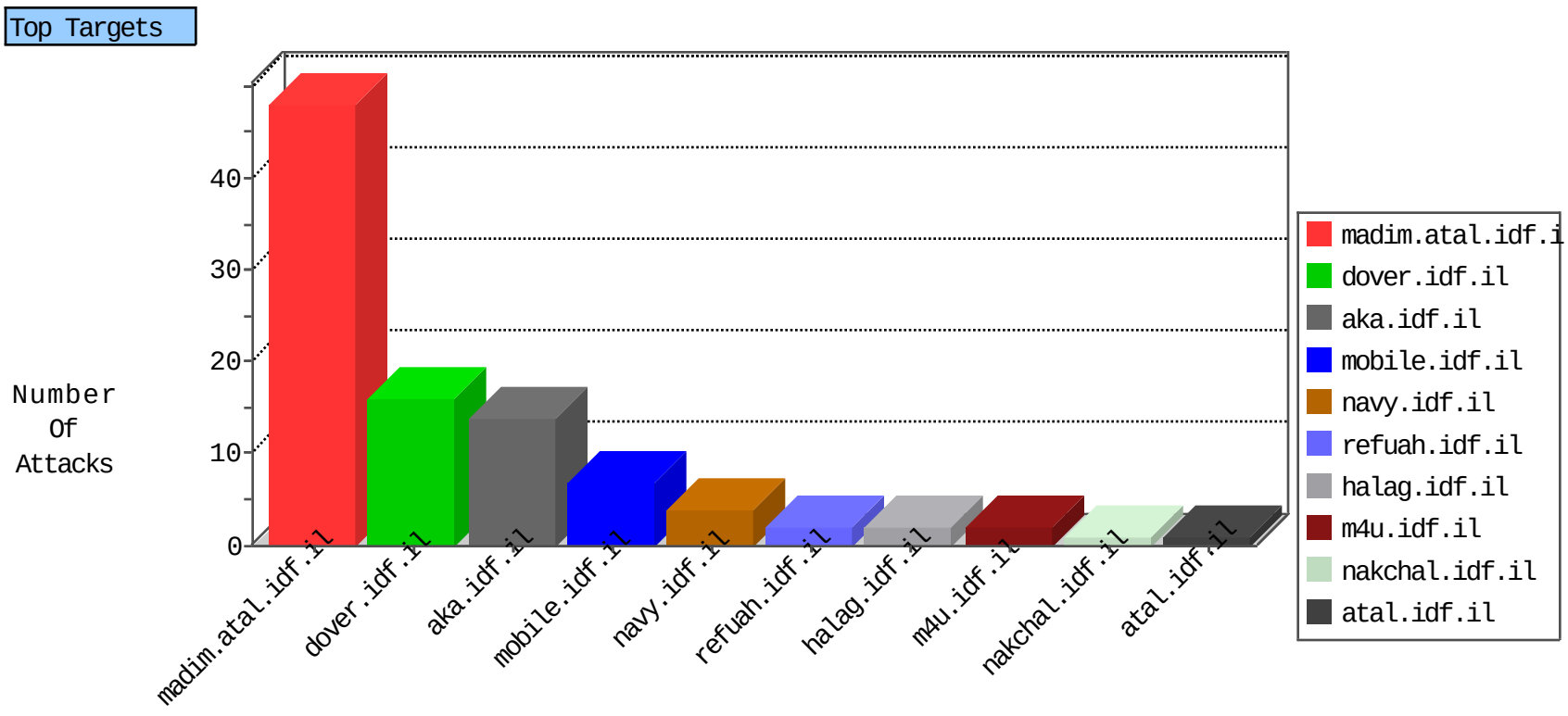
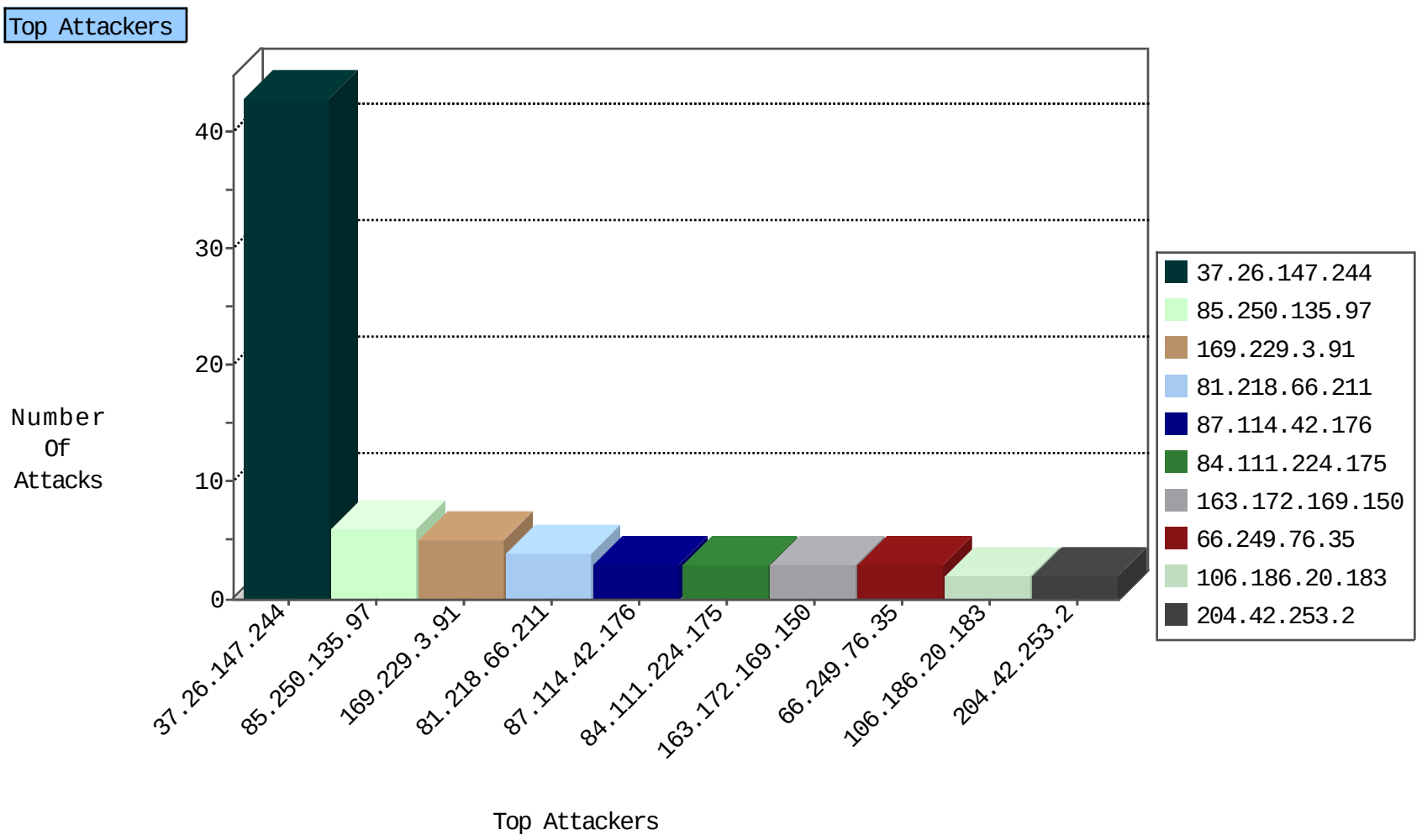
09-02-2016-07:04:00 to 09-02-2016-08:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-02-2016-07:04:00 to 09-02-2016-08:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
204.42.253.2	United States	147.237.76.86	navy.idf.il	Black List	drop	2

09-02-2016-07:04:00 to 09-02-2016-08:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-02-2016-07:04:00 to 09-02-2016-08:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
87.114.42.176	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	2
163.172.169.150	147.237.76.86	United Kingdom	navy.idf.il	ET SCAN NMAP -sS window 1024	1
106.186.20.183	147.237.77.234	Japan	halag.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	147.237.77.216	Canada	dover.idf.il	ET SCAN NMAP -sS window 4096	1
66.249.64.240	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	1
163.172.169.150	147.237.77.233	United Kingdom	atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.169.150	147.237.76.31	United Kingdom	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
106.186.20.183	147.237.0.33	Japan	idf.il	ET SCAN Potential SSH Scan	1
103.207.39.11	147.237.72.156	Vietnam	aman.idf.il	ET SCAN NMAP -sS window 1024	1
87.114.42.176	147.237.77.74	United Kingdom	law.idf.il	Tehila - Perl LWP with fake user agent	1
45.56.98.154	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential SSH Scan	1

09-02-2016-07:04:00 to 09-02-2016-08:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
81.218.66.211	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
141.212.122.35	United States	147.237.0.200	m4u.idf.il	drop		drop	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.8.28	e.mobile-ks.idf.il	drop	First packet isn't SYN	drop	1
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
87.69.200.86	Israel	147.237.72.166	aka.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
216.218.206.118	United States	147.237.0.35	akaws.idf.il	drop		drop	1
109.253.217.235	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.34	United States	147.237.0.200	m4u.idf.il	drop		drop	1
169.229.3.91	United States	147.237.77.227	e.hamaz.idf.il	drop	First packet isn't SYN	drop	1

09-02-2016-07:04:00 to 09-02-2016-08:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.147.244	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	43
85.250.135.97	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 85.250.135.97	Block	4
84.111.224.175	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
66.249.76.35	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.35	Block	2
73.22.155.10	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/	Block	2
77.124.14.82	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
85.250.135.97	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
157.55.39.14	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/smalim/default.asp	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/default.aspx	Block	1
66.249.76.30	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1664	Block	1
87.69.123.135	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
68.180.230.47	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1113-2.stm" target="_blank	Block	1
40.77.167.2	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1
157.55.39.97	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
93.172.195.64	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 93.172.195.64	Block	1
66.249.64.99	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.tech.atal.idf.il/templates/news/null	Block	1
199.30.24.223	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.76.35	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/.well-known/assetlinks.json	Block	1
136.243.67.234	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
66.249.69.67	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/2424.jpg	Block	1
207.46.13.64	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/valtam/main/procedure.asp	Block	1
66.249.76.70	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	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
78.46.23.198	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/rights/asp/info.asp	Block	1
66.249.69.127	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/2973.jpg	Block	1
87.69.123.135	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 87.69.123.135 (Open Mode)	None	1
68.180.228.87	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/shared/usercontrols/headerupper/	Block	1

09-02-2016-07:04:00 to 09-02-2016-08:04:00