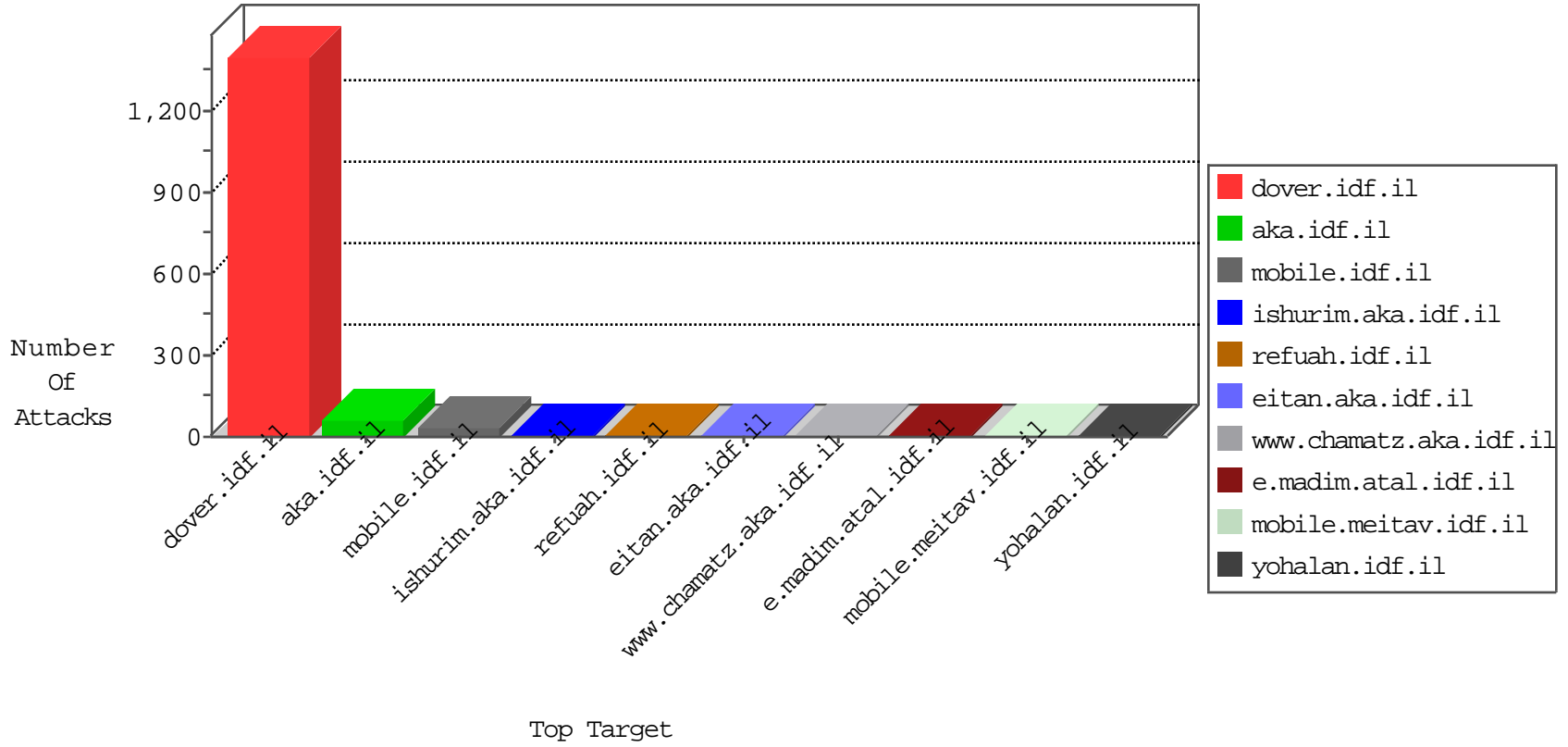


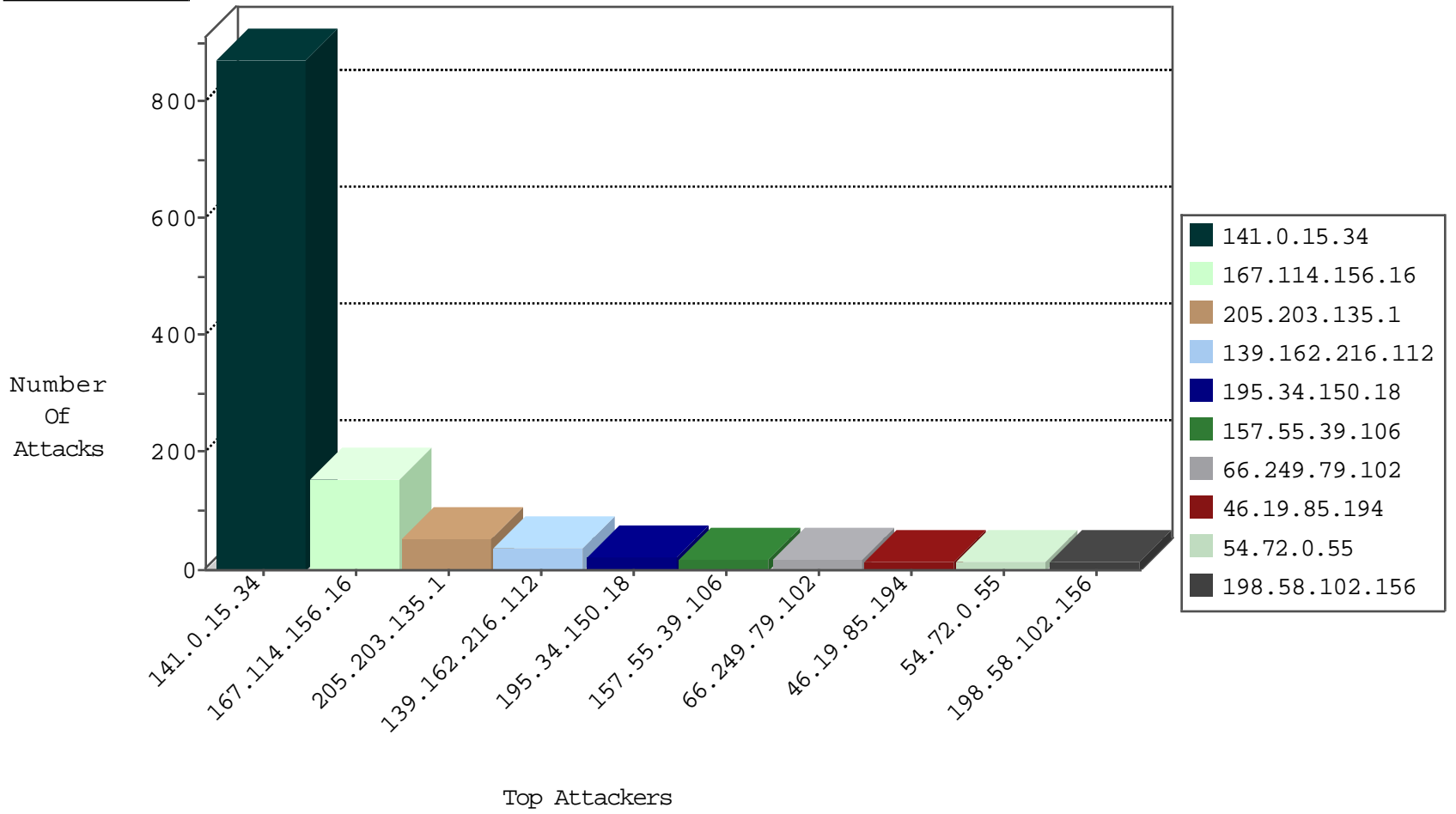
IDF Under Attack Daily Report



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	HTTP-POST-Segmented-DoS	dest-reset	5576
68.225.216.19	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2930
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2734
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1664
23.27.13.103	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1049
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	10
94.102.52.10	Netherlands	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
204.42.253.132	United States	147.237.76.148	ggcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
46.174.54.63	Russian Federation	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
209.126.136.2	United States	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	TCP handshake violation, first packet not syn	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	3
203.86.29.220	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN NMAP -f -sS	1
80.82.78.38	147.237.76.34	Netherlands	yochalan.idf.il	ET SCAN NMAP -sS window 1024	1
41.140.253.9	147.237.8.27	Morocco	e.madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
13.92.122.143	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sS window 2048	1
212.129.15.245	147.237.72.217	France	e.idf.il	ET SCAN NMAP -sS window 1024	1
203.86.29.220	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
41.140.253.9	147.237.8.27	Morocco	e.madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
13.92.122.143	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sS window 3072	1
13.92.122.143	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -f -sS	1
203.86.29.220	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN NMAP -sS window 2048	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
141.0.15.34	Norway	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	873
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
66.249.79.102	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
162.243.125.185	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.194	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
87.203.102.200	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.102.156	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
54.244.162.211	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
66.102.6.131	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
88.254.110.197	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.102.6.188	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
79.180.62.195	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.32.179.245	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
157.55.39.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
92.247.181.29	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
41.42.6.49	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.93.184	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.242.136	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.102.6.191	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
149.78.109.205	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
8.37.227.69	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.93.247	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.116.53.232	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.69.38	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.116.92.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.144.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
23.27.13.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
176.13.10.87	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.179.172.58	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.88.230	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
54.242.61.88	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.253.227.60	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.126.52	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.21.145	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.131.72	Israel	147.237.77.216	dover.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
176.13.21.145	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	2
54.212.115.207	United States	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1380-he/dover.aspx parameter PageNum	Block	1
194.12.229.104	Bulgaria	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
72.29.127.13	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	1
184.105.139.70	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
66.249.64.119	Israel	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on navy.idf.il/gyus/forum/asp/showforum.asp	Block	1
198.20.69.74	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
83.68.225.42	Sweden	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/66846.pp'a=0	Block	1
184.168.200.23	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
66.249.65.112	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
199.30.25.79	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
104.236.222.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-ar	Block	1
188.165.204.224	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.177	Block	1
212.0.137.106	Sudan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
176.9.127.69	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/	Block	1
54.188.252.77	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1380-he/dover.aspx	Block	1
194.12.229.104	Bulgaria	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 194.12.229.104	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/view_imgtop.asp	Block	1