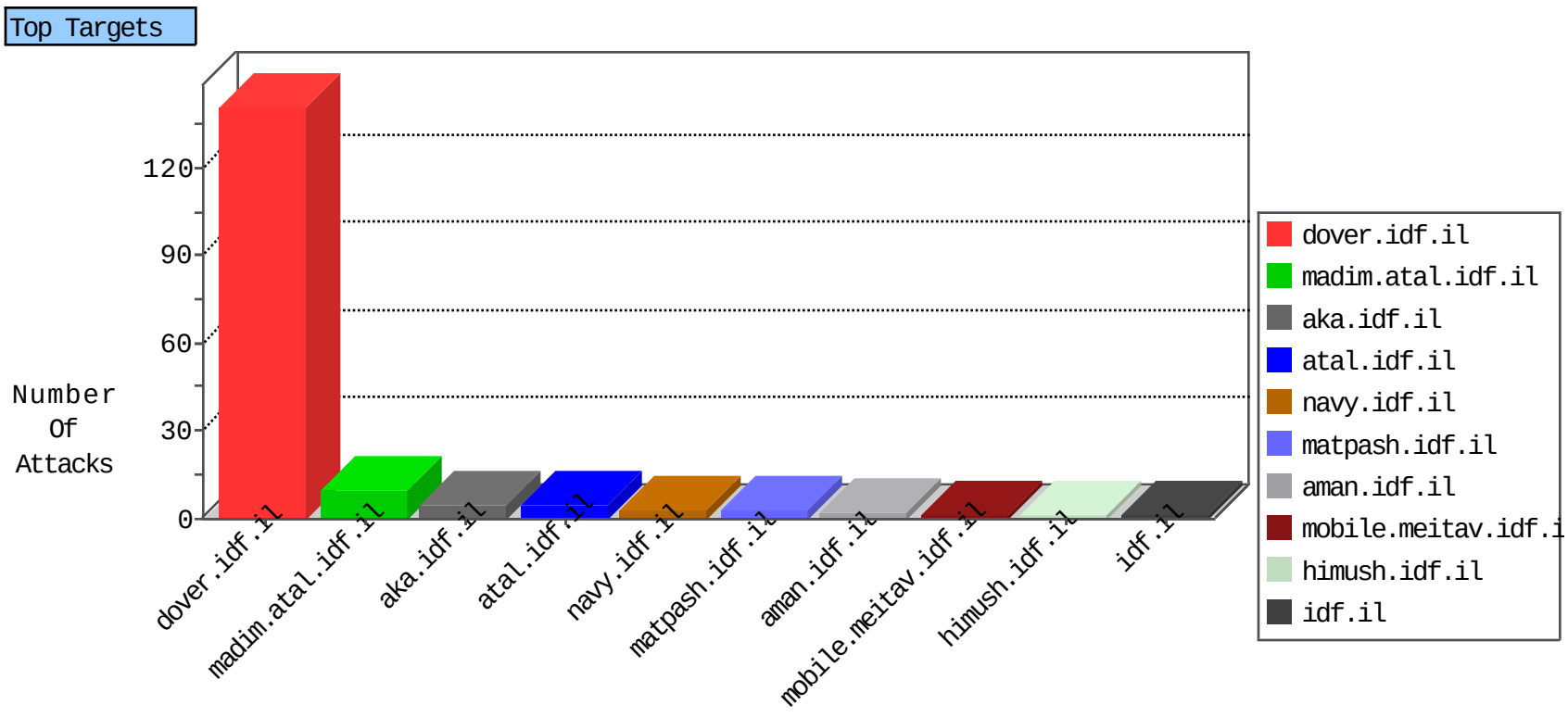
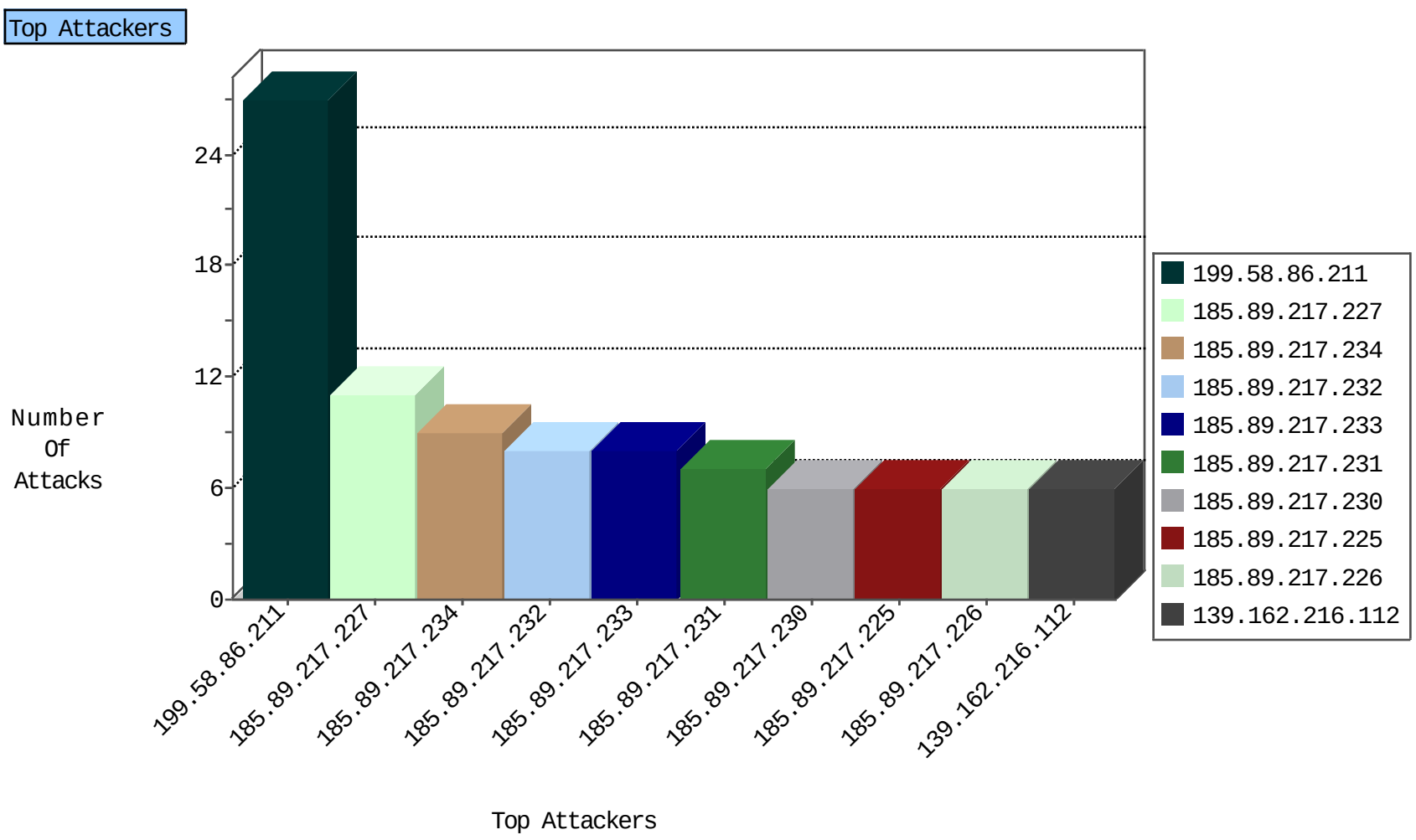
08-22-2016-07:04:07 to 08-22-2016-08:04:07

IDF Under Attack Daily Report





08-22-2016-07:04:07 to 08-22-2016-08:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.171.7.67	Netherlands	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
192.249.66.247	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
82.80.78.2	Israel	147.237.77.176	matpash.idf.il	Black List	drop	1
89.248.168.21	Netherlands	147.237.76.30	himush.idf.il	Black List	drop	1
69.172.200.236	United States	147.237.77.205	prisha.idf.il	Invalid TCP Flags	drop	1
89.248.168.21	Netherlands	147.237.76.202	e.halag.idf.il	Black List	drop	1

08-22-2016-07:04:07 to 08-22-2016-08:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
164.132.161.96	Italy	147.237.72.156	aman.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
1.179.134.194	Thailand	147.237.72.166	aka.idf.il	13076: HTTP: Apache Struts 2 OGNL Command Injection Vulnerability	Block	1
51.255.65.65	France	147.237.76.200	eitan.aka.idf.i	C1000146: HTTP: AhrefBot crawler	Block	1

08-22-2016-07:04:07 to 08-22-2016-08:04:07

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	5

08-22-2016-07:04:07 to 08-22-2016-08:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
199.58.86.211	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
185.89.217.227	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
185.89.217.232	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
185.89.217.233	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
185.89.217.225	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.89.217.231	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.89.217.226	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.89.217.234	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
199.58.86.211	United States	147.237.77.216	dover.idf.il	drop		drop	6
185.89.217.230	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.89.217.228	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
199.58.86.211	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
193.227.170.194	Lebanon	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	4
185.89.217.235	Netherlands	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
5.22.129.251	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	3
78.19.224.39	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
157.55.39.110	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
83.28.208.139	Poland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
113.35.251.98	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
199.30.25.118	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.92.114	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
173.252.74.104	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
173.252.74.108	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
121.214.179.141	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
184.105.247.246	United States	147.237.0.33	idf.il	drop		drop	1

08-22-2016-07:04:07 to 08-22-2016-08:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.130.14	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
2.53.7.233	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
185.89.217.234	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
213.57.195.103	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
217.132.131.94	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
77.139.11.9	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/yohalan/main/main.asp	Block	2
2.53.17.128	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
173.186.135.99	United States	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
37.26.147.151	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	1
207.46.13.20	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.180.35.148	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-login.php	Block	1
185.89.217.227	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/9/71539.pdf	Block	1
185.89.217.231	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/5/71565.pdf	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
85.65.216.87	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1462-he/atal.aspx	Block	1
185.89.217.235	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.180.35.148	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1

08-22-2016-07:04:07 to 08-22-2016-08:04:07