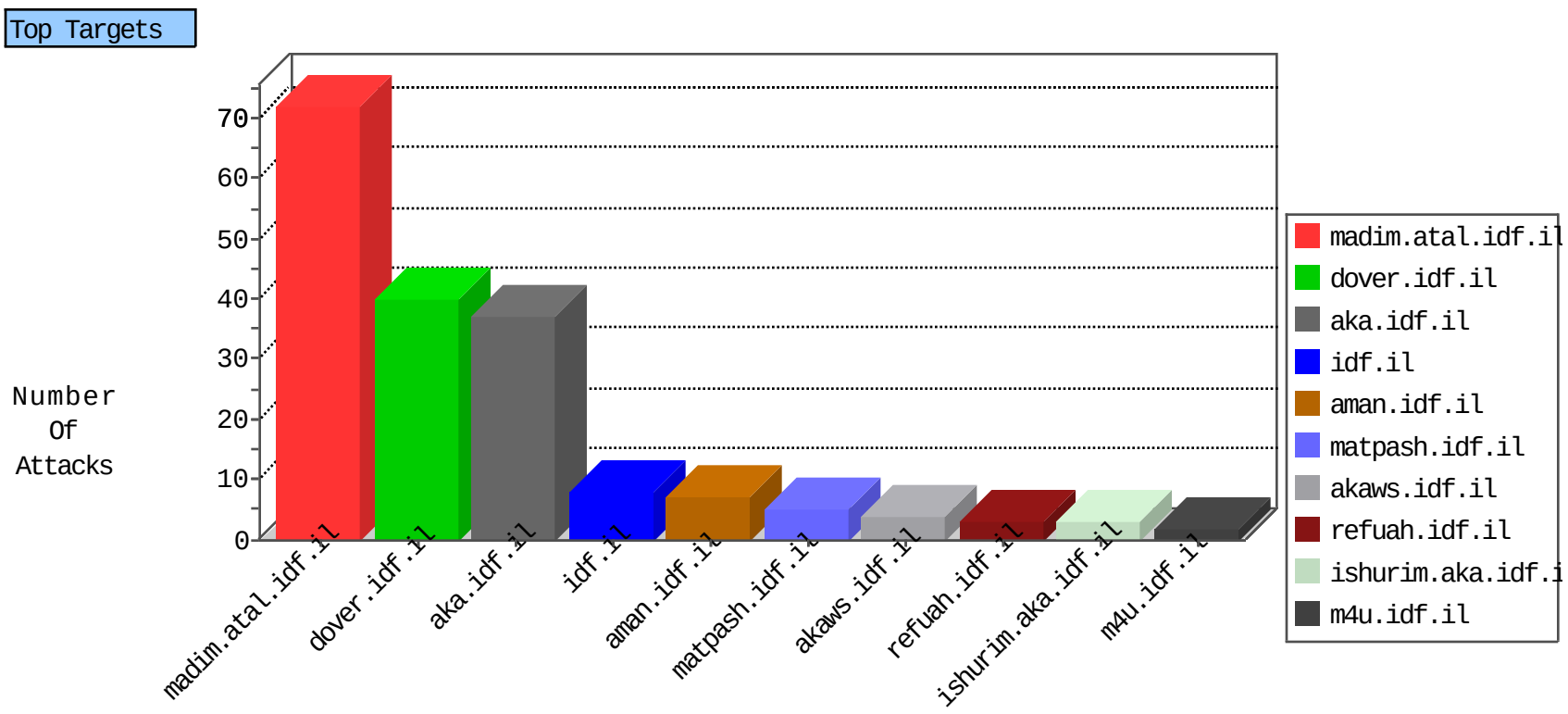
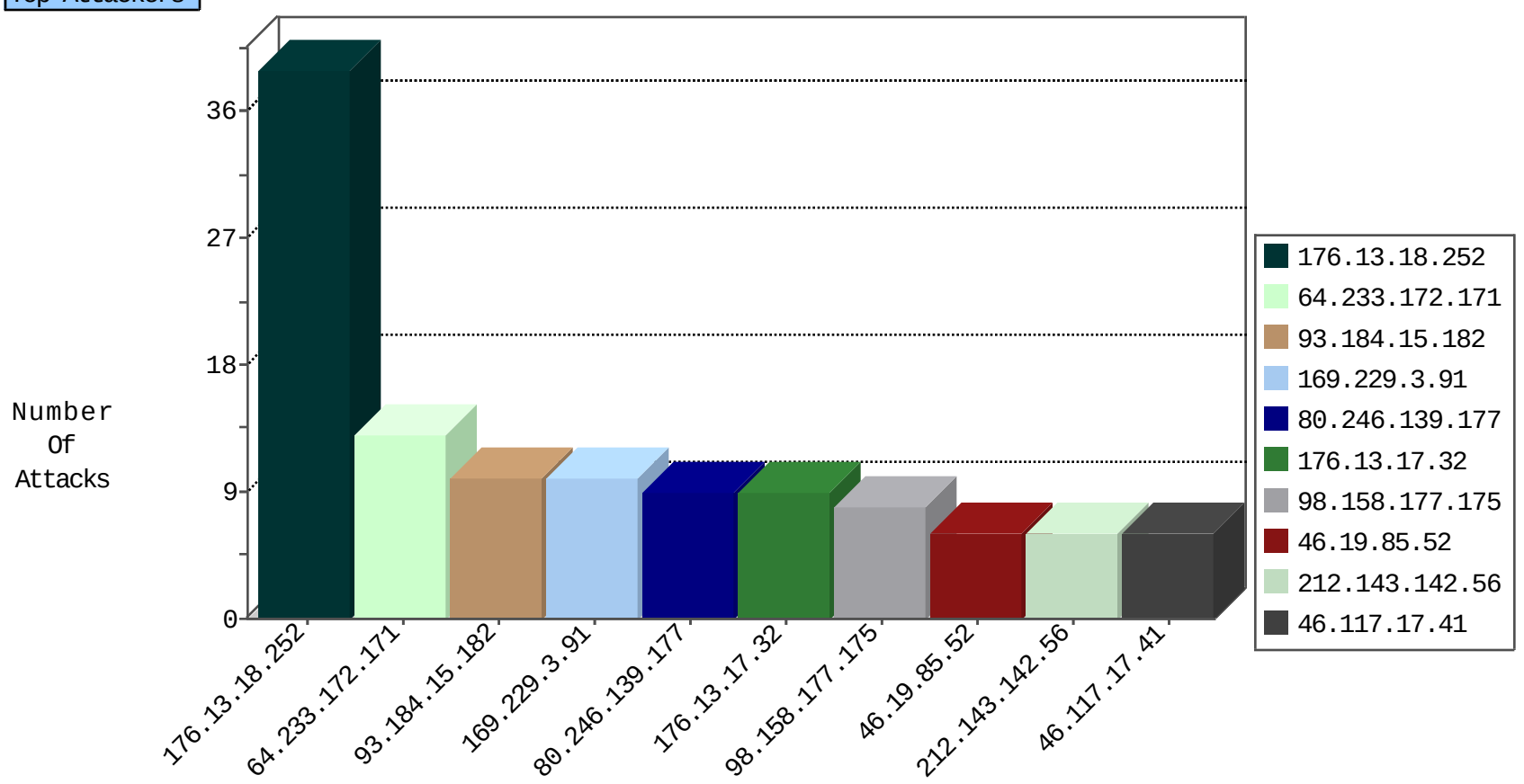
09-02-2016-11:04:02 to 09-02-2016-12:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-02-2016-11:04:02 to 09-02-2016-12:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
68.180.230.47	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2

09-02-2016-11:04:02 to 09-02-2016-12:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-02-2016-11:04:02 to 09-02-2016-12:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
192.243.55.131	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
98.158.177.175	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
98.158.177.175	147.237.76.30	United States	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
98.158.177.175	147.237.72.166	United States	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
98.158.177.175	147.237.0.33	United States	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.174.93.220	147.237.8.14	Netherlands	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
81.171.107.110	147.237.0.33	France	idf.il	ET SCAN Potential SSH Scan	1
5.233.249.192	147.237.77.216	Iran, Islamic Republic of	dover.idf.il	portscan: TCP Distributed Portscan	1
193.201.225.138	147.237.72.167	Ukraine	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
176.47.69.93	147.237.77.216	Saudi Arabia	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
98.158.177.175	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
98.158.177.175	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
98.158.177.175	147.237.0.200	United States	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
98.158.177.175	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
84.229.48.84	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sA (2)	1
66.249.79.114	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sA (2)	1

09-02-2016-11:04:02 to 09-02-2016-12:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
64.233.172.171	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
176.13.17.32	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
93.184.15.182	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
106.39.60.180	China	147.237.0.33	idf.il	drop		drop	6
176.13.237.7	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
93.184.15.182	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
185.89.217.235	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	2
109.253.133.146	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
176.13.225.102	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	1
109.226.40.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
216.243.31.2	United States	147.237.0.200	m4u.idf.il	drop		drop	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.94	United States	147.237.0.35	akaws.idf.il	drop		drop	1
82.81.86.250	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	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	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	drop	First packet isn't SYN	drop	1
207.46.13.90	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.76.198	e.yohalan.idf.il	drop	First packet isn't SYN	drop	1
109.253.203.118	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
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	147.237.76.200	eitan.aka.idf.il	drop	First packet isn't SYN	drop	1
125.77.28.26	China	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
216.243.31.2	United States	147.237.0.35	akaws.idf.il	drop		drop	1
169.229.3.91	United States	147.237.76.201	e.atal.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.93	United States	147.237.0.35	akaws.idf.il	drop		drop	1
82.80.64.158	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1

09-02-2016-11:04:02 to 09-02-2016-12:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.18.252	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	39
80.246.139.177	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
46.19.85.52	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
46.117.17.41	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.117.17.41	Block	5
80.246.139.119	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
185.120.124.24	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.55.24.19	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.177.230.183	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.194.77	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.141.116	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
77.138.7.120	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/sachar	Block	2
77.138.175.66	France	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.69.14	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
66.249.76.127	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/webservices/wscity.asmx	Block	1
66.102.9.24	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
212.76.123.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.108.56.93	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/wp-login.php	Block	1
79.177.28.159	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
66.249.76.37	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/7/שקופית2	Block	1
46.117.17.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
185.32.179.56	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	1
66.249.79.114	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/.well-known/assetlinks.json	Block	1
212.76.123.215	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
95.35.163.124	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
79.177.85.155	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
52.37.76.55	United States	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 52.37.76.55 (Unsupported Cipher)	None	1
77.124.6.50	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
213.151.35.216	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
66.249.64.240	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 66.249.64.240	Block	1
106.39.60.187	China	147.237.0.19	madim.atal.idf.i	Untraceable SSL Sessions: Open Mode	None	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
52.37.76.55	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Unsupported Cipher	None	1
192.243.55.137	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/general	Block	1
84.108.5.185	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
66.249.64.240	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/general.aspx	Block	1
79.178.46.178	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 79.178.46.178 (Open Mode)	None	1
66.249.76.121	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/civiladministration/minhalnews/pages/hakalahom.aspx	Block	1
66.102.9.24	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 66.102.9.24	Block	1
207.46.13.77	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.108.56.93	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1

09-02-2016-11:04:02 to 09-02-2016-12:04:02