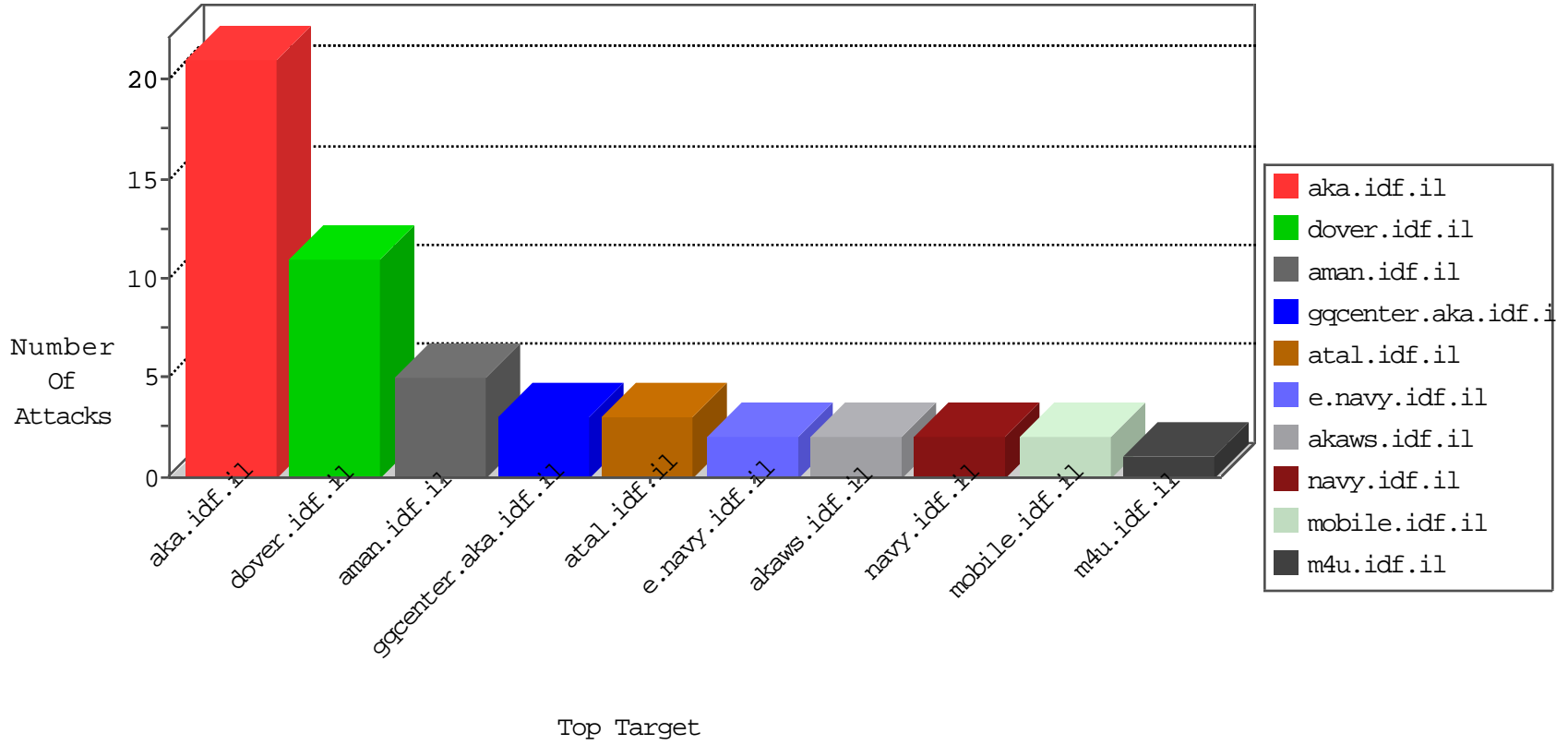


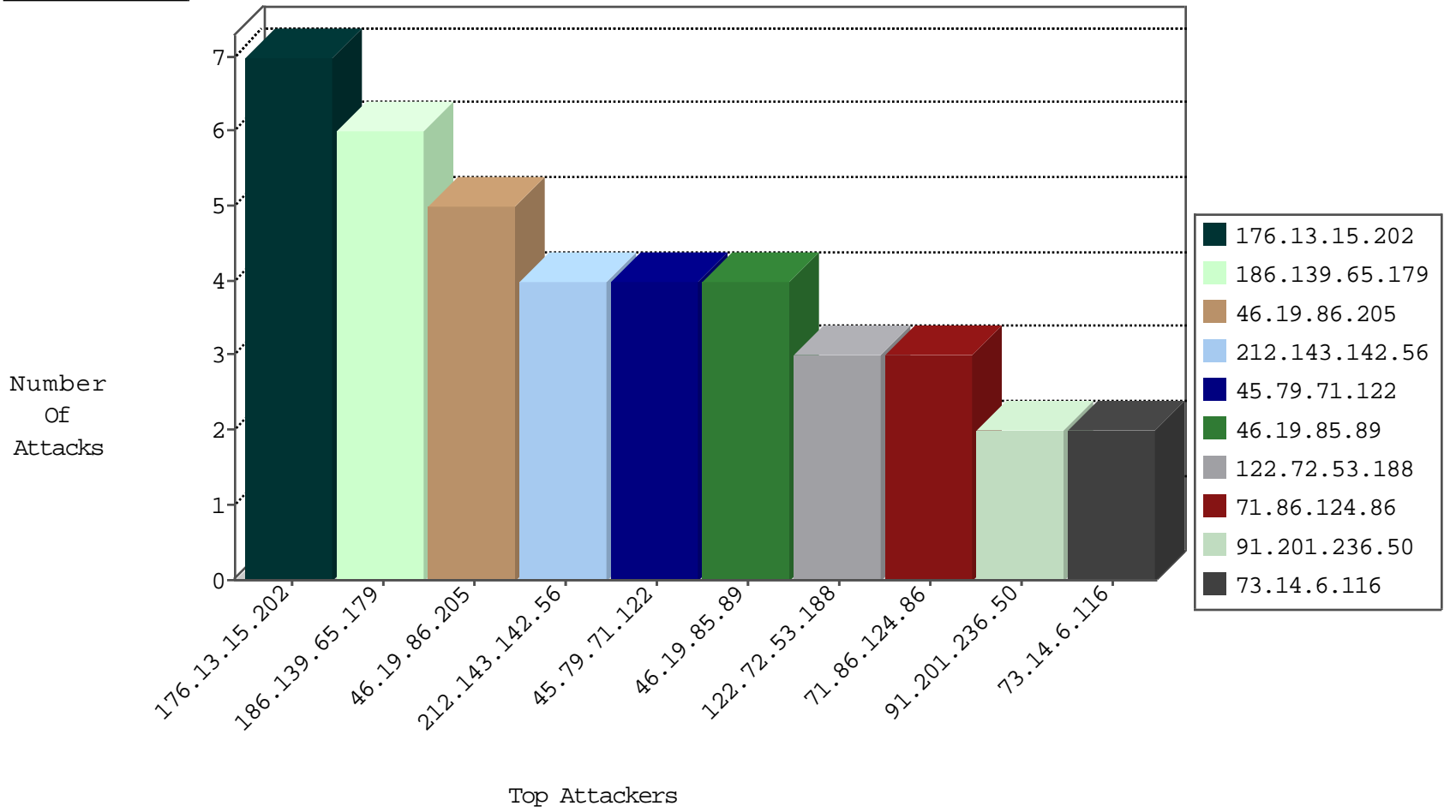
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
217.23.9.123	Netherlands	147.237.76.201	e.atal.idf.il	Black List	drop	1
64.137.196.36	Canada	147.237.76.86	navy.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.197	e.himush.idf.il	Black List	drop	1
217.23.9.123	Netherlands	147.237.76.176	test.ncore.idf.il	Black List	drop	1

09-04-2016-04:04:04 to 09-04-2016-05:04:04

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
73.14.6.116	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	2
71.86.124.86	147.237.76.148	United States	ggcenter.aka.idf.i	ET SCAN NMAP -f -sS	1
5.206.239.211	147.237.76.30		himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
186.119.97.102	147.237.0.35	Colombia	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
122.72.53.188	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
122.72.53.188	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.50	147.237.77.121	Ukraine	e.navy.idf.il	ET SCAN NMAP -sS window 4096	1
71.86.124.86	147.237.76.148	United States	ggcenter.aka.idf.i	ET SCAN NMAP -sS window 2048	1
45.79.71.122	147.237.72.166	United States	aka.idf.il	WEB-MISC Chunked-Encoding transfer attempt	1
163.172.169.150	147.237.72.217	United Kingdom	e.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
122.72.53.188	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
104.237.234.109	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.77.121	Ukraine	e.navy.idf.il	ET SCAN NMAP -sS window 3072	1
71.86.124.86	147.237.76.148	United States	ggcenter.aka.idf.i	ET SCAN NMAP -sS window 4096	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.86.205	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	5
176.13.15.202	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.89	Israel	147.237.72.156	aman.idf.il	drop	SAM rule	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
176.13.15.202	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
187.153.123.227	Mexico	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
186.139.65.179	Argentina	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	6
99.228.213.56	Canada	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	2
66.249.64.193	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/1074-he/aspix.	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
45.79.71.122	United States	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 3	Block	1
66.249.64.236	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/.well-known/apple-app-site-association	Block	1
94.199.151.22	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
45.79.71.122	United States	147.237.72.166	aka.idf.il	Malformed URL	Block	1
66.249.69.149	Israel	147.237.76.200	eitan.aka.idf.	Unauthorized URL Access to www.eitan.aka.idf.il/templates/general/eitan.aspx	Block	1
99.172.76.186	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-en/dover.aspx	Block	1
45.79.71.122	United States	147.237.72.166	aka.idf.il	Unknown HTTP Request Method 1 in URL	Block	1
66.249.76.30	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/apple-app-site-association	Block	1
66.249.64.73	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
77.139.146.174	France	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1