219	None	1

08-24-2016-05:04:03 to 08-24-2016-06:04:03