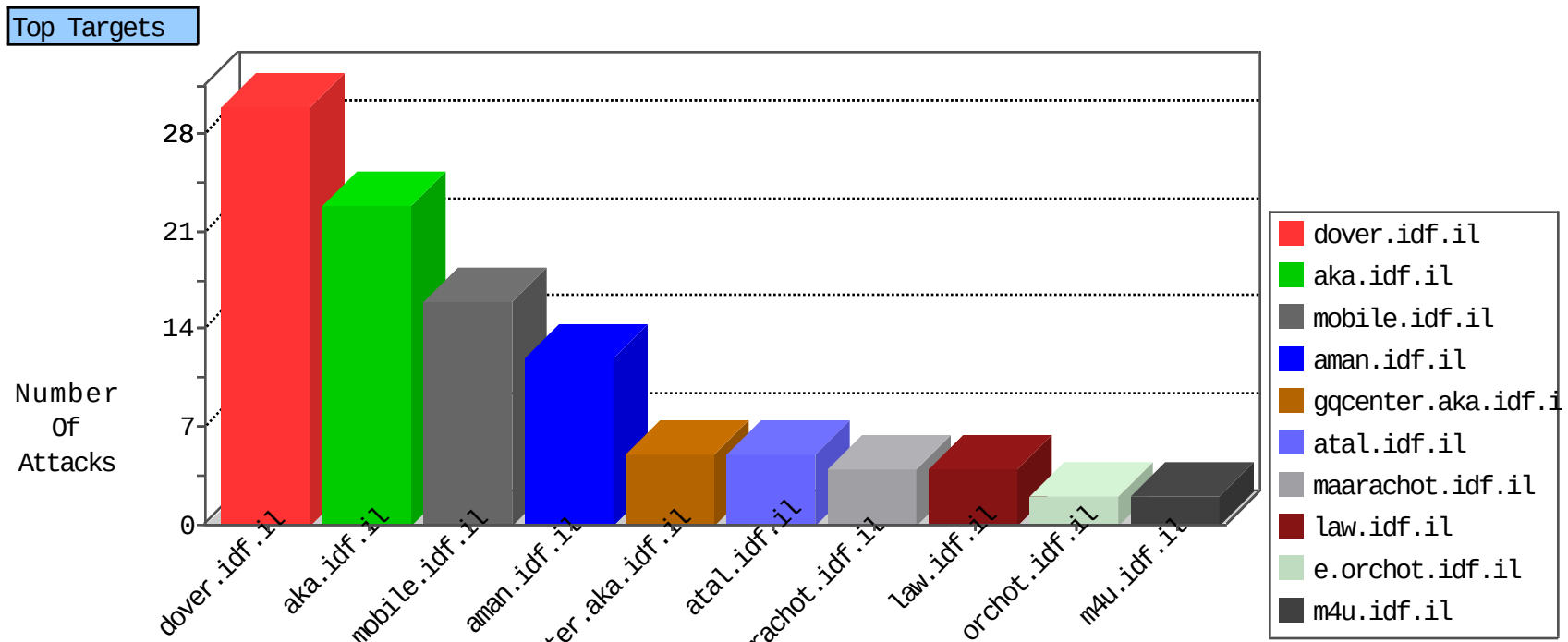
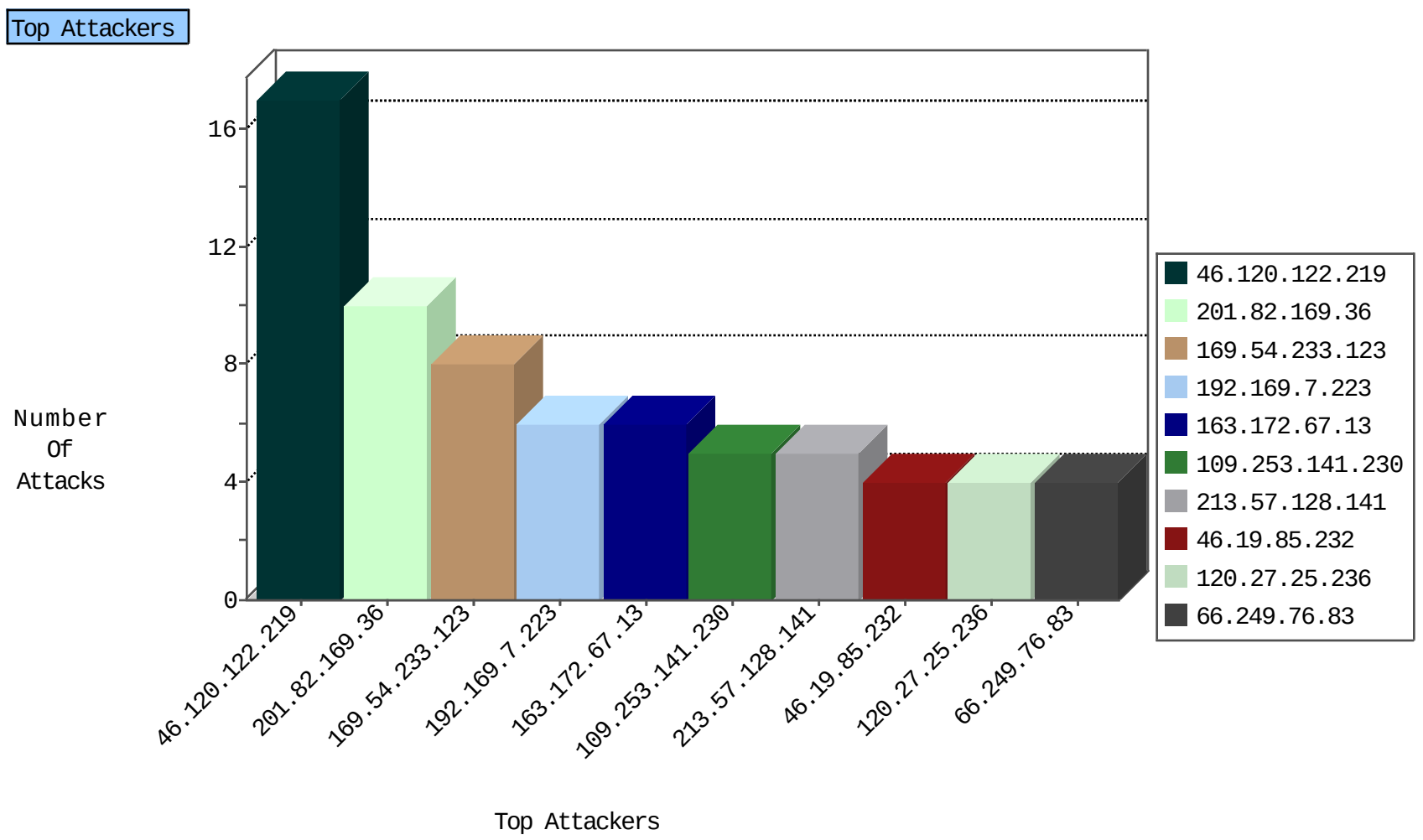
08-30-2016-02:04:06 to 08-30-2016-03:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-30-2016-02:04:06 to 08-30-2016-03:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.2.241	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
120.132.50.135	China	147.237.77.234	halag.idf.il	block-sp-traf1	forward	1

08-30-2016-02:04:06 to 08-30-2016-03:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
61.135.189.120	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
216.119.125.57	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

08-30-2016-02:04:06 to 08-30-2016-03:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	6
46.120.122.219	147.237.77.170	Israel	maarachot.idf.il	Xenu Link Sleuth User Agent	4
216.119.125.57	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	2
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	2
46.120.122.219	147.237.77.74	Israel	law.idf.il	Xenu Link Sleuth User Agent	2
163.172.67.13	147.237.76.42	United Kingdom	refuah.idf.il	ET SCAN Potential SSH Scan	1
120.27.25.236	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
201.38.68.132	147.237.77.235	Brazil	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
120.27.25.236	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
169.54.233.123	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
89.109.238.79	147.237.8.14	Russian Federation	e.orchot.idf.il	ET SCAN NMAP -sS window 4096	1
169.54.233.123	147.237.77.176	United States	matpash.idf.il	ET SCAN Potential SSH Scan	1
79.220.92.136	147.237.8.46	Germany	e.chinuch.idf.il	ET SCAN NMAP -sS window 4096	1
169.54.233.123	147.237.72.156	United States	aman.idf.il	ET SCAN Potential SSH Scan	1
169.54.233.123	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
163.172.67.13	147.237.76.196	United Kingdom	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
163.172.67.13	147.237.76.147	United Kingdom	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
163.172.67.13	147.237.8.46	United Kingdom	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
120.27.25.236	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
169.54.233.123	147.237.77.234	United States	halag.idf.il	ET SCAN Potential SSH Scan	1
120.27.25.236	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
169.54.233.123	147.237.77.216	United States	dover.idf.il	ET SCAN Potential SSH Scan	1
89.109.238.79	147.237.8.14	Russian Federation	e.orchot.idf.il	ET SCAN NMAP -sS window 3072	1
169.54.233.123	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
169.54.233.123	147.237.8.45	United States	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
163.172.67.13	147.237.77.227	United Kingdom	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
163.172.67.13	147.237.76.176	United Kingdom	test.ncore.idf.il	ET SCAN Potential SSH Scan	1

08-30-2016-02:04:06 to 08-30-2016-03:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
201.82.169.36	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
192.169.7.223	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	5
109.253.141.230	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
176.13.244.128	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
89.139.149.30	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
189.179.70.241	Mexico	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
120.132.67.190	China	147.237.0.200	m4u.idf.il	drop		drop	1
139.162.37.113	United States	147.237.0.35	akaws.idf.il	drop		drop	1
183.129.160.229	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.0.200	m4u.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	1

08-30-2016-02:04:06 to 08-30-2016-03:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.57.128.141	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	5
46.19.85.232	Israel	147.237.77.243	mobile.idf.i	Distributed Suspicious Response Code	Block	4
89.237.66.97	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	3
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.120.122.219	Block	3
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	3
176.13.23.47	Israel	147.237.77.243	mobile.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.25	Israel	147.237.77.243	mobile.idf.i	Distributed Suspicious Response Code	Block	3
207.46.13.64	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.53.52.240	Israel	147.237.77.243	mobile.idf.i	Distributed Suspicious Response Code	Block	2
105.225.92.220	South Africa	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
192.169.7.223	United States	147.237.76.42	refuah.idf.i	Unauthorized Method HEAD for 147.237.76.42/	Block	1
176.13.7.67	Israel	147.237.77.243	mobile.idf.i	Distributed Suspicious Response Code	Block	1
89.237.66.97	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
61.135.189.120	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
176.13.10.200	Israel	147.237.77.243	mobile.idf.i	Distributed Suspicious Response Code	Block	1
79.178.33.211	Israel	147.237.77.243	mobile.idf.i	Distributed Suspicious Response Code	Block	1
207.46.13.109	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
95.221.211.70	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
66.102.9.2	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
81.218.229.198	Israel	147.237.0.34	tikshuv.idf.i	Multiple Unauthorized URL Access from 81.218.229.198	Block	1
105.225.92.220	South Africa	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
176.13.251.217	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
81.218.229.198	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 81.218.229.198	Block	1

08-30-2016-02:04:06 to 08-30-2016-03:04:06