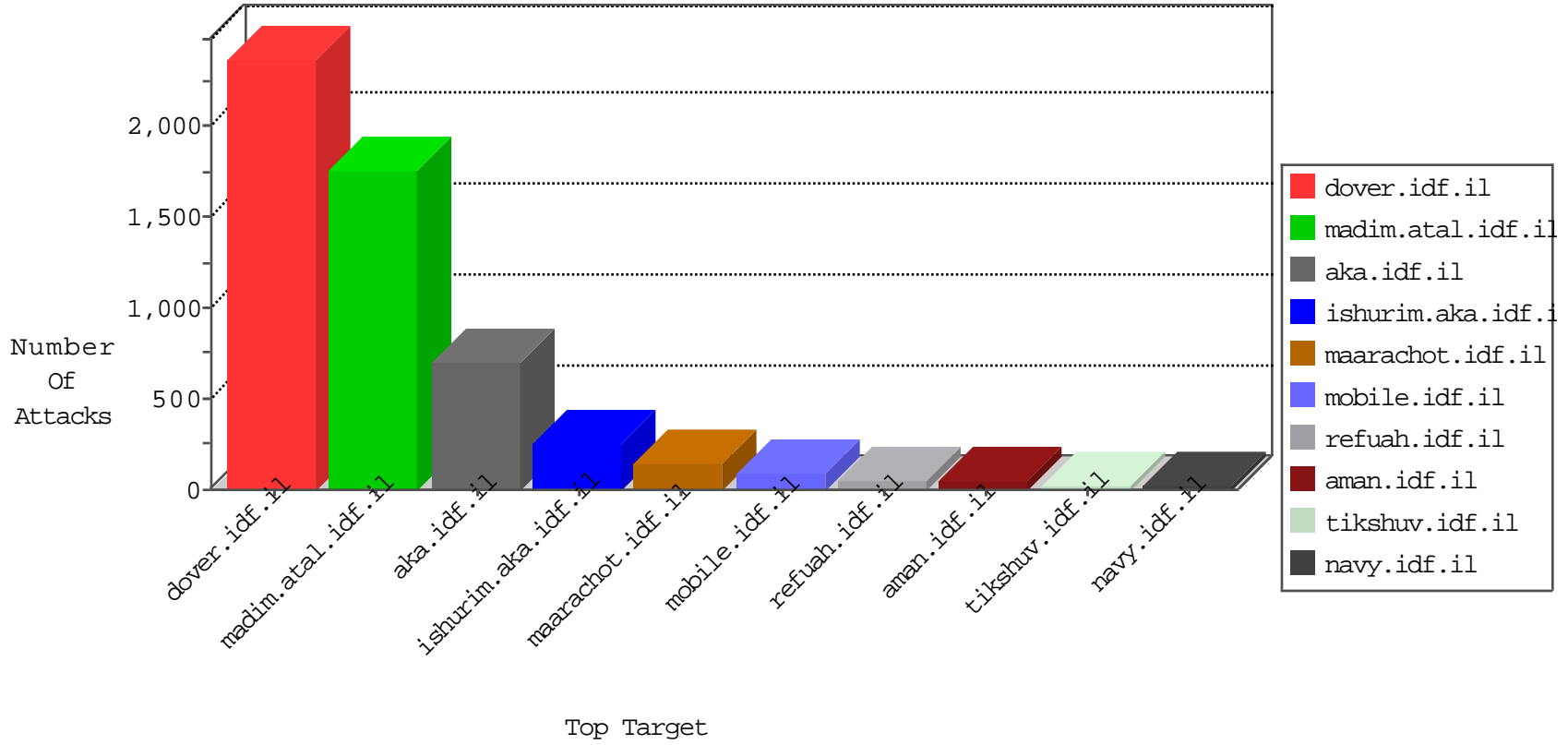


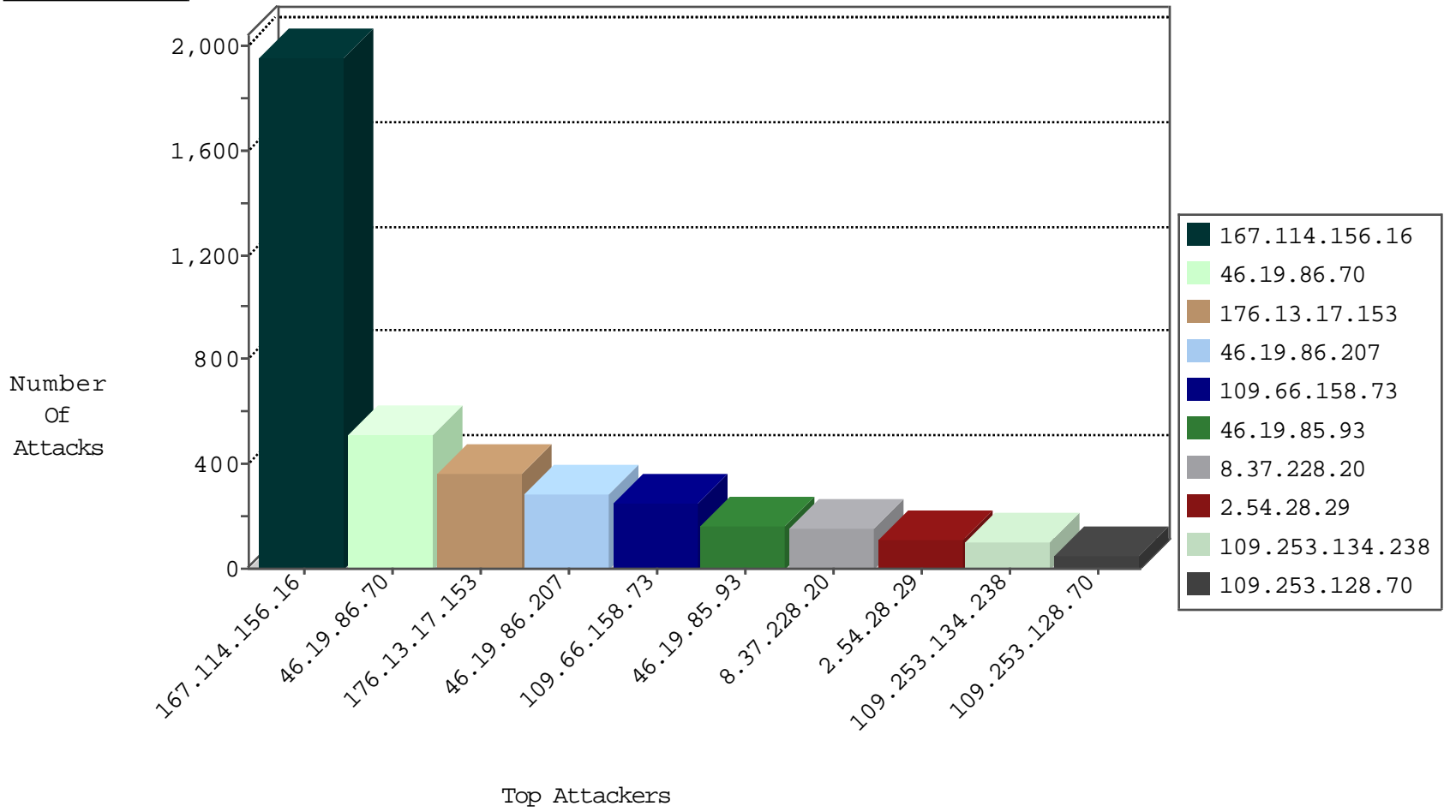
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3212
84.109.13.208	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	15
109.66.160.66	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
8.37.228.20	Anonymous Proxy	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	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
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.66.158.73	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	234
8.37.228.20	Anonymous Proxy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	82
8.37.228.20	Anonymous Proxy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
149.88.205.69	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	38
185.120.125.43		147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	33
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
2.52.143.138	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	28
107.167.108.45	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
217.132.131.205	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
173.252.121.115	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
149.88.5.240	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
2.52.148.15	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
173.252.121.119	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
109.66.158.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
85.250.157.191	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
85.64.248.8	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.246.136.200	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
12.26.51.99	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
217.194.199.151	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
212.143.233.133	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
66.249.65.103	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
109.67.48.56	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
77.125.9.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
132.66.100.56	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
2.52.2.59	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.86.21	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
87.68.145.23	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
37.46.39.55	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
2.54.28.29	Israel	147.237.0.19	medim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
173.252.121.116	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.201	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
2.52.2.59	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	8
172.56.3.96	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.76	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.64.149.185	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
46.19.85.232	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.202	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
207.232.21.105	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
62.90.35.162	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.217	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
172.85.9.66		147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.202	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.180.12.109	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
5.22.130.171	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.217	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.94.164.24	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.246.139.222	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
79.176.9.182	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.70	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	276
46.19.86.207	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	177
176.13.17.153	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	170
46.19.86.70	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	164
176.13.17.153	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	135
109.253.134.238	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	105
2.54.28.29	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
46.19.86.207	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
46.19.85.93	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	84
46.19.86.70	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	75
46.19.85.93	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	74
176.13.17.153	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	59
109.253.128.70	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	50
176.13.5.210	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	42
46.19.85.232	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	24
46.19.86.224	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	24
109.67.48.56	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.67.48.56	Block	13
46.19.86.203	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	13
46.19.85.19	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
46.19.85.62	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
109.253.202.69	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
176.12.146.110	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
109.253.138.132	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	3
2.54.15.43	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.148.211	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.23.127	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.140.75	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.136.200	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.160	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.47	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.50.50	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.56	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.178.13.216	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	3
109.253.203.165	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.16.229	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.146.222	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
84.108.5.0	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
52.90.147.70	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 52.90.147.70	Block	2
93.172.238.83	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
213.151.38.51	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
79.180.166.161	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1362-he/dover.aspx	Block	2
85.64.248.8	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
82.81.193.82	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	2
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
84.110.212.189	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
212.25.82.123	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	2
2.54.15.141	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2