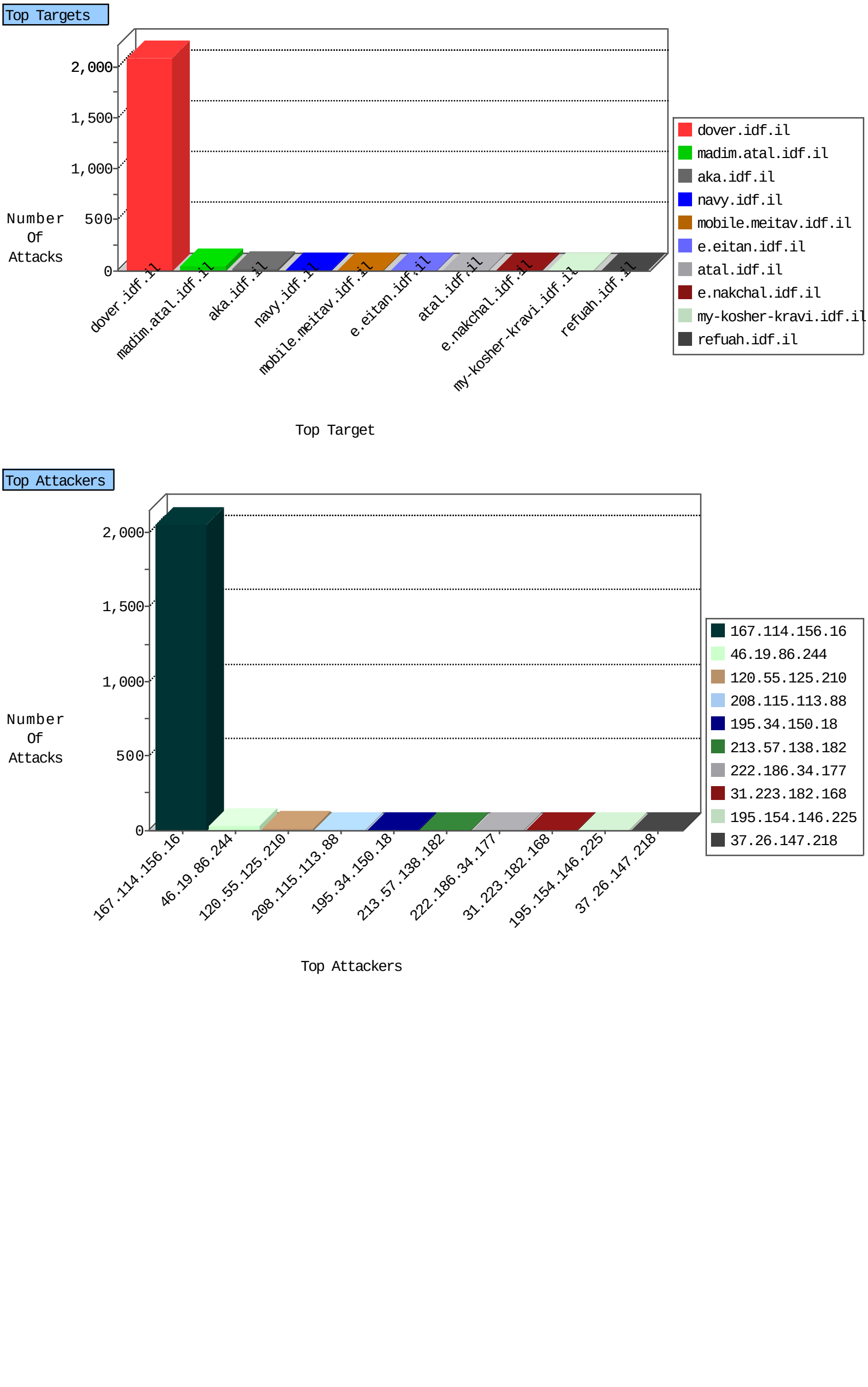
01-05-2016-03:04:04 to 01-05-2016-04:04:04

IDF Under Attack Daily Report



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

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	3122
204.42.253.130	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	2
71.6.216.46	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
146.185.239.100	Russian Federation	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	drop	1

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

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.8.236.222	Czech Republic	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1

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

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
120.55.125.210	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	1
222.186.34.177	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
120.55.125.210	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
222.186.34.177	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
120.55.125.210	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
195.154.154.131	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
93.174.93.203	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.224	147.237.77.216		dover.idf.il	ET SCAN NMAP -sS window 1024	1
91.218.246.103	147.237.76.177	Russian Federation	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
120.55.125.210	147.237.77.243	China	mobile.idf.il	ET SCAN Potential SSH Scan	1
40.115.58.160	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
120.55.125.210	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
120.55.125.210	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
120.55.125.210	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
222.186.34.177	147.237.77.216	China	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
120.55.125.210	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
222.186.34.177	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
120.55.125.210	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
104.128.144.131	147.237.76.197	Canada	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
91.218.246.103	147.237.76.199	Russian Federation	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
168.62.238.153	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
61.149.161.186	147.237.8.45	China	e.eitan.idf.il	GPL SCAN nmap TCP	1
120.55.125.210	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
120.55.125.210	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
120.55.125.210	147.237.77.205	China	prisha.idf.il	ET SCAN Potential SSH Scan	1

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

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	36
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	4
31.223.182.168	Palestinian Territory, Occupied	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	3
109.253.201.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.147.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.57.138.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
23.254.138.210	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 23.254.138.210	Block	2
79.178.71.57	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.178.172.151	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	2
141.212.122.112	United States	147.237.77.74	law.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
85.10.210.199	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.64.235	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
213.57.138.182	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
195.154.146.225	France	147.237.77.216	dover.idf.il	Illegal HTTP Version HTTP/	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/yoman.asp	Block	1
66.249.64.180	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/eitan/listpage/	Block	1
141.212.122.112	United States	147.237.77.234	halag.idf.il	Multiple Malformed URL from 141.212.122.112	Block	1
99.238.58.173	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/volunteer	Block	1
66.249.64.238	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19020-he/dover.aspx×¦×™×œ×•×?:	Block	1
195.154.146.225	France	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
115.230.126.48	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/ckfinder	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-ar/dover.aspx	Block	1
66.249.64.185	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
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	1
149.202.47.181	Germany	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	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/atal1/izkor/view_imgtop.asp	Block	1
195.154.146.225	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-trackback.php	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-12715-he/dover.aspx	Block	1
212.76.102.252	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
157.55.39.75	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18287-he/dover.aspx	Block	1
23.254.138.210	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.66.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/jquery.nyromodal-1.6.2.js	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
46.166.137.193	Netherlands	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	147.237.0.19	madim.atal.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
184.105.247.195	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
31.210.187.78	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.253.147.131	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.66.191	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/expand.js	Block	1
61.135.190.197	China	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1