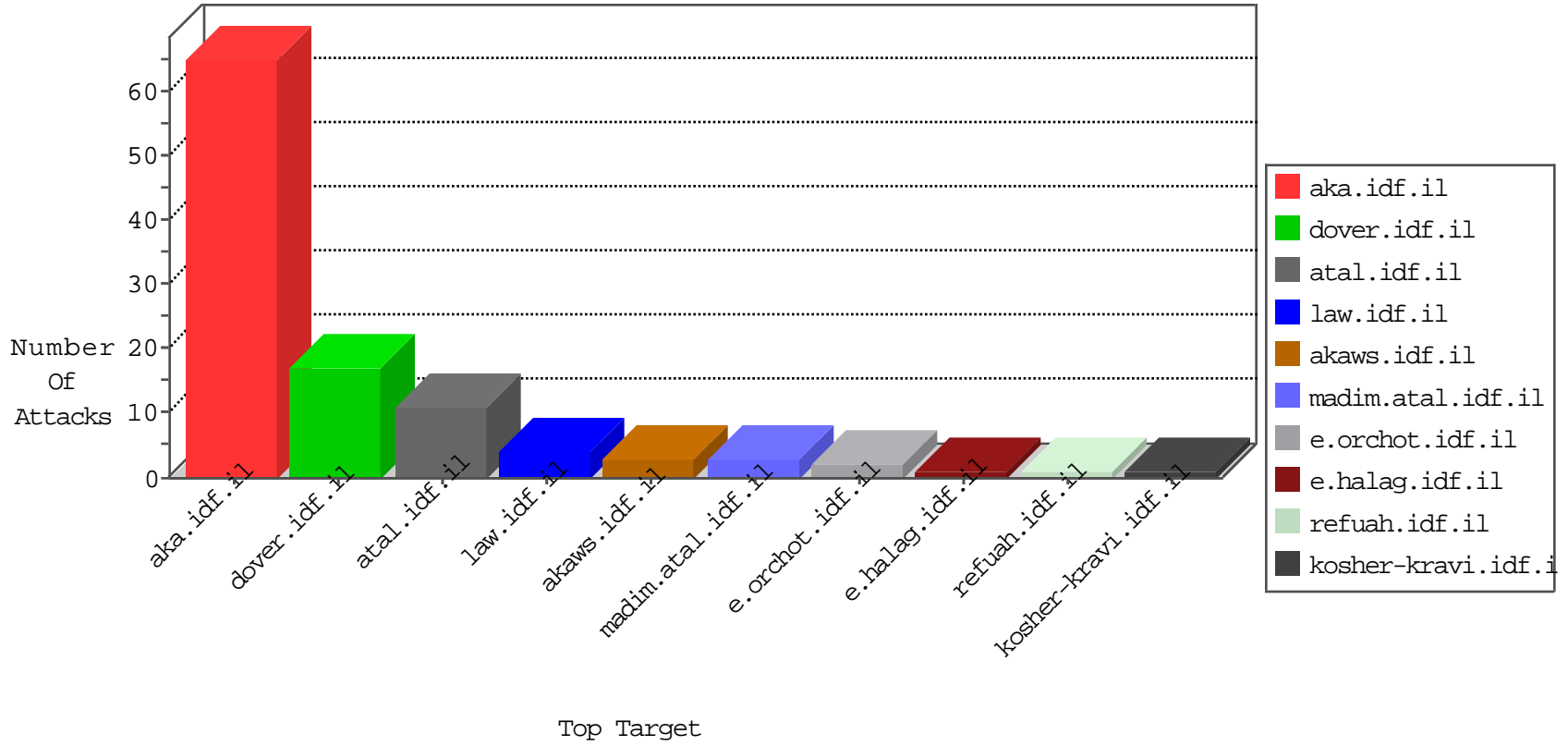


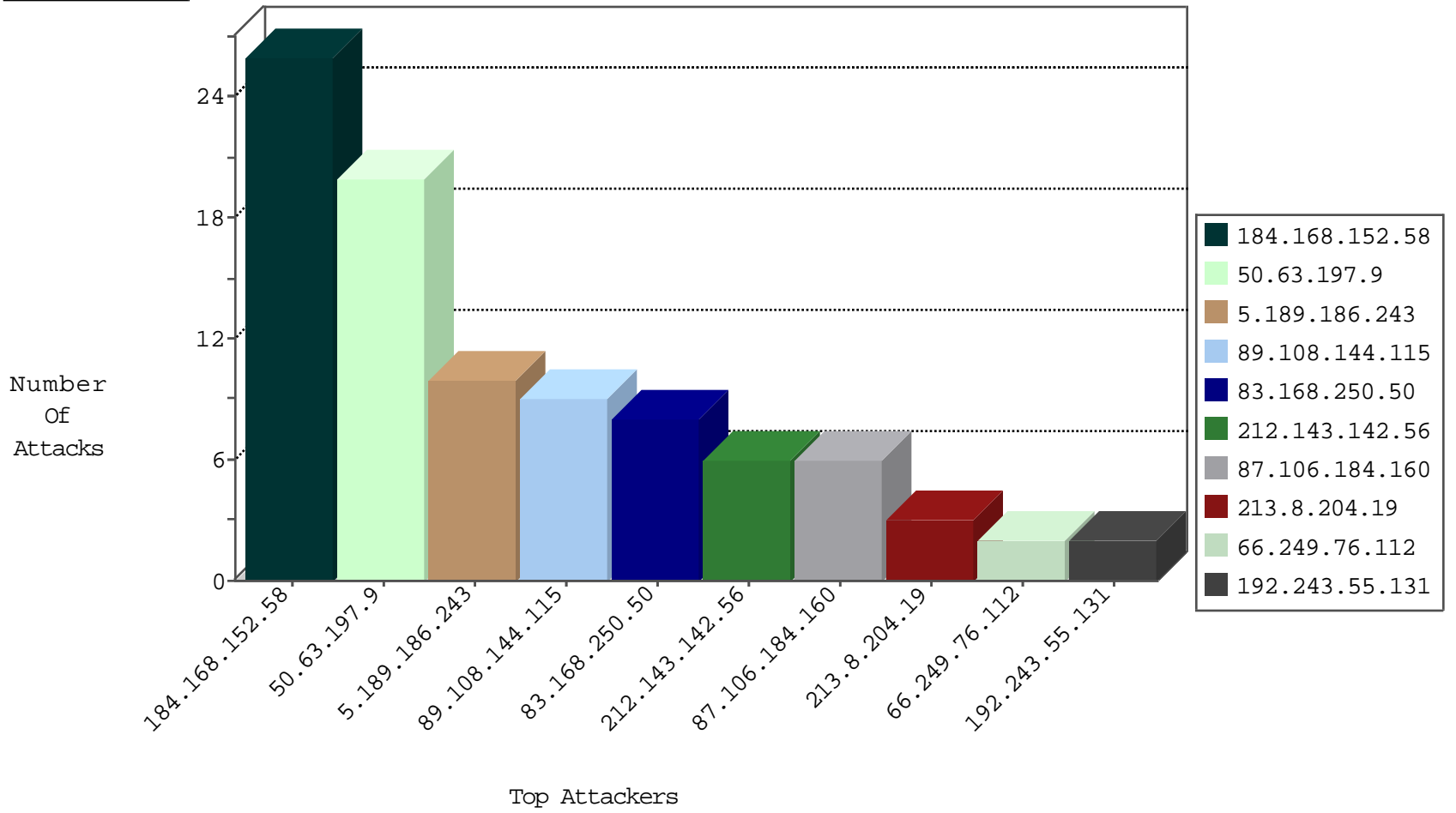
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.158.200.97	Netherlands	147.237.76.42	refuah.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.196	e.sviva.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.200	eitan.aka.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.197	e.himush.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.201	e.atal.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.176	test.ncore.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.202	e.halag.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.177	ncore.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.199	e.nakchal.idf.il	Black List	drop	1

09-02-2016-03:04:00 to 09-02-2016-04:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
184.168.152.58	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	26
50.63.197.9	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	20
83.168.250.50	147.237.77.233	Sweden	atal.idf.il	SQL Injection - Select From	8
137.117.8.203	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	2
208.100.26.228	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.220.201	147.237.0.34	United Kingdom	tikshuv.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
71.36.27.214	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 4096	1
66.249.76.117	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
66.249.64.139	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	1
208.73.143.36	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 1024	1
178.220.165.231	147.237.8.24		e.lifestyle.idf.il	ET SCAN NMAP -sS window 4096	1
146.185.146.112	147.237.8.27	Netherlands	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
71.36.27.214	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 3072	1
66.249.76.112	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
89.108.144.115	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
87.106.184.160	Germany	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.131	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
184.105.139.119	United States	147.237.0.35	akaws.idf.il	drop		drop	1
141.212.122.165	United States	147.237.0.35	akaws.idf.il	drop		drop	1
141.212.122.166	United States	147.237.0.35	akaws.idf.il	drop		drop	1

09-02-2016-03:04:00 to 09-02-2016-04:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.8.204.19	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
85.65.71.23	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
128.232.110.28	United Kingdom	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
192.174.3.200	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
148.251.2.180	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/iturim/asp/displayonesoldier.asp	Block	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
192.243.55.133	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatz	Block	1
157.55.39.206	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
66.249.76.117	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
207.46.13.64	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
91.197.61.250	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
187.169.188.44	Mexico	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
66.249.88.151	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
128.232.110.28	United Kingdom	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 128.232.110.28	Block	1
191.96.249.42	Chile	147.237.77.233	atal.idf.il	Unauthorized URL Access to /phpmyadmin/scripts/setup.php	Block	1
68.180.229.153	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in nakchal.idf.il/1073-he/nakchal.aspx	Block	1

09-02-2016-03:04:00 to 09-02-2016-04:04:00