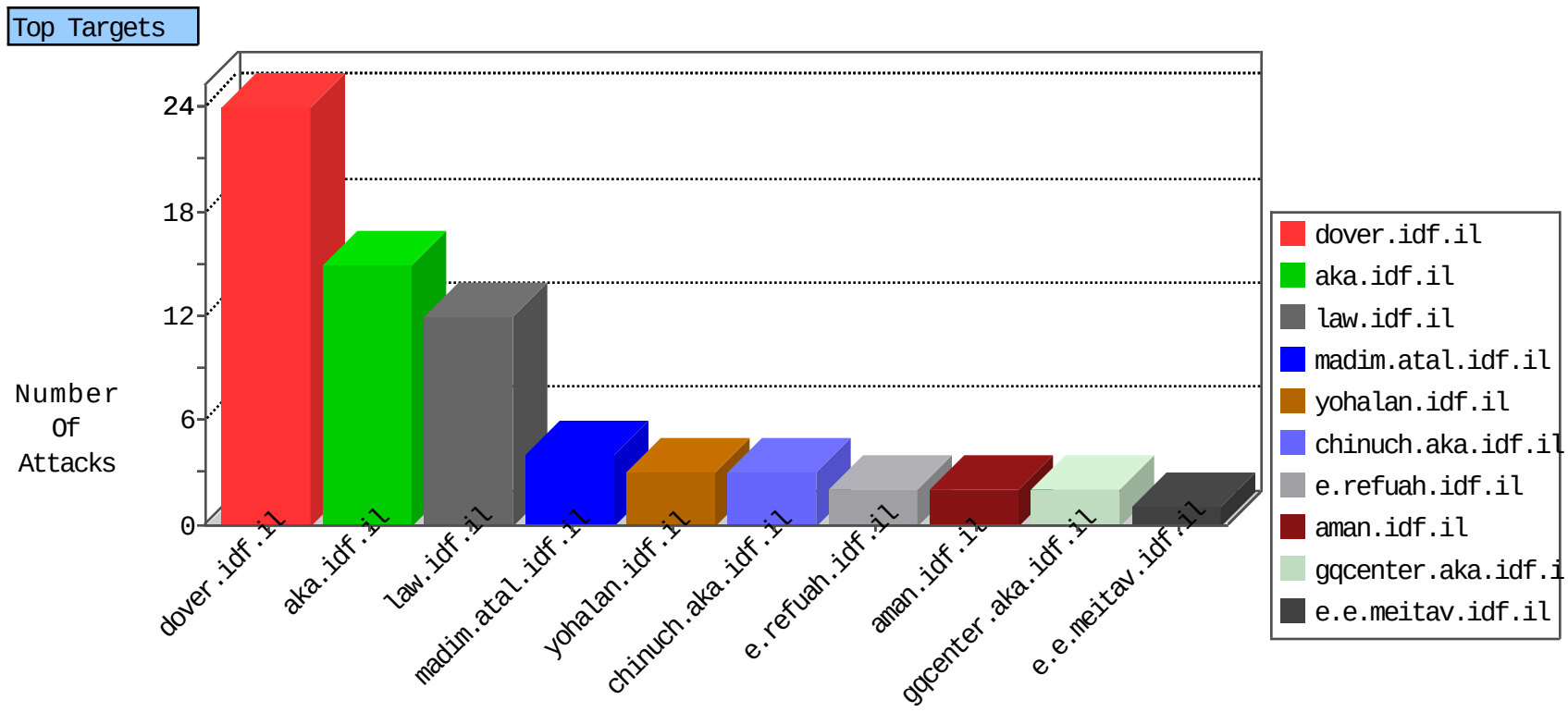
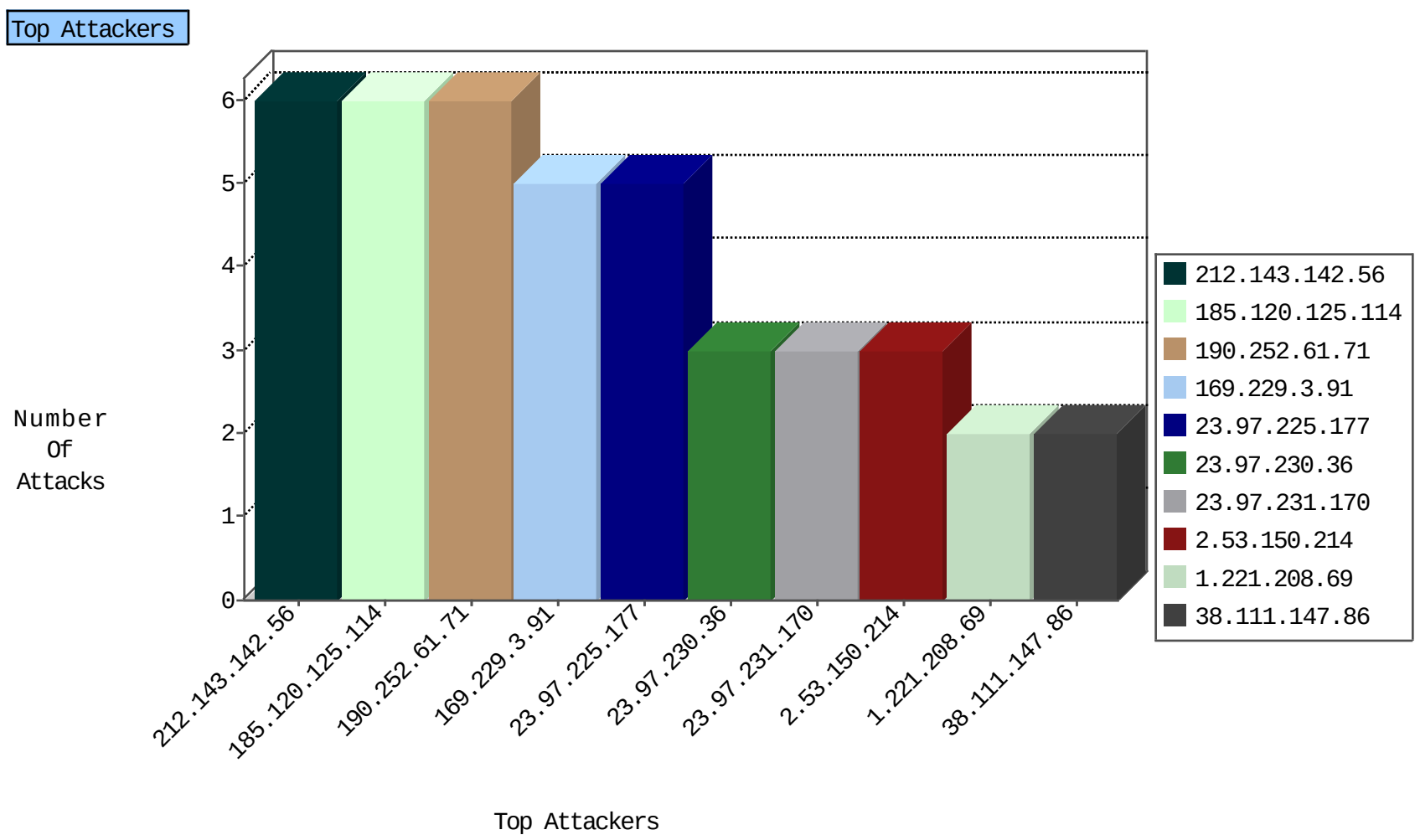
08-18-2016-02:04:06 to 08-18-2016-03:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-18-2016-02:04:06 to 08-18-2016-03:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
1.221.208.69	Korea, Republic of	147.237.76.147	chinuch.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
82.80.78.2	Israel	147.237.77.216	dover.idf.il	Black List	drop	1
89.248.171.2	Netherlands	147.237.76.44	e.refuah.idf.il	Black List	drop	1
109.65.4.192	Israel	147.237.76.201	e.atal.idf.il	Black List	drop	1

08-18-2016-02:04:06 to 08-18-2016-03:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.212.73.211	Netherlands	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
23.97.230.36	Netherlands	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
23.97.231.170	Netherlands	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
23.97.225.177	Netherlands	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

08-18-2016-02:04:06 to 08-18-2016-03:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
23.97.225.177	147.237.77.74	Netherlands	law.idf.il	SQL Injection - Select From	4
23.97.231.170	147.237.77.74	Netherlands	law.idf.il	SQL Injection - Select From	2
23.97.230.36	147.237.77.74	Netherlands	law.idf.il	SQL Injection - Select From	2
87.121.13.85	147.237.76.31	Bulgaria	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
176.98.64.215	147.237.72.166	Ukraine	aka.idf.il	Xenu Link Sleuth User Agent	1
163.172.59.55	147.237.0.15	United Kingdom	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
52.33.91.214	147.237.77.74	United States	law.idf.il	Xenu Link Sleuth User Agent	1
5.255.90.133	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.59.55	147.237.76.147	United Kingdom	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1

08-18-2016-02:04:06 to 08-18-2016-03:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
185.120.125.114	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
190.252.61.71	Colombia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
38.111.147.86	United States	147.237.77.216	dover.idf.il	drop		drop	2
169.229.3.91	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
141.212.122.134	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
141.212.122.135	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
141.212.122.154	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
141.212.122.155	United States	147.237.76.34	yohalan.idf.il	drop		drop	1

08-18-2016-02:04:06 to 08-18-2016-03:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.150.214	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	3
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/apple-app-site-association	Block	1
5.29.217.24	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 5.29.217.24	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.i	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.146	Block	1
192.118.10.10	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.118.10.10	Block	1
68.180.228.185	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1399-en/dover.aspx	Block	1
62.219.142.66	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/maslul.aspx?catid=60643&docid=72470	Block	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Multiple Untraceable SSL Sessions from 169.229.3.91 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/894-he/chinuch.aspx	Block	1
207.46.13.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
68.180.228.185	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1806-he/dover.aspx	Block	1
65.55.210.78	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	1
213.57.62.94	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il./	Block	1
73.138.60.38	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-21587-he/idfgdover.aspx	Block	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.78.190	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1392-en/cogat.asp	Block	1
157.55.39.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/kamlar/klali/default.asp	None	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
174.22.175.14	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/sites/home/default.asp	Block	1

08-18-2016-02:04:06 to 08-18-2016-03:04:06