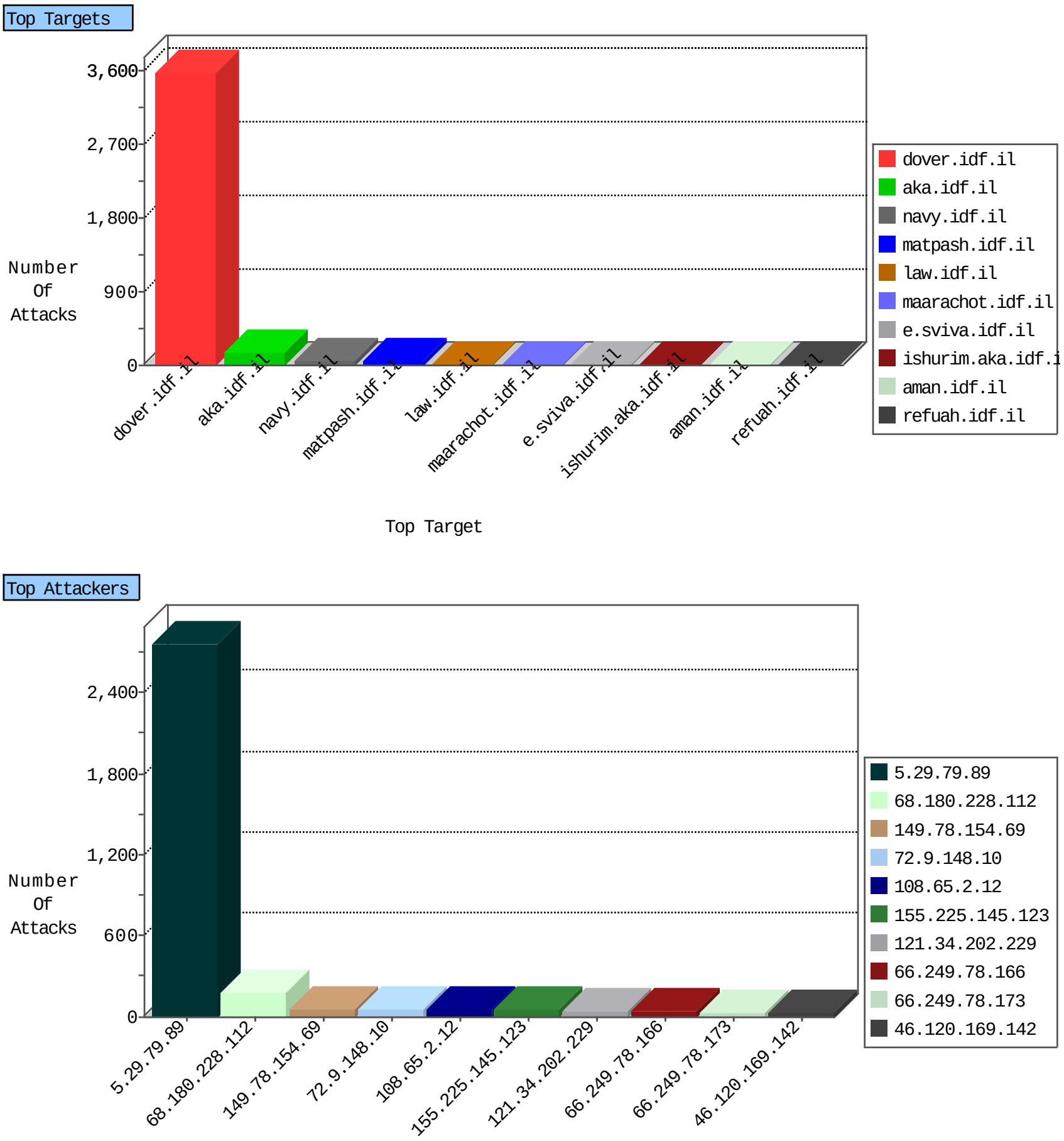
10-27-2015-05:04:05 to 10-27-2015-06:04:05

IDF Under Attack
Daily Report



10-27-2015-05:04:05 to 10-27-2015-06:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
146.185.239.100	Russian Federation	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	drop	1
45.63.1.137		147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
185.117.72.113		147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
96.44.156.198	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
96.44.156.198	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

10-27-2015-05:04:05 to 10-27-2015-06:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-27-2015-05:04:05 to 10-27-2015-06:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	**Signature**	**Count**

10-27-2015-05:04:05 to 10-27-2015-06:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.29.79.89	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2766
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
155.225.145.123	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
46.120.169.142	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
150.101.191.105	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
40.77.167.35	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
80.246.130.49	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
99.57.138.198	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
79.179.192.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.66.26.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
50.157.32.176	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
108.65.2.12	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
157.55.39.13	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
40.77.167.35	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
66.249.78.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
157.55.39.7	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
77.126.250.9	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
40.77.167.37	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.64.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
207.46.13.104	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
157.55.39.7	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.78.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
80.246.130.49	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
176.106.226.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
126.12.13.229	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
65.19.138.33	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
108.228.14.170	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
85.16.128.245	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
188.247.77.128	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.65.24.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.64.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
52.23.156.32	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
84.108.175.24	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.178.97.188	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
40.77.167.33	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
81.218.234.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

10-27-2015-05:04:05 to 10-27-2015-06:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	168
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	56
108.65.2.12	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation SearchText in www.cogat.idf.il/938-en/cogat.aspx	Block	42
121.34.202.229	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/default.aspx	Block	42
46.121.214.39	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	28
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/robots.txt	Block	14
45.35.71.179		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	14
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_text.asp	Block	14
77.126.250.9	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 77.126.250.9	Block	14
66.249.64.245	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	14
157.55.39.209	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/giyus/qanda/default.asp	None	14
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/elram	Block	14
84.110.34.29	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	14
66.249.67.247	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on 147.237.77.170/robots.txt	Block	14
188.165.15.205	France	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/164-he/patzar.aspx	Block	14
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	14
85.93.91.84	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_text.asp	Block	11

10-27-2015-05:04:05 to 10-27-2015-06:04:05