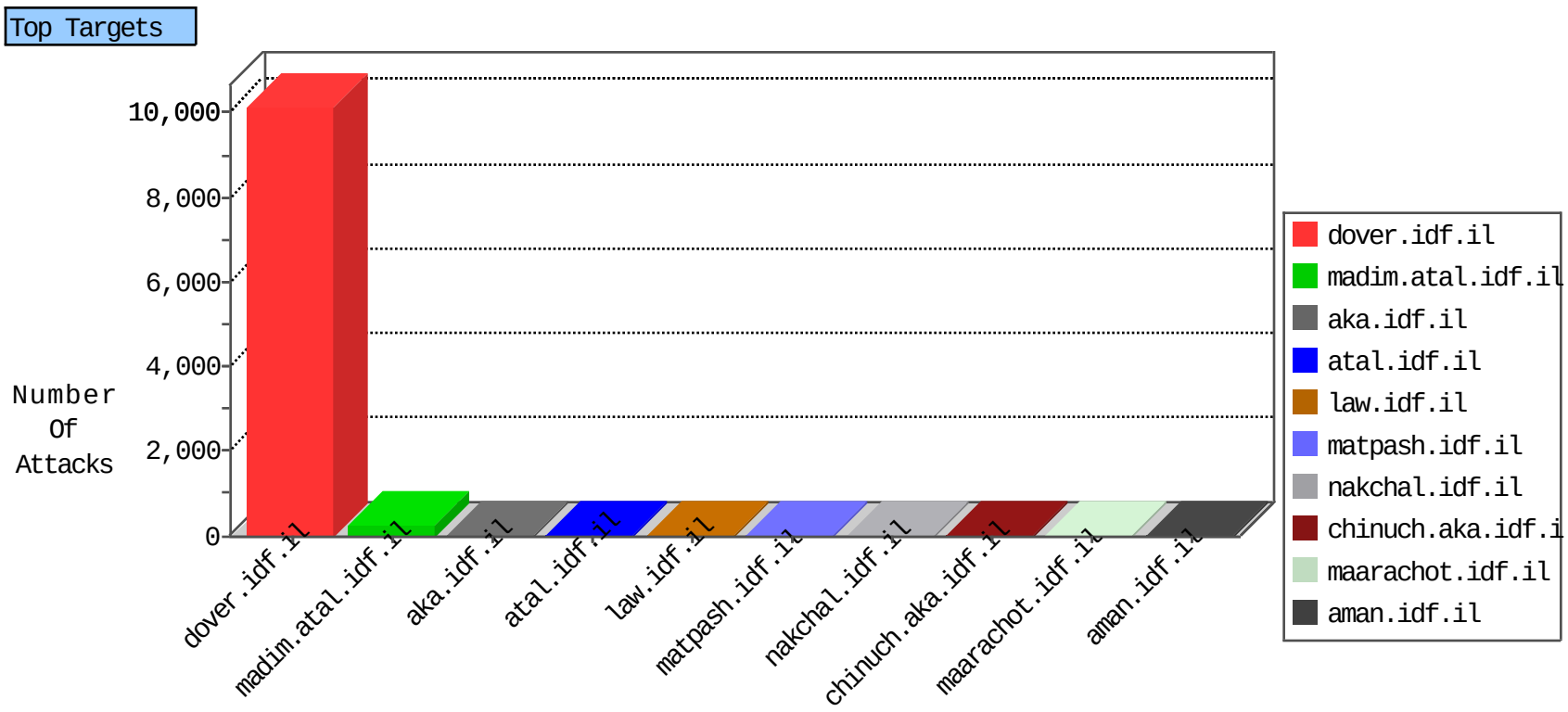
08-27-2016-17:04:00 to 08-27-2016-18:04:00

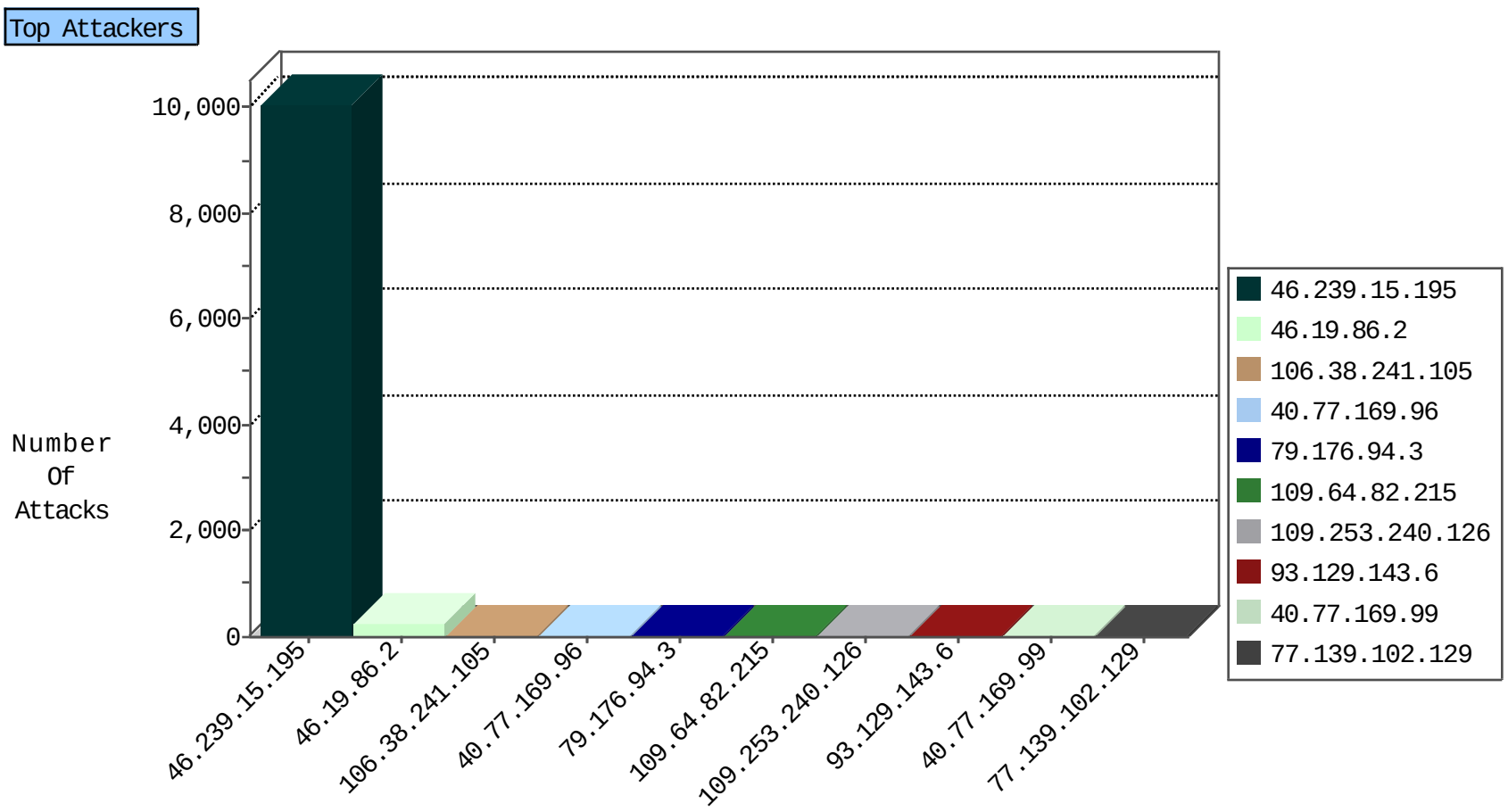
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

08-27-2016-17:04:00 to 08-27-2016-18:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.78.2	Israel	147.237.72.166	aka.idf.il	Black List	drop	3
46.239.15.195	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	2
123.59.59.52	China	147.237.77.235	sviva.idf.il	block-sp-traf1	forward	1
176.228.185.241	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
104.148.35.34	United States	147.237.76.44	e.refuah.idf.il	Black List	drop	1
188.165.30.46	Lithuania	147.237.76.38	e.e.meitav.idf.i	Black List	drop	1
120.132.50.135	China	147.237.77.235	sviva.idf.il	block-sp-traf1	forward	1

08-27-2016-17:04:00 to 08-27-2016-18:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

08-27-2016-17:04:00 to 08-27-2016-18:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
109.64.82.215	147.237.77.233	Israel	atal.idf.il	ET SCAN NMAP -sA (2)	11
79.176.125.30	147.237.76.147	Israel	chinuch.aka.idf.il	ET SCAN NMAP -sA (2)	2
5.102.254.88	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	2
66.203.215.242	147.237.77.61	Canada	e.cogat.idf.il	ET SCAN NMAP -f -sS	1
46.227.67.172	147.237.77.74	Sweden	law.idf.il	ET SCAN NMAP -sS window 1024	1
211.141.78.56	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
181.51.247.123	147.237.76.30	Colombia	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
106.3.132.14	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.197.206.193	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 4096	1
94.102.48.195	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
66.203.215.242	147.237.77.61	Canada	e.cogat.idf.il	ET SCAN NMAP -sS window 2048	1
46.227.67.172	147.237.77.121	Sweden	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
211.23.156.152	147.237.72.156	Taiwan	aman.idf.il	ET SCAN Potential SSH Scan	1
163.172.169.150	147.237.77.233	United Kingdom	atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
106.3.132.14	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
106.3.132.14	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
97.105.173.114	147.237.0.15	United States	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1

08-27-2016-17:04:00 to 08-27-2016-18:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.239.15.195	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9971
46.239.15.195	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop		drop	100
40.77.169.96	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	15
79.176.94.3	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
106.38.241.105	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	13
93.129.143.6	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
40.77.169.99	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
106.38.241.105	China	147.237.77.74	law.idf.il	drop	SAM rule	drop	5
185.27.105.79	Israel	147.237.72.166	aka.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	3
68.180.230.171	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
79.176.48.135	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.67.226.126	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
79.179.0.151	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
106.38.241.105	China	147.237.76.86	navy.idf.il	drop	SAM rule	drop	1
216.243.31.2	United States	147.237.0.200	m4u.idf.il	drop		drop	1
109.67.30.188	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
106.38.241.105	China	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	1
176.13.235.249	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
216.243.31.2	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
106.38.241.105	China	147.237.72.156	aman.idf.il	drop	SAM rule	drop	1
106.38.241.105	China	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	1
109.253.194.183	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
185.31.136.59	Finland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
106.38.241.105	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
128.232.110.28	United Kingdom	147.237.0.35	akaws.idf.il	drop		drop	1
106.38.241.105	China	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	1
66.240.219.146	United States	147.237.0.35	akaws.idf.il	drop		drop	1
106.38.241.105	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
128.232.110.28	United Kingdom	147.237.76.34	yohalan.idf.il	drop		drop	1

08-27-2016-17:04:00 to 08-27-2016-18:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.2	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	228
109.253.240.126	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
77.139.102.129	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.139.102.129	Block	5
79.177.164.12	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.180.5.188	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
185.27.105.66	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
185.120.126.14	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.64.158.161	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
40.77.169.101	United States	147.237.77.176	matpash.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
40.77.169.97	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
84.109.202.86	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	2
132.74.95.19	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/4/112994.pdf	Block	2
77.138.71.114	France	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
40.77.169.100	United States	147.237.77.176	matpash.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
46.121.16.52	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
40.77.169.100	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
80.246.136.154	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.102.8.197	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/giyus/main/default.asp	Block	1
40.77.169.97	United States	147.237.77.176	matpash.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
84.109.202.86	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 84.109.202.86	Block	1
77.126.31.224	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
66.102.8.253	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/giyus/main/default.asp	Block	1
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
40.77.169.103	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
77.138.42.226	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/	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
40.77.169.98	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
79.181.251.210	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.109.202.86	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/2/	Block	1
66.249.66.197	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-22924-he/idfgdover.aspx	Block	1
80.246.130.48	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	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
5.102.254.88	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/lomdim/	Block	1
109.64.82.215	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.69.44	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/8/638.pdf	Block	1
71.6.146.185	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1

08-27-2016-17:04:00 to 08-27-2016-18:04:00