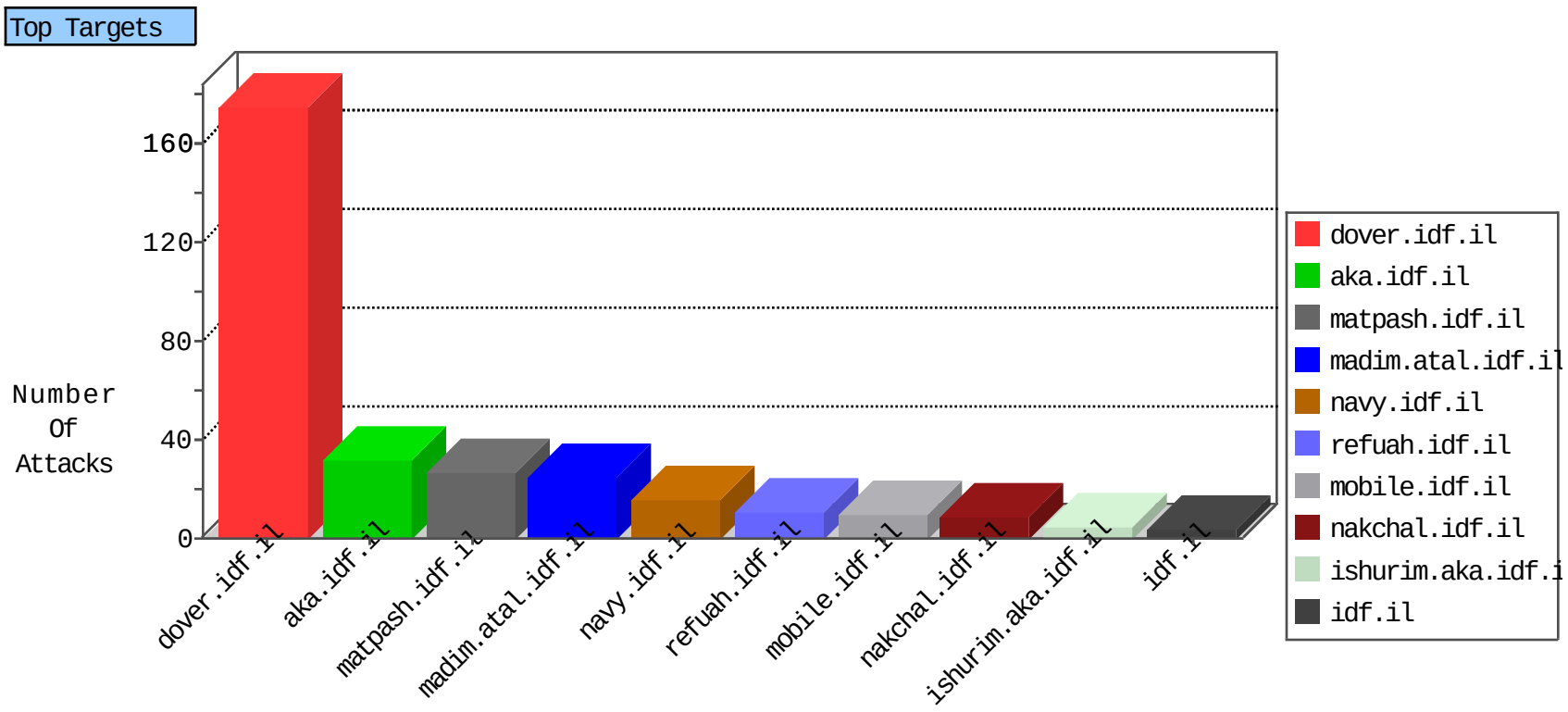
08-25-2016-20:04:00 to 08-25-2016-21:04:00

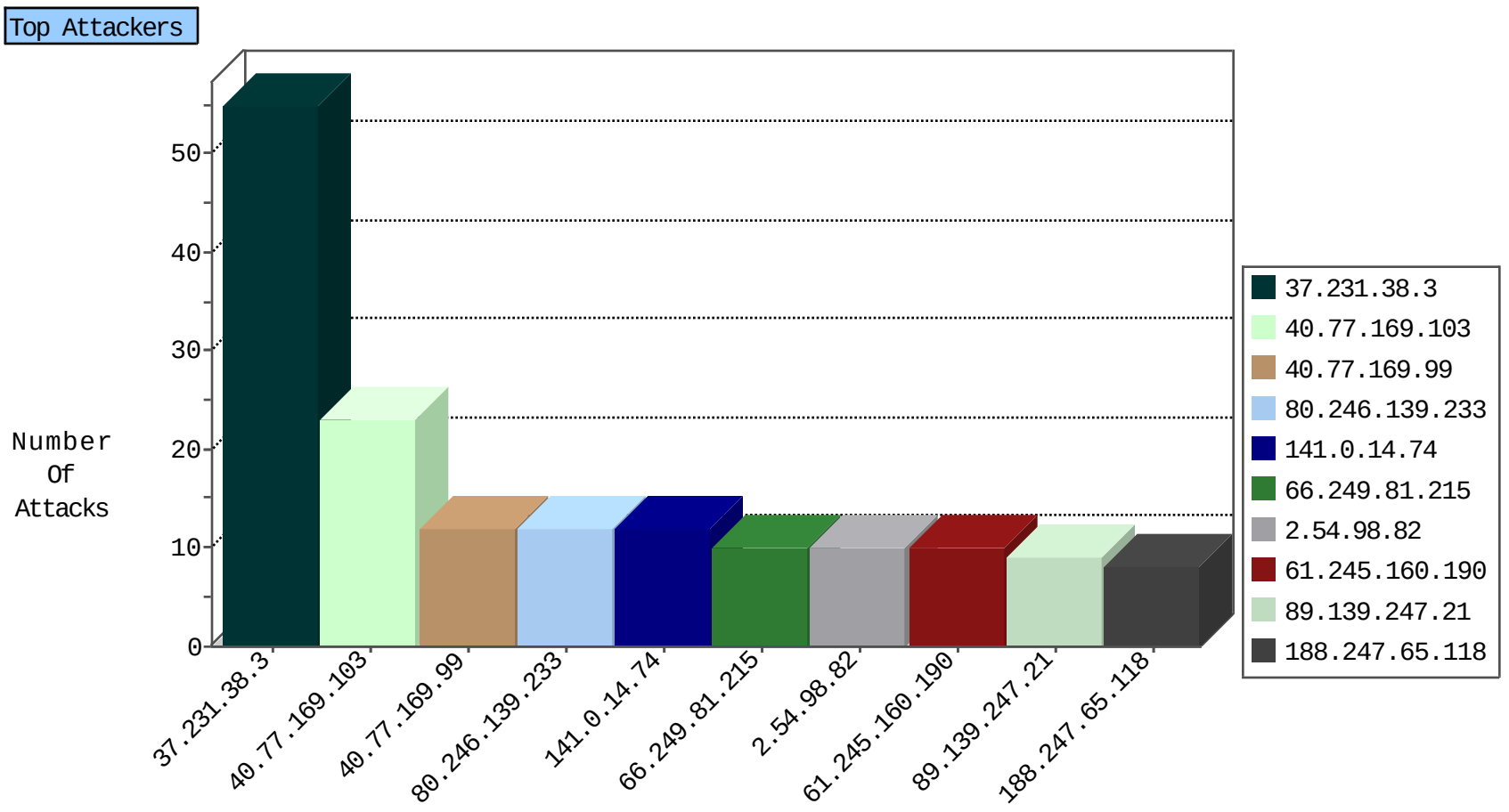
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

08-25-2016-20:04:00 to 08-25-2016-21:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.78.2	Israel	147.237.77.216	dover.idf.il	Black List	drop	1

08-25-2016-20:04:00 to 08-25-2016-21:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
154.241.113.41		147.237.77.216	dover.idf.il	15323: HTTP: User-Agent (MRSPUTNIK)	Block	1

08-25-2016-20:04:00 to 08-25-2016-21:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
177.42.51.73	147.237.8.27	Brazil	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
133.208.21.66	147.237.76.199	Japan	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.245	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
201.238.202.219	147.237.76.30	Chile	himush.idf.il	ET SCAN NMAP -sS window 1024	1
40.117.47.129	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 1024	1
186.115.186.227	147.237.0.33	Colombia	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
183.60.48.25	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
180.97.106.162	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
180.97.106.161	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
133.208.21.66	147.237.77.226	Japan	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
85.64.235.175	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
50.116.123.135	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.74	147.237.72.217	United States	e.idf.il	ET DROP Dshield Block Listed Source	1
37.26.146.186	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.162	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1

08-25-2016-20:04:00 to 08-25-2016-21:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.231.38.3	Kuwait	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
40.77.169.103	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	18
141.0.14.74	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.54.98.82	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	10
89.139.247.21	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	9
61.245.160.190	Sri Lanka	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
100.92.44.163		147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	8
188.247.65.118	Jordan	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
40.77.169.97	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
40.77.169.99	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
185.130.6.49	Lithuania	147.237.76.86	navy.idf.il	drop	SAM rule	drop	6
40.77.169.99	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
86.42.255.206	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
184.151.63.194	Canada	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
40.77.169.103	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
64.233.172.171	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
85.65.55.104	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.53.156.8	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
91.135.104.252	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
85.130.194.23	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	3
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
166.216.165.21	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.67.106.172	Israel	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	3
64.233.172.163	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.53.160.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
41.249.52.208	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
157.55.39.181	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
100.92.251.132		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
141.212.122.74	United States	147.237.0.33	idf.il	drop		drop	1
216.243.31.2	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
169.229.3.91	United States	147.237.76.44	e.refuah.idf.il	drop	SAM rule	drop	1
109.253.141.45	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
85.65.101.235	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.75	United States	147.237.0.33	idf.il	drop		drop	1
169.229.3.91	United States	147.237.76.202	e.halag.idf.il	drop	SAM rule	drop	1
109.253.219.32	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	1
176.13.23.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
27.147.242.21	Bangladesh	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
82.102.169.113	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	1
176.13.229.13	Israel	147.237.72.167	ishurim.aka.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	drop	SAM rule	drop	1
109.253.133.22	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.248.125	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1

08-25-2016-20:04:00 to 08-25-2016-21:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.139.233	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	10
38.126.138.21	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
212.76.117.67	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	4
176.13.224.221	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
176.13.14.208	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
40.77.169.98	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
80.246.140.68	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
212.76.117.67	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 212.76.117.67	Block	2
212.76.117.67	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/8/	Block	2
79.177.181.29	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ishurim.	Block	2
87.71.6.189	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
159.220.74.2	United Kingdom	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 159.220.74.2	Block	1
79.180.44.64	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1
66.249.75.64	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
195.150.96.90	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/idf_in_pictures/hasata/thumb.jpg	Block	1
109.160.226.41	Israel	147.237.77.233	atal.idf.il	Suspicious Response Code	Block	1
66.249.64.105	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/main/smalim/showbig.aspx	Block	1
66.249.75.75	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
109.253.206.46	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$questionUpdate$hiddenUpdateQuestion in www.aka.idf.il/main/giyus/faq.aspx	None	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/size100x0/3294.jpg	Block	1
176.13.21.4	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
40.77.169.100	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
109.253.218.237	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
77.125.64.222	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/size100x0/sip_storage	Block	1
66.249.69.72	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/images/shared/mailthisclose.png	Block	1
85.114.121.88	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.112	Block	1
40.77.169.104	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
157.55.39.179	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	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/1/size100x0/3261.jpg	Block	1
176.85.196.17	Spain	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
5.22.132.71	Israel	147.237.77.176	matpash.idf.il	Parameter Type Violation SearchText in www.cogat.idf.il/938-en/cogat.aspx	Block	1
61.245.160.190	Sri Lanka	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

08-25-2016-20:04:00 to 08-25-2016-21:04:00