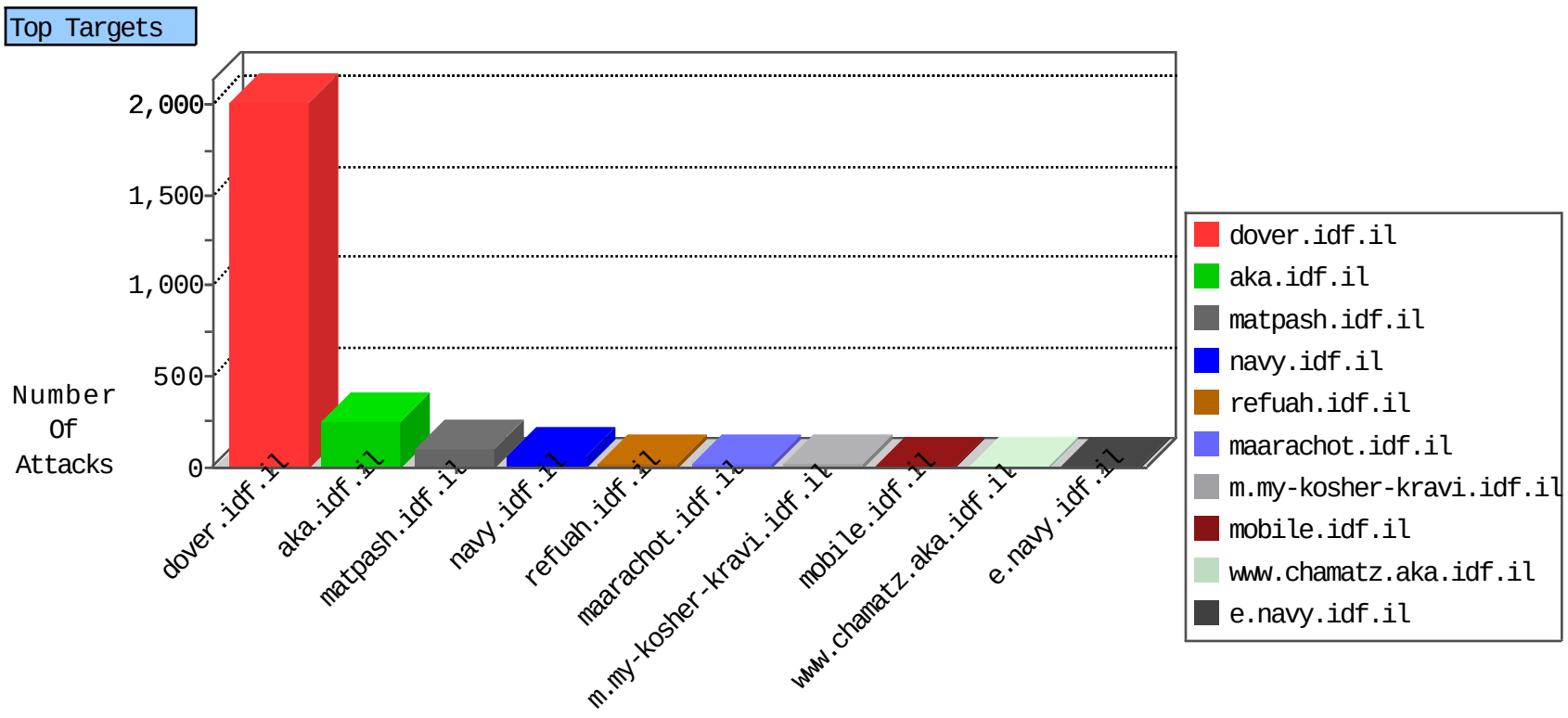
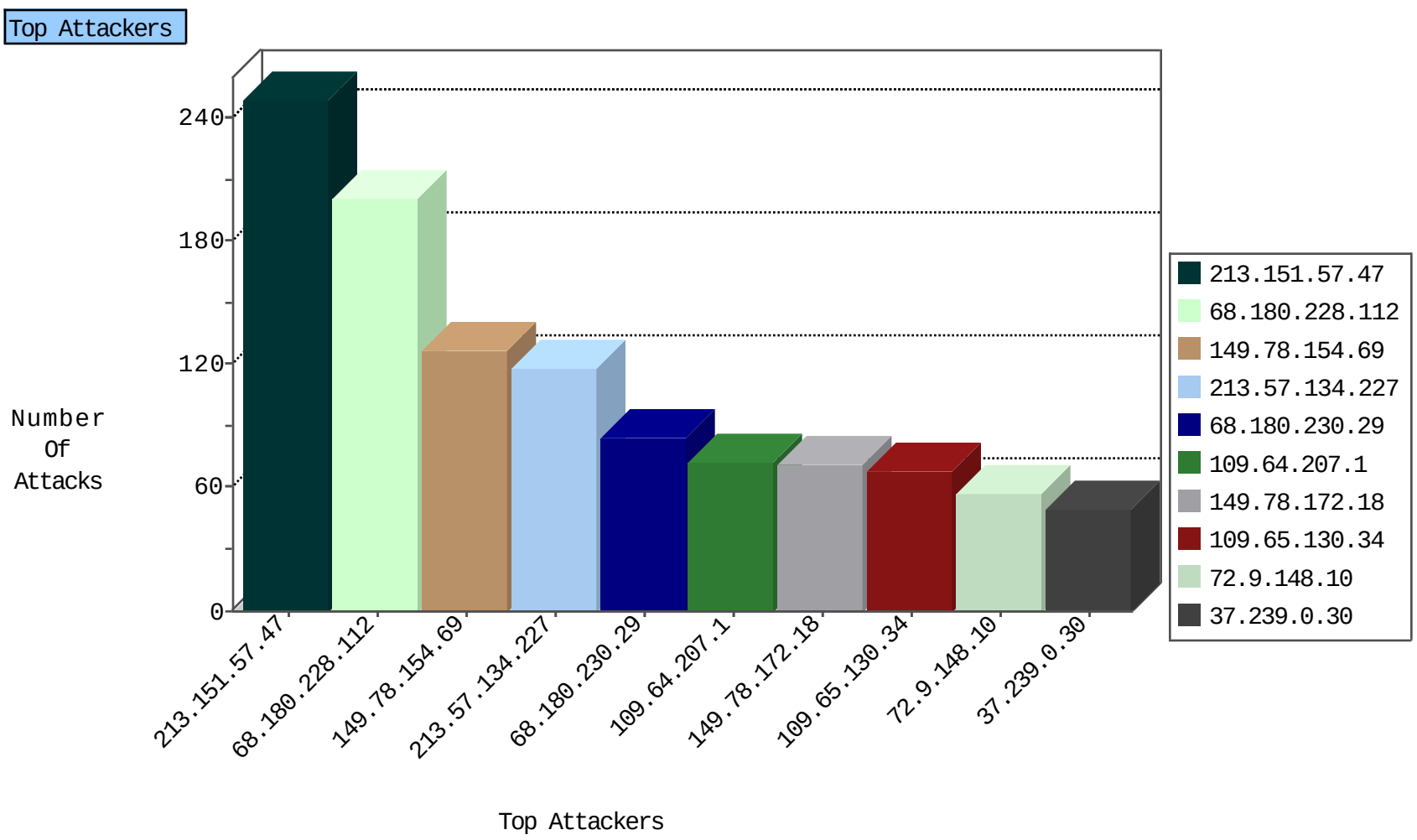
10-27-2015-01:04:05 to 10-27-2015-02:04:05

IDF Under Attack Daily Report





10-27-2015-01:04:05 to 10-27-2015-02:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.151.57.47	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
176.13.7.164	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
89.248.172.98	Netherlands	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1

10-27-2015-01:04:05 to 10-27-2015-02:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
74.208.66.220	United States	147.237.76.31	nakchal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	2
74.208.66.220	United States	147.237.76.31	nakchal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

10-27-2015-01:04:05 to 10-27-2015-02:04:05

Top Attackers In IDS

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

10-27-2015-01:04:05 to 10-27-2015-02:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
213.151.57.47	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	245
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	127
213.57.134.227	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	105
149.78.172.18	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	71
24.135.201.246		147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	48
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	47
213.136.56.41	Sweden	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	43
79.183.113.118	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	40
174.57.78.19	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	40
109.64.207.1	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	37
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	30
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	29
69.112.208.131	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	27
79.182.19.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	SAM rule	drop	27
66.249.78.173	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
80.178.213.48	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	23
176.13.18.91	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
65.94.23.12	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
40.77.167.37	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
66.249.78.159	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
207.46.13.178	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
212.179.90.106	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
191.115.37.67	Chile	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
212.199.182.150	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
109.66.41.148	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
109.64.207.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
85.54.75.14	Spain	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
74.101.165.28	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
109.64.207.1	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
66.102.7.233	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
217.147.92.69	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
65.55.210.119	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
157.55.39.255	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.65.130.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
82.145.209.106	Europe	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
67.236.214.195	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
176.12.142.100	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
89.155.86.155	Portugal	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
69.171.228.123	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
206.248.134.124	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
207.46.13.178	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
2.52.141.132	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
207.46.13.144	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
173.254.216.66	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
40.77.167.33	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
69.171.228.119	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8

10-27-2015-01:04:05 to 10-27-2015-02:04:05

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	154
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-he/cogat.aspx	Block	84
109.65.130.34	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	56
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
37.239.0.30	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	42
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	14
54.157.28.22	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to www.m.my-kosher-kravi.idf.il/	Block	14
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mmmmmmm=d507fb8emmmmmmm_d507fb8e	Block	14
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	14
2.52.3.243	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
66.249.67.134	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on 147.237.77.170/robots.txt	Block	14
188.143.232.14	Russian Federation	147.237.77.176	matpash.idf.il	Parameter Type Violation fromDate in www.cogat.idf.il/901-en/cogat.aspx	Block	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	14
2.52.175.222	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	14
79.182.19.206	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/viewpniot.aspx	None	14
66.249.67.224	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	14
188.143.232.19	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-14146-he/dover.asp	Block	14
5.41.201.126	Romania	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	14
84.109.226.204	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	14
66.249.75.16	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	14
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/6/size220x0/17396.jpg	Block	14

10-27-2015-01:04:05 to 10-27-2015-02:04:05