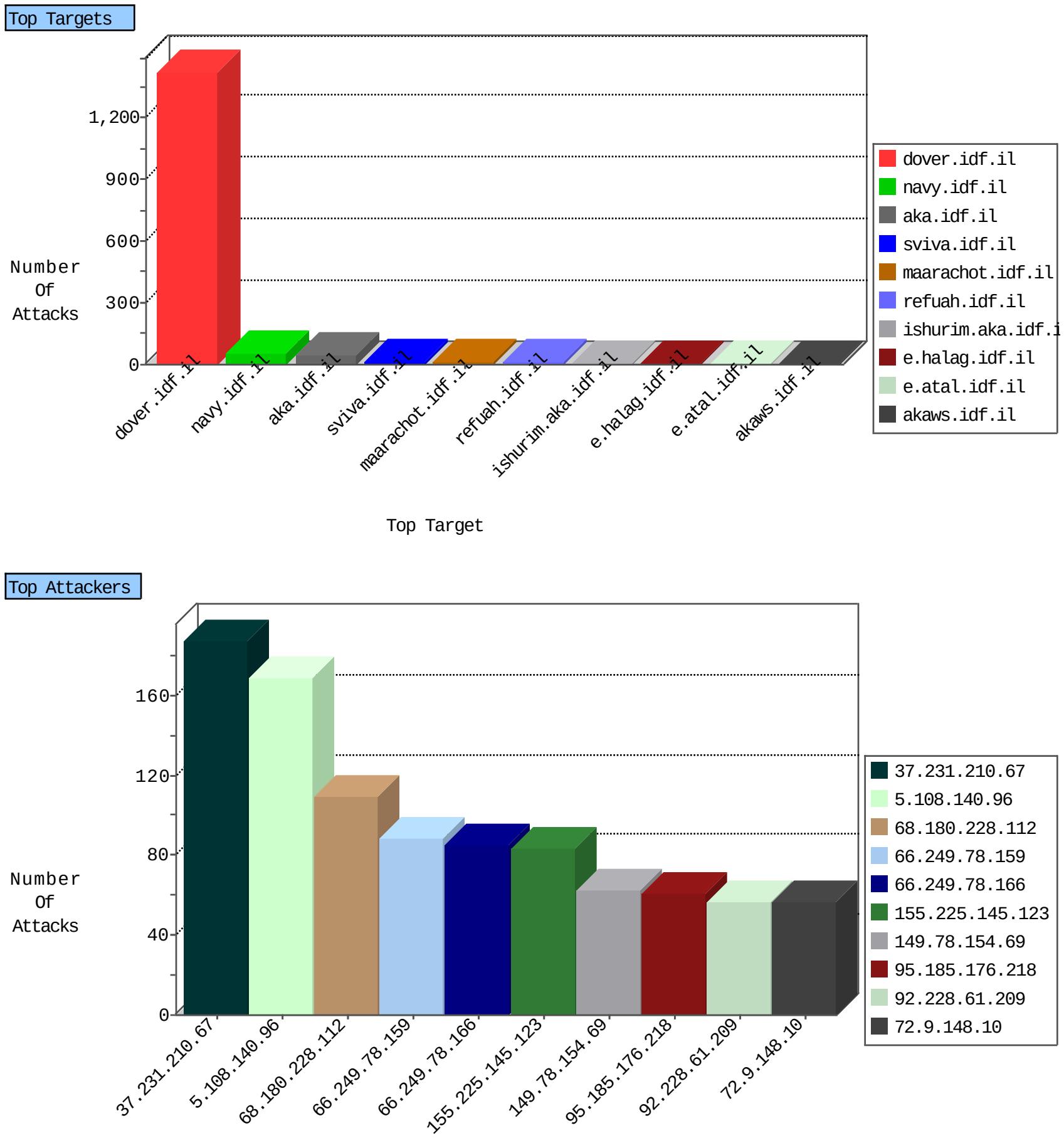
10-27-2015-04:04:02 to 10-27-2015-05:04:02

IDF Under Attack Daily Report



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

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
204.42.253.130	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	2
45.63.1.137		147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
112.175.228.11	Korea, Republic of	147.237.72.217	e.idf.il	Invalid TCP Flags	drop	1
45.63.1.137		147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
185.117.72.113		147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
45.63.1.137		147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
45.63.1.137		147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1

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

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
45.79.109.226		147.237.72.167	ishurim.aka.idf.il	3624: HTTP: SQL Injection (SELECT)	Block	1

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

Top Attackers In IDS

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

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

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.231.210.67	Kuwait	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	188
5.108.140.96	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	169
155.225.145.123	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
95.185.176.218	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
92.228.61.209	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
188.161.246.21	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
66.65.39.35	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
68.96.59.120	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
37.140.188.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
66.249.78.166	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
98.227.176.223	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
46.117.217.98	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
40.77.167.37	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.103.102	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
73.24.182.255	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
24.93.244.230	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
24.217.34.218	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
70.48.36.156	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.65.24.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
40.77.167.33	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
92.228.61.209	Germany	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.120.2.136	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
139.162.216.112	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
142.105.57.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.78.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.78.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
95.185.176.218	Saudi Arabia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.22.131.187	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
157.55.39.26	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
95.185.176.218	Saudi Arabia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
2.54.38.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.139.131	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
50.187.57.105	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
95.185.176.218	Saudi Arabia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
37.142.68.98	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
5.22.131.187	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

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

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	Suspicious Response Code	Block	96
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
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	42
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	28
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
188.165.15.162	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8870-he/refuah.aspx	Block	14
66.249.67.143	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	14
142.91.231.106	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/print_bottom.asp	Block	14
207.46.13.35	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	14
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
142.91.231.106	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	14
77.237.138.51	Czech Republic	147.237.77.235	sviva.idf.il	Unauthorized URL Access to /	Block	14
184.173.183.173	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1415-10812-he/dover.aspx&usg=alkjrhieipnzunr58pdkqm3uzz9_ejsh6a	Block	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover	Block	14
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	14
104.194.26.204	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	14
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	14
188.138.17.205	France	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	14
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	14
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	14
104.194.26.204	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	14

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