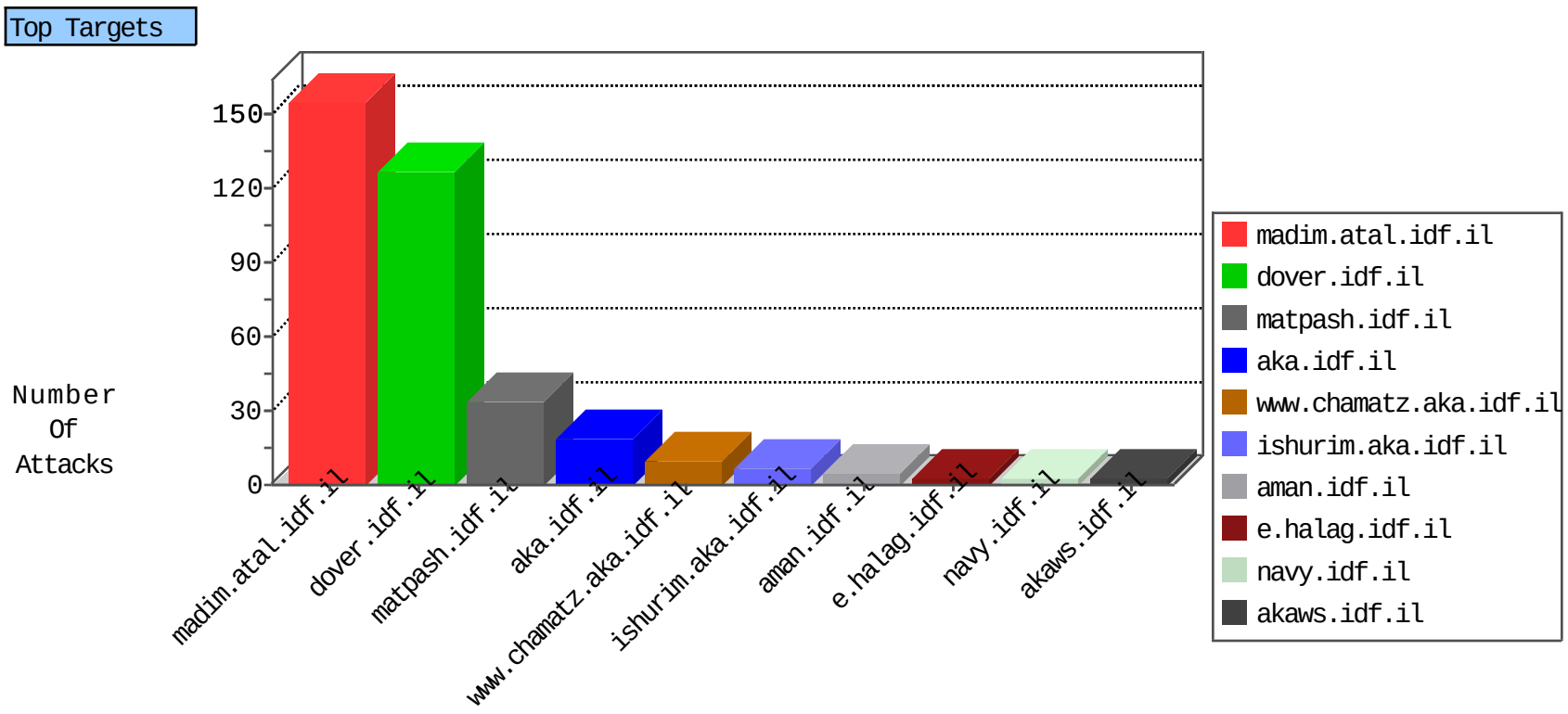
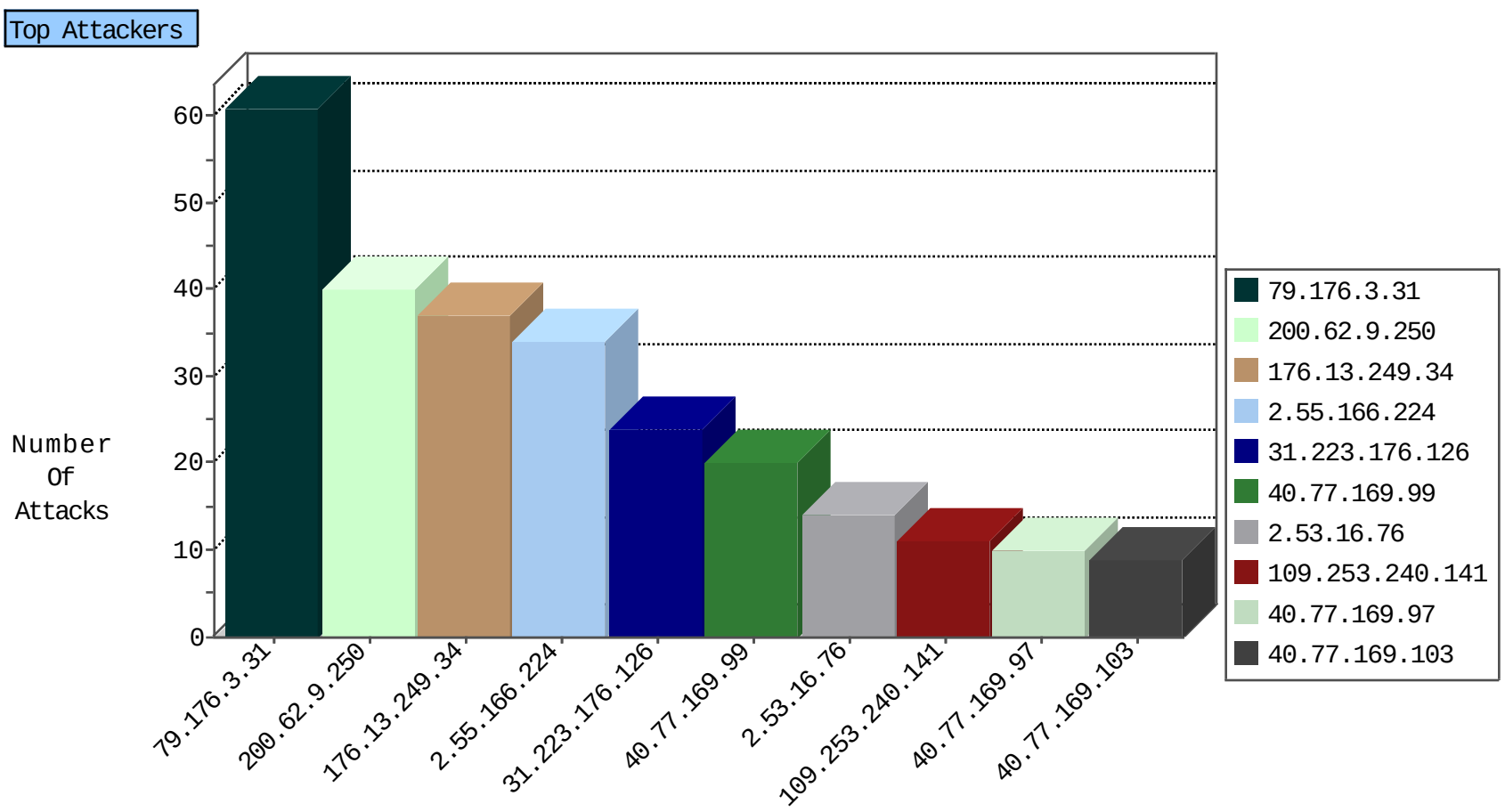
08-25-2016-19:04:08 to 08-25-2016-20:04:08

IDF Under Attack Daily Report





08-25-2016-19:04:08 to 08-25-2016-20:04:08

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	4
82.80.78.2	Israel	147.237.77.176	matpash.idf.il	Black List	drop	2
95.211.187.209	Netherlands	147.237.76.44	e.refuah.idf.il	Black List	drop	1
71.6.135.131	United States	147.237.76.34	yohalan.idf.il	Black List	drop	1
95.211.187.209	Netherlands	147.237.76.42	refuah.idf.il	Black List	drop	1

08-25-2016-19:04:08 to 08-25-2016-20:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.58.86.211	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

08-25-2016-19:04:08 to 08-25-2016-20:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
200.62.9.250	147.237.77.216	Venezuela	dover.idf.il	GPL SCAN nmap TCP	40
74.91.23.106	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
50.116.123.135	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
50.116.123.135	147.237.76.30	United States	himush.idf.il	ET SCAN Potential SSH Scan	1
180.97.106.37	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
103.207.38.14	147.237.76.202	Vietnam	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
74.91.23.106	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 3072	1
66.203.215.242	147.237.8.14	Canada	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
50.116.123.135	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.254	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
201.238.202.219	147.237.77.121	Chile	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
180.97.106.162	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
133.242.4.52	147.237.76.202	Japan	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
74.91.23.106	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1

08-25-2016-19:04:08 to 08-25-2016-20:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
31.223.176.126	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	24
40.77.169.99	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	14
40.77.169.97	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	10
109.253.240.141	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	10
40.77.169.103	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	9
40.77.169.99	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	6
176.13.249.34	Israel	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.29.226.100	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
176.13.11.5	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.218.52	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
100.92.103.213		147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	2
61.245.160.190	Sri Lanka	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
109.253.204.214	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
40.77.169.101	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
85.130.176.160	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
212.179.210.101	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.228.65	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
100.92.76.46		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
216.218.206.116	United States	147.237.0.200	m4u.idf.il	drop		drop	1
46.119.127.129	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
176.13.239.4	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	1
163.172.38.173	United Kingdom	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	1
46.243.173.2	Russian Federation	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
109.253.147.70	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.7.21	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

08-25-2016-19:04:08 to 08-25-2016-20:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.176.3.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	61
2.55.166.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
176.13.249.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
2.53.16.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
66.249.85.221	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	8
66.249.85.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	7
66.249.85.224	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	4
176.13.14.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.216.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.240.65	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 109.253.240.65	Block	2
77.124.42.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.108.175.47	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	2
186.141.198.35	Argentina	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
79.178.98.56	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/homepage/homepage.aspx	Block	2
40.77.169.100	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
68.180.228.231	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-ar/cogat.aspx	Block	2
212.159.169.79	United Kingdom	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.167	Israel	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/general/general.aspx	Block	1
157.55.39.143	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/main/drushim/misrot.aspx	Block	1
2.53.59.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
79.179.9.131	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/main/giyus/general.aspx	Block	1
40.77.169.102	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
178.63.101.134	Germany	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/rights/asp/info.asp	Block	1
213.200.47.136	Ukraine	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.249.69.14	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
157.55.39.181	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.53.163.147	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.102.9.1	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
185.120.125.11	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
109.253.240.141	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
159.220.74.2	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/patzar/news/default.asp	Block	1
85.64.255.47	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.102.9.54	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	1
136.243.67.234	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/rights/asp/info.asp	Block	1
66.249.76.70	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
31.13.100.117	Ireland	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/&usg=afqjcnhrohl-5mv1-e2hp5hs1kbggyhg4g&sig2=ukqzmmppevtg2t4w5ig5jw	Block	1
85.130.176.160	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.76.117.67	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
66.249.64.58	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
157.55.39.93	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.179.9.131	Israel	147.237.72.167	ishurim.aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.112	Block	1

08-25-2016-19:04:08 to 08-25-2016-20:04:08