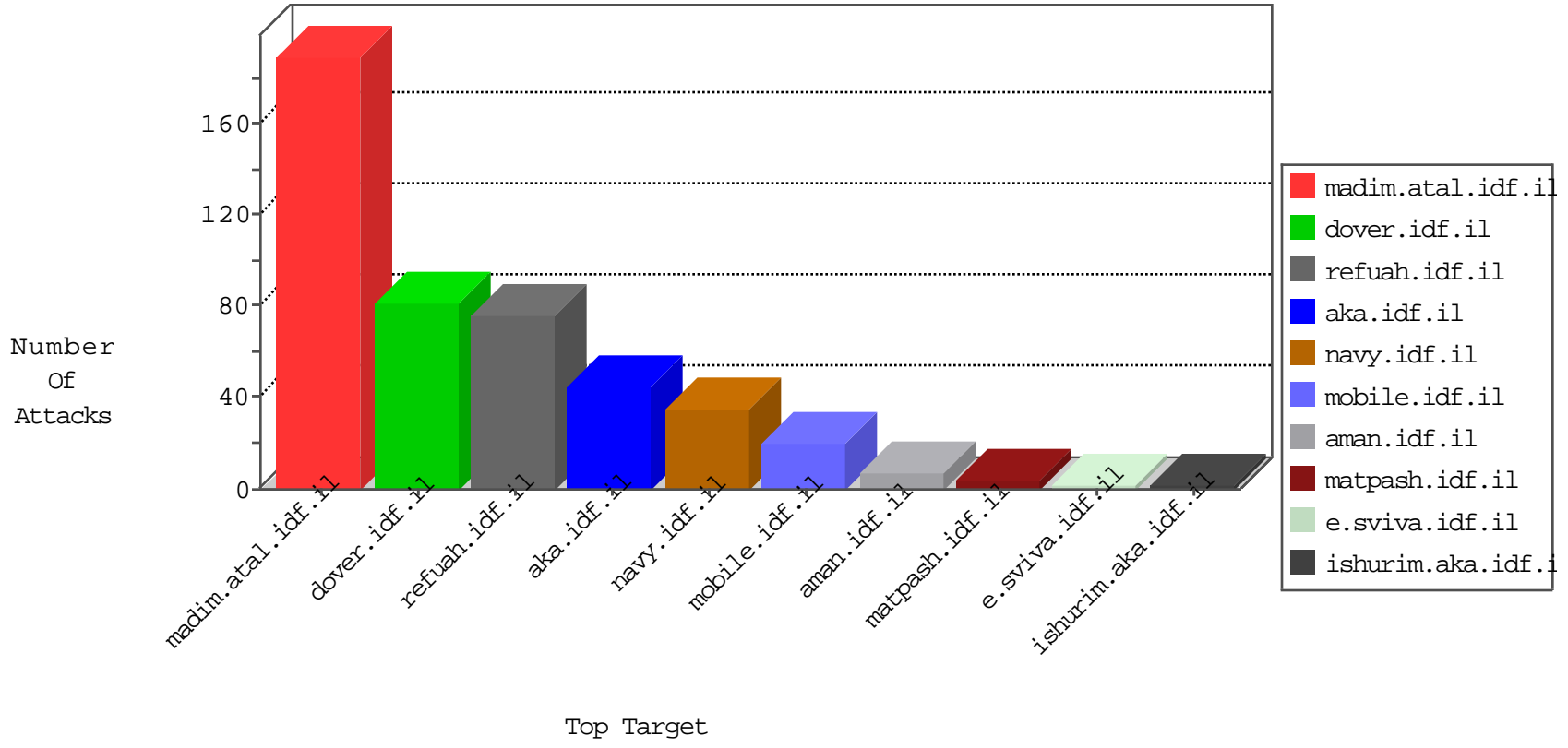


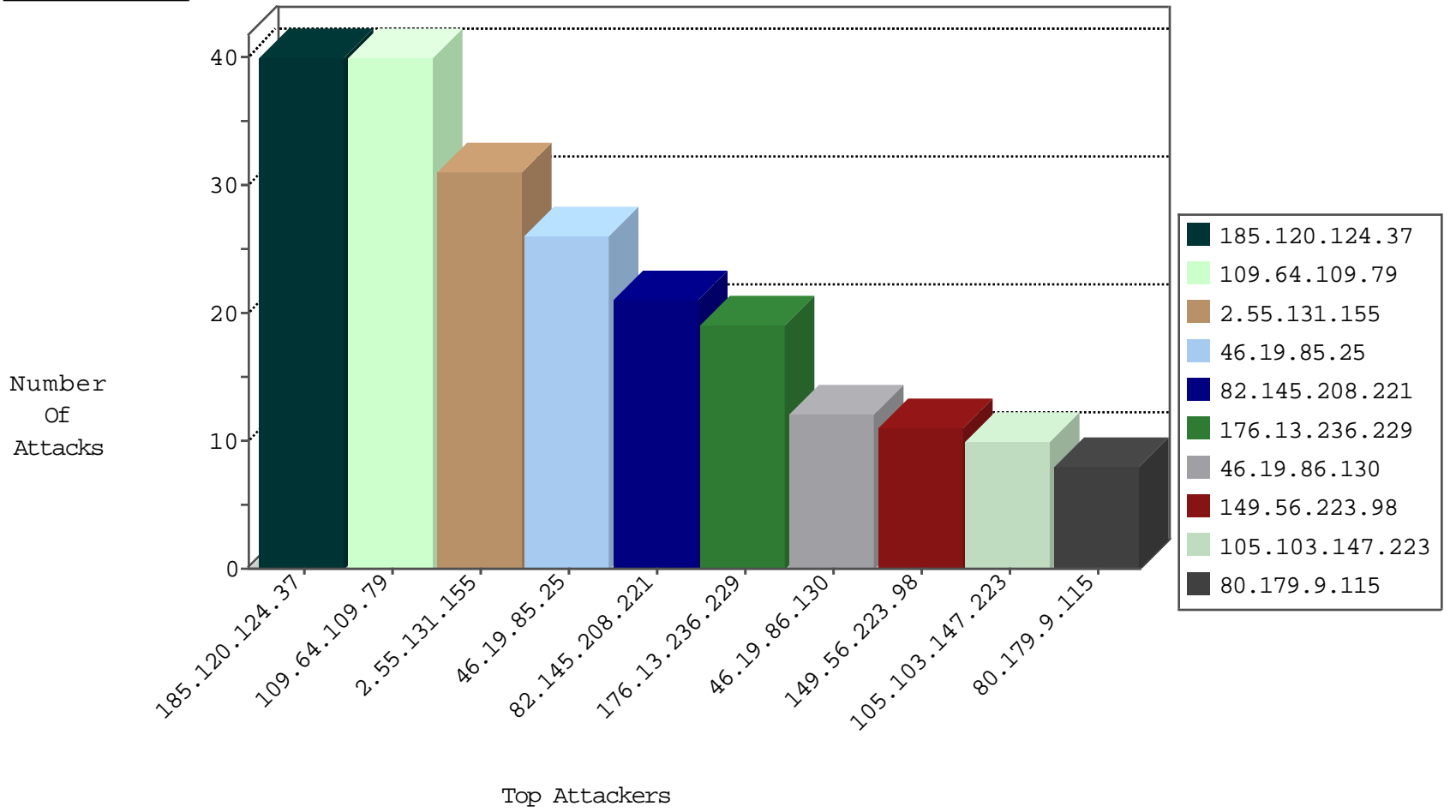
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.145.208.221	Europe	147.237.76.86	navy.idf.il	Black List	drop	21
105.103.147.223	Algeria	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-dun	dest-reset	10
46.19.85.65	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
103.24.202.225	Netherlands	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
82.80.78.2	Israel	147.237.77.176	matpash.idf.il	Black List	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
104.255.70.247	United States	147.237.76.196	e.sviva.idf.il	Black List	drop	1
46.121.24.174	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
89.248.171.2	Netherlands	147.237.76.148	ggcenter.aka.idf.il	Black List	drop	1
2.53.33.135	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
104.255.70.247	United States	147.237.76.197	e.himush.idf.il	Black List	drop	1
89.248.171.2	Netherlands	147.237.76.196	e.sviva.idf.il	Black List	drop	1
37.26.148.225	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.56.223.98	United States	147.237.76.86	navy.idf.il	C1000016: HTTP: administrator in URI	Permit	8
184.172.106.100	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
66.240.192.138	United States	147.237.77.243	mobile.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
------------------	----------------	------------------	------	-----------	-------

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.179.9.115	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
80.179.9.7	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
193.106.54.33	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
62.0.211.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
66.102.9.42	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.253.215.202	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
66.102.9.31	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
186.125.147.36	Argentina	147.237.72.156	anan.idf.il	drop	First packet isn't SYN	drop	3
149.56.223.104	United States	147.237.76.86	navy.idf.il	drop	SAM rule	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
103.224.131.1	New Zealand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
112.205.236.227	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
103.224.131.22	New Zealand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
209.208.126.125	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
103.224.131.66	New Zealand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.221.45	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.13.17.148	Israel	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	2
109.253.141.147	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
89.248.168.29	Netherlands	147.237.76.197	e.himush.idf.il	drop	SAM rule	drop	1
216.218.206.100	United States	147.237.0.35	akaws.idf.il	drop		drop	1
176.13.20.25	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.201.169	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
74.82.47.15	United States	147.237.0.33	idf.il	drop		drop	1
109.253.240.0	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	1
46.120.166.188	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.21.51	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
109.253.204.188	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
176.13.237.21	Israel	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	1
176.13.242.97	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
89.248.168.29	Netherlands	147.237.8.14	e.orchot.idf.il	drop	SAM rule	drop	1
180.97.106.162	China	147.237.8.27	e.madim.atal.idf.il	drop	SAM rule	drop	1
109.253.223.80	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
185.120.124.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
109.64.109.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
2.55.131.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
46.19.85.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
176.13.236.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
46.19.86.130	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	12
46.117.45.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
77.138.29.175	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/about.aspx	Block	4
109.253.210.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.14.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.63.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.64.35.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.239	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
66.249.76.52	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
37.26.148.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.102.9.42	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.53.135.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.165.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.135.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
88.202.218.240	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.53.169.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
80.230.224.238	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/scriptresource.axd	Block	1
77.139.136.22	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/gyiyus/yahash/sheelon.aspx	Block	1
80.230.225.198	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/jquery.nyromodal-1.6.2.js	Block	1
66.249.76.36	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
80.230.225.181	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/datepicker.css	Block	1
80.230.224.147	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/1740.png	Block	1
80.230.224.44	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/size100x0/3481.jpg	Block	1
80.230.225.252	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/ui/i18n/jquery-ui-i18n.js	Block	1
46.116.67.204	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
80.230.225.152	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
80.230.224.15	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/ui/ui.datepicker.js	Block	1
80.230.225.225	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery.plugins/jquery.equalheights.js	Block	1
5.29.155.138	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/	Block	1
80.230.225.58	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/shared/clientscripts/ui/ui.datepicker.js	Block	1
80.230.224.189	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/2317.png	Block	1
149.56.223.98	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/admin.php	Block	1
68.180.228.231	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1035-ar/cogat.aspx	Block	1
80.230.225.193	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/shared/clientscripts/jquery/expand.js	Block	1
80.230.224.105	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/print.css	Block	1
92.90.16.102	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.102.9.31	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
80.230.225.165	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/images/shared/menuright.png	Block	1
80.230.225.117	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/size100x0/3468.gif	Block	1
80.230.224.39	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/scriptresource.axd	Block	1
80.230.225.232	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/scriptresource.axd	Block	1
80.230.225.207	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/1.he/scroller/skin.css	Block	1
2.53.169.187	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
80.230.225.40	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/size100x0/3469.jpg	Block	1