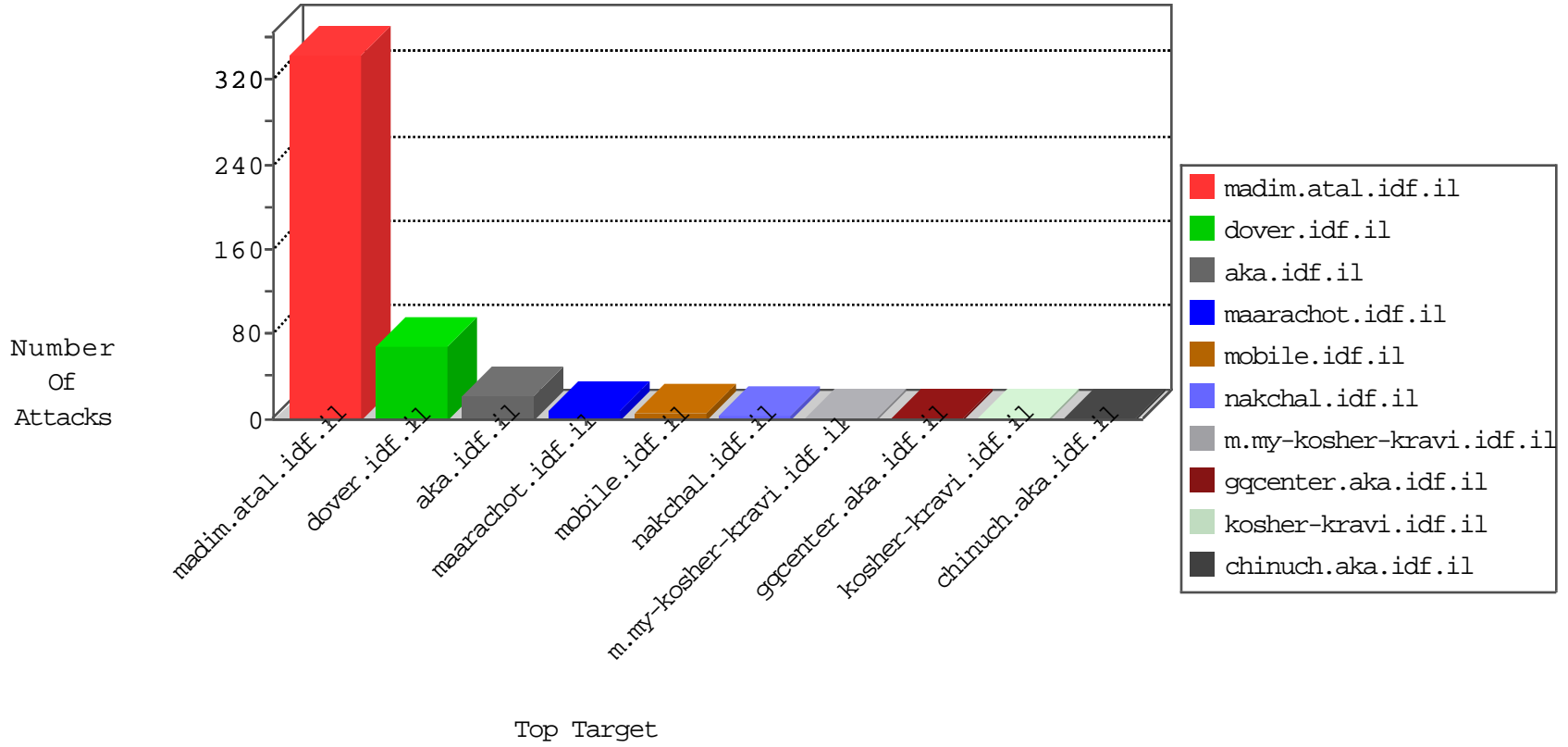




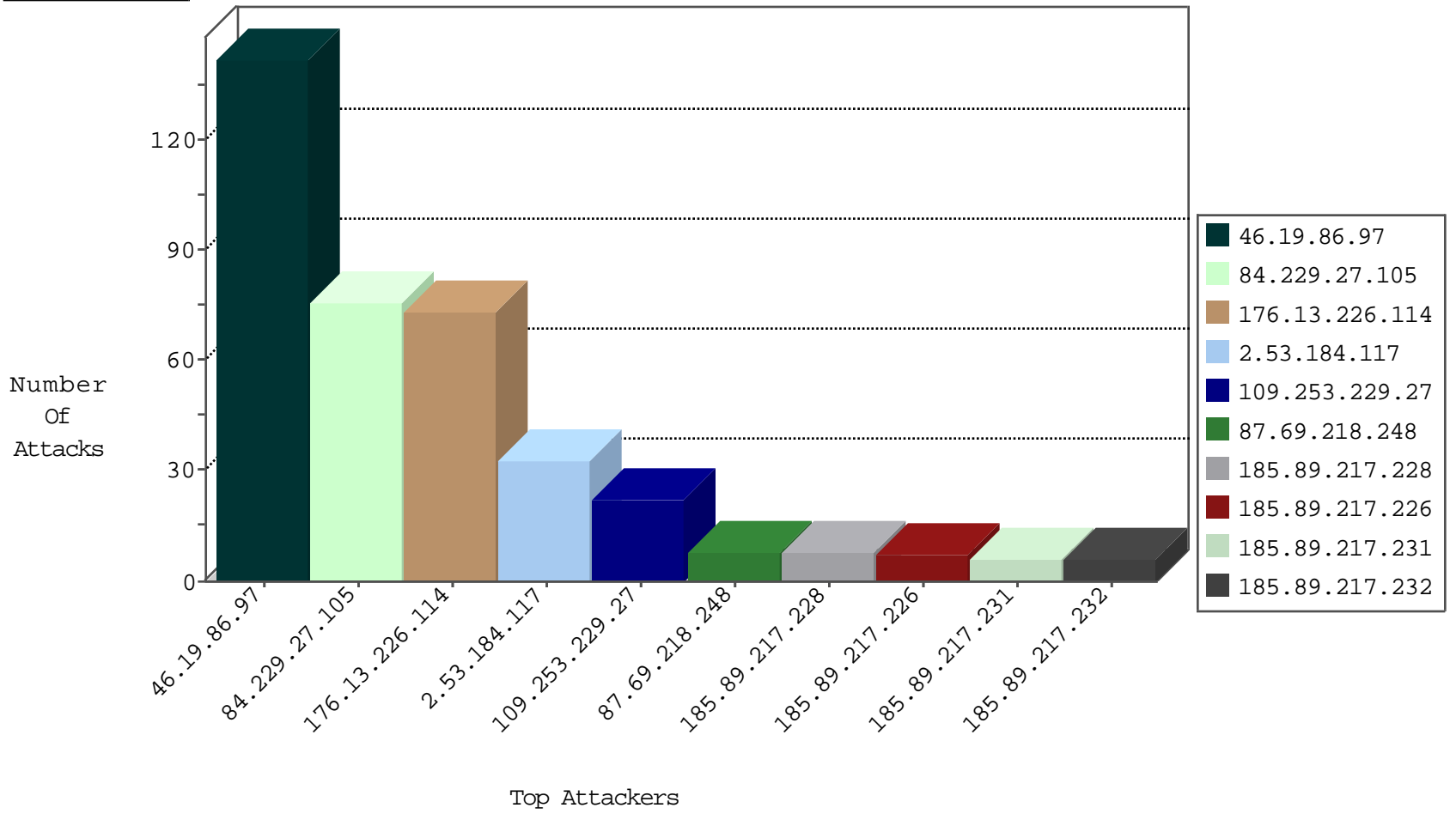
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.59.59.52	China	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	2
204.42.253.2	United States	147.237.76.148	ggcenter.aka.idf.il	Black List	drop	2
82.80.78.2	Israel	147.237.72.166	aka.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.147	chinuch.aka.idf.il	Black List	drop	2
161.18.96.101	Colombia	147.237.77.243	mobile.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
71.6.165.200	United States	147.237.76.201	e.atal.idf.il	Black List	drop	1
167.0.228.48	Colombia	147.237.76.199	e.nakchal.idf.il	JLM_Under_Attack_Con_Tcp	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.9.89.170	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
188.209.52.109	Netherlands	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
185.65.134.79	Sweden	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
84.109.180.213	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	2
198.167.223.33	147.237.76.31	Saint Kitts and Nevis	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
84.109.180.213	147.237.77.170	Israel	maarachot.idf.il	Xenu Link Sleuth User Agent	1
37.26.146.212	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
220.178.78.138	147.237.77.212	China	e.dover.idf.il	ET SCAN NMAP -sS window 4096	1
50.198.251.213	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.89.217.235	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.89.217.226	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.89.217.232	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.89.217.228	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.129.25.167	Greece	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
185.89.217.225	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
185.89.217.231	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
185.89.217.227	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
185.89.217.233	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
185.89.217.234	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
185.89.217.230	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
31.210.189.8	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	2
109.253.217.182	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
62.210.178.103	France	147.237.0.15	kosher-kravi.idf.il	drop	First packet isn't SYN	drop	2
62.210.178.103	France	147.237.0.17	m.my-kosher-kravi.idf.il	drop	First packet isn't SYN	drop	2
62.210.178.103	France	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	1
212.199.11.78	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
176.13.242.65	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	139
84.229.27.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	76
176.13.226.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	73
2.53.184.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
109.253.229.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
87.69.218.248	Israel	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	4
46.19.86.97	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	3
87.69.218.248	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/sip_storage/files/4/	Block	3
77.138.171.208	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar	Block	3
185.89.217.231	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
185.89.217.234	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
185.89.217.228	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
77.237.138.202	Czech Republic	147.237.77.235	sviva.idf.il	Unauthorized Method HEAD for /	Block	1
77.125.7.72	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$cb15031275 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
185.89.217.226	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.128	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/0/68480.gif	Block	1
77.138.69.157	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
185.89.217.227	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
87.69.164.38	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.69.249	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/gyus/general.aspx	Block	1
185.120.125.59	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
40.77.167.32	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
87.69.218.248	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 87.69.218.248	Block	1
66.249.76.33	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/error/styles/error.css	Block	1
192.95.29.116	Canada	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1
178.59.49.246	Greece	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/gyus/	Block	1
77.139.51.236	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gyus	Block	1
185.89.217.230	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.76.58	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/error/styles/error.css	Block	1
185.89.217.225	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1