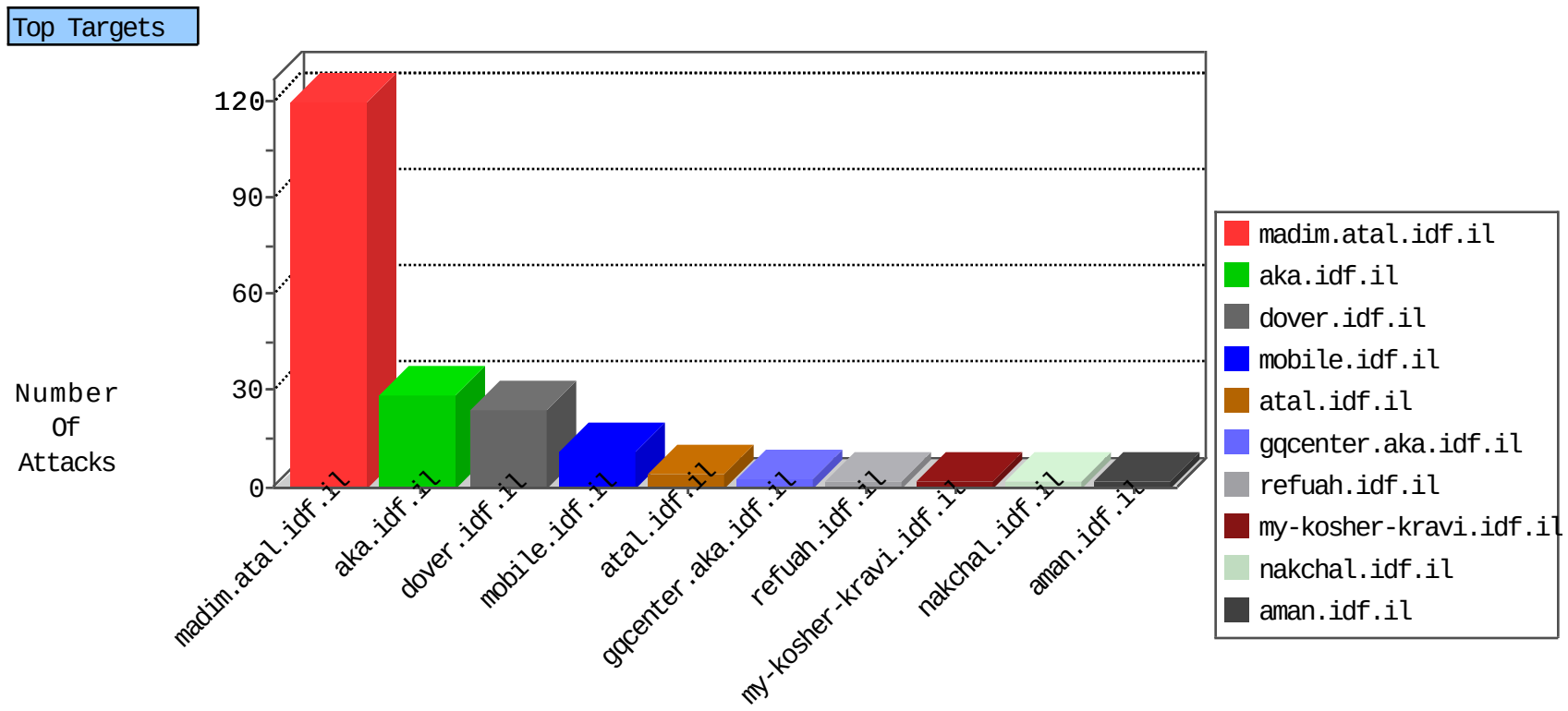
08-31-2016-06:04:09 to 08-31-2016-07:04:09

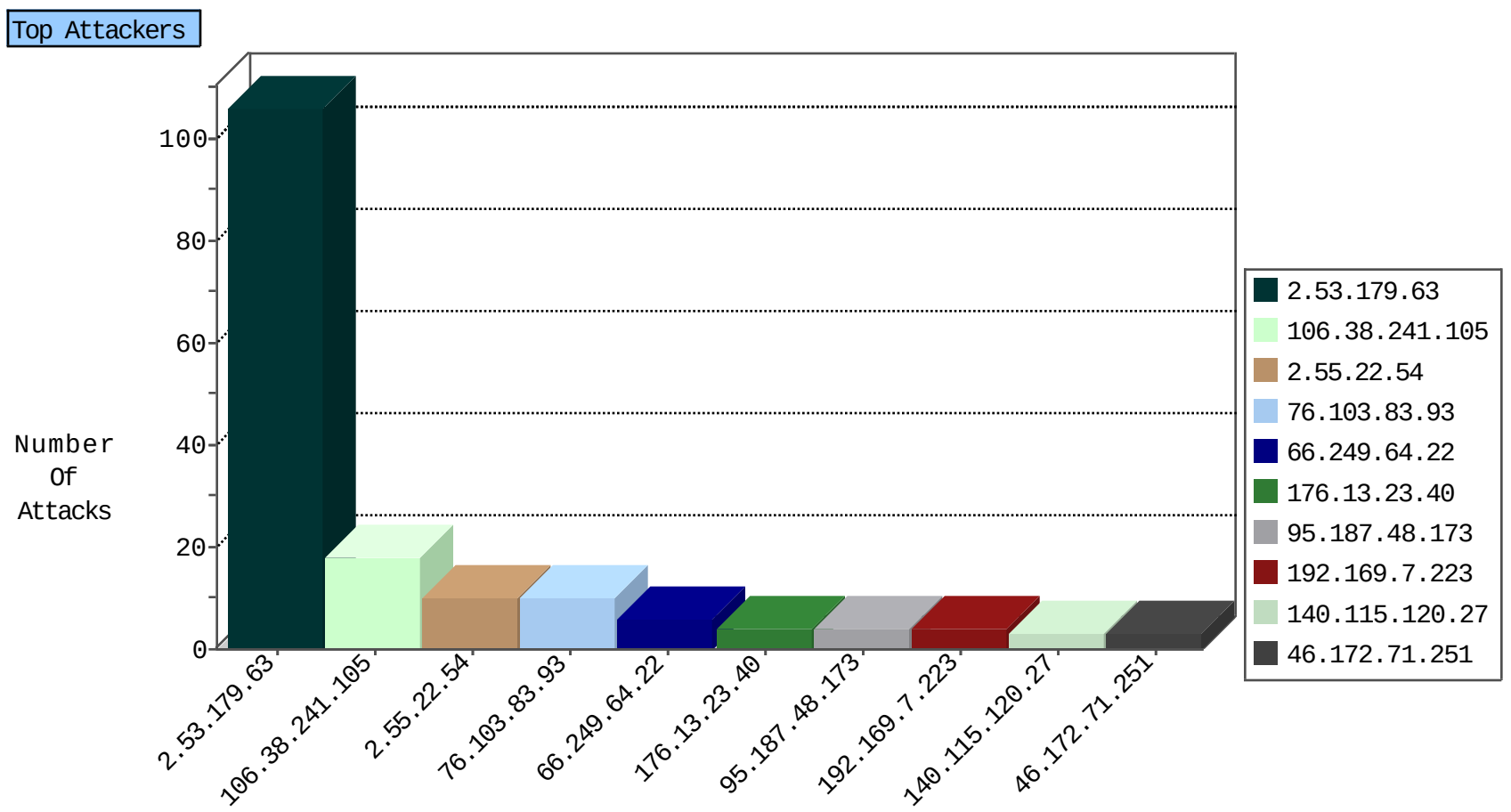
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

08-31-2016-06:04:09 to 08-31-2016-07:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
95.187.48.173	Saudi Arabia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
2.53.8.130	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
120.132.50.135	China	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	1
163.172.216.36	United Kingdom	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
85.93.93.95	Germany	147.237.76.34	yohalan.idf.il	Black List	drop	1

08-31-2016-06:04:09 to 08-31-2016-07:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	16
106.38.241.105	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2

08-31-2016-06:04:09 to 08-31-2016-07:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
140.115.120.27	147.237.72.166	Taiwan	aka.idf.il	ET SCAN NMAP -sS window 1024	1
120.27.25.236	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
93.174.91.29	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
46.172.71.251	147.237.0.34	Ukraine	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
46.172.71.251	147.237.0.16	Ukraine	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
201.238.202.219	147.237.72.14	Chile	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.77.243	United Kingdom	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
140.115.120.27	147.237.77.227	Taiwan	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
140.115.120.27	147.237.8.14	Taiwan	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
120.27.25.236	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
87.236.194.161	147.237.76.199	Czech Republic	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
46.172.71.251	147.237.0.33	Ukraine	idf.il	ET SCAN NMAP -sS window 1024	1
5.189.163.119	147.237.77.233	Germany	atal.idf.il	ET SCAN NMAP -sS window 1024	1
223.194.35.67	147.237.0.19	Korea, Republic of	madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
198.167.223.33	147.237.76.44	Saint Kitts and Nevis	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.8.45	United Kingdom	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1

08-31-2016-06:04:09 to 08-31-2016-07:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
76.103.83.93	United States	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	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
79.177.221.194	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
137.116.71.170	United States	147.237.0.35	akaws.idf.il	drop		drop	1
176.13.244.178	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1

08-31-2016-06:04:09 to 08-31-2016-07:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.179.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	106
2.55.22.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
66.249.64.22	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.22	Block	5
176.13.23.40	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
109.253.223.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.163.202	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
204.79.180.219	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/miluim/templates/inner.asp	Block	1
68.180.229.49	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
66.249.66.176	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/tizmoret/gallery/showpicture.asp	Block	1
217.132.64.116	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
71.6.135.131	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
66.249.64.22	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/iaf/iaf7	Block	1
2.53.128.72	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	1
157.55.39.37	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
66.249.66.179	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
5.102.195.131	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
77.138.135.209	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.57	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
2.53.163.80	Israel	147.237.72.166	aka.idf.il	Redundant HTTP Headers Referer	Block	1
66.249.76.100	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
46.19.85.232	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
77.138.245.180	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/	Block	1
66.249.66.109	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/6/שקופית2	Block	1
192.169.7.223	United States	147.237.76.42	refuah.idf.il	Unauthorized Method HEAD for 147.237.76.42/	Block	1
66.249.79.61	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/.well-known/apple-app-site-association	Block	1
46.117.124.58	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
77.139.14.108	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
66.249.66.174	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in 147.237.72.166/main/giyus/general.aspx	Block	1

08-31-2016-06:04:09 to 08-31-2016-07:04:09