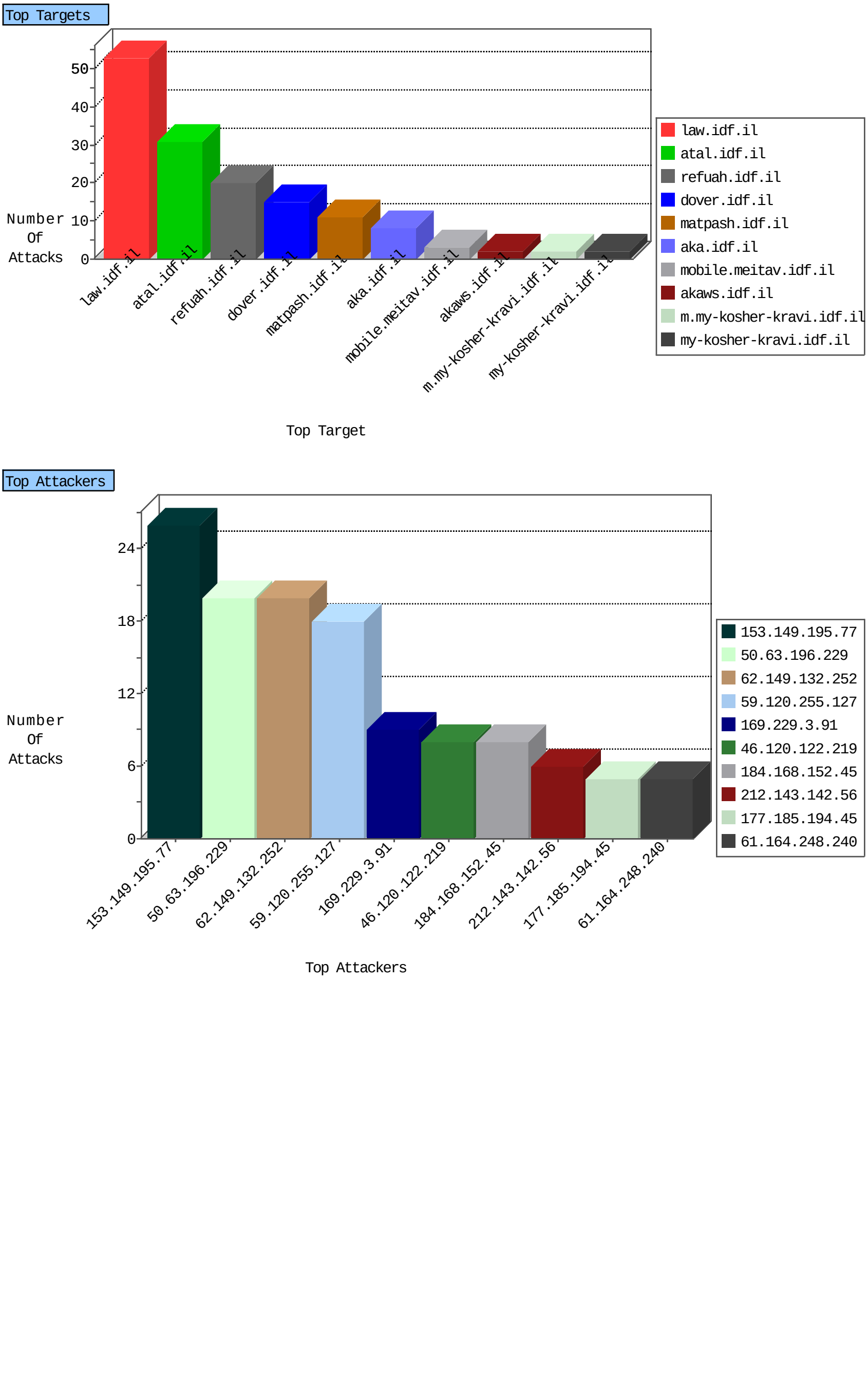
09-02-2016-04:04:08 to 09-02-2016-05:04:08

IDF Under Attack
Daily Report



09-02-2016-04:04:08 to 09-02-2016-05:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.42.253.2	United States	147.237.76.38	e.e.meitav.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.39	mobile.meitav.idf.il	Black List	drop	2
5.189.186.243	Germany	147.237.76.201	e.atal.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.202	e.halag.idf.il	Black List	drop	1
123.151.42.61	China	147.237.76.177	ncore.idf.il	JLM_Under_Attack_Con_Udp	drop	1

09-02-2016-04:04:08 to 09-02-2016-05:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-02-2016-04:04:08 to 09-02-2016-05:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
50.63.196.229	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	20
62.149.132.252	147.237.76.42	Italy	refuah.idf.il	SQL Injection - Select From	20
59.120.255.127	147.237.77.74	Taiwan	law.idf.il	SQL Injection - Select From	18
153.149.195.77	147.237.77.74	Japan	law.idf.il	Tehila - Perl LWP with fake user agent	16
184.168.152.45	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
46.120.122.219	147.237.77.176	Israel	matpash.idf.il	Xenu Link Sleuth User Agent	6
209.15.196.171	147.237.77.233	Canada	atal.idf.il	SQL Injection - Select From	4
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	2
71.36.27.214	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 3072	1
61.164.248.240	147.237.77.235	China	sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.164.248.240	147.237.77.216	China	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.164.248.240	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.169.150	147.237.8.14	United Kingdom	e.orchot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
139.162.247.40	147.237.8.14	United States	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
45.33.116.208	147.237.76.34	United States	yohalan.idf.il	ET SCAN Potential SSH Scan	1
116.12.175.233	147.237.72.166	Singapore	aka.idf.il	ET SCAN NMAP -sS window 4096	1
103.28.61.32	147.237.77.212	Korea, Republic of	e.dover.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
61.164.248.240	147.237.77.233	China	atal.idf.il	ET SCAN NMAP -sS window 1024	1
61.164.248.240	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 1024	1
210.59.240.96	147.237.0.15	Taiwan	kosher-kravi.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
45.56.98.154	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
139.162.179.166	147.237.77.176	United States	matpash.idf.il	ET SCAN Potential SSH Scan	1
116.12.175.233	147.237.72.166	Singapore	aka.idf.il	ET SCAN NMAP -sS window 1024	1

09-02-2016-04:04:08 to 09-02-2016-05:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
177.185.194.45	Brazil	147.237.77.233	atal.idf.il	drop	SAM rule	drop	5
46.19.86.170	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	2
89.242.97.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
169.229.3.91	United States	147.237.0.35	akaws.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.76.202	e.halag.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.0.16	my-kosher-kravi.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.76.176	test.ncore.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.77.205	prisha.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.0.17	m.my-kosher-kravi.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.76.197	e.himush.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.77.227	e.hamaz.idf.il	drop	First packet isn't SYN	drop	1
128.232.110.28	United Kingdom	147.237.76.34	yohalan.idf.il	drop		drop	1
183.129.160.229	China	147.237.0.35	akaws.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.76.201	e.atal.idf.il	drop	First packet isn't SYN	drop	1

09-02-2016-04:04:08 to 09-02-2016-05:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
153.149.195.77	Japan	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 153.149.195.77	Block	6
153.149.195.77	Japan	147.237.77.74	law.idf.il	PHP Attempt	Block	3
54.165.230.219	United States	147.237.77.176	matpash.idf.il	Suspicious Response Code	Block	2
54.173.35.122	United States	147.237.77.176	matpash.idf.il	Distributed Suspicious Response Code	Block	2
157.55.39.56	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/scripts.asmx/getjs	Block	2
128.232.110.28	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
153.149.195.77	Japan	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/images/stories/magic.php.png	Block	1
67.245.1.115	United States	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	1
128.232.110.28	United Kingdom	147.237.76.30	himush.idf.il	Unauthorized Method HEAD for 147.237.76.30/	Block	1
67.245.1.115	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-he/	Block	1
5.255.253.75	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
128.232.110.28	United Kingdom	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
66.249.64.124	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim/templates/ http:/www.aka.idf.il/sip_storage/files/6/66556.pdf	Block	1
187.169.188.44	Mexico	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
77.138.240.165	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
50.242.158.11	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
66.249.76.35	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/default.aspx	Block	1
54.165.230.219	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/163-7247-	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1

09-02-2016-04:04:08 to 09-02-2016-05:04:08