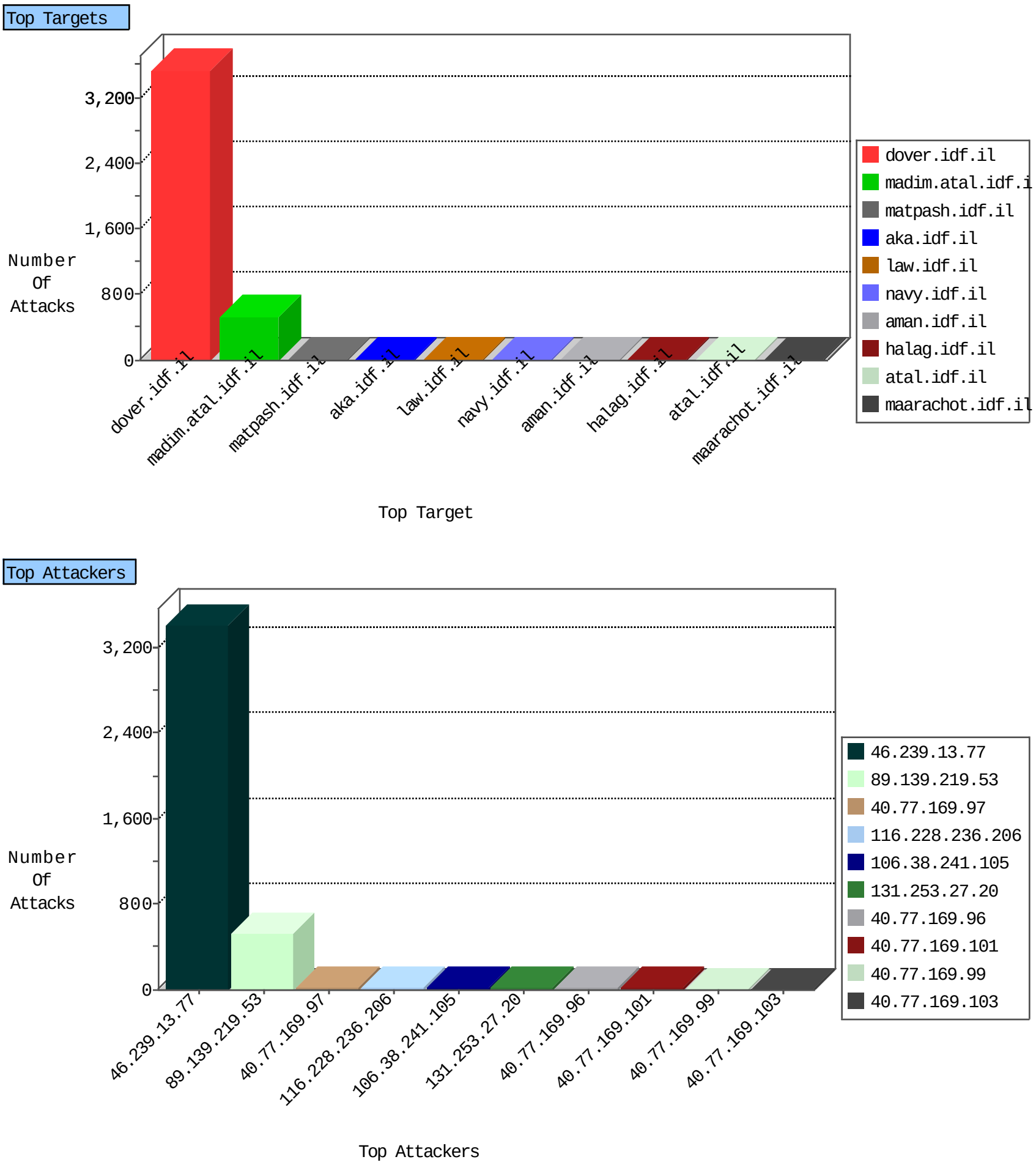
08-27-2016-08:04:03 to 08-27-2016-09:04:03

IDF Under Attack Daily Report



08-27-2016-08:04:03 to 08-27-2016-09:04:03

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	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	1
137.74.157.88	Hong Kong	147.237.76.44	e.refuah.idf.il	Black List	drop	1
59.172.23.26	China	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
82.80.78.2	Israel	147.237.72.166	aka.idf.il	Black List	drop	1

08-27-2016-08:04:03 to 08-27-2016-09:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

08-27-2016-08:04:03 to 08-27-2016-09:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
116.228.236.206	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	3
116.228.236.206	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	2
116.228.236.206	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
116.228.236.206	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
116.228.236.206	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
116.228.236.206	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
163.172.169.150	147.237.76.199	United Kingdom	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
116.228.236.206	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
163.172.169.150	147.237.0.200	United Kingdom	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
116.228.236.206	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
163.172.169.150	147.237.0.17	United Kingdom	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
116.228.236.206	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
122.72.53.188	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
116.228.236.206	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
116.228.236.206	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
116.228.236.206	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
116.228.236.206	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
116.228.236.206	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
116.228.236.206	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN Potential SSH Scan	1
116.228.236.206	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
91.224.160.106	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
198.52.97.92	147.237.77.74	United States	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
116.228.236.206	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
163.172.169.150	147.237.0.200	United Kingdom	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
116.228.236.206	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
5.39.222.253	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.0.33	United Kingdom	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
116.228.236.206	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
123.206.73.185	147.237.0.19	China	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
116.228.236.206	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
116.228.236.206	147.237.77.243	China	mobile.idf.il	ET SCAN Potential SSH Scan	1
116.228.236.206	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1

08-27-2016-08:04:03 to 08-27-2016-09:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.239.13.77	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3170
46.239.13.77	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop		drop	250
40.77.169.97	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
40.77.169.96	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	15
40.77.169.101	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	9
40.77.169.99	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	8
40.77.169.99	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
106.38.241.105	China	147.237.76.86	navy.idf.il	drop	SAM rule	drop	7
40.77.169.101	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
177.185.192.98	Brazil	147.237.77.233	atal.idf.il	drop	SAM rule	drop	6
91.219.122.2	Poland	147.237.77.74	law.idf.il	drop	SAM rule	drop	6
106.38.241.105	China	147.237.72.156	aman.idf.il	drop	SAM rule	drop	6
106.38.241.105	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
40.77.169.103	United States	147.237.77.234	halag.idf.il	drop	SAM rule	drop	5
40.77.169.103	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
40.77.169.96	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
156.211.113.202	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.76.83	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.46	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.222	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
40.77.169.97	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
106.38.241.105	China	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	1
106.38.241.105	China	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	1
106.38.241.105	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
106.38.241.105	China	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	1

08-27-2016-08:04:03 to 08-27-2016-09:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.139.219.53	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	530
131.253.27.20	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	21
40.77.169.98	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
37.26.147.206	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
40.77.169.102	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
66.249.64.105	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.105	Block	2
46.121.65.43	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 46.121.65.43	Block	2
46.121.65.43	Israel	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	2
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/doctrine/doctrine.stm.1986	Block	1
66.102.6.3	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	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
40.77.169.100	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
169.1.208.239	South Africa	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
68.180.228.231	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-he/cogat.aspx	Block	1
199.30.16.190	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
77.138.236.183	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
207.46.13.110	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.64.105	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/main/smalim/showbig.aspx	Block	1

08-27-2016-08:04:03 to 08-27-2016-09:04:03