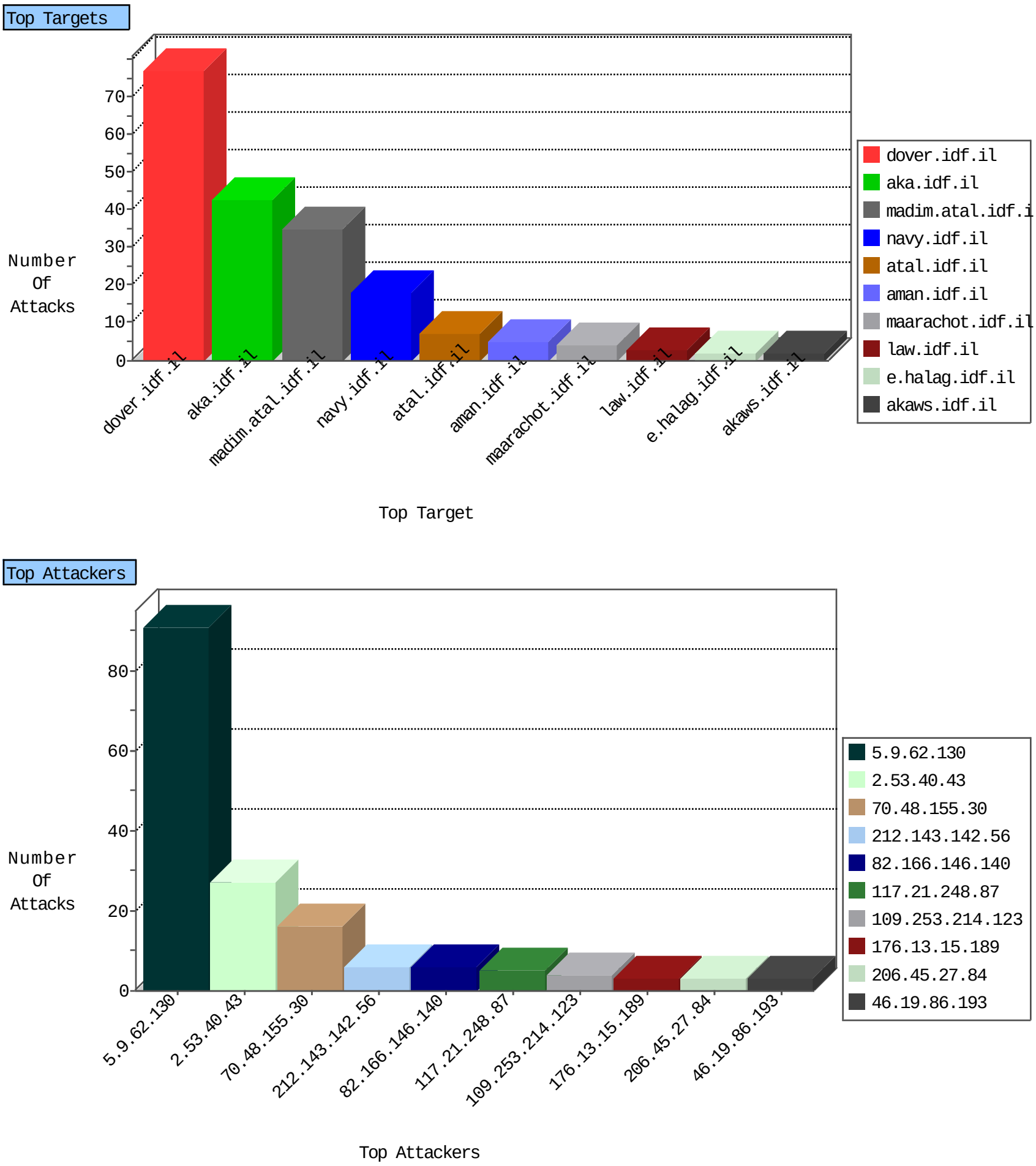
08-18-2016-01:08:21 to 08-18-2016-02:08:21

IDF Under Attack
Daily Report



08-18-2016-01:08:21 to 08-18-2016-02:08:21

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
104.148.55.162	United States	147.237.76.176	test.ncore.idf.il	Black List	drop	1

08-18-2016-01:08:21 to 08-18-2016-02:08:21

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.9.62.130	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	61
5.9.62.130	Germany	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	16
5.9.62.130	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	10
5.9.62.130	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	2
5.9.62.130	Germany	147.237.77.170	maarachot.idf.il	C1000074: HTTP: majestic bot	Permit	2
149.202.54.34	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

08-18-2016-01:08:21 to 08-18-2016-02:08:21

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
82.166.146.140	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	6
94.102.48.195	147.237.77.74	Netherlands	law.idf.il	ET SCAN NMAP -sS window 1024	1
87.236.194.161	147.237.72.167	Czech Republic	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
220.231.195.122	147.237.76.202	China	e.halag.idf.il	ET SCAN NMAP -sS window 3072	1
54.153.99.128	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
190.255.211.108	147.237.0.19	Colombia	madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
50.245.143.138	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 3072	1
123.206.85.139	147.237.0.19	China	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
117.21.248.87	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
117.21.248.87	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
113.175.162.14	147.237.8.27	Vietnam	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.91.29	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
87.236.194.161	147.237.0.16	Czech Republic	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
72.252.249.125	147.237.72.166	Jamaica	aka.idf.il	ET SCAN NMAP -sS window 1024	1
220.231.195.122	147.237.76.202	China	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
50.245.143.138	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 4096	1
123.206.85.139	147.237.0.35	China	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
5.255.90.133	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
117.21.248.87	147.237.77.243	China	mobile.idf.il	ET SCAN Potential SSH Scan	1
117.21.248.87	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
117.21.248.87	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1

08-18-2016-01:08:21 to 08-18-2016-02:08:21

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
70.48.155.30	Canada	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.253.214.123	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
188.169.80.22	Georgia	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
109.66.190.114	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
176.13.6.223	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.154	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
176.13.232.209	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.155	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
82.166.235.69	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.0.35	akaws.idf.il	drop		drop	1

08-18-2016-01:08:21 to 08-18-2016-02:08:21

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.40.43	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	27
176.13.228.54	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
206.45.27.84	Canada	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	3
176.13.15.189	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
77.139.88.125	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/giyus	Block	2
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
2.55.133.247	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
131.253.25.195	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.86.193	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method ww.idf.il/1585-he/Dover.aspx in URL	Block	1
204.79.180.167	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/miluim/templates/inner.asp	Block	1
68.173.133.157	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	1
5.22.135.109	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
136.243.16.208	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 136.243.16.208	Block	1
50.159.80.219	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	1
77.126.52.225	Israel	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	1
5.29.127.81	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
159.220.74.2	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/patzar/news/default.asp	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
77.126.52.225	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-login.php	Block	1
46.19.86.193	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1226-3.stm).	Block	1
2.53.169.224	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
46.19.86.193	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1

08-18-2016-01:08:21 to 08-18-2016-02:08:21