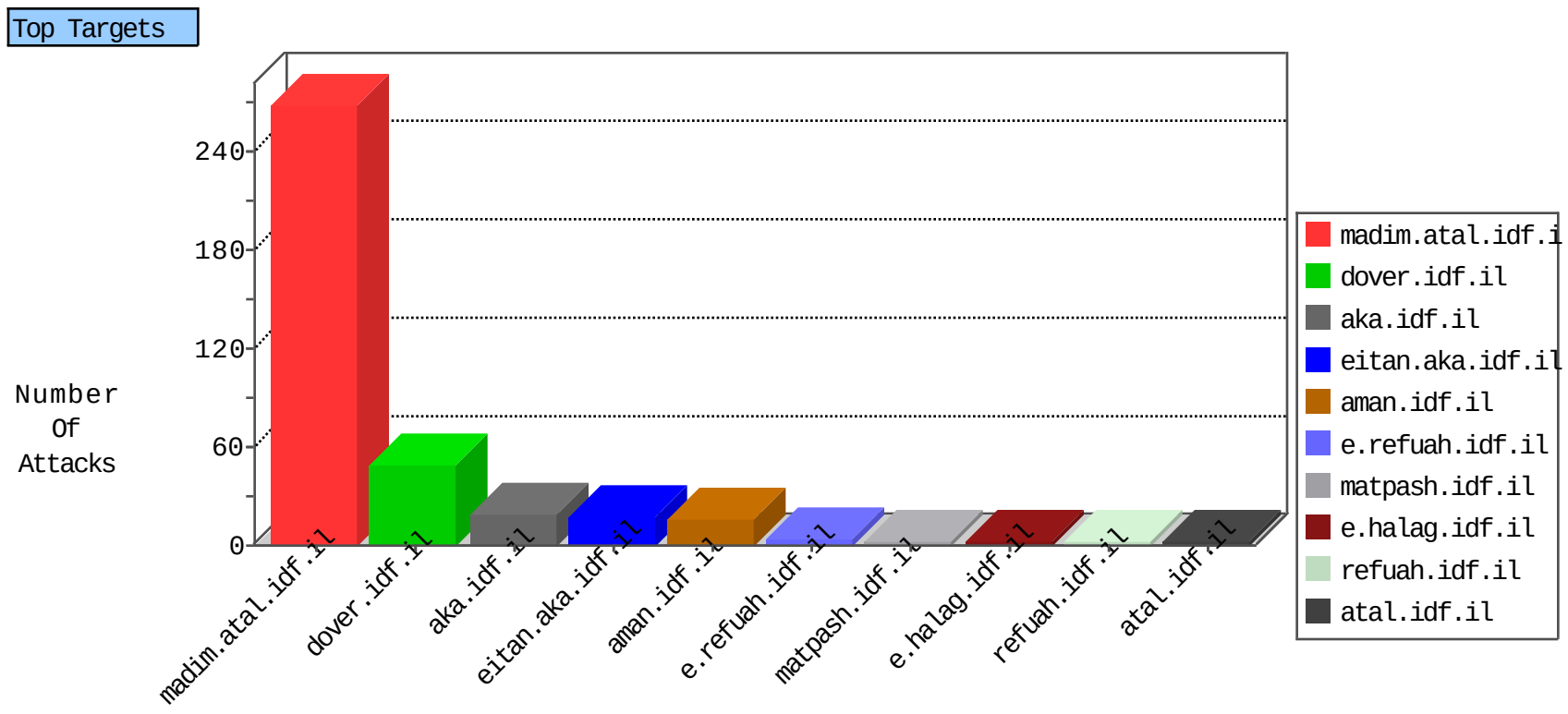
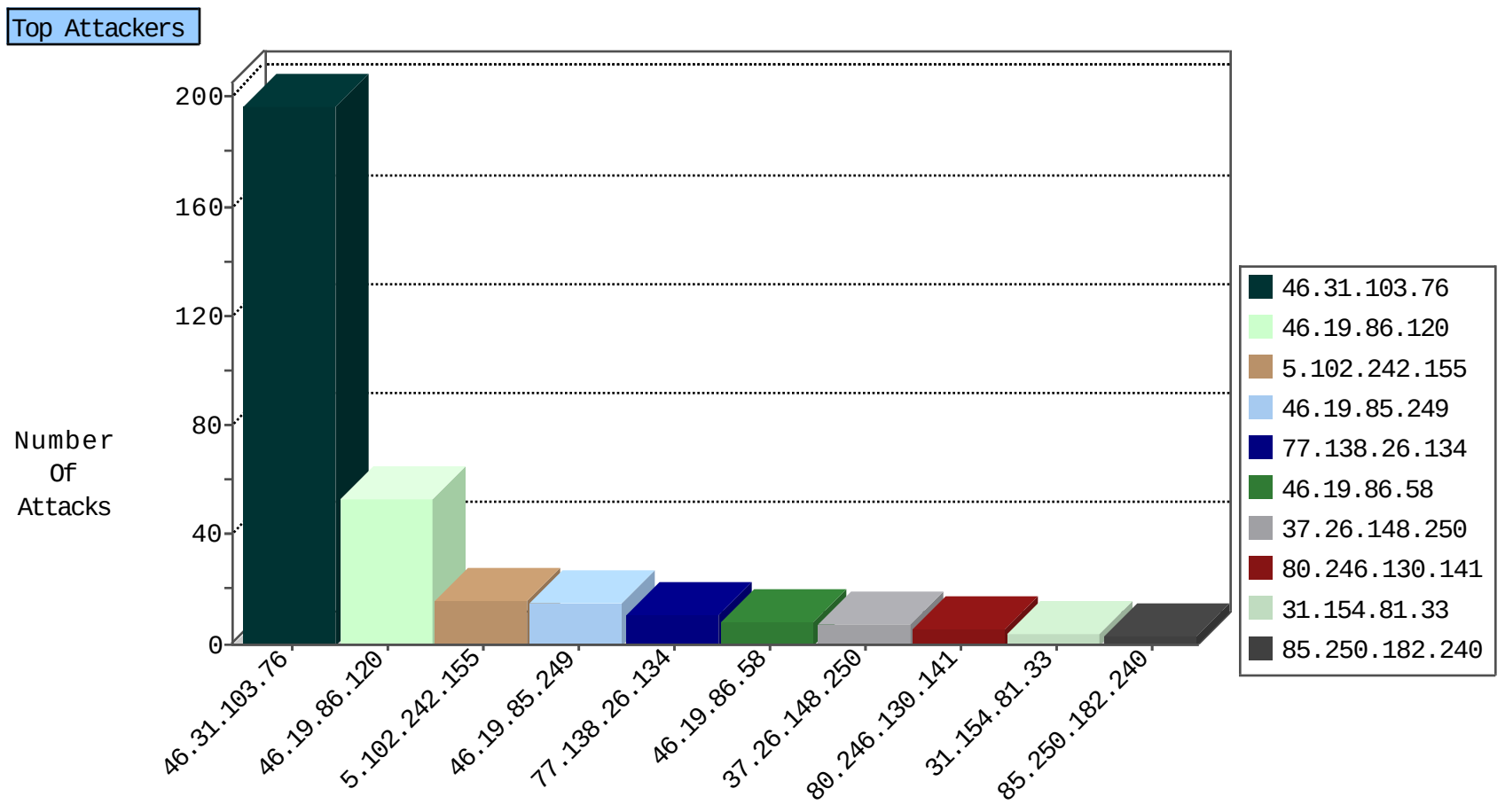
09-02-2016-16:04:04 to 09-02-2016-17:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-02-2016-16:04:04 to 09-02-2016-17:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.47.57	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
84.109.104.55	Israel	147.237.77.216	dover.idf.il	Black List	drop	1
37.26.148.250	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
46.116.172.133	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

09-02-2016-16:04:04 to 09-02-2016-17:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-02-2016-16:04:04 to 09-02-2016-17:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
85.250.182.240	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	2
61.153.237.122	147.237.76.44	China	e.refuah.idf.il	GPL SCAN nmap TCP	2
220.133.207.21	147.237.0.16	Taiwan	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
208.100.26.228	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
197.211.244.181	147.237.76.44	Zimbabwe	e.refuah.idf.il	ET SCAN NMAP -sS window 3072	1
113.161.74.250	147.237.0.16	Vietnam	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
104.232.98.38	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.64.230	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
211.141.78.56	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
197.211.244.181	147.237.76.44	Zimbabwe	e.refuah.idf.il	ET SCAN NMAP -sS window 4096	1
194.60.242.6	147.237.76.202	Ukraine	e.halag.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
104.232.98.38	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 3072	1
93.168.20.187	147.237.77.216	Saudi Arabia	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
85.250.182.240	147.237.77.170	Israel	maarachot.idf.il	Xenu Link Sleuth User Agent	1

09-02-2016-16:04:04 to 09-02-2016-17:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.86.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.26.148.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
31.154.81.33	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
82.205.25.31	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
79.179.154.148	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
141.212.122.153	United States	147.237.0.33	idf.il	drop		drop	1
109.67.132.174	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
77.138.26.134	France	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
109.253.144.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
31.168.242.219	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
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.145.50	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.152	United States	147.237.0.33	idf.il	drop		drop	1
37.157.215.153	Armenia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

09-02-2016-16:04:04 to 09-02-2016-17:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.31.103.76	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	197
46.19.86.120	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	53
5.102.242.155	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/homepage/homepage.aspx	Block	16
46.19.85.249	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
77.138.26.134	France	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	8
80.246.130.141	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
94.74.211.130	Czech Republic	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar	Block	3
77.138.207.62	France	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
66.102.9.13	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
80.246.130.32	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
213.151.45.141	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
66.8.122.86	South Africa	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
2.36.17.94	Italy	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/	Block	1
77.139.184.242	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
66.249.76.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
188.165.233.34	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1
79.181.53.61	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.26.134	France	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 77.138.26.134 (Open Mode)	None	1
109.253.215.210	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
2.53.47.57	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
77.139.208.106	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
196.0.57.234	Uganda	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
77.138.26.134	France	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.64.41	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/headerupper/	Block	1
5.22.135.174	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 5.22.135.174	Block	1
112.209.170.144	Philippines	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.139.254.42	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	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
197.239.5.109	Uganda	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1283-en/dover.aspx	Block	1
66.249.64.122	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/drushim/misrot.aspx	Block	1
157.55.39.34	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
79.177.221.212	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.88.154	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
207.46.13.90	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	1
62.110.65.165	Italy	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
81.218.143.187	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
77.139.51.154	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
46.19.85.107	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
164.160.172.206		147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/general.aspx	Block	1
79.180.202.180	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	1

09-02-2016-16:04:04 to 09-02-2016-17:04:04