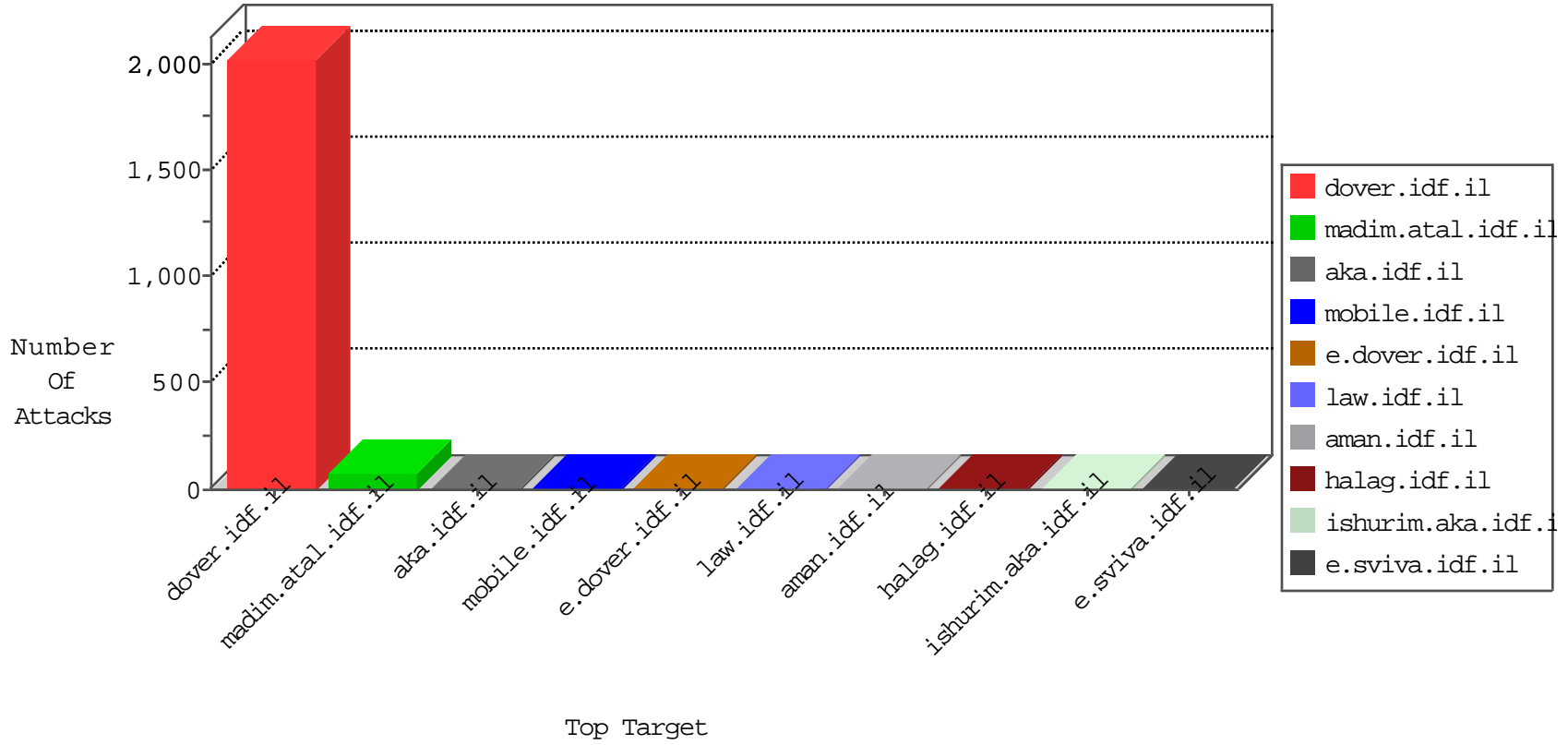


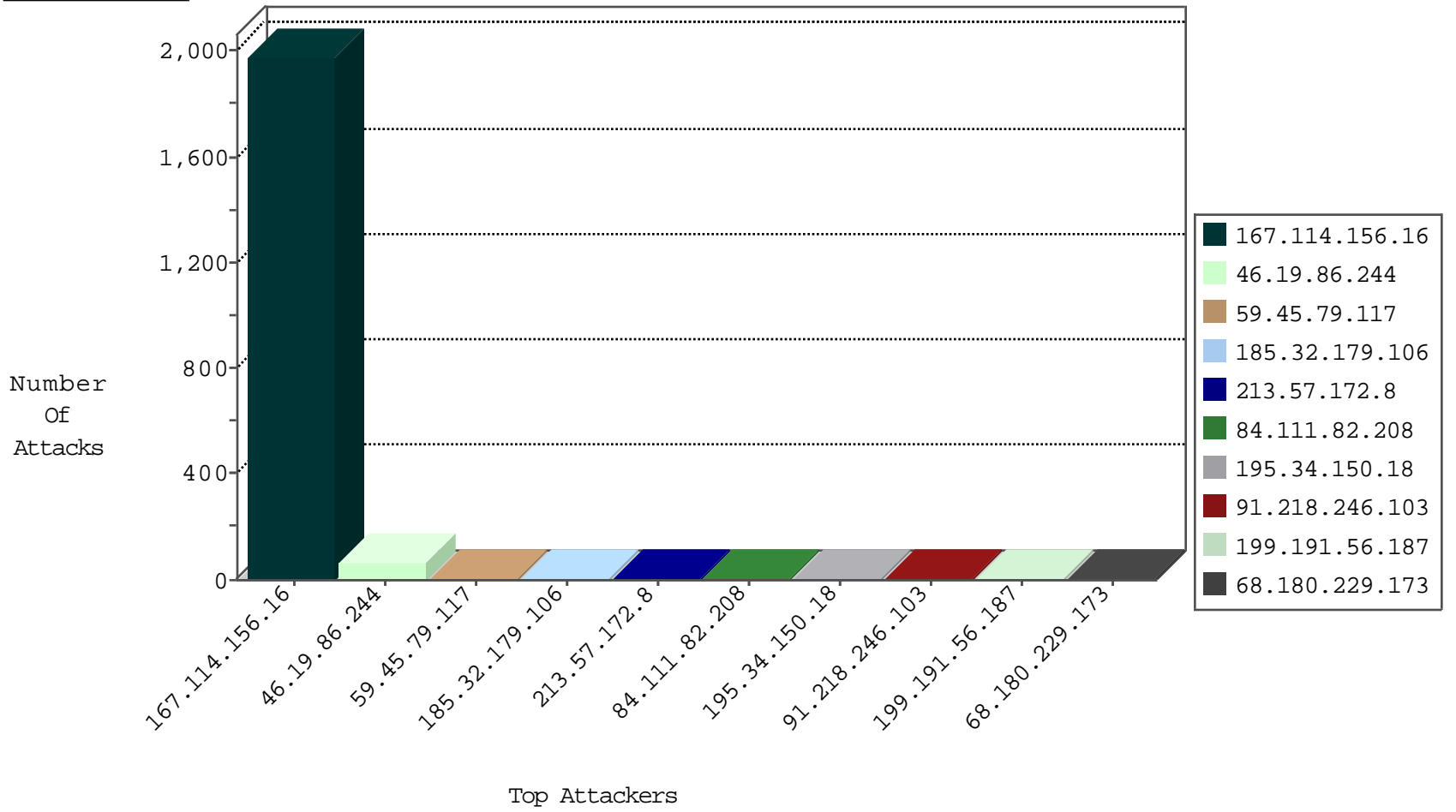
IDF Under Attack Daily Report



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	3084
193.192.59.216	Germany	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1

01-05-2016-02:04:01 to 01-05-2016-03:04:01

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
91.218.246.103	147.237.76.200	Russian Federation	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
201.172.138.194	147.237.77.234	Mexico	halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
61.244.49.137	147.237.76.39	Hong Kong	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
199.191.56.187	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 2048	1
59.45.79.117	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
199.191.56.187	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -f -sS	1
59.45.79.117	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.224	147.237.77.234		halag.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
185.93.204.74	147.237.8.28		e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	147.237.77.74	Canada	law.idf.il	ET SCAN NMAP -sS window 3072	1
98.119.105.221	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 3072	1
91.218.246.103	147.237.77.19	Russian Federation	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
91.218.246.103	147.237.76.196	Russian Federation	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
201.172.138.194	147.237.77.74	Mexico	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
199.191.56.187	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.224	147.237.72.167		ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
109.228.33.167	147.237.8.46	United Kingdom	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
104.128.144.131	147.237.76.34	Canada	yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
98.119.105.221	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 1024	1

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
46.19.86.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	67
213.57.172.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
84.111.82.208	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	6
185.32.179.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
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	2
68.180.229.173	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
150.70.173.50	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	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
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
193.90.12.87	Norway	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
149.78.165.83	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.248	United States	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/sachar/faq/outerfaq.asp	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.64.243	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/view_img.asp	Block	1
150.70.97.85	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
84.228.64.72	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
2.54.166.115	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
171.25.193.77	Sweden	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	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
207.46.13.75	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/ylcebowm67a	Block	1
150.70.97.85	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
94.159.203.94	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
40.77.167.26	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/armored/hativa7/kkkkkkk=8f27f2e3kkkkkk_8f27f2e3	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1927-he/cogat.aspx	Block	1
150.70.173.50	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
95.175.97.229	Finland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
141.212.122.112	United States	147.237.76.86	navy.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
77.247.181.165	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1