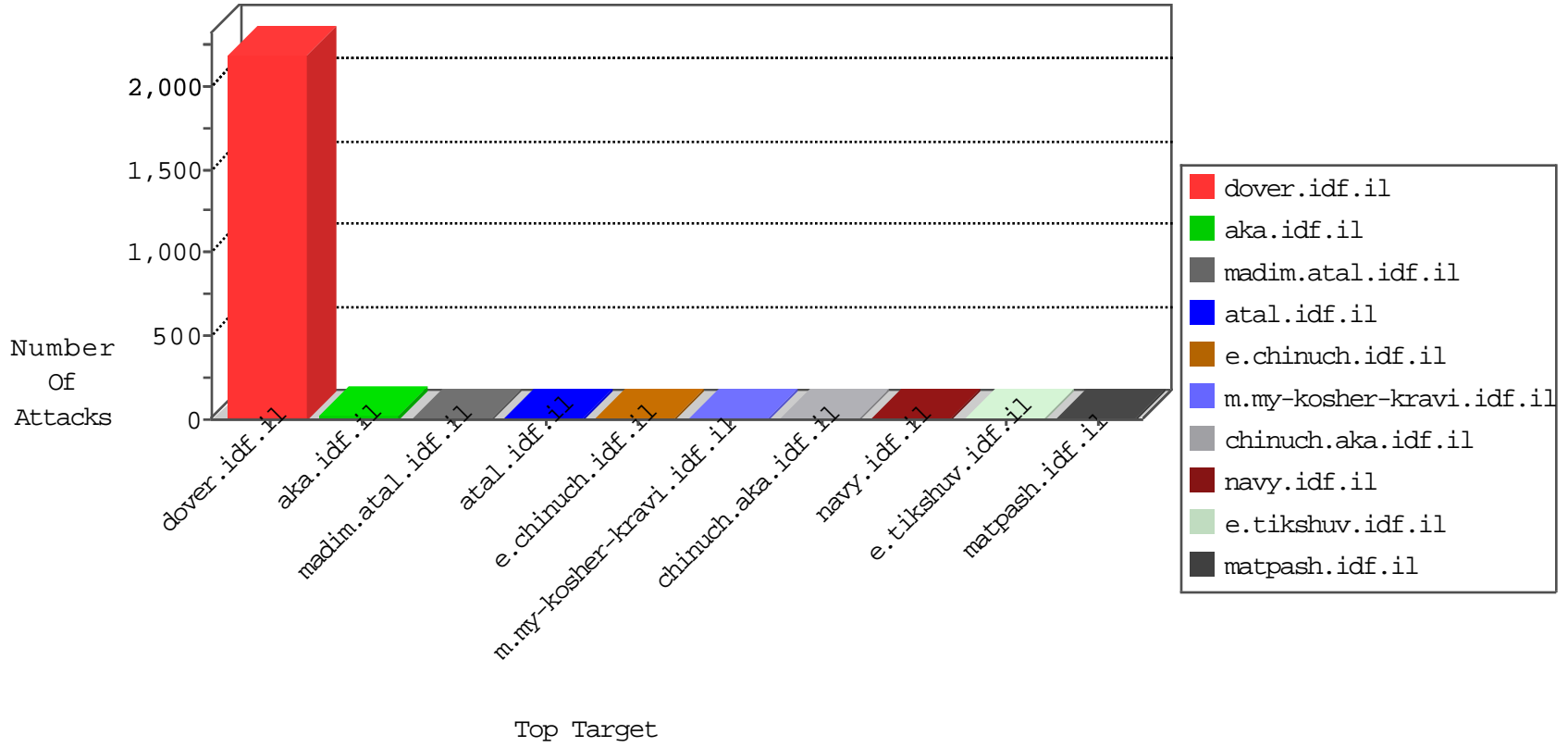


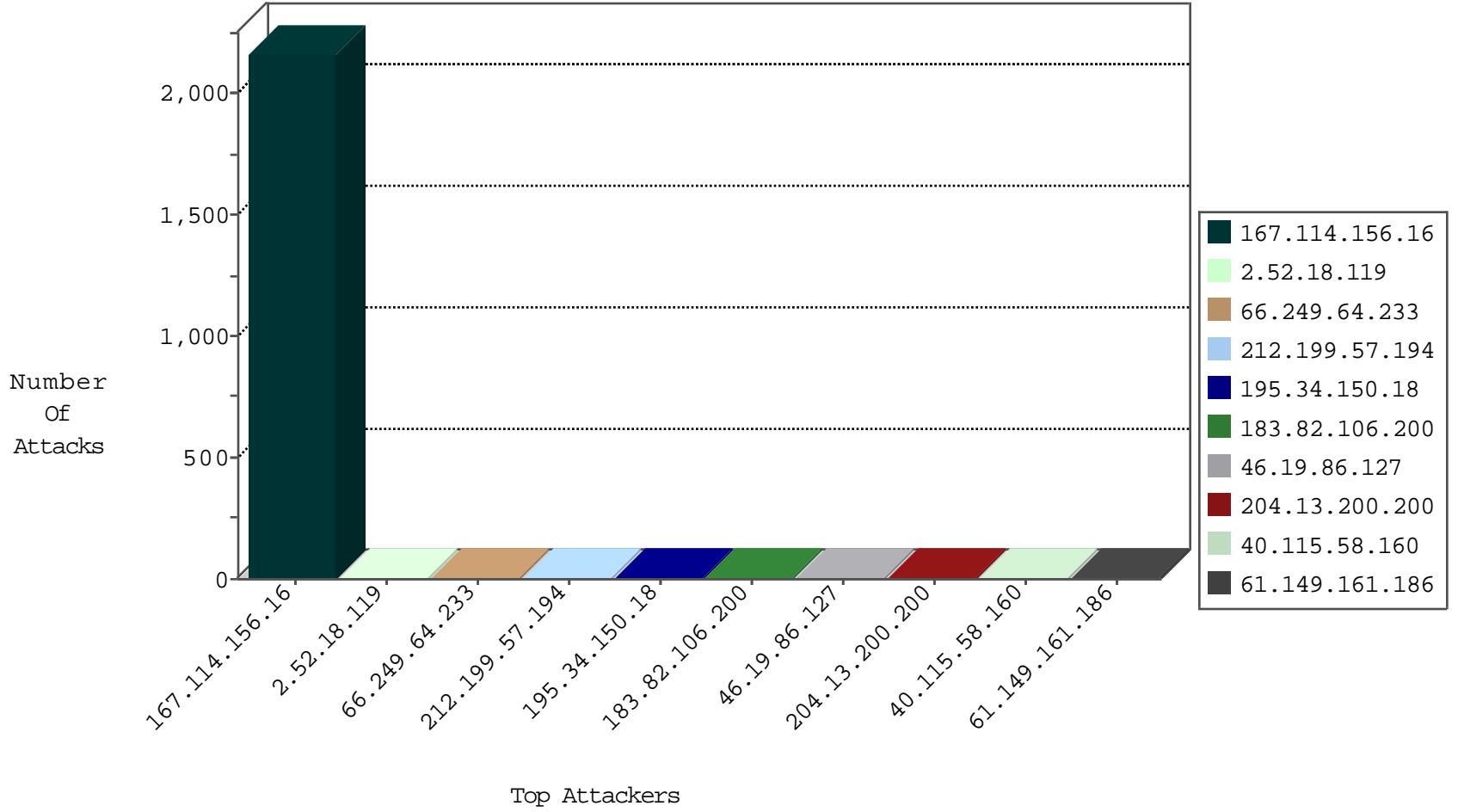
# IDF Under Attack Daily Report



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	3538
71.6.216.53	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1

01-05-2016-05:04:00 to 01-05-2016-06:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
182.50.130.136	Singapore	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1

## 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
212.199.57.194	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
61.149.161.186	147.237.77.233	China	atal.idf.il	GPL SCAN nmap TCP	2
185.130.5.224	147.237.77.216		dover.idf.il	ET SCAN NMAP -sS window 1024	1
183.82.106.200	147.237.8.46	India	e.chinuch.idf.i	ET SCAN NMAP -sS window 2048	1
40.115.58.160	147.237.76.34	United States	yochalan.idf.il	ET SCAN NMAP -sS window 1024	1
183.82.106.200	147.237.8.46	India	e.chinuch.idf.i	ET SCAN NMAP -sS window 3072	1
183.82.106.200	147.237.8.46	India	e.chinuch.idf.i	ET SCAN NMAP -f -sS	1
40.115.58.160	147.237.76.38	United States	e.e.meitav.idf.	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.8.50	United States	e.tikshuv.idf.i	ET SCAN NMAP -sS window 1024	1

01-05-2016-05:04:00 to 01-05-2016-06:04:00

Top Attackers In FW

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

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.18.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	6
212.199.57.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.127	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	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
213.57.61.84	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
109.253.146.86	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1395-en/dover.aspx	Block	1
66.249.64.238	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
185.120.126.77		147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.179.57.105	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
66.249.64.229	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1234-he/atal.aspx	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
109.253.146.86	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 109.253.146.86	None	1
68.180.229.31	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
66.249.64.243	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
199.16.156.125	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 199.16.156.125	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.111	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/gyus/general.aspx	Block	1
141.212.122.112	United States	147.237.77.176	matpash.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
66.249.69.20	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/gyus/forum/asp/showforum.asp	Block	1
37.26.149.153	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
199.16.156.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/size220x0/17882.jpg	Block	1
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	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/gyus/general.aspx	Block	1
212.199.57.194	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1246-he/atal.aspx	Block	1
173.252.89.56	United States	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 173.252.89.56 (sigalgs DoS Attack)	None	1
74.82.47.2	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.75.107	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/yohalan/main/main.asp	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/	Block	1
66.249.64.234	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1486-he/atal.aspx	Block	1
173.252.90.90	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.176.185.164	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
66.249.78.52	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
54.152.151.136	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/60042.pdf	Block	1