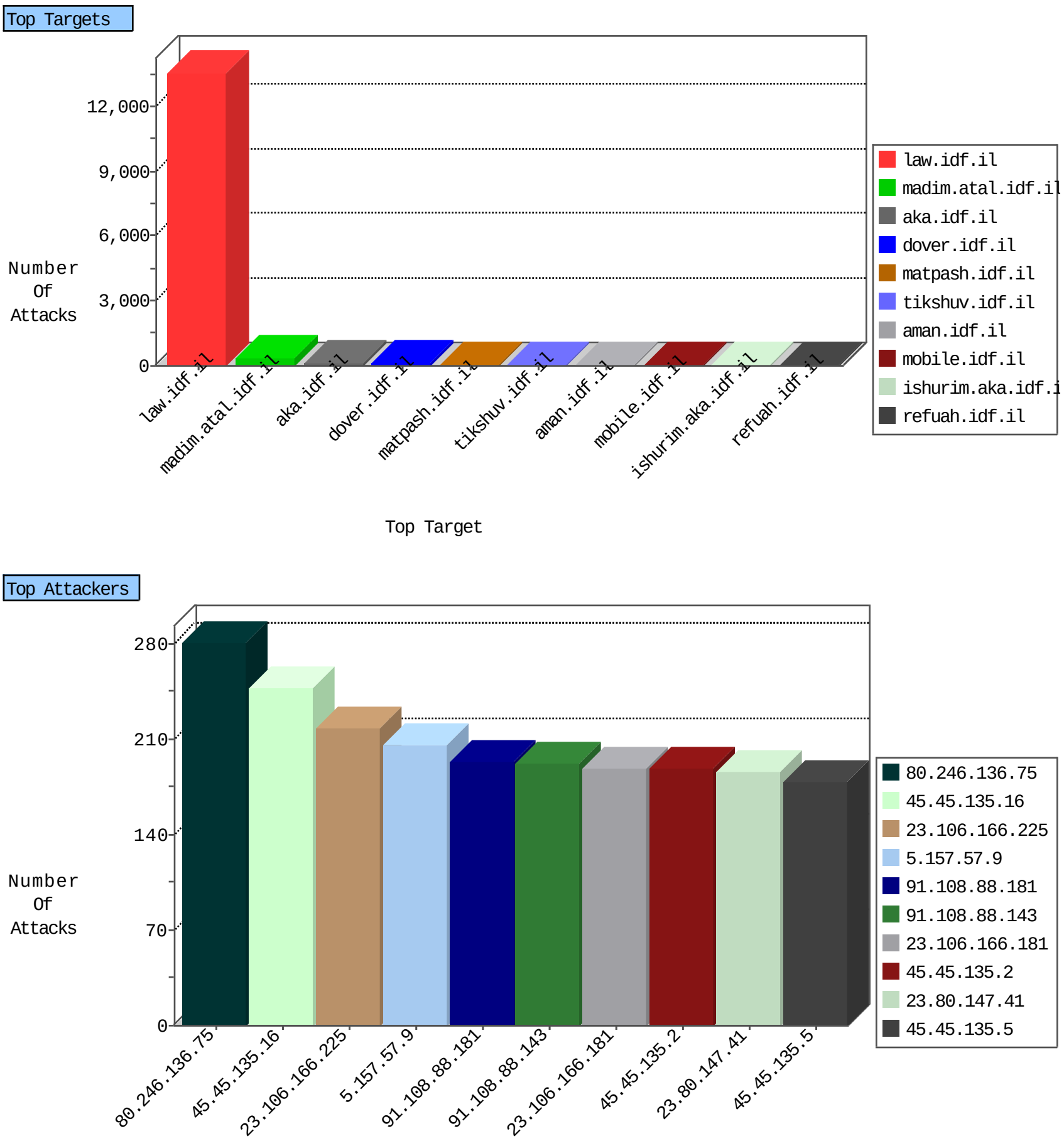
02-16-2016-07:04:03 to 02-16-2016-08:04:03

IDF Under Attack
Daily Report



02-16-2016-07:04:03 to 02-16-2016-08:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.182.4.147	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
202.101.62.39	China	147.237.76.201	e.atal.idf.il	JLM_Under_Attack_Con_Http	drop	2
115.239.228.10	China	147.237.0.16	my-kosher-kravi.idf.il	Frk_Under_Attack_Con_Http	drop	2
115.239.228.10	China	147.237.0.16	my-kosher-kravi.idf.il	Frk_Purple_Con_Limit_Http	drop	1
78.179.196.163	Turkey	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1

02-16-2016-07:04:03 to 02-16-2016-08:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-16-2016-07:04:03 to 02-16-2016-08:04:03

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	3
80.83.135.131	147.237.77.74	Georgia	law.idf.il	ET SCAN Potential SSH Scan	1
37.193.70.30	147.237.77.243	Russian Federation	mobile.idf.il	ET SCAN Potential SSH Scan	1
37.193.70.30	147.237.77.170	Russian Federation	maarachot.idf.il	ET SCAN Potential SSH Scan	1
193.105.134.220	147.237.0.19	Sweden	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
115.29.197.215	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -sS window 1024	1
80.83.135.131	147.237.77.243	Georgia	mobile.idf.il	ET SCAN Potential SSH Scan	1
80.83.135.131	147.237.77.227	Georgia	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
80.83.135.131	147.237.77.178	Georgia	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
80.83.135.131	147.237.77.170	Georgia	maarachot.idf.il	ET SCAN Potential SSH Scan	1
80.83.135.131	147.237.77.19	Georgia	law-forum.idf.il	ET SCAN Potential SSH Scan	1
37.193.70.30	147.237.77.212	Russian Federation	e.dover.idf.il	ET SCAN Potential SSH Scan	1
193.105.134.220	147.237.77.74	Sweden	law.idf.il	ET SCAN NMAP -sS window 1024	1
37.193.70.30	147.237.8.50	Russian Federation	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
149.78.154.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
88.249.106.23	147.237.72.156	Turkey	aman.idf.il	ET SCAN NMAP -sS window 1024	1
80.83.135.131	147.237.77.234	Georgia	halag.idf.il	ET SCAN Potential SSH Scan	1
80.83.135.131	147.237.77.212	Georgia	e.dover.idf.il	ET SCAN Potential SSH Scan	1
80.83.135.131	147.237.77.176	Georgia	matpash.idf.il	ET SCAN Potential SSH Scan	1

02-16-2016-07:04:03 to 02-16-2016-08:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
45.45.135.16		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	248
23.106.166.225	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	218
5.157.57.9	Sweden	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	206
91.108.88.181	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	194
91.108.88.143	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	192
45.45.135.2		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	189
23.106.166.181	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	189
23.80.147.41	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	186
45.45.135.5		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	179
45.45.135.18		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	168
91.108.88.94	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	154
23.80.147.142	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	149
23.106.161.77	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	149
84.200.45.159	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	147
91.108.88.121	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	147
91.108.88.226	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	146
104.251.91.180		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	145
23.106.239.249	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	142
91.108.88.112	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	141
84.200.45.27	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	139
23.106.161.125	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	135
91.108.88.83	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	122
23.81.205.200	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	112
23.106.211.43	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	110
23.80.148.22	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	107
45.45.135.9		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	105
5.157.57.15	Sweden	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	102
5.157.56.145	Sweden	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	101
23.106.85.203	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	100
23.81.69.119	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	99
23.106.239.108	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	99
91.108.88.144	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	99
5.157.57.61	Sweden	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	98
84.200.45.38	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	98
31.14.33.53	Romania	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	98
5.231.27.139	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	98
23.106.164.164	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	98
84.200.45.12	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	98
91.108.88.146	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	97
91.108.88.3	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	97
91.108.88.120	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	97
91.108.88.222	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	97
23.106.166.182	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	96
45.45.135.15		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	96
91.108.88.73	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	96
91.108.88.156	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	95
91.108.88.147	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	95
91.108.88.150	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	95
84.200.45.13	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	94
45.45.135.8		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	93

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.136.75	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 80.246.136.75	Block	160
80.246.136.75	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
185.32.179.97	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	35
2.54.136.2	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	19
2.52.4.92	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 2.52.4.92	Block	13
80.246.136.75	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 80.246.136.75	Block	13
85.250.25.89	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 85.250.25.89	Block	9
85.250.25.89	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	6
37.26.149.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
46.19.86.122	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	3
109.253.206.42	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
186.202.150.213	Brazil	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 186.202.150.213	Block	3
109.253.145.250	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
85.250.25.89	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/ajax/updatestatus.php	Block	2
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
186.202.150.213	Brazil	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
109.65.16.212	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
178.163.0.215	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation FileName in www.law.idf.il/templates/getfile/getfile.aspx	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	1
207.46.13.85	United States	147.237.77.233	atal.idf.il	Abnormally Long Request URL	Block	1
109.66.98.21	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ https:/twitter.com/	Block	1
80.246.136.75	Israel	147.237.0.19	madim.atal.idf.i	Too Many 404: Response Code per Session	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
178.163.0.215	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation InfoCenterItem in www.law.idf.il/templates/getfile/getfile.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/1966-he/cogat.aspx	Block	1
5.29.248.213	Israel	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	1
77.87.117.6	Russian Federation	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	1
5.29.248.213	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/xmlrpc.php	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
2.52.4.92	Israel	147.237.0.34	tikshuv.idf.il	Too Many 404: Response Code per Session	Block	1
87.69.31.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	1
80.246.133.223	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
160.62.4.100	Switzerland	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/moreinfo/tichnun.yosh@gmail.com	Block	1
80.246.137.3	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1