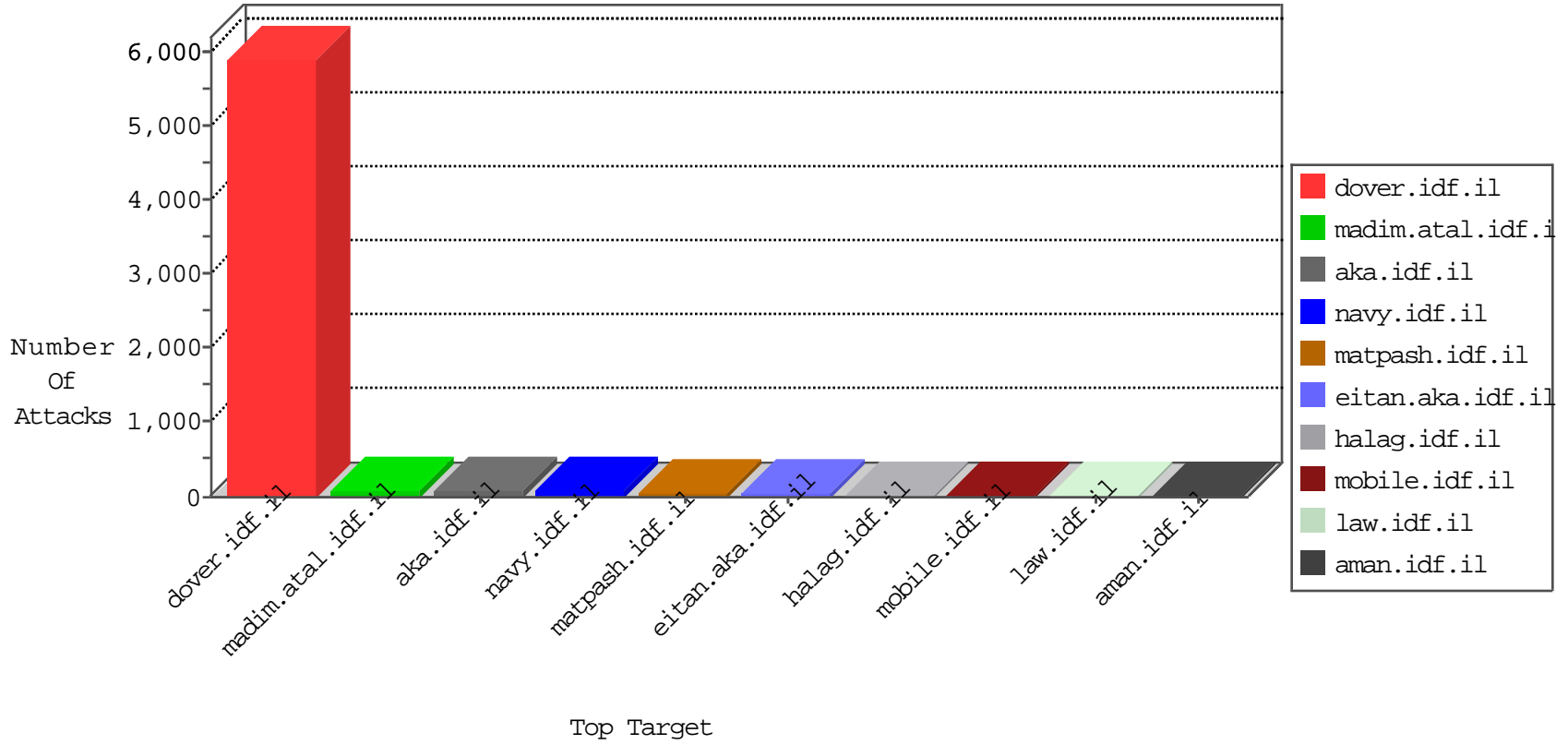


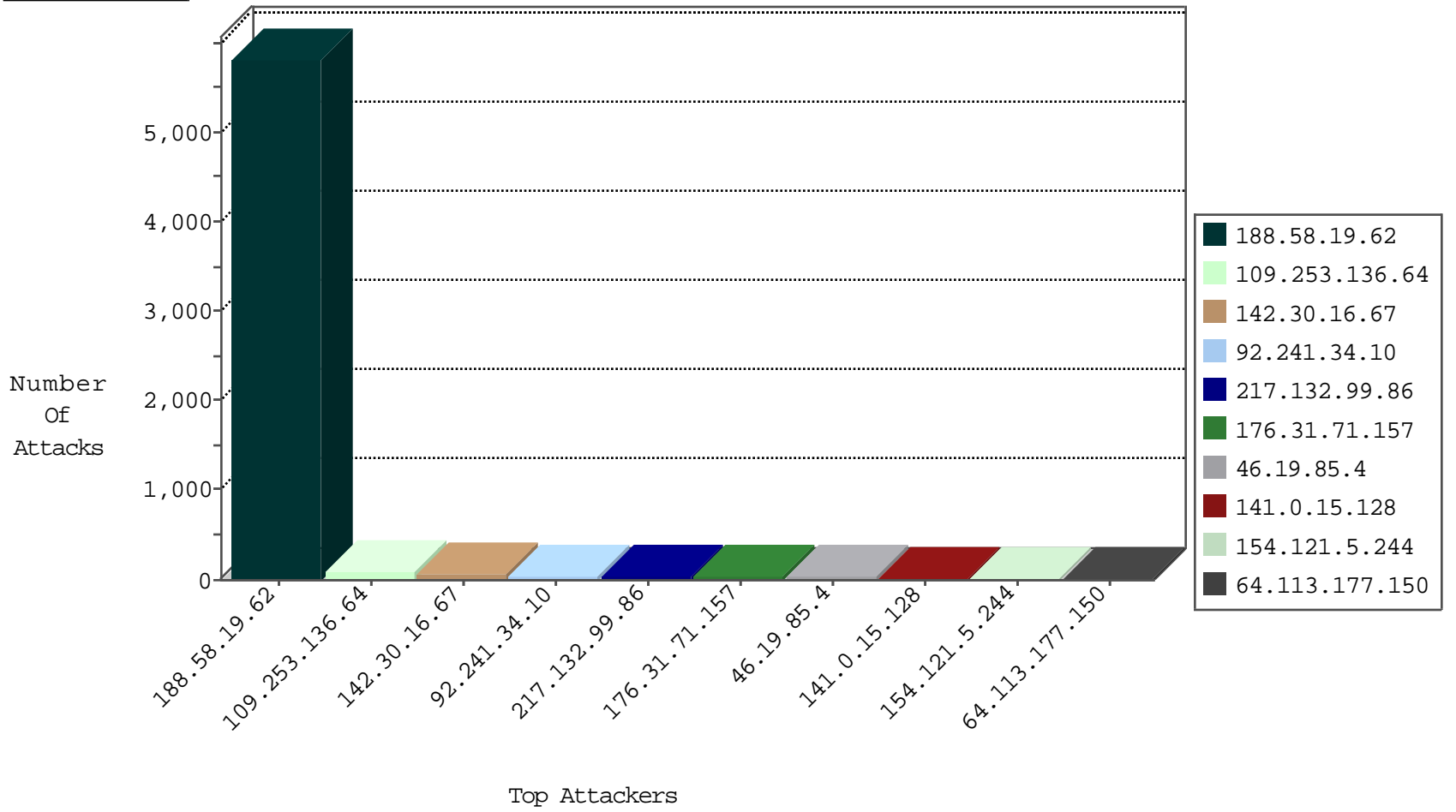
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	doover.idf.il	HTTP Page Flood Attack	forward	3
66.240.192.138	United States	147.237.76.177	ncore.idf.il	Black List	drop	1
80.82.78.27	Netherlands	147.237.76.148	ggcenter.aka.idf.il	Black List	drop	1

Top Attackers In IPS

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

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
208.100.26.228	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.0.16	United Kingdom	ny-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
54.196.69.137	147.237.0.15	United States	kosher-kravi.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
163.172.169.150	147.237.77.179	United Kingdom	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
93.158.203.196	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
188.58.19.62	Turkey	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5798
142.30.16.67	Canada	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	45
92.241.34.10	Jordan	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	43
217.132.99.86	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
141.0.15.128	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	20
64.113.177.150	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
84.229.82.73	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
109.253.136.22	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.4	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	9
46.19.85.4	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
46.19.85.4	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
46.19.85.217	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.217	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
154.121.5.244	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.43.122.122	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
154.121.5.244	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
154.121.5.244	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
141.0.14.210	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
154.121.5.244	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
185.120.124.49	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.186	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.245.246	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
142.30.16.67	Canada	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	3
82.166.235.55	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.117.105.230	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
142.30.16.67	Canada	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	2
176.31.71.157	France	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
84.229.39.100	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
176.31.71.157	France	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
142.30.16.67	Canada	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
176.31.71.157	France	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
187.227.214.90	Mexico	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
2.53.171.87	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
176.31.71.157	France	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.85.71	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
176.31.71.157	France	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
187.227.214.90	Mexico	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
176.31.71.157	France	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
176.13.8.236	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
154.121.5.244	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
176.13.21.123	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
85.65.6.213	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
176.31.71.157	France	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.85.13	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
37.26.148.146	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
176.31.71.157	France	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
207.46.13.10	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.4	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
185.3.147.90	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.136.64	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	87
185.32.179.184	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.245.235	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.252	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/1/64381.pdf	Block	1
79.182.112.210	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1407-he/atal.aspx	Block	1
46.19.86.186	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.76.79	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
190.238.207.11	Peru	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
83.130.64.253	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
157.55.39.115	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
68.180.230.47	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1398-en/dover.aspx	Block	1
213.151.35.214	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/giyus/	Block	1
84.229.82.73	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.65.24	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-21998-he/idfgdover.aspx	Block	1
172.98.84.95	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/drushim/general.aspx	Block	1
68.180.230.161	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakchal.idf.il/1117-he/nakhal.aspx	Block	1
87.68.11.255	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/giyus/general.aspx	Block	1
66.249.69.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/chinuch/gallery/showpicture.asp	Block	1
183.160.115.123	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1819-he/idfg.aspx/trackback/	Block	1
77.139.73.200	France	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/general.aspx	None	1