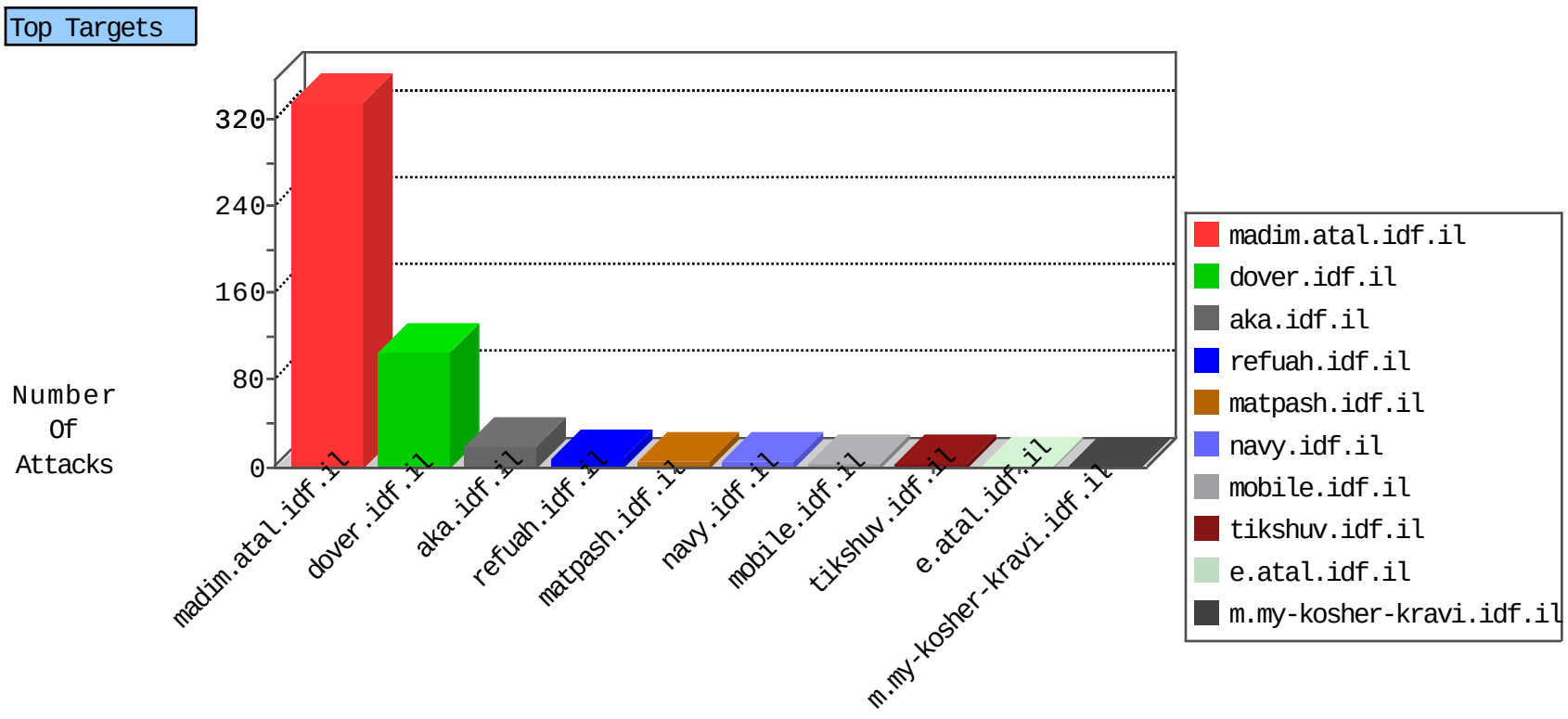
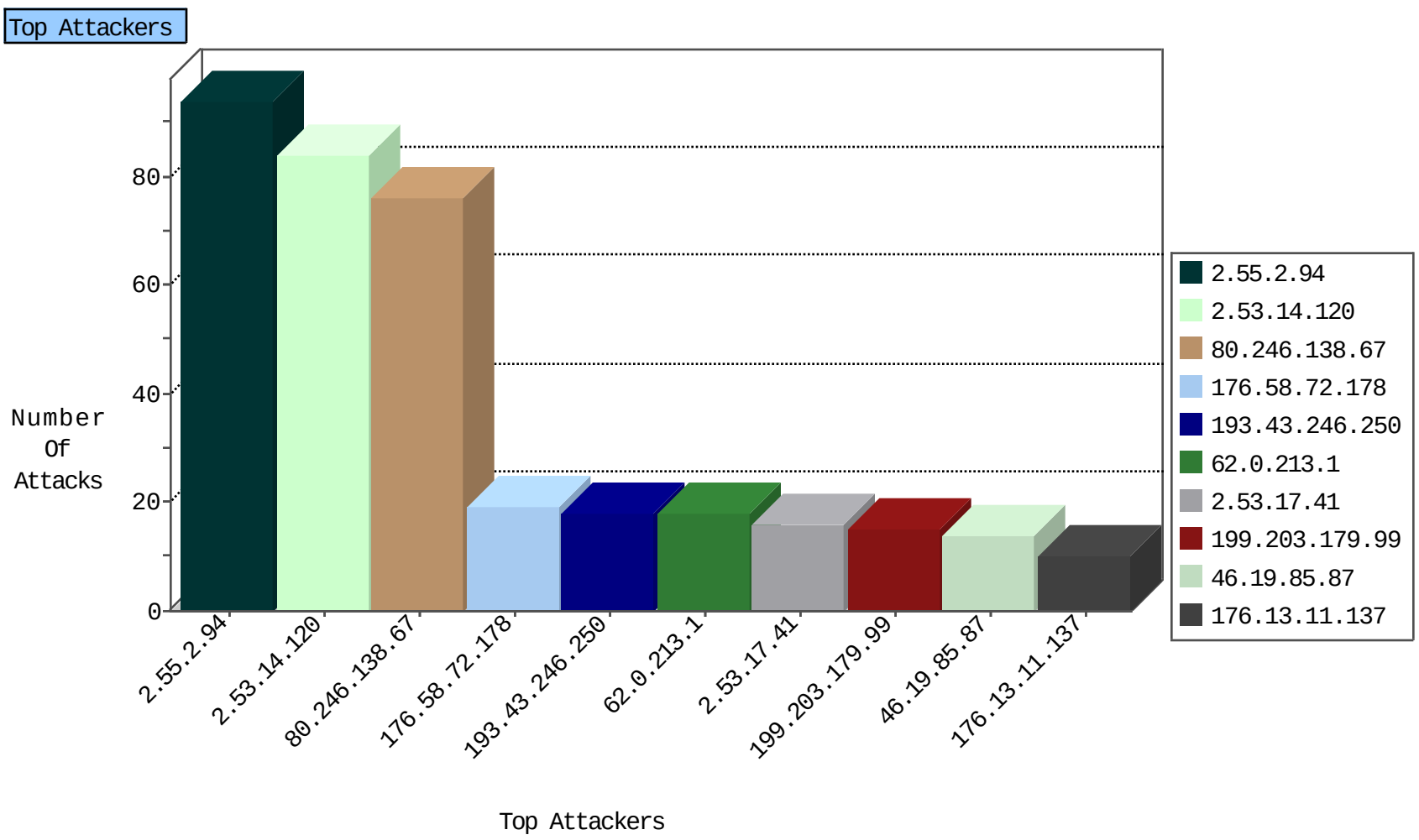
08-21-2016-08:04:09 to 08-21-2016-09:04:09

IDF Under Attack Daily Report





08-21-2016-08:04:09 to 08-21-2016-09:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.3.68	Israel	147.237.77.243	mobile.idf.il	DOSS-SSL-ClearText	drop	3
123.59.59.52	China	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	2
61.147.103.179	China	147.237.76.201	e.atal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
115.230.125.146	China	147.237.77.226	www.chamatz.aka.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
82.80.78.2	Israel	147.237.77.216	dover.idf.il	Black List	drop	1
89.248.168.21	Netherlands	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
37.26.146.217	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
93.158.200.86	Netherlands	147.237.76.86	navy.idf.il	Black List	drop	1
221.214.216.69	China	147.237.76.38	e.e.meitav.idf.il	Invalid TCP Flags	drop	1

08-21-2016-08:04:09 to 08-21-2016-09:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

08-21-2016-08:04:09 to 08-21-2016-09:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
162.213.1.246	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	2
212.25.88.141	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.235.254.181	147.237.0.34	Turkey	tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
104.227.112.24	147.237.0.19	United States	madim.atal.idf.il	WEB-CGI redirect access	1
84.108.136.240	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.44.38	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.201.225.149	147.237.77.212	Ukraine	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
109.235.254.181	147.237.0.34	Turkey	tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
109.235.254.181	147.237.0.34	Turkey	tikshuv.idf.il	ET SCAN NMAP -f -sS	1
87.236.194.161	147.237.76.197	Czech Republic	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
23.94.86.8	147.237.0.19	United States	madim.atal.idf.il	WEB-CGI redirect access	1

08-21-2016-08:04:09 to 08-21-2016-09:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
62.0.213.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
199.203.179.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
176.58.72.178	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
64.62.219.157	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
64.62.219.158	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
176.58.72.178	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
212.143.225.47	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
80.87.205.246	Russian Federation	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	2
80.87.205.246	Russian Federation	147.237.0.15	kosher-kravi.idf.il	drop	First packet isn't SYN	drop	2
64.62.219.156	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
80.87.205.246	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	drop	First packet isn't SYN	drop	2
80.87.205.246	Russian Federation	147.237.0.17	m.my-kosher-kravi.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.200	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.244.177	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
68.180.228.185	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
195.110.35.144	France	147.237.72.156	aman.idf.il	drop	SAM rule	drop	1
109.253.146.41	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
195.110.35.144	France	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
109.253.156.76	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
216.218.206.124	United States	147.237.0.35	akaws.idf.il	drop		drop	1
5.29.197.22	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	1
109.253.214.85	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
184.105.247.204	United States	147.237.0.33	idf.il	drop		drop	1
5.29.197.22	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
212.143.120.209	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
176.13.17.110	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.2.94	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	94
2.53.14.120	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	84
80.246.138.67	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	76
2.53.17.41	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	16
46.19.85.87	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
176.13.11.137	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	10
80.246.136.216	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
2.53.135.69	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
77.138.173.220	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	5
2.53.62.121	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
81.218.241.25	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	4
109.253.144.205	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.53.39.234	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.3.68	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.147.189	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.0	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
66.249.65.177	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.177	Block	3
109.64.97.23	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.25	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
2.55.188.50	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
87.69.140.25	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
37.26.146.166	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
131.253.26.228	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
64.62.219.156	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
5.29.75.57	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
93.190.152.161	Europe	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
77.139.91.194	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
131.253.26.242	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.53.129.182	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/size100x0/2414.jpg	Block	1
65.55.211.247	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
10.30.5.57	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 10.30.5.57	Block	1
193.169.70.108	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 193.169.70.108	Block	1
98.234.185.53	United States	147.237.76.42	refuah.idf.il	Unauthorized Method POST for 147.237.76.42/	Block	1
79.178.9.129	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
157.55.39.110	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/default.aspx	Block	1
10.30.5.57	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/yohalan	Block	1
212.199.118.19	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 212.199.118.19	Block	1
80.246.130.235	Israel	147.237.76.42	refuah.idf.il	Suspicious Response Code	Block	1
173.196.142.146	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
84.95.208.186	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
68.180.228.231	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1956-he/cogat.aspx	Block	1
37.26.146.139	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1