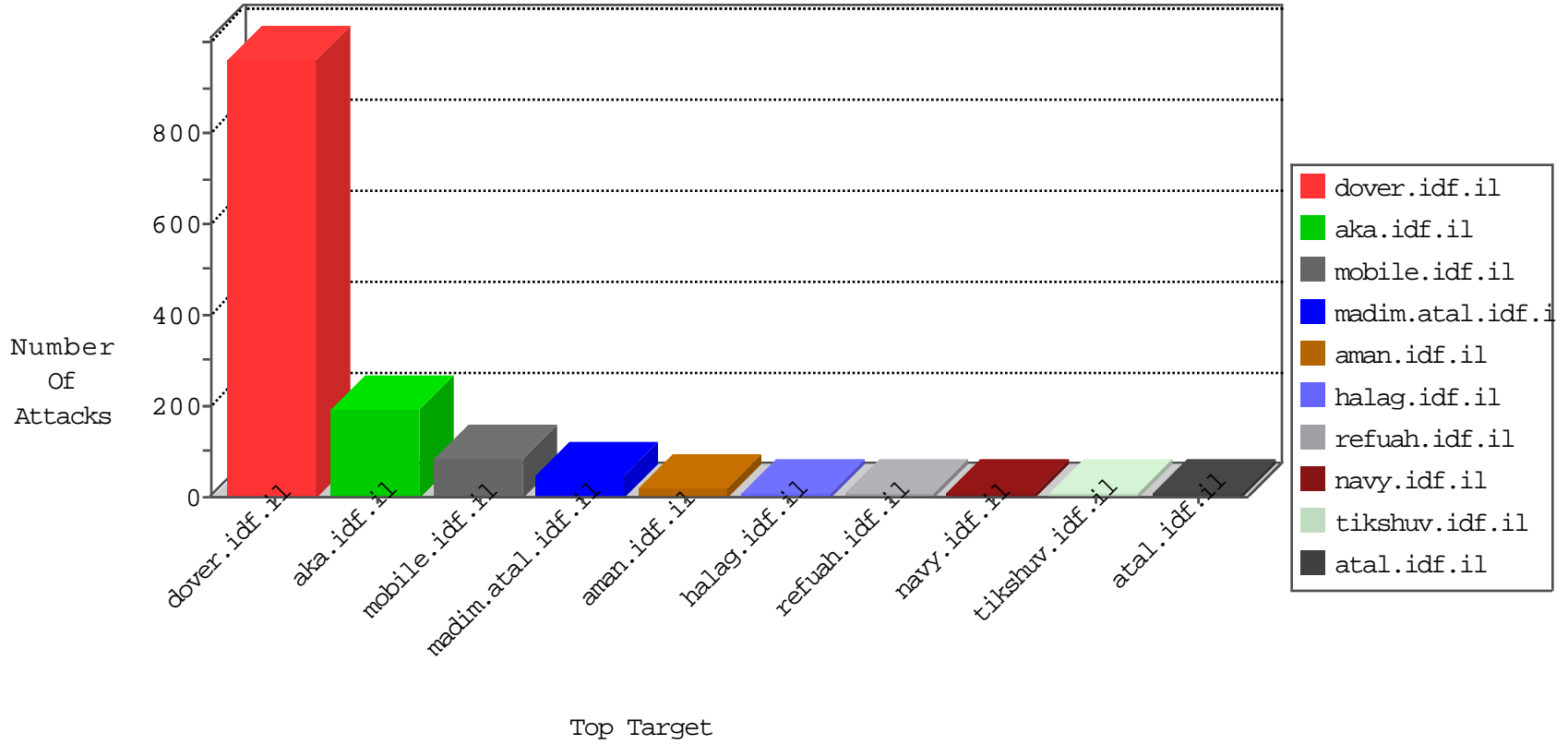


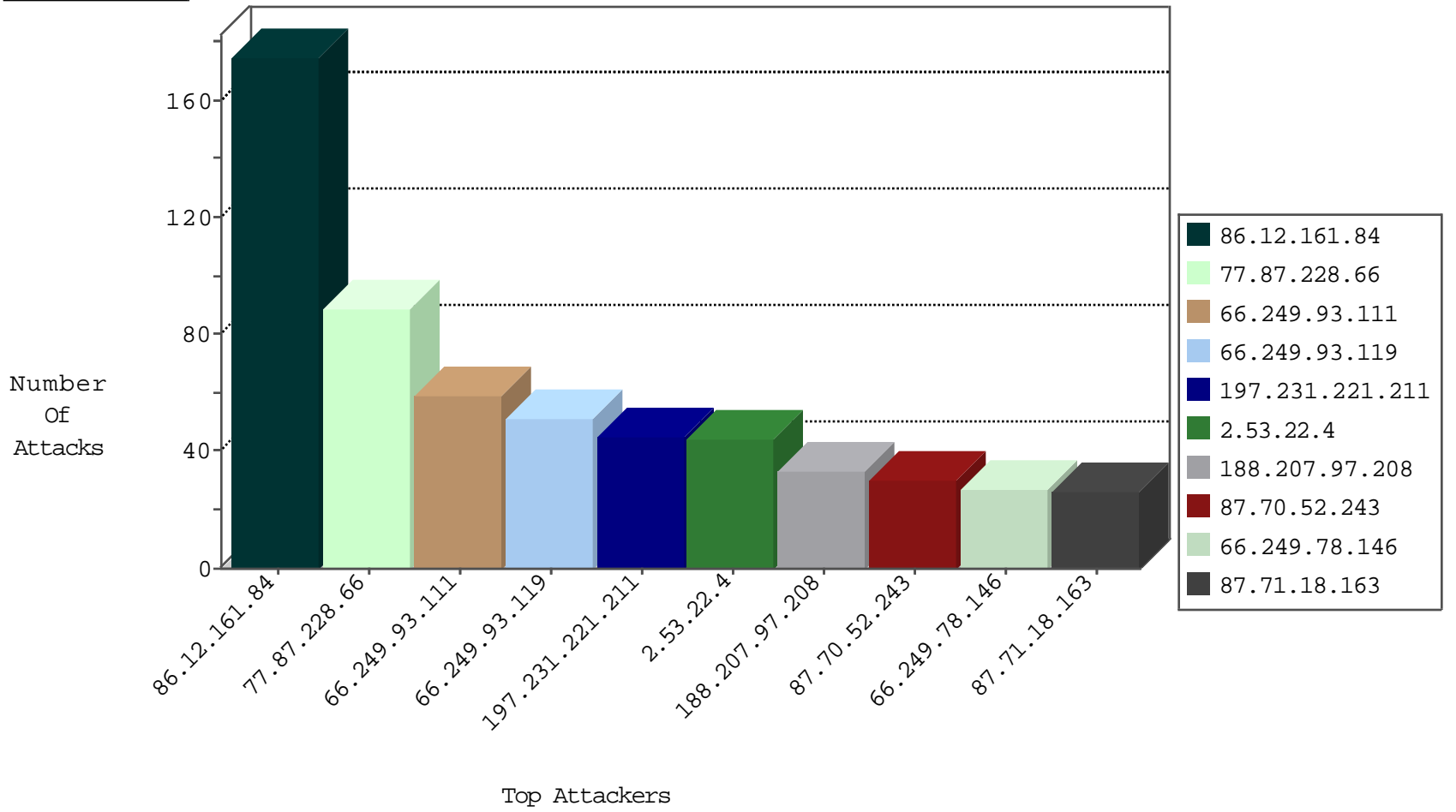
# IDF Under Attack Daily Report



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	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1343
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	736
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
62.75.207.109	Germany	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
62.75.207.109	Germany	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
198.20.69.74	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	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	4
46.121.200.140	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	2
188.210.114.110	147.237.0.34	Iran, Islamic Republic of	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
107.158.255.194	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.77.212	Ukraine	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
84.94.105.215	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
163.172.140.23	147.237.0.33	United Kingdom	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.201.236.155	147.237.77.212	Ukraine	e.dover.idf.il	ET SCAN NMAP -sS window 2048	1
91.201.236.155	147.237.77.212	Ukraine	e.dover.idf.il	ET SCAN NMAP -f -sS	1
202.124.226.211	147.237.0.16	Palau	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
86.12.161.84	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	175
77.87.228.66	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	86
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
188.207.97.208	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
66.249.93.119	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
66.249.93.111	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
87.71.18.163	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	26
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
185.89.217.225	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
87.203.102.200	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
185.89.217.228	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
84.109.210.87	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
185.89.217.229	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
185.89.217.231	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
109.186.150.36	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
185.89.217.233	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
66.249.81.218	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
84.228.84.83	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	13
66.249.81.212	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
52.29.223.39	Germany	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
46.19.85.218	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
198.58.102.117	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
147.75.208.236	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.13.3.165	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.103.91	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
2.53.62.174	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
89.187.219.146	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
80.246.133.55	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
128.242.249.12	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
157.55.39.209	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.93.111	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
207.46.13.137	United States	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
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.93.115	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
147.75.208.225	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.179.180.48	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
147.75.208.231	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.253.219.233	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.89.217.234	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.22.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
84.109.210.87	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
109.186.150.36	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
37.46.39.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.108.95.55	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 84.108.95.55	Block	2
109.253.219.233	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.51.194.114	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ https://twitter.com/	Block	1
66.249.78.111	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/tfasim.aspx	Block	1
2.53.62.174	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
185.3.144.33	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
50.232.195.6	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
147.75.208.225	Switzerland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.183.129.128	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	1
5.29.179.244	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
87.69.122.69	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1274-he/atal.aspx	Block	1
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
54.189.220.2	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation ForumId in www.tikshuv.idf.il/modules/forums/forum.aspx	Block	1
147.75.208.228	Switzerland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.94.105.215	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/templates/homepage/mobile	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/yoman.asp	Block	1
88.135.250.93	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/66846.ppt'a=0	Block	1
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.75.16	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/scroller/skin.css	Block	1
149.78.175.142	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
66.249.79.89	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/profs.asp	Block	1
40.77.167.38	United States	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.93.111	Israel	147.237.77.216	dover.idf.il	Multiple URL is Above Root Directory from 66.249.93.111	Block	1
66.249.75.24	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layout.css	Block	1
157.55.39.133	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/misrot.aspx	Block	1
84.108.95.55	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/gyus/login.aspx	Block	1
66.249.79.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
46.116.7.180	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct117 in www.aka.idf.il/main/sachar/payslips.aspx	None	1