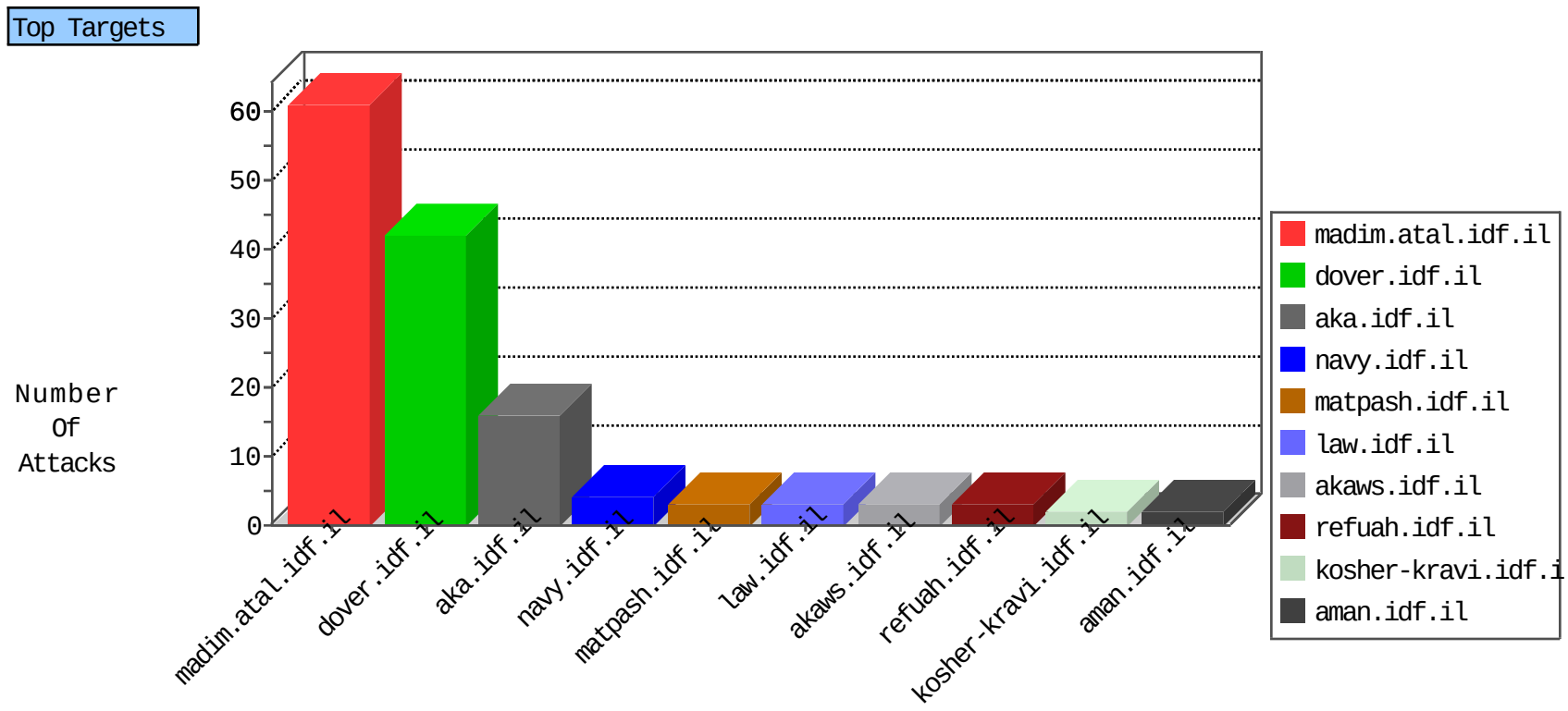
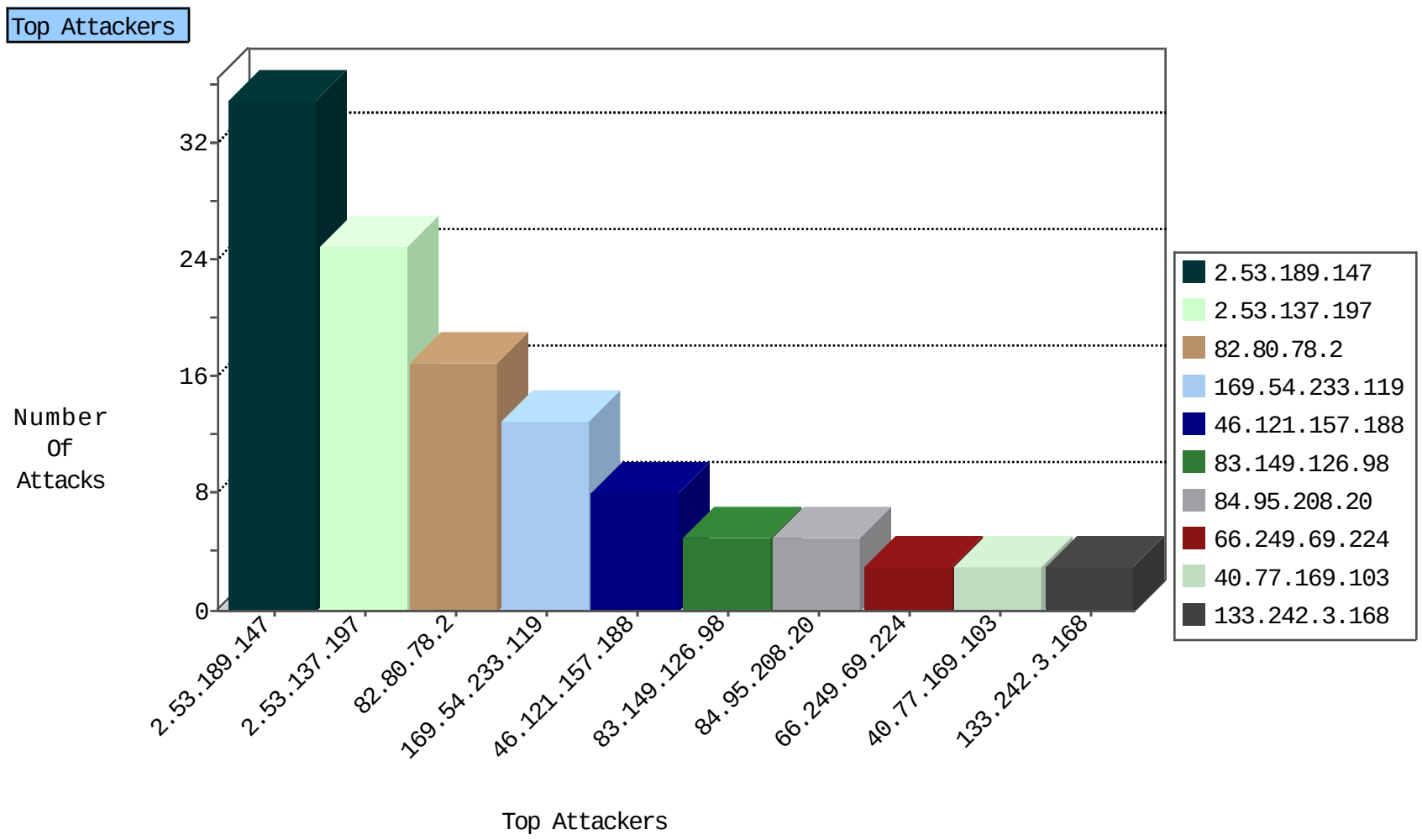
08-25-2016-01:07:51 to 08-25-2016-02:07:51

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-25-2016-01:07:51 to 08-25-2016-02:07:51

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.78.2	Israel	147.237.77.216	dover.idf.il	Black List	drop	17
109.64.116.225	Israel	147.237.77.74	law.idf.il	Black List	drop	2
120.132.50.135	China	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2

08-25-2016-01:07:51 to 08-25-2016-02:07:51

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
83.149.126.98	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	5
46.165.197.141	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

08-25-2016-01:07:51 to 08-25-2016-02:07:51

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
77.125.49.59	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	2
133.242.3.168	147.237.77.178	Japan	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
201.238.202.219	147.237.76.177	Chile	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.49.190	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	1
169.54.233.119	147.237.77.235	United States	sviva.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.72.166	Netherlands	aka.idf.il	ET SCAN NMAP -sS window 1024	1
169.54.233.119	147.237.77.216	United States	dover.idf.il	ET SCAN Potential SSH Scan	1
91.125.184.101	147.237.77.74	United Kingdom	law.idf.il	Tehila - Perl LWP with fake user agent	1
169.54.233.119	147.237.76.201	United States	e.atal.idf.il	ET SCAN Potential SSH Scan	1
46.227.67.172	147.237.72.167	Sweden	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
169.54.233.119	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
46.172.71.251	147.237.8.46	Ukraine	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
169.54.233.119	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
169.54.233.119	147.237.8.14	United States	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
169.54.233.119	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
201.238.202.219	147.237.76.201	Chile	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
133.242.3.168	147.237.72.166	Japan	aka.idf.il	ET SCAN NMAP -sS window 1024	1
185.56.80.144	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.72.217	Netherlands	e.idf.il	ET SCAN NMAP -sS window 1024	1
169.54.233.119	147.237.77.234	United States	halag.idf.il	ET SCAN Potential SSH Scan	1
93.115.96.31	147.237.72.217	France	e.idf.il	ET SCAN NMAP -sS window 3072	1
169.54.233.119	147.237.77.179	United States	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
169.54.233.119	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
46.227.67.172	147.237.72.166	Sweden	aka.idf.il	ET SCAN NMAP -sS window 1024	1
169.54.233.119	147.237.76.42	United States	refuah.idf.il	ET SCAN Potential SSH Scan	1
46.172.71.251	147.237.8.27	Ukraine	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
169.54.233.119	147.237.72.14	United States	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
169.54.233.119	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1

08-25-2016-01:07:51 to 08-25-2016-02:07:51

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
46.121.157.188	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
141.212.122.26	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
141.212.122.27	United States	147.237.0.35	akaws.idf.il	drop		drop	1
89.248.174.4	Netherlands	147.237.0.33	idf.il	drop		drop	1
141.212.122.27	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
109.253.217.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.28	United States	147.237.0.35	akaws.idf.il	drop		drop	1
133.242.3.168	Japan	147.237.0.35	akaws.idf.il	drop		drop	1

08-25-2016-01:07:51 to 08-25-2016-02:07:51

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.189.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
2.53.137.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
2.53.137.197	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	6
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	3
40.77.169.99	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
40.77.169.103	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
176.40.165.162	Turkey	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.i	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
40.77.169.97	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
85.250.40.229	Israel	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
66.249.69.228	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
180.76.15.161	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to www.kosher-kravi.idf.il/default.aspx	Block	1
85.250.40.229	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-login.php	Block	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/yohalan/main/main	Block	1
207.46.13.34	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
40.77.169.103	United States	147.237.77.176	matpash.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
90.209.20.17	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/	Block	1
66.249.93.72	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
5.22.132.119	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/994-7237-he/atal.aspx	Block	1
207.46.13.140	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	PHP Attempt	Block	1
157.55.39.37	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
77.138.156.18	France	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/giyus	Block	1
37.46.34.83	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 37.46.34.83	Block	1
213.151.35.216	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/giyus/	Block	1
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1

08-25-2016-01:07:51 to 08-25-2016-02:07:51